EdgeADC

EdgeADC 管理指南

软件版本

5.0.0

目录

文件属性

文件编号：2 .0。3.19.25.12.03

文件创建日期：19 March 2025

文件最后编辑日期 19 March 2025

文件作者：杰伊-萨沃尔

文件 最后编辑人

文件：EdgeADC - 版本 5.0.0

文件免责声明

由于产品版本的不同，本手册的屏幕截图和图形可能与您的产品略有不同。Edgenexus 保证尽一切合理努力确保本文档中的信息完整准确。Edgenexus 对任何错误不承担任何责任。如有需要，Edgenexus 将在今后的版本中对本文档中的信息进行更改和更正。

版权

商标

Edgenexus 支持

如果您对本产品有任何技术问题，请发送支持邮件至： support@edgenexus.io。

导言

您之所以阅读本指南，是因为您打算部署 Edgenexus EdgeADC 并以高效、经济的方式对基于服务器的应用程序进行负载平衡。

EdgeADC 是围绕一个高度安全的引擎构建的，它具有高可扩展性、安全性、高性能和非常易于使用的管理界面。这些因素确保了您所部署的系统能够实现最佳的拥有成本。

本文件的目的

编写本文档的目的是让您可以使用其简易的网络界面管理 EdgeADC。本文档详细介绍了各项功能及其配置，希望能满足您对 EdgeADC 的配置要求。

本文件面向谁?

本文档面向具备网络知识，特别是协议、应用程序和服务器知识的人员。

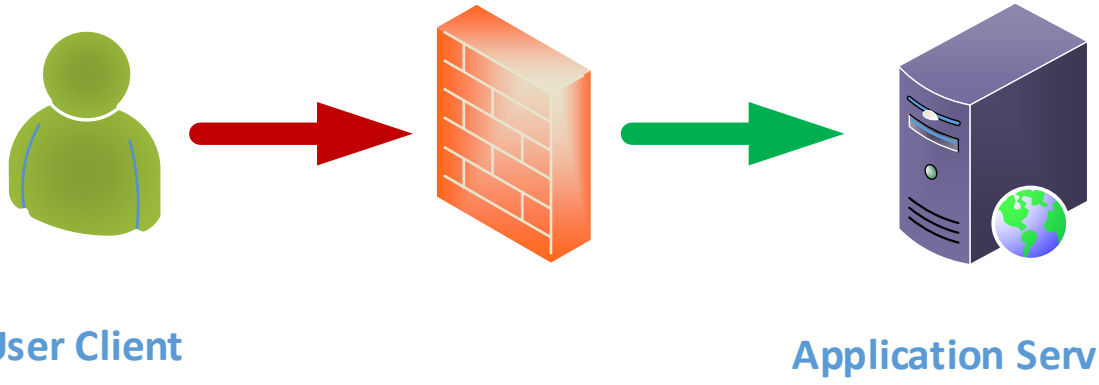
负载平衡 101

什么是负载平衡器或 ADC？

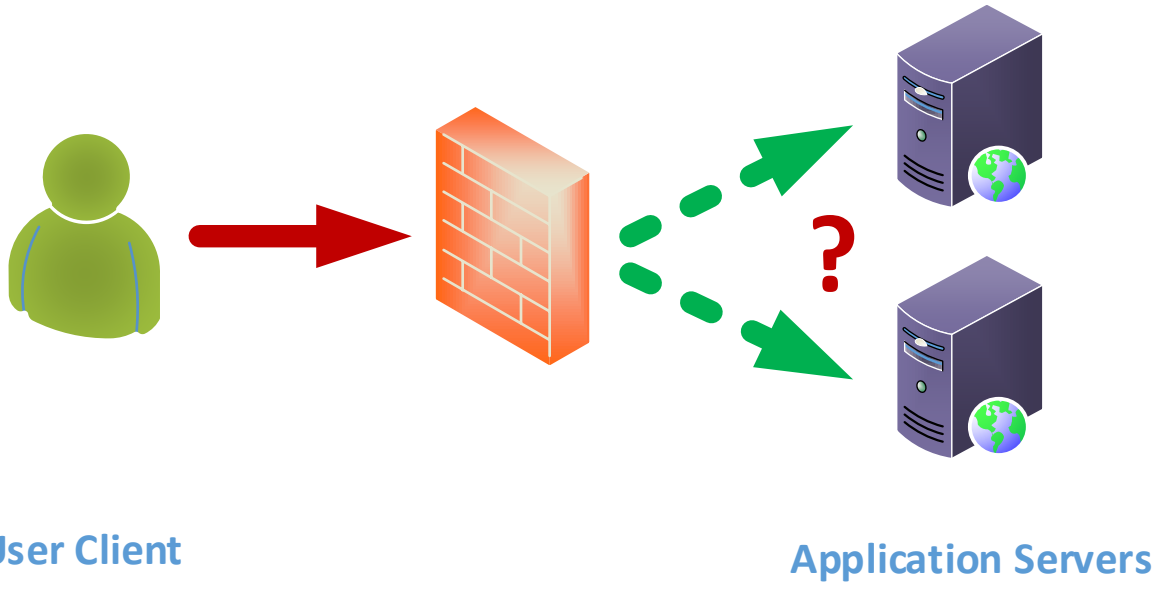
负载平衡器已经有了巨大的发展，其引擎中内置的智能比以前要多得多。如今，它们通常被称为应用交付控制器或 ADC。

在了解什么是负载平衡器或 ADC 之前，我们需要先了解 IT 人员和用户的问题。那么，让我们举个例子。

- 某公司有一个网络应用程序要发布到互联网上。该应用程序托管在一台网络服务器上，数据存放在另一台数据库服务器上。



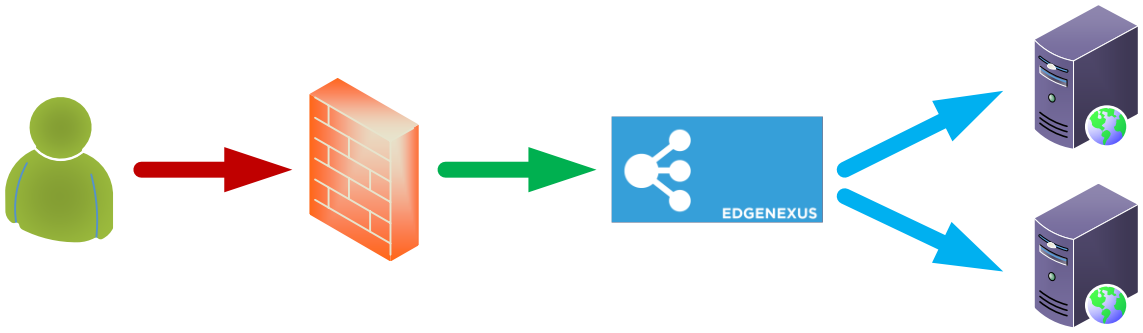
- 本服务器使用的 IP 地址为 1.2.3.4。
- 访问应用程序的客户数量在不断增加，有些人指出应用程序的性能正在下降。
- 对服务器进行的分析表明，访问服务器的流量大幅增加，而且还在继续增加。
- 因此，决定再增加一台服务器来托管应用程序。
- 新的第二台服务器使用 1.2.3.5 的 IP 地址。
- 问题是如何将客户端导向新的和当前的服务器，以分担负载，并确保用户的会话在第一个登录的服务器上得到维护。



- 答案就是负载平衡器或 ADC。

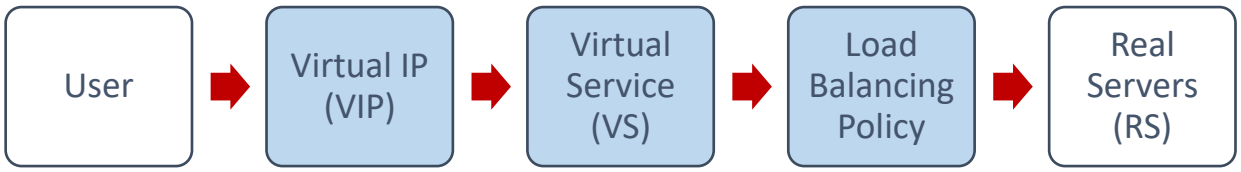
现在是解决方案。

- 我们在两个应用服务器前放置了一个 ADC。

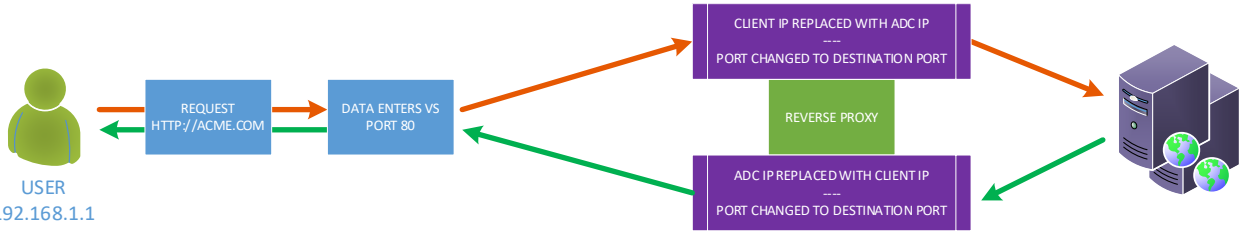


User Client **ADC** **Application Servers**

- ADC 的对外 IP 地址为 1.2.3.6，防火墙会将请求 NAT 重定向到该地址，而不是之前的 1.2.3.4。
- 接收请求的 ADC IP 称为 VIP，配置称为虚拟服务。
- ADC 将接收来自客户端用户的请求，并使用负载平衡策略将其反向代理到真正的服务器，同时监控应用服务器的健康状况，以确保效率。



- ADC 根据使用中的负载平衡策略、负载性质以及应用服务器的状态，平衡服务器的流量。
- 来自服务器的流量将通过 ADC 以相反的方向发送回客户端。
- 由于反向代理的性质，服务器和客户端之间是匿名的。



- 反向代理技术可确保最佳的安全级别。

VIP 和虚拟服务 (VS) 解读

从本质上讲，VIP 是为在 EdgeADC 上使用而定义的 IP 地址，允许用户访问与之绑定的服务。这就是 VIP 的基本含义。由于 EdgeADC 的工作方式，VIP 无需与真实服务器位于同一子网，这种网络地址转换方法使该技术非常安全，不会受到试图访问内部服务器的黑客攻击。

注意： VIP 的 IP 地址不能与管理 IP 使用的 IP 地址相同。

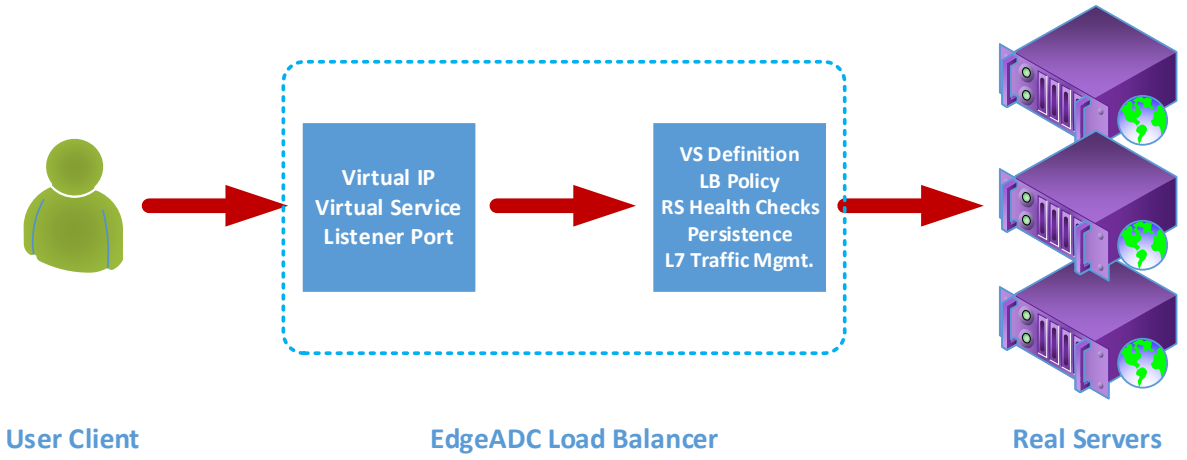
虚拟服务是 EdgeADC 代理和负载平衡技术的核心。虚拟 IP 是虚拟服务向网络和世界发布的地址，它负责监听希望使用其服务的应用程序的客户端的流量和请求。

当客户访问 VS 时，VS 将被配置为对流量执行多种操作，包括但不限于

- 客户端连接的代理
- 具体功能包括压缩、加速、负载平衡、流量检测等。
- 将客户请求转发到虚拟服务负载平衡策略中定义的目标服务器。

您可以将 VS 视为与 EdgeADC 为准备数据请求而监听的 IP 地址（VIP）相匹配。当进行标准 TCP 或 HTTP 配置时，客户端将连接到 VIP，EdgeADC 将根据构成 VS 的定义处理请求。处理完成后，EdgeADC 将把流量发送到指定的真实服务器上。

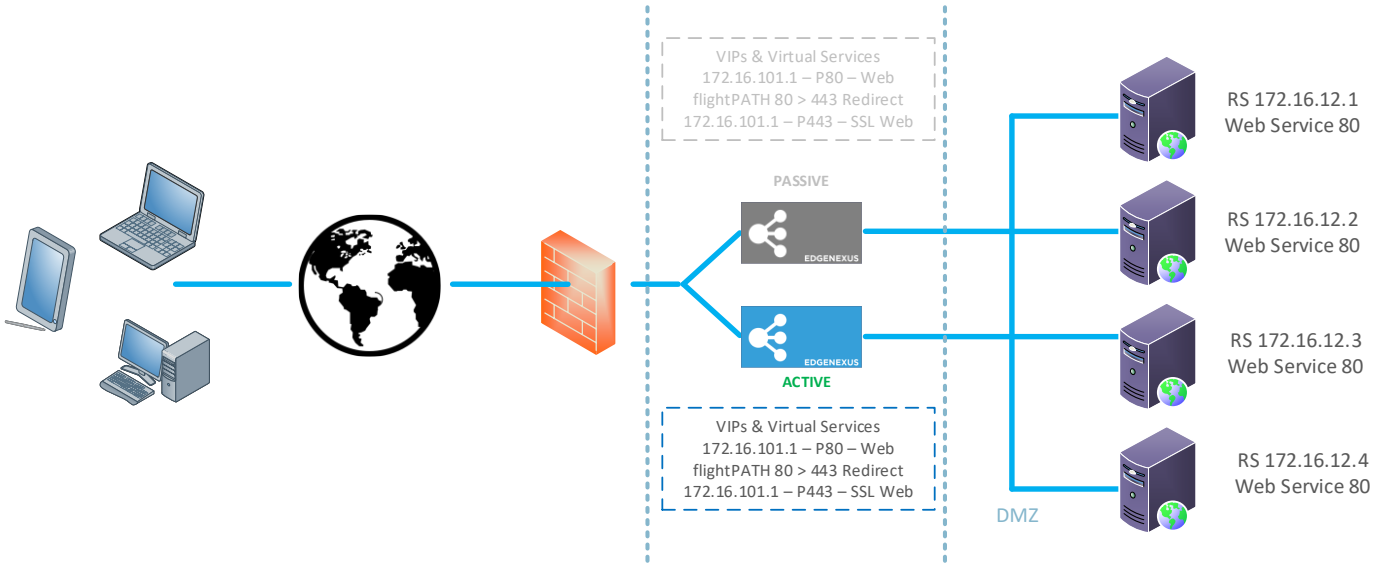
VS 在典型配置中接收连接和数据，然后使用 EdgeADC 中的反向代理引擎终止或代理。然后，EdgeADC 继续打开与真实服务器的新连接，并继续发送数据。当真实服务器响应请求时，EdgeADC 将使用类似的反向路径向客户端发送响应，这取决于真实服务器负载平衡选项卡中连接选项的设置。



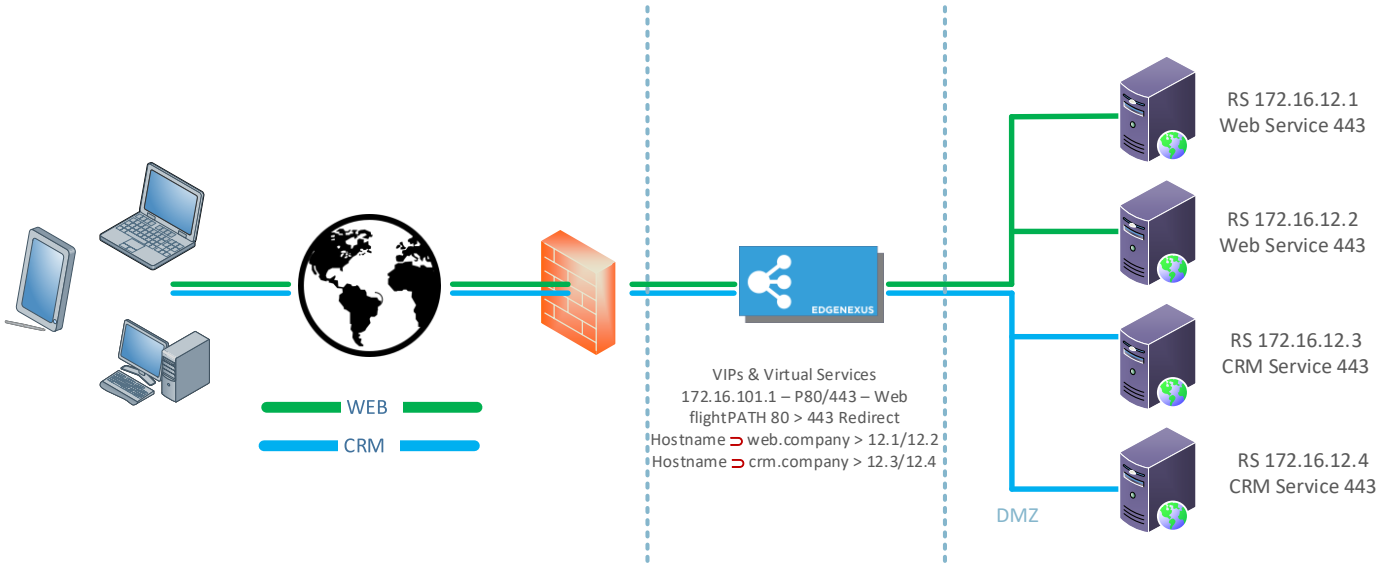
虚拟服务定义由一个 IP 地址（VIP）和一组端口组成，这些端口使用各种协议作为不同服务的入口点。

例如，您需要对一系列网络服务器进行负载平衡，以提供弹性。现在，让我们假设将使用 https://myweb.company.com 通过 HTTPS 安全通信访问这些系统。

如果查看这种配置的定义，就会发现它由一个 VIP 和两个条目组成，一个用于 80 端口，另一个用于 443 端口。端口 80 VIP 将附加一个 flightPATH 规则，强制将流量转换为 HTTPS。端口 443 的第二个条目将把流量发送到其下定义的真实服务器上。同样，你也可以在同一 VIP 下设置其他服务，以平衡邮件服务器或其他应用服务器的流量。



对于功能较弱的 ADC，使用相同端口的服务需要不同的 VIP，但 ADC 及其 flightPATH 系统允许您在使用相同端口的多个服务中使用单个 VIP。因此，你可以让两个都使用 443 访问且主机名不同的应用程序使用一个 VIP。下面是一个示例。



EdgeADC 的系统非常灵活，可以定义非常复杂的功能配置。

什么是负载平衡服务类型?

负载平衡服务类型包括用于在服务器池之间智能分配或负载平衡流量的算法和方法。ADC 提供的方法和算法取决于被负载平衡的服务器上使用的服务类型或应用程序，也取决于网络和服务器的使用状态。需要注意的是，选择使用的负载平衡服务类型也取决于通过 ADC 发送的流量水平。因此，当流量吞吐量或负载较低时，负载平衡服务类型可以很简单。但当负载较大时，您可能需要选择更复杂的类型，以便更有效地向后端服务器分配负载。

EdgeADC 提供以下负载平衡服务类型。

DICOM	第 4 层 UDP	RPC
文件传输协议	第 4 层 tcp/udp	RPC/ADS
HTTP(S)	DNS	RPC/CA/PF
IMAP	POP3	SMTP
第 4 层 TCP	RDP	GSLB

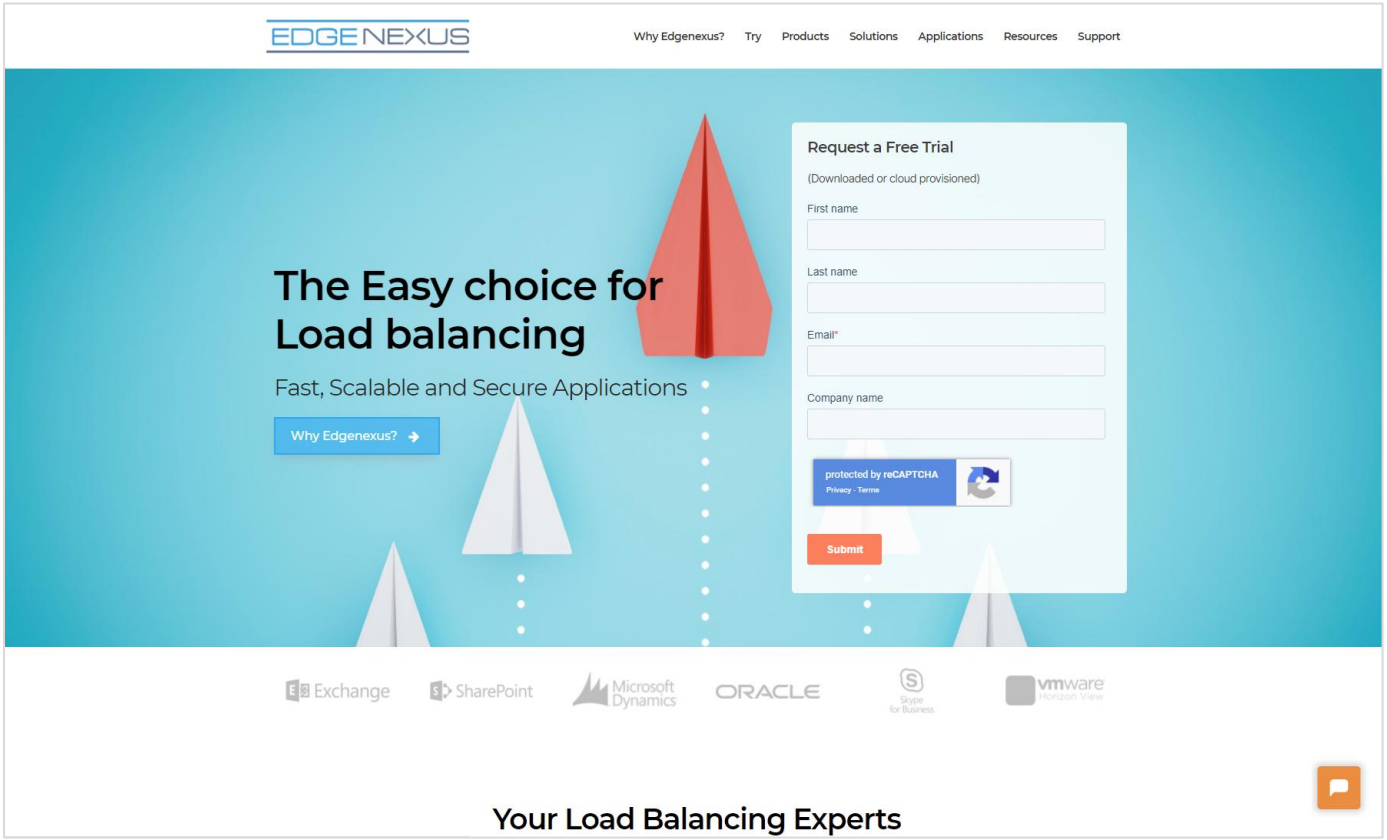
旅程的开始

下载 EdgeADC

安装前，第一步是下载适合您环境的 EdgeADC。

我们提供适用于大多数虚拟化环境的版本，以及直接安装在裸机硬件上的 ISO 版本。

第一步是填写 Edgenexus 网站上的评估表，网址是 https://www.edgenexus.io/products/load-balancer/free-trial/。



过程很简单，填写表格并提交后，您将进入下载页面，选择适合您环境的正确图像。

EdgeADC 版本适用于以下虚拟化系统：

- VMware ESX
- 微软 Hyper-V
- Citrix XenServer
- Nutanix
- KVM

您还可以选择使用 Microsoft Azure 或 Amazon AWS 市场版本在云中进行测试。

如果您选择下载软件进行内部安装，您将收到带有内置 14 天试用许可证的 EdgeADC。我们建议您联系 sales@edgenexus.io，申请一个 30 天的许可证密钥，并启用所有功能。

安装

安装 ng EdgeADC

EdgeADC (ADC) 可安装在多种平台目标上，每种目标都需要安装程序，注册下载后即可使用。

这些是现有的各种安装模式。

- VMware ESXi
- KVM
- Citrix Xen
- Nutanix AHV
- 微软 Hyper-V
- 甲骨文虚拟机
- Proxmox （使用 OVA）
- 裸机硬件 ISO

用于托管 ADC 的虚拟机的大小取决于用例场景和数据吞吐量。

安装到 VMware ESXi

ADC 支持在 VMware ESXi 5.x 及以上版本上安装。

- 使用下载电子邮件中提供的相应链接下载最新的 ADC 安装 OVA 包。
- 下载完成后，请解压到 ESXi 主机或 SAN 上的合适目录中。
- 在 vSphere 客户端中，选择文件：部署 OVA/OVF 模板。
- 浏览并选择保存文件的位置；选择 OVF 文件并单击**下一步**
- ESX 服务器会要求输入设备名称。键入合适的名称，然后单击 **NEXT**
- 选择 ADC 设备运行所在的数据存储。
- 选择一个有足够空间的数据存储，然后单击 **NEXT**
- 然后，您将收到有关产品的信息；点击**下一步**
- 点击**下一步。**
- 将文件复制到数据存储后，就可以安装虚拟设备了。

启动 vSphere 客户端查看新的 ADC 虚拟设备。

- 右键单击 VA，转到电源 > 开机
- 然后 VA 将启动，控制台上将显示 ADC 启动屏幕。

安装 VMXNET3 接口

支持 VMXnet3 驱动程序，但需要先更改网卡设置。

注意 - 切勿升级 VMware-tools

在新导入的虚拟机（从未启动）上启用 VMXNET3 接口

1. 从虚拟机中删除两个网卡
2. 右键单击列表中的虚拟机，选择升级虚拟硬件（不要启动 VMware 工具安装或更新，只执行硬件升级）。
3. 添加两个网卡并将其选为 VMXNET3
4. 使用标准方法启动 VA。它可以与 VMXNET3

在已运行的虚拟机上启用 VMXNET3 接口

1. 停止虚拟机（CLI 关闭命令或 GUI 关闭电源）
2. 获取两个网卡的 MAC 地址（记住网卡在列表中的顺序）
3. 从虚拟机中删除两个网卡
4. 升级虚拟机硬件（不要启动 VMware 工具安装或更新，只执行硬件升级）
5. 添加两个网卡并将其选为 VMXNET3
6. 根据步骤 2 为新网卡设置 MAC 地址
7. 重新启动 VA

我们支持将 VMware ESXi 作为生产平台。 出于评估目的，您可以使用 VMware Workstation 和 Player。

请参阅 "**首次启动配置** "部分继续操作。

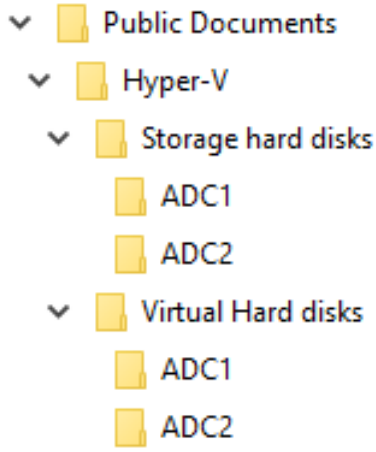
在 Microsoft Hyper-V 上安装

Edgenexus ADC 虚拟设备可轻松安装在 Microsoft Hyper-V 虚拟化框架内。本指南假定您已正确指定和配置 Hyper-V 系统和系统资源，以适应 ADC 及其负载平衡架构。

请注意，每台设备都需要一个唯一的 MAC 地址。

- 将下载的 Hyper-V 兼容 ADC-VA 文件解压到本地计算机或服务器。

- 打开 Hyper-V 管理器。
- 创建一个包含 ADC VA "虚拟硬盘 "的新文件夹和另一个包含 "存储硬盘 "的新文件夹，例如 C:\Users\Public\Documents\Hyper-V\Virtual hard disks\ADC1 和 C:\Users\Public\Documents\Hyper-V\Storage hard disks\ADC1
- **注意**：每个虚拟 ADC 实例安装都需要为 Virtual hard disks\ 和 Storage hard disks\ 创建新的 ADC 特定子文件夹，如下所示：



- 将解压缩的 EdgeADC .vhd 文件复制到上面创建的 "存储硬盘 "文件夹中。
- 在 Hyper-V Manager 客户端，右键单击服务器并选择 "导入虚拟机"。
- 浏览到包含之前提取的已下载 ADC VA 映像文件的文件夹
- 选择虚拟机--选中要导入的虚拟机并单击下一步
- 选择虚拟机--选中要导入的虚拟机并单击下一步
- 选择导入类型 - 选择 "**复制虚拟机（创建新的唯一 ID）**"，单击下一步
- 为虚拟机文件选择文件夹 - 目的地可以保留为 Hyper-V 默认设置，也可以选择不同的位置
- 找到虚拟硬盘 - 浏览并选择上面创建的虚拟硬盘文件夹，然后单击下一步
- 选择存储虚拟硬盘的文件夹 - 浏览并选择之前创建的存储硬盘文件夹，然后单击下一步
- 验证 "完成导入向导摘要 "窗口中的详细信息是否正确，然后单击 "完成"。
- 右键单击新导入的 **ADC** 虚拟机并选择启动

注意：根据 HTTP://SUPPORT.MICROSOFT.COM/KB/2956569，您应忽略 "已降级（需要升级集成服务）"状态信息，该信息可能会在 VA 启动后显示如下。无需采取任何行动，服务未降级

- 在虚拟机初始化过程中，您可以右键单击虚拟机条目并选择连接.....然后您将看到 EdgeADC 控制台。

- 配置网络属性后，VA 将重新启动并显示 VA 控制台的登录信息。

请参阅 "**首次启动配置** "部分继续操作。

在 Citrix XenServer 上安装

ADC 虚拟设备可安装在 Citrix XenServer 上。

- 将 ADC OVA ALB-VA 文件解压缩到本地计算机或服务器。
- 打开 Citrix XenCenter Client。
- 在 XenCenter 客户端中，选择 **"文件：导入"。**
- 浏览并选择 **OVA** 文件，然后点击 **"下一步打开"。**
- 根据要求选择虚拟机创建位置。
- 选择要安装的 XenServer，然后单击 **"NEXT"。**
- 根据要求选择用于放置虚拟磁盘的存储存储库 (SR)。
- 选择一个有足够空间的 SR，然后点击 **"NEXT"。**
- 映射虚拟网络接口。两个接口都将显示为 Eth0；但请注意，底部的接口是 Eth1。
- 为每个接口选择目标网络，然后单击**下一步**
- **请勿**勾选 "使用操作系统修复"。
- 点击 **"下一步**
- 选择要用于临时传输虚拟机的网络接口。
- 选择管理界面，通常是网络 0，并将网络设置保留为 DHCP。请注意，如果没有可用于传输的 DHCP 服务器，则必须分配静态 IP 地址详情。否则将导致导入提示 "连接中"，然后提示 "失败"。点击 **"下一步**
- 然后查看所有信息并检查设置是否正确。点击 **"完成"。**
- 虚拟机将开始传输虚拟磁盘 "ADC"，完成后将显示在 XenServer 下。
- 在 XenCenter 客户端中，现在可以看到新的虚拟机。
  右键单击虚拟机，然后单击 "**开始**"。
- 然后虚拟机将启动，并显示 ADC 启动屏幕。

- 配置完成后，就可以登录到退伍军人事务部。

请参阅 "**首次启动配置** "部分继续操作。

在 KVM 上安装

下面将介绍如何在 KVM 平台上安装 EdgeADC。本练习使用的 KVM 平台运行在 CentOS v8 操作系统上，并安装了 Cockpit 和虚拟化。

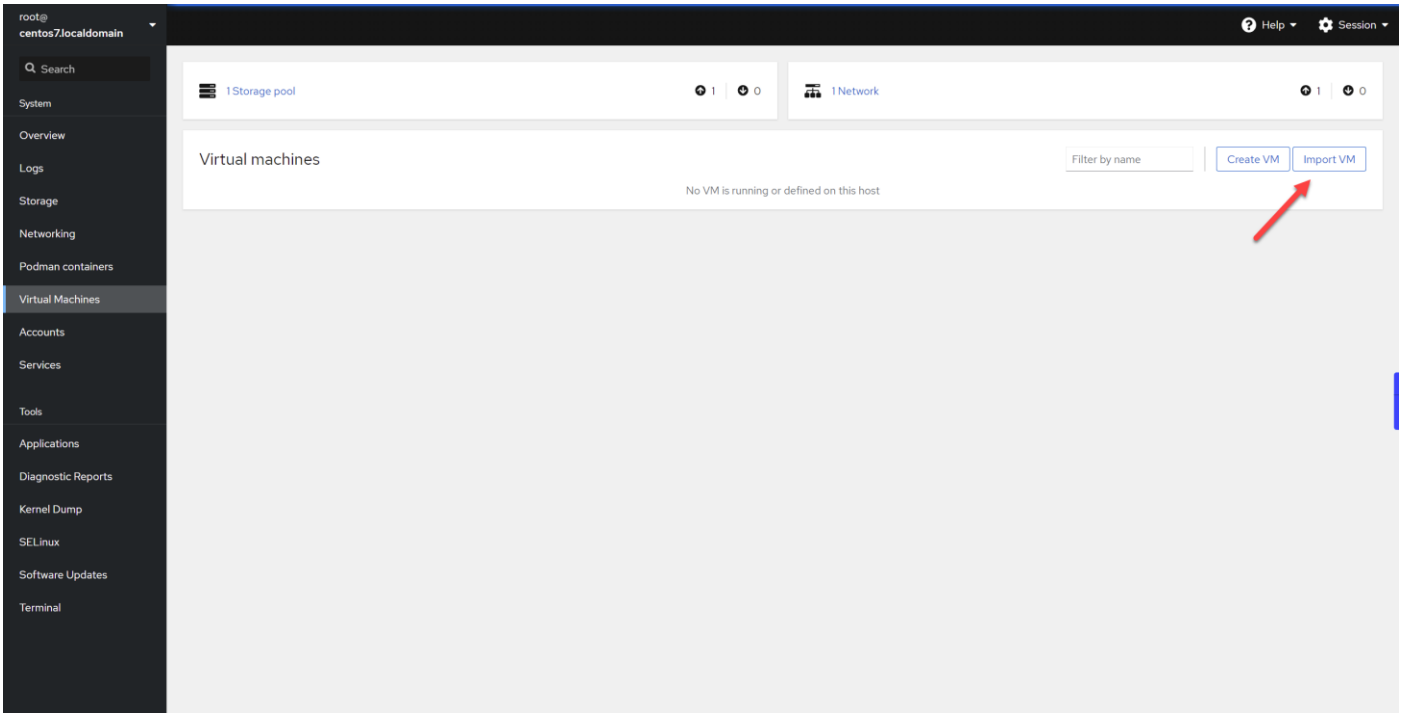
要求和版本

本指南适用于 EdgeADC 4.2.6 及以上版本。

以下指南不包括 KVM 的安装或联网。

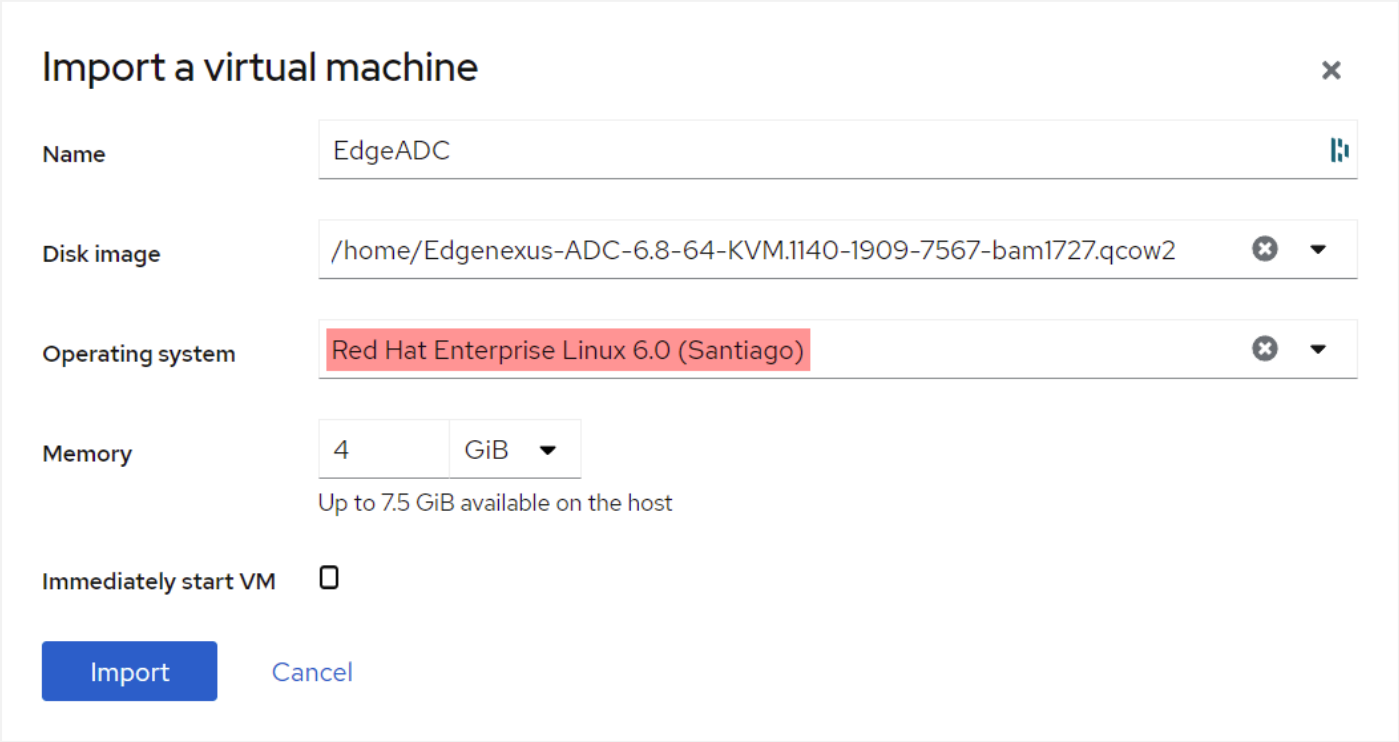
我们假设您已经下载了 KVM 虚拟设备，并将其存储在主机上可访问的位置。

- 第一步是登录驾驶舱控制台。

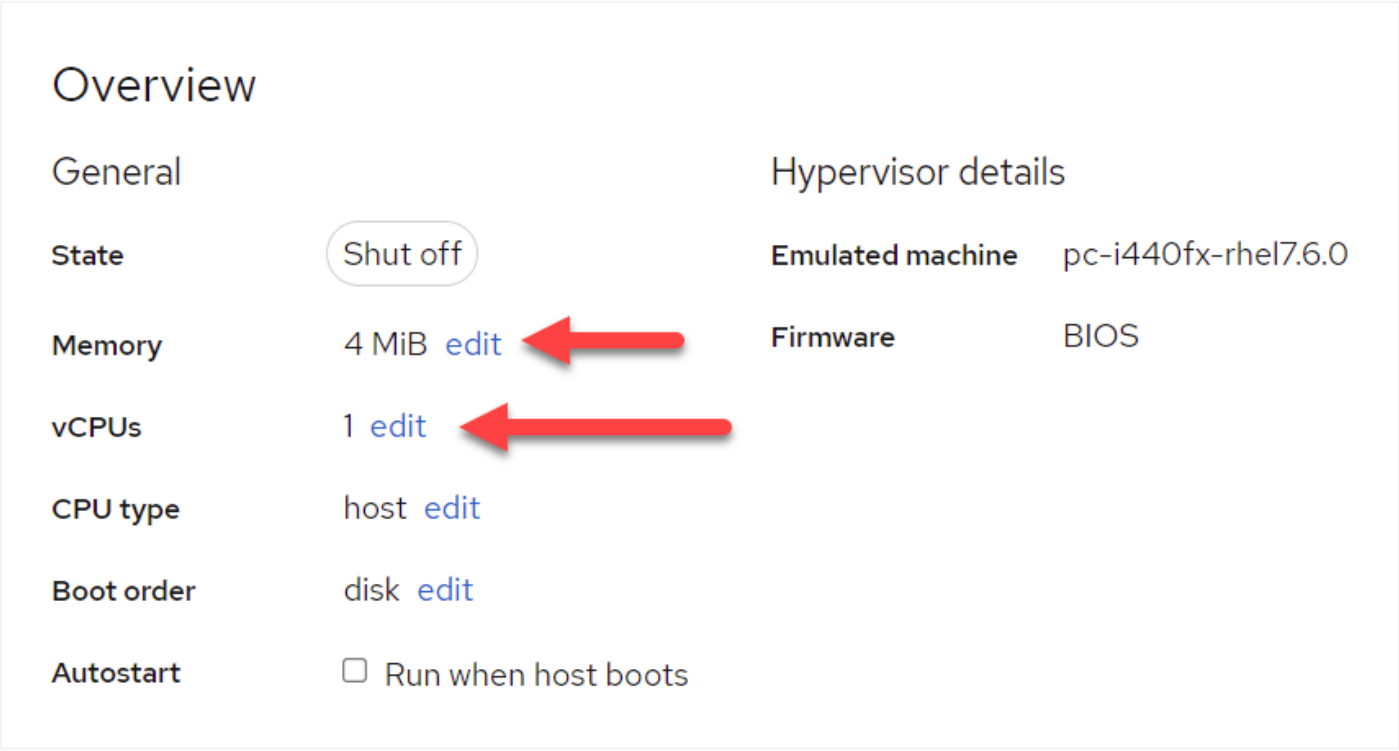


- 单击导入虚拟机

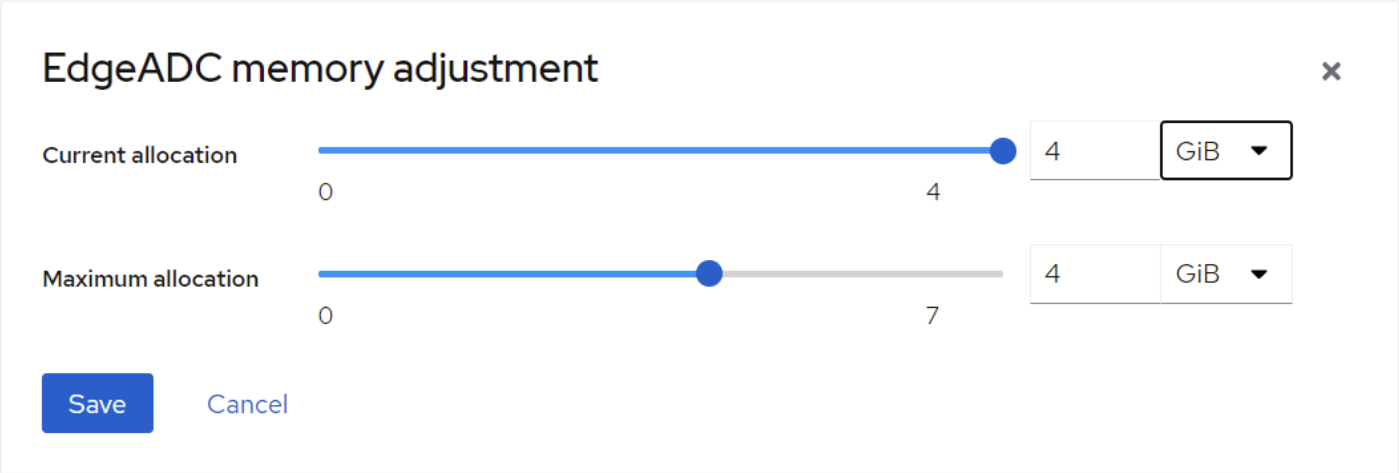
- 在第一个对话框中，您需要指定虚拟设备导入的详细信息。字段内容请参见下图。必须指定 Red Hat Enterprise 6.0 为操作系统。



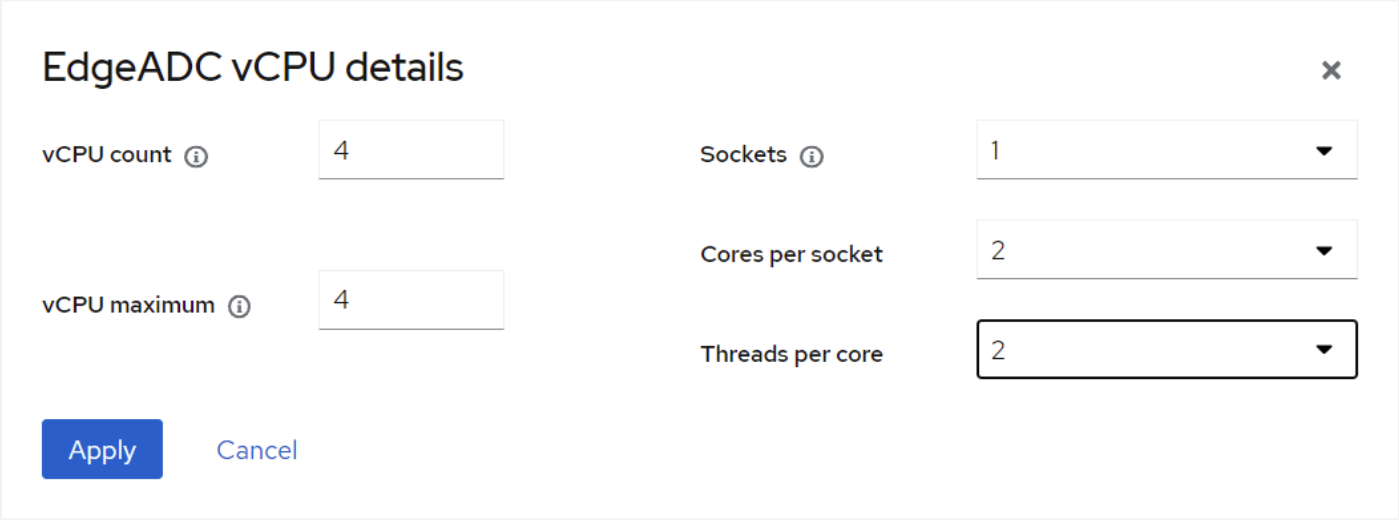
- 请确保未选中 "立即启动虚拟机"。
- 填写完详细信息后，请单击 "导入 "按钮。
- 下一步是指定您可能希望使用的 vCPU 和内存分配。



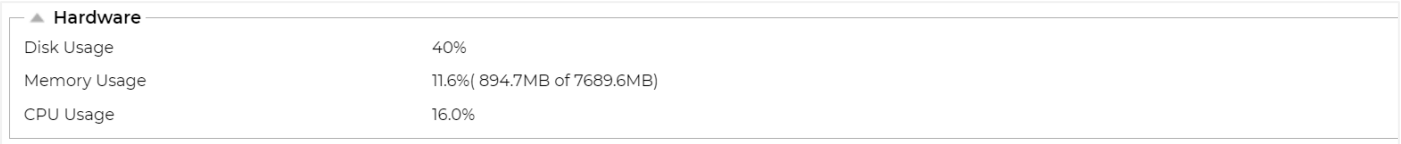
- 要分配内存，您会看到类似下面的对话框。



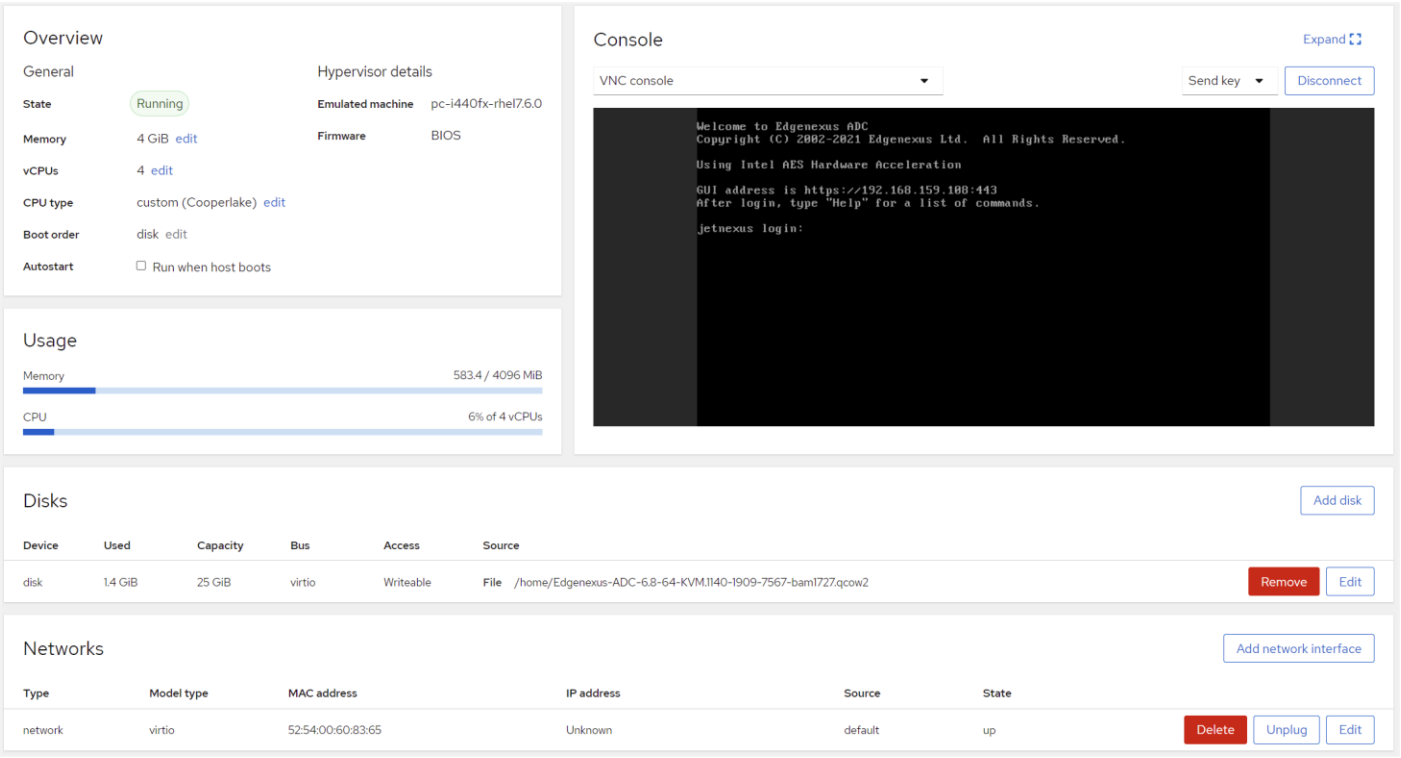
- 要分配 vCPU，您将看到类似下图的对话框。



- 我们所做的选择只是示例，但可行，除非您使用 SSL 重新加密的高吞吐量，在这种情况下，您需要使用 "查看 ">"统计 "下的 "硬件 "部分进行相应调整。



- 现在您已经在 KVM 中安装了一个正常工作的 ADC。请看下图。



在 Nutanix AHV 上安装

下面将介绍如何在 Nutanix AHV 平台上安装 EdgeADC。

要求和版本

本指南适用于 EdgeADC 4.2.6 及以上版本。

所有版本的 Nutanix 管理程序都兼容，但认证是在 Nutanix 5.10.9 版本上进行的。

- 第一步是登录 Nutanix Prism Central。

上传 EdgeADC 映像

- 导航至虚拟基础架构 > 映像
- 单击 "添加图像 "按钮
- 选择已下载的 EdgeADC 图像文件，然后单击 "打开 "按钮上传图像。
- 在图像描述字段中输入图像名称。
- 选择适当的类别
- 选择图片并点击右箭头键
- 选择 "所有图像"，然后单击 "保存"。

创建虚拟机

- 导航至虚拟基础架构 > 虚拟机
- 单击 "创建虚拟机 "按钮
- 输入虚拟机的名称、希望拥有的 CPU 数量以及希望分配给虚拟机的内核数量。

- 然后向下滚动对话框，输入希望分配给虚拟机的内存大小。可以从 4GB 开始，然后根据使用情况增加。

添加磁盘

- 接下来，单击 "添加新磁盘 "链接
- 在操作下拉菜单中选择从映像服务克隆选项。
- 选择已添加的 EdgeADC 图像，然后单击添加按钮。
- 选择要作为可启动磁盘的磁盘。

添加 NIC、网络和亲和性

- 下一步，单击添加新 NIC 按钮。您需要有两个 NICS。
- 选择网络并单击添加按钮
- 单击 "设置亲和力 "按钮
- 选择允许虚拟机运行的 Nutanix 主机，然后单击 "保存 "按钮。
- 确认设置并单击保存按钮

启动虚拟机

- 从虚拟机列表中，单击刚创建的虚拟机名称
- 单击虚拟机的 "打开电源 "按钮
- 虚拟机启动后，单击 "启动控制台 "按钮

配置 EdgeADC 网络

- 按照首次启动环境一节中的说明进行操作。
- 现在 EdgeADC 已准备就绪，您可以使用浏览器和管理 IP 地址访问其图形用户界面。

在 ProxMox 上安装

ProxMox 的安装很简单，但需要几个额外步骤。

我们将使用 VMWare OVA 版本进行安装。这是一个多步骤的过程，需要掌握 ProxMox 的 shell 命令。不过，我们的说明尽可能简单易懂。我们假定您已经熟悉 ProxMox，因此不会深入介绍 ProxMox 的功能。

将 OVA 上传到 ProxMox

由于我们使用的是 OVA 版本，因此首先需要将 OVA 上传到 ProxMox。

- 登录 ProxMox 控制台
- 创建名为 OVA_Import 的文件夹。
- 现在，您需要使用 WinSCP（Windows）或 CyberDuck（Mac）等 SFTP 客户端来传输 OVA 文件。
- 文件传输完成后，您将在创建的文件夹中看到该文件。
- 键入以下命令提取 OVA 文件的内容。
- Tar xvf {文件名}。请参见下面的示例。

```
tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
```

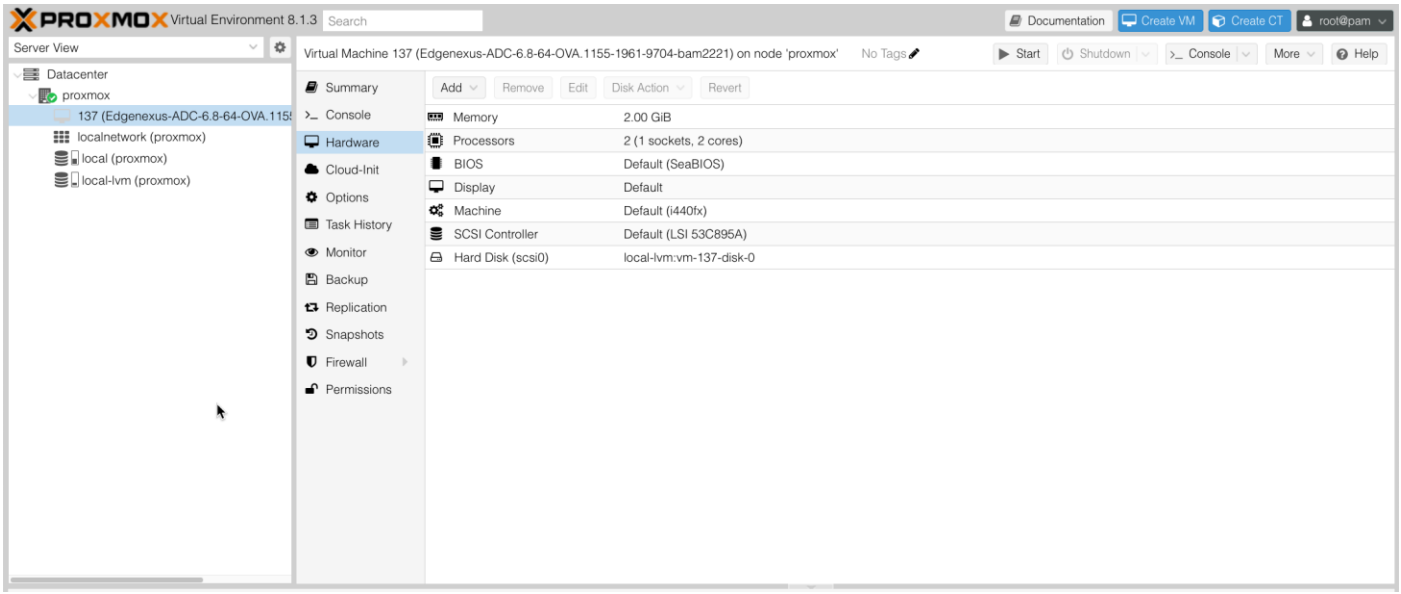
- 提取后，您应该会看到类似下面的示例。

```
root@proxmox:~/OVA_Import# ls
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
root@proxmox:~/OVA_Import# tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ovf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.mf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221-disk1.vmdk
root@proxmox:~/OVA_Import#
```

- 共有三个文件。.ovf 和 .mf 是配置文件。.vmdk 是容纳 ADC 的虚拟磁盘。
- 下一步是将 VMDK 导入 ProxMox 并创建虚拟机。
- 键入以下命令，使用配置文件创建虚拟机。

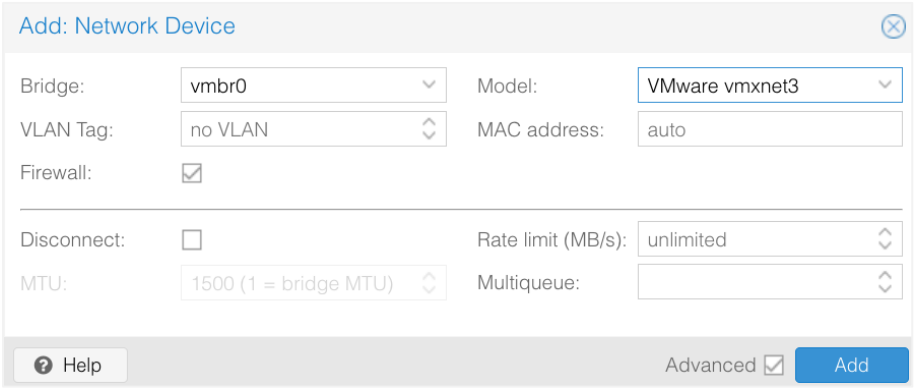
```
qm importovf 137 ./{filename.ovf} local-lvm --format qcow2
```

- 在本示例中，我们给出的 ID 是 100，但如果您已经在 ProxMox 中创建了虚拟机，您的安装情况可能会有所不同。您可以通过在 ProxMox 中开始创建虚拟机的过程来确定下一个 ID，或者选择一个比 100 更高的数字，这样就可以安全地使用了。
- 虚拟机现已创建。



- 下一步是为虚拟机添加网络接口。
- 点击右侧面板上的硬件。

- 单击添加并选择网络接口。



- 如上图所示进行配置。重要的是要将模型选择为 VMware vmxnet3。
- 配置完成后点击添加。
- 您可以根据需要增加网络适配器。
- 现在可以启动虚拟机，并继续使用首次启动配置一章中的说明。

首次启动配置

第一次启动时，ADC（下文也称为 VA）会显示以下屏幕，要求为生产操作进行配置。

首次启动 - 手动网络详细信息

首次启动时，您有 10 秒钟的时间中断通过 DHCP 自动分配 IP 详细信息。

要中断此过程，请单击控制台窗口并按任意键。然后，您可以手动输入以下详细信息。

- IP 地址
- 子网掩码
- 网关
- DNS 服务器

这些更改是持久性的，重启后也不会消失，无需在 VA 上再次配置。

首次启动 - DHCP 成功

如果不中断网络分配过程，ADC 将在超时后联系 DHCP 服务器，以获取网络详细信息。如果联系成功，机器将被分配以下信息。

- IP 地址
- 子网掩码
- 默认网关
- DNS 服务器

我们建议，只有当 IP 地址与 DHCP 服务器中 ADC 的 MAC 地址永久链接时，才使用 DHCP 地址操作 ADC。我们建议在使用虚拟设备时始终使用**固定 IP 地址**。请按照**更改管理 IP 地址**和后续章节中的步骤操作，直至完成网络配置。

首次启动 - DHCP 失败

如果没有 DHCP 服务器或连接失败，将分配 IP 地址 192.168.100.100。

IP 地址将以 "1 "递增，直到 VA 找到空闲的 IP 地址。同样，VA 也会检查 IP 地址是否正在使用，如果正在使用，则会再次递增并重新检查。

更改管理 IP 地址

您可以随时使用 **set greenside=n.n.n.n** 命令更改 VA 的 IP 地址，如下所示。

```
set greenside={IP 地址}
```

更改 eth0 的子网掩码

网络接口使用前缀 "eth"；基本网络地址称为 eth0。可以使用命令 **set mask [NIC] [MASK]** 更改子网掩码或 netmask。下面是一个示例。

```
设置掩码 eth0 {mask}
```

指定默认网关

VA 的运行需要一个默认网关。要设置默认网关，请使用 **route add default gw [GATEWAY IP]** 命令，如下例所示。

```
路由添加默认 gw {IP 地址}
```

检查默认网关 值

要检查默认网关是否已添加且正确，请使用 **route** 命令。该命令将显示网络路由和默认网关值。请参见下面的示例。

```
Command:route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
255.255.255.255 *               255.255.255.255 UH    0      0        0 eth0
192.168.101.0   *               255.255.255.0   U     0      0        0 eth0
default         192.168.101.254 0.0.0.0         UG    0      0        0 eth0
```

您现在可以访问图形用户界面 (GUI)，为生产或评估用途配置 ADC。

访问网络界面

您可以使用任何带有 JavaScript 的 Internet 浏览器来配置、监控 ADC 并将其部署到运行中。

在浏览器 URL 字段中，键入 **HTTPS://{IP ADDRESS} 或 HTTPS://{FQDN}**

ADC 默认使用自签名 SSL 证书。您可以将 ADC 更改为使用自己选择的 SSL 证书。

浏览器到达 ADC 后，会显示登录屏幕。ADC 的出厂默认用户名是

Username: admin / Pwd: jetnexus

命令参考表

指挥	参数 1	参数 2	说明	示例
日期			显示当前配置的日期和时间	世界协调时 2013 年 9 月 3 日（星期二）13:00
默认			为设备指定出厂默认设置	
出口			退出命令行界面	
帮助			显示所有有效命令	
ifconfig	[空白]		查看所有接口的接口配置	ifconfig
	eth0		仅查看 eth0 的接口配置	ifconfig eth0
machineid			该命令将提供用于许可 ADC ADC 的机器 ID	EF4-3A35-F79
烟			退出命令行界面	
重新启动			终止所有连接并重新启动 ADC ADC	重新启动
重新启动			重启 ADC ADC 虚拟服务	
途径	[空白]		查看路由表	途径
	增加	默认 gw	添加默认网关 IP 地址	route add default gw 192.168.100.254
设置	菜园		为 ADC 设置管理 IP 地址	set greenside=192.168.101.1
	面罩		设置接口的子网掩码。接口名称为 eth0、eth1....。	设置掩码 eth0 255.255.255.0
展览			显示全局配置设置	
关闭			终止所有连接并关闭 ADC ADC	
地位			显示当前数据统计	
顶级			查看 CPU 和内存等进程信息	
查看日志	信息		显示原始系统日志信息	查看日志信息

请注意：命令不区分大小写。没有命令历史记录。

网络控制台

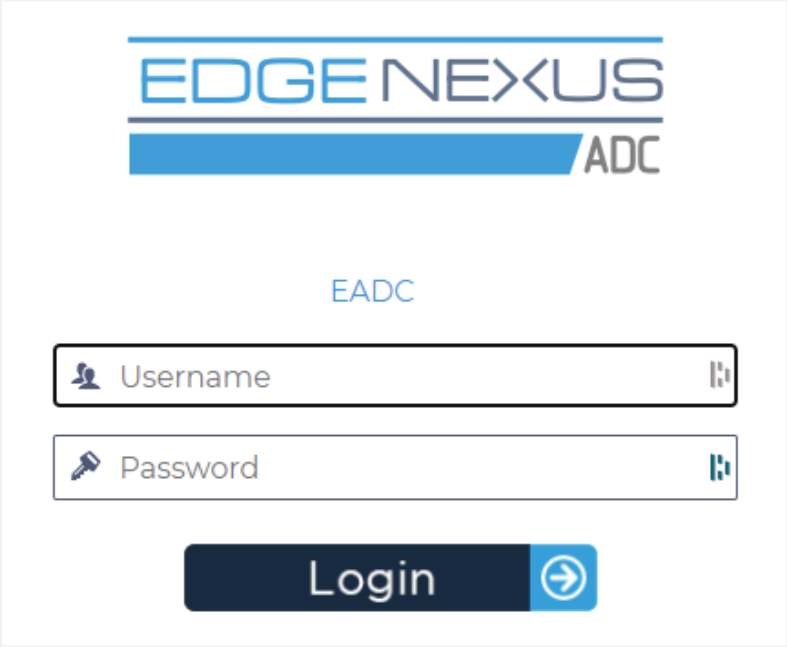
启动 ADC 网络控制台

ADC 上的所有操作都通过网络控制台进行配置和执行。网络控制台可使用任何带 JavaScript 的浏览器访问。

要启动 ADC 网络控制台，请在 URL 字段中输入 ADC 的 URL 或 IP 地址。我们将以 adc.company.com 为例：

https://adc.company.com

启动后，ADC 的网络控制台如下图所示，允许您以管理员用户身份登录。



默认登录凭证

默认登录凭证为

Username: admin / Pwd: jetnexus

您可以随时通过*系统* > 用户中的用户配置进行更改。

成功登录后，屏幕上将显示 ADC 的主仪表板。

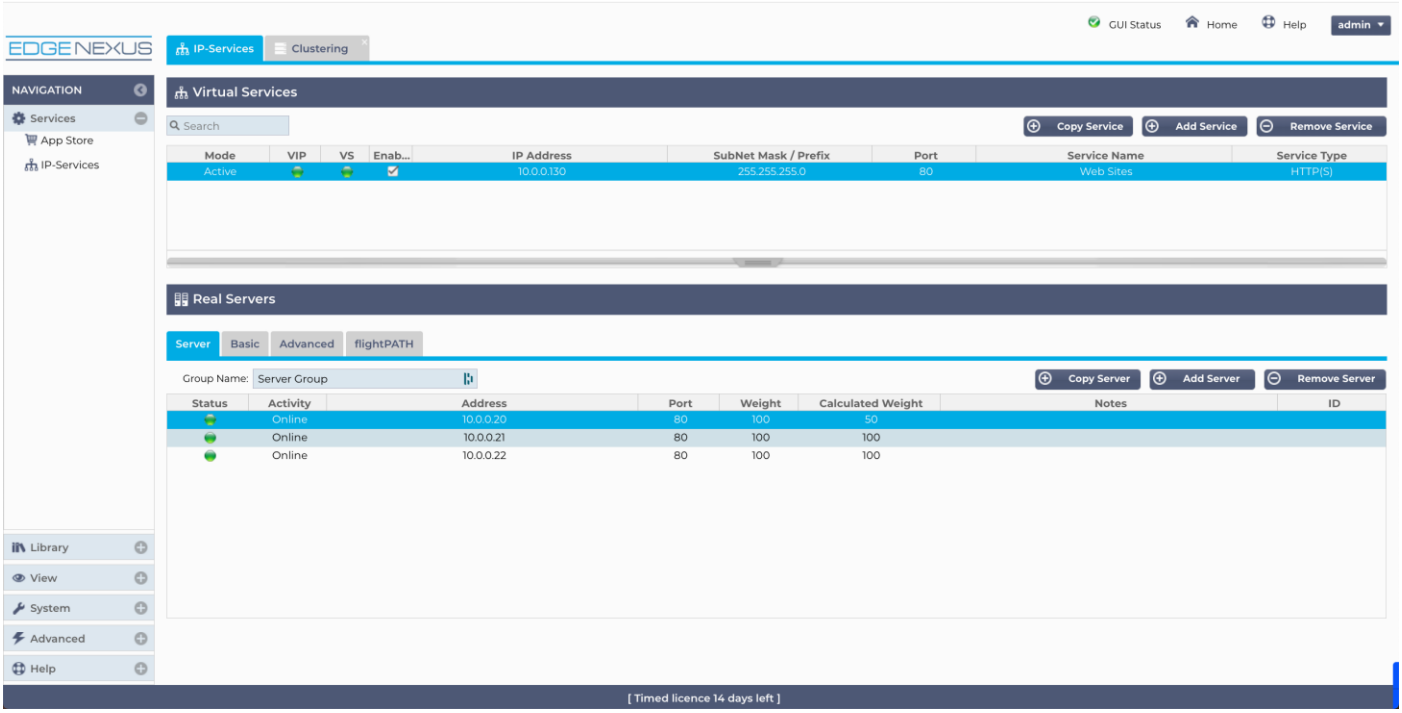
使用外部身份验证服务

如果希望使用外部身份验证服务，可以通过配置身份验证服务器和身份验证服务来实现。

有关信息请参阅认证 和认证服务

主仪表板

下图展示了 ADC 的主仪表板或 "主页 "的外观。我们可能会偶尔进行一些改进，但所有功能都将保留。



通过左侧的 "导航 "部分，可以浏览 ADC 功能的各个区域。默认情况下，选择 "服务 "部分，并打开 IP 服务子部分，虚拟服务部分上方的选项卡会显示该子部分。该选项卡是固定的，始终显示。

当你点击导航栏中的某个部分时，该部分就会展开并显示其内容。点击版块内的选项，右侧将打开版块内容，并在顶部放置一个标签，以便快速切换。

后续章节将详细介绍不同的导航部分。

服务

知识产权服务

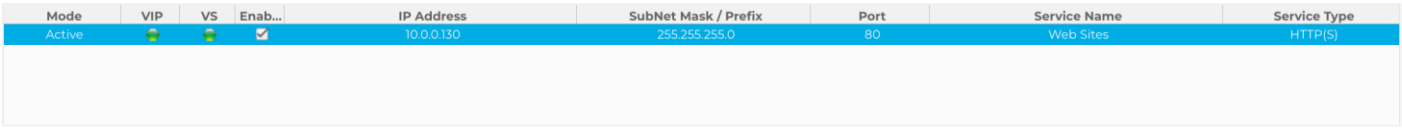
ADC 的 IP 服务部分允许您添加、删除和配置特定用例所需的各种虚拟 IP 服务。设置和选项分为以下几个部分。这些部分位于应用程序屏幕的右侧。

虚拟服务

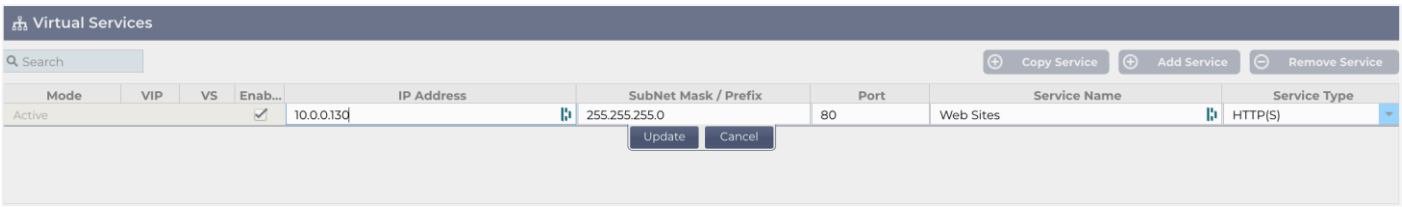
虚拟服务结合了一个虚拟 IP（或 VIP）和 ADC 监听的 TCP/UDP 端口。到达虚拟 IP 的流量会被重定向到与该服务相关的真实服务器之一。虚拟 IP 地址不能与 ADC 的管理地址相同，如 eth0、eth1 等。

ADC 会根据真实服务器部分基本选项卡中设置的负载平衡策略，决定如何将流量重新分配给服务器。

使用新 VIP 创建新虚拟服务



- 单击上述添加虚拟服务按钮。



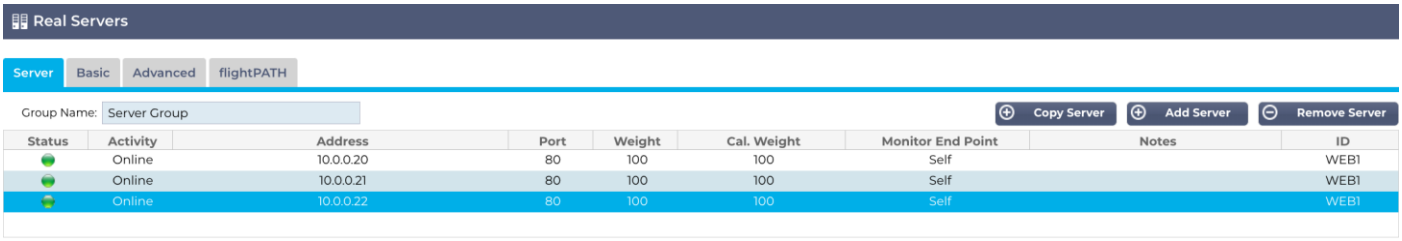
然后进入**编辑行**模式。

- 完成高亮显示的四个字段，然后单击更新按钮。

请使用 TAB 键浏览字段。

现场	说明
IP 地址	输入一个新的虚拟 IP 地址，作为访问真实服务器的目标入口点。用户或应用程序将通过此 IP 访问负载平衡应用程序。
子网掩码/前缀	该字段用于输入与 ADC 所在网络相关的子网掩码
港口	访问 VIP 时使用的入口端口。如果使用反向代理，此值不一定要与真实服务器相同。
服务名称	服务名称是 VIP 目的的文字表述。它是可选项，但我们建议您提供，以便更清楚地说明。请注意，在使用 GSLB 时，该字段还可用于其他特定用途。
服务类型	有许多不同的服务类型供您选择。第 4 层服务类型不能使用 flightPATH 技术。

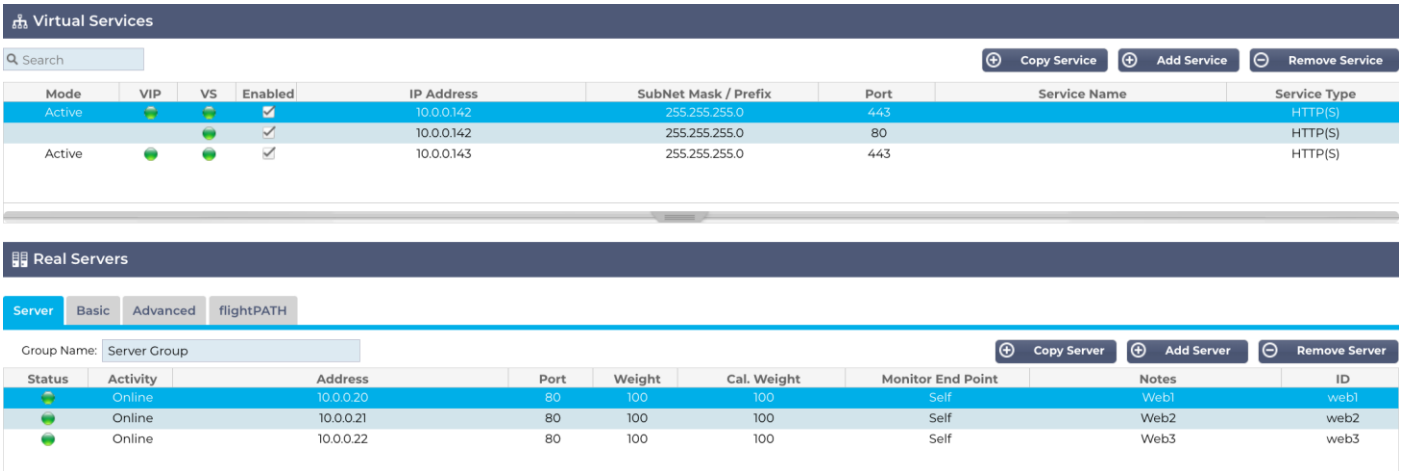
现在您可以按下更新按钮来保存此部分，并自动跳转到下面详细介绍的真实服务器部分：



现场	说明
活动	活动 "字段可用于显示和更改负载平衡真实服务器的状态。 在线 - 表示服务器处于活动状态，正在接收负载平衡请求。 脱机 - 服务器处于脱机状态，不接收请求。 耗尽 - 服务器已进入耗尽模式，以便清除持久性并将服务器移至离线状态，而不会影响用户。 备用 - 服务器已进入备用状态
IP 地址	此值是真实服务器的 IP 地址。它必须准确无误，且不应是 DHCP 地址。
港口	真实服务器上的目标访问端口。使用反向代理时，该端口可能与 VIP 上指定的入口端口不同。
加权	此设置通常由 ADC 自动配置。如果希望更改优先权加权，则可以进行更改。
卡尔重量	如果将 "加权 "设置为默认值，ADC 将根据响应时间自动计算加权。
监控终点	默认值为 "Self"。不过，您可以将其更改为端口值或 IP 地址：端口。该字段用于监控不同的端点，并确定是否应将流量传递给虚拟服务。请参阅**如何使用**监控终点 。

- 单击更新按钮或按 Enter 保存更改
- 如果服务器健康检查成功，状态指示灯将首先变为灰色，然后变为绿色。如果真实服务器监控失败，状态指示灯将变为红色。
- 状态指示灯为红色的服务器不会实现负载平衡。

已完成的虚拟服务示例

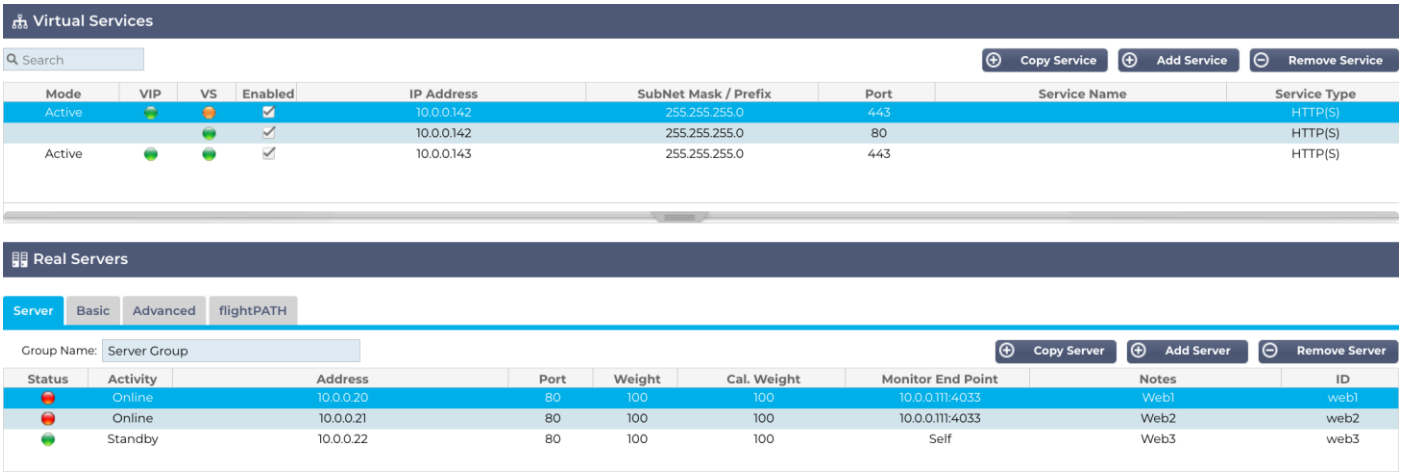


如何使用监控终点

示例 1

让我们以一个基础架构为例，它由两个负载平衡的网络服务器组成，向终端用户提供网络应用程序。网络应用程序连接到后端的数据库服务器。数据库服务器访问中断，但网络应用程序服务器仍在运行。用户在尝试使用网络应用程序时会收到错误信息。

解决方案是使用监控终端。



- 示例显示了两个网络服务器 10.0.0.20 和 10.0.0.21，以及第三个网络服务器 10.0.0.22。10.0.0.22 服务器已进入待机模式。
- 两个活动网络服务器的监控端点值为 10.0.0.111:4033，这是数据库服务器连接的 IP 地址和端口。
- 如果数据库服务器连接中断，两台运行中的服务器将进入离线模式，而备用服务器将联机，并提供一个网页，通知客户系统正在维护中。

示例 2

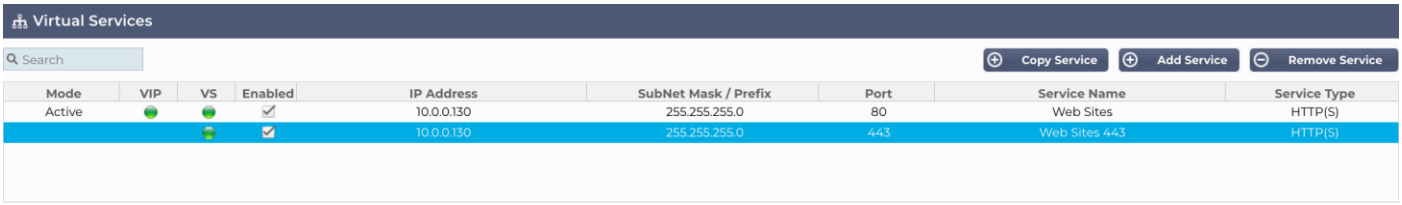
使用监控端点的另一个例子是在对 UDP 协议服务器（如 Always-On-VPN）进行负载平衡时。如你所知，UDP 端口无法得到可靠监控，因此需要监控 TCP 端口。

使用监控端点就可以做到这一点。Always-on-VPN 服务器使用的主要端口是 53/udp，但你要监控的是 8433/tcp。在这种情况下，只需在监控端点字段中输入端口值即可。

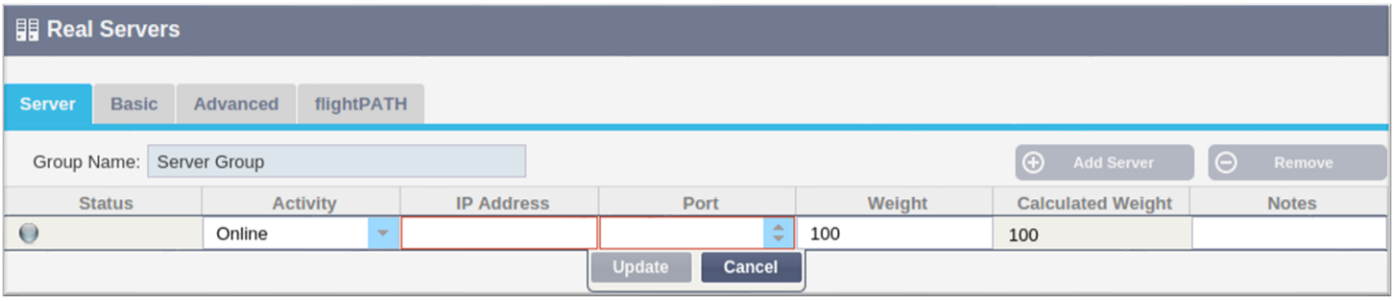
创建子虚拟服务

如果需要在同一 VIP 上使用不同端口进行负载平衡，也可以创建子虚拟服务。例如，可能有服务器使用同一虚拟 IP 访问 80、8088 和 443 端口，因此需要创建子虚拟服务来适应这种情况。

- 突出显示要复制的虚拟服务。
- 单击添加虚拟服务进入行编辑模式。



- IP 地址和子网掩码会自动复制。
- 输入服务的端口号。
- 输入可选的服务名称
- 选择服务类型。
- 现在您可以按下更新按钮来保存这一部分，并自动跳转到下面的真实服务器部分

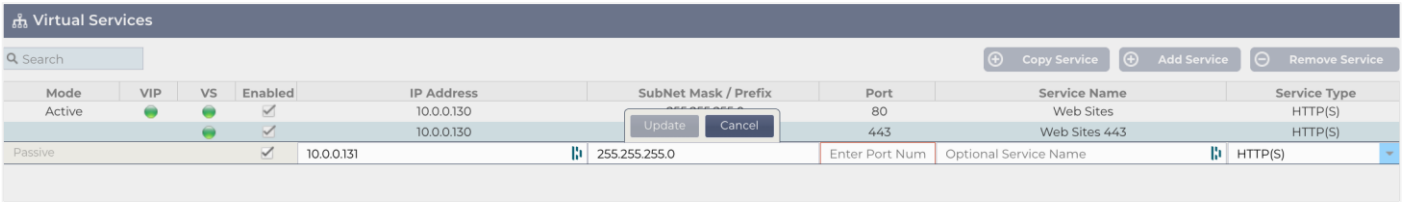


- 将服务器 "活动 "选项保留为 "在线"--这意味着如果服务器通过了默认的 TCP 连接健康监控，就会实现负载平衡。如果需要，稍后可以更改此设置。
- 输入真实服务器的 IP 地址
- 输入真实服务器的端口号
- 在备注字段中输入真实服务器的可选名称。请记住，此备注字段用于其他特定用途，如 flightPATH 变量等。
- 单击 "更新 "保存更改。
- 如果真实服务器监控器监控成功，状态指示灯将首先变为灰色，然后变为绿色。如果真实服务器监控器失败，状态指示灯将变为红色。
- 状态指示灯为红色的服务器将无法实现负载平衡。

更改虚拟服务的 IP 地址

您可以随时更改现有虚拟服务或 VIP 的 IP 地址。

- 突出显示要更改其 IP 地址的虚拟服务。
- 单击该服务的 IP 地址字段，将其更改为可编辑状态。



- 将 IP 地址更改为您希望使用的地址
- 单击更新按钮保存更改。

注意： 更改虚拟服务的 IP 地址将更改与 VIP 关联的所有服务的 IP 地址。

使用 "复制服务 "创建新虚拟服务

- 复制服务 "按钮将复制整个服务，包括与其相关的所有真实服务器、基本设置、高级设置和 flightPATH 规则。
- 突出显示要复制的服务，然后单击 "复制服务"。
- 行编辑器将出现，IP 地址列上的光标将闪烁
- 您必须更改 IP 地址，使其具有唯一性；如果您希望保留 IP 地址，则必须编辑端口，使其对该 IP 地址具有唯一性。

如果更改负载平衡策略、Real Server 监控程序或删除 flightPATH 规则等设置，请记住编辑每个选项卡。

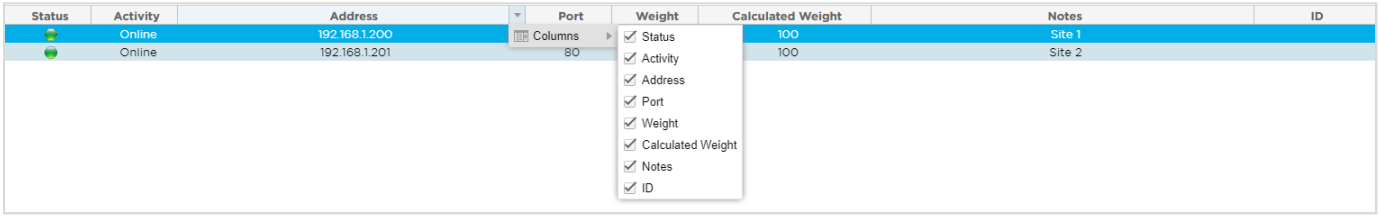
过滤显示数据

搜索特定术语

搜索框允许您使用任何值搜索表，如 IP 地址或服务名称的八位字节。

选择列的可见性

您还可以选择希望在仪表板中显示的列。



- 将鼠标移至任意一列上
- 您会看到栏右侧出现一个小箭头
- 单击复选框可选择希望在仪表板中看到的列。

了解虚拟服务栏

初级/模式

模式列显示为当前 VIP 选择的高可用性角色。有关模式，请参阅系统 > 集群 > 角色。

选项	说明
活跃	在群集模式下，该字段的值为 "活动"。当数据中心中有一对 HA ADC 设备时，其中一个将显示 "活动"，另一个显示 "被动"。如果当前设备
被动式	当 ADC 作为群集的辅助成员时，"模式 "一栏显示 "被动"。

手册	手动角色允许 ADC 对以主动-主动模式运行不同的虚拟 IP 地址。在这种情况下，"主 "列将在每个唯一的虚拟 IP 地址旁包含一个方框，可选择 "主动 "或不打钩选择 "被动"。
单机版	ADC 作为独立设备运行，不在高可用性模式下。因此，"主要 "栏将显示 "独立"。

贵宾

本栏提供有关每个虚拟服务状态的直观反馈。指标以彩色编码，具体如下：

发光二极管	意义
●	在线
●	故障转移-备用。此虚拟服务为热备
●	表示 "次级 "为 "初级 "暂缓。
●	服务需要注意。此指示可能是由于真实服务器未通过健康监控检查或已手动更改为脱机。流量将继续流动，但真实服务器容量会降低
●	脱机。内容服务器无法访问，或未启用内容服务器
●	调查结果
●	未获得许可或超过许可的虚拟 IP

已启用

该选项的默认值为已启用，复选框显示为已勾选。双击该行，取消勾选复选框，然后单击 "更新 "按钮，即可禁用虚拟服务。

IP 地址

添加以十进制点号表示的 IPv4 地址或 IPv6 地址。此值即为您服务的虚拟 IP 地址 (VIP)。IPv4 示例 "192.168.1.100"。示例 IPv6"2001:0db8:85a3:0000:0000:8a2e:0370:7334"。

子网掩码/前缀

以十进制点号形式添加子网掩码。例如 "255.255.255.0"。也可以使用子网值（如 /24），或在 IPv6 中添加前缀。有关 IPv6 的更多信息，请参阅 **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

港口

添加与服务相关的端口号。端口可以是 TCP 或 UDP 端口号。例如，TCP "80 "用于 Web 流量，TCP "443 "用于安全 Web 流量。您也可以指定一个数值范围，如 80-87。

目前，无法使用逗号分隔值来指定不连续的端口值。

服务名称

添加一个友好的名称来标识您的服务。例如 "生产网络服务器"。使用 GSLB 时也要使用此字段。

服务类型

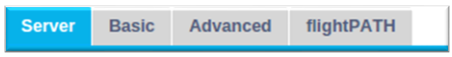
请注意，对于所有 "第 4 层 "服务类型，ADC 不会与数据流交互或修改数据流，因此 flightPATH 对第 4 层服务类型不可用。第 4 层服务只是根据负载平衡策略对流量进行负载平衡：

服务类型	端口/协议	服务层	评论
第 4 层 TCP	任何 TCP 端口	第 4 层	ADC 不会更改数据流中的任何信息，并将根据负载平衡策略执行标准的流量负载平衡
第 4 层 UDP	任何 UDP 端口	第 4 层	与第 4 层 TCP 一样，ADC 不会更改数据流中的任何信息，并将根据负载平衡策略对流量进行标准负载平衡。
第 4 层 TCP/UDP	任何 TCP 或 UDP 端口	第 4 层	如果您的服务有 UDP 等主要协议，但会回退到 TCP，那么 ADC 就是最理想的选择。ADC 不会更改数据流中的任何信息，并将根据负载平衡策略执行标准的流量负载平衡。
DNS	TCP/UDP	第 4 层	用于负载平衡 DNS 服务器。
HTTP(S)	HTTP 或 HTTPS 协议	第 7 层	ADC 可以使用 flightPATH 对数据流进行交互、操作和修改。
文件传输协议	文件传输协议	第 7 层	在客户端和服务器之间使用独立的控制和数据连接
SMTP	简单邮件传输协议	第 4 层	在对邮件服务器进行负载平衡时使用
POP3	邮局礼宾	第 4 层	在对邮件服务器进行负载平衡时使用
IMAP	互联网信息存取协议	第 4 层	在对邮件服务器进行负载平衡时使用
RDP	远程桌面协议	第 4 层	在平衡终端服务服务器负载时使用
RPC	远程程序调用	第 4 层	在使用 RPC 调用对系统进行负载平衡时使用
RPC/ADS	Exchange 2010 地址簿服务静态 RPC	第 4 层	在平衡 Exchange 服务器负载时使用
RPC/CA/PF	用于客户端访问和公共文件夹的 Exchange 2010 静态 RPC	第 4 层	在平衡 Exchange 服务器负载时使用

DICOM	医学数字成像与通信	第 4 层	在使用 DICOM 协议对服务器进行负载平衡时使用

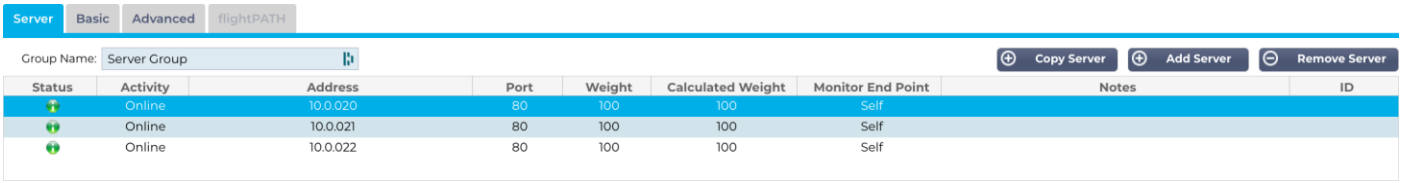
真实服务器

仪表板的 "真实服务器 "部分有几个选项卡：服务器、基本、高级和 flightPATH。



服务器

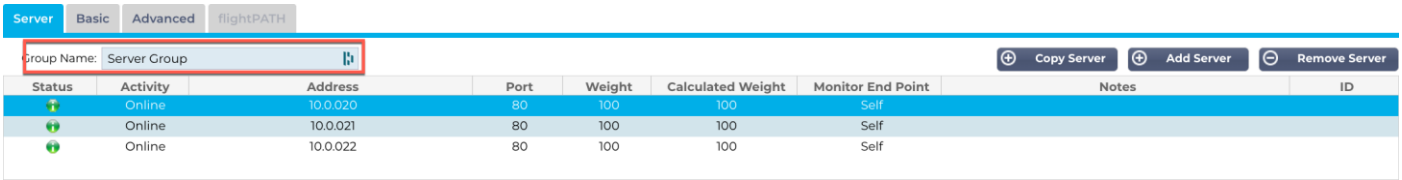
服务器 "选项卡包含与当前选定的虚拟服务配对的真实后端服务器的定义。您需要在真实服务器部分添加至少一个服务器。



添加服务器

- 选择先前定义的相应 VIP。
- 单击添加服务器
- 新行将出现，光标在 IP 地址列上闪烁
- 以点十进制符号输入服务器的 IPv4 地址。真实服务器可以与虚拟服务位于同一网络、任何直接连接的本地网络或 ADC 可以路由的任何网络。例如 "10.1.1.1"。
- 点选端口列，输入服务器的 TCP/UDP 端口号。端口号可以与虚拟服务端口号相同，也可以是反向代理连接的另一个端口号。ADC 将自动转换为该端口号。
- 点选 "备注 "部分，添加服务器的任何相关细节。例如"IIS Web 服务器 1

组名



添加组成负载平衡组的服务器后，还可以附加组名称。编辑完此字段后，无需按更新按钮即可保存内容。

真实服务器状态指示灯

您可以通过 "状态 "栏中的浅色来查看真实服务器的状态。见下图：

发光	意义

二极管	
●	已连接
◎	未监测
●	排水
●	离线
●	备用
●	未连接
●	调查结果
●	未获得许可或许可的真实服务器超标

活动

您可以随时使用下拉菜单更改真实服务器的活动。为此，请双击真实服务器行，使其进入编辑模式。

选项	说明
在线	所有在线分配的真实服务器都将根据 "基本 "选项卡中设置的负载平衡策略接收流量。
排水	分配为 "耗尽 "的所有真实服务器将继续为现有连接提供服务，但不会接受任何新连接。在排水过程中，状态指示灯将闪烁绿色/蓝色。一旦现有 连接自然关闭，真实服务器将离线，状态指示灯将显示为纯蓝色。您还可以通过导航 > 监控 > 状态部分查看这些连接。 可以在高级设置选项卡中更改排水行为。
离线	所有设置为脱机的真实服务器将立即脱机，不会接收任何流量。
备用	所有设置为备用的真实服务器都将保持离线状态，直到**所有**在线组服务器都无法通过服务器健康监控检查。发生这种情况时，备用组将根据负载平衡策略接收流量。如果联机组中有一台服务器通过了服务器健康监控检查，这台联机服务器将接收所有流量，而备用组将停止接收流量。

IP 地址

此字段是真实服务器的 IP 地址。例如 "192.168.1.200"。

港口

真实服务器为服务监听的 TCP 或 UDP 端口号。例如，网络流量为 "80"。

重量

指定了适当的负载平衡策略后，此列将可编辑。

真实服务器的默认权重为 100，您可以输入 1-100 之间的值。100 表示最大负载，1 表示最小负载。

三台服务器的示例如下：

- 服务器 1 重量 = 100
- 服务器 2 重量 = 50
- 服务器 3 重量 = 50

如果我们将负载平衡策略设置为 "最少连接"，并且总共有 200 个客户端连接；

- 服务器 1 将获得 100 个并发连接
- 服务器 2 将获得 50 个并发连接
- 服务器 3 将获得 50 个并发连接

如果我们使用循环罗宾作为负载平衡方法，通过负载平衡服务器集轮流处理请求，那么改变权重就会影响服务器被选为目标的频率。

如果我们认为 "最快 "负载均衡策略使用的是获取响应所需的最短时间，那么调整权重就会改变偏差，与 "最少连接 "策略类似。

计算重量

每台服务器的 "计算权重 "可动态查看，它是自动计算的，不可编辑。该字段显示 ADC 在考虑手动加权和负载平衡策略时使用的实际权重。

监控终点

此功能允许您指定要监控的特定端点，从而确定真实服务器条目的健康状态。您可以将其保留为默认值 "自"，这样它将依赖于为虚拟服务指定的真实服务器监控器。或者，您也可以指定一个 IP 地址、端口或 IP 地址：端口，以便监控网络上的另一个端点。例如，服务所依赖的数据库服务器。

说明

在 "备注 "字段中输入任何有助于描述已定义条目的特殊备注。例如 "IIS Server1 - London DC"。此字段可用于满足 flightPATH 规则和 GSLB 的特定需求。

身份证

这种设置有多种用途。

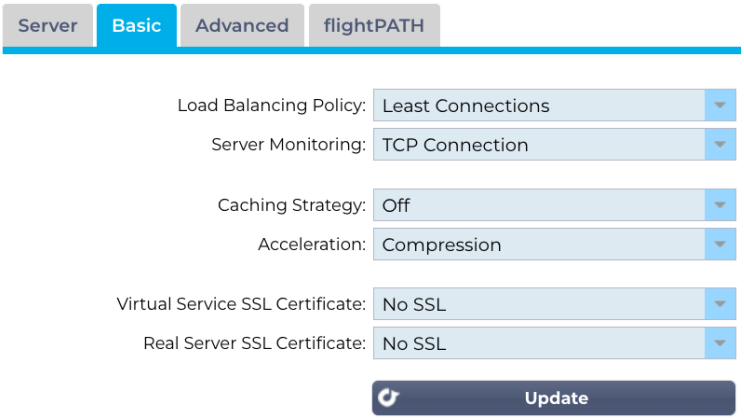
坚持不懈

该值可与基于 Cookie ID 的持久化方法结合使用。这种方法与基于会话的 PHP 持久化方法非常相似，但使用了一种称为基于 Cookie ID 和 cookie RegEx h=[^;]+ 的新技术。基于 Cookie ID 的持久化方法将使用 ID 字段中的值生成 Cookie。

flightPATH 使用方法

您还可以使用该字段中的值来引导流量等。

基础



负载平衡策略

下拉列表显示当前支持的负载平衡策略。负载平衡策略列表及说明如下。

Least Connections
Fastest
Persistent Cookie
Round Robin
IP-Bound
IP List Based
Shared IP List Based
Classic ASP Session Cookie
ASP.NET Session Cookie
JSP Session Cookie
JAX-WS Session Cookie
PHP Session Cookie
RDP Cookie Persistence
Cookie ID Based

选项	说明
最少连接	负载平衡器将跟踪每个真实服务器的当前连接数。连接数最少的真实服务器将接收随后的新请求。
最快	最快负载平衡策略会自动计算每台服务器上所有请求的响应时间，并随时间推移进行平滑处理。计算权重列包含自动计算的值。只有在使用此负载平衡策略时才可以手动输入。

持久 Cookie	第 7 层会话亲和性/持久性 基于 IP 列表的负载平衡模式用于每个首次请求。ADC 会在第一个 HTTP 响应的标题中插入 cookie。之后，ADC 会使用客户端 cookie 将流量路由到同一个后端服务器。当客户端每次都必须访问同一个后端服务器时，这个 cookie 就会被用于持久化。Cookie 将在 2 小时后过期，连接将根据基于 IP 列表的算法进行负载平衡。该过期时间可通过 jetPACK 进行配置。
循环赛	轮循通常用于防火墙和基本负载平衡器，是最简单的方法。每个真实服务器按顺序接收新请求。这种方法只适用于需要将请求平均负载平衡到服务器的情况，例如查找网络服务器。但是，如果需要根据应用程序负载或服务器负载进行负载平衡，甚至需要确保在会话中使用同一台服务器，则不适合使用轮循方法。
IP 约束	第 3 层会话亲和性/持久性 Cookie。 在这种模式下，客户端的 IP 地址是选择哪个真实服务器接收请求的依据。此操作提供了持久性。HTTP 和第 4 层协议可以使用这种模式。这种方法适用于已知网络拓扑结构的内部网络，可以确保上游没有 "超级代理"。使用第 4 层和代理时，所有请求看起来都像是来自一个客户端，因此负载会不均衡。在 HTTP 中，当存在代理时，会使用标头（X-Forwarder-For）信息。
基于 IP 列表	使用 "最少连接 "启动与真实服务器的连接，然后根据客户端的 IP 地址实现会话亲和性。默认情况下，列表会保留 2 小时，但可以使用 jetPACK 进行更改。
基于共享 IP 列表	此服务类型仅在连接模式设置为直接服务器返回时可用。添加该服务类型主要是为了支持 VMware 负载均衡。
持久 Cookie	第 7 层会话亲和性/持久性 基于 IP 列表的负载平衡模式用于每个首次请求。ADC 会在第一个 HTTP 响应的标题中插入 cookie。之后，ADC 会使用客户端 cookie 将流量路由到同一个后端服务器。当客户端每次都必须访问同一个后端服务器时，这个 cookie 就会被用于持久化。Cookie 将在 2 小时后过期，连接将根据基于 IP 列表的算法进行负载平衡。该过期时间可通过 jetPACK 进行配置。
经典 ASP 会话 Cookie	Active Server Pages (ASP) 是一种微软服务器端技术。选中该选项后，如果在已知 cookie 列表中检测到并找到 ASP cookie，ADC 将保持会话持续到同一服务器。检测到新的 ASP cookie 时，将使用 "最少连接 "算法进行负载平衡。
ASP.NET 会话 Cookie	此模式适用于 **ASP.net**。选择该模式后，如果检测到 ASP.NET cookie 并在其已知 cookie 列表中找到该 cookie，ADC 将保持会话持续到同一服务器。检测到新的 ASP cookie 时，将使用 "最少连接 "算法进行负载平衡。
JSP 会话 Cookie	Java Server Pages (JSP) 是 Oracle 服务器端技术。选择该模式后，如果检测到 JSP cookie 并在其已知 cookie 列表中找到该 cookie，ADC 将保持会话持续到同一服务器。检测到新的 JSP cookie 时，将使用 "最少连接 "算法进行负载平衡。
JAX-WS 会话 Cookie	Java Web 服务 (JAX-WS) 是 Oracle 服务器端技术。选择该模式后，如果检测到 JAX-WS cookie 并在其已知 cookie 列表中找到该 cookie，ADC 将保持会话持续到

	同一服务器。检测到新的 JAX-WS cookie 时，它将使用 "最少连接 "算法进行负载平衡。
PHP 会话 Cookie	个人主页 (PHP) 是一种开源服务器端技术。选择该模式后，当检测到 PHP cookie 时，ADC 将在同一服务器上保持会话持久性。
RDP Cookie 持久性	这种负载平衡方法使用基于用户名/域的 Microsoft 创建的 RDP Cookie 来提供与服务器的持久性。这种方法的优点是，即使客户端的 IP 地址发生变化，也能保持与服务器的连接。
基于 CookieID	与 "PhpCookieBased "和其他负载平衡方法非常相似的新方法，但使用的是 CookieIDBased 和 cookie RegEx h=[^;]+ 该方法将使用真实服务器备注字段 "ID=X; "中设置的值作为 cookie 值来识别服务器。因此，这意味着它是一种与 CookieListBased 类似的方法，但使用不同的 cookie 名称并存储唯一的 cookie 值，而不是加扰 IP，而是真实服务器的 ID（在加载时读入）。 默认值为 CookieIDName="h"；但是，如果虚拟服务器的高级设置配置中有覆盖值，请使用此值。**注意**：如果设置了该值，我们将覆盖上面的 cookie 表达式，用新值替换 h=。 最后一点是，如果未知 cookie 值到达并与其中一个真实服务器 ID 匹配，则应选择该服务器；否则，使用下一个方法（委托。）

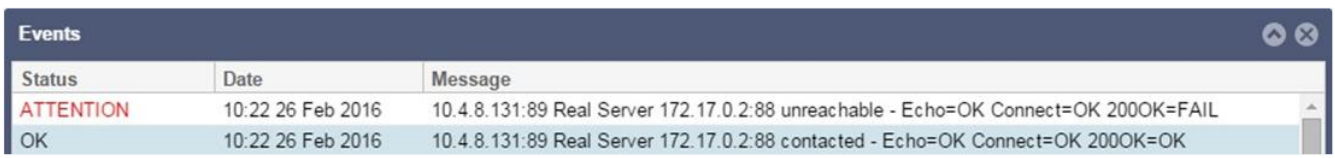
服务器监控

ADC 包含多种预定义的真实服务器监控方法。

选择希望应用于虚拟服务 (VIP) 的监控方法

为服务选择合适的监控器至关重要。例如，如果真实服务器是 RDP 服务器，那么 200OK 监视器就没有意义。同样，选择 TCP 连接和 200OK 也没有意义，因为 200OK 需要一个正常的 TCP 连接才能工作。如果不确定选择哪个监视器，默认的 TCP 连接是一个很好的起点

您可以单击希望应用于服务的每个监控程序，从而选择多个监控程序。所选监控程序会按照您选择顺序执行；因此，请先从较低层的监控程序开始。例如，设置监视器 Ping/ICMP Echo、TCP 连接和 200OK 后，仪表板事件将显示如下图所示：



我们可以看到，如果查看最上面一行，第 3 层 Ping 和第 4 层 TCP 连接已经成功，但第 7 层 200OK 失败。这些监控结果提供了足够的信息，表明路由正常，相关端口上有服务在运行，但网站没有正确响应请求的页面。现在可以查看网络服务器和库 > 实时服务器监控部分，以了解故障监控的详细信息。

选项	说明
无	在此模式下，真实服务器不受监控，始终正常运行。无 "设置适用于监控会扰乱服务器的情况，也适用于不应加入 ADC 故障切换操作的服务。它是托管不可靠系统或对 H/A 操作不重要的传统系统的一种途径。对任何服务类型都可使用此监控方法。
Ping/ICMP Echo	在这种模式下，ADC 会向内容服务器的 IP 发送 ICMP echo 请求。如果收到有效的回声响应，ADC 就会认为真实服务器正常运行，服务器的流量吞吐也会继续。它还将保持 H/A 对上的服务可用。这种监控方法适用于任何服务类型。
TCP 连接	在此模式下，会与真实服务器建立 TCP 连接，并在不发送任何数据的情况下立即中断连接。如果连接成功，ADC 就会认为真实服务器正常运行。这种监控方法适用于任何服务类型，UDP 服务目前不适合 TCP 连接监控。
ICMP 无法连接	ADC 将向服务器发送 UDP 健康检查，并在收到 ICMP 端口不可达消息时将真实服务器标记为不可用。当需要检查服务器上的 UDP 服务端口（如 DNS 53 端口）是否可用时，这种方法会很有帮助。
RDP	在这种模式下，TCP 连接的初始化过程如 ICMP 不可到达方法中所述。连接初始化后，将请求第 7 层 RDP 连接。如果链接得到确认，ADC 就会认为真实服务器已启动并正在运行。这种监控方法适用于任何 Microsoft 终端服务器。
200 OK	在这种方法中，一个 TCP 连接初始化到真实服务器。连接成功后，ADC 向真实服务器发送 HTTP 请求。等待 HTTP 响应并检查 "200 OK "响应代码。如果收到 "200 OK "响应代码，ADC 就会认为真实服务器已启动并正在运行。如果 ADC 因任何原因（包括超时、连接失败和其他原因）未收到 "200 OK "响应代码，则 ADC 会标记真实服务器不可用。这种监控方法只适用于 HTTP 和加速 HTTP 服务类型。如果 HTTP 服务器使用的是第 4 层服务类型，则在真实服务器上未使用 SSL 或未通过 "内容 SSL "设施进行适当处理的情况下可以使用。
DICOM	以 DICOM 模式初始化与真实服务器的 TCP 连接，并在连接时向真实服务器发出 Echoscu "关联请求"。包括来自内容服务器的 "关联接受"、少量数据传输以及 "释放请求 "和 "释放响应 "的对话将成功结束监控。如果监控未成功完成，则真实服务器会因任何原因被视为停机。
用户定义	在真实服务器监控部分配置的任何监控器都将出现在列表中。

缓存策略

默认情况下，缓存策略被禁用并设置为关。如果服务类型为 HTTP，则可以应用两种缓存策略。

请参阅 "配置缓存 "页面配置详细的缓存设置。请注意，当缓存应用于具有加速 "HTTP "服务类型的 VIP 时，压缩对象不会被缓存。

选项	说明
主持人	每个主机的缓存基于每个主机名的应用程序。每个域/主机名都有一个单独的缓存。这种模式非常适合可根据域为多个网站提供服务的网络服务器。

虚拟服务	选择此选项时，可对每个虚拟服务进行缓存。通过虚拟服务的所有域/主机名将只存在一个缓存。该选项是用于单个站点的多个克隆的专业设置。

加速度

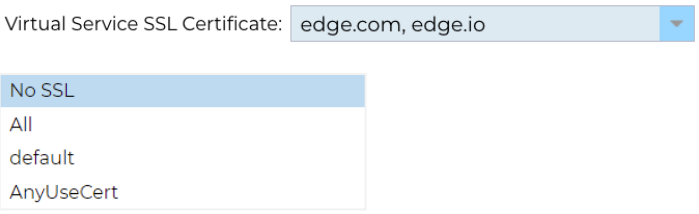
选项	**说明**
关闭	关闭虚拟服务的压缩功能
压缩	选中后，该选项将打开所选虚拟服务的压缩功能。ADC 会根据请求向客户端动态压缩数据流。此过程只适用于包含 content-encoding: gzip 标头的对象。示例内容包括 HTML、CSS 或 JavaScript。您还可以使用 "全局排除 "部分排除某些内容类型。

注：如果对象是可缓存的，ADC 将存储一个压缩版本，并静态（从内存）提供该版本，直到内容过期并重新验证。

虚拟服务 SSL 证书（客户端与 ADC 之间的加密）

默认情况下，设置为无 SSL。如果服务类型为 "HTTP"，则可以从下拉菜单中选择一个证书应用于虚拟服务。已创建或导入的证书将显示在此列表中。

您还可以高亮显示多个证书，以便应用于一项服务。此操作将自动启用 SNI 扩展，以允许使用基于客户端请求的 "域名 "的证书。



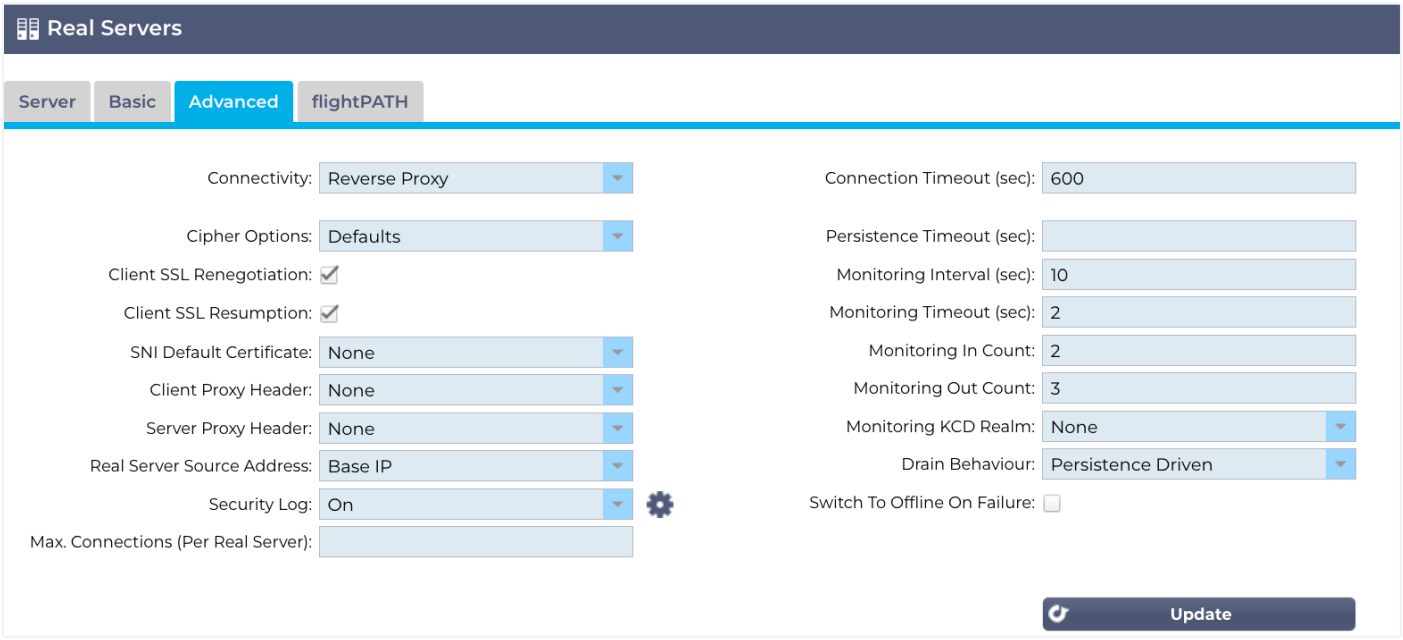
选项	**说明**
无 SSL	从信号源到 ADC 的流量不加密。
全部	加载所有可用证书以供使用
默认值	该选项会将本地创建的名为 "默认 "的证书应用到通道的浏览器端。在尚未创建或导入 SSL 时，可使用此选项测试 SSL。

真实服务器 SSL 证书（ADC 与真实服务器之间的加密）

该选项的默认设置为无 SSL。如果服务器需要加密连接，则该值必须是 "无 SSL "以外的值。已创建或导入的证书将显示在此列表中。

选项	说明
无 SSL	从 ADC 到真实服务器的流量不加密。在浏览器端选择证书意味着可以在客户端选择 "无 SSL"，以提供所谓的 "SSL 卸载"。
任何	ADC 充当客户端，接受真实服务器提供的任何证书。选择该选项时，从 ADC 到真实服务器的流量将被加密。在虚拟服务端指定证书时使用 "任意 "选项，提供所谓的 "SSL 桥接 "或 "SSL 重新加密"。
SNI	SNI 或服务器名称指示是 TLS 网络协议的扩展，客户端在 握手过程开始时，会使用 SNI 指示试图连接的主机名。此设置允许 ADC 在同一虚拟 IP 地址和 TCP 端口上显示多个证书。
默认值	您生成的任何自签名证书都会出现在这里。

高级



连接性

您的虚拟服务可配置不同类型的连接。请选择适用于服务的连接模式。

选项	说明
反向代理	反向代理是默认值，与第 7 层一起使用时会使用压缩和缓存。在第 4 层，反向代理不使用缓存或压缩。在这种模式下，ADC 充当反向代理，成为真实服务器看到的源地址。
服务器直接返回	直接服务器返回或 DSR 也称为 DR - Direct Routing，允许负载平衡器后面的服务器绕过 ADC 直接响应客户端。DSR 仅适用于第 4 层负载平衡。因此，选择该选项时，缓存和压缩功能不可用。 **该模式只能用于 TCP、UDP 和 TCP/UDP 服务类型。** 负载平衡持续策略也仅限于 "最少连接"、"基于共享 IP 列表"、"轮循 "和 "基于 IP 列表"。

	Least Connection Shared IP List Based Round Robin IP List Based 使用 DSR 还需要对真实服务器进行更改。请参阅 "真实服务器更改 "部分。
北约	默认情况下，ADC 使用 ADC 的 IP 地址作为源 IP 地址，然后真实服务器将响应发送回 ADC，再返回给客户端。这在几乎所有情况下都没有问题，但在某些情况下，真实服务器需要看到客户端而不是 ADC 的源 IP 地址。 应用 NAT 模式时，ADC 会接收传入的请求，然后在将源 IP 地址改回虚拟服务（VIP 地址）后将其发送到真实服务器。 **该模式只能与以下负载平衡策略一起使用：** Least Connection Round Robin IP List Based
网关	网关模式允许您通过 ADC 路由所有流量，允许真实服务器通过 ADC 虚拟服务或硬件接口路由到其他网络。在多接口模式下运行时，将设备用作真实服务器的网关设备最为理想。 负载平衡持续策略也仅限于 "最少连接"、"基于共享 IP 列表"、"轮循 "和 "基于 IP 列表"。 Least Connection Shared IP List Based Round Robin IP List Based 此方法要求真实服务器将其默认网关设置为 ADC 的本地接口地址（eth0、eth1 等）。请参阅 "真实服务器更改 "部分。 ***请注意，网关模式不支持群集环境中的故障切换。***

密码选项

密码是 SSL 加密技术的基础，对于成功、安全地传输网络内容和应用程序极为重要。

ADC 内置一套默认密码，包括最新的安全密码。

有时用户希望公布一组特定的密码，ADC 允许通过用户编写的 jetPACKS 创建此类密码。

每个 VIP 都有特定的密码选项，具有高度的灵活性和安全性。

有关密码选项的更多信息，请参阅：*Cipher*

客户端 SSL 重新协商

如果希望允许客户端启动 SSL 重新协商，请勾选该复选框。取消勾选此选项，禁用客户端 SSL 重新协商，以防止任何可能针对 SSL 层的 DDOS 攻击。

客户端 SSL 恢复

如果希望启用添加到会话缓存的 SSL 恢复服务器会话，请勾选此框。当客户端提议重新使用会话时，服务器将尝试重新使用已找到的会话。如果未选中恢复，客户端或服务器都不会进行会话缓存。

SNI 默认证书

在启用客户端 SNI 的 SSL 连接期间，如果请求的域与分配给服务的任何证书不匹配，ADC 将显示 SNI 默认证书。默认设置为 "无"，如果没有完全匹配的证书，则会有效地中断连接。从下拉菜单中选择任何已安装的证书，以便在 SSL 证书精确匹配失败时显示。

代理协议

代理协议旨在允许网络代理将客户端连接信息（如源 IP 地址和端口号）转发到接收服务器。当流量通过负载平衡器或反向代理时，需要保留实际的最终用户 IP 地址，这时该协议就特别有用。它有助于为日志、统计或安全目的保留原始客户端的源 IP，提高根据流量的真实来源做出明智决策的能力。

客户端代理标头

客户端代理标头（Client Proxy Header）是指 ADC 添加到客户端请求中的标头，封装了原始连接信息（如客户端的 IP 地址和端口）。在 ADC 充当代理的环境中，这一点至关重要，因为服务器需要知道原始客户端详细信息，以便进行日志记录、安全评估和维护客户端特定行为。客户端代理标头确保，尽管 ADC 起着中介作用，服务器仍能准确识别客户端的原始连接详细信息并与之交互。

选项包括

选项	说明
无	当没有代理标头或当前服务类型不支持代理标头时
移除	删除 TCP 数据包中的代理标头
转发	将代理标头转发给服务器

服务器代理标头

服务器代理标头有两个版本：版本 1 和版本 2。

选项	说明
版本 1	• 基于文本格式，易于实施和调试。 • 提供客户端连接的基本信息，包括源 IP、目标 IP、源端口和目标端口。 • 协议行被添加到 TCP 连接的开头，使其可由人工读取，但与二进制格式相比，在性能方面效率略低。
第 2 版	• 二进制格式，旨在提高性能和效率。 • 扩展可转发的连接信息，支持地址族和协议特定信息等附加数据。 • 确保更好地兼容现代网络协议和功能，包括支持 IPv6 和 TCP 以外的传输协议。

客户端代理标头和服务器代理标头选项仅适用于第 4 层和第 7 层 HTTP 服务类型。

真实服务器源地址

该设置与反向代理和第 4 层 TCP、第 4 层 UDP 或 HTTP(S) 服务一起使用。该设置提供三个选项供您选择。

选项	说明
基础 IP（默认）	使用 ADC 的 eth0 或 Base IP 地址作为请求的源 IP。
虚拟 IP	使用服务的虚拟 IP。
<IP 地址	允许您指定属于 ADC 的 IP 地址。这可以是不同的网络接口或不同的 VIP。

安全日志

开 "是默认值，以每个服务为单位，启用将身份验证信息记录到 W3C 日志的服务。单击 Cog 图标将进入系统 > 日志页面，在这里可以检查 W3C 日志的设置。

最大连接数

限制真实服务器并发连接数，按服务设置。例如，如果您将其配置为 1000 并拥有两个真实服务器，则 ADC 会将**每个**真实服务器的并发连接数限制为 1000。您还可以选择在所有服务器达到此限制后显示 "服务器太忙 "页面，帮助用户了解出现无响应或延迟的原因。留空表示无限制连接。此处的设置取决于系统资源。

连接超时

默认连接超时为 600 秒或 10 分钟。此设置将调整连接在无活动时的超时时间。对于无状态的短时网络流量（通常为 90 秒或更短），请缩短超时时间。对于有状态连接（如 RDP），可根据您的基础架构，将此值增

加到 7200 秒（2 小时）或更长。RDP 超时示例意味着，如果用户的不活动时间为 2 小时或更短，连接将保持打开。

持久性超时

负载平衡器中的 "持久超时 "设置指定了负载平衡器维护客户端会话信息的持续时间。这可确保同一客户端的后续请求指向同一后端服务器，从而促进会话一致性和有状态通信。一旦过了指定的超时时间，客户端没有进一步的活动，会话信息就会被丢弃，新的请求可能会被路由到不同的服务器。

监测间隔

间隔是显示器之间的时间间隔（以秒为单位）。默认间隔为 1 秒。对于大多数应用来说，1 秒是可以接受的，但对于其他应用或在测试期间，增加间隔时间可能会有好处。

监控超时

超时值是指 ADC 等待服务器响应连接请求的时间。默认值为 2 秒。如果服务器繁忙，请增加此值。

监测计数

此设置的默认值为 2。 2 表示真实服务器必须通过两次成功的健康监控检查后才能上线。增加该值将提高服务器可以提供流量的概率，但根据时间间隔的不同，服务器投入使用的时间会更长。降低该值将使服务器更快投入使用。

监测输出计数

此设置的默认值为 3，这意味着真实服务器监控器必须失败三次，ADC 才会停止向服务器发送流量，并将其标记为 "RED "和 "无法访问"。增加这个数字 将带来更好、更可靠的服务，但要牺牲 ADC 停止向该服务器发送流量所需的时间。

监测 KCD 领域

此设置允许您启用对在 Kerberos 定义中设置的 Kerberos 受限委托域的监控。请参阅身份验证 > Kerberos。

排水行为

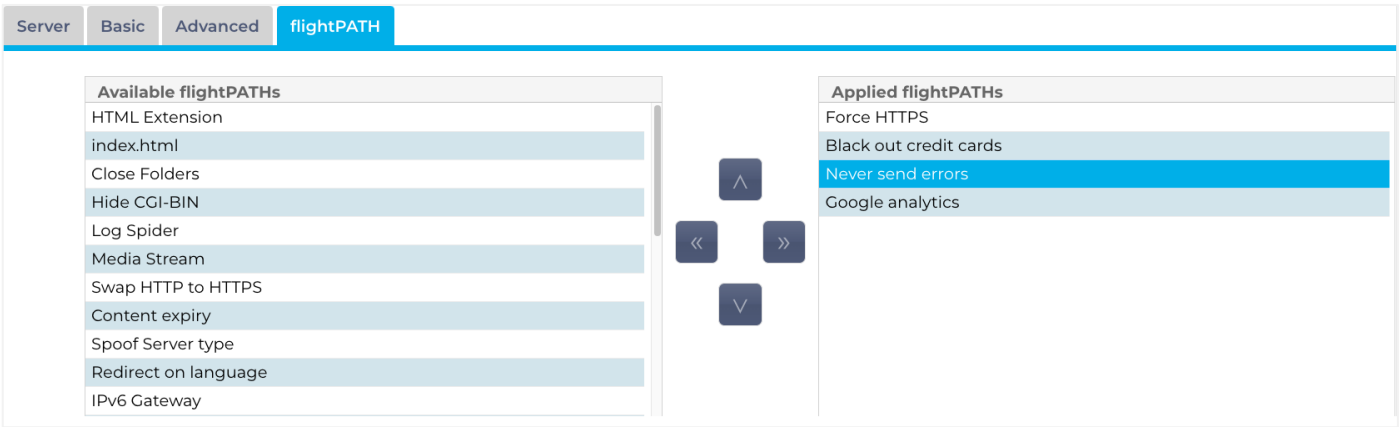
无论何时将任何真实服务器置于耗尽模式，最好都能控制向其发送的流量行为。通过 "耗尽行为 "菜单，可以根据每个虚拟服务选择流量行为。选项包括

选项	说明
持久性驱动	这是默认选择。 每当用户使用持久会话访问时，该会话就会被扩展。 在 24 小时使用的情况下，有可能永远不会发生排水。 但是，如果连接到真实服务器的连接数达到 0，泄流就会结束，持久会话就会被删除，所有访问者都会在下一次连接时重新获得平衡。
迁移游客	重新连接时忽略持久会话 - （2022 年之前的传统行为） 新的 TCP 连接（无论是否属于现有会话的一部分）总是连接到在线的真实服务器。 如果持久化会话是指向耗尽的真实服务器，则会被覆盖。 虚拟服务将有效忽略任何新连接的持久性，并将它们负载平衡到新服务器上。
退休会议	持续会话未扩展。 传入的用户连接将被分配到所需的服务器，但其持续会话不会被延长。 因此，在超过持续会话时间后，它们将被视为新连接并被转移到不同的服务器上。

故障时切换到脱机状态

选中此选项后，健康检查失败的真实服务器将被置于脱机状态，只能手动设置为联机。

飞行路径



flightPATH 是 Edgenexus 设计的流量管理技术，仅在 ADC 中提供。与其他供应商基于规则的引擎不同，flightPATH 不通过命令行或脚本输入控制台进行操作。相反，它使用图形用户界面来选择不同的参数、条件和要执行的操作，以达到所需的目的。这些功能使 flightPATH 非常强大，网络管理员可以用非常有效的方式操纵 HTTPS 流量。

flightPATH 仅适用于 HTTPS 连接，当虚拟服务类型不是 HTTP 时，此部分将不可见。

从上图可以看到，左侧是可用规则列表，右侧是应用于虚拟服务的规则。

应用可用规则的方法是将规则从左侧拖放到右侧，或突出显示一条规则并单击右箭头将其移到右侧。

执行顺序至关重要，最先执行的规则开始执行。要更改执行顺序，请选中规则并使用箭头上下移动。

必须了解的是，ADC 这一部分中的 flightPATH 规则是以布尔 "**或** "为基础运行的，而 flightPATH 定义区域中的条件和操作是以 **"和 "**为基础运行的。

要删除规则，可将其拖放回左侧的规则清单，或高亮显示规则并单击向左箭头。

您可以在本指南的 "配置 flightPATH "部分添加、删除和编辑 flightPATH 规则。

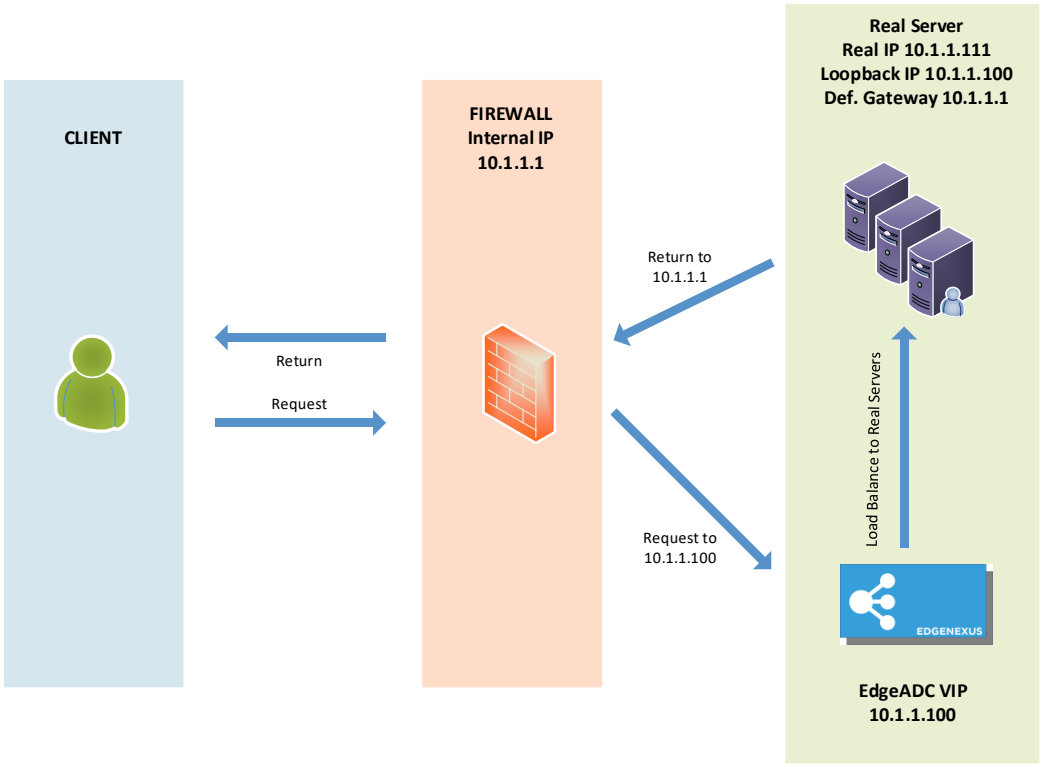
直接返回服务器的真实服务器变更

直接服务器返回（Direct Server Return）或广为人知的 DSR（DR - Direct Routing）允许 ADC 后面的服务器直接响应客户端，在响应时绕过 ADC。DSR 仅适用于第 4 层负载平衡。启用 DSR 后，将无法使用缓存和压缩功能。

使用这种方法的第 7 层负载平衡不可行，因为除了源 IP 外，没有其他持久性支持。使用此方法实现 SSL/TLS 负载平衡并不理想，因为只支持源 IP 持久性。

如何使用

- 客户端向 EdgeADC VIP 发出请求
- EdgeADC 收到的请求
- 请求路由至内容服务器
- 不通过 EdgeADC 直接发送给客户端的响应



所需内容服务器配置

一般情况

- 内容服务器默认网关应按正常方式配置。(不通过 ADC）
- 内容服务器和负载平衡器必须位于同一子网内

视窗

- 内容服务器需要在环回或别名中配置
  通道或 VIP 的 IP 地址
    - 网络度量必须为 254，以防止响应 ARP 请求
    - 在 Windows Server 2012 中添加环回适配器 - 单击此处
    - 在 Windows Server 2003/2008 中添加环回适配器 - 点击此处
- 针对 Windows Real 服务器上配置的每个网络接口，在命令提示符下运行以下命令

netsh interface ipv4 set interface "Windows 网络接口名称" weakhostreceive=enable

netsh interface ipv4 set interface "Windows loopback interface name" weakhostreceive=enable

netsh interface ipv4 set interface "Windows loopback interface name" weakhostsend=enable

利纳克斯

- 添加永久环回接口
- 编辑"/etc/sysconfig/network-scripts"（/etc/sysconfig/网络脚本

ifcfg-lo:1
DEVICE=lo:1
IPADDR=x.x.x.x
NETMASK=255.255.255.255
BROADCAST=x.x.x.x
ONBOOT=yes

- 编辑"/etc/sysctl.conf"

net.ipv4.conf.all.arp_ignore = 1
net.ipv4.conf.eth0.arp_ignore = 1
net.ipv4.conf.eht1.arp_ignore = 1
net.ipv4.conf.all.arp_announce = 2
net.ipv4.conf.eth0.arp_announce = 2
net.ipv4.conf.eth1.arp_announce = 2

- 运行 "sysctl - p"

真实服务器更改 - 网关模式

网关模式允许您通过 ADC 路由所有流量，这样就可以通过 ADC 将源自内容服务器的流量通过 ADC 设备上的接口路由到其他网络。在多接口模式下运行时，应将设备用作内容服务器的网关设备。

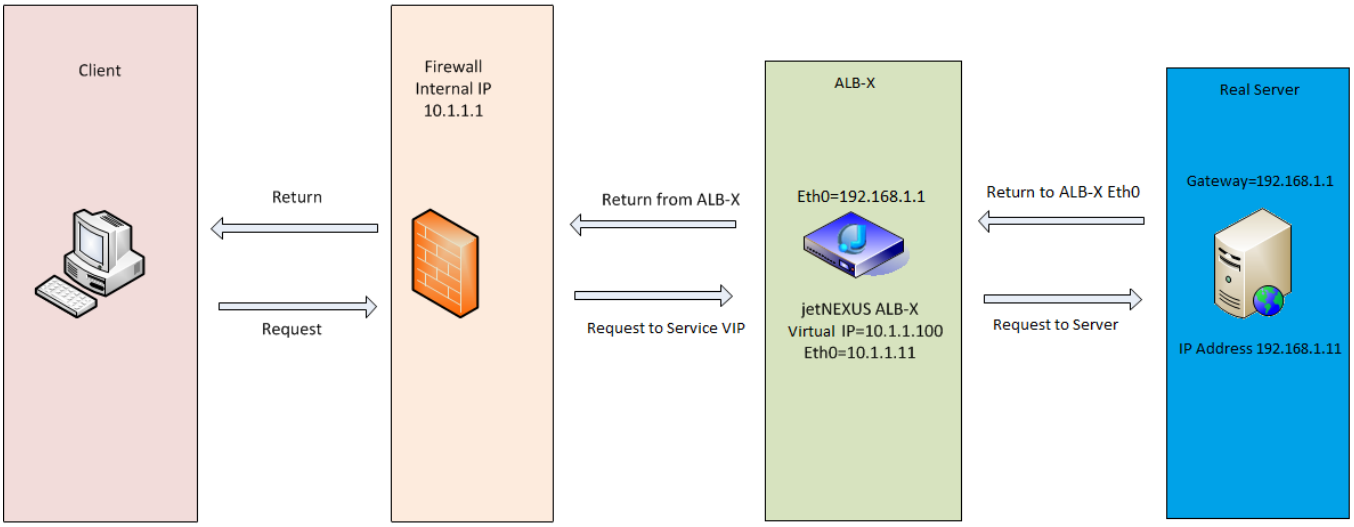
工作原理

- 客户端向 EdgeADC 发送请求
- EdgeADC 收到请求
- 向内容服务器发送请求
- 已向 EdgeADC 发出答复
- ADC 将响应路由到客户端

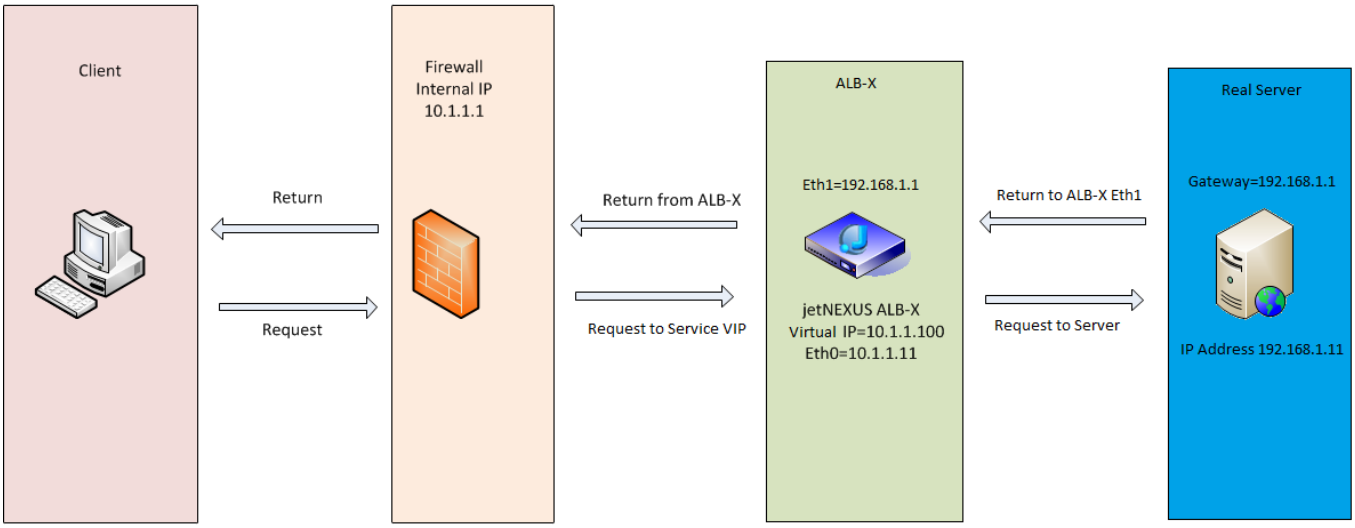
所需内容服务器配置

- 单臂模式 - 使用一个接口，但服务 VIP 和真实服务器必须位于不同的子网。
- 双臂模式 - 使用两个接口，但服务 VIP 和实际服务器必须位于不同的子网。
- 在单臂和双臂的每种情况下，真实服务器都需要将其默认网关配置为相关子网中的 ADC 接口地址。

单臂示例



双臂示例

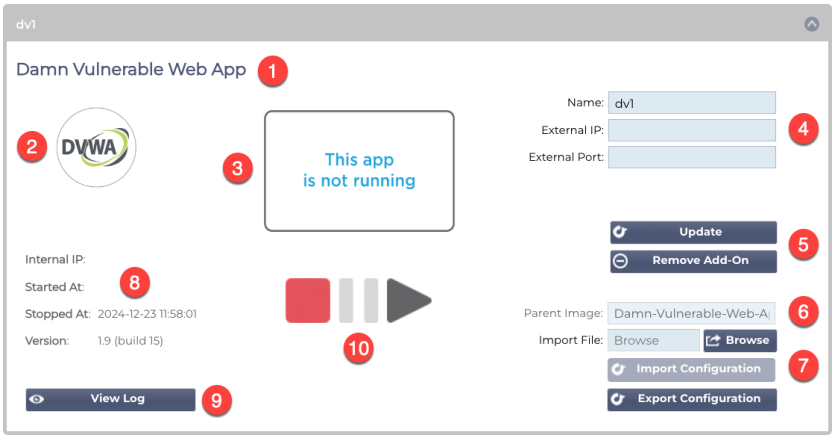

Client
Return
Request
Firewall
Internal IP
10.1.1.1
Return from ALB-X
Request to Service VIP
ALB-X
Eth1=192.168.1.1
jetNEXUS ALB-X
Virtual IP=10.1.1.100
Eth0=10.1.1.11
Return to ALB-X Eth1
Request to Server
Real Server
Gateway=192.168.1.1
IP Address 192.168.1.11

图书馆

附加组件

附加组件是作为容器加载的应用程序，在 ADC 内以隔离模式运行。附加组件的例子可以是应用防火墙，甚至是 ADC 本身的微型实例。

如本指南所述，应用程序通过应用程序页面部署到附加组件部分。应用程序部署完成后会显示如下内容。



从上图可以看出，有几个元素被突出显示。

项目	说明
❶	应用程序标题
❷	应用程序图标
❸	应用程序运行显示。如果应用程序正在运行，则会显示屏幕的缩略图。
❹	访问详情： **名称**：这是一个内部名称，用于在虚拟服务部分中引用应用程序。不能使用 IP 地址引用应用程序。只能是字母数字，不能有空格。 **外部 IP**：这是您必须为应用程序提供的 IP 地址。这将是你的网络子网的一部分。 **外部端口**：这是一个重要字段。您需要指定用于访问 App 的端口。当外部流量访问 App 时，您需要使用以下符号指定端口：53/tcp 或 53/udp。此外，您还需要指定 App 的用户界面端口。这些信息显示在每个 App 的字段工具提示中。
❺	更新按钮：填写❸ 中指定的详细信息后，单击此按钮确认条目并配置应用程序。 移除附加组件按钮用于将其从应用程序部分移除。要移除应用程序，请确保在尝试移除之前移除应用程序的所有引用。
❻	父图像是一个信息字段，从用户角度看未使用。
❼	导入和导出配置对于备份设置非常重要。 使用此功能可执行导入和导出功能。
❽	运行详情提供内部 API IP 地址、开始和停止时间以及应用程序版本号等信息。
❾	此按钮允许您下载并查看日志。这主要用于需要开支持单时。
❿	应用程序的操作通过这些按钮进行。红色=停止，金色=启动，绿色=运行。

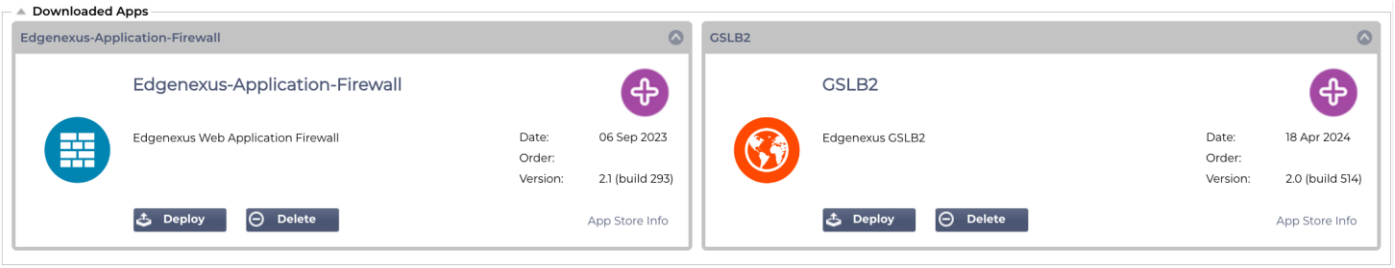
应用程序

应用程序 "部分有几个子部分，用于处理 ADC 上可用的应用程序。它们是 "过滤器"、"下载的应用程序 "和 "购买的应用程序"。

过滤器

通过 "筛选器"，您可以根据应用程序/工具的类型对其进行筛选。

下载的应用程序

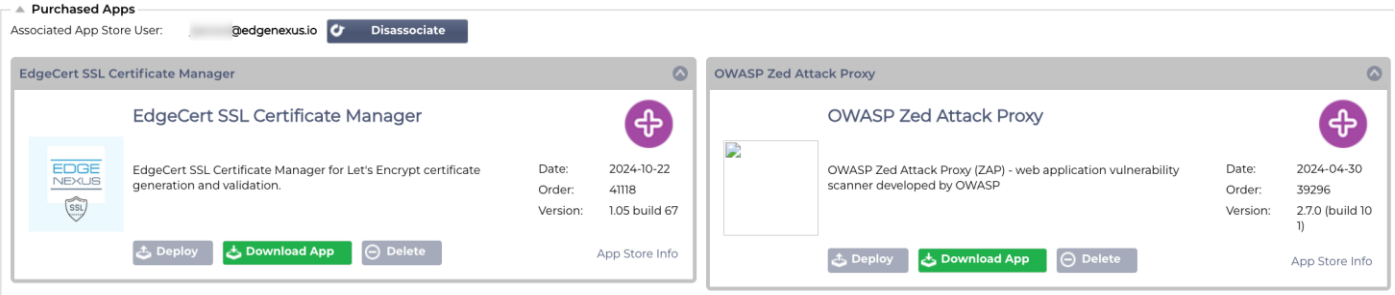


本部分包含已下载到 ADC 的应用程序。您可以将它们下载到本地桌面，然后上传到 ADC，也可以通过内置的 App Store 门户下载。

每个应用程序都配有两个按钮，以及显示其版本号和发布日期的数据。

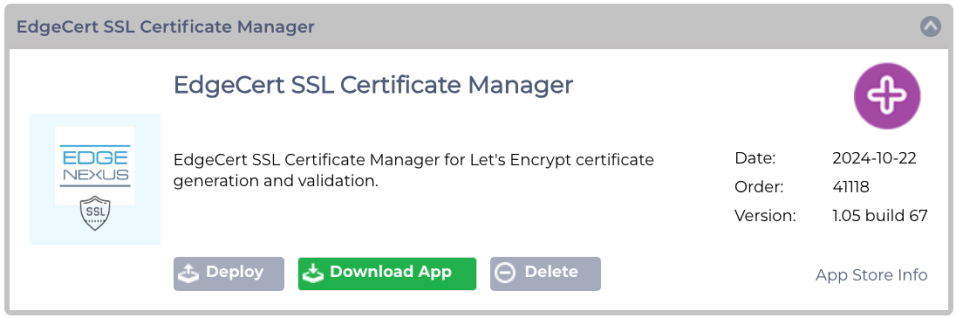
部署按钮将以安全容器的形式部署应用程序，而删除按钮将从 ADC 中删除应用程序。

购买的应用程序



首先要注意的是关联 App Store 用户及其相关按钮。您需要使用 App Store 凭据登录，以便将 ADC 与 App Store 关联。在此下方，您可以找到与您账户关联的应用程序。

直接或通过内置门户登录 App Store 后，即可购买应用程序。这些应用程序将在本节中显示，并可上传到 ADC 以备部署。



每个应用程序都有多个按钮：部署、下载应用程序和删除。除此以外，右侧还有一个 App Store Info（应用商店信息）链接，它将带您进入相关的 App Store 页面，并显示有关该插件的信息。

部署

附加组件中的 "应用程序 "部分详细列出了您已购买、下载和部署的应用程序。一旦部署，应用程序将显示在 "已下载 "部分。

下载应用程序

点击此按钮可从 App Store 下载该应用程序。

删除

如果您想删除已下载的应用程序。

认证

图书馆> 身份验证页面允许您设置身份验证服务器和创建身份验证规则。

设置身份验证 - 工作流程

请至少执行以下步骤，将身份验证应用到您的服务中。

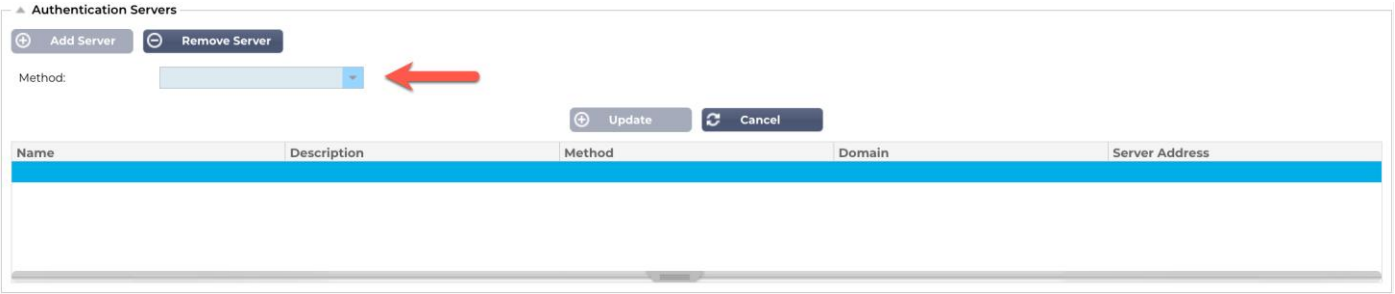
1. 创建身份验证服务器。
2. 创建使用身份验证服务器的身份验证规则。
3. 创建使用身份验证规则的 flightPATH 规则。
4. 将 flightPATH 规则应用于服务

认证服务器

要建立有效的身份验证方法，我们必须首先建立一个身份验证服务器。

第一阶段是选择所需的身份验证方法。

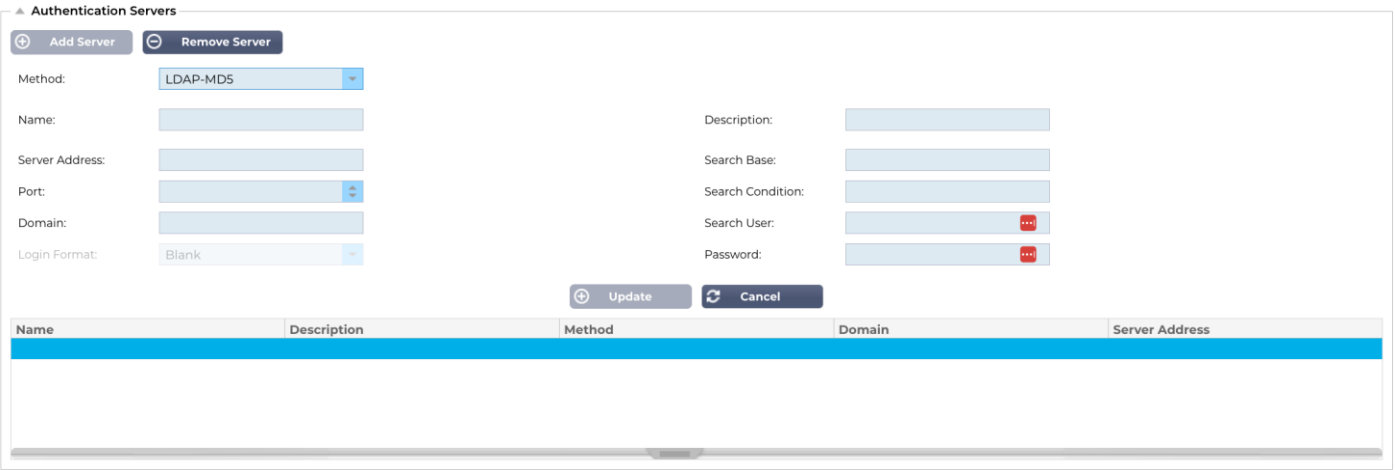
- 单击添加服务器。
- 从下拉菜单中选择方法。



身份验证服务器功能是动态的，只显示您选择的身份验证方法所需的字段。

- 请准确填写，以确保与服务器的正确连接。

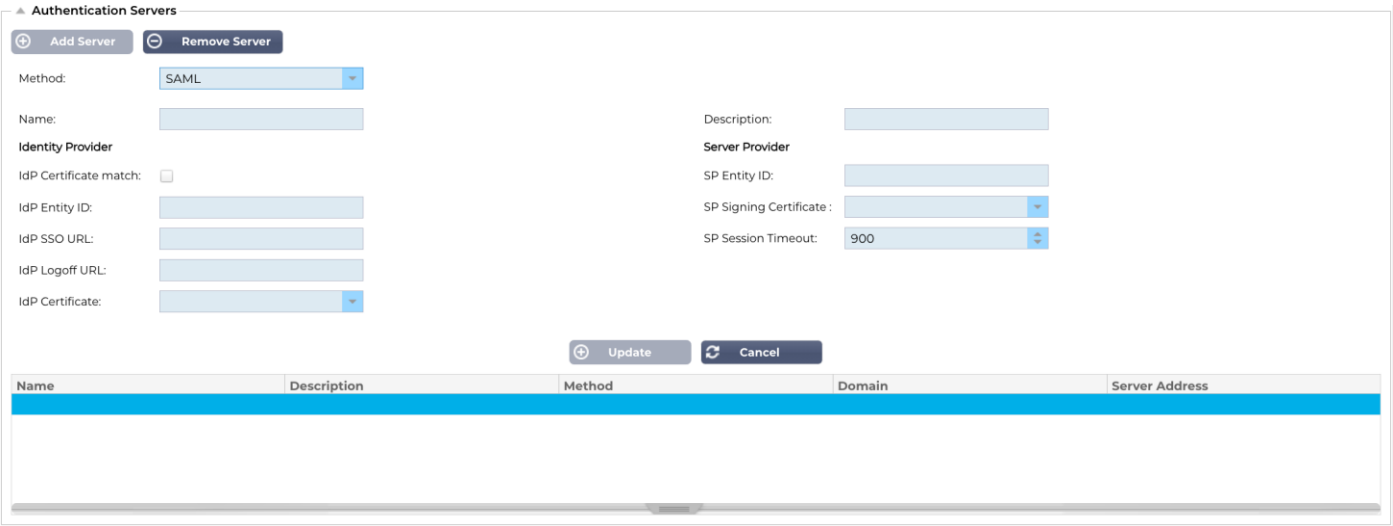
LDAP、LDAP-MD5、LSAPS、LDAPS-MD5、Radius 和 SAML 的选项



选项	说明
方法	选择验证方法 LDAP - 基本 LDAP，用户名和密码以明文发送到 LDAP 服务器。 LDAP-MD5 - 基本 LDAP，用户名为明文，密码为 MD5 哈希值，以提高安全性。 LDAPS - 通过 SSL 的 LDAP。通过 ADC 和 LDAP 服务器之间的加密隧道以明文发送密码。 LDAPS-MD5 - 通过 SSL 的 LDAP。在 ADC 和 LDAP 服务器之间的加密隧道中，密码经过 MD5 散列处理，以提高安全性。
名称	为您的服务器起一个用于识别的名称--该名称将在任何规则中使用。
服务器地址	添加身份验证服务器的 IP 地址或主机名
港口	对于 LDAP 和 LDAPS，端口默认设置为 389 和 636。 Radius 的端口一般为 1812。 对于 SAML，端口在 ADC 中设置。
域名	添加 LDAP 服务器的域名。
登录格式	使用您需要的登录格式。 用户名 - 选择此格式后，只需输入用户名。用户输入的任何用户和域信息都会被删除，并使用服务器上的域信息。 用户名和域 - 用户必须输入完整的域和用户名语法。例如：*mycompany\jdoe OR jdoe@mycompany*。在服务器级别输入的域信息将被忽略。 空白 - ADC 将接受用户输入的任何内容并将其发送到身份验证服务器。使用 MD5 时使用此选项。
说明	添加说明
搜索基地	该值是在 LDAP 数据库中搜索的起点。 示例 *dc=mycompany,dc=local*
搜索条件	搜索条件必须符合 RFC 4515。例如 (MemberOf=CN=Phone-VPN,CN=Users,DC=mycompany,DC=local）。
搜索用户	在目录服务器中搜索域管理用户。
密码	域管理员用户的密码。
死亡时间	非活动服务器重新标记为活动的时间长度

SAML 身份验证的选项

重要：通过 SAML 设置身份验证时，需要为 Entra ID 身份验证创建企业应用程序。相关说明请参阅在 Microsoft Entra 中设置 Entra ID 身份验证应用程序

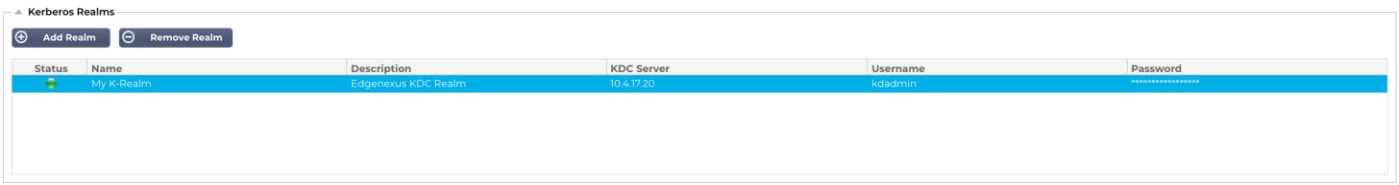


选项	说明
方法	选择验证方法 LDAP - 基本 LDAP，用户名和密码以明文发送到 LDAP 服务器。 LDAP-MD5 - 基本 LDAP，用户名为明文，密码为 MD5 哈希值，以提高安全性。 LDAPS - 通过 SSL 的 LDAP。通过 ADC 和 LDAP 服务器之间的加密隧道以明文发送密码。 LDAPS-MD5 - 通过 SSL 的 LDAP。在 ADC 和 LDAP 服务器之间的加密隧道中，密码经过 MD5 散列，以提高安全性。
名称	为您的服务器起一个用于识别的名称--该名称将在任何规则中使用。
身份供应商	
IdP 证书匹配	身份提供者证书匹配是指验证身份提供者（IdP）用于签署 SAML 声明的数字证书与服务提供商（SP）信任的证书是否匹配的过程。这种验证可确保身份提供者是合法的，其发送的断言是真实的，未被篡改。SP 通常会在其元数据中存储 IdP 的证书，并将 SAML 声明中嵌入的证书与存储的证书进行比较，以确定是否匹配。
IDP 实体 ID	SAML IdP 实体 ID 是一个全球唯一的标识符，是安全断言标记语言（SAML）生态系统中身份提供商（IdP）的明确地址。该标识符通常是一个 URL 或 URI，可将 IDP 与参与基于 SAML 的身份验证和授权流程的其他实体唯一区分开来。它在建立信任和促进 IdP、服务提供商 (SP) 与用户之间的安全通信方面发挥着至关重要的作用。
IdP SSO URL	IdP SSO URL 是单点登录 URL 的简称，是由身份提供商（IdP）提供的特定端点 URL，用作启动单点登录（SSO）会话的身份验证网关。将用户重定向到该 URL 时，IdP 会提示用户使用其凭据进行身份验证，身份验证成功后，IdP 会将用户重定向回服务提供商 (SP)，并提供包含其身份信息的断言。然后，SP 验证该断言，允许用户访问 SP 的资源，而无需重新进行身份验证。

IdP 注销 URL	SAML IdP 注销 URL 是身份供应商（IdP）上的一个特定端点，用于启动和管理单点登录（SSO）会话的注销流程。当用户点击应用程序上的注销按钮时，应用程序会将用户重定向到 IdP 的注销 URL。然后，IdP 会使用户在与 SSO 身份验证相关的所有依赖方上的会话失效，并向应用程序发送注销响应，从而有效地将用户注销所有已连接的应用程序。
IDP 证书	SAML IdP 证书是由可信机构向参与安全断言标记语言（SAML）验证协议的身份提供者（IdP）签发的 X.509 数字证书。该证书是验证身份提供者身份以及验证身份提供者与服务提供商（SP）之间交换的 SAML 信息的完整性和保密性的安全手段。 您可以使用下拉菜单选择将安装在 ADC 中的 IdP 证书。
说明	对定义的描述。
搜索用户	搜索域管理员用户。
密码	用于指定管理员用户的密码。
服务器提供商	
SP 实体 ID	SP 实体 ID 是一个唯一标识符，在 SAML 协议中作为特定服务提供商 (SP) 的全局地址。它是标识 SP 的一种标准化方式，通常是一个 URL 或其他 URI，用于定位 SP 的 SAML 元数据，其中包含加密证书和验证端点等关键信息。
SP 签名证书	SAML SP 签名证书是服务提供商（SP）用来签署 SAML 响应的 X.509 证书，可确保单点登录（SSO）验证过程中 SP 和身份提供商（IdP）之间交换信息的真实性和完整性。SP 使用私钥签署响应，IdP 使用与证书相关的公钥验证签名，确认发送者的身份和信息内容未被篡改。
SP 会话超时	SP 会话超时是指通过身份供应商（IdP）成功单点登录（SSO）后，用户的认证会话在服务供应商（SP）端被视为有效的最长持续时间。超过规定时间后，SP 将终止会话，并要求用户重新认证，以重新获得受保护资源的访问权。这种机制有助于防止未经授权的访问，并确保用户会话不会长时间闲置。

KDC 领域

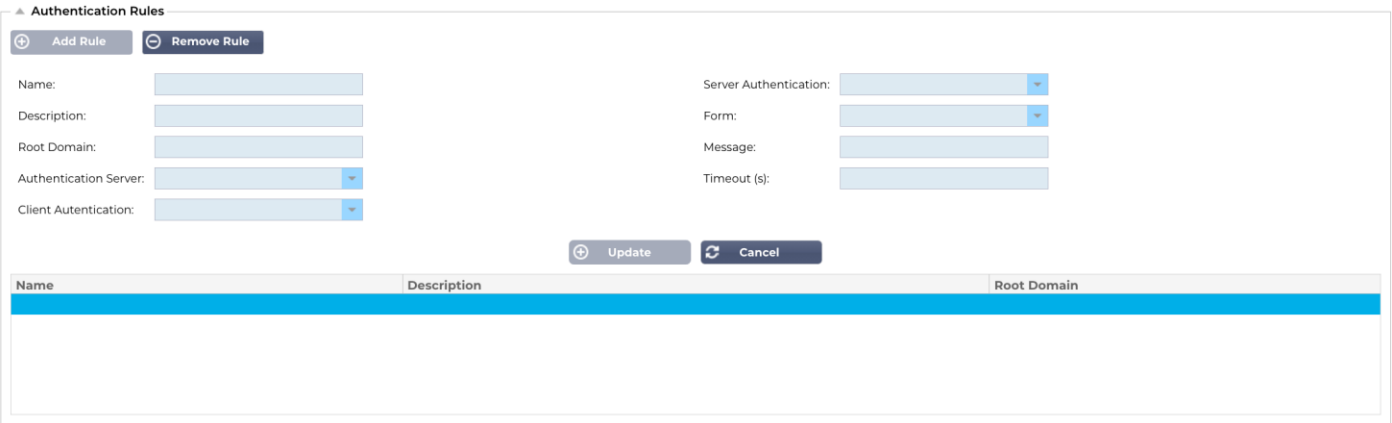
KDC 领域指的是 Kerberos 身份验证协议中的配置，其中每个领域本质上都是一个在单一密钥分发中心（KDC）下运行的域或网络。这种设置划定了在同一个主 KDC 管理下的一组系统，有利于整个网络的安全身份验证和票据授予机制。域可以是分层的，也可以是非分层的，域之间可以建立信任关系，以实现安全的域间身份验证。



ADC 提供的用户界面（如上图所示）允许您定义 Kerberos 领域。这些信息可以在身份验证规则中使用。

验证规则

下一阶段是创建与服务器定义一起使用的身份验证规则。



现场	说明
名称	为身份验证规则添加合适的名称。
说明	添加合适的描述。
根域	除非需要跨子域单点登录，否则必须留空。
认证服务器	这是一个下拉框，包含您已配置的服务器。
客户端验证：	选择适合您需要的值： 基本 (401) - 此方法使用标准 401 验证方法 表单 - 这将向用户显示 ADC 默认表单。您可以在表单中添加信息。您可以通过以下部分选择已上传的表单。
服务器验证	选择合适的值。 无 - 如果您的服务器没有任何现有身份验证，请选择此设置。此设置意味着您可以为以前没有任何身份验证功能的服务器添加身份验证功能。 基本 - 如果服务器已启用基本身份验证 (401)，则选择 BASIC。 NTLM - 如果服务器已启用 NTLM 身份验证，则选择 NTLM。
形式	选择合适的值 默认值 - 选择该选项后，ADC 将使用其内置形式。 自定义 - 您可以添加自己设计的表单，并在此处进行选择。
留言	在表格中添加个人信息。
超时	在规则中添加超时，超时后用户需要再次进行身份验证。请注意，超时设置只对基于表单的身份验证有效。

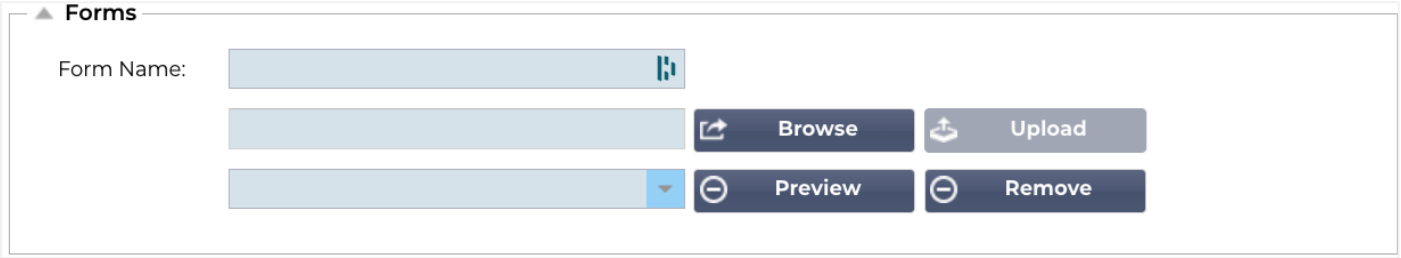
如果希望为用户提供单点登录，请在根域字段中填写您的域名。本例中为 mycompany.com。现在，我们可以使用 edgenexus.io 作为根域来提供多个服务，而且用户只需登录一次。如果我们考虑以下服务

- SharePoint.mycompany.com

- usercentral.mycompany.com
- App Store.mycompany.com

这些服务可以位于一个 VIP 上，也可以分布在 3 个 VIP 上。首次访问 usercentral.mycompany.com 的用户将看到一个要求他们登录的表单，具体取决于所使用的验证规则。然后，同一用户可以连接到 App Store.mycompany.com，并由 ADC 自动进行身份验证。您可以设置超时时间，一旦达到此不活动时间段，就会强制进行身份验证。

表格



本部分可让您上传自定义表单。

如何创建自定义表单

虽然 ADC 提供的基本表单足以满足大多数目的，但在某些情况下，公司希望向用户展示自己的身份。在这种情况下，您可以创建自己的自定义表单，让用户填写。该表单必须是 HTM 或 HTML 格式。

选项	说明
名称	表单名称 = loginform action = %JNURL% 方法 = POST
用户名	语法：name = "JNUSER"
密码	name="JNPASS"
可选信息 1：	%JNMESSAGE%
可选信息 2：	%jnauthmessage%
图片	如果您希望添加图片，请使用 Base64 编码在行内添加。

非常基本和简单的表格的 HTML 代码示例

```
<HTML>
<标题
<标题>认证表单示例</标题
</HEAD>
<BODY
%JNMESSAGE%<br>
<form name="loginform" action="%JNURL%" method="post"> 用户： <input type="text" name="JNUSER" size="20" value=""></br>
```

密码： <input type="password" name="JNPASS" size="20" value=""></br>

<input type="submit" name="submit" value="OK">

</form>

</BODY>

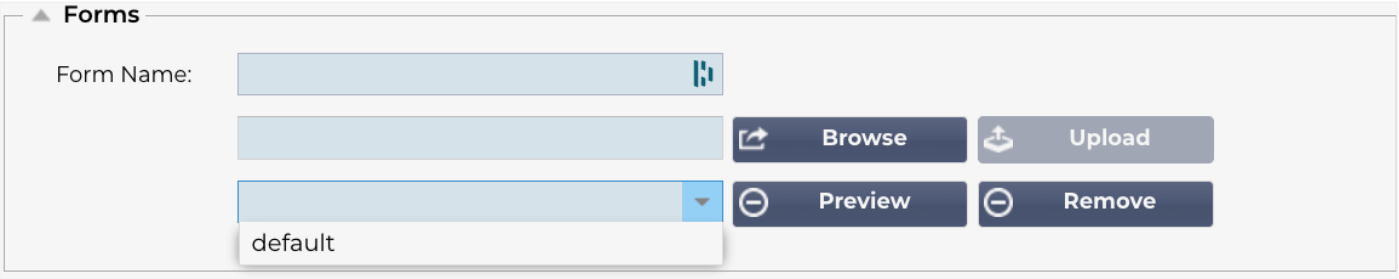
</HTML>

添加自定义表单

创建自定义表单后，可使用表单部分添加表单。

1. 选择表格名称
2. 在本地浏览您的表格
3. 点击上传

预览自定义表单

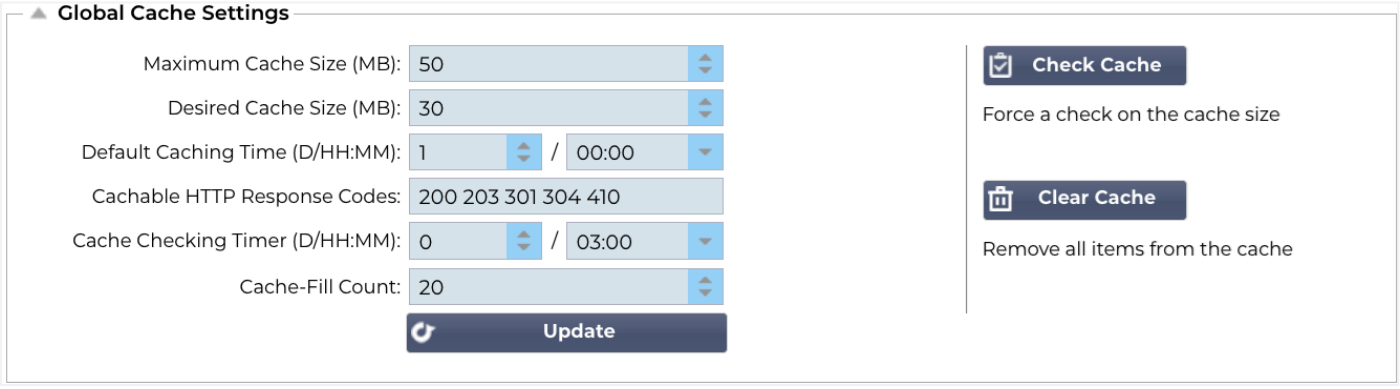


要查看刚刚上传的自定义表单，请选择该表单并单击 "预览"。您还可以使用此部分删除不再需要的表单

注意：使用 AdGuard 等 Cookie 过滤产品时，可能会收到 404 错误信息。将 ADC 的 IP 地址列入白名单可避免出现这种情况。

缓存

ADC 能够在内部存储器中缓存数据，并增强网络服务的交付能力。本节提供了管理此功能的设置。



全局缓存设置

最大缓存大小（MB）

该值决定了缓存可消耗的最大 RAM。ADC 缓存是内存中的缓存，也会定期刷新到存储介质中，以便在重启、重启和关机操作后保持缓存的持久性。这一功能意味着最大缓存大小必须适合设备的内存占用空间（而不是磁盘空间），并且不应超过可用内存的一半。

所需的缓存大小（MB）

该值表示将对高速缓存进行修整的最佳 RAM 值。最大缓存大小代表缓存的绝对上限，而期望缓存大小则是在自动或手动检查缓存大小时，缓存应尝试达到的最佳大小。最大缓存大小和所需缓存大小之间的间隙是为了适应在定期检查缓存大小以删除过期内容之间新内容的到达和重叠。同样，接受默认值（30 MB）并定期检查 "监控 -> 统计 "下的缓存大小以确定适当的大小可能会更有效。

默认缓存时间（日/时：月）

此处输入的值表示没有明确过期值的内容的有效期。默认缓存时间是流量标头中没有 "不存储 "指令或明确过期时间的内容的存储期限。

字段输入的形式为 "D/HH:MM"，因此输入 "1/01:01"（默认为 1/00:00）表示 ADC 将存储一天的内容，"01:00 "表示一小时，"00:01 "表示一分钟。

可缓存的 HTTP 响应代码

其中一个缓存数据集是 HTTP 响应。缓存的 HTTP 响应代码包括

- 200 - 成功 HTTP 请求的标准响应
- 203 - 标头不是确定的，而是从本地或第三方副本中收集的
- 301 - 已为请求的资源分配了新的永久 URL

- 304 - 自上次请求后未修改，应使用本地缓存副本代替
- 410 - 服务器不再提供资源，且不知道转发地址

由于最常见的可缓存响应代码已经列出，因此应谨慎编辑此字段。

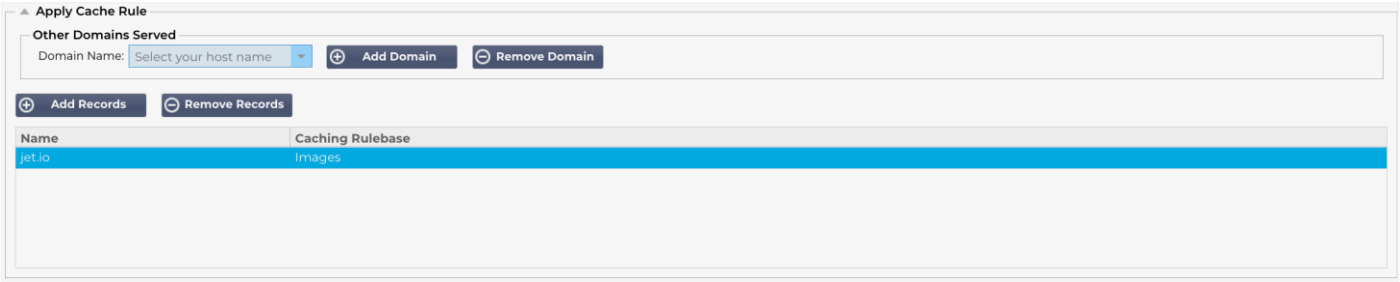
缓存检查计时器（日/时：月）

此设置可确定缓存修整操作之间的时间间隔。

缓存填充计数

此设置是一种辅助功能，当检测到一定数量的 304 时，可帮助填充缓存。

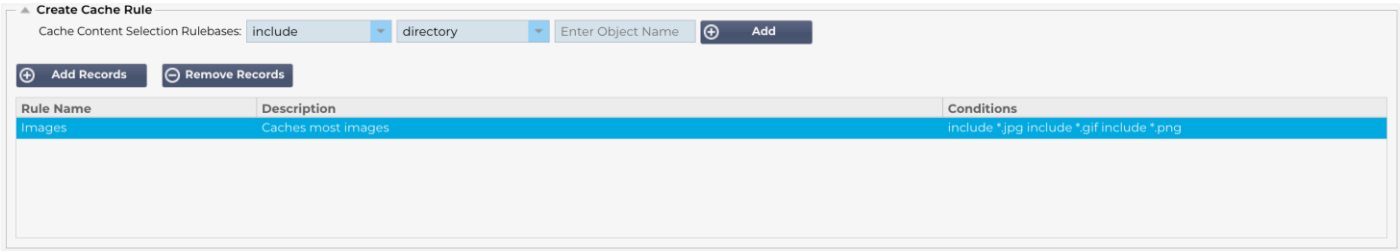
应用缓存规则



本节允许您对域应用缓存规则：

- 使用添加记录按钮手动添加域名。必须使用完全合格的域名或以点十进制表示的 IP 地址。示例 www.mycompany.com 或 192.168.3.1:80
- 点击下拉箭头，从列表中选择你的域名
- 只要流量已通过虚拟服务，且已对虚拟服务应用缓存策略，就会填充该列表
- 双击缓存规则库列，从列表中选择缓存规则

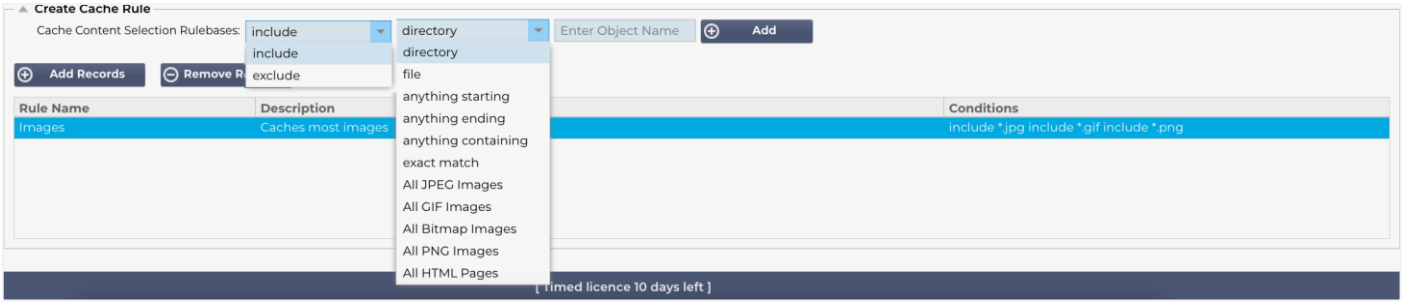
创建缓存规则



本节允许您创建几种不同的缓存规则，然后将其应用于域：

- 单击 "添加记录 "并为规则命名和说明
- 您可以手动输入条件，或使用添加条件

使用选择规则库添加条件：



- 选择 "包括 "或 "不包括"。
- 选择选择标准，例如，所有 JPEG 图像
- 点击 + 添加符号。
- 你会看到 "包含 *.jpg "已被添加到条件中。
- 您可以添加更多条件。如果您选择手动添加，则需要在新行中添加每个条件。请注意，您的规则将显示在同一行中，直到您点击条件框，它们才会显示在单独一行中。

飞行路径

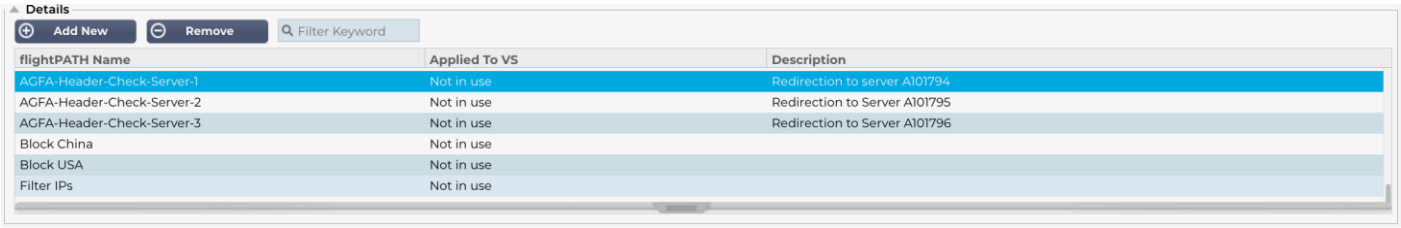
flightPATH 是 ADC 内置的流量管理技术，可以实时检测 HTTP 和 HTTPS 流量，并根据情况执行相应的操作。

要使用 flightPATH 规则，必须使用真实服务器部分的 flightPATH 选项卡将其应用于虚拟服务。

飞行路径规则由四个要素组成：

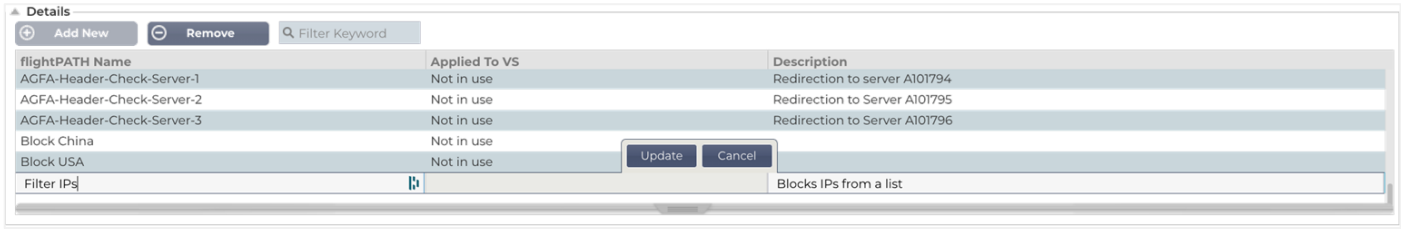
1. 详细信息，在这里您可以定义 flightPATH 名称和附加的服务。
2. 可定义的导致触发规则的条件。
3. 评估功能允许定义可在 "操作 "中使用的变量。
4. 用于管理在满足条件时应发生什么的操作。

详细信息



详细信息部分显示可用的 flightPATH 规则。您可以从该部分添加新的 flightPATH 规则或删除已定义的规则。

添加新的 flightPATH 规则



现场	说明
FlightPATH 名称	此字段为 flightPATH 规则的名称。您在此提供的名称会出现在 ADC 的其他部分中并被引用。
适用于 VS	此列为只读，显示应用了 flightPATH 规则的 VIP。
说明	为便于阅读而提供的描述值。

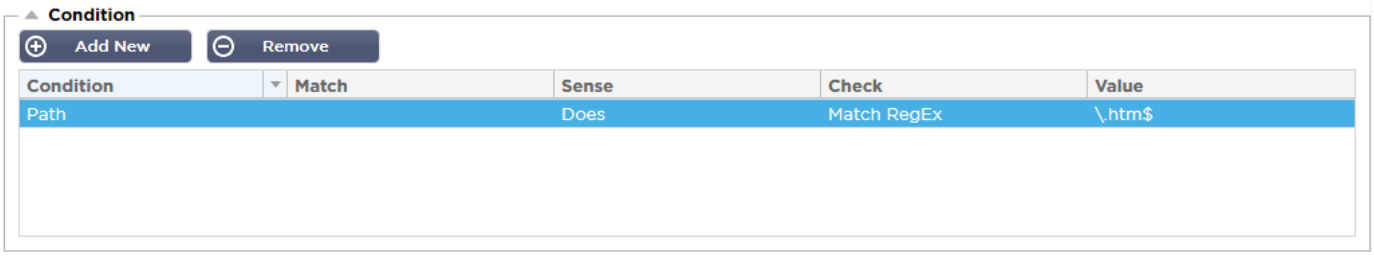
添加 flightPATH 规则的步骤

1. 首先，单击 "详细信息 "部分的 "添加新内容 "按钮。
2. 输入规则名称。示例 Auth2

3. 输入规则描述
4. 一旦将规则应用于服务，就会看到 "应用于 "栏自动填充 IP 地址和端口值
5. 不要忘了点击 "更新 "按钮来保存更改，如果你做错了，只需点击 "取消 "按钮即可恢复到之前的状态。

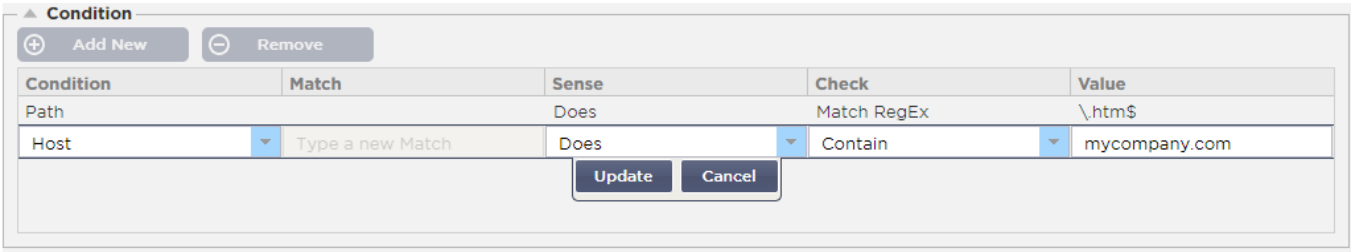
条件

flightPATH 规则可以包含任意数量的条件。这些条件以 **AND** 为基础，允许您设置触发操作的条件。如果要使用 **OR** 条件，请创建额外的 flightPATH 规则，并按正确顺序将其应用到 VIP。



您还可以在 "检查 "字段中选择 "匹配 RegEx"，并在 "值 "字段中选择 RegEx 值，从而使用 RegEx。RegEx 评估的加入极大地扩展了 flightPATH 的功能。

创建新的 flightPATH 条件



首先，您必须从条件列中选择一个值。

我们在下拉菜单中提供了多个条件，涵盖了所有可预见的情况。当添加新条件时，这些条件将通过 Jetpack 更新提供。

可供选择的选项有

状况	说明	示例
<form	HTML 表单用于向服务器传递数据	示例 "表单长度不为 0"
GEO 位置	将源 IP 地址与 ISO 3166 国家代码进行比较	地理位置等于 GB，或地理位置等于德国
主持人	从 URL 中提取的主机	www.mywebsite.com 或 192.168.1.1
语言	从语言 HTTP 标头提取的语言	该条件将产生一个下拉菜单，显示语言列表
方法	HTTP 方法下拉菜单	包括 GET、POST 等的下拉列表
原产地 IP	如果上游代理支持 X-Forwarded-for (XFF)，它将使用真正的原点地址	客户端 IP。它也可以使用多个 IP 或子网。 10\.1\.2\.* 是 10.1.2.0 /24 子网 10\.1\.2\.3|10\.1\.2\.4 使用 | 表示多个 IP

路径	网站路径	/mywebsite/index.asp
职位	POST 请求方法	检查上传至网站的数据
查询	查询的名称和值，可以接受查询名称，也可以接受查询值	"Best=jetNEXUS"，其中匹配项为 Best，值为 edgeNEXUS
查询字符串	字符后的整个查询字符串	
申请 Cookie	客户请求的 cookie 名称	MS-WSMAN=afYfn1CDqqCDqUD: :
请求标题	任何 HTTP 标头	推荐人、用户代理、发件人、日期
申请版本	HTTP 版本	http/1.0 或 http/1.1
响应机构	用户在回复正文中定义的字符串	服务器升级
响应代码	响应的 HTTP 代码	200 确定，304 未修改
响应曲奇	服务器发送的 cookie 的名称	MS-WSMAN=afYfn1CDqqCDqUD: :
响应标头	任何 HTTP 标头	推荐人、用户代理、发件人、日期
响应版本	服务器发送的 HTTP 版本	http/1.0 或 http/1.1
来源 IP	可以是源 IP、代理服务器 IP 或其他集合 IP 地址	客户端 IP、代理 IP、防火墙 IP。也可使用多个 IP 和子网。必须转义点，因为这些点是 RegEX 。示例 10\.1\.2\.3 是 10.1.2.3

比赛

匹配 "字段可以是下拉或文本值，其定义取决于 "条件 "字段中的值。例如，如果 "条件 "设置为 "主机"，则匹配字段不可用。如果 "条件 "设置为 <form>，则匹配字段显示为文本字段；如果 "条件 "设置为 POST，则匹配字段显示为包含相关值的下拉列表。

可供选择的选项有

匹配	说明	示例
接受	可接受的内容类型	接受: text/plain
接受编码	可接受的编码	接受编码: <compress | gzip | deflate | sdch | identity>
接受语言	可接受的答复语言	接受语言: en-US
接受范围	该服务器支持哪些部分内容范围类型	接受范围：字节
授权	用于 HTTP 验证的验证凭据	授权：Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
收费	包含所申请方法应用成本的账目信息	

内容编码	使用的编码类型	Content-Encoding: gzip
内容长度	以八位字节（8 位字节）为单位的响应正文长度	内容长度： 348
内容类型	请求正文的 MIME 类型（用于 POST 和 PUT 请求）	Content-Type: 应用程序/x-www-form-urlencoded
饼干	服务器先前通过 Set-Cookie 发送的 HTTP cookie（如下所示）	Cookie: $Version=1; Skin=new ；
日期	发出信息的日期和时间	日期 = "日期" ":" HTTP-date
ETag	资源特定版本的标识符，通常是信息摘要	ETag："aed6bdb8e090cd1:0"
来自	提出申请的用户的电子邮件地址	发件人：user@example.com
如果-修改-自	如果内容未变，允许返回 304 Not Modified（未修改	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
最后修改	请求对象的最后修改日期（RFC 2822 格式	Last-Modified：Tue, 15 Nov 1994 12:45:26 GMT
Pragma	执行：特定标头，可在请求-响应链的任何位置产生各种影响。	Pragma: no-cache
推荐人	链接到当前请求页面的前一个网页的地址	Referrer: HTTP://www.edgenexus.io
服务器	服务器名称	服务器：Apache/2.4.1 (Unix)
设置	HTTP cookie	Set-Cookie：UserID=JohnDoe; Max-Age=3600; Version=1
用户代理	用户代理的用户代理字符串	用户代理：Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
不同	告诉下游代理如何匹配未来的请求标头，以决定 是否可以使用缓存的响应，而不是从源服务器请求新的响应。 响应	可变：User-Agent
X-Powered-By	指定支持网络应用程序的技术（如 ASP.NET、PHP、JBoss）。	X-Powered-By：PHP/5.4.0

感觉

意义 "字段是一个下拉布尔字段，包含 "是 "或 "否 "选项。

检查

校验字段允许根据条件设置校验值。

可供选择的选项有包含、结束、相等、存在、有长度、匹配 RegEx、匹配列表、开始、超过长度

检查	说明	示例
存在	这并不关心条件的细节，只关心它是否存在。	主机> 是否> 存在
开始	字符串以值开头	路径 >> 是否开始 /secure>
结束	字符串以 "值 "结尾	路径 >> 是否结束 - .jpg
包含	字符串确实包含值	请求头> 接受 >> 是否包含> 图像
平等	字符串确实等于值	主机 >> 是否等于> www.edgenexus.io
有长度	字符串的长度值为	主机 >> 是否有长度> 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
匹配 RegEx	可以输入完整的 Perl 兼容正则表达式	来源 IP >> 是否与 Regex 匹配
比赛列表	使您可以将值与值列表进行匹配。这在需要匹配特定 IP 地址时非常有用。值之间用逗号（,）或括号（|）分隔。	源 IP> 是否 > 匹配列表 > 10.10.10.1 、10.10.10.2、10.10.10.3 等
超出长度	允许检查数值是否超过指定长度。	路径 > 是否 > 超过长度 > 200

添加条件的步骤

添加新的 flightPATH 条件非常简单。上图是一个示例。

1. 单击 "条件 "区域中的 "添加新条件 "按钮。
2. 从下拉框中选择一个条件。以主机为例。您也可以在字段中输入，ADC 会在下拉框中显示该值。
3. 选择一种感觉。例如，是否
4. 选择检查。例如，包含
5. 选择一个值。例如，mycompany.com

上面的示例显示，有两个条件都必须为 "true"，规则才能完成

- 首先是检查请求的对象是否是图像
- 第二步是检查 URL 中的主机是否为 www.imagepool.com

评估

添加可定义变量的功能非常强大。其他 ADC 使用脚本或命令行选项提供这种功能，对任何人来说都不理想。EdgeADC 允许您使用易于使用的图形用户界面定义任意数量的变量，如下图所示。

flightPATH 变量定义包括四个需要输入的条目。

- 变量 - 这是变量的名称
- 来源 - 可能来源点的下拉列表
- 详细信息 - 从下拉菜单中选择数值或手动输入。
- 值 - 变量的值，可以是字母数字值或用于微调的 RegEx。

内置变量

内置变量已被硬编码，因此无需为其创建评估条目。

您可以在 "操作 "部分使用下面列出的任何变量。

- $sourceip$ - 请求的源 IP 地址
- $sourceport$ - 使用的源端口
- $clientip$ - 客户机的 IP 地址
- $clientport$ - 客户端使用的端口
- $host$ - 请求中指定的主机
- $method$ - 使用的方法：GET、POST 等
- $path$ - 申请中指定的路径
- $querystring$ - 请求中使用的查询字符串
- $version$ - REQUEST 中 HTTP 请求的版本（目前只允许使用 1 和 1.1）。
- $resp$ - 服务器的响应，如 200OK、404 等。
- $geolocation$ - 请求的地理位置。

行动	目标
操作 = 重定向 302	目标 = HTTPs://$host$/404.html
操作 = 日志	目标 = 来自 $sourceip$:$sourceport$ 的客户端刚刚请求 $path$ 页面

解释：

- 客户访问不存在的页面时，通常会看到浏览器的 404 错误页面
- 相反，用户会被重定向到他们使用的原始主机名，但错误的路径会被 404.html 代替
- 系统日志中会添加一条记录："来自 154.3.22.14:3454 的客户端刚刚请求了错误的 html 页面"。

行动

流程的下一阶段是添加与 flightPATH 规则和条件相关的操作。

在本例中，我们要重写 URL 的路径部分，以反映用户键入的 URL。

- 单击添加新内容
- 从操作下拉菜单中选择重写路径
- 在目标字段中，键入 $path$/myimages
- 点击更新

此操作将在路径中添加 /myimages，因此最终 URL 将变为 www.imagepool.com/myimages

行动	说明	示例
添加请求 Cookie	在 "目标 "部分添加请求 cookie 的详细信息，并在 "数据 "部分添加值	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
添加请求标题	在数据部分添加带值的目标类型请求标头	目标= 接受 数据= 图像/png
添加响应 Cookie	在 "目标 "部分详细添加 "响应 Cookie"，并在 "数据 "部分添加值	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
添加响应标头	在 "目标 "部分添加详细的请求标头，并在 "数据 "部分添加值	Target= Cache-Control Data= max-age=8888888
车身全部更换	搜索回复正文并替换所有实例	Target= http://（搜索字符串） Data= https://（替换字符串）
首先更换机身	搜索回复正文，仅替换第一例	Target= http://（搜索字符串） Data= https://（替换字符串）
机身 最后更换	搜索回复正文，仅替换最后一个实例	Target= http://（搜索字符串） Data= https://（替换字符串）
下降	这将中断连接	目标= 不适用 数据= 不适用

电子邮件	将向电子邮件事件中配置的地址发送电子邮件。您可以使用变量作为地址或信息	Target= "flightPATH 已通过电子邮件发送此事件" Data= N/A
日志事件	这将在系统日志中记录一个事件	Target= "flightPATH 已将此记录到系统日志中" Data= N/A
重定向 301	这将发出永久重定向	目标= http://www.edgenexus.io 数据= 不适用
重定向 302	这将发出临时重定向	目标= http://www.edgenexus.io 数据= 不适用
删除请求 Cookie	移除 "目标 "部分详细介绍的请求 cookie	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
删除请求标题	删除 "目标 "部分详细说明的请求标头	目标=服务器 数据=N/A
移除响应	移除 "目标 "部分中详细说明的响应 cookie Cookie	目标=jnAccel
移除响应	删除 "目标 "一节中详细说明的响应标头 标头	目标= Etag 数据= 不适用
替换请求 Cookie	用 "数据 "部分的值替换 "目标 "部分详细列出的请求 cookie	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
替换请求标题	用数据值替换目标中的请求标头	目标= 连接 数据= 保持有效
替换	用数据部分的值替换目标部分的响应 cookie Cookie	Target=jnAccel=afYfn1CDqqCDqCVii Date=MSWSMAN=afYfn1CDqqCDqCVii
替换响应	用 "数据 "部分的值替换 "目标 "部分中详细说明的响应标头 标头	目标= 服务器 数据= 为安全起见不公开

重写路径	这将允许您根据条件将请求重定向到新的 URL	Target= /test/path/index.html$querystring$ Data= N/A
使用安全服务器	选择要使用的安全服务器或虚拟服务	Target=192.168.101:443 Data=N/A
使用	选择要使用的服务器或虚拟服务	目标= 192.168.101:80 数据= 不适用
加密 Cookie	这将对 cookie 进行 3DES 加密，然后进行 base64 编码	Target= 输入要加密的 cookie 名称，可在末尾使用 * 作为通配符 Data= 输入加密的通行短语

一个 flightPATH 规则场景

一位客户拥有一个电子商务网站，但遇到了 cookie 被最新版本浏览器阻止的问题。

客户对问题进行了追踪，发现根本原因是相关 cookie 缺乏 "安全 "和 "同站点 "标记。

让我们看看 flightPATH 如何提供帮助。

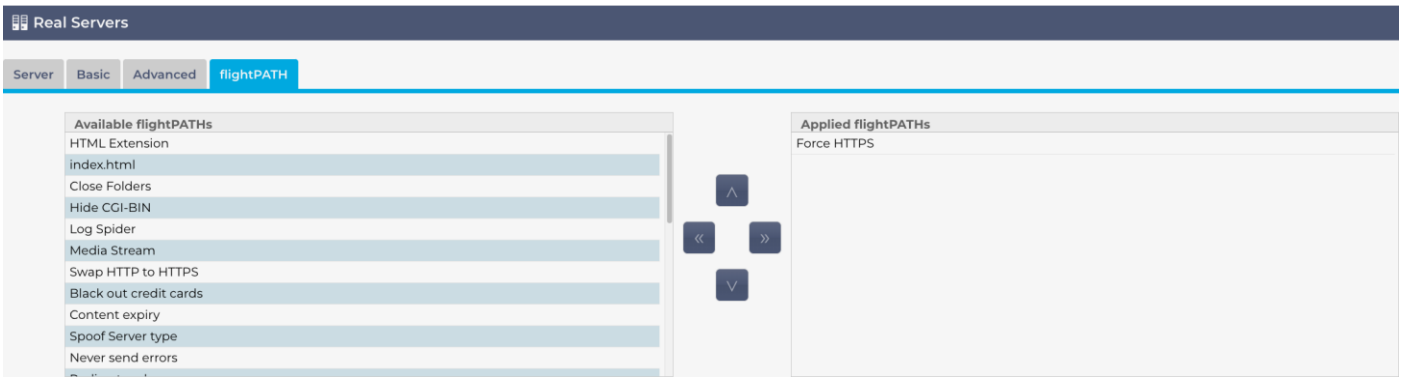
- 我们有一个名为 "wp_woocommerce_session_97929973749972642 "的 cookie
- cookie 的名称是 "wp_woocommerce_session_"，随机唯一 ID 值为 "97929973749972642"，由电子商务系统生成。
- 同一站点 "和 "安全 "标签似乎是空白的，因此浏览器的新安全限制阻止了 cookie。
- 为了防止这种情况发生，我们可以创建以下 flightPATH 规则。
- **会话 ID 的 flightPATH 规则**
    - **条件**：
      留空
    - **评估**：
      变量 = $variable_1$
      来源 = 响应 cookie
      详情 = wp_woocommerce_session_*
    - 操作
      操作 = 替换响应 Cookie
      目标 = wp_woocommerce_session_*
      数据 = $variable_1$
- **标签的 flightPATH 规则**

- **条件：**
  条件 = 响应 Cookie
  匹配 = woocommerce_cart_hash
  意义 = 是否
  检查 = 存在
  值 = 留空
- **评估：**
  变量 = $variable_2$
  来源 = 响应 Cookie
  详细信息 = woocommerce_cart_hash
  值 = 留空
- **操作：**
  操作 = 替换响应 Cookie
  目标 = woocommerce_cart_hash
  Data = $variable_2$,SameSite=None,Secure

现在，您可以将规则应用到需要这些规则的虚拟服务。

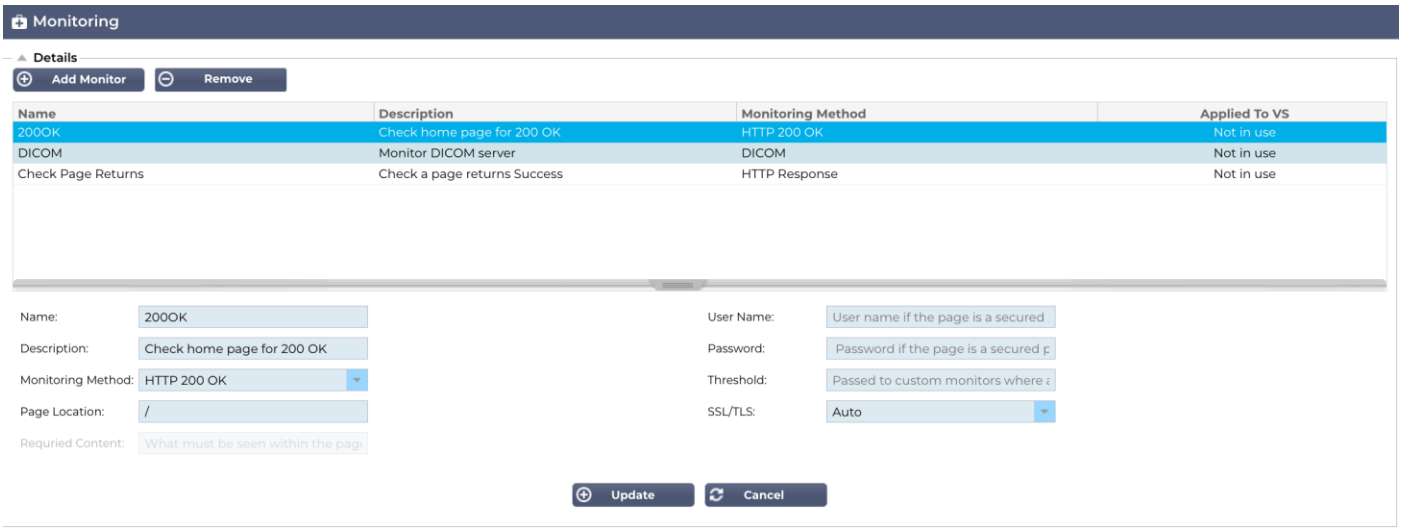
应用飞行路径规则

任何 flightPATH 规则的应用都是在每个 VIP/VS 的 flightPATH 选项卡中进行的。



- 导航至服务 > IP 服务，然后选择要为其分配 flightPATH 规则的 VIP。
- 您将看到如下所示的真实服务器列表
- 点击 flightPATH 选项卡
- 选择您已配置的 flightPATH 规则或支持的预置规则之一。如有需要，您可以选择多个 flightPATH 规则。
- 将所选数据集拖放到 "已应用的 flightPATHs "部分，或单击 >> 箭头按钮。
- 规则将移动到右侧并自动应用。

真实服务器监视器



在负载均衡方案中，监控真实服务器对于检测和应对服务器问题、确保负载均衡分配、优化资源利用率、确定关键服务的优先级以及识别和解决软件漏洞非常重要。

库> 真实服务器监控页面允许您添加、查看和编辑自定义监控。这些是第 7 层服务器 "健康检查"，可从您定义的虚拟服务 "基本 "选项卡内的 "服务器监控 "字段中选择。

真实服务器监视器的类型

有几种可用的真实服务器监控器，下表对此进行了说明。当然，你也可以使用 PERL 编写其他监控程序。

监测方法	说明	示例
HTTP 200 OK	与真实服务器建立 TCP 连接。建立连接后，会向真实服务器发送一个简短的 HTTP 请求。收到响应后，会检查是否有 "200 OK "字符串。如果有，则认为服务器正常运行。 请注意，使用此显示器会获取整个页面的内容。 这种监控方法实际上只能用于 HTTP 和加速 HTTP 服务类型。不过，如果 HTTP 服务器使用的是第 4 层服务类型，而真实服务器上未使用 SSL 或 "内容 SSL "设施未进行适当处理，则仍可使用该方法。	**要求** GET / HTTP/1.1 主机： 192.168.159.200 接受：*/* 接受语言: en-gb 用户代理：Edgenexus-ADC/4.0 连接 Keep-Alive Cache-Control: no-cache **回应** http/1.1 200 ok Content-Type: text/html Last-Modified：Wed, 31 Jan 2018 15:08:18 GMT 接受范围：字节 ETag："0dd3253a59ad31:0" 服务器：Microsoft-IIS/10.0 日期： Tue, 13 Jul 2021 15:55:47 GMTTue, 13 Jul 2021 15:55:47 GMT 内容长度：1364

		<! DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <标题 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <标题>jetNEXUS</标题 <style type="text/css"> <!-- 主体 { color:#FFFFFF ; ... </body> </html>
HTTP 200 头	与真实服务器建立 TCP 连接，PATH 字段指定要检查的位置。 从服务器获取响应的头部，并丢弃内容。检查响应是否为 200 OK。如果存在，则认为服务器正常运行。 请注意，使用该显示器只能获取头部部分。 这种监控方法实际上只能用于 HTTP 和加速 HTTP 服务类型。不过，如果 HTTP 服务器使用的是第 4 层服务类型，而真实服务器上未使用 SSL 或 "内容 SSL "设施未进行适当处理，则仍可使用该方法。	**要求** head / http/1.1 主机： 192.168.159.200 接受：*/* 接受语言: en-gb 用户代理：Edgenexus-ADC/4.0 连接 Keep-Alive Cache-Control: no-cache **回应** http/1.1 200 ok 内容长度：1364 Content-Type: text/html Last-Modified：Wed, 31 Jan 2018 15:08:18 GMT 接受范围：字节 ETag："0dd3253a59ad31:0" 服务器：Microsoft-IIS/10.0 日期： Tue, 13 Jul 2021 15:49:19 GMTTue, 13 Jul 2021 15:49:19 GMT
HTTP 200 选项	与真实服务器建立 TCP 连接，并提出选项请求。 返回选项并检查 200 OK 内容。 如果找到 200 OK 内容，则认为服务器可用。	**要求** 选项 / http/1.1 主机： 192.168.159.200 接受：*/* 接受语言: en-gb 用户代理：Edgenexus-ADC/4.0 连接 Keep-Alive Cache-Control: no-cache **回应** http/1.1 200 ok 允许选项、跟踪、获取、头部、职位 服务器：Microsoft-IIS/10.0 公开：选项、跟踪、获取、头部、职位 日期： Tue, 13 Jul 2021 16:23:39 GMTTue, 13 Jul 2021 16:23:39 GMT 内容长度：0

HTTP 头	HTTP Head 监视器允许我们在 HTTP 流的 Head 部分检查特定值。我们可以在相应字段中输入路径和所需响应，然后在响应中检查该值。 如果在 "头 "中找到 "所需的响应 "值，则服务器被视为正常运行并可用。 我们还可以在需要用户名和密码的特别保护网页上使用这种方法。这样，监控结果就可以被认为是准确的。 例如，在路径和必填响应字段中提供 **/ispagethere.html** 和 **200 OK** 值，如果服务器正常运行、页面可用并响应请求，就会返回成功结果。 这种监控方法实际上只能用于 HTTP 和加速 HTTP 服务类型。不过，如果 HTTP 服务器使用的是第 4 层服务类型，而真实服务器上未使用 SSL 或 "内容 SSL "设施未进行适当处理，则仍可使用该方法。	**要求** HEAD /ispagethere.htm HTTP/1.1 主机： 192.168.159.200 接受：*/* 接受语言: en-gb 用户代理：Edgenexus-ADC/4.0 连接 Keep-Alive Cache-Control: no-cache **回应** http/1.1 200 ok 内容长度：1364 Content-Type: text/html Last-Modified：Wed, 31 Jan 2018 15:08:18 GMT 接受范围：字节 ETag："0dd3253a59ad31:0" 服务器：Microsoft-IIS/10.0 日期 Wed, 14 Jul 2021 08:28:18 GMT
HTTP 选项	通过 HTTP 选项监控器，您可以检查返回的选项数据中的特定值。 我们在相应字段中输入路径和必填回复，然后检查回复。 如果在选项数据中找到所需的响应，则说明服务器可用并正在运行。 必填响应值可以是以下任何一种：OPTIONS、TRACE、GET、HEAD 和 POST。 例如，提供 **/ispagethere.html** 并在 "路径 "和 "必填响应 "字段中**输入 GET** 值，如果服务器正常运行、页面可用并响应请求，就会返回成功结果。 这种监控方法实际上只能用于 HTTP 和加速 HTTP 服务类型。不过，如果 HTTP 服务器使用的是第 4 层服务类型，而真实服务器上未使用 SSL 或 "内容 SSL "设施未进行适当处理，则仍可使用该方法。	**要求** 选项 /ispagethere.htm HTTP/1.1 主机： 192.168.159.200 接受：*/* 接受语言: en-gb 用户代理：Edgenexus-ADC/4.0 连接 Keep-Alive Cache-Control: no-cache **回应** http/1.1 200 ok 允许选项、跟踪、获取、头部、职位 服务器：Microsoft-IIS/10.0 公开：选项、跟踪、获取、头部、职位 日期 Wed, 14 Jul 2021 09:47:27 GMT 内容长度：0
HTTP 响应	与真实服务器建立连接和 HTTP 请求/响应，并按照前面的示例进行检查。 但不是检查 "200 OK "响应代码，而是检查 HTTP 响应的页眉是否包含自定义文本内容。文	**要求** GET /ispagethere.htm HTTP/1.1 主机： 192.168.159.200 接受：*/* 接受语言: en-gb 用户代理：Edgenexus-ADC/4.0 连接 Keep-Alive

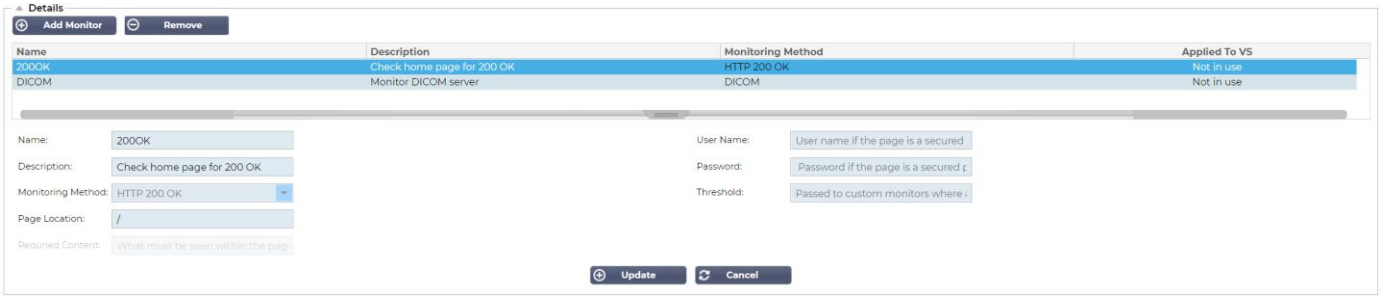
	本可以是完整的页眉、页眉的一部分、页面部分内容中的一行，也可以只有一个单词。 例如，在右图所示的示例中，我们指定 **/ispagethere.htm** 为路径，**Microsoft-IIS** 为所需响应。 如果找到文本，则认为真实服务器已启动并运行。 这种监控方法实际上只能用于 HTTP 和加速 HTTP 服务类型。 但是，如果 HTTP 服务器使用了第 4 层服务类型，而真实服务器上没有使用 SSL 或 "内容 SSL "设施没有进行适当处理，则仍可使用该服务类型。	Cache-Control: no-cache **回应** http/1.1 200 ok Content-Type: text/html Last-Modified：Wed, 31 Jan 2018 15:08:18 GMT 接受范围：字节 ETag："0dd3253a59ad31:0" 服务器：Microsoft-IIS/10.0 日期 Wed, 14 Jul 2021 10:07:13 GMT 内容长度：1364 <! DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <标题 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <标题>jetNEXUS</标题 <style type="text/css"> <!-- 主体 { color:#FFFFFF ; ...
多端口 TCP 监视器	该方法与上述方法类似，只是可以有多个不同的端口。只有在 "所需内容 "部分指定的所有端口都正确响应时，监控器才被视为成功。	名称： 多端口监视器多端口监视器 说明成功监控多个端口 页面位置：不适用 所需内容：135,59534,59535
TCP 带外	TCP 带外方法类似于 TCP 连接，但您可以在所需内容栏中指定要监控的端口。该端口通常与流量端口不同，用于将服务绑定在一起。	名称：TCP 带外 描述监控带外/流量端口 页面位置：不适用 必填内容：555
DICOM	我们使用所需内容列中的 "源调用 "AE 标题值发送 DICOM 回声。您也可以在每个服务器的备注栏中设置 "目的地调用 "AE 标题值。您可以在 IP Services- 中找到 Notes 栏。 -虚拟服务--服务器页面。	名称： DICOMDICOM 描述 DICOM 服务的 L7 健康检查 监测方法：DICOM 页面位置：不适用 必填内容：AET 价值
LDAPS	这一新的健康检查用于检查 LDAP/AD 服务器的健康状况和响应。	名称名称： LDAPS 描述 LDAP/AD 服务器健康检查 使用参数如下 **用户名**： cn=username,cn=users,dc=domainname,dc=local **密码**域名用户密码 **内容**：200OK
SNMP v2	这种监控方法允许您使用服务器的 SNMP MIB 响应来检查服务器的可用性状态。	

	要求回复值应包含社区名称。
DNS 服务器检查	在对 DNS 服务器进行负载平衡时，查看服务器是否对 DNS 查询做出响应很有帮助。 监视器的使用方法如下： • 路径字段用于查询 FQDN。例如，如果要查询 www.edgenexus.io，则在路径字段中输入。 • 如果留空，则监视器将使用默认查询进行查询。 • 要求回复 "字段可以留空，监控程序会认为任何回复都是有效的。否则，应在 "要求响应 "字段中输入预期 IP。例如，可以是 101.10.10.100。如果查询返回此值，监控程序将标记为成功；否则将标记为失败。 成功结果表明正在进行负载平衡的 DNS 服务器处于运行状态。

真实服务器监视器 "页面分为三个部分。

详细信息

详细信息 "部分用于添加新的监视器和删除不需要的监视器。您也可以双击现有监视器对其进行编辑。



名称

您为显示器选择的名称。

说明

该监控器的文字说明，我们建议最好尽可能描述清楚。

监测方法

从下拉列表中选择监控方法。可选项有

- HTTP 200 OK
- HTTP 200 头
- HTTP 200 选项
- HTTP 头
- HTTP 选项
- HTTP 响应

- 多端口 TCP 监视器
- TCP 带外
- DICOM
- SNMP v2
- DNS 服务器检查
- LDAPS

页面位置

URL HTTP 监视器的页面位置。该值可以是一个相对链接，如 /folder1/folder2/page1.html 。也可以使用绝对链接，即网站与主机名绑定。

必填内容

该值包含监控程序需要检测和使用的任何内容。此处表示的值将根据所选的监控方法而改变。

适用于 VS

此字段将自动填入应用监控器的虚拟服务的 IP/端口。您将无法删除任何已与虚拟服务一起使用的监控程序。

用户

某些自定义监控程序可以使用此值和密码字段登录真实服务器。

密码

某些自定义监控程序可以使用此值和用户字段登录真实服务器。

阈值

阈值字段是一个通用整数，用于需要 CPU 级别等阈值的自定义监控器。

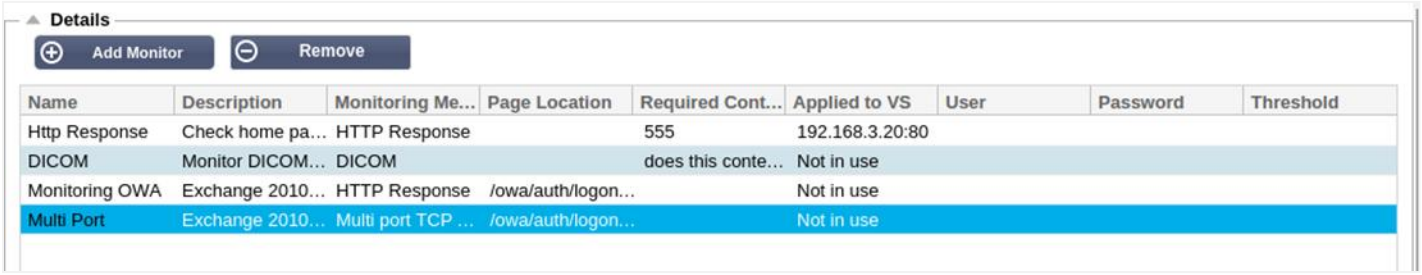
注意：请确保应用服务器返回的响应不是 "分块 "响应

SSL/TLS

该字段允许您强制决定是否使用 SSL。设置如下：

- 开 - 这将强制 SSL
- 关 - 这将禁用 SSL
- 自动 - 保持当前状态

真实服务器监控器示例



上传监控器

在很多情况下，用户希望创建自己的自定义监视器，本部分允许用户将其上传到 ADC。

自定义监控器使用 PERL 脚本编写，文件扩展名为 .pl。

- 为监视器命名，以便在监视方法列表中进行识别
- 浏览 .pl 文件
- 单击上传新监视器
- 您的文件将上传到正确的位置，并作为新的监控方法显示。

定制显示器

在本节中，您可以查看上传的自定义监视器，如果不再需要，可以将其删除。

- 点击下拉框
- 选择自定义监视器的名称
- 点击移除
- 您的自定义监控器将不再出现在监控方法列表中

创建自定义监控 Perl 脚本

注意：本节内容面向有 Perl 使用和编写经验的人员。

本节将向您介绍可在 Perl 脚本中使用的命令。

#Monitor-Name: 命令是存储在 ADC 上的 Perl 脚本的名称。如果不包含这一行，将无法找到您的脚本！

以下是必填项

- #Monitor-Name
- 严格使用；
- 使用警告；

Perl 脚本在 CHROOTED 环境中运行。它们经常调用另一个应用程序，如 WGET 或 CURL。有时需要针对 SNI 等特定功能更新这些程序。

动态价值观

- my $host = $_[0]; ### 主机 IP 或名称（来自 RS 详细信息或 OOB（如果使用））。
- my $port = $_[1]; ### 主机端口（来自 RS 详细信息或 OOB（如果使用））。
- my $content = $_[2]; ### 监控设置中的必填内容（必须在响应中看到的内容）
- my $notes = $_[3];###来自 IP 服务中 RS 详情的注释（使用此注释可对每个 RS 监视器进行独特定制）
- my $page = $_[4]; ### 显示器设置中的页面位置
- my $user = $_[5]; ### 监视器设置中的用户名
- my $password = $_[6]; ### 监控设置中的密码
- my $threshold = $_[7]; ### 监视器设置中的阈值参数
- my $rsaddr = $_[8]; ### RS IP（如果是带外监控，则与 _[0] 不同）
- my $rsport = $_[9]; ### RS 端口（如果是带外监测，则与 _[1] 不同）
- my $timeout = $_[10]; ### 从 IP 服务 > 真实服务器 > 高级 > 监控超时，以秒为单位监控联系超时。

自定义健康检查有两种结果

- 成功
  返回值 1
  向系统日志打印成功信息
  标记真实服务器在线（前提是 IN COUNT 匹配）
- 不成功
  返回值 2
  向 Syslog 打印一条信息，说明未成功
  标记真实服务器脱机（前提是 OUT 计数匹配）

自定义健康监控器示例

```
#监控器名称 HTTPS_SNI

使用严格：

使用警告；

# 在可用健康检查的下拉菜单中显示上述监控器名称

# 传递给该脚本的值有 6 个（见下文）

# 脚本将返回以下值
```

```
# 1 表示测试成功

# 2 如果测试不成功 次级监控器

{
我的 Shost      = $_[0]; ### 主机 IP 或名称
my Sport        = $_[1]; ### 主机端口
我的 Scontent  = $_[2]; ### 要查找的内容（在网页和 HTTP 标头中）
我的注释        = $_[3]; ### 虚拟主机名
我的 Spage      = $_[4]; ### 主机地址后的 URL 部分
我的 Suser      = $_[5]:### 域名/用户名（可选）
我的密码        = $_[6]; ### 密码（可选）
我的 $resolve；
我的 $auth      =;
如果 ($port)
{
        $resolve = "$notes:$port:$host"：
}
否则 {
        $resolve = "$notes:$host"；
}
if ($user && $password) {
        $auth = "-u $user:$password  ：
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@lines)=~/$content/).2>&1'; if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} looking for - $content - Health check successful.\n"；
        返回（1）；
        }
不然
        {
        print "HTTPs://${notes}${page} looking for - $content - Health check failed.\n"；
        返回(2)
        }
}
监控（@ARGV）：
```

注意：

自定义监控 - 无法使用全局变量。只能使用局部变量--函数内部定义的变量

RegEx 的使用 - 所有正则表达式必须使用与 Perl 兼容的语句语法。

SSL 证书

要在使用 SSL 加密连接的服务器上成功使用第 7 层负载平衡，ADC 必须配备目标服务器上使用的 SSL 证书。这样，数据流才能在发送到目标服务器之前被解密、检查、管理，然后重新加密。

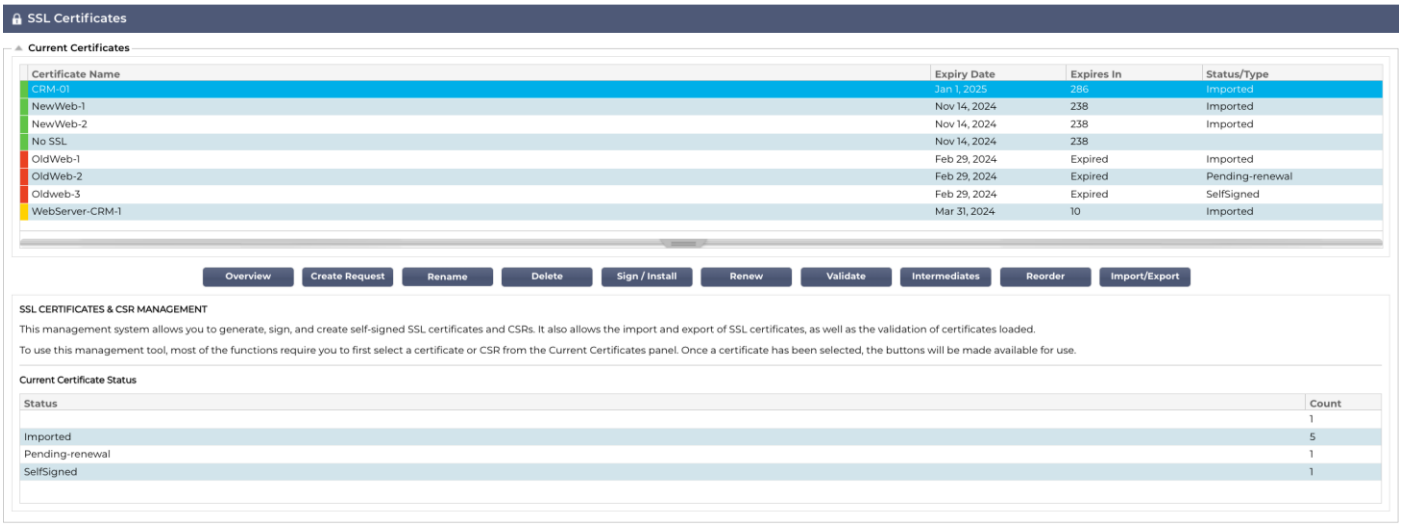
SSL 证书可以是 ADC 可以生成的自签名证书，也可以是可信提供商提供的传统证书（包括通配符）。您还可以使用从 Active Directory 生成的域签名证书。

ADC 如何处理 SSL 证书?

ADC 可根据数据内容执行流量管理规则 (flightPATH)。这种管理无法对 SSL 加密数据执行。当 ADC 需要检查数据时，它首先需要解密数据，为此需要获得服务器使用的 SSL 证书。解密后，ADC 就能检查并执行 flightPATH 规则。之后，数据将使用 SSL 证书重新加密，并发送到最终的真实服务器上。

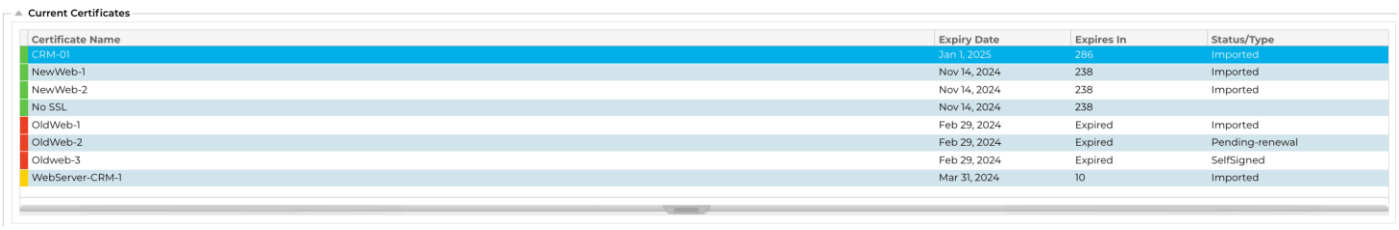
SSL 配置管理器

从 196X 版本开始，配置和管理 SSL 证书和证书请求的方法更加简单明了。



SSL 配置管理器有三个主要部分。

证书列表区



管理器顶部显示的是可使用的 SSL 证书或有待可信机构激活的 SSL 证书。

证书以四栏显示，显示证书名称、有效期、过期天数和证书状态/类型。

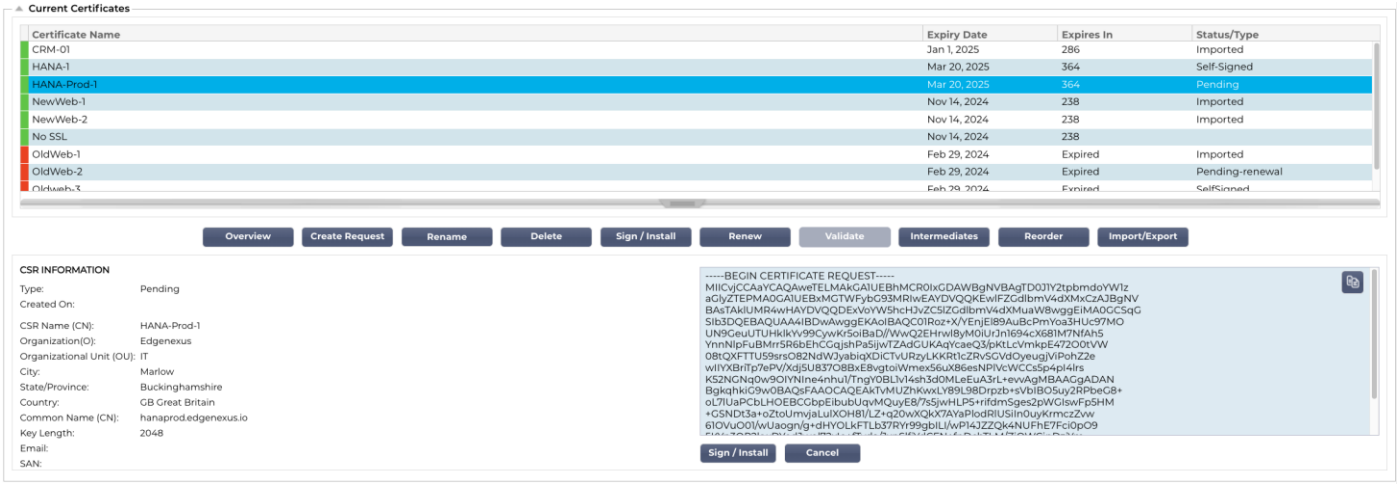
颜色编码

如您所见，每一行都显示了一个证书和一个彩色编码块。下面的表格显示了不同颜色编码块及其含义。

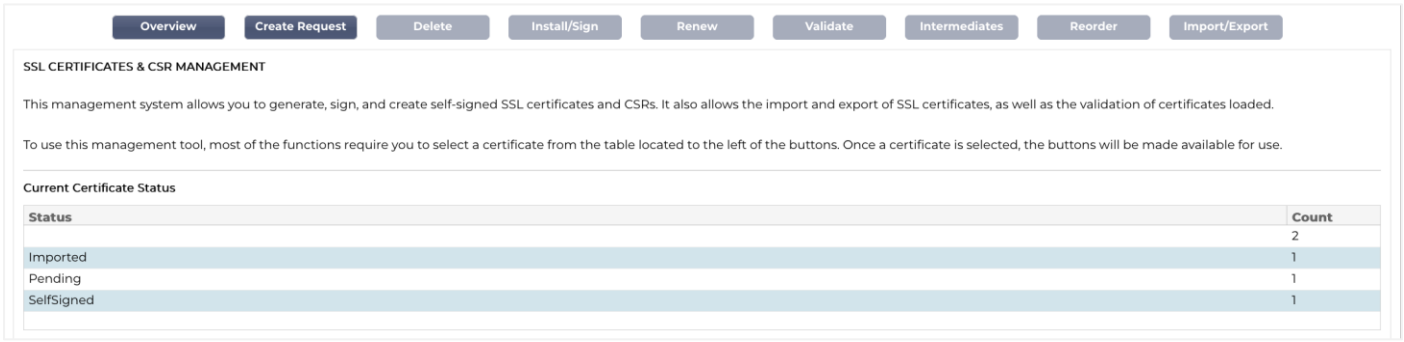
颜色代码	意义
	证书有效且距到期日超过 60 天
	证书将在 30 天内到期
	证书有效期为 30 至 60 天
	证书即将过期，还剩 <1 天
	证书已过期

证书/CSR 信息显示屏

点击证书或 CSR 会在底部面板显示其信息。见下图。

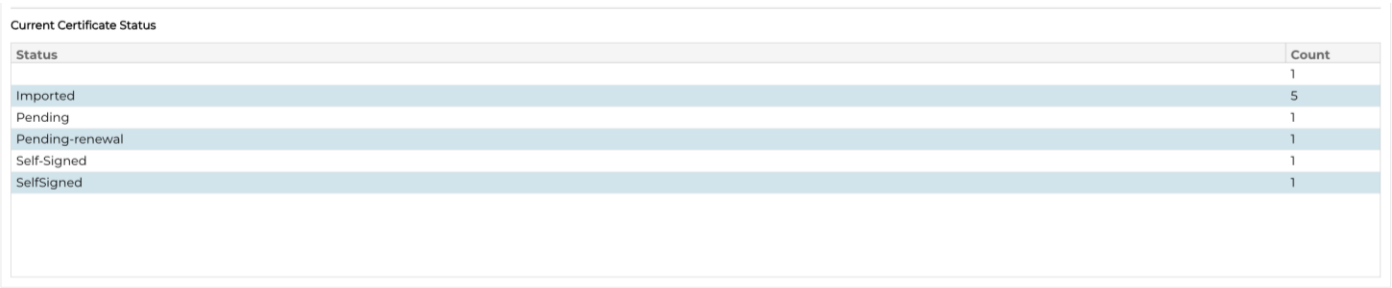


操作按钮和配置区域



在 "列表 "中选择证书时，有许多操作按钮可用并发挥作用。

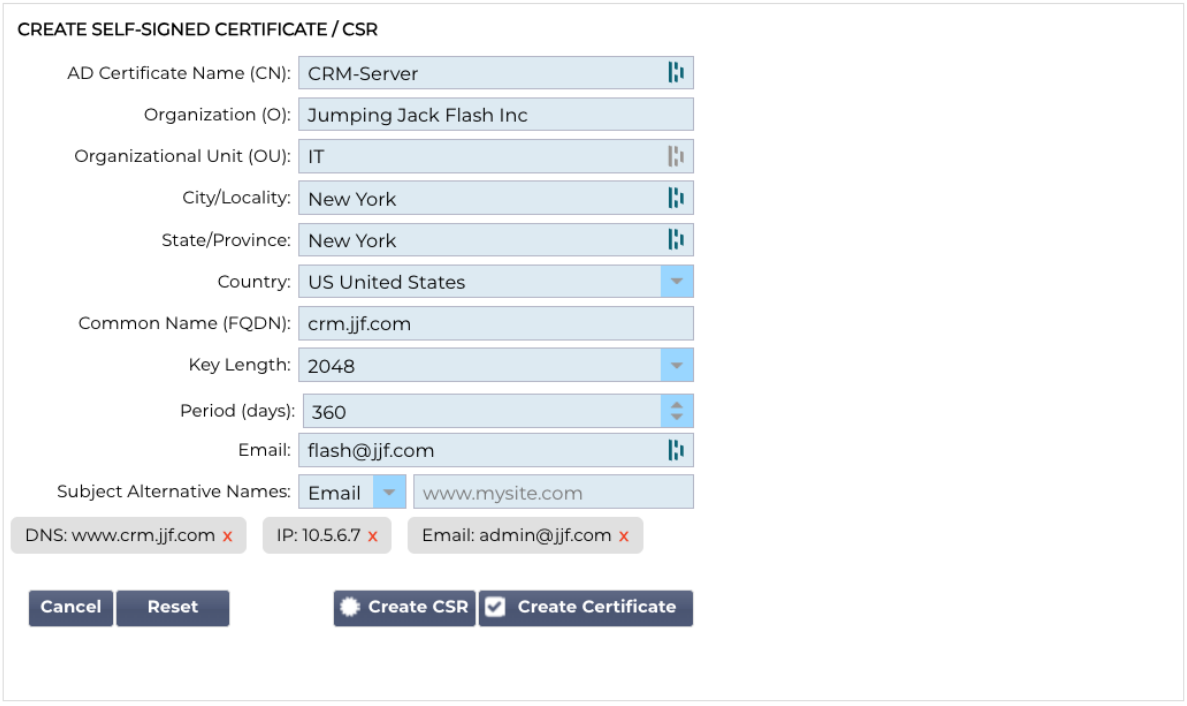
概述



概览 "按钮在底部显示证书的整体情况。与其他操作不同，"概览 "按钮是独立的，不需要选择证书。

创建请求

如果要创建自签名证书或 CSR，则需要单击 "创建请求 "按钮。这将弹出一个通用输入面板，让您提供所需的所有详细信息。



AD 证书名 (CN)

这是一个描述性字段，用于在 ADC 中显示证书名称。字段输入应为字母数字，不留空格。

组织 (O)

该字段用于指定将使用证书的机构名称。

组织单位（OU）

通常用于指定部门或组织单位，这是一个可选字段。

城市/地区

顾名思义，用户一般倾向于指定组织的所在地。

州/省

在此字段中指定州、县或省。

国家

这是必填字段，必须选择使用证书的国家。请确保此处提供的信息准确无误。

通用名称（FQDN）

这是一个关键字段，用于指定使用证书保护的服务器的完全合格域名 (FQDN)。可以是 **www.edgenexus.io** 或 **edgenexus.io**，甚至通配符 ***.edgenexus.io**。如果希望将证书绑定到 IP 地址上，也可以使用 IP 地址。

钥匙长度

用于指定 SSL 证书的加密密钥长度。

期间（天数）

证书有效期，以天为单位。一旦过期，证书将无法使用。

电子邮件

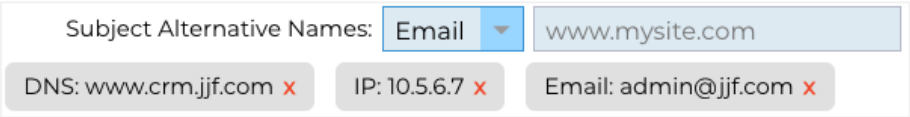
这是证书使用的管理电子邮件 ID。

主题替代名称（SAN）

主题备选名称（SAN）是 SSL 证书中的一个扩展名，允许在单个证书下保护多个域名。该功能尤其适用于保护具有多个子域或不同域名的网站，使 SSL 管理更简化、更具成本效益。通过 SAN，单个 SSL 证书可覆盖多个域名和子域，从而无需为每个网站地址提供单独的证书，从而简化了确保网络通信安全的过程，并确保跨不同域的数据加密。

该字段由两个元素组成，一个是允许选择 SAN 类型的下拉框，另一个是指定值的文本字段。

EdgeADC 有以下 SAN 可供使用：DNS、IP 地址、电子邮件地址和 URI。您可以为证书或 CSR 选择并指定多个 SAN。



单击每个 SAN 值中的红色 **x** 可删除已指定的 SAN。

- **DNS** - DNS 主题备用名 (SAN) 允许您指定证书有效的其他域名。与只允许一个域名的通用名 (CN) 字段不同，SAN 字段可包含多个域名，从而为证书管理提供了灵活性和可扩展性。这对跨不同域和子域托管多种服务的组

织特别有用，因为它允许组织在单个 SSL/TLS 证书下确保所有这些实体的通信安全，从而简化管理并提高安全性。

- **IP 地址** - IP 主题替代名称 (SAN) 允许将 IP 地址与域名一起作为受证书保护的实体。该功能对于确保通过 IP 地址直接访问服务至关重要，可确保在不通过域名而直接通过 IP 地址访问服务器时也能建立加密连接。通过采用 IP SAN，企业可以为基于域名和基于 IP 的通信启用 SSL/TLS 加密，从而增强 其网络安全性，使其成为访问内部资源或特定服务时可能不使用或不首选域名的环境中的通用工具。
- **电子邮件地址** - 电子邮件地址主题备选名称（SAN）允许您指定与证书相关联的其他电子邮件地址，而不是证书签发的主域或实体。这样，证书就能验证多个电子邮件地址的签发者身份，而不仅仅是单个域或通用名称 (CN)。在需要对同一组织或实体下的多个电子邮件地址进行安全电子邮件通信的情况下，它尤其有用，可确保加密电子邮件交换得到验证，并与证书验证的签发人身份绑定。这使得电子邮件地址 SAN 成为在加密框架内提高电子邮件通信安全性和可信度的关键功能。
- **URI** - URI（统一资源标识符）SAN 用于指定证书所保护的单个实体的 URI 所代表的其他身份。与通常包括域名（DNS 名称）或 IP 地址的传统 SAN 条目不同，URI SAN 使证书能将实体与特定 URI（如指向特定资源或服务端点的 URL）关联起来。这样可以更灵活、更精确地识别，使安全连接能够与域内的特定资源或服务建立，而不仅仅是确保域本身的安全，从而提高 SSL/TLS 证书的粒度和范围。

正确填写后，您可以选择创建证书签名请求（CSR）并发送给证书颁发机构进行签名，或者创建自签名证书以供立即使用。

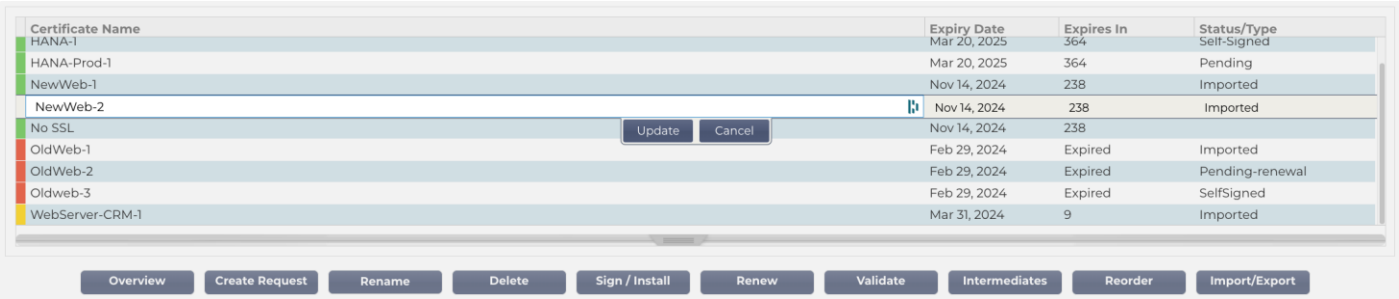
取消 "按钮将取消整个请求，而 "重置 "按钮将重置所有字段。

重新命名

重命名按钮允许您重命名虚拟服务中未使用的证书。

要使用此功能

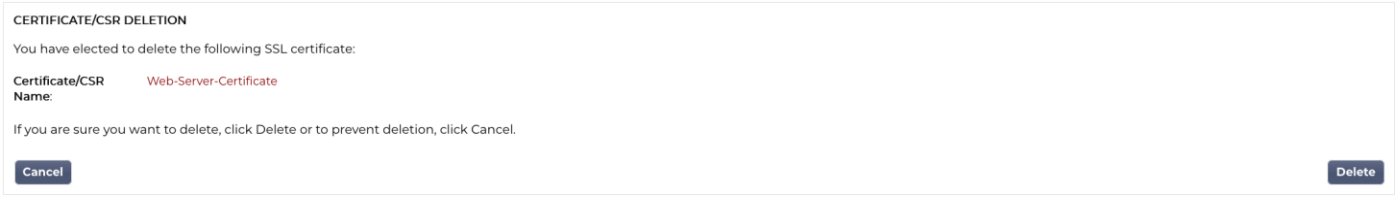
- 点击要重命名的证书，然后点击重命名按钮。
- 证书行将发生变化，您可以更改其名称。



- 完成后，单击 "更新 "按钮。
- 您也可以双击证书，重新命名证书。

删除

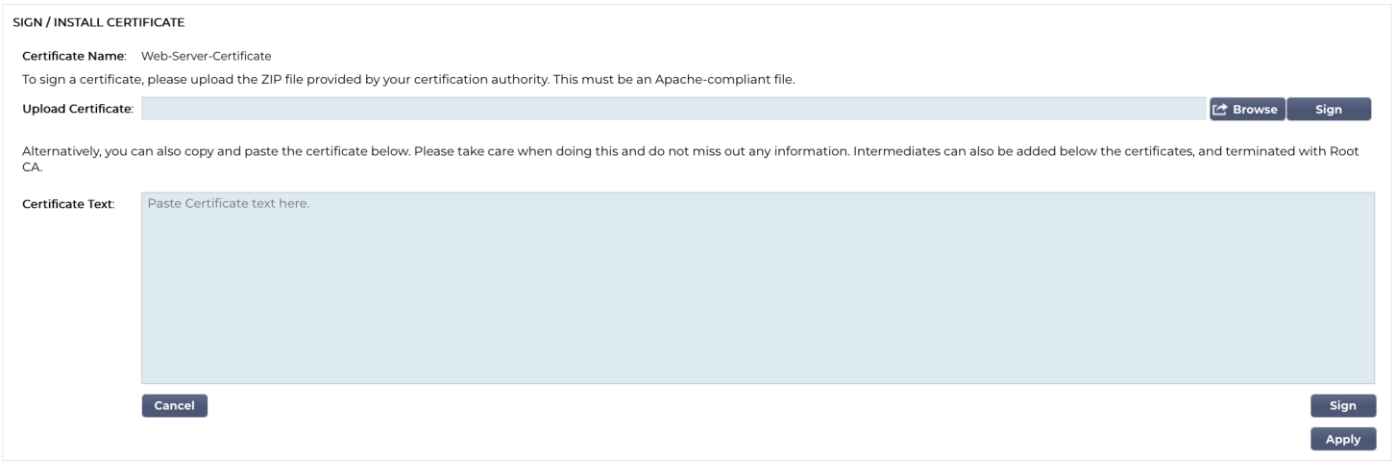
删除按钮只有在选择证书时才可用。点击后将显示以下内容



底部窗格将显示删除请求以及请求删除的证书名称。

单击窗格右下角的 "删除 "按钮，继续删除。

安装/签署



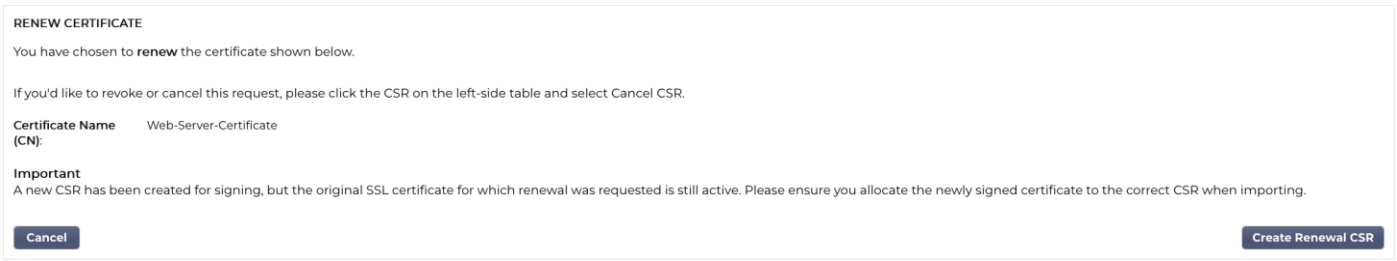
当您创建 CSR 并希望由证书颁发机构（CA）签署该请求时，您将把 CSR 发送给证书颁发机构。作为回报，CA 会将已签署的证书连同私钥文件以及使证书正常运行所需的任何中间件一起发送。

他们可能会向您发送一个包含所有必要元素的 ZIP 文件，您可以使用右侧窗格的上半部分上传该文件。

或者，也可以在文本编辑器中创建证书集，并将内容粘贴到窗格下部的证书文本字段中。

使用这两种方法之一后，单击 "签署 "按钮，然后单击 "应用 "按钮。现在，已签署的证书将显示在左侧窗格中。

更新



当证书超过有效期数据时，"更新 "按钮允许您延长和更新证书。续期有两种类型。

自签名证书

自签名证书与受信任证书不同，不能使用 CSR 更新。相反，自签证书的更新是通过使用现有数据提交新配置来实现的。然后，允许用户为证书指定一个新名称和一个新的到期值。

完成此操作后，新的自签名证书就会创建并保存在证书存储区中。然后，管理员有责任确保及时重新配置使用该证书的虚拟服务。

可信签名证书

当涉及到由认证机构签署的可信证书时，就需要使用 CSR。

点击顶部面板中即将过期的证书，然后点击 "更新"，就会显示一个使用当前证书详细信息的新 CSR。然后就可以下载 CSR 并提交给认证机构进行签署，之后就可以安装已签署的证书了。

您要求更新的证书将有一个新的状态，即 "正在更新"。签名证书安装完毕后，系统会要求你为证书分配一个新名称。新名称将显示为 "受信任"。原始证书将被保留，任何使用该证书的服务都应尽快配置为使用新证书。

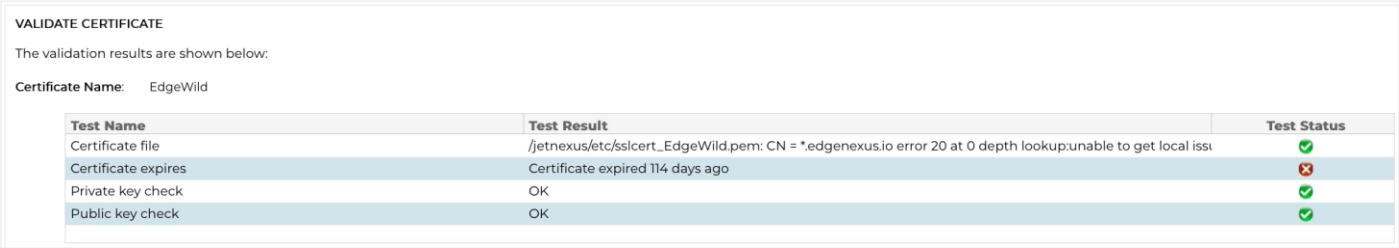
验证证书

SSL 证书由多个部分组成，这些部分不仅必须齐全，而且顺序必须正确。下文列出了验证从第三方机构获取的 SSL 证书的原因。

- **验证**：验证：确保证书来自受信任的机构，并验证网站或服务器的身份。这有助于防止中间人攻击，即攻击者可以拦截客户端和服务器之间的通信。
- **完整性**：通过验证 SSL 证书，可以确保证书未被篡改或更改。这对维护安全连接的完整性至关重要。
- **信任链验证**：SSL 证书由证书颁发机构 (CA) 颁发。验证证书包括验证证书是否链回到受信任的根 CA。这一过程可确保证书的合法性和可信度。
- **撤销状态**：在验证过程中，检查 SSL 证书是否已被签发 CA 撤销也很重要。如果证书签发有误、网站私钥泄露或网站不再需要证书，证书就可能被撤销。导入已撤销的证书可能会导致安全漏洞。
- **过期检查**：SSL 证书有特定的有效期。在导入时验证证书包括检查其过期日期，以确保证书仍然有效。使用过期证书可能会导致漏洞，并可能导致浏览器或客户端拒绝安全连接。
- **配置和兼容性**：验证确保证书的配置与客户的安全策略以及服务器或应用程序的技术要求相兼容。这包括检查所使用的算法、证书的用途和其他技术细节。
- **合规性**：在某些行业，法规可能要求验证 SSL 证书，以确保敏感信息的安全处理。这在金融、医疗保健和电子商务等行业尤为重要。

ADC 的 SSL 管理系统可对导入的 SSL 证书进行验证。

- 选择已导入的 SSL 证书。
- 单击验证按钮。
- 结果如下图所示。

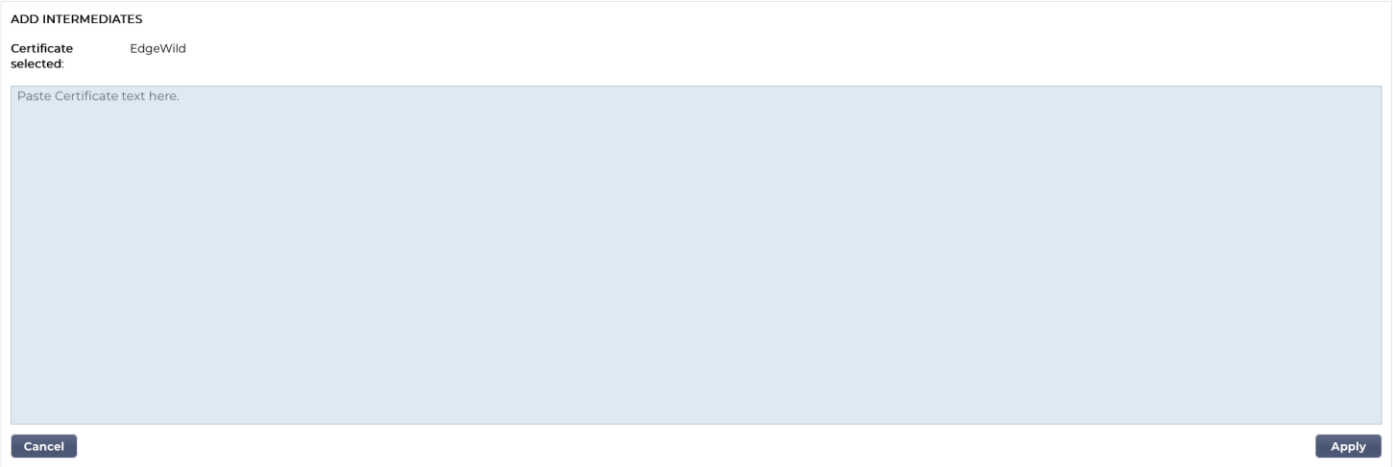


添加中间体

如前所述，SSL 证书由几部分组成，其中一部分是中间证书，它们构成了完整的证书链。

ADC 中的 SSL 管理器允许您添加任何缺失的中间证书。

- 点击要添加中间证书的 SSL。
- 单击 "中间人 "按钮。
- 显示的面板如下图所示。



- 粘贴中间证书的内容。
- 单击 "应用"。

可能需要更改中间证书的顺序，以便正确验证 SSL 证书。这可以使用重新排序按钮来完成。

重新订购

SSL 证书必须按正确的顺序排列才能正常运行。

黄金法则是发送方证书必须放在首位，而最终的根证书必须放在链的最后。一般来说，这看起来有点像下面的表示法：

```
原始签发人 > 中间件 1 > 最终根。
```

最终根证书是由证书颁发机构提供的受信任根证书。

在某些情况下，会有多个中间证书，这些证书也应放在正确的位置。从根本上说，后面的每个证书都必须对前面的证书进行认证。因此，最终的结果可能是这样的。

```
原始签发人 > 中间件 1 > 最终根目录
```

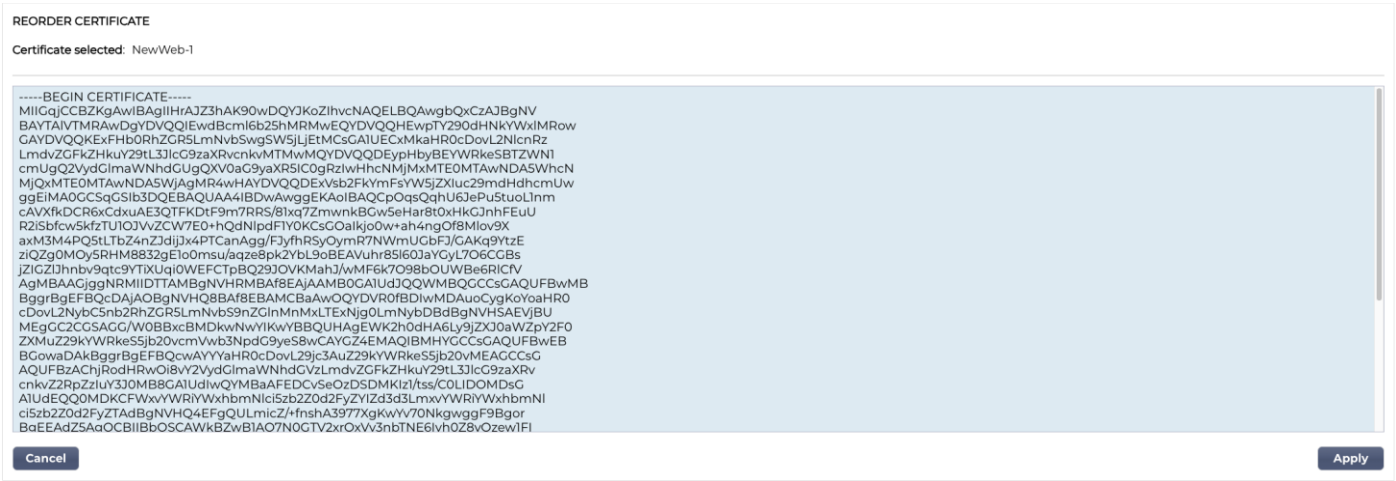
例如，当您导入中间体 2 时，它可能被放在链的末端，这将意味着认证失效。因此，需要重新排序，将中间件 2 放到正确的位置（如红色所示）。

所以，最终的结果会是这样的：

```
原始发行人 > 中间件 1 > 中间件 2 > 最终根目录
```

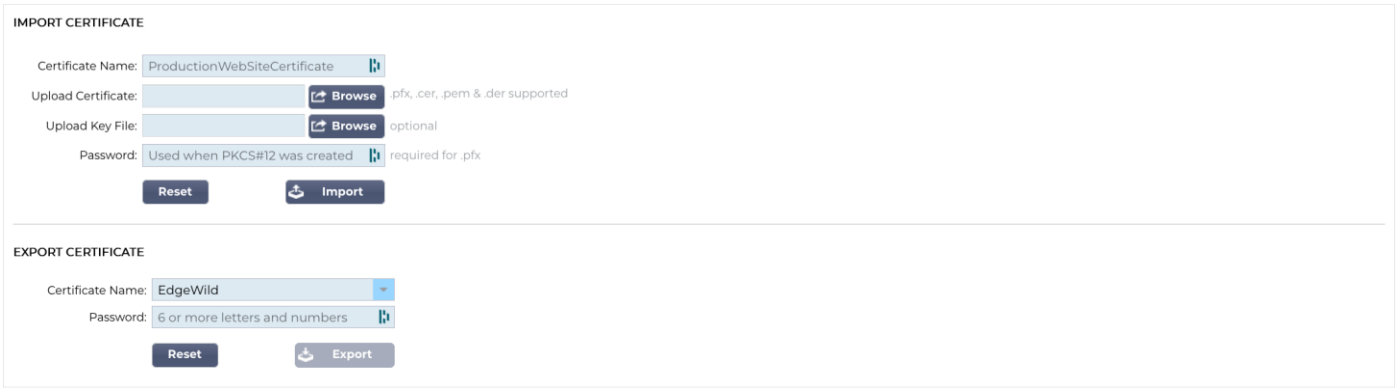
```
-----begin certificate-----
MIIFKTCCBBGgAwIBAgISA/UUyBjJ71fucZuvpiLsdfsfsdfsdfd
...
hoFWWJt3/SeBKn+ci03RRvZsdfdsfsdfw=
-----end certificate-----
-----begin certificate-----
MIIFFjCCAv6gAwIBAgIRAJErCErPDBinsdfsfsdfsdfdsfsdfsdfd
....
nLRbwHqsdqD7hHwg==
-----end certificate-----
-----begin certificate-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----end certificate-----
-----begin certificate-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----end certificate-----
```

选择证书并按下重新排序按钮后，重新排序部分如下图所示。



要重新排列证书部分的顺序，可复制框内的文本，在文本编辑器中编辑并重新排列内容，然后粘贴回去替换现有内容。完成后，点击 "应用 "按钮。

进口/出口



每当你从 SSL 证书提供商处收到证书时，它都会以 ZIP 文件或一组文件的形式出现。这些文件将包含 SSL 证书、密钥文件和根 ca 以及任何中间文件

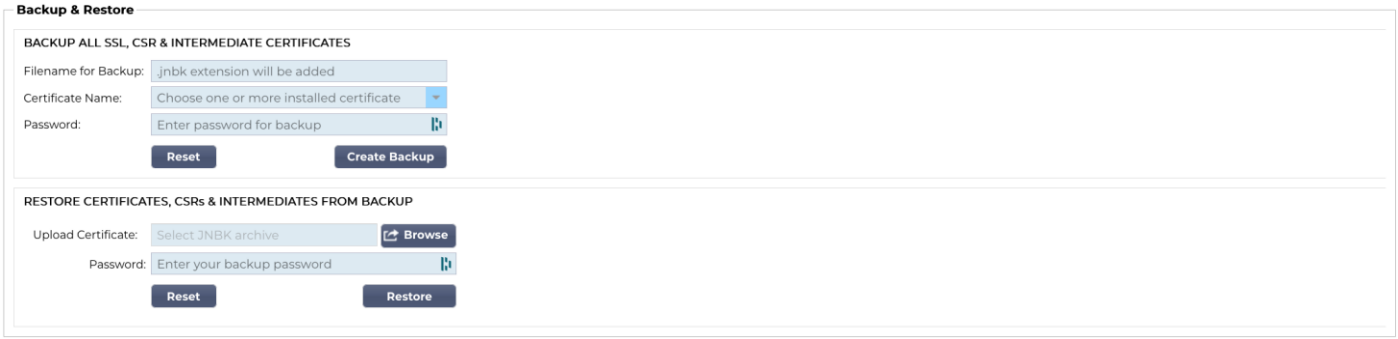
您需要将它们导入 ADC，因此我们提供了一种导入方法。

SSL 证书有多种格式，如 CER、DER、PEM 和 PFX。某些格式要求在导入程序中添加 KEY 文件。PFX 文件需要密码才能导入 PFX 证书。

如果需要，我们还提供了从 ADC 导出证书的方法。导出时，文件将是 PFX 格式，因此需要密码才能创建导出。

备份和恢复

备份



为了备份 ADC 证书存储库中的证书：

- 添加用于备份的文件名。
- 使用下拉菜单选择单个证书，或选择 ALL 备份所有证书。
- 添加密码
- 单击创建备份按钮。
- 创建的文件是经过加密的 JNBK 文件。

重要事项

备份只适用于已导入的受信任证书。

恢复

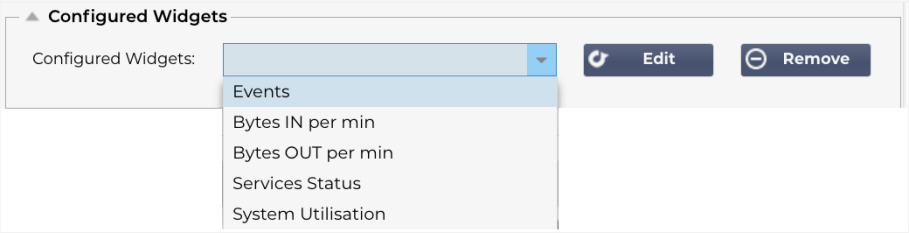
要还原备份时，请使用 "备份和还原 "部分的下部。

- 浏览并找到备份文件。
- 输入密码。
- 单击 "还原 "按钮。
- 备份文件中的证书将被恢复。

小工具

库 > 小工具页面允许您配置自定义仪表盘中显示的各种轻量级可视化组件。

配置小工具

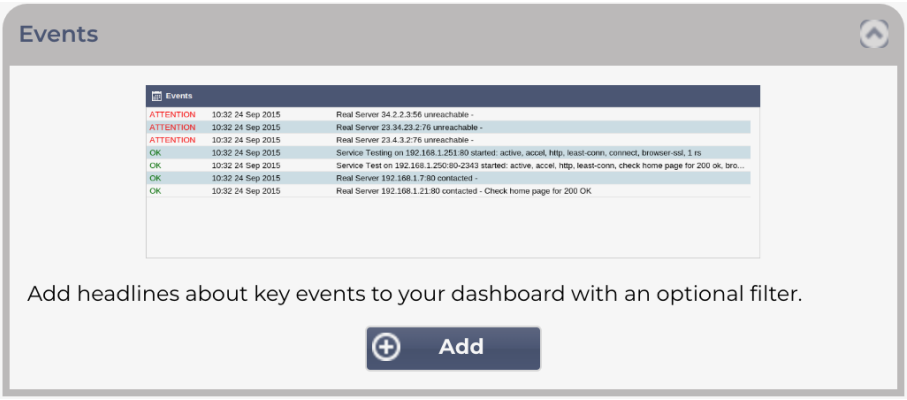


在 "已配置部件 "部分，您可以查看、编辑或删除从可用部件部分创建的任何部件。

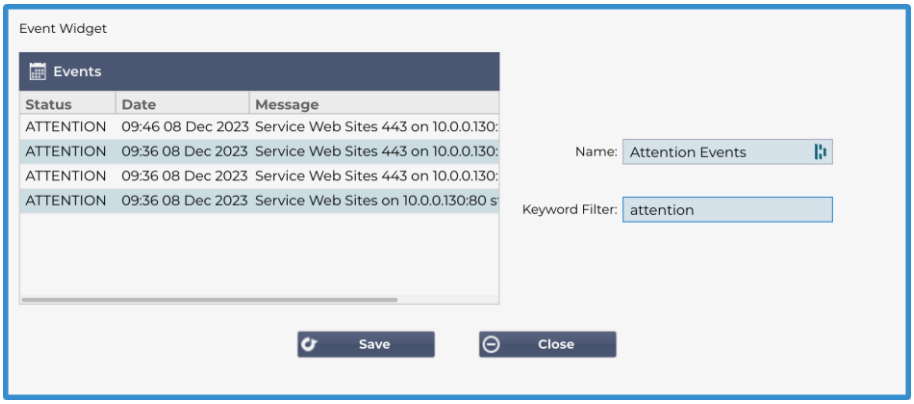
可用的小工具

ADC 提供五种不同的部件，您可以根据自己的要求进行配置。

活动小工具

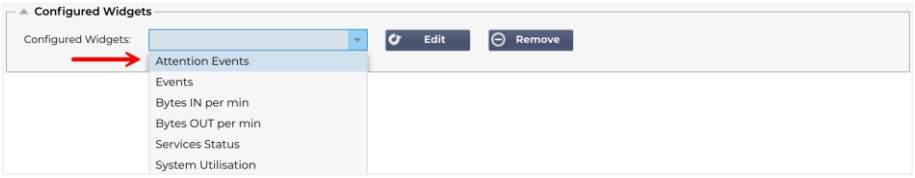


- 要在 "事件 "部件中添加事件，请单击 "添加 "按钮。
- 提供事件名称。在我们的示例中，我们添加了 "关注事件 "作为事件名称。
- 添加关键词过滤器。我们还添加了关注的过滤值



- 单击保存，然后关闭

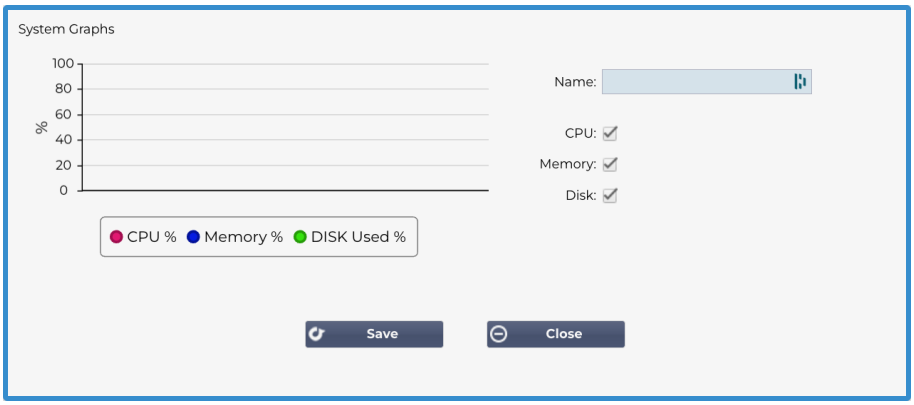
- 现在，您将在 "已配置部件 "下拉菜单中看到一个名为 "关注事件 "的额外部件。



- 您可以看到，我们已经在 "视图">"仪表盘 "部分添加了这个部件。
- 选择 "关注事件 "窗口部件，在仪表板中显示该窗口部件。请参见下文。

您还可以单击 "暂停实时数据 "按钮暂停和重启实时数据馈送。此外，您还可以随时单击 "默认仪表盘 "按钮恢复到默认仪表盘。

系统图表小工具

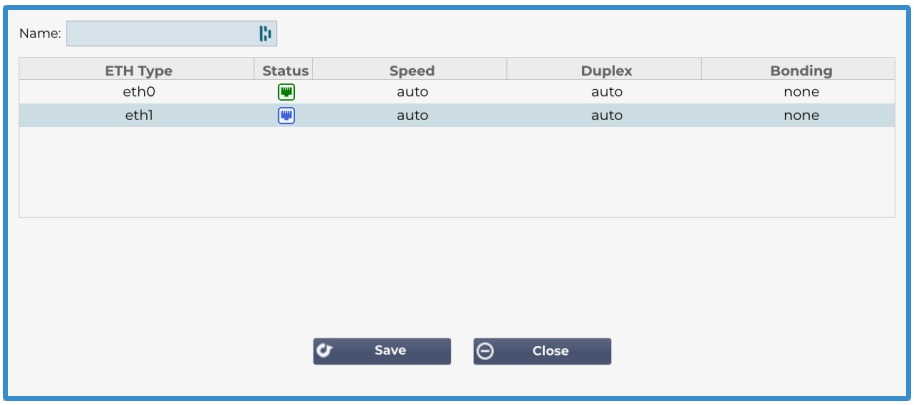


ADC 有一个可配置的系统图表部件。单击部件上的添加按钮，可以添加显示以下监控图表。

- CPU
- 存储器
- 磁盘

添加后，它们将在仪表板的小部件菜单中单独显示。

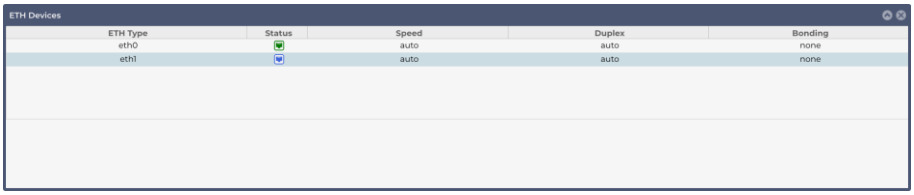
界面小工具



通过接口窗口小部件，可以显示所选网络接口（如 ETH0、ETH1 等）的数据。可供添加的接口数量取决于为虚拟设备定义或在硬件设备中配置的网络接口数量。

完成后，单击 "保存 "按钮，然后单击 "关闭 "按钮。

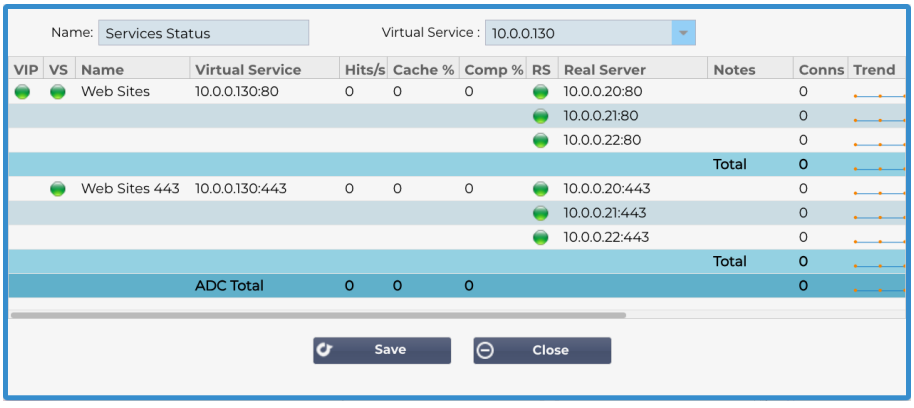
从仪表板中的小部件下拉菜单中选择您刚刚自定义的小部件。您将看到如下界面。



状态小工具

通过状态窗口小部件，您可以查看负载平衡的运行情况。您还可以过滤视图以显示特定信息。

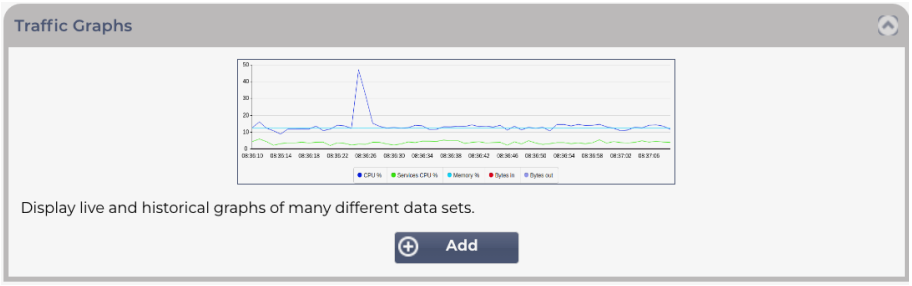
- 单击添加。



- 输入要监控的服务名称
- 您还可以单击列标题，选择要在 widget 中显示的列。
- 满意后，单击 "保存"，然后单击 "关闭"。
- 所选的 "状态 "小组件将出现在 "仪表板 "部分。

交通图形小工具

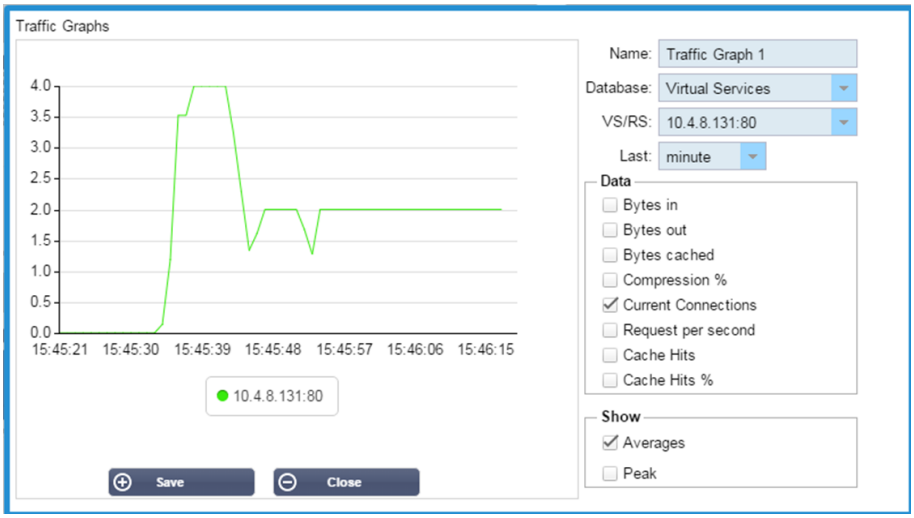
可以对该部件进行配置，以显示每个虚拟服务和真实服务器的当前和历史流量数据。此外，您还可以查看全球流量的当前和历史总体数据



- 点击添加按钮
- 为小部件命名
- 从虚拟服务、真实服务器或系统中选择数据库。
- 如果选择虚拟服务，则可以从 VS/RS 下拉菜单中选择虚拟服务。
- 从 "最后 "下拉菜单中选择一个时间段。
    - 分钟 - 最后 60 秒
    - 小时 - 过去 60 分钟内每分钟的汇总数据
    - 日 - 过去 24 小时内每小时的汇总数据
    - 周 - 前七天中每天的汇总数据
    - 月 - 过去七天每周的汇总数据
    - 年份 - 过去 12 个月中每个月的汇总数据
- 根据所选数据库选择可用数据
    - 虚拟服务数据库
    - 字节数
    - 字节输出
    - 缓存字节数
    - 压缩率
    - 当前连接
    - 每秒请求次数
    - 缓存点击率
    - 缓存点击率 %
- 真实服务器
    - 字节数
    - 字节输出

    - 当前连接
    - 每秒请求次数
    - 响应时间
- 系统
    - CPU %
    - 服务 CPU
    - 内存 %
    - 磁盘空闲 %
    - 字节数
    - 字节输出
- 选择显示平均值或峰值
- 选择所有选项后，点击保存并关闭

交通图示例



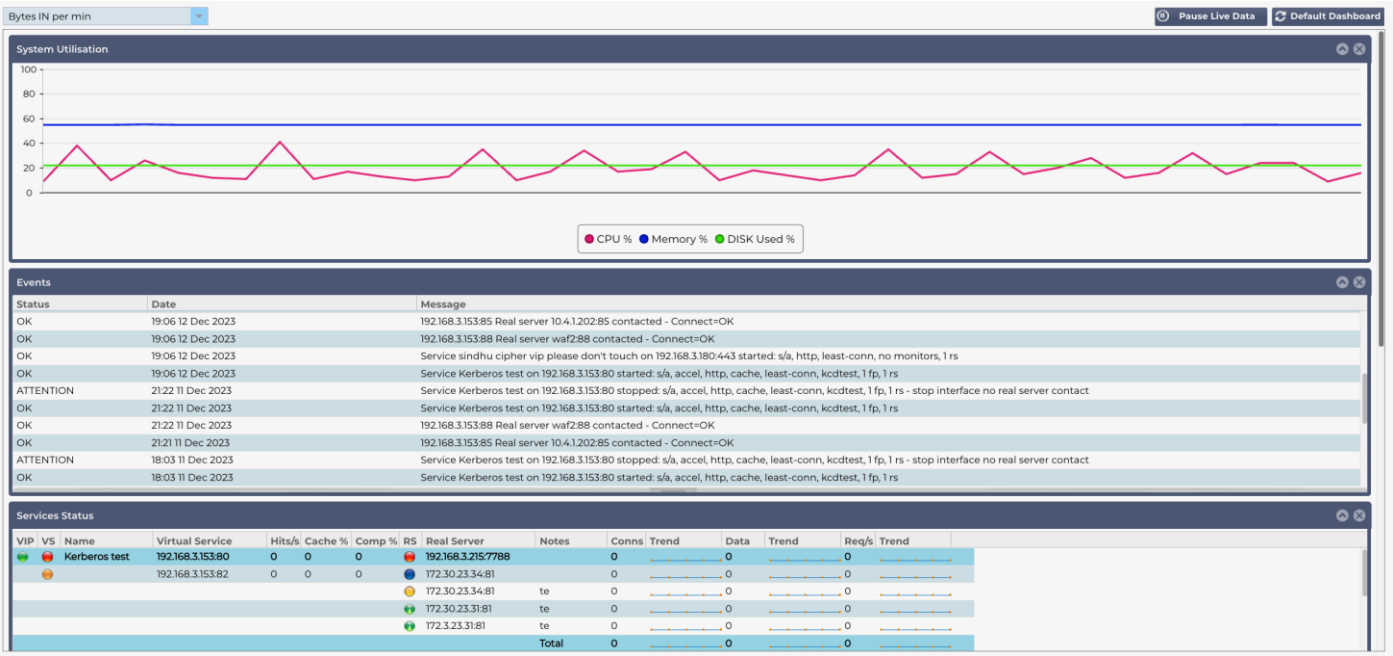
现在您可以将流量图表部件添加到 View> Dashboard。

查看

仪表板

与所有 IT 系统管理界面一样，您有时需要查看 ADC 正在处理的性能指标和数据。我们为您提供了一个可定制的仪表板，让您可以轻松而有意义地完成这项工作。

使用导航面板的 "视图 "分段可进入仪表板。选中后，它将显示多个默认部件，并允许您选择任何已定义的自定义部件。



仪表板的使用

仪表盘 U 有四个元素：小工具菜单、暂停/播放按钮和默认仪表盘按钮。

小工具菜单

仪表板左上角的小工具菜单允许您选择并添加已定义的任何标准或自定义小工具。要使用该功能，请从下拉菜单中选择部件。

暂停实时数据按钮

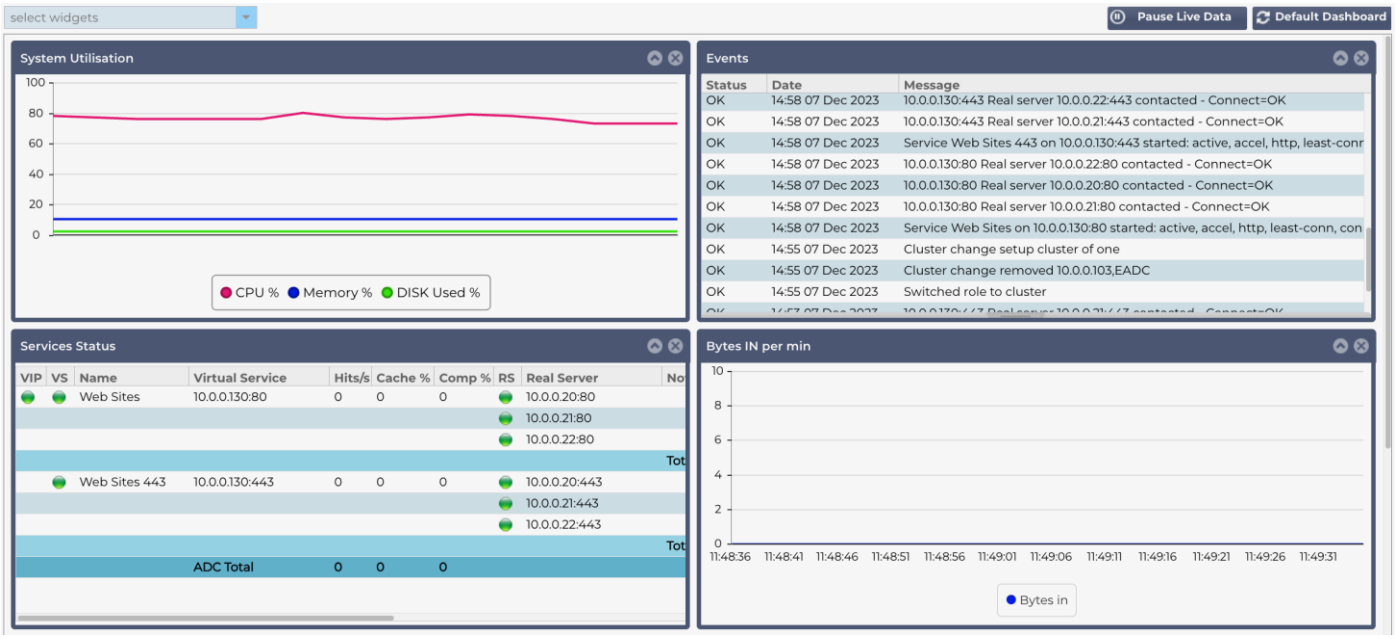
通过此按钮可以选择 ADC 是否实时更新仪表板。一旦暂停，仪表板部件将不会更新，您可以在闲暇时检查内容。一旦开始暂停，该按钮就会改变状态，显示 "播放实时数据"。

完成后，只需单击 "播放实时数据 "按钮，即可重新启动数据收集并更新仪表板。

默认仪表板按钮

您可能希望将仪表板布局重置为默认设置。在这种情况下，请按下默认仪表板按钮。一旦点击，对仪表板所做的所有更改都将丢失。

调整大小、最小化、重新排序和删除 部件



调整部件大小

您可以非常容易地调整 Widget 的大小。单击并按住 widget 的标题栏，然后将其拖动到仪表板区域的左侧或右侧。你会看到一个虚线矩形，代表新的 widget 大小。将 Widget 放入矩形中，然后松开鼠标按钮。如果您想将调整过大小的 widget 放在先前调整过大小的 widget 旁边，您会看到矩形出现在您想放在旁边的 widget 旁边。

最小化部件

您可以随时通过单击部件的标题栏来最小化部件。此操作将最小化窗口部件，只显示标题栏。

移动小部件顺序

要移动 Widget，可以点击标题栏并按住不放，然后移动鼠标进行拖放。

删除小工具

点击小部件标题栏中的⊗ 图标，即可删除小部件。

历史

历史记录选项可从导航器中选择，允许管理员检查 ADC 的历史性能。可为虚拟服务、真实服务器和系统生成历史视图。

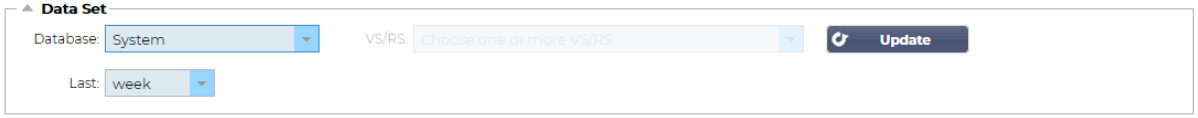
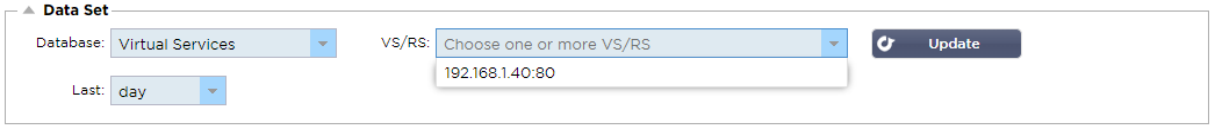
它还能让您看到负载平衡的运行情况，并帮助捕捉任何需要调查的错误或模式。请注意，必须在系统 > 历史记录中启用历史记录才能使用此功能。

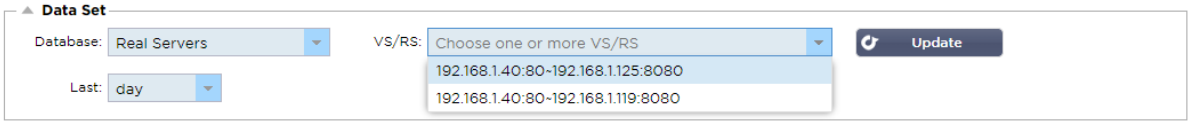
查看图形数据

数据集

要查看图表格式的历史数据，请按以下步骤操作：

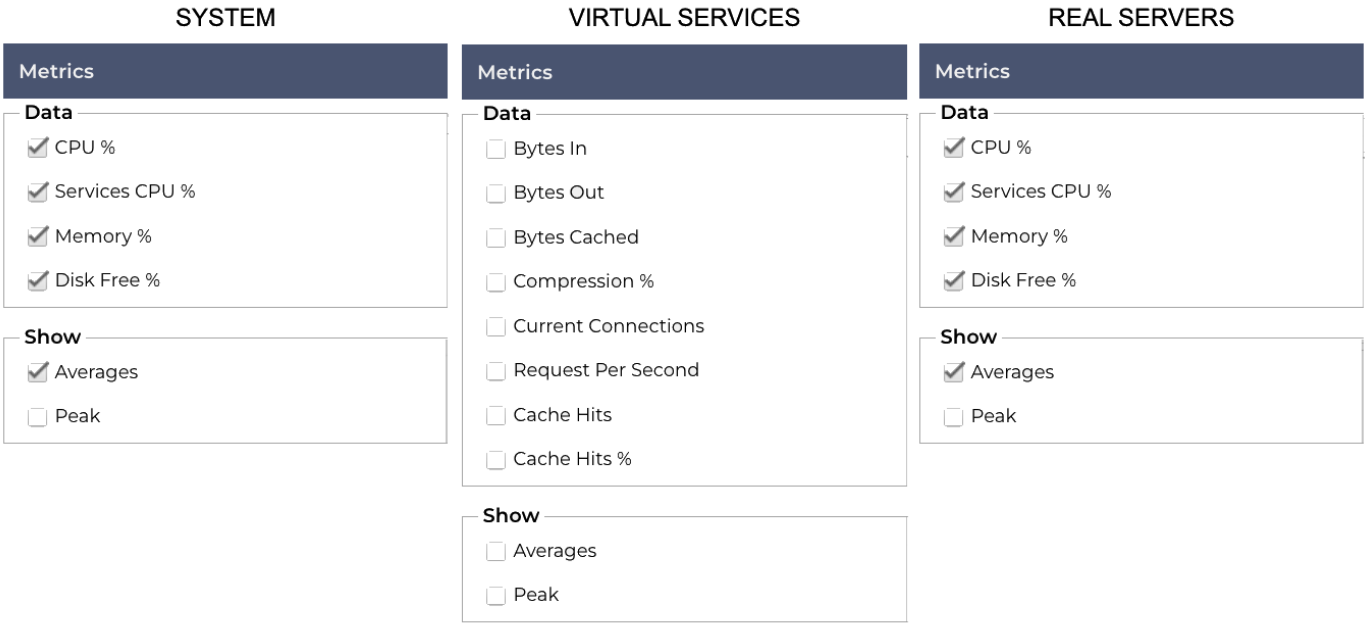
第一步是选择与要查看的信息相关的数据库和时间段。您可以从 "最后 "下拉菜单中选择的时间段包括分钟、小时、日、周、月和年。

数据库	说明
系统	选择该数据库可查看一段时间内的 CPU、内存和磁盘驱动器空间 
虚拟服务	选择该数据库后，您就可以选择数据库中从开始记录数据时起的所有虚拟服务。您将看到一个虚拟服务列表，可以从中选择一个。 

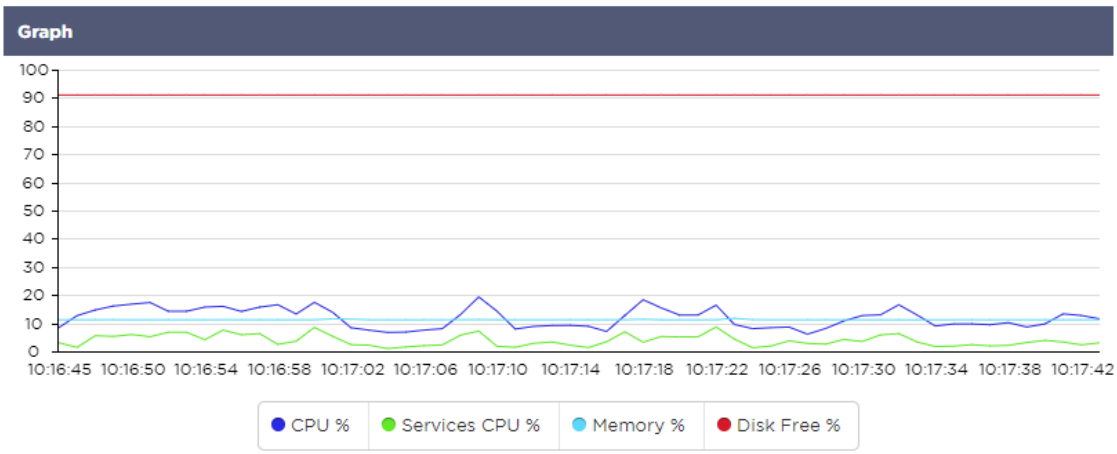
真实服务	选择此数据库后，您就可以选择从开始记录数据时起数据库中的所有真实服务器。您将看到一个真实服务器列表，可以从中选择一个。 

衡量标准

选择了要使用的数据集后，就可以选择要显示的指标了。下图显示了可供管理员选择的指标：这些选择分别对应系统、虚拟服务和真实服务器（从左到右）。



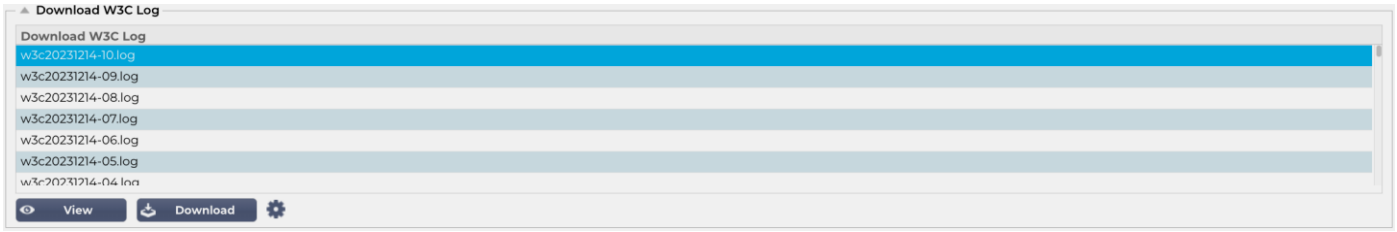
示例图表



日志

查看 "部分中的 "日志 "页面允许您预览和下载 W3C 和系统日志。该页面分为两个部分，详情如下。

万维网联盟日志



W3C 日志可在系统 > 日志部分启用。W3C 日志是 Web 服务器的访问日志，其中生成的文本文件包含每个访问请求的数据，包括源 Internet 协议 (IP) 地址、HTTP 版本、浏览器类型、引用页面和时间戳。W3C 日志可以变得非常庞大，这取决于数据量和记录的日志类别。

在 W3C 部分，您可以选择所需的日志，然后查看或下载。

查看按钮

查看按钮允许您在记事本等文本编辑器窗口中查看所选日志。

下载按钮

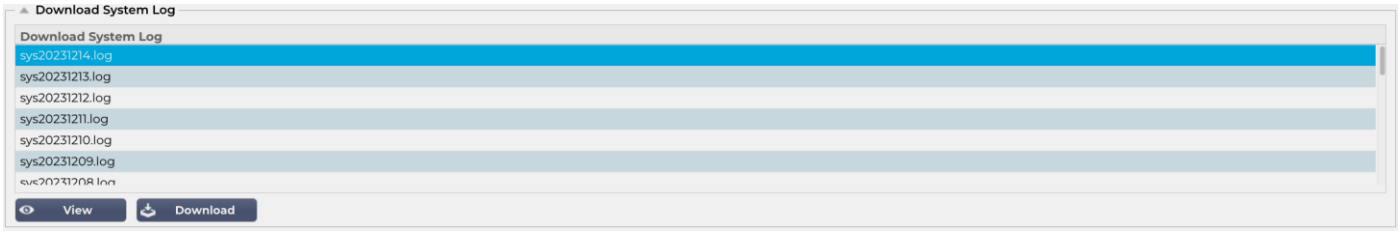
通过此按钮，您可以将日志下载到本地存储器，以便日后查看。

齿轮图标

单击该图标可进入系统 > 日志中的 W3C 日志设置部分。我们将在本指南的日志部分对此进行详细讨论。

系统日志

系统日志对于调试或检查 ADC 的运行情况至关重要。它适用于 IT 部门有一定经验的人员。



查看按钮

查看按钮允许您在记事本等文本编辑器窗口中查看所选日志。

下载按钮

通过此按钮，您可以将日志下载到本地存储器，以便日后查看。

统计资料

ADC 的 "统计 "部分是系统管理员经常使用的区域，他们希望确保 ADC 的性能符合他们的期望。

压缩

ADC 的整个目的是监控数据，并将其导向配置为接收数据的真实服务器。ADC 提供压缩功能是为了提高 ADC 的性能。有时，管理员会希望测试和检查 ADC 的数据压缩信息；这些数据由 "统计"（Statistics）中的 "压缩"（Compression）面板提供。

迄今为止的内容压缩

Content Compression To Date	
Compression	0%
Throughput Before Compression	0
Throughput After Compression	0

本节显示的数据详细说明了 ADC 对可压缩内容所达到的压缩水平。我们将 60-80% 的值称为典型值。

迄今为止的总体压缩情况

Overall Compression To Date			Current Values
Compression	0%		0%
Throughput Before Compression	0		0.00 Mbps (data)
Throughput After Compression	0		0.00 Mbps (data)
Throughput From Cache	0		0.00 Mbps (data)
		Total	0.00 Mbps (data)

本节提供的值会报告 ADC 对所有内容进行压缩的程度。典型的压缩百分比取决于服务中包含多少预压缩图像。图像数量越多，整体压缩百分比就可能越小。

总投入/产出

Total Input	345.9 MB	Input/s	12.7 kbps
Total Output	296.8 MB	Output/s	25.7 kbps

总输入/输出数字表示输入和输出 ADC 的原始数据量。随着数据量从 kbps 到 Mbps 再到 Gbps 的增长，测量单位也会发生变化。

点击和连接

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

点击和连接 "部分包含通过 ADC 的点击和事务的总体统计数据。那么，点击数和连接数是什么意思呢？

- 命中被定义为第 7 层事务。通常用于网络服务器，这是对图像等对象的 GET 请求。

- 连接被定义为第 4 层 TCP 连接。一个 TCP 连接上可以进行许多交易。

总点击数

本节中的数字显示自上次重置以来非缓存点击的累计次数。右侧的数字将显示当前每秒的点击数。

连接总数

总连接数 "值表示上次重置后的 TCP 连接累积数。第二列中的数字表示 ADC 每秒的 TCP 连接数。右侧列中的数字是每秒与真实服务器建立的 TCP 连接数。示例 6/8 连接/秒。在所示示例中，虚拟服务每秒有 6 个 TCP 连接，真实服务器每秒有 6 个 TCP 连接。

峰值连接

连接数峰值表示 ADC 的最大 TCP 连接数。最右边一列的数字表示当前活动 TCP 连接的数量。

缓存

如您所见，ADC 配备了压缩和缓存功能。本节显示应用于通道时与缓存相关的总体统计数据。如果缓存未应用于通道且配置正确，则缓存内容为 0。

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

来自缓存

点击数：第一列显示自上次重置以来 ADC 缓存提供的事务总数。还提供了占总事务的百分比。

字节：第二列显示 ADC 缓存提供的数据总量（千字节）。还提供了数据总量的百分比。

来自服务器

点击数：第 1 列显示了自上次重置以来真实服务器提供服务的交易总数。同时还提供了交易总数的百分比。

字节：第二栏以千字节为单位列出了真实服务器提供的数据总量。还提供了数据总量的百分比。

缓存内容

点击数：这个数字表示 ADC 缓存中包含的对象总数。

字节：第一个数字表示 ADC 缓存对象的总大小（兆字节）。还提供了最大缓存大小的百分比。

应用缓冲区

Buffer Type	Connections Used/Free	Memory Used/Free	Average Buffer Fill Size
Low	0/5k(0%)	0/655MB(0%)	0
Medium	0/5k(0%)	0/30MB(0%)	0
High	0/10k(0%)	0/20MB(0%)	0

在 ADC 中使用应用缓冲区有助于优化性能、提高吞吐量，并确保数据在客户端和服务器之间可靠高效地流动。ADC 对缓冲区大小、处理策略和其他参数进行了优化，以便根据应用和基础设施的具体要求对负载进行微调。

在 EdgeADC 中，我们为您做了大量工作，并根据需要自动调整缓冲参数。

会话持久性

Total current sessions	0
% used (of max)	0
New sessions this min	0
Revalidations this min	0
Expired sessions this min	0

会话持久性部分提供了几个参数的信息。

当前会话总数

这将显示有多少个持续会话正在进行 - 每分钟更新一次

已用百分比（最大值）

这显示了会话信息总空间的使用情况

本分钟的新课程

这显示了在最后一分钟内添加了多少个新的持续会话

重新确认该分钟

这显示了在最后一分钟内，有多少现有的持续会话被更多流量重新验证。

本分时段已过期

这显示了在最后一分钟内，有多少现有的持续会话由于在超时时间内没有进一步的流量而过期。

硬件

无论您是在虚拟环境中还是在硬件中使用 ADC，本节都将为您提供有关设备性能的宝贵信息。

Disk Usage	2%
Memory Usage	10.1%(185.4MB of 1832.7MB)
CPU Usage	76.0%

磁盘使用量

第 2 列中提供的值给出了当前使用的磁盘空间百分比，其中包括日志文件和缓存数据的信息，这些数据会定期存储在存储空间中。

内存使用情况

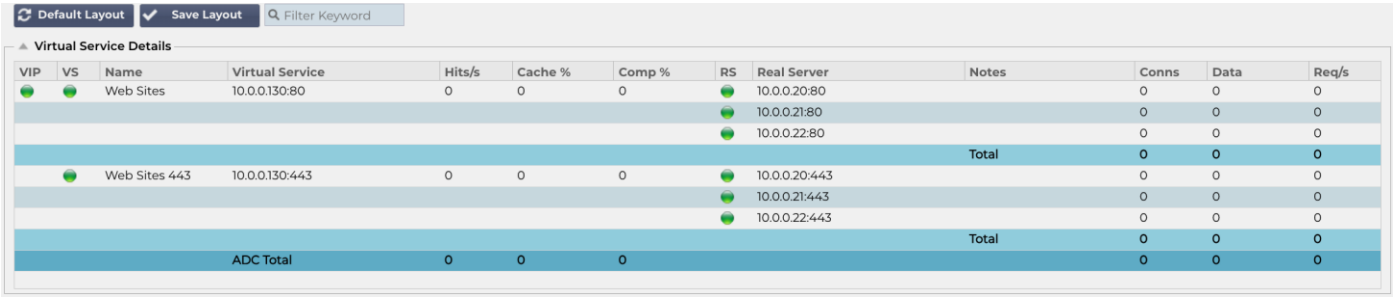
第二列显示当前使用的内存百分比。括号中更重要的数字是分配给 ADC 的内存总量。建议为 ADC 分配至少 2GB 内存。

CPU 使用率

提供的关键值之一是 ADC 当前使用的 CPU 百分比。这个数值自然会有波动。

现状

查看 > 状态页面显示通过 ADC 为您定义的虚拟服务传输的实时流量。它还会显示连接数和每个真实服务器的数据，让你实时体验负载平衡。



虚拟服务详情

贵宾专栏

指示灯的颜色表示与一个或多个虚拟服务相关联的虚拟 IP 地址的状态。

现状	说明
●	在线
●	故障转移-备用。此虚拟服务为热备用
●	表示 "被动 "为 "主动 "暂时搁置
●	脱机。真实服务器无法访问，或未启用真实服务器
●	调查结果
●	未获得许可或超过许可的虚拟 IP

VS 状态栏

指示灯的颜色表示虚拟服务的状态。

现状	说明
●	在线
●	故障转移-备用。此虚拟服务为热备
●	表示 "被动 "为 "主动 "暂时搁置
●	服务需要注意。此状态指示可能是由于真实服务器未能通过健康监控或已手动更改为脱机。流量将继续流动，但真实服务器容量会降低。
●	脱机。真实服务器无法访问，或未启用真实服务器
●	调查结果
●	未获得许可或超过许可的虚拟 IP

名称

虚拟服务的名称

虚拟服务（VIP）

服务的虚拟 IP 地址和端口，以及用户或应用程序将使用的地址。

命中/秒

客户端每秒进行 7 层交易。

缓存%

这里提供的数字表示从 ADC 的 RAM 缓存中提供服务的对象百分比。

压缩率

该数字表示客户端与 ADC 之间已压缩对象的百分比。

RS 状态（远程服务器）

下表概述了与 VIP 关联的真实服务器状态的含义。

现状	说明
●	已连接
●	未监测
●	排水或离线
●	备用
●	未连接
●	调查结果
●	未获得许可或超过许可的虚拟 IP

真实服务器

真实服务器 IP 地址和端口。

说明

该值可以是任何有用的注释，以便他人了解条目的目的。

康纳斯（连接）

通过表示每个真实服务器的连接数，您可以看到负载平衡的运行情况。这对验证负载平衡策略是否正常工作非常有帮助。

数据

此列中的值显示发送到每个真实服务器的数据量。

Req/Sec（每秒请求次数）

每秒发送到每个真实服务器的请求数。

系统

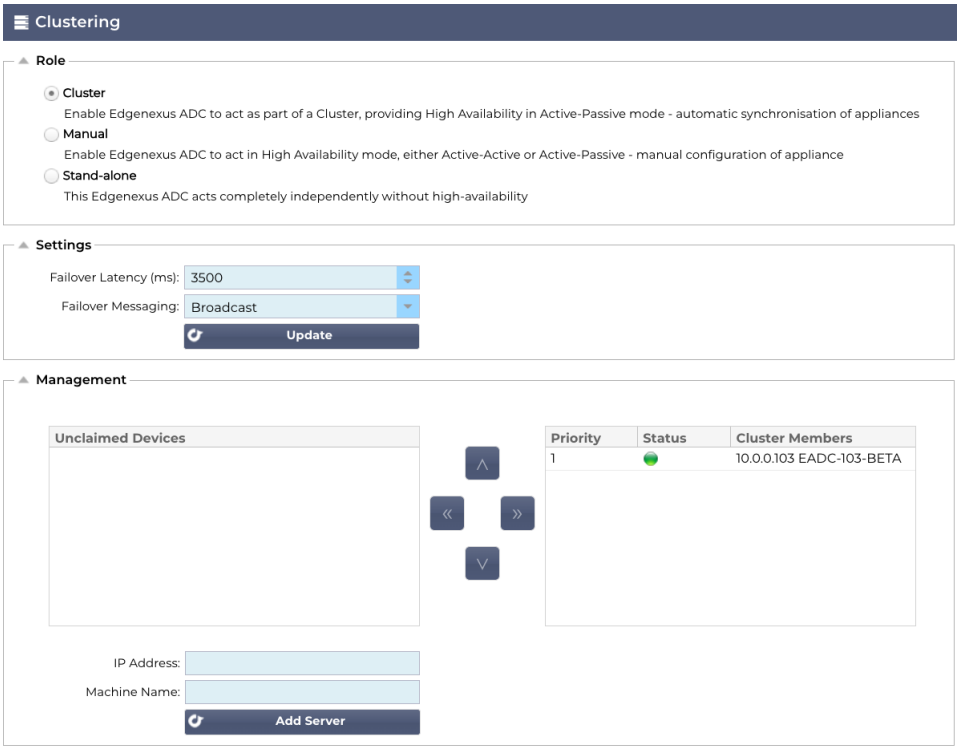
聚类

ADC 可以作为单个独立设备使用，而且使用效果非常好。但是，如果考虑到 ADC 的目的是对服务器进行负载平衡，那么对 ADC 本身进行集群的必要性就显而易见了。ADC 易于浏览的用户界面设计使集群系统的配置简单明了。

系统 > 集群 "页面是配置 ADC 设备高可用性的地方。本节分为几个部分。

重要说明

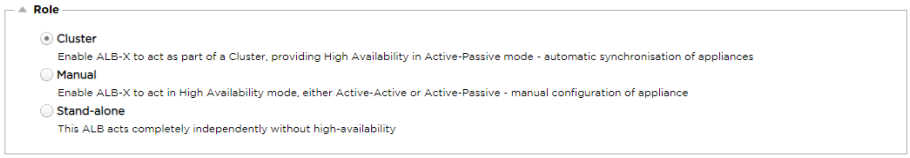
- ADC 对之间无需专用电缆即可保持高可用性心跳。
- 心跳发生在与需要高可用性的虚拟服务相同的网络上。
- ADC 设备之间没有状态故障切换。
- 在两个或更多 ADC 上启用高可用性后，每个机箱将通过 UDP 广播其配置为提供的虚拟服务。
- 高可用性故障切换使用单播信息和免费 ARP 通知新的主动负载平衡器交换机。



角色

在为高可用性配置 ADC 时，有三种群集角色可用。

群组



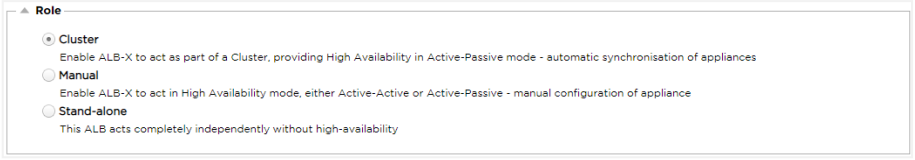
- 默认情况下，新 ADC 将使用群集角色启动。在此角色下，每个群集成员都将具有相同的 "工作配置"，因此在任何时候，群集中只有一个 ADC 处于活动状态。
- 工作配置 "指所有配置参数，但管理 IP 地址、ALB 名称、网络设置、接口详情等需要唯一性的项目除外。
- 在 "群集成员 "框中处于优先级 1（最顶端位置）的 ADC 是群集所有者和主动负载平衡器，而所有其他 ADC 都是被动成员。
- 您可以编辑群集中的任何 ADC，更改将同步到群集的所有成员。
- 从群集中删除 ADC 时，将从该 ADC 中删除所有虚拟服务。
- 您不能将群集的最后一个成员移至无人认领设备。要删除最后一个成员，请将角色更改为手动或独立。
- 下列对象不同步：
    - 手动日期和时间部分 -（NTP 部分同步）
    - 故障切换延迟（毫秒）
    - 硬件部分
    - 电器部分
    - 网络部分

群组所有者故障

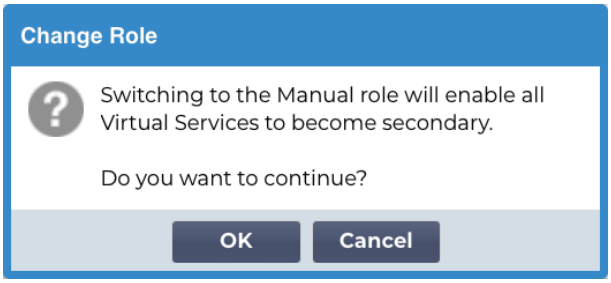
- 当群集所有者发生故障时，其余成员之一将自动接替，继续平衡流量负载。
- 当群集所有者返回时，它将恢复负载平衡流量并接管所有者角色。
- 假设 "所有者 "发生故障，由一名 "成员 "接管负载平衡。如果您希望接管负载平衡流量的成员成为新的所有者，请高亮显示该成员并单击向上箭头将其移动到优先级 1 的位置。
- 如果您编辑了其余群组成员中的一个，而群组所有者宕机，则已编辑的成员将自动升级为群组所有者，而不会损失流量

从群集角色改为手动角色

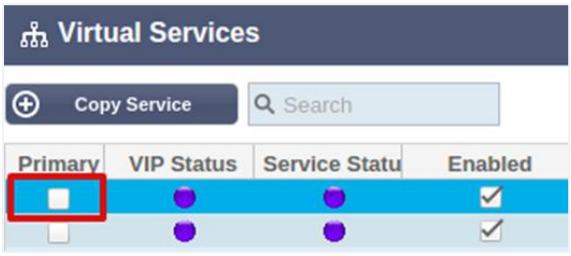
- 如果希望将角色从群集改为手动，请单击手动角色选项旁边的单选按钮



- 点击单选按钮后，您将看到以下信息：



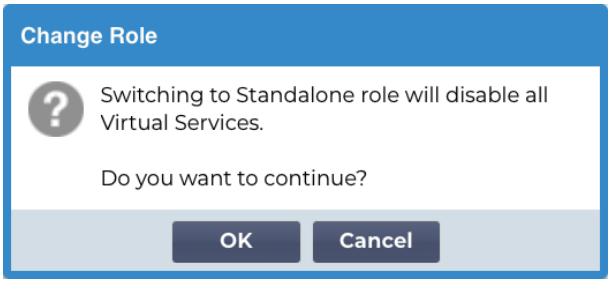
- 单击 "确定 "按钮
- 检查虚拟服务部分。您会发现 "主要 "一栏现在显示了一个未勾选的框。



- 这是一项安全功能，意味着如果您的另一个 ADC 拥有相同的虚拟服务，则流量不会中断。

从群集向独立角色转变

- 如果希望将角色从群集改为单机，请单击单机选项旁边的单选按钮。
- 系统将提示您以下信息：



- 单击 "确定 "更改角色。
- 检查虚拟服务。您会看到 "主要 "栏更名为 "独立"。
- 您还会看到，出于安全原因，所有虚拟服务都已禁用（未勾选）。
- 一旦确定同一网络中没有其他 ADC 有重复的虚拟服务，就可以依次启用每个虚拟服务。

手册作用

手动角色中的 ADC 将与其他手动角色中的 ADC 协同工作，以提供高可用性。与群集角色相比，手动角色的主要优点是可以为虚拟 IP 设置哪个 ADC 处于活动状态。缺点是 ADC 之间没有配置同步。任何更改都必须通过图形用户界面手动复制到每台设备上，或者对于大量更改，可以从一台 ADC 创建 jetPACK 并发送到另一台。

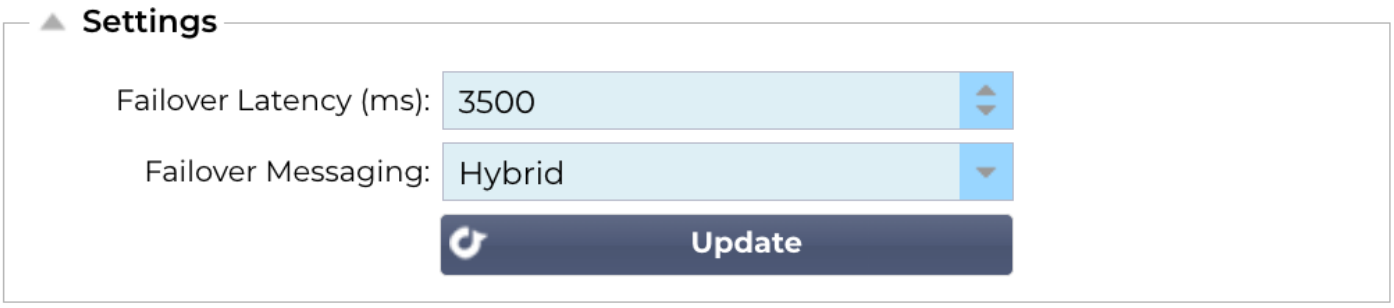
- 要使虚拟 IP 地址 "激活"，请勾选主栏中的复选框（IP 服务页面）
- 要将虚拟 IP 地址设为 "被动"，请将主栏（IP 服务页面）中的复选框留空。

- 如果主动服务故障切换到被动服务：
  - 如果两个 "主要 "栏都打勾，则会进行选举，最低的 MAC 地址将处于 "活动 "状态。
  - 如果两者都未勾选，则进行相同的选举过程。此外，如果两者都未勾选，则不会自动退回到原来的活动 ADC

独立角色

处于独立角色的 ADC 不会就其服务与任何其他 ADC 通信，因此所有虚拟服务都将保持绿色状态和连接。您必须确保所有虚拟服务都有唯一的 IP 地址，否则网络上会出现冲突。

设置

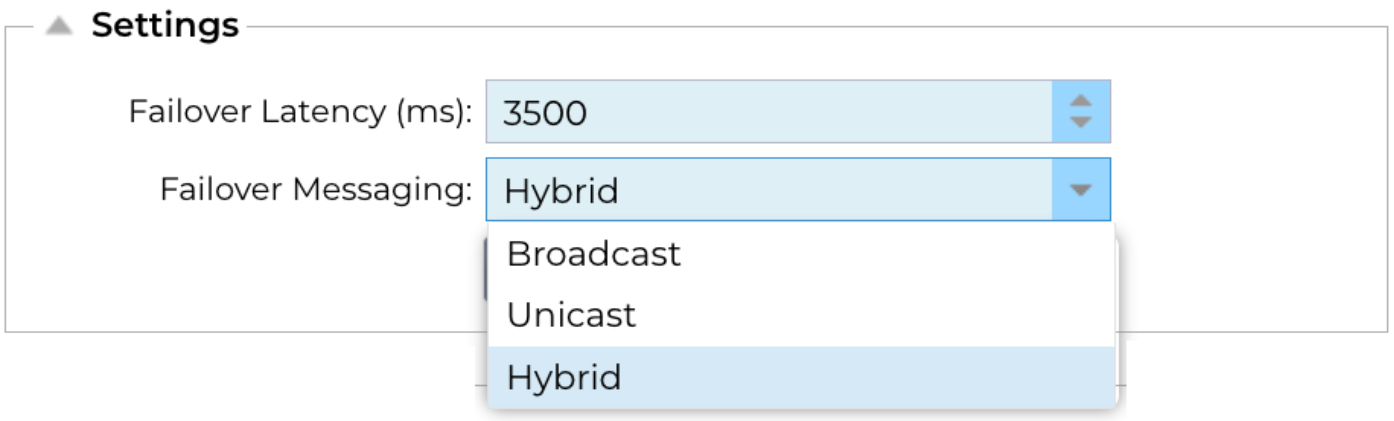


故障切换延迟（毫秒）

可以毫秒为单位设置故障转移延迟。这是主动 ADC 出现故障后，被动 ADC 在接管虚拟服务前等待的时间。

我们建议将其设置为 10000ms 或 10 秒，但您也可以根据自己的网络和要求减少或增加该值。可接受的值介于 1500ms 和 20000ms 之间。如果在较低延迟时群集出现不稳定，则应增加该值。

故障切换信息传送

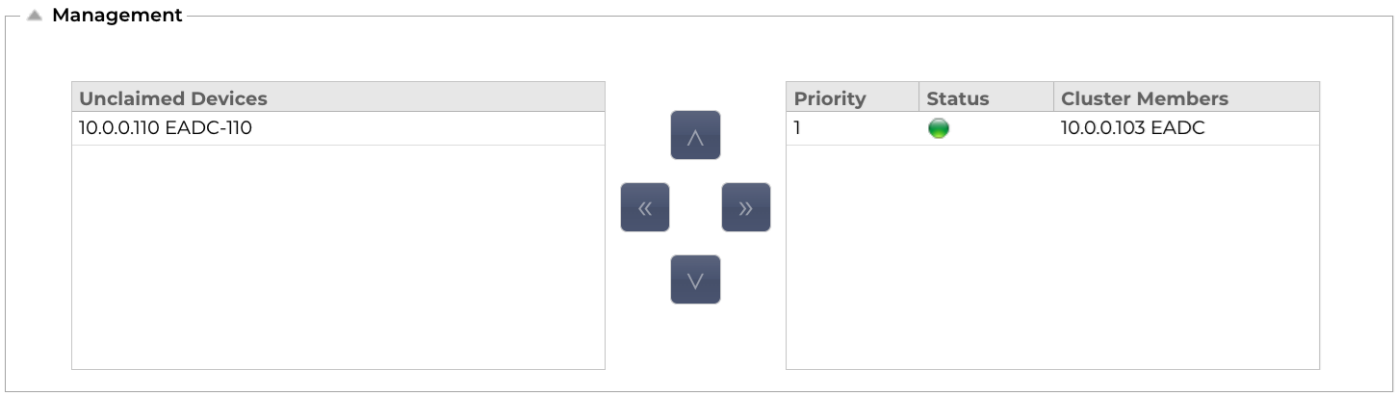


默认情况下，ADC 使用广播发送故障转移消息。不过，有些网络会阻止广播，因此我们提供了单播和混合（单播和广播的混合）功能。

在默认的广播模式下运行时，将自动列出无人认领的设备，并使用广播信息进行故障切换。在混合模式下运行时，无人认领的设备仍将通过广播发布广告，但故障切换通信将通过单播进行。单播模式不会广播，可能需要手动输入群集成员。

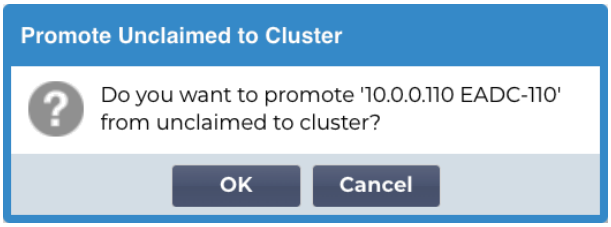
管理层

在本节中，您可以添加和删除群集成员，同时更改群集中 ADC 的优先级。该部分由两个面板和中间的一组箭头键组成。左边的区域是无人认领的设备，最右边的区域是群集本身。

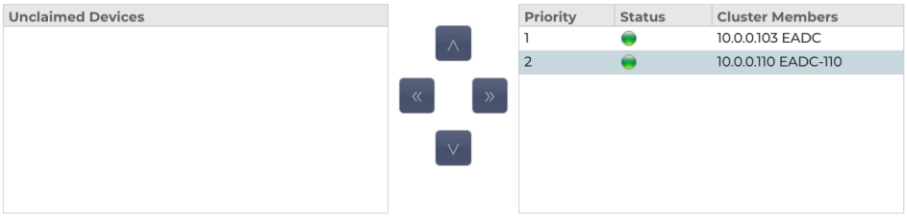


将 ADC 添加到群集

- 将 ADC 添加到群集之前，必须确保所有 ADC 设备都已在系统 > 网络部分设置了唯一名称。
- 在 "管理 "部分的 "群集成员 "列中，您应看到 ADC 为优先级 1，状态为绿色，其名称为绿色。该 ADC 是默认的主设备。
- 所有其他可用的 ADC 都将显示在管理部分的 "无人认领的设备 "窗口中。无人认领设备是指已在群集角色中分配但未配置虚拟服务的 ADC。
- 从 "无人认领的设备 "窗口中选中 ADC，然后单击向右箭头按钮。
- 现在您将看到以下信息：

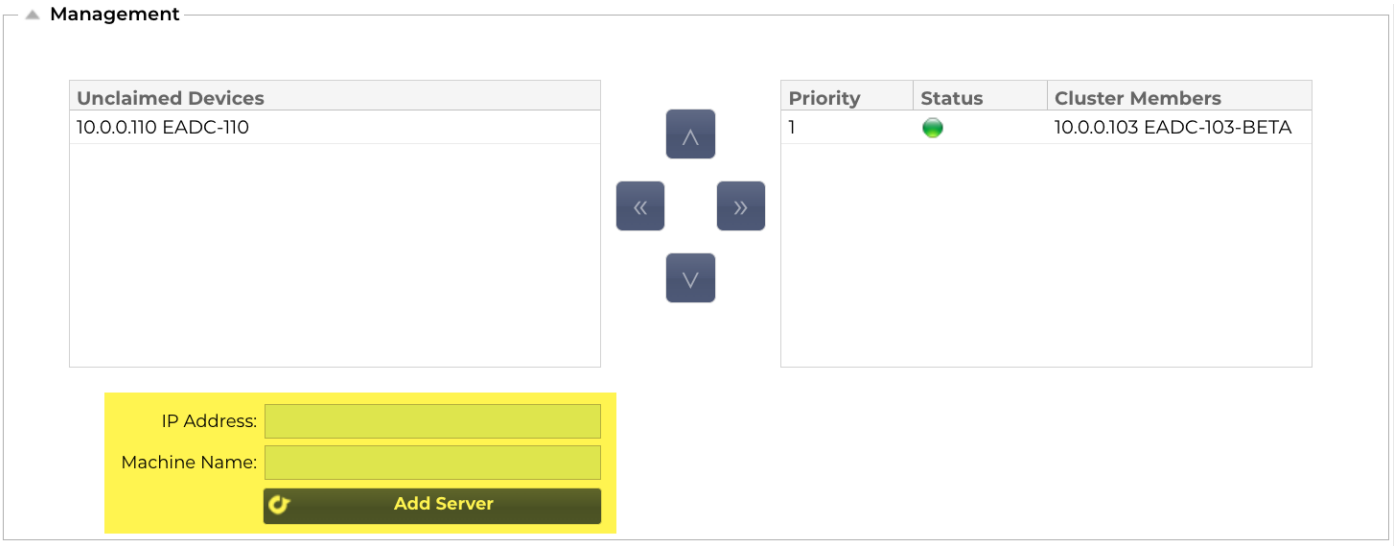


- 单击 "确定 "将 ADC 升级到群集。
- 现在，您的 ADC 在群集成员列表中应显示为优先级 2。



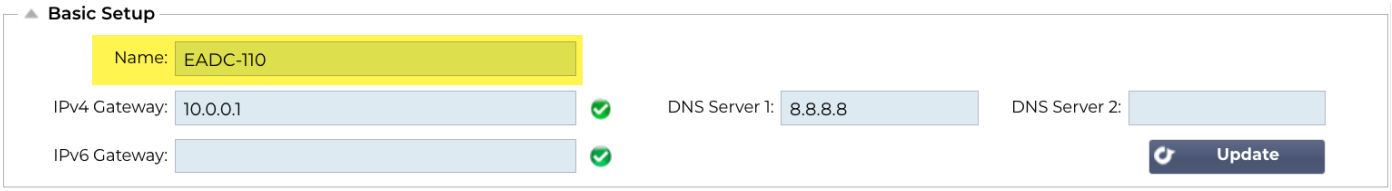
手动将 ADC 添加到群集

在禁止广播的系统中，您需要选择单播或混合模式，才能将 ADC 添加到群集中。



要将 ADC 手动添加到群集：

1. 提供 IP 地址
2. 提供机器名称--可在系统 > 网络部分找到。



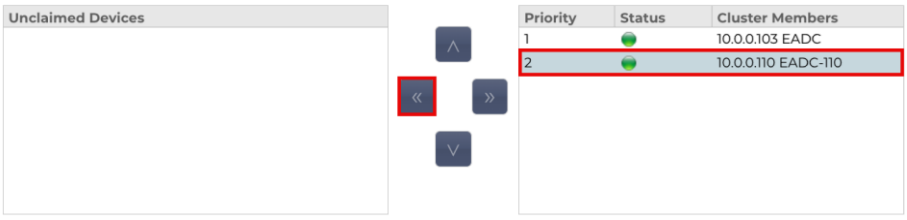
3. 单击添加服务器

然后，ADC 将被添加到群集中。

如果您要添加的 ADC 已在群集中，系统将显示一条错误信息。

删除群组成员

- 突出显示要从群集中删除的群组成员。
- 点击左箭头按钮。

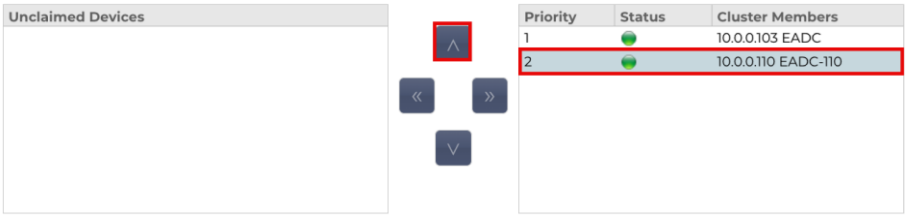


- 您将收到一份确认请求。
- 单击 "确定 "确认。
- 您的 ADC 将被移除，并显示在无人认领设备一侧。

更改 ADC 的优先级

有时您可能希望更改成员名单中 ADC 的优先级。

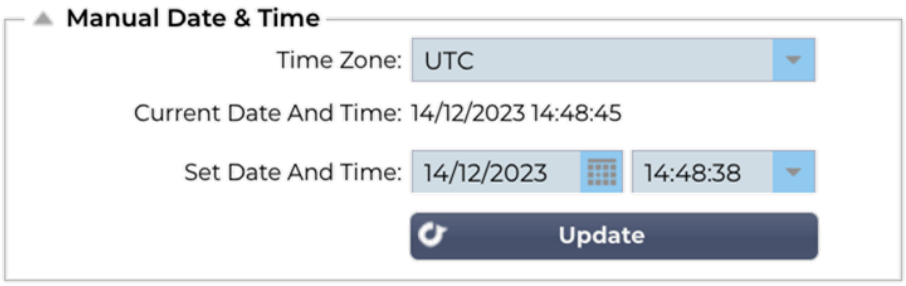
- 群集成员列表顶部的 ADC 优先级为 1，是所有虚拟服务的活动 ADC
- 列表中排名第二的 ADC 优先级为 2，是所有虚拟服务的被动 ADC
- 要更改哪个 ADC 处于活动状态，只需选中该 ADC，然后单击向上箭头，直到它位于列表顶部。



日期和时间

日期和时间部分允许设置 ADC 的日期/时间特性，包括 ADC 所在的时区。日期和时间与时区一起，在与 SSL 加密相关的加密过程中发挥着重要作用。

手动日期和时间



时区

在此字段中设置的值代表 ADC 所在的时区。

- 点击时区下拉框，开始输入您的位置。
- 例如伦敦
- 开始键入时，ADC 会自动显示包含字母 L 的位置。
- 继续输入 "Lon"，以此类推--列出的地点将缩小到包含 "Lon "的地点。
- 如果您在伦敦，则选择欧洲/伦敦设置您的位置

如果上述更改后日期和时间仍然不正确，请手动更改日期

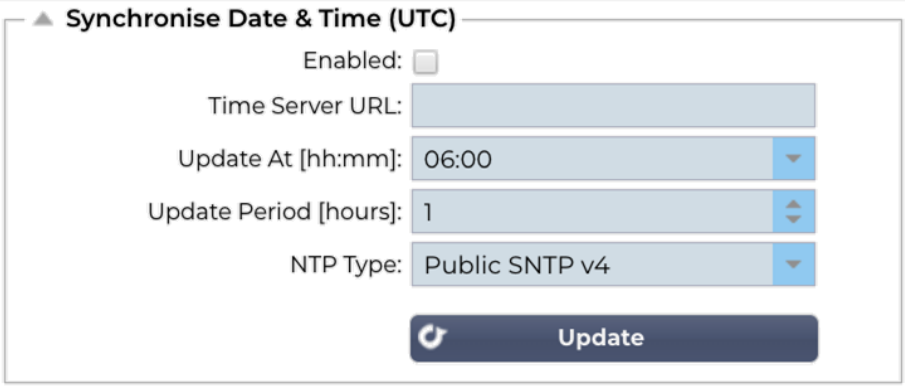
设置日期和时间

该设置代表实际日期和时间。

- 从第一个下拉菜单中选择正确的日期、
  或者，您也可以按照以下格式输入日期 DD/MM/YYYY
- 按以下格式添加时间 hh：mm：ss，例如，06:00:10 表示上午 6 点和 10 秒。
- 输入正确后，请单击 "更新 "进行申请。
- 然后，您将看到新的日期和时间，并以粗体字显示。

同步日期和时间（UTC）

您可以使用 NTP 服务器来准确同步日期和时间。NTP 服务器遍布全球，如果您的基础设施对外部访问有限制，您也可以拥有自己的内部 NTP 服务器。



时间服务器 URL

输入 NTP 服务器的有效 IP 地址或完全合格域名 (FQDN)。如果服务器是互联网上的全球服务器，建议使用 FQDN。

更新时间 [hh:mm]

选择 ADC 与 NTP 服务器同步的预定时间。

更新周期 [小时]:

选择希望同步的频率。

NTP 类型:

- 公共 SNTP V4 - 这是当前与 NTP 服务器同步的首选方法。**RFC 5905**
- 通过 TCP 的 NTP v1 - 通过 TCP 的传统 NTP 版本。**RFC 1059**
- UDP 上的 NTP v1 - UDP 上的传统 NTP 版本。**RFC 1059**

注意：请注意，同步仅以 UTC 为单位。如果要设置本地时间，只能手动完成。这一限制将在以后的版本中修改，以启用选择时区的功能。

电子邮件活动

ADC 是一个关键设备，与任何重要系统一样，它具备向系统管理员通报任何可能需要注意的问题的功能。

系统 > 电子邮件事件页面允许您配置电子邮件服务器连接并向系统管理员发送通知。该页面分为以下几个部分。

地址

将活动发送至电子邮件地址

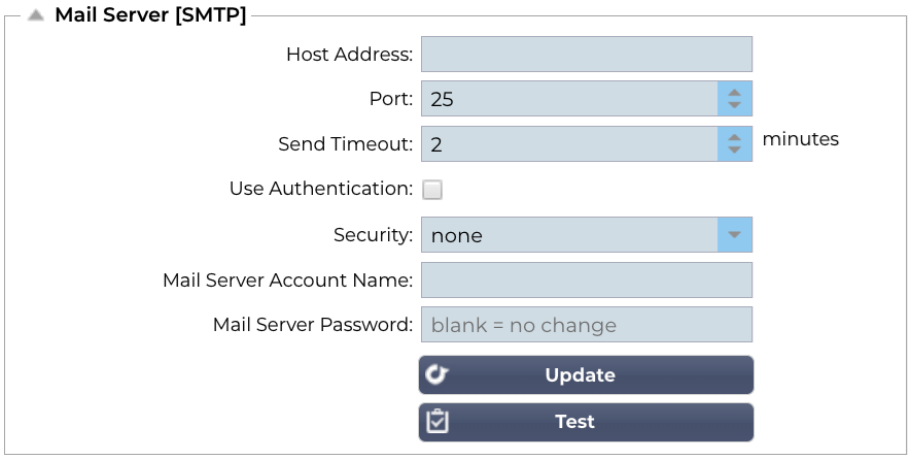
添加有效的电子邮件地址，以便向其发送警报、通知和事件。示例 support@domain.com 。您也可以使用逗号分隔符添加多个电子邮件地址。

返回电子邮件地址：

添加将出现在收件箱中的电子邮件地址。示例 。 adc@domain.com

邮件服务器（SMTP）

在这一部分，您必须添加用于发送邮件的 SMTP 服务器详细信息。请确保用于发送邮件的电子邮件地址已获得授权。



主机地址

添加 SMTP 服务器的 FQDN 或 IP 地址。

港口

添加 SMTP 服务器的端口。SMTP 默认端口为 25，如果使用 SSL，则为 587。

发送超时

添加 SMTP 超时。默认设置为 2 分钟。

使用验证

如果您的 SMTP 服务器要求验证，请勾选该复选框。

安全

- 无
- 默认设置为无。
- SSL - 如果您的 SMTP 服务器需要安全套接字层验证，请使用此设置。
- TLS - 如果您的 SMTP 服务器要求传输层安全验证，请使用此设置。

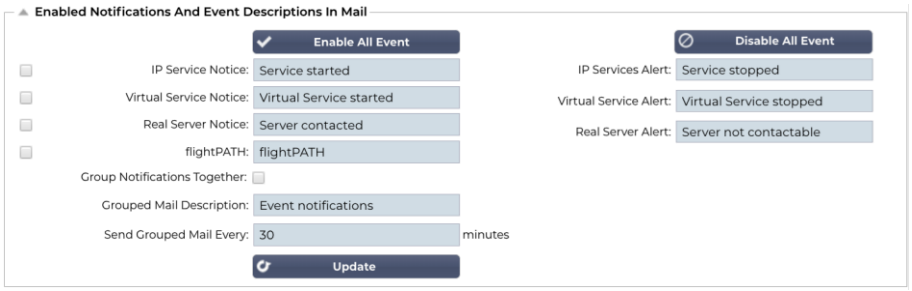
主服务器账户名

添加验证所需的用户名。

邮件服务器密码

输入验证所需的密码。

通知和警报



ADC 将向配置为接收者的人员发送多种类型的事件通知。您可以勾选并启用应发送的通知和警报。当联系到真实服务器或启动通道时会发出通知。当无法联系到真实服务器或通道停止工作时会发出警报。

IP 服务 通知

当任何虚拟 IP 地址在线或停止工作时，IP 服务通知将通知您。此操作针对属于 VIP 的所有虚拟服务。

虚拟服务 通知

通知收件人虚拟服务已上线或已停止工作。

真实服务器 通知

当真实服务器和端口已连接或无法联系时，ADC 将发送真实服务器通知。

飞行路径

该通知是在满足某个条件时发送的电子邮件，其中配置的操作指示 ADC 通过电子邮件发送该事件。

分组通知

勾选将通知分组。打勾后，所有通知和警报都将汇总到一封电子邮件中。

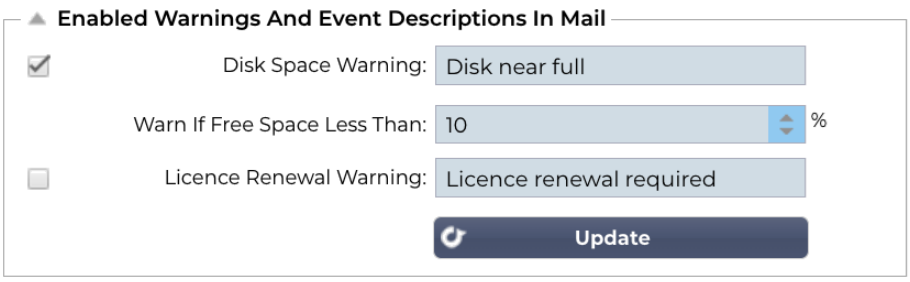
群组邮件描述

指定集体通知电子邮件的相关主题。

群组发送间隔

规定发送群组通知邮件前的等待时间。最短等待时间为 2 分钟。默认设置为 30 分钟。

启用邮件中的警告 和事件描述



警告邮件有两种类型，两种类型都不能忽视。

磁盘空间

设置发出警告前可用磁盘空间的百分比。当达到该百分比时，系统将向您发送电子邮件。

如果可用空间小于

您可以在此设置一个百分比值，这样当磁盘空间低于此阈值时，ADC 就会发送一封警告邮件。

许可证到期

此设置允许您启用或禁用发送给系统管理员的许可证过期警告电子邮件。当达到此值时，您将收到电子邮件。

历史

在 "系统 "部分，有一个 "系统历史记录 "选项，允许提供 CPU、内存、每秒请求数等元素的历史数据和其他功能。启用后，可通过 "查看">"历史记录 "页面以图表形式查看结果。该页面还允许您将历史文件备份或恢复到本地 ADC。

收集数据

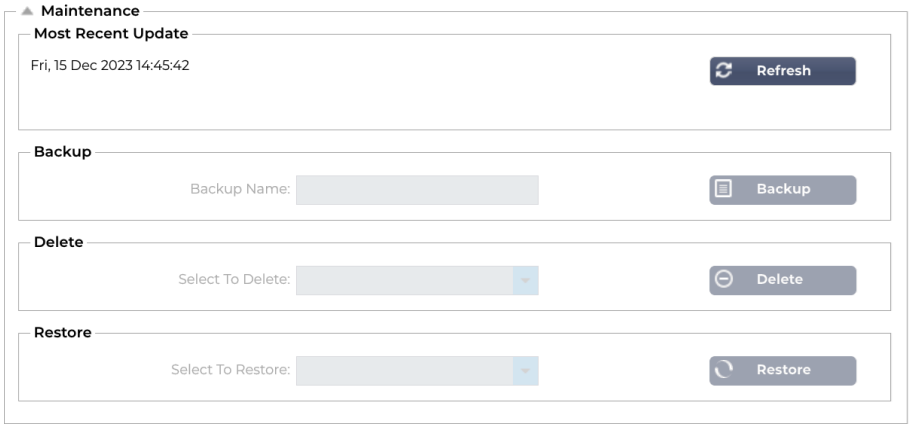
启用

如需收集数据，请勾选复选框。

每次收集数据

然后，设置希望 ADC 收集数据的时间间隔。时间范围为 1-60 秒。

维护



最新更新

这显示了上次从 ADC 采集历史数据的时间。

如果已启用历史日志记录，本部分将显示为灰色。请取消 "收集数据 "部分的 "已启用 "复选框，然后单击 "更新 "以允许维护历史日志。

基于惠普企业的 ADC

本部分功能仅适用于安装在 HPE ProLiant 裸机服务器上并使用 ILO 的 ADC。

备份

为备份命名。单击 "备份 "将所有文件备份到 ADC

删除

从下拉列表中选择备份文件。单击 "删除 "从 ADC 中删除备份文件

恢复

选择先前存储的备份文件。单击 "还原"，从该备份文件中填充数据。

许可证

ADC 授权使用以下任一型号，具体取决于您的购买参数和客户类型。

许可证类型	说明
永久	客户有权永久使用 ADC 和其他软件。这并不排除您需要购买支持以获得帮助和更新。
SaaS	SaaS 或 "软件即服务"（Software-as-a-Service）意味着你基本上是以持续或 "即用即付 "的方式租用软件。在这种模式下，你每年为软件支付租金。您并不拥有软件的永久使用权。
MSP	托管服务提供商可将 ADC 作为一项服务提供，并按每个 VIP 购买许可证，每年收费并支付一次。

许可证详细信息

每个许可证都包含与购买者或组织相关的具体细节。

许可证 ID

许可证 ID 与机器 ID 以及与您购买的 ADC 设备相关的其他详细信息直接相关。该信息非常重要，当您希望从 App Store 获取更新和其他项目时需要该信息。

机器 ID

机器 ID 使用 ADC 设备的 eth0 IP 地址生成。如果更改 ADC 设备的 IP 地址，许可证将不再有效。您必须联系支持人员寻求帮助。我们建议您的 ADC 设备使用固定 IP 地址，并指示 IT 人员不得更改。您可以在 https://www.edgenexus.io/support 上申请技术支持。

注意：不得更改 ADC 设备的 IP 地址。如果您使用的是虚拟化框架，则请固定 MAC ID 并使用静态 IP 地址。

颁发给

该值包含与 ADC 机器 ID 相关联的购买者名称。

联系人

该值包含与机器 ID 相关联的客户公司的联系人信息

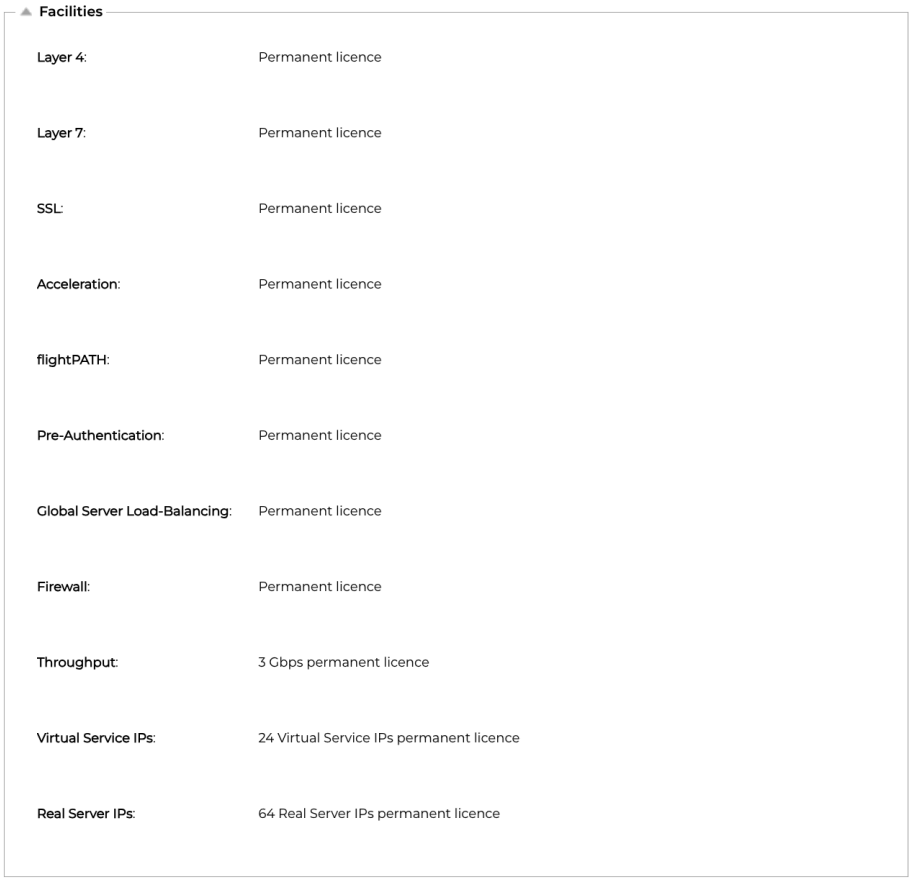
发布日期 d

许可证签发日期。

名称

此值显示您在系统 > 网络中为 ADC 设备提供的描述性名称。

设施



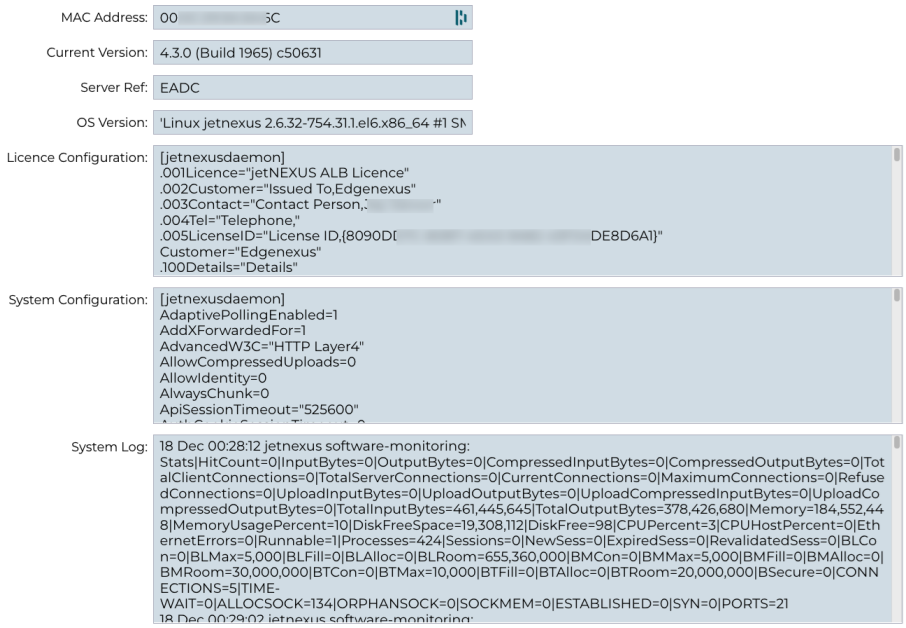
设施 "部分为您提供有关 ADC 内哪些功能已获得使用许可以及许可有效期的信息。同时显示的还有 ADC 的许可吞吐量和真实服务器的数量。这些信息取决于您购买的许可证。

安装许可证 e

- 安装新许可证非常简单。当您从 Edgenexus 收到新的或替换的许可证时，它将以文本文件的形式发送。您可以打开该文件，然后将内容复制并粘贴到 "粘贴许可证 "字段中。
- 如果不能复制/粘贴，也可以上传到 ADC。
- 完成上述操作后，请点击更新按钮。
- 许可证现已安装。

许可证服务信息

单击 "许可证服务信息 "按钮将显示许可证的所有信息。此功能可用于将详细信息发送给支持人员。

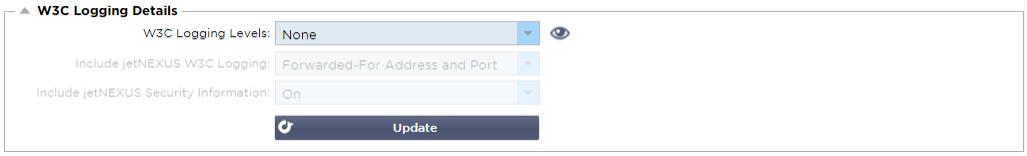


记录

通过系统 > 日志页面，可以设置 W3C 日志级别，并指定自动导出日志的远程服务器。该页面分为以下四个部分。

万维网联盟日志详细信息

启用 W3C 日志会使 ADC 开始记录 W3C 兼容日志文件。W3C 日志是一种 Web 服务器访问日志，其中生成的文本文件包含每个访问请求的相关数据，包括源 Internet 协议 (IP) 地址、HTTP 版本、浏览器类型、引用页面和时间戳。该格式由万维网联盟（W3C）开发，该组织致力于推广网络发展标准。文件采用 ASCII 文本格式，列以空格分隔。文件中包含以 # 字符开头的注释行。这些注释行中有一行指明了字段（提供列名），以便挖掘数据。HTTP 和 FTP 协议有单独的文件。



万维网联盟日志级别

有不同的记录级别，根据服务类型的不同，提供的数据也不同。

上表描述了 W3C HTTP 的日志记录级别。

价值	说明
无	W3C 登录已关闭。
简介	存在的字段有#Fields: time c-ip c-port s-ip method uri x-c-version x-r-version sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x- round-trip-time cs(User-Agent) x-sc(Content-Type).
全部	这是一种与处理器更兼容的格式，具有独立的日期和时间字段。有关字段含义的信息，请参阅下面的字段摘要。显示的字段有#字段： 日期 时间 c-ip c-port cs-username s-ip s-port cs-method cs-uri-stem cs-ur- -query sc-status cs（User-Agent） referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-roun-trip-time x-sc（Content-Type）.
网站	此格式与 "完整 "非常相似，但多了一个字段。有关字段含义的信息，请参阅下面的字段摘要。显示的字段有#字段： 日期 时间 x-mil c-ip c-port cs-username s-ip s-port cs-host cs-method cs-uri-stem cs-ur--query sc-status cs(User-Agent) 引用器 x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-sc(Content-Type)。
诊断	此格式包含与开发和支持人员相关的各种信息。有关字段含义的信息，请参阅下面的字段摘要。显示的字段有#Fields：date time c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new、rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x- compress-action x-sc(Content-Type) x-cache-action X-finish

下表列出了 W3C FTP 的日志记录级别。

价值	说明
简介	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param sc-status sc-param sr-method sr-param rs-status rs-param
全部	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes
诊断	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

包括 W3C 日志

该选项允许您设置 W3C 日志中应包含哪些 ADC 信息。

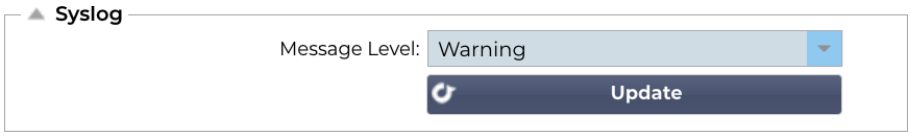
价值	说明
客户网络地址和端口	此处显示的值显示实际客户端 IP 地址和端口。
客户网络地址	该选项将包括并只显示实际的客户端 IP 地址。
转发地址和端口	该选项将显示 XFF 标头中的详细信息，包括地址和端口。
转发地址	该选项将显示 XFF 标头中的详细信息，仅包括地址。

包括安全信息

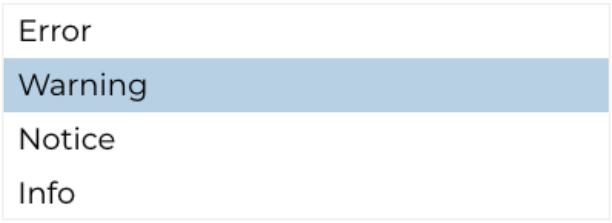
该菜单包括两个选项：

价值	说明
关于	此设置为全局设置。设置为开启时，当任何虚拟服务使用身份验证并启用 W3C 日志时，用户名将被附加到 W3C 日志中。
关闭	这将在全局范围内关闭将用户名记录到 W3C 日志的功能。

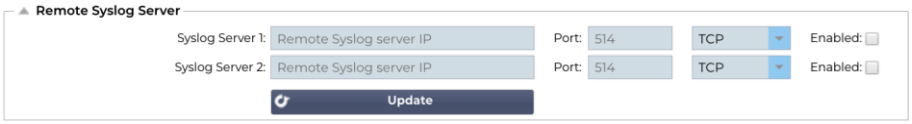
系统日志服务器



本节允许您设置向 SYSLOG 服务器执行的消息记录级别。可用选项如下。



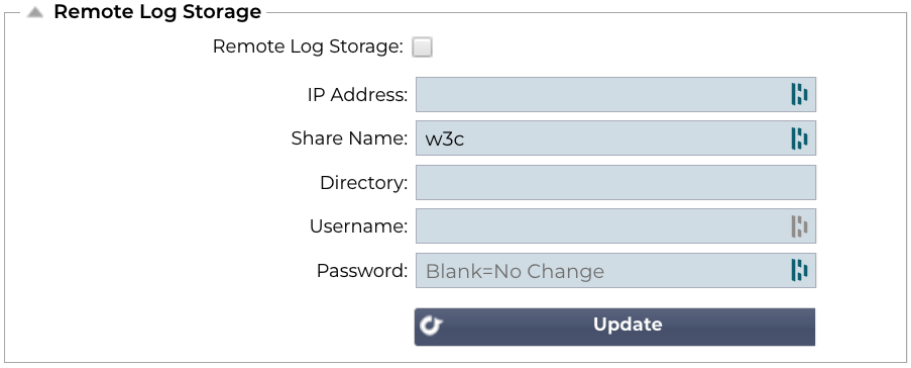
远程系统日志服务器



在本节中，您可以配置两个外部 Syslog 服务器来发送所有系统日志。

- 添加 Syslog 服务器的 IP 地址
- 添加端口
- 选择使用 TCP 还是 UDP
- 勾选已启用复选框开始记录
- 点击更新

远程日志存储



所有 W3C 日志每小时都会以压缩形式存储到 ADC 中。当磁盘空间剩余 30% 时，最旧的文件将被删除。如果希望将这些文件导出到远程服务器保存，可以使用 SMB 共享进行配置。请注意，W3C 日志在文件完成压缩之前不会传输到远程位置。由于日志每小时写入一次，虚拟机设备可能需要两小时，硬件设备可能需要五小时。

Col1	**Col2**
远程日志存储	勾选复选框以启用远程日志存储
IP 地址	指定 SMB 服务器的 IP 地址。应使用点分十进制符号。例如：10.1.1.23
共享名称	指定 SMB 服务器上的共享名称。例如：w3c.
目录	指定 SMB 服务器上的目录。例如/log。
用户名	指定 SMB 共享的用户名。
密码	为 SMB 共享指定密码

实地总结

条件	**说明**
日期	非本地化 = 始终为 YYYY-MM-DD（格林尼治标准时间/夏令时间）
时间	非本地化 = HH:MM:SS 或 HH:MM:SS.ZZZ （GMT/UTC） * 注--不幸的是，这有两种格式（网站）。
	没有 .ZZZ 毫秒）。
x-mil	仅网站格式 = 时间戳的毫秒数
c-ip	根据网络或 X-Forwarded-For 标头得出的客户端 IP
c 端口	从网络或 X-Forwarded-For 标头得出的最佳客户端端口
cs-username	客户的用户名请求字段
s-ip	ALB 的监听端口
s 端口	ALB 聆听 VIP
x-xff	X-Forwarded-For 标头的值
x-xffcustom	配置命名的 X-Forwarded-For 类型请求标头的值
cs 主机	请求中的主机名
x-r-ip	使用的真实服务器 IP 地址
x-r 端口	使用的真实服务器端口
cs 方法	HTTP 请求方法 * Brief 格式除外
方法	* 只有简短格式的 cs-method 使用此名称
cs-uri-stem	请求资源的路径 * Brief 格式除外
cs-uri-query	查询所请求的资源 * Brief 格式除外
uri	* 简短格式记录综合路径和查询字符串
sc-status	HTTP 响应代码

cs(User-Agent)	浏览器的 User-Agent 字符串（由客户端发送）
推荐人	推荐页面（由客户发送）
x-c 版本	客户端请求的 HTTP 版本
x-r 版本	内容-服务器响应 HTTP 版本
cs-bytes	请求中来自客户端的字节数
sr-bytes	请求中转发给真实服务器的字节数
rs-bytes	来自真实服务器的字节，在响应中
字节数	响应中发送给客户端的字节数
x 百分比	压缩百分比 * = 100 * (1 - 输出/输入) 包括标头
所用时间	真实服务器的运行时间（秒
x-trip-times new pcon	从连接到在 "新手列表 "中发帖的毫秒数 从连接到将连接放置到真实服务器的毫秒数
鸳	从连接到完成与真实服务器的连接的毫秒数
rcon	从连接到建立真实服务器连接的毫秒数
rqf	从连接到接收到客户端第一个字节请求的毫秒数
rql	从连接到收到客户端最后一个字节请求的毫秒数
tqf	从连接到向真实服务器发送第一个字节请求的毫秒数
tql	从连接到向真实服务器发送最后一个字节请求的毫秒数
rsf	从连接到收到真实服务器第一个字节响应的毫秒数
rsl	从连接到收到真实服务器最后一个字节响应的毫秒数
tsf	从连接到向客户端发送第一个字节响应的毫秒数
tsl	从连接到向客户端发送最后一个字节响应的毫秒数
剥夺	从连接到断开的毫秒数（双方 - 最后断开的一方）
登录	从连接到此日志记录的毫秒数，后面通常跟（负载平衡策略和推理）
x 往返时间	ALB 所需的时间（秒
x closed-by	是什么操作导致连接关闭（或保持打开状态）
x-compress-action	如何进行或防止压缩
x-sc(Content-Type)	响应内容类型
x-cache-action	缓存如何响应或被阻止
x 饰面	导致此日志记录的触发器

清除日志文件

此功能允许您清除 ADC 中的日志文件。您可以从下拉菜单中选择要删除的日志类型，然后单击 "清除 "按钮。

网络

通过库中的网络部分可以配置 ADC 的网络接口及其行为。

重要事项

在虚拟环境中管理虚拟网络接口

在 ESXi 等虚拟化环境中部署虚拟机时，会自动创建网络接口（如 eth0、eth1）并将其映射到主机配置网络适配器（如网络适配器 1、网络适配器 2）。然而，由于操作系统规则将接口与特定 MAC 地址绑定，这些映射可能并不总是一致的。本节概述了管理主机网络接口的步骤，以防止用户无法访问虚拟机时中断服务。

主要考虑因素

1. **MAC 地址持久性**：
    a. 操作系统根据将名称与特定 MAC 地址关联的规则分配接口名称（如 eth0、eth1）。
    b. 删除并重新创建虚拟机网络接口而不重新使用原始 MAC 地址，会导致网络配置不一致或无法运行。
2. **ADC (EdgeOS) 中的内部映射**：
    a. 虚拟网络接口由 ADC（应用交付控制器）自动识别并在内部映射。
    b. 从虚拟机主机移除网络接口会在 ADC 中留下陈旧的映射，可能会中断管理访问或网络服务。

主机配置的建议步骤

1. **移除 NIC 之前**：
    a. 记录要删除的接口的 MAC 地址。这可以在 ESXi 主机的虚拟机设置中查看。
2. **添加替换网卡时**：
    a. 将先前记录的 MAC 地址分配给新的网络适配器，以确保虚拟机的接口映射保持一致。
3. **防止意外删除关键网卡**：
    a. 确定哪些 NIC 映射到关键 ADC 接口（例如，用于管理访问的 ETH0 (Greenside)）。除非绝对必要，否则避免移除这些 NIC。
4. **验证 MAC 地址一致性**：
    a. 确保分配给虚拟机网络接口的 MAC 地址与 ADC 中的预期配置相匹配。使用 ESXi 主机工具确认此映射。
5. **与虚拟机管理员协调**：
    a. 如果有必要进行可能会影响内部虚拟机配置的更改，请通知虚拟机管理员，为可能出现的中断做好准备，并确保保持正确的映射。

示例场景

1. **初始设置**：
    a. ADC VM 有两个 NIC：NIC1（MAC：00:11:22:33:44:55）和 NIC2（MAC：00:11:22:33:44:66）。
2. **操作**：删除 NIC1 并添加新的 NIC（NIC3）。
    a. 在 ESXi 主机上创建时，将原始 MAC 地址 (00:11:22:33:44:55) 分配给 NIC3。

3. **避免影响**：
    a. 通过重新使用原始 MAC 地址，ADC 的内部映射（如 ETH0）将保持一致，从而避免对管理访问或网络服务造成任何干扰。

在虚拟化环境中管理网络接口时，保持 MAC 地址分配的一致性至关重要。如果无法访问虚拟机，则必须在主机端完成所有必要步骤，以确保无缝运行并防止服务中断。务必与相关管理员协调，以有效解决潜在影响。

避免关键设备频繁 vMotion

vMotion 是 VMware 的一项强大功能，可在 ESXi 主机之间实时迁移虚拟机 (VM)，而无需停机。不过，虽然 vMotion 在保持基础架构的灵活性和可用性方面非常有用，但不建议频繁迁移负载平衡器等关键设备，尤其是当它们正在积极管理大量连接时。

可能还有其他供应商提供的类似技术，但在本节中，我们将以 VMware 为基础进行讨论。

为什么不建议频繁进行 vMotion

1. **会议中断**：
    a. 负载平衡器管理客户机和后端服务器之间的活动会话。在 vMotion 操作期间，会有一段短暂的时间重新初始化网络状态，可能会中断这些会话。
    b. 中断可能会导致连接中断，客户需要重新建立会话，这可能会降低用户体验。
2. **延迟和数据包丢失**：
    a. 在迁移虚拟机的过程中，需要暂时中止并同步其内存和状态。对于处理实时流量的设备来说，这种暂停可能会导致延迟甚至丢包。
    b. 依赖低延迟响应的应用程序可能会出现性能下降或超时。
3. **提高资源利用率**：
    a. vMotion 需要 CPU、内存和网络带宽资源，以便在源主机和目标主机之间同步数据。
    b. 频繁迁移会造成基础设施资源紧张，并可能影响同一环境中托管的其他虚拟机和服务。
4. **对高可用性配置的影响**：
    a. 在具有高可用性 (HA) 配置的环境中，频繁的 vMotion 可能会与故障切换机制发生冲突，从而导致意外行为或故障切换操作延迟。
5. **业务复杂性**：
    a. 不断移动关键虚拟机会增加网络配置的复杂性，包括 VLAN 映射和防火墙规则，从而导致配置错误。

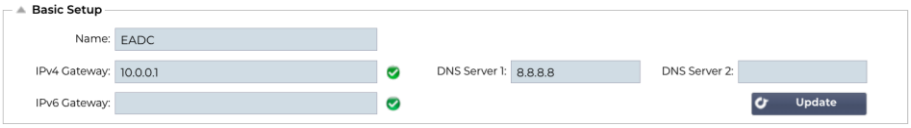
管理关键设备的建议

1. **在维护窗口期间计划 vMotion 操作**：
    a. 将迁移安排在流量较低的时段，以尽量减少对活动会话的影响。
2. **实施负载平衡器集群**：
    a. 对负载平衡器使用群集或高可用性配置以确保冗余。这允许在 vMotion 操作期间将流量无缝重定向到另一个节点。

3. **监控基础设施资源**：
    a. 在启动 vMotion 之前，确保有足够的 CPU、内存和网络带宽，以防止资源争用。
4. **尽量减少迁移频率**：
    a. 将关键设备的 vMotion 限制在绝对必要的情况下，如主机维护或故障恢复。
5. **生产前测试**
    a. 在暂存环境中测试 vMotion 操作，以了解其对活动会话的影响，并确保优化配置。

vMotion 是虚拟机管理的重要工具，但对于负载平衡器等关键设备来说，应谨慎使用。频繁迁移会中断服务、增加延迟并造成资源紧张。通过 仔细规划 vMotion 操作并采用集群和维护调度等策略，可以确保可靠的服务交付并最大限度地降低中断风险。

基本设置



ALB 名称

为 ADC 设备指定名称。请注意，如果群集中有多个成员，则无法更改。请参阅 "群集 "部分。

IPv4 网关

指定 IPv4 网关地址。该地址必须与现有适配器位于同一子网。如果网关添加错误，会在红圈内看到一个白叉。添加正确的网关后，页面底部会出现绿色的成功横幅，IP 地址旁边的绿色圆圈中会出现一个白色的"√"。

IPv6 网关

指定 IPv6 网关地址。该地址必须与现有适配器位于同一子网。如果网关添加错误，你会看到一个红圈中的白叉。添加正确的网关后，页面底部会出现绿色的成功横幅，IP 地址旁边的绿色圆圈中会出现一个白色的"√"。

DNS 服务器 1 和 DNS 服务器 2

添加第一个和第二个 DNS 服务器（可选）的 IPv4 地址。

适配器详细信息

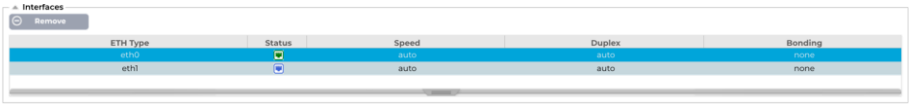
网络面板的这一部分显示 ADC 设备中安装的网络接口。您可以根据需要添加或移除适配器。

专栏	说明

适配器	此列显示设备上安装的物理适配器。点击可用适配器列表中的某个适配器--双击该列表行将进入编辑模式。
VLAN	双击为适配器添加 VLAN ID。VLAN 是一种虚拟局域网，可创建一个不同的广播域。VLAN 具有与物理局域网相同的属性，但如果终端站不在同一个网络交换机上，VLAN 可以更方便地将终端站分组。
IP 地址	双击可添加与适配器接口相关联的 IP 地址。您可以为同一接口添加多个 IP 地址。该地址应是以四点十进制表示的 IPv4 32 位数字。示例 192.168.101.2
子网掩码	双击添加分配给适配器接口的子网掩码。这应该是以四点十进制表示的 IPv4 32 位数字。示例 255.255.255.0
网关	为接口添加网关。添加后，ADC 将设置一个简单的策略，允许从该接口发起的连接通过该接口返回到指定的网关路由器。这样，ADC 就可以安装在更复杂的网络环境中，而无需手动配置复杂的路由策略。
说明	双击为您的适配器添加描述。公共接口示例。 注：ADC 会自动将第一个接口命名为 "绿侧"，第二个接口命名为 "红侧"，第三个接口命名为 "侧 3"，等等。 请根据自己的喜好更改这些命名规则。
网络控制台	双击该列，然后勾选复选框，将接口指定为图形用户界面 Web 控制台的管理地址。更改 Web 控制台监听的接口时请务必小心。您需要设置正确的路由，或与新界面位于同一子网，才能在更改后访问 Web 控制台。将其改回来的唯一方法是访问命令行并发出 set greenside 命令。这将删除除 eth0 以外的所有接口。

接口

网络面板中的 "接口 "部分允许配置与网络接口有关的某些元素。您还可以单击 "移除 "按钮，从列表中移除网络接口。使用虚拟设备时，您在这里看到的接口会受到底层虚拟化框架的限制。



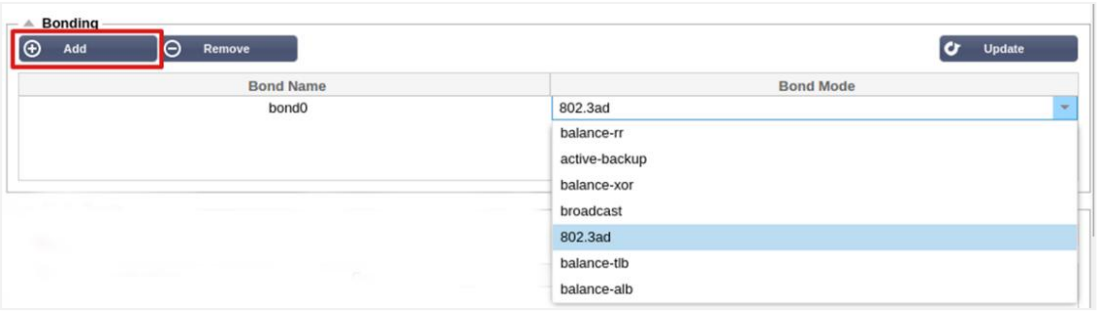
专栏	说明
ETH 类型	该值表示操作系统内部对网络接口的引用。此字段不能自定义。值从 ETH0 开始，根据网络接口的数量依次递增。
现状	此图形显示网络接口的当前状态。绿色状态表示接口已连接并正常运行。其他状态指示如下所示。 **适配器 UP** 适配器下降 拔下适配器插头 适配器丢失
速度	默认情况下，该值设置为自动协商速度。但您可以将接口的网速更改为下拉菜单中的任意值（10/100/1000/AUTO）。
双工	此字段的值可自定义，您可以在自动（默认）、全双工和半双工之间进行选择。
粘接	您可以从已定义的绑定类型中选择一种。更多详情，请参阅 "绑定 "部分。

粘接

网络接口绑定有许多名称：端口中继（Port Trunking）、通道绑定（Channel Bonding）、链路聚合（Link Aggregation）、网卡组（NIC teaming）等。绑定将多个网络连接合并或聚合到 一个单一的通道绑定接口。绑定允许两个或多个网络接口作为一个接口运行，提高吞吐量，并提供冗余或故障切换。

ADC 内核有一个内置的绑定驱动程序，用于将多个物理网络接口聚合为一个逻辑接口（例如，将 eth0 和 eth1 聚合为 bond0）。您可以为每个绑定接口定义模式和链路监控选项。共有七种不同的模式选项，每种模式都提供特定的负载平衡和容错特性。如下图所示。

注：只能为基于硬件的 ADC 设备配置绑定。



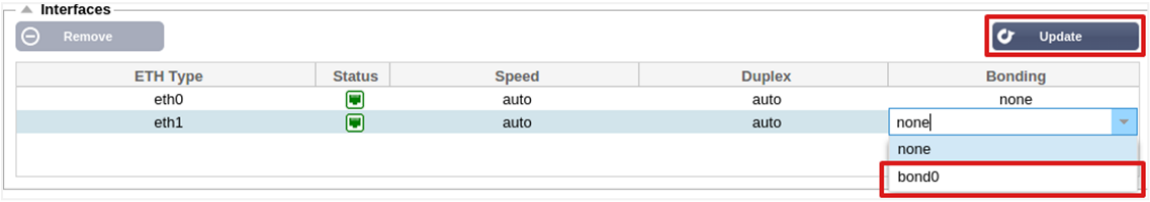
创建粘合档案

- 单击 "添加 "按钮添加新邦德
- 提供绑定配置的名称

- 选择要使用的粘合模式

然后从 "接口 "部分，从网络接口的 "绑定 "下拉字段中选择要使用的绑定模式。

在下面的示例中，eth0、eth1 和 eth2 现在是 bond0 的一部分。而 eth0 仍作为管理接口独立存在。

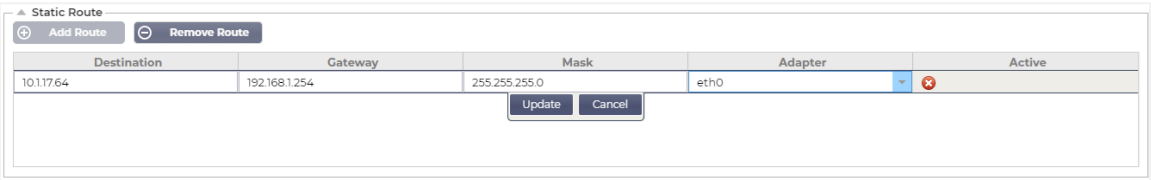


粘合模式

粘合模式	说明
平衡-rr：	数据包按顺序逐个通过每个接口传输/接收。
主动备份：	在这种模式下，一个接口处于活动状态，第二个接口处于备用状态。只有当第一个接口上的活动连接发生故障时，第二个接口才会处于活动状态。
balance-xor：	根据源 MAC 地址与目标 MAC 地址的 XOR 值进行传输。该选项为每个目标 Mac 地址选择相同的从属设备。
广播：	该模式将在所有从属接口上传输所有数据。
802.3ad：	创建共享相同速度和双工设置的聚合组，并按照 802.3ad 规范使用活动聚合器中的所有从属设备。
balance-tlb：	自适应传输负载平衡绑定模式：提供无需任何特殊交换机支持的通道绑定。传出流量根据每个从站的当前负载（相对于速度计算）进行分配。当前从站接收传入流量。如果接收从属设备出现故障，则由另一个从属设备接管故障接收从属设备的 MAC 地址。
balance-alb：	自适应负载平衡绑定模式：也包括用于 IPV4 流量的平衡-tlb 和接收负载平衡（rlb），不需要任何特殊的交换机支持。接收负载平衡通过 ARP 协商实现。绑定驱动程序会拦截本地系统发送的 ARP 回复，并用绑定中一个从属设备的唯一硬件地址覆盖源硬件地址，这样不同的对等设备就会使用不同的服务器硬件地址。

静态路由

有时，您需要为网络中的特定子网创建静态路由。ADC 可让您使用静态路由模块来实现这一功能。



添加静态路由

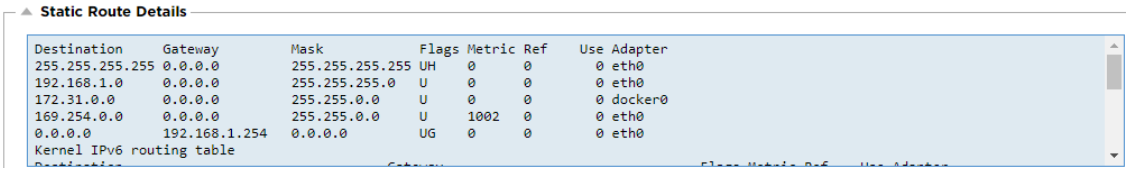
- 单击 "添加路由 "按钮

- 以下表中的详细信息为指导填写该字段。
- 完成后点击更新按钮。

现场	说明
目的地	用十进制点号输入目标网络地址。示例 123.123.123.5
网关	以十进制点符号输入网关 IPv4 地址。示例 10.4.8.1
面罩	以十进制点符号输入目标子网掩码。示例 255.255.255.0
适配器	输入可以连接到网关的适配器。例如 eth1。
活跃	绿色复选框表示可以连接到网关。红叉表示该接口无法连接到网关。请确保已在与网关相同的网络上设置了接口和 IP 地址

静态路由详细信息

本节将介绍 ADC 上配置的所有路由信息。



高级网络设置

纳格尔是什么?

纳格尔算法（Nagle's Algorithm），又称 TCP 无延迟算法，是一种用于网络通信的技术，可减少因数据失序而重新传输的数据包数量。它的工作原理是，如果没有收到前一个数据包的确认，则延迟发送小数据包。这有助于确保数据以正确的顺序到达，并减少网络负载。

参见**维基百科关于纳格尔的文章**

服务器 Nagle

勾选此框可启用服务器 Nagle 设置。服务器 Nagle 是一种通过减少需要在网络上发送的数据包数量来提高 TCP/IP 网络效率的方法。此设置适用于交易的服务器端。必须注意服务器设置，因为 Nagle 和延迟 ACK 可能会严重影响性能。

客户 Nagle

勾选复选框以启用客户端 Nagle 设置。同上，但适用于交易的客户端。

SNAT

SNAT 是源网络地址转换（Source Network Address Translation）的缩写，不同供应商在 SNAT 的实现上略有不同。EdgeADC SNAT 的简单解释如下。

在正常情况下，入站请求会被定向到 VIP，VIP 会看到请求的源 IP。因此，举例来说，如果浏览器端点的 IP 地址是 81.71.61.51，VIP 就会看到这个地址。

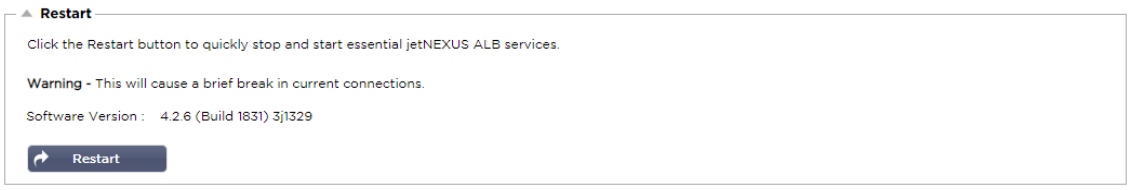
当 SNAT 生效时，VIP 将看不到请求的原始源 IP，取而代之的是 SNAT 规则中提供的 IP 地址。因此，SNAT 可用于第 4 层和第 7 层负载平衡模式。

现场	说明
来源 IP	源 IP 地址是可选项，可以是网络 IP 地址（带/掩码），也可以是纯 IP 地址。掩码既可以是网络掩码，也可以是普通数字，指定网络掩码左侧 1 的个数。因此，/24 的掩码相当于 255.255.255.0。
目的地 IP	目标 IP 地址是可选项，可以是网络 IP 地址（带/掩码），也可以是纯 IP 地址。掩码既可以是网络掩码，也可以是普通数字，指定网络掩码左侧 1 的个数。因此，/24 的掩码相当于 255.255.255.0。
来源港	源端口是可选项，它可以是一个数字，在这种情况下，它只指定该端口；也可以包含一个冒号，在这种情况下，它指定一系列端口。示例：80 或 5900:5905：80 或 5900:5905。
目的港	目标端口是可选的，它可以是一个数字，在这种情况下只指定该端口，也可以包含一个冒号，在这种情况下指定一系列端口。例如 80 或 5900:5905。
规程	您可以选择在单个协议或所有协议上使用 SNAT。我们建议具体问题具体分析。
SNAT 转 IP	SNAT 至 IP 是一个强制 IP 地址或 IP 地址范围。例如：10.0.0.1 或 10.0.0.1-10.0.0.3：10.0.0.1 或 10.0.0.1-10.0.0.3。
SNAT 至端口	SNAT to Port（SNAT 至端口）是可选的，它可以是一个数字，在这种情况下只指定该端口，也可以包含一个破折号，在这种情况下指定一系列端口。例如 80 或 5900-5905。
说明	用它来起一个友好的名字，以提醒自己规则存在的原因。这也有助于在 Syslog 中进行调试。

电源

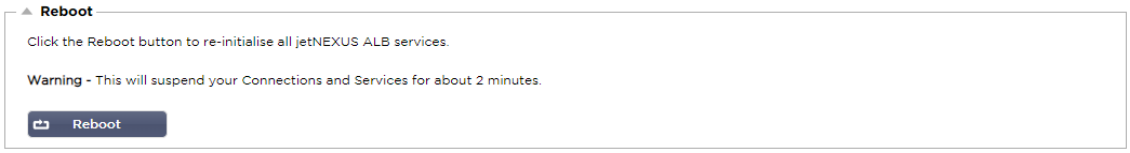
此 ADC 系统功能还允许您在 ADC 上执行若干与电源相关的任务。

重新启动



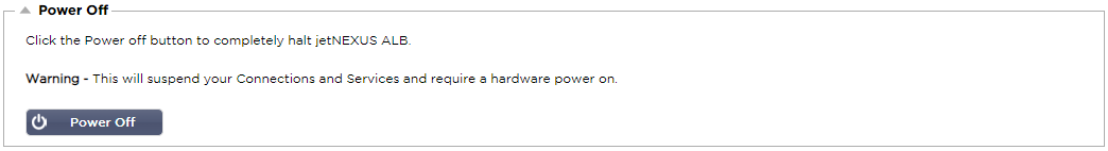
此设置会启动所有服务的全局重启，从而中断所有当前活动连接。所有服务将在短时间后自动恢复，但时间取决于配置的服务数量。系统将弹出一个窗口，要求确认重启操作。

重新启动



单击 "重启 "按钮将对 ADC 进行电源循环，使其自动恢复到活动状态。此时会弹出一个窗口，要求确认重启操作。

关闭电源



单击 "关机 "按钮将关闭 ADC。如果是硬件设备，则需要对设备进行物理访问才能重新启动。系统将弹出一个窗口，要求确认关闭操作。

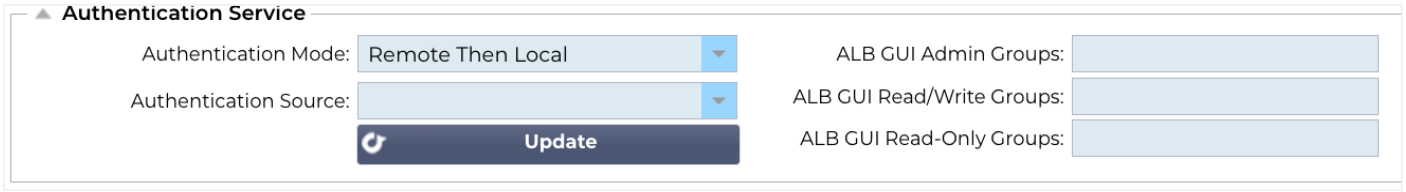
安全

本节允许您更改网络控制台密码，启用或禁用安全外壳访问。还可以启用 REST API 功能。

SSH

选项	说明
安全 Shell 远程连接	如果希望使用 SSH 访问 ADC，请勾选该复选框。"Putty "是一个很好的应用程序。

认证服务



大多数机构都要求必须通过公司自己的身份验证服务来访问 ADC 的管理界面。

针对这种情况，我们提供了此处描述的身份验证服务功能。该功能可与本地目录服务以及 SAML 等外部服务一起运行。

选项	说明
认证模式	仅限本地：这是默认模式，使用 ADC 内的本地数据库，例如用户 admin。 先远程后本地：ADC 将尝试根据 "验证源 "字段中指定的远程验证服务器验证用户。如果验证不成功，它将使用本地数据库作为验证源。
认证源	该下拉菜单允许您选择在库 > 身份验证中定义的一个身份验证服务器。
ALB GUI 管理组	指定允许的管理员组别。
ALB GUI 读写组	指定允许的读写组
ALB GUI 只读组	指定允许的只读组。

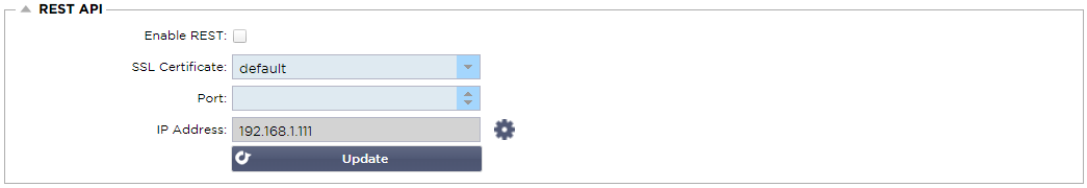
网络控制台

SSL 证书 从下拉列表中选择一个证书。您选择的证书将用于确保与 ADC 网络用户界面连接的安全性。您可以在 ADC 中创建自签名证书，也可以从 **SSL 证书**部分导入证书。

选项	说明
安全端口	网络控制台的默认端口是 TCP 443。如果出于安全考虑希望使用其他端口，可以在此进行更改。

REST API

REST API 也称为 RESTful API，是一种符合 REST 架构风格的应用程序接口，允许对 ADC 进行配置或从 ADC 提取数据。REST 是计算机科学家罗伊-菲尔丁（Roy Fielding）创造的表征状态转移（representational state transfer）的缩写。



选项	说明
启用 REST	勾选此框可启用 REST API 访问。请注意，您还必须配置启用 REST 的适配器。请参阅下面的 Cog 链接说明。
SSL 证书	为 REST 服务选择证书。下拉菜单将显示 ADC 上安装的所有证书。
港口	设置 REST 服务的端口。最好使用 443 以外的端口。
IP 地址	这将显示 REST 服务绑定的 IP 地址。您可以单击 Cog 链接访问网络页面，更改 REST 服务启用的适配器。
齿轮链接	点击该链接将进入网络页面，在这里可以为 REST 配置适配器。

REST API 文档

有关如何使用 REST API 的文档如下：**jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

注意：如果您在 Swagger 页面上遇到错误，这是因为它们对查询字符串的支持有问题。越过错误滚动到 jetNEXUS REST API

实例

使用 CURL 获取 GUID：

- 指挥

```
curl -k HTTPs://<rest ip>/POST/32 -H "Content-Type: application/json" -X POST -d '{"<rest username>":"<password>"}'"。
```

- 将返回

```
{"Loginstatus": "OK", "Username":"<rest username>", "GUID":"<guid>"}
```

- 有效性
    - GUID 的有效期为 24 小时

许可证详细信息

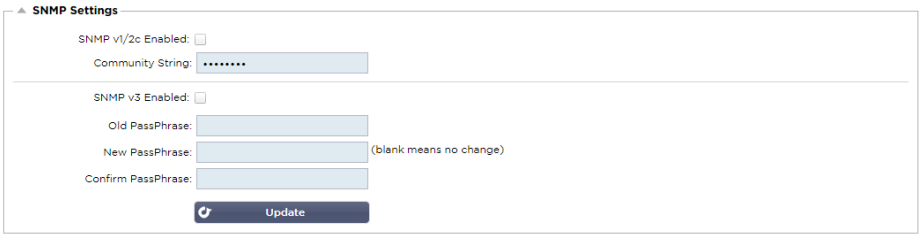
- 指挥

```
curl -k HTTPs://<rest ip>/GET/39 -GET -b 'GUID=<guid;>
```

简单网络管理协议

SNMP 部分允许配置 ADC 内部的 SNMP MIB。然后，能够与配备 SNMP 的设备进行通信的第三方软件就可以查询 MIB。

SNMP 设置



选项	说明
SNMP v1 / V2C	勾选复选框以启用 V1/V2C MIB。 SNMP v1 符合 RFC-1157。SNMP V2c 符合 RFC-1901-1908 标准。
SNMP v3	勾选复选框以启用 V3 MIB。RFC-3411-3418。 V3 的用户名为 admin。 示例：- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
社区字符串	这是在代理上设置的只读字符串，管理器使用它来检索 SNMP 信息。默认社区字符串为 jetnexus
密码	这是启用 SNMP v3 时所需的密码，必须至少包含 8 个字符或更多字符，且只能包含字母 Aa-Zz 和数字 0-9。默认密码为 **jetnexus**

SNMP MIB

可通过 SNMP 查看的信息由管理信息库（MIB）定义。MIB 描述了管理数据的结构，并使用分层对象标识符 (OID)。每个 OID 都可以通过 SNMP 管理应用程序读取。

MIB 下载

可在此处下载 MIB：

ADC OID

根 OID

```
iso.org.dod.internet.private.enterprise = .1.3.6.1.4.1
```

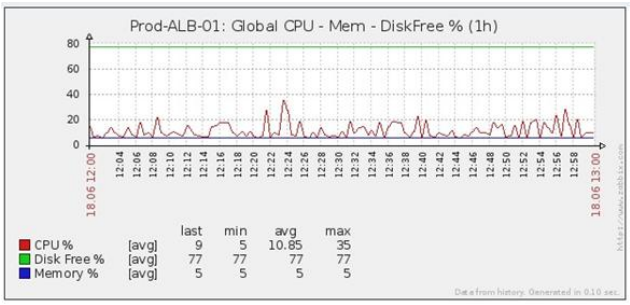
我们的 OID

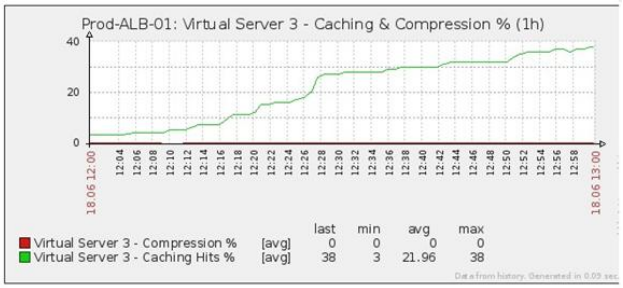
```
.38370 jetnexusMIB
      .1 jetnexusData   (1.3.6.1.4.1.38370.1)
            .1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
            .2 jetnexusVirtualServices   (1.3.6.1.4.1.38370.1.2)
            .3 jetnexusServers   (1.3.6.1.4.1.38370.1.3)
```

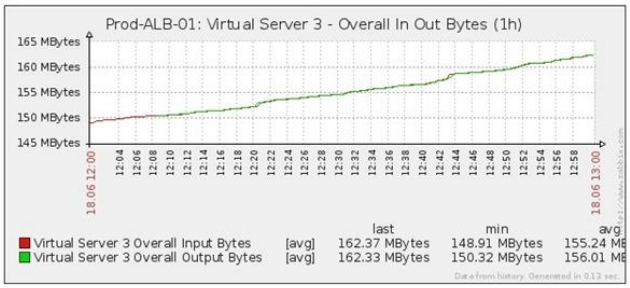
```
.1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
      .1 jetnexusOverallInputBytes (1.3.6.1.4.1.38370.1.1.1.0)
      .2 jetnexusOverallOutputBytes (1.3.6.1.4.1.38370.1.1.2.0)
      .3 jetnexusCompressedInputBytes (1.3.6.1.4.1.38370.1.1.3.0)
      .4 jetnexusCompressedOutputBytes (1.3.6.1.4.1.38370.1.1.4.0)
      .5 jetnexusVersionInfo (1.3.6.1.4.1.38370.1.1.5.0)
      .6 jetnexusTotalClientConnections (1.3.6.1.4.1.38370.1.1.6.0)
      .7 jetnexusCpuPercent (1.3.6.1.4.1.38370.1.1.7.0)
      .8 jetnexusDiskFreePercent (1.3.6.1.4.1.38370.1.1.8.0)
      .9 jetnexusMemoryPercent (1.3.6.1.4.1.38370.1.1.9.0)
      .10 jetnexusCurrentConnections (1.3.6.1.4.1.38370.1.1.10.0)

.2 jetnexusVirtualServices (1.3.6.1.4.1.38370.1.2)
      .1 jnvirtualserviceEntry (1.3.6.1.4.1.38370.1.2.1)
            .1 jnvirtualserviceIndexvirtualservice (1.3.6.1.4.1.38370.1.2.1.1)
            .2 jnvirtualserviceVSAddrPort (1.3.6.1.4.1.38370.1.2.1.2)
            .3 jnvirtualserviceOverallInputBytes (1.3.6.1.4.1.38370.1.2.1.3)
            .4 jnvirtualserviceOverallOutputBytes (1.3.6.1.4.1.38370.1.2.1.4)
            .5 jnvirtualserviceCacheBytes (1.3.6.1.4.1.38370.1.2.1.5)
            .6 jnvirtualserviceCompressionPercent (1.3.6.1.4.1.38370.1.2.1.6)
            .7 jnvirtualservicePresentClientConnections (1.3.6.1.4.1.38370.1.2.1.7)
            .8 jnvirtualserviceHitCount (1.3.6.1.4.1.38370.1.2.1.8)
            .9 jnvirtualserviceCacheHits (1.3.6.1.4.1.38370.1.2.1.9)
            .10 jnvirtualserviceCacheHitsPercent (1.3.6.1.4.1.38370.1.2.1.10)
            .11 jnvirtualserviceVSStatus (1.3.6.1.4.1.38370.1.2.1.11)

.3 jetnexusRealServers (1.3.6.1.4.1.38370.1.3)
      .1 jnrealserverEntry (1.3.6.1.4.1.38370.1.3.1)
            .1 jnrealserverIndexVirtualService (1.3.6.1.4.1.38370.1.3.1.1)
            .2 jnrealserverIndexRealServer (1.3.6.1.4.1.38370.1.3.1.2)
            .3 jnrealserverChAddrPort (1.3.6.1.4.1.38370.1.3.1.3)
            .4 jnrealserverCSAddrPort (1.3.6.1.4.1.38370.1.3.1.4)
            .5 jnrealserverOverallInputBytes (1.3.6.1.4.1.38370.1.3.1.5)
            .6 jnrealserverOverallOutputBytes (1.3.6.1.4.1.38370.1.3.1.6)
            .7 jnrealserverCompressionPercent (1.3.6.1.4.1.38370.1.3.1.7)
            .8 jnrealserverPresentClientConnections (1.3.6.1.4.1.38370.1.3.1.8)
            .9 jnrealserverPoolUsage (1.3.6.1.4.1.38370.1.3.1.9)
            .10 jnrealserverHitCount (1.3.6.1.4.1.38370.1.3.1.10)
            .11 jnrealserverRSStatus (1.3.6.1.4.1.38370.1.3.1.11)
```

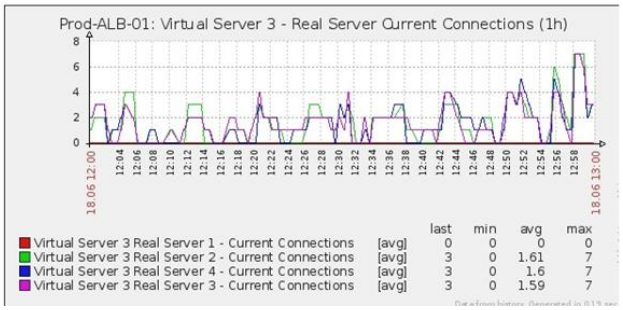
历史图表

ADC 的自定义 SNMP MIB 的最佳用途是将历史图表卸载到您选择的管理控制台。下面是 Zabbix 针对上述各种 OID 值轮询 ADC 的一些示例。


Prod-ALB-01: Global CPU - Mem - DiskFree % (1h)
80
60
40
20
0
18.06 12:00
18.06 13:00
last min avg max
CPU % [avg] 9 5 10.85 35
Disk Free % [avg] 77 77 77 77
Memory % [avg] 5 5 5 5


Prod-ALB-01: Virtual Server 3 - Caching & Compression % (1h)
40
20
0
18.06 12:00
18.06 13:00
last min avg max
Virtual Server 3 - Compression % [avg] 0 0 0 0
Virtual Server 3 - Caching Hits % [avg] 38 3 21.96 38


Prod-ALB-01: Virtual Server 3 - Overall In Out Bytes (1h)
165 MBytes
160 MBytes
155 MBytes
150 MBytes
145 MBytes
18.06 12:00
18.06 13:00
last min avg
Virtual Server 3 Overall Input Bytes [avg] 162.37 MBytes 148.91 MBytes 155.24 MB
Virtual Server 3 Overall Output Bytes [avg] 162.33 MBytes 150.32 MBytes 156.01 MB


Prod-ALB-01: Virtual Server 3 - Real Server Current Connections (1h)
8
6
4
2
0
18.06 12:00
18.06 13:00
last min avg max
Virtual Server 3 Real Server 1 - Current Connections [avg] 0 0 0 0
Virtual Server 3 Real Server 2 - Current Connections [avg] 3 0 1.61 7
Virtual Server 3 Real Server 4 - Current Connections [avg] 3 0 1.6 7
Virtual Server 3 Real Server 3 - Current Connections [avg] 3 0 1.59 7

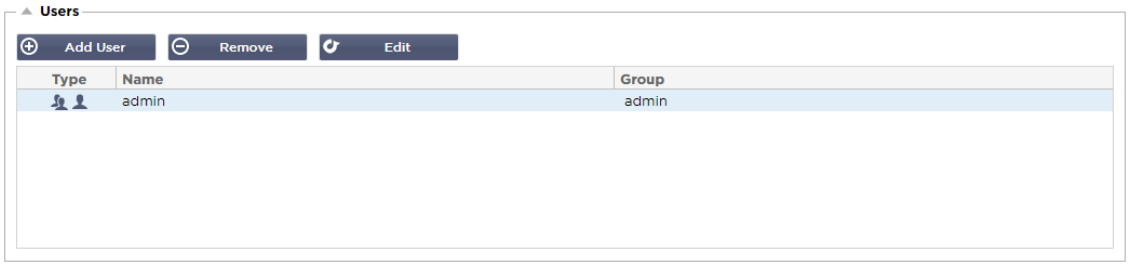
用户和审计日志

ADC 可提供一组内部用户来配置和定义 ADC 的功能。在 ADC 中定义的用户可根据其角色执行各种操作。

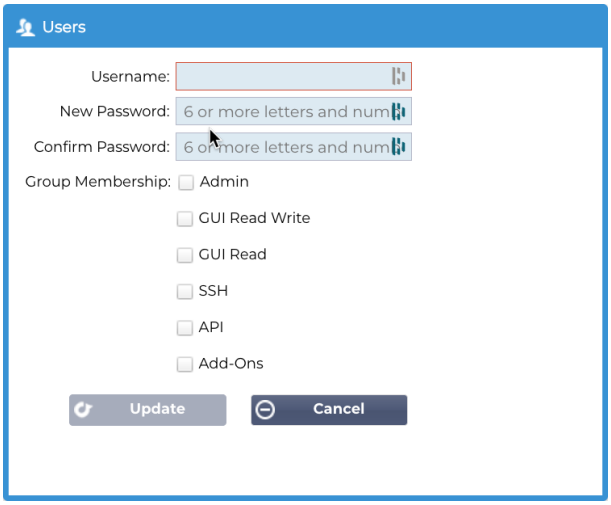
默认用户名为 **admin**，在首次配置 ADC 时使用。admin 的默认密码是 **jetnexus**。

用户

用户 "部分用于创建、编辑和删除 ADC 中的用户。



添加用户



单击上图中的添加用户按钮，弹出添加用户对话框。

参数	说明/用途
用户名	输入您选择的用户名。 用户名必须符合以下要求： • 最少字符数 1 • 最大字符数 32 • 字母可以是大写字母，也可以是小写字母。 • 可以使用数字。 • 不允许使用符号
密码	输入符合以下要求**的强**密码。 • 最少字符数 6 • 最大字符数 32 • 必须至少使用字母和数字的组合。 • 字母可以是大写或小写。 • 允许使用符号，以下示例中的符号除外 **£**, **%**, &, **<** 、 **>**
确认密码	再次确认密码，确保正确无误
团体会员	勾选希望用户所属的组。 • 管理员 - 该小组无所不能。 • GUI 读写 - 该组用户可以访问 GUI 并通过 GUI 进行更改。 • GUI 读取 - 该组用户只能访问 GUI 查看信息。不能进行任何更改。 • SSH - 该组中的用户可以通过安全外壳访问 ADC。选择此选项可访问命令行，该命令行只有最基本的可用命令集。 • API - 本组用户可访问 SOAP 和 REST 可编程接口。REST 将从软件版本 4.2.1 开始提供 • 附加组件 - 授予访问附加组件配置的权限。

用户类型

	本地用户 单机或手动 H/A 角色的 ADC 只能创建本地用户。 默认情况下，名为 "admin "的本地用户是 admin 组的成员。为了向后兼容，该用户永远不能删除。 您可以更改或删除用户的密码，但不能删除上一个本地管理员。
	集群用户 群集中的 ADC 角色只能创建群集用户。 在群集中的所有 ADC 上同步群集用户 对群集用户的任何更改都会影响群集的所有成员。 如果您以群集用户身份登录，则无法将角色从群集切换为手动或独立角色

	群组和本地用户 在单机或手动角色下创建的任何用户都将复制到群集。 如果 ADC 随后离开群集，则只保留本地用户。 用户上次配置的密码将有效。

删除用户

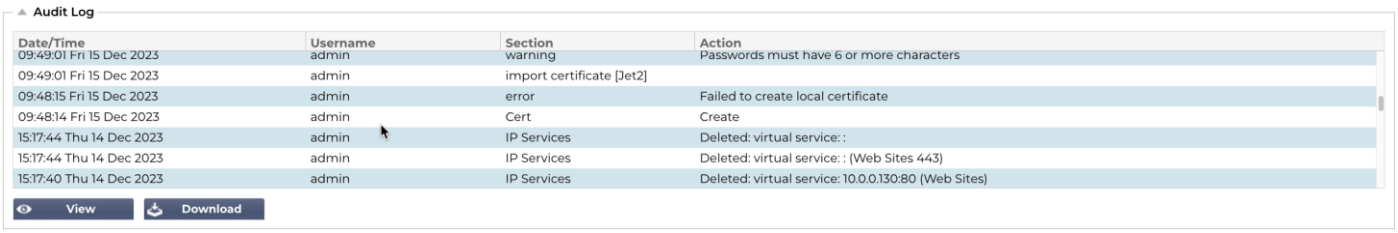
- 突出显示现有用户。
- 单击删除。
- 您将无法删除当前已登录的用户。
- 您将无法删除管理员组中的最后一个本地用户。
- 您将无法删除管理员组中剩余的最后一个群集用户。
- 为了向后兼容，您将无法删除管理员用户。
- 如果从群集中删除 ADC，除本地用户外的所有用户都将被删除。

编辑用户

- 突出显示现有用户。
- 点击编辑
- 您可以通过勾选相应的框并更新来更改用户的组员资格。
- 如果您有管理员权限，还可以更改用户密码。

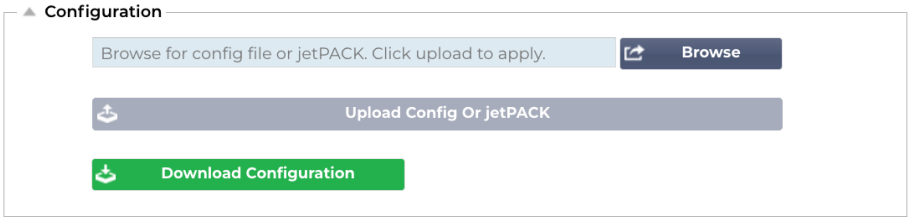
审计日志

ADC 会记录单个用户对 ADC 配置所做的更改。审计日志将提供所有用户执行的最近 50 次操作。您也可以在日志部分看到所有条目。例如



高级

配置



在 ADC 完全设置好并按要求工作后，最好下载并保存其配置。您可以使用配置模块下载和上传配置。

Jetpack 是标准应用程序的配置文件，由 Edgenexus 提供，可简化您的工作。这些文件也可以通过配置模块上传到 ADC。

配置文件本质上是一个基于文本的文件，因此可以使用 Notepad++、Nano 或 VI 等文本编辑器进行编辑。按要求编辑后，即可将配置文件上传到 ADC。

小心：

编辑 EdgeADC 的配置文件仅供受过培训的专家使用。如果您决定自行编辑配置文件，并由此引发技术问题，Edgenexus 技术支持部门将无法再为产品提供支持。

下载配置

- 要下载 ADC 的当前配置，请按下载配置按钮。
- 系统会弹出一个窗口，要求您打开或保存 .conf 文件。
- 保存到方便的位置。
- 您可以使用任何文本编辑器（如记事本++）打开它。

上传配置

- 您可以通过浏览已保存的 .conf 文件来上传已保存的配置文件。
- 点击 "上传配置或 Jetpack "按钮。
- ADC 将上传并应用配置，然后刷新浏览器。如果没有自动刷新浏览器，请点击刷新浏览器。
- 完成后，您将跳转到 "控制面板 "页面。

关键：在未咨询 Edgenexus 支持人员之前，请勿尝试将配置从一个 ADC 复制到另一个 ADC，这一点至关重要。这样做可能会导致 ADC 无法恢复。

上传 JetPACK

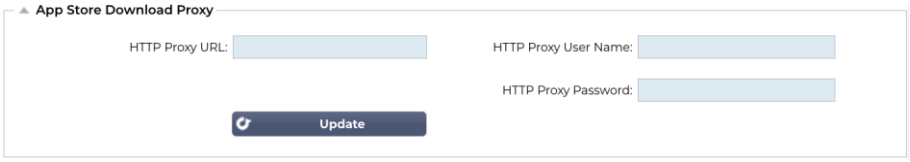
- JetPACK 是对现有配置的一组配置更新。
- 一个 JetPACK 可以小到更改 TCP 超时值，大到完整的特定应用程序配置，如 Microsoft Exchange 或 Microsoft Lync。
    - 您可以从本指南末尾所示的支持门户获取 JetPACK。
- 浏览 jetPACK.txt 文件。

- 点击上传。
- 上传后，浏览器将自动刷新。
- 完成后，您将跳转到 "控制面板 "页面。
- 对于 Microsoft Lync 等更复杂的部署，导入时间可能更长。

全局设置

全局设置部分允许您更改各种元素，包括 SSL 密码库。

应用程序商店下载代理



除非通过组织的代理服务器发送数据，否则安全网络通常不允许访问互联网。EdgeADC 是一个周边设备，需要能够访问 Edgenexus 服务器，以确定支持的有效性，并访问 App Store 下载更新和应用程序。

HTTP 代理 URL

此字段用于指定代理服务器的主机名或 IP 地址。

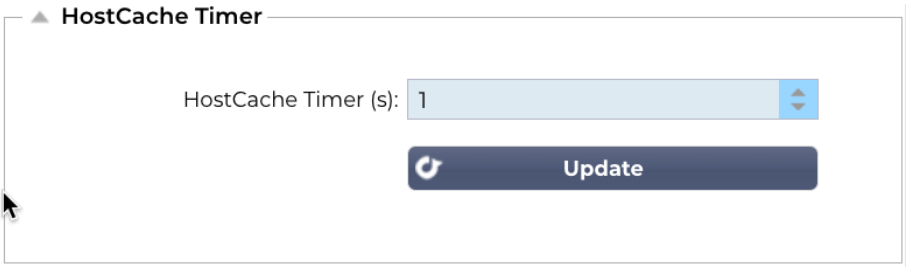
HTTP 代理用户名

输入专门用于授权使用代理服务器的设备和用户的用户名。

HTTP 代理密码

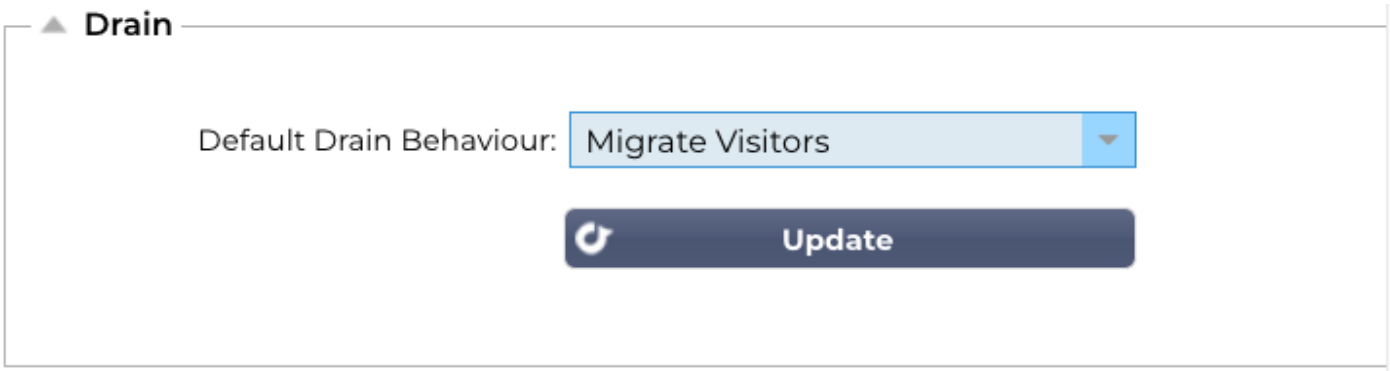
HTTP 代理用户名中指定的用户名将是安全的。您需要在此字段中输入相关密码。

主机高速缓存计时器



主机缓存定时器是一种设置，当使用域名而不是 IP 地址时，可在给定时间内存储真实服务器的 IP 地址。缓存会在真实服务器发生故障时被刷新。将此值设置为零将防止缓存被刷新。此设置没有最大值。

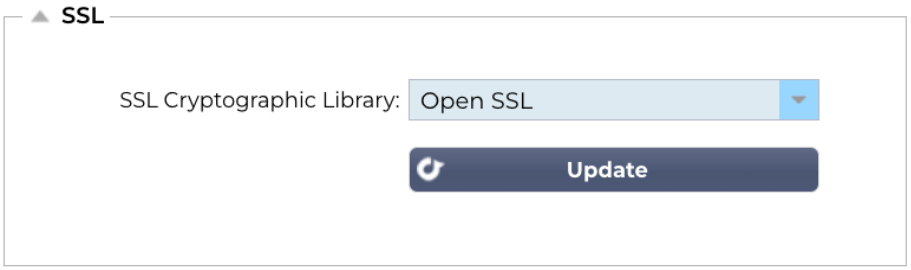
排水



无论何时将任何真实服务器置于耗尽模式，最好都能控制向其发送的流量行为。通过 "耗尽行为 "菜单，可以根据每个虚拟服务选择流量行为。选项包括

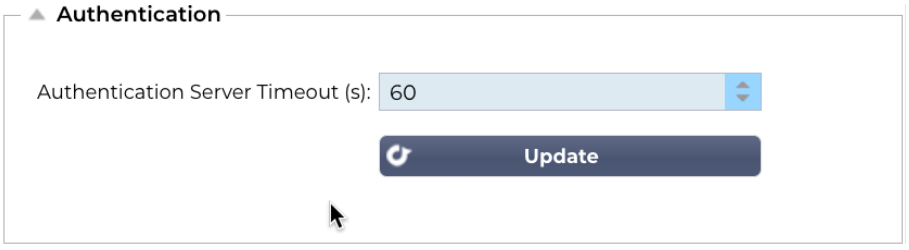
选项	说明
持久性驱动	这是默认选择。 每当用户使用持久会话访问时，该会话就会被扩展。 在 24 小时使用的情况下，有可能永远不会发生排水。 但是，如果连接到真实服务器的连接数达到 0，泄流就会结束，持久会话就会被删除，所有访问者都会在下一次连接时重新获得平衡。
迁移游客	重新连接时忽略持久会话 - （2022 年之前的传统行为） 新的 TCP 连接（无论是否属于现有会话的一部分）总是连接到在线的真实服务器。 如果持久化会话是指向正在耗尽的真实服务器，则会被覆盖。 虚拟服务将有效忽略任何新连接的持久性，并将这些连接负载平衡到新服务器。
退休会议	持续会话不会延长。 传入的用户连接将被分配到所需的服务器上，但其持续会话不会被延长。因此，在超过持续会话时间后，它们将被视为新连接并被转移到不同的服务器上。

SSL



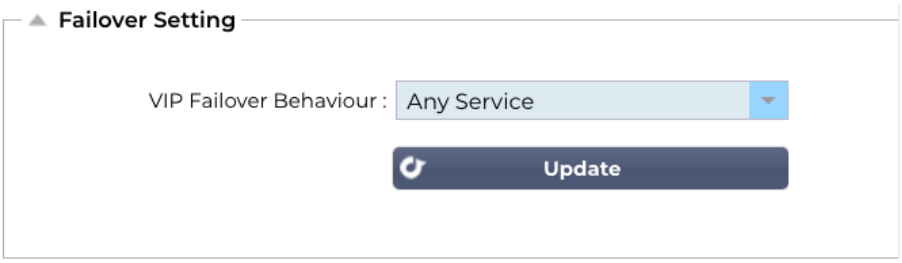
此全局设置允许根据需要更改 SSL 库。ADC 使用的默认 SSL 加密库来自 OpenSSL。如果想使用其他加密库，可以在此进行更改。

认证



该值用于设置身份验证的超时值，超时后身份验证尝试将被视为失败。

故障切换设置



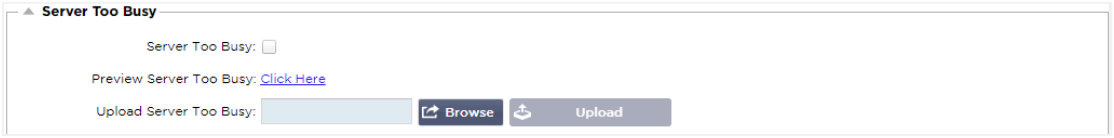
创建集群 ADC 时，现在有两种方法可以指定虚拟服务的故障转移方式。

选项	说明
任何服务	选择此选项时，VIP 中任何服务的故障都会导致整个 VIP 及其虚拟服务故障转移到群集合作伙伴。 例如，您可能有一个 VIP 10.0.100.101，其虚拟服务分别使用 443、8080、4399、2020 等端口。如果其中任何一个子服务发生故障，整个 VIP 都将发生故障。
所有服务	选择此选项后，如果一个或多个子服务发生故障，VIP 将保留在当前群集成员上。只有当**所有**服务**都**发生故障时，VIP 才会切换到群集伙伴。 当您希望禁用某个特定服务，但又不希望 VIP 故障切换时，这种方法非常有用。

规程

协议 "部分用于设置 HTTP 协议的许多高级设置。

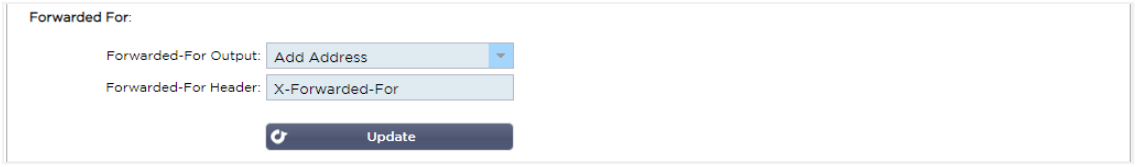
服务器太忙



假设您限制了真实服务器的最大连接数；您可以选择在达到此限制后显示友好的网页。

- 创建一个包含您的信息的简单网页。您可以将外部链接指向其他网络服务器和网站上的对象。另外，如果您想在网页上显示图片，可以使用内嵌的 base64 编码图片。
- 浏览新创建的网页 HTM(L) 文件。
- 点击上传
- 如果您想预览页面，可点击此处链接。

转发



Forwarded For 是通过第 7 层负载均衡器和代理服务器识别连接到网络服务器的客户端源 IP 地址的事实标准。

转发输出

选项	说明
关闭	ADC 不会更改 Forwarded-For 标头。
添加地址和端口	此选项会将连接到 ADC 的设备或客户端的 IP 地址和端口附加到 Forwarded-For 标头。
添加地址	此选项会将连接到 ADC 的设备或客户端的 IP 地址附加到 Forwarded-For 标头。
替换地址和端口	此选项将用连接到 ADC 的设备或客户端的 IP 地址和端口替换 Forwarded-For 标头的值。
更换地址	此选项将用连接到 ADC 的设备或客户端的 IP 地址替换 Forwarded-For 标头的值。

转发标题

该字段允许你指定 Forwarded-For 头信息的名称。通常是 "X-Forwarded-For"，但在某些环境下可能会更改。

IIS 高级日志记录 - 自定义日志记录

您可以通过安装 IIS 高级日志 64 位应用程序来获取 X-Forwarded-For 信息。下载后，按以下设置创建名为 X-Forwarded-For 的自定义日志字段。

从 "类别 "列表的 "源类型 "列表中选择 "默认"，在 "源名称 "框中选择 "请求标头"，然后键入 X-Forwarded-For。

HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging

更改 Apache HTTPd.conf

您需要对默认格式进行几处修改，以记录 X-Forwarded-For 客户端 IP 地址，如果不存在 X-Forwarded-For 标头，则记录实际的客户端 IP 地址。

这些变化如下：

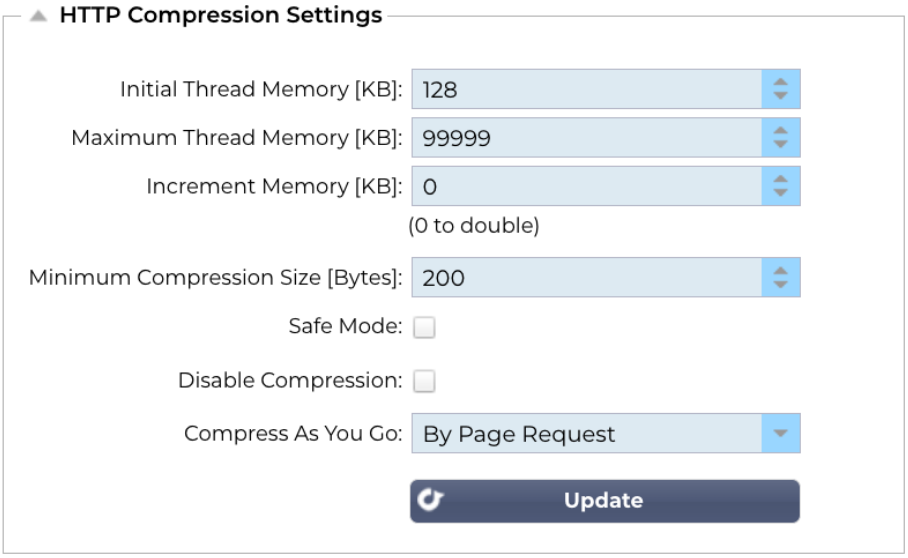
类型	价值
日志格式：	"%h %l %u %t （"%r/"） %>s %b （"%{Referer}i/"）\结合起来
日志格式：	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" %{User-Agent}i\" proxy SetEnvIf X- Forwarded-For "^.*\.*.\代理 SetEnvIf X- Forwarded-For "^.*\.*\.*" forwarded
自定义日志：	"logs/access_log "组合 env=!forwarded
自定义日志：	"logs/access_log "代理 env=forwarded

这种格式利用了 Apache 对基于环境变量的条件日志的内置支持。

- 第 1 行是默认的标准组合日志格式字符串。
- 第 2 行将 %h（远程主机）字段替换为从 X-Forwarded-For 标头提取的值，并将此日志文件模式的名称设置为 "proxy"。
- 第 3 行是对环境变量 "forwarded "的设置，其中包含一个与 IP 地址匹配的松散正则表达式，在本例中没有问题，因为我们更关心 X-Forwarded-For 头中是否存在 IP 地址。
- 另外，第 3 行可以理解为"如果有 X-Forwarded-For 值，请使用它"。
- 第 4 和第 5 行告诉 Apache 使用哪种日志模式。如果存在 X-Forwarded-For 值，则使用 "代理 "模式，否则对请求使用 "组合 "模式。为了便于阅读，第 4 行和第 5 行没有使用 Apache 的旋转日志（管道式）日志功能，但我们认为几乎每个人都会使用该功能。

这些更改将导致每次请求都记录一个 IP 地址。

HTTP 压缩设置



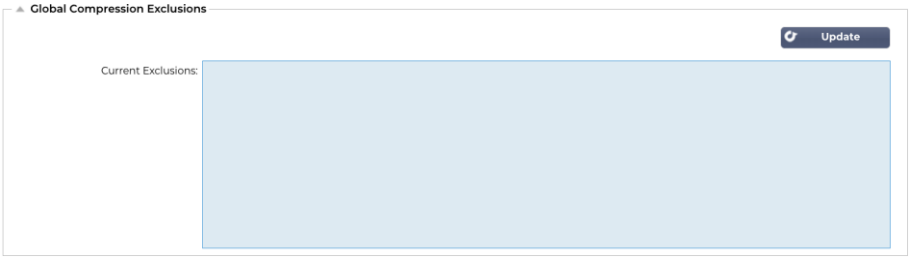
压缩是一种加速功能，可在 IP 服务页面上为每个服务启用。

警告 - 调整这些设置时要格外小心，因为不适当的设置会对 ADC 的性能产生不利影响。

选项	说明
初始线程内存 [KB]	该值是 ADC 收到的每个请求最初可能分配的内存量。为获得最高效的性能，该值应设置为刚刚超过网络服务器可能发送的最大未压缩 HTML 文件的值。
最大线程内存 [KB]	该值是 ADC 在一次请求中分配的最大内存量。为获得最佳性能，ADC 通常将所有内容存储并压缩在内存中。如果处理的内容文件特别大，超过了这个值，ADC 将把数据写入磁盘并压缩。
增量存储器 [KB]	该值用于设置在需要更多内存时添加到初始线程内存分配中的内存量。默认设置为零。这意味着当数据超过当前分配（如 128Kb、256Kb、512Kb 等）时，ADC 将加倍分配，直至达到 "每线程最大内存使用量 "设置的限制。当大部分页面大小一致，但偶尔会出现较大文件时，这种方法很有效。(例如，大部分页面大小为 128KB 或更小，但偶尔会有 1Mb 大小的响应）。在文件大小可变的情况下，设置一个较大大小的线性增量会更有效（例如，响应大小为 2Mb 至 10Mb，则初始设置为 1Mb，增量为 1Mb 会更有效）。
最小压缩大小 字节	该值是 ADC 不会尝试压缩的大小（以字节为单位）。这个值非常有用，因为小于 200 字节的文件都不会被很好地压缩，甚至会因为压缩头的开销而增大。
安全模式	勾选该选项可防止 ADC 对 JavaScript 的样式表进行压缩。这样做的原因是，尽管 ADC 知道哪些浏览器可以处理压缩内容，但其他一些代理服务器即使声称符合 HTTP/1.1 标准，也无法正确传输压缩样式表和 JavaScript。如果通过代理服务器传输样式表或 JavaScript 时出现问题，可使用此选项禁用这些类型的压缩。不过，这会减少内容的总体压缩量。
禁用压缩	勾选此项可阻止 ADC 压缩任何响应。

边走边压缩	ON - 在此页面使用 "边运行边压缩"。这会将从服务器接收到的每个数据块压缩成可完全解压缩的离散块。 OFF - 在此页面上不使用 "边运行边压缩"。 按页面请求 - 按页面请求使用 "边运行边压缩"。

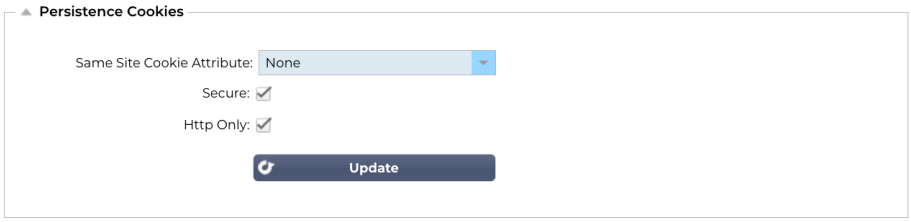
全球压缩排除



任何在排除列表中添加扩展名的页面都不会被压缩。

- 键入单个文件名。
- 点击更新。
- 如果要添加文件类型，只需输入 "*.css "即可排除所有层叠样式表。
- 每个文件或文件类型都应添加到新行中。

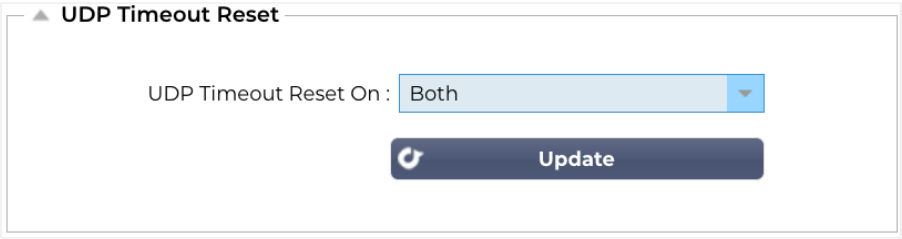
持久性 Cookie



此设置允许您指定如何处理 Persistence Cookie。

现场	说明
同一地点库克属性	**无**：脚本可访问所有 cookie **宽松**：防止跨网站访问 cookie，但如果访问拥有 cookie 的网站，则会将 cookie 存储为可访问的内容并提交给该网站 **严格**：防止访问或存储不同网站的任何 cookie **关**：返回浏览器默认行为
安全	选中该复选框后，持久性将应用于安全流量
仅 HTTP	选中后，仅允许在 HTTP 流量中使用持久 Cookes

UDP 超时重置



UDP 超时重置是网络通信中使用的一种机制，用于重启与 UDP（用户数据报协议）会话相关的超时。 重置有助于保持会话处于活动状态，确保数据流不间断。

选项	说明
两者	重置服务器和客户端的 UDP 超时。
服务器	重置服务器上的 UDP 超时。
客户	重置客户端的 UDP 超时。

软件

软件部分允许您更新 ADC 的配置和固件。

软件升级详情

如果您有正常的互联网连接，本部分的信息将被填入。如果您的浏览器没有互联网链接，本部分将为空白。连接成功后，您将收到下面的横幅信息。

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

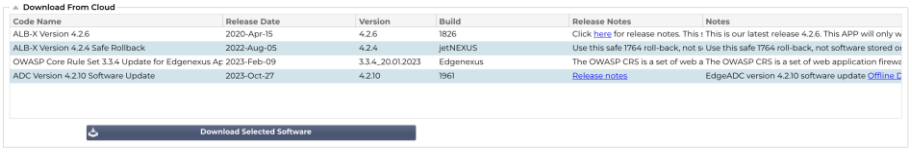
下图所示的 "从云下载 "部分将显示您的支持计划中可用的更新信息。请注意支持类型和支持到期日期。

注意：我们使用您浏览器的互联网连接来查看 Edgenexus 云的可用内容。只有当 ADC 具有互联网连接时，您才能下载软件更新。

检查一下

- 高级--故障排除--Ping
- IP 地址 - App Store.edgenexus.io
- 点击平移
- 如果结果显示 "ping：未知主机 App Store.edgenexus.io"。
- ADC 无法从云端下载任何内容

从云端下载



如果您的浏览器已连接到互联网，您将看到云中可用软件的详细信息。

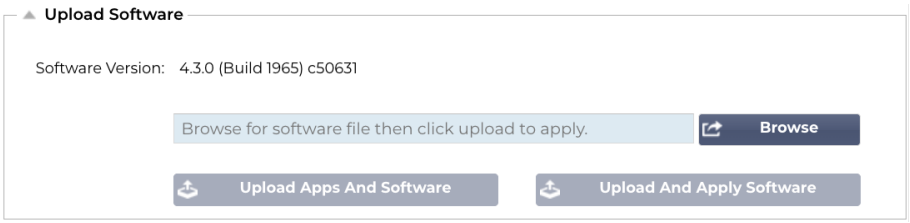
- 突出显示您感兴趣的行，然后单击 "将所选软件下载到 ALB "按钮。
- 点击后，所选软件将下载到您的 ALB 上，可在下面的 "应用存储在 ALB 上的软件 "部分进行应用。

注意： 如果 ADC 无法直接访问互联网，则会出现类似下面的错误：

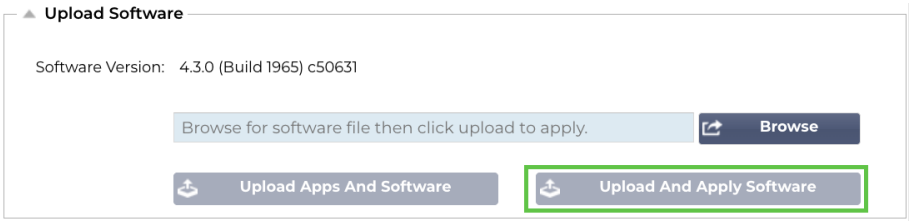
下载错误，ALB 无法访问 build1734-3236-v4.2.1-Sprint2-update-64.software.alb 文件的 ADC 云服务

如果您的网络受代理服务器保护，请参阅应用程序商店下载代理

上传软件



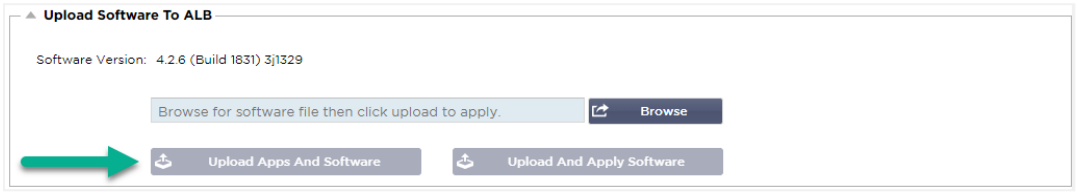
应用程序上传



如果您有以 <appname> .<apptype>.alb 结尾的应用程序文件，可以使用此方法上传。

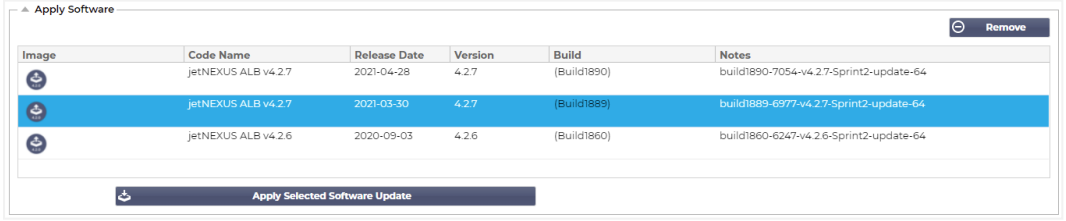
- 应用程序有五种类型
  - <appname>flightpath.alb
  - <appname>.monitor.alb
  - <appname>.jetpack.alb
  - <appname>.addons.alb
  - <appname>.featurepack.alb
- 上传后，每个应用程序都可以在 "库">"应用程序 "部分找到。
- 然后，您必须单独部署该部分中的每个应用程序。

软件 / 固件更新



- 如果您希望上传软件而不应用软件，请使用突出显示的按钮。
- 软件文件为 <softwarename>.software.alb。
- 然后，它将显示在 "ALB 上存储的软件 "部分，您可以在方便的时候应用它。

应用存储在 ADC 上的软件



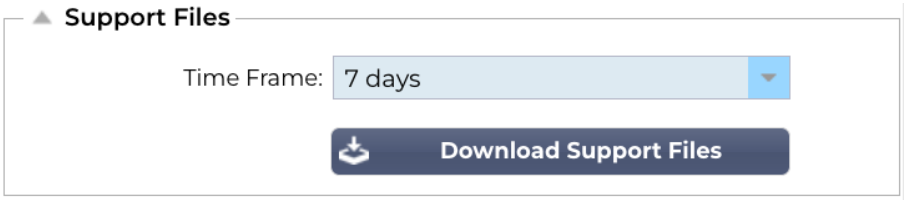
本节将显示 ALB 上存储的所有软件文件，这些文件可用于部署。列表将包括更新的 Web 应用程序防火墙 (WAF) 签名。

- 突出显示您有兴趣使用的软件行。
- 点击 "从所选软件中应用软件"。
- 如果是 ALB 软件更新，请注意上传后需要重启 ALB 才能应用。
- 如果您应用的更新是 OWASP 签名更新，则无需重启即可自动应用。

故障排除

总有一些问题需要排除故障，找出根本原因和解决方案。本节将为您提供这方面的帮助。

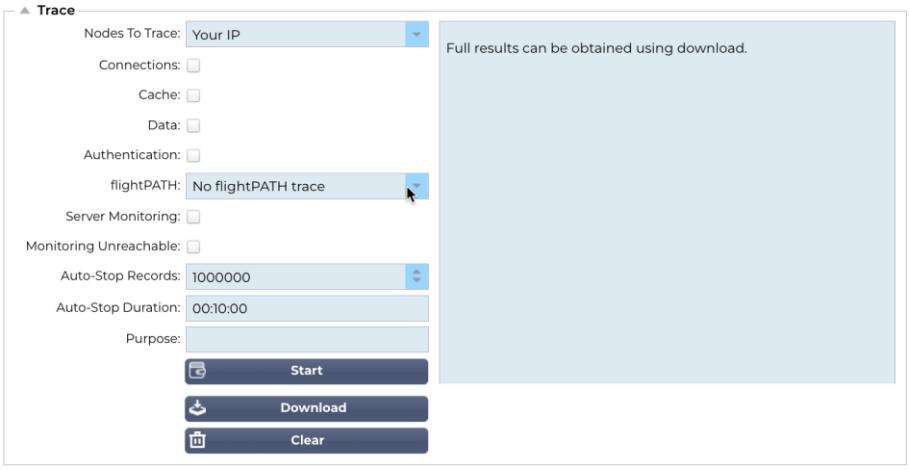
支持文件



如果您遇到 ADC 问题并需要开支持单，技术支持人员通常会要求 ADC 设备提供几个不同的文件。这些文件现已合并为一个 .dat 文件，可通过本节下载。

- 从下拉菜单中选择一个时间段：您可以选择 3 天、7 天、14 天或所有天数。
- 点击 "下载支持文件
- 下载的文件格式为 Support-jetNEXUS-yyymmddhh-NAME.dat
- 在支持门户网站上提出支持请求，详情请见本文件末尾。
- 确保您详细描述了问题，并将 .dat 文件附件到票据中。

跟踪



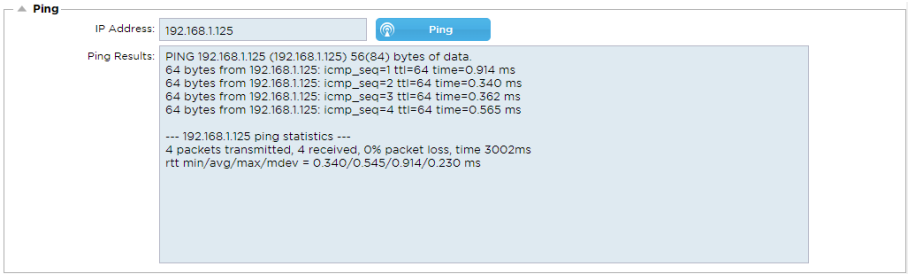
跟踪 "部分允许您检查信息，以便调试问题。所提供的信息取决于您从下拉菜单和复选框中选择的选项。

选项	说明
要跟踪的节点	**您的 IP**：这将过滤输出，使用您访问图形用户界面时使用的 IP 地址（注意，不要为 "监控 "选择此选项，因为 "监控 "将使用 ADC 接口地址） **所有 IP**： 不应用过滤。需要注意的是，在繁忙状态下，这将对性能产生不利影响。
连接	选中该复选框后，将显示有关客户端和服务器端连接的信息。

缓存	选中该复选框将显示有关缓存对象的信息。
数据	选中该复选框时，将包括 ADC 处理的进出原始数据字节。
飞行路径	通过 flightPATH 菜单，您可以选择要监控的特定 flightPATH 规则或所有 flightPATH 规则。
服务器监控	选中该复选框后，将显示 ADC 上激活的服务器健康监控器及其各自的结果。
监控无法连接	选择该选项后，其行为与服务器监控非常相似，但它只会显示失败的监控，因此只起到过滤这些信息的作用。
自动停止记录	默认值为 1,000,000 条记录，之后跟踪功能将自动停止。该设置是一种安全防范措施，可防止意外开启跟踪功能并影响 ADC 性能。
自动停止持续时间	默认时间设置为 10 分钟，之后跟踪功能将自动停止。该功能是一项安全防范措施，可防止跟踪功能意外开启而影响 ADC 性能。
开始	单击此项手动启动跟踪设备。
停止	单击可在达到自动记录或时间之前手动停止跟踪设施。
下载	虽然您可以在右侧看到实时查看器，但信息显示可能太快。相反，您可以下载 Trace.log 查看当天在各种跟踪过程中收集到的所有信息。该功能是跟踪信息的过滤列表。如果您想查看前几天的跟踪信息，可以下载当天的 Syslog，但必须手动过滤。
清晰	清除跟踪日志

平

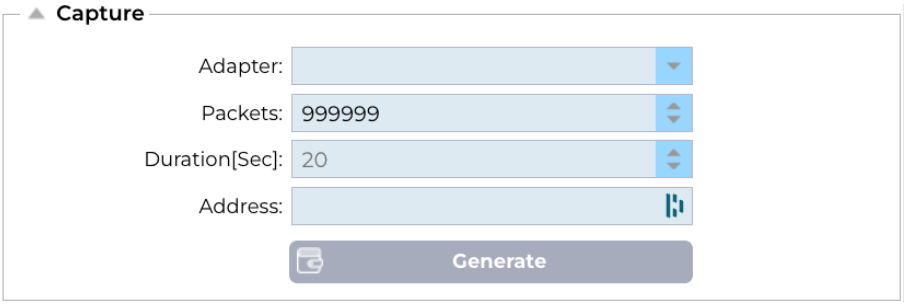
您可以使用 Ping 工具检查基础设施中服务器和其他网络对象的网络连接情况。



键入要测试的主机 IP 地址，例如使用点分十进制符号的默认网关或 IPv6 地址。按下 "Ping "按钮后，可能需要等待几秒钟才能反馈结果。

如果已配置 DNS 服务器，则可键入完全合格的域名。您可以在 **DNS 服务器 1 和 DNS 服务器 2** 部分配置 DNS 服务器。按下 "Ping "按钮后，可能需要等待几秒钟才能反馈结果。

捕获



要捕捉网络流量，请按照下面的简单说明操作。

- 填写表格中的选项
- 单击生成
- 捕获运行后，浏览器会弹出并询问您希望将文件保存在哪里。文件格式为 "jetNEXUS.cap.gz"。
- 在支持门户网站上提出支持请求，详情请见本文件末尾。
- 请确保您详细描述了问题，并将文件附在工作单上。
- 您还可以使用 Wireshark 查看内容

选项	说明
适配器	从下拉菜单中选择适配器，通常是 eth0 或 eth1。您也可以使用 "any "捕获所有接口。
数据包	此值为捕获数据包的最大数量。通常为 99999
持续时间	选择抓取运行的最长时间。对于高流量网站，一般为 15 秒。捕获期间将无法访问图形用户界面
地址	此值将过滤框中输入的任何 IP 地址。留空表示不过滤。

为了保证性能，我们将下载文件限制在 10MB。如果您发现这不足以捕获所需的全部数据，我们可以增加这一数字。

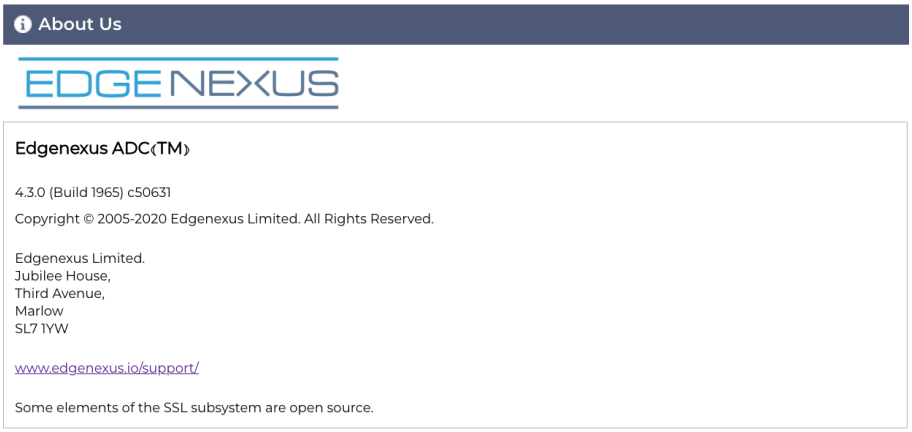
注意：这会影响实时网站的性能。要增加可用捕获大小，请使用全局设置 jetPACK 来增加捕获大小。

帮助

通过 "帮助 "版块，您可以访问有关 Edgenexus 的信息、用户指南和其他有用信息。

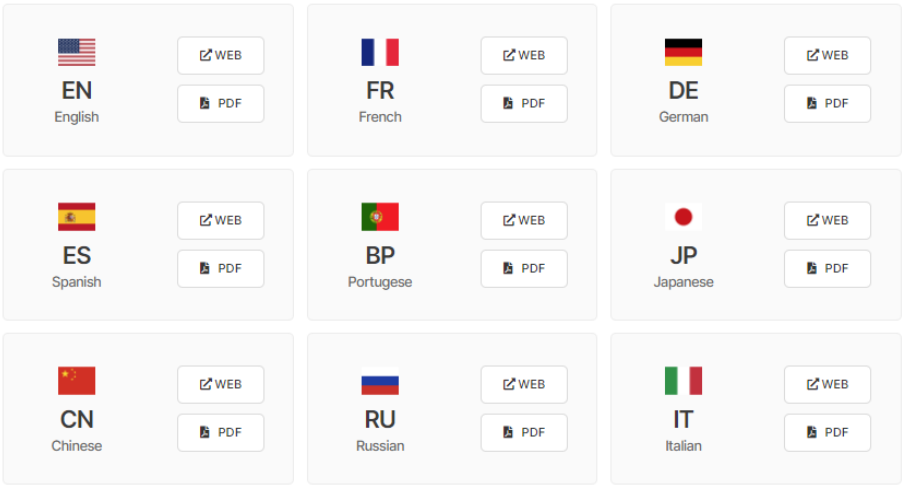
关于我们

点击 "关于我们 "选项将显示有关 Edgenexus 及其公司办公室的信息。



参考资料

参考选项将打开包含用户指南和其他有用文件的网页。也可以使用 https://www.edgenexus.io/documentation 查找该网页。



如果没有找到所需的信息，请联系 。support@edgenexus.io

JetPacks

Edgenexus jetPACK s

jetPACK 是一种针对特定应用即时配置 ADC 的独特方法。这些易于使用的模板经过预配置和全面调整，包含所有特定应用设置，您可以从 ADC 享受优化的服务交付。某些 jetPACK 使用 flightPATH 来处理流量，您必须获得 flightPATH 许可证才能使用该元素。要了解您是否拥有 flightPATH 许可证，请参阅**许可证**页面。

下载 jetPACK

- 下面创建的每个 jetPACK 都有一个唯一的虚拟 IP 地址，该地址包含在 jetPACK 的标题中。例如，下面第一个 jetPACK 的虚拟 IP 地址为 1.1.1.1
- 您可以按原样上传 jetPACK 并在图形用户界面中更改 IP 地址，也可以使用 Notepad++ 等文本编辑器编辑 jetPACK，然后搜索并用虚拟 IP 地址替换 1.1.1.1。
- 此外，每个 jetPACK 还创建了 2 个真实服务器，其 IP 地址分别为 127.1.1.1 和 127.2.2.2。您也可以在上传后或使用记事本++事先在图形用户界面中更改这些地址。
- 点击下面的 jetPACK 链接，并将链接保存为 jetPACK-VIP-Application.txt 文件，放在您选择的位置上

微软 Exchange

应用	下载链接	它有什么作用？	包括哪些内容？
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	该 jetPACK 将为 Microsoft Exchange 2010 负载平衡添加基本设置。其中包含一个 flightPATH 规则，用于将 HTTP 服务上的流量重定向到 HTTPS，但这只是一个选项。如果您没有 flightPATH 许可证，此 jetPACK 仍可使用。	全局设置：服务超时 2 小时 监控器用于 Outlook 网络应用程序的第 7 层监控器，以及用于客户端访问服务的第 4 层带外监控器 虚拟服务 IP： 1.1.1.1 虚拟服务端口：80, 443, 135, 59534, 59535 真实服务器：127.1.1.1 127.2.2.2 flightPATH：添加从 HTTP 到 HTTPS 的重定向
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	同上，但会在反向代理连接中的 25 端口添加 SMTP 服务。SMTP 服务器会将 ALB-X 接口地址视为源 IP。	全局设置：服务超时 2 小时 监控器：用于 Outlook 网络应用程序的第 7 层监控器。客户端访问服务的第 4 层带外监控器 虚拟服务 IP： 1.1.1.1 虚拟服务端口：80、443、135、59534、59535、25（反向代理） 真实服务器：127.1.1.1 127.2.2.2 flightPATH：添加从 HTTP 到 HTTPS 的重定向
	jetPACK-1.1.1.3-Exchange-	与上述相同，但该 jetPACK 将配置 SMTP 服务使用直接服务器返回连接。如果 SMTP	全局设置：服务超时 2 小时

	2010-SMTP-DSR	服务器需要查看客户端的实际 IP 地址，则需要使用此 jetPACK。	监控器：用于 Outlook 网络应用程序的第 7 层监控器。客户端访问服务的第 4 层带外监控器 虚拟服务 IP： 1.1.1.1 虚拟服务端口：80、443、135、59534、59535、25（直接返回服务器） 真实服务器：127.1.1.1 127.2.2.2 flightPATH：添加从 HTTP 到 HTTPs 的重定向
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	此设置为 HTTP 和 HTTPS 流量增加了一个 VIP 和两个服务，所需的 CPU 资源最少。可以为 VIP 添加多个健康检查，以检查每个服务是否正常运行。	全局设置： 监控器针对 OWA、EWS、OA、EAS、ECP、OAB 和 ADS 的第 7 层监控器 虚拟服务 IP： 2.2.2.1 虚拟服务端口：80, 443 真实服务器：127.1.1.1 127.2.2.2 flightPATH：添加从 HTTP 到 HTTPS 的重定向
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	这种设置为每个服务使用一个唯一的 IP 地址，因此比上述设置使用更多的资源。您必须将每个服务配置为单独的 DNS 条目 例 owa.edgenexus.com、ews.edgenexus.com 等。将为每个服务添加监控程序，并将其应用于相关服务	全局设置： 监控器针对 OWA、EWS、OA、EAS、ECP、OAB、ADS、MAPI 和 PowerShell 的第 7 层监控器 虚拟服务 IP： 2.2.3.1、2.2.3.2、2.2.3.3、2.2.3.4、2.2.3.5、2.2.3.6、2.2.3.7、2.2.3.8、2.2.3.9、2.2.3.10 虚拟服务端口：80, 443 真实服务器：127.1.1.1 127.2.2.2 flightPATH：添加从 HTTP 到 HTTPs 的重定向
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	该 jetPACK 将在不同端口上添加一个唯一 IP 地址和多个虚拟服务。 然后，flightPATH 将根据目的地路径进行上下文切换，以选择正确的虚拟服务。此 jetPACK 需要最多的 CPU 来执行上下文切换	全局设置： 监控器针对 OWA、EWS、OA、EAS、ECP、OAB、ADS、MAPI 和 PowerShell 的第 7 层监控器 虚拟服务 IP： 2.2.2.3 虚拟服务端口：80, 443, 1, 2, 3, 4, 5, 6, 7 真实服务器：127.1.1.1 127.2.2.2 flightPATH：添加从 HTTP 到 HTTPS 的重定向

Microsoft Lync 2010/2013

反向代理	前端	边缘内部	边缘外部

jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -End	jetPACK-3.3.3.3-Lync-Edge-Internal	jetPACK-3.3.3.4-Lync-Edge-External

网络服务

正常 HTTP	SSL 卸载	SSL 重新加密	SSL 直通
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Web-SSL 卸载	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL 穿透

微软远程桌面

正常
jetPACK-5.5.5.1-Remote-Desktop

DICOM - 医学数字成像和通信

正常 HTTP
jetPACK-6.6.6.1-DICOM

Oracle 电子商务套件

SSL 卸载	
jetPACK-7.7.7..1-Oracle-EBS	

VMware Horizon View

连接服务器 - SSL 卸载	安全服务器 - SSL 重新加密
jetPACK-8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-encryption

全局设置

- GUI 安全端口 443 - 该 jetPACK 将把 GUI 安全端口从 27376 更改为 443。HTTPs://x.x.x.x
- 图形用户界面超时 1 天 - 图形用户界面每隔 20 分钟会要求您输入密码。此设置将把请求时间延长至 1 天
- ARP 刷新 10 - 在 HA 设备之间进行故障切换时，此设置将增加**免费 ARP 的**数量，以便在切换过程中为交换机提供帮助
- 捕获大小 16MB - 默认捕获大小为 2MB。此值将把大小增加到最大 16MB

Cipher s 和 Cipher jetPACKs

EdgeADC 将最佳实践密码作为标准配置。 这些密码与各自的 TLS 协议相结合，使用户使用起来更加方便。

如果您需要，我们还提供了一套附加密码供您使用。

强密码

增加了从密码选项列表中选择 "强密码 "的功能：

```
ALL：RC4+RSA：+RC4：+HIGH：！DES-CBC3-SHA：！SSLv2：！ADH：！EXP：！ADHexport：！MD5
```

反野兽

增加了从密码选项列表中选择 "反野兽 "的功能：

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
```

无 SSLv3

增加了从密码选项列表中选择 "无 SSLv3 "的功能：

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

无 SSLv3 无 TLSv1 无 RC4

增加了从密码选项列表中选择 "No-TLSv1 No-SSLv3 No-RC4 "的功能：

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

NO_TLSv1.1

增加了从密码选项列表中选择 "NO_TLSv1.1 "的功能：

```
ECDH+AESGCM：DH+AESGCM：ECDH+AES256：DH+AES256：ECDH+AES128：DH+AES：RSA+AESGCM：RSA+AES：HIGH：！3DES：！aNULL：！MD5：！DSS：！MD5：！aNULL：！EDH：！RC4
```

启用 TLS-1.0-1.1 密码

从版本 4.2.10 开始，TLS1.0 和 TLS 1.1 协议的密码支持已被弃用。不过，一些客户仍在其内部服务器中使用这些旧的传统协议。以下密码添加了启用 TLS v1.0 和 TLS v1.1 的功能。

```
aes128-sha:aes256-sha:des-cbc-sha:des-cbc3-sha:exp-des-cbc-sha:rc4-sha:rc4-md5:dhe-rsa-aes128-sha:dhe-rsa-aes256-sha：EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

密码 jetPACK 示例

密码通过 jetPACK 导入 ADC。jetPACK 是一个简单的文本文件，其中包含 ADC 可以识别的参数。下面的示例显示了使用启用 TLS-1.0-1.1 密码的 jetPACK。

```
#更新

[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]

Cipher="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA：EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"。

Cipher1=""

Cipher2=""
```

```
CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"
Description=" 已启用 TLS v1.0 - v1.1"
```

- X-Content-Type-Options - 如果不存在，请添加此标头，并将其设置为 "nosniff"--防止浏览器自动进行 "MIME-嗅探"。
- X-Frame-Options - 如果不存在，请添加此标题，并将其设置为 "SAMEORIGIN" - 网站上的页面可以包含在框架中，但只能包含在同一网站的其他页面上。
- X-XSS-Protection - 如果不存在，请添加此标头，并将其设置为 "1; mode=block" - 启用浏览器跨站脚本保护功能
- Strict-Transport-Security - 如果不存在，则添加标头，并将其设置为 "max-age=31536000 ; includeSubdomains"--确保客户端遵守所有链接在最大年龄内都应为 HTTPs:// 的规定

应用 jetPACK

您可以以任何顺序应用任何 jetPACK，但要注意不要使用具有相同虚拟 IP 地址的 jetPACK。此操作将导致配置中出现重复的 IP 地址。如果您不小心这样做了，可以在图形用户界面中进行更改。

- 导航至高级 > 更新软件
- 配置部分
- 上传新配置或 jetPACK
- 浏览 jetPACK
- 点击上传
- 浏览器屏幕变白后，请单击 "刷新"，等待 "控制面板 "页面出现。

创建 jetPACK

jetPACK 的一大优点是您可以创建自己的配置。您可能已经为某个应用程序创建了完美的配置，并希望将其独立用于其他几个盒子。

- 首先从现有的 ALB-X 中复制当前配置。
    - 高级
    - 更新软件
    - 下载当前配置
- 用记事本++编辑此文件
- 打开一个新的 txt 文档，将其命名为 "yourname-jetPACK1.txt"。
- 将配置文件中的所有相关部分复制到 "yourname-jetPACK1.txt "中
- 完成后保存

重要： 每个 jetPACK 都分为不同的部分，但所有 jetPACK 的页面顶部都必须有 #!jetpack 字样。

建议编辑/复制的部分如下。

第 0 节：

```
#!jetpack
```

这一行必须位于 jetPACK 的顶部，否则当前配置将被覆盖。

第 1 节：

```
[jetnexusdaemon]
```

本部分包含全局设置，一旦更改，将适用于所有服务。其中一些设置可以通过网络控制台更改，但其他设置只能在这里更改。

例如

```
ConnectionTimeout=600000
```

本例中的 TCP 超时值单位为毫秒。该设置意味着 TCP 连接在 10 分钟未活动后将被关闭

```
ContentServerCustomTimer=20000
```

该示例是以毫秒为单位的内容服务器健康检查之间的延迟，用于 DICOM 等自定义监视器

```
jnCookieHeader="MS-WSMAN"
```

此示例将把持久负载平衡中使用的 cookie 标头名称从默认的 "jnAccel "更改为 "MS-WSMAN"。Lync 2010/2013 反向代理需要这一特殊更改。

第 2 节

```
[jetnexusdaemon-Csm-规则]
```

本节包含自定义服务器监控规则，这些规则通常从此处的网络控制台进行配置。

例如

```
[jetnexusdaemon-Csm-Rules-0]（jetnexusdaemon-Csm-Rules-0）。
Content="服务器启动"
Desc="显示器 1
Method="CheckResponse"
Name="健康检查 - 服务器是否正常运行"
Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

第 3 节

```
[jetnexusdaemon-本地接口]
```

本节包含 IP 服务部分的所有详细信息。每个接口都有编号，并包括每个通道的子接口。如果您的通道应用了 flightPATH 规则，那么它也将包含一个 "路径 "部分。

例如

```
[jetnexusdaemon-本地接口1]
1.1="443″
1.2="104″
```

```
1.3="80″
1.4="81″
已启用=1
Netmask=”255.255.255.0″
PrimaryV2=”{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}”
[jetnexusdaemon-本地接口1.1]
1=">,""安全组"",2000,"
2="192.168.101.11:80,Y,""IIS WWW 服务器 1"""
3="192.168.101.12:80,Y,""IIS WWW 服务器 2"""
地址分辨率=0
缓存端口=0
CertificateName="default"
ClientCertificateName="No SSL"
压缩=1
连接限制=0
DSR=0
DSRProto="tcp"
已启用=1
负载平衡策略="基于 CookieBased"
最大连接数=10000
监控策略="1″
PassThrough=0
协议="加速 HTTP"
ServiceDesc="安全服务器 VIP"
SNAT=0
SSL=1
SSLClient=0
SSLInternalPort=27400
[jetnexusdaemon-LocalInterface1.1-Path]。
1="6″
第 4 节：
[jetnexusdaemon-路径]
```

本节包含所有 flightPATH 规则。数字必须与应用到接口的规则一致。在上面的示例中，我们看到 flightPATH 规则 "6 "已应用于通道，下面以它为例。

例如

```
[jetnexusdaemon-Path-6]。
Desc="强制某些目录使用 HTTPS"
```

Name="Gary - 强制 HTTPS"

[jetnexusdaemon-Path-6-Condition-1]。

检查="包含"

条件="路径"

匹配=

Sense="does"

Value="/secure/"

[jetnexusdaemon-Path-6-Evaluate-1]。

详细信息=

Source="host"

值=

变量="$host$"[jetnexusdaemon-Path-6-Function-1]。

Action="redirect"

Target="HTTPs://$host$$path$$querystring$"

值=

飞行路径

flightPATH 简介

什么是 flightPATH?

flightPATH 是 Edgenexus 开发的智能规则引擎，用于处理和路由 HTTP 和 HTTPS 流量。它具有高度可配置性，功能非常强大，而且非常易于使用。

虽然 flightPATH 的某些组件是 IP 对象（如源 IP），但 flightPATH 只能应用于等于 HTTP(s) 的第 7 层服务类型。如果选择任何其他服务类型，IP 服务中的 flightPATH 选项卡将是空白。

flightPATH 能做什么?

flightPATH 可用于修改传入和传出 HTTP(s) 内容和请求。

除了使用简单的字符串匹配（如 "开始于 "和 "结束于"）外，还可以使用强大的 Perl 兼容正则表达式（RegEx）进行完全控制。

有关 RegEx 的更多信息，请参阅此有用网站 。

此外，还可以在 "评估 "部分创建自定义变量，并将其用于 "操作 "区域，从而实现多种不同的可能性。

flightPATH 规则由三个部分组成：

选项	说明
详细信息	用于添加或删除 flightPATH，并列出可用的 flightPATH
条件	设置多个标准以触发 flightPATH 规则。
评估	允许使用可在操作区使用的变量。
行动	规则触发后的行为。

条件

在本节中，您可以指定适用于 "条件 "的五个参数。以下是每个选项的说明和示例。

条件	说明	示例
<form	HTML 表单用于向服务器传递数据	示例 "表单长度不为 0"
GEO 位置	将源 IP 地址与 ISO 3166 国家代码进行比较	地理位置等于 GB 或地理位置等于德国
主持人	这是从 URL 中提取的主机信息	www.mywebsite.com 或 192.168.1.1
语言	这是从语言 HTTP 头信息中提取的语言信息	该条件将产生一个下拉菜单，显示语言列表
方法	这是 HTTP 方法的下拉列表	这是一个下拉菜单，包括 GET、POST 等

原产地 IP	如果上游代理支持 X-Forwarded-for (XFF)，它将使用真正的原点地址	客户端 IP。也可使用多个 IP 或子网。 10\.1\.2\.* 是 10.1.2.0 /24 子网 10\.1\.2\.3|10\.1\.2\.4 使用 | 表示多个 IP
路径	这是网站的路径	/mywebsite/index.asp
职位	POST 请求方法	检查上传至网站的数据
查询	这是查询的名称和值，因此它既可以接受查询名称，也可以接受查询值。	"Best=edgeNEXUS"，其中匹配项为 Best，值为 edgeNEXUS
查询字符串	字符后的整个查询字符串	
申请 Cookie	这是客户请求的 cookie 的名称	MS-WSMAN=afYfn1CDqqCDqUD: :
请求标题	这可以是任何 HTTP 标头	推荐人、用户代理、发件人、日期
申请版本	这是 HTTP 版本	http/1.0 或 http/1.1
响应机构	用户在回复正文中定义的字符串	服务器升级
响应代码	响应的 HTTP 代码	200 确定，304 未修改
响应曲奇	这是服务器发送的 cookie 的名称	MS-WSMAN=afYfn1CDqqCDqUD: :
响应标头	这可以是任何 HTTP 标头	推荐人、用户代理、发件人、日期
响应版本	服务器发送的 HTTP 版本	http/1.0 或 http/1.1
来源 IP	这可以是源 IP、代理服务器 IP 或其他聚合 IP 地址	客户端 IP、代理 IP、防火墙 IP。还可以使用多个 IP 和子网。您必须 必须转义点，因为这些点是 RegEX。例如 10\.1\.2\.3 是 10.1.2.3

比赛

根据条件参数的值，匹配参数对上下文敏感。

比赛	说明	示例
接受	可接受的内容类型	接受: text/plain
接受编码	可接受的编码	接受-编码: <compress | gzip | deflate | sdch | identity>
接受语言	可接受的答复语言	接受语言: en-US
接受范围	该服务器支持哪些部分内容范围类型	接受范围：字节
授权	用于 HTTP 验证的验证凭据	授权：Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
收费	包含所申请方法应用成本的账目信息	

内容编码	数据使用的编码类型。	Content-Encoding: gzip
内容长度	以八位字节（8 位字节）为单位的响应正文长度	内容长度： 348
内容类型	请求正文的 MIME 类型（用于 POST 和 PUT 请求）	Content-Type: 应用程序/x-www-form-urlencoded
饼干	服务器先前通过 Set-Cookie 发送的 HTTP cookie（如下所示）	Cookie: $Version=1; Skin=new ；
日期	发出信息的日期和时间	日期 = "日期" ":" HTTP-date
ETag	资源特定版本的标识符，通常是信息摘要	ETag："aed6bdb8e090cd1:0"
来自	提出申请的用户的电子邮件地址	发件人：user@example.com
如果-修改-自	如果内容未变，允许返回 304 Not Modified（未修改	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
最后修改	请求对象的最后修改日期（RFC 2822 格式	Last-Modified：Tue, 15 Nov 1994 12:45:26 GMT
Pragma	特定于实现的标头可能会在请求-响应链的任何地方产生各种影响。	Pragma: no-cache
推荐人	这是上一个网页的地址，从该网页链接到当前请求的网页	Referrer: HTTP://www.edgenexus.io
服务器	服务器名称	服务器：Apache/2.4.1 (Unix)
设置	HTTP cookie	Set-Cookie：UserID=JohnDoe; Max-Age=3600; Version=1
用户代理	用户代理的用户代理字符串	用户代理：Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
不同	告诉下游代理如何匹配未来的请求标头，以决定是否可以使用缓存的响应，而不是从源服务器请求新的响应。 响应	可变：User-Agent
X-Powered-By	指定支持网络应用程序的技术（如 ASP.NET、PHP、JBoss）。	X-Powered-By：PHP/5.4.0

检查

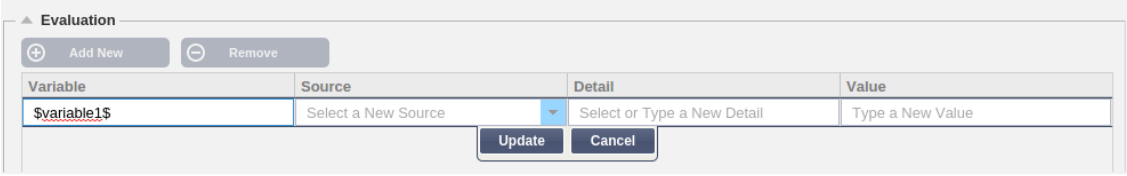
检查	**说明**	**示例**
存在	这并不关心条件的细节，只关心它是否存在。	主机> 是否> 存在
开始	字符串以值开头	路径 > > 是否开始 /secure>
结束	字符串以 "值 "结尾	路径 > > 是否结束> .jpg
包含	字符串确实包含值	请求头> 接受 > > 是否包含> 图片

平等	字符串确实等于值	主机 > > 是否等于> www.edgenexus.io
有长度	字符串确实有长度值	主机 > > 是否有长度> 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
超出长度	检查数值是否超过指定长度。	路径 > 是否 > 超过长度 - 10
匹配 RegEx	这样就可以输入一个完整的 Perl 兼容正则表达式	Origin IP> Does> Match Regex> 10\..* | 11\..*
比赛列表	允许提供一个以 PIPE (|) 为分隔符的数值列表，供您对照检查。	源 IP > 是否 > 匹配列表 > 10.0.0.1 | 10.0.0.100 | 192.178.28.32

示例

- 该示例有两个条件，必须**同时**满足这**两个**条件才能执行操作
- 首先是检查请求的对象是否是图像
- 第二种是检查特定主机名

评估



添加变量是一项引人注目的功能，可让您从请求中提取数据并在操作中加以利用。例如，如果出现安全问题，您可以记录用户用户名或发送电子邮件。

- 变量：必须以 $ 符号开头和结尾。例如 $variable1$
- 来源：从下拉框中选择变量来源
- 详细信息：从列表中选择相关内容。如果 Source=Request Header（请求头），则详细信息可以是 User-Agent
- 值：输入文本或正则表达式，对变量进行微调。

内置变量

- 内置变量已被硬编码，因此无需为其创建评估条目。
- 您可以在操作中使用下列任何变量
- 上表中的 "条件 "对每个变量进行了解释
    - 方法 = $method$
    - 路径 = $path$

- 查询字符串 = $querystring$
- 源 IP = $sourceip$
- 响应代码（文本还包括 "200 OK"）= $resp$
- 主机 = $host$
- 版本 = $version$
- 客户端口 = $clientport$
- 客户 = $clientip$
- 地理位置 = $geolocation$"

行动范例:

- 操作 = 重定向 302
  - 目标 = HTTPs://$host$/404.html
- 操作 = 日志
  - 目标 = 来自 $sourceip$:$sourceport$ 的客户端刚刚请求 $path$ 页面

解释:

- 客户访问不存在的页面时，浏览器通常会显示 404 页面
- 在这种情况下，用户会被重定向到他们使用的原始主机名，但错误的路径会被替换为 404.html
- 在系统日志中添加了一条记录："来自 154.3.22.14:3454 的客户端刚刚请求访问 wrong.html 页面"。

资料来源	说明	示例
饼干	这是 cookie 标头的名称和值	MS-WSMAN=afYfn1CDqqCDqUD:::其中名称为 MS-WSMAN，值为 afYfn1CDqqCDqUD: :
主持人	这是从 URL 中提取的主机名	www.mywebsite.com 或 192.168.1.1
语言	这是从语言 HTTP 标头中提取的语言	该条件将产生一个包含语言列表的下拉列表。
方法	这是 HTTP 方法的下拉列表	下拉菜单将包括 GET、POST
路径	这是网站的路径	/mywebsite/index.html
职位	POST 请求方法	检查上传至网站的数据
查询项目	这是查询的名称和值。因此，它既可以接受查询名，也可以接受查询值。	"Best=jetNEXUS"，其中匹配项为 Best，值为 edgeNEXUS
查询字符串	这是在"..... "字符之后的整个字符串	HTTP://server/path/program?query_string
请求标题	可以是客户端发送的任何标头	Referrer、User-Agent、From、Date...
响应标头	可以是服务器发送的任何标头	Referrer、User-Agent、From、Date...
版本	这是 HTTP 版本	HTTP/1.0 或 HTTP/1.1

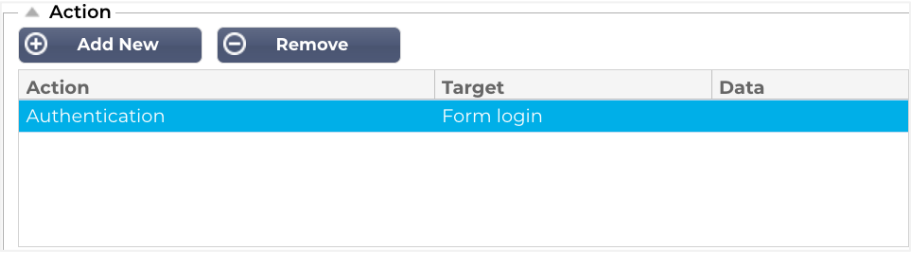
详细信息	说明	示例

接受	可接受的内容类型	接受: text/plain
接受编码	可接受的编码	接受-编码: <compress | gzip | deflate | sdch | identity>
接受语言	可接受的答复语言	接受语言: en-US
接受范围	该服务器支持哪些部分内容范围类型	接受范围：字节
授权	用于 HTTP 验证的验证凭据	授权：Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
收费	包含所申请方法应用成本的账目信息	
内容编码	数据使用的编码类型。	Content-Encoding: gzip
内容长度	以八位字节（8 位字节）为单位的响应正文长度	内容长度： 348
内容类型	请求正文的 MIME 类型（用于 POST 和 PUT 请求）	Content-Type: 应用程序/x-www-form-urlencoded
饼干	服务器先前通过 Set-Cookie 发送的 HTTP cookie（如下所示）	Cookie: $Version=1; Skin=new；
日期	发信日期和时间 发出信息的日期和时间	日期 = "日期" ":" HTTP-date
ETag	资源特定版本的标识符，通常是信息摘要	ETag："aed6bdb8e090cd1:0"
来自	提出申请的用户的电子邮件地址	发件人：user@example.com
如果-修改-自	如果内容未变，允许返回 304 Not Modified（未修改	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
最后修改	请求对象的最后修改日期（RFC 2822 格式	Last-Modified：Tue, 15 Nov 1994 12:45:26 GMT
Pragma	特定于实现的标头，可在请求-响应链的任何位置产生各种影响。	Pragma: no-cache
推荐人	这是上一个网页的地址，从该网页链接到当前请求的网页	Referrer: HTTP://www.edgenexus.io
服务器	服务器名称	服务器：Apache/2.4.1 (Unix)
设置	一个 HTTP cookie	Set-Cookie：UserID=JohnDoe; Max-Age=3600; Version=1
用户代理	用户代理的用户代理字符串	用户代理：Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
不同	告诉 告诉下游代理如何匹配未来的请求标头，以决定是否可以使用缓存响应，而不是请求新的响应。是否可以使用缓存的响应，而不是从源服务器请	可变：User-Agent

	求新的响应。 响应	
X-Powered-By	指定支持网络应用程序的技术（如 ASP.NET、PHP、JBoss）。	X-Powered-By：PHP/5.4.0

行动

操作是在满足条件后启用的一项或多项任务。



行动

双击 "操作 "栏，查看下拉列表。

目标

双击目标列，查看下拉列表。列表会根据操作而改变。

您也可以手动输入某些操作。

数据

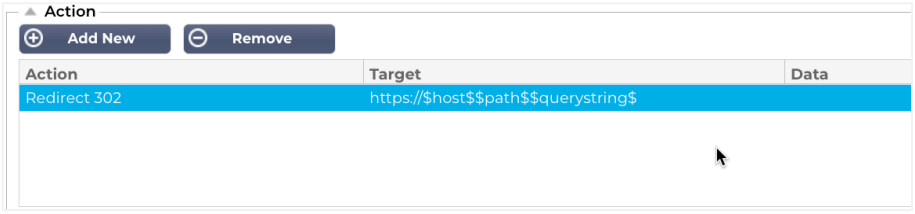
双击数据列，手动添加想要添加或替换的数据。

所有行动的详细清单如下：

行动	说明	示例
添加请求 Cookie	在 "目标 "部分添加请求 cookie 的详细信息，并在 "数据 "部分添加值	目标= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
添加请求标题	在数据部分添加带值的目标类型请求标头	目标= 接受 数据= 图像/png
添加响应 Cookie	在 "目标 "部分详细添加 "响应 Cookie"，并在 "数据 "部分添加值	目标= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
添加响应标头	在 "目标 "部分添加详细的请求标头，并在 "数据 "部分添加值	Target= 缓存控制 Data= max-age=8888888
车身全部更换	搜索回复正文并替换所有实例	Target= HTTP://（搜索字符串） Data= HTTPs://（替换字符串）

首先更换机身	搜索回复正文，仅替换第一例	Target= HTTP://（搜索字符串） Data= HTTPs://（替换字符串）
机身 最后更换	搜索回复正文，仅替换最后一个实例	Target= HTTP://（搜索字符串） Data= HTTPs://（替换字符串）
下降	这将中断连接	目标= 不适用 数据= 不适用
电子邮件	将向电子邮件事件中配置的地址发送电子邮件。您可以使用变量作为地址或信息	Target= "flightPATH 已通过电子邮件发送此事件" 数据= 不适用
日志事件	这将在系统日志中记录一个事件	Target= "flightPATH 已将此记录到系统日志中" 数据= 不适用
重定向 301	这将发出永久重定向	Target= HTTP://www.edgenexus.io Data= N/A
重定向 302	这将发出临时重定向	Target= HTTP://www.edgenexus.io Data= N/A
删除请求 Cookie	移除 "目标 "部分详细介绍的请求 cookie	目标= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
删除请求标题	删除 "目标 "部分详细说明的请求标头	目标=服务器 数据=N/A
移除响应 Cookie	移除 "目标 "部分详细说明的响应 cookie	目标=jnAccel
移除响应标头	移除 "目标 "部分详细说明的响应标头	目标= Etag 数据= 不适用
替换请求 Cookie	用 "数据 "部分的值替换 "目标 "部分详细列出的请求 cookie	目标= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
替换请求标题	用数据值替换目标中的请求标头	目标= 连接 Data= keep-alive
替换响应 Cookie	用 "数据 "部分的值替换 "目标 "部分详细说明的响应 cookie	Target=jnAccel=afYfn1CDqqCDqCVii Date=MS-WSMAN=afYfn1CDqqCDqCVii
替换响应标头	用 "数据 "部分中的值替换 "目标 "部分中详细说明的响应标头	目标= 服务器 数据= 为安全起见不公开
重写路径	这将允许您根据条件将请求重定向到新的 URL	Target= /test/path/index.html$querystring$ 数据= 不适用
使用安全服务器	选择要使用的安全服务器或虚拟服务	Target=192.168.101:443 数据=N/A
使用服务器	选择要使用的服务器或虚拟服务	目标= 192.168.101:80 数据= 不适用
加密 Cookie	这将对 cookie 进行 3DES 加密，然后进行 base64 编码	Target=输入要加密的 cookie 名称，可在末尾使用 "*"作为通配符 Data= 输入用于加密的通行短语

例如



下面的操作将向浏览器发出临时重定向，使其访问安全的 HTTPS 虚拟服务。它将使用与请求相同的主机名、路径和查询字符串。

常见用途

应用程序防火墙和安全

- 阻止不受欢迎的 IP
- 强制用户使用 HTTPS 访问特定（或全部）内容
- 阻止或重定向蜘蛛
- 防止跨站点脚本并发出警报
- 防止 SQL 注入并发出警报
- 隐藏内部目录结构
- 重写 cookie
- 特定用户的安全目录

特点

- 根据路径重定向用户
- 提供跨多个系统的单点登录功能
- 根据用户 ID 或 Cookie 对用户进行分类
- 为 SSL 卸载添加标头
- 语言检测
- 重写用户请求
- 修复损坏的 URL
- 日志和电子邮件警报 404 响应代码
- 防止目录访问/浏览
- 向蜘蛛发送不同的内容

预建规则

HTML 扩展

将所有 .htm 请求更改为 .html

条件：

- 条件 = 路径
- 感觉 = 是否
- 检查 = 匹配 RegEx
- 值 =\.htm$

评估：

- 空白

行动：

- 操作 = 重写路径
- 目标 = $path$I

索引.html

在请求文件夹时强制使用 index.html。

条件：此条件为一般条件，可匹配大多数对象

- 条件 = 主机
- 感觉 = 是否
- 检查 = 存在

评估：

- 空白

行动：

- 操作 = 重定向 302
- 目标 = HTTP://$host$path$index.html$querystring$

关闭文件夹

拒绝文件夹请求。

条件：此条件为一般条件，可匹配大多数对象

- 条件 = 需要适当考虑
- 感觉 =
- 检查 =

评估：

- 空白

行动：

- 行动 =
- 目标 =

隐藏 CGI-BBIN:

在请求 CGI 脚本时隐藏 cgi-bin 目录。

条件：此条件为一般条件，可匹配大多数对象

- 条件 = 主机
- 感觉 = 是否
- 检查 = 匹配 RegEX
- 值 =\.cgi$

评估：

- 空白

行动：

- 操作 = 重写路径
- 目标 = /cgi-bin$path$

原木蜘蛛

记录常用搜索引擎的蜘蛛请求。

条件：此条件为一般条件，可匹配大多数对象

- 条件 = 请求标头
- 匹配 = 用户代理
- 感觉 = 是否
- 检查 = 匹配 RegEX
- 值 = Googlebot|Slurp|bingbot|ia_archiver

评估：

- 变量 = $crawler$
- 来源 = 请求标头
- 详细信息 = 用户代理

行动：

- 操作 = 记录事件
- 目标 = [$crawler$] $host$$path$$querystring$

强制 HTTPS

强制某些目录使用 HTTPS。在这种情况下，如果客户正在访问包含 /secure/ 目录的任何内容，那么他们将被重定向到所请求 URL 的 HTTPs 版本。

条件：

- 条件 = 路径
- 感觉 = 是否
- 检查 = 包含
- 值 = /secure/

评估：

- 空白

行动：

- 操作 = 重定向 302
- 目标 = HTTPs://$host$$path$$querystring$

媒体流:

将 Flash 媒体流重定向到适当的服务。

条件：

- 条件 = 路径
- 感觉 = 是否
- 检查 = 结束
- 值 = .flv

评估：

- 空白

行动：

- 操作 = 重定向 302
- 目标 = HTTP://$host$:8080/$path$

将 HTTP 转换为 HTTPS

将任何硬编码 HTTP:// 更改为 HTTPS://

条件：

- 条件 = 响应代码
- 感觉 = 是否

- 检查 = 相同
- 值 = 200 OK

评估：

- 空白

行动：

- 操作 = 全部替换主体
- 目标 = HTTP://
- 数据 = HTTPs://

空白信用卡

检查回复中是否有信用卡，如果发现有信用卡，则将其空白。

条件：

- 条件 = 响应代码
- 感觉 = 是否
- 检查 = 相同
- 值 = 200 OK

评估：

- 空白

行动：

- 操作 = 全部替换主体
- Target = [0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+
- 数据 = xxxx-xxxx-xxxx-xxxxxx

内容过期

在页面上添加合理的内容有效期，以减少请求和 304 的数量。

条件：这是一个通用条件，可以一网打尽。建议将此条件集中在您的

- 条件 = 响应代码
- 感觉 = 是否
- 检查 = 相同
- 值 = 200 OK

评估：

- 空白

行动：

- 操作 = 添加响应标头
- 目标 = 高速缓存控制
- 数据 = max-age=3600

欺骗服务器类型

获取服务器类型，并将其更改为其他类型。

条件：这是一个通用条件，可以一网打尽。建议将此条件集中在您的

- 条件 = 响应代码
- 感觉 = 是否
- 检查 = 相同
- 值 = 200 OK

评估：

- 空白

行动：

- 操作 = 替换响应头
- 目标 = 服务器
- 数据 = 保密

永不发送错误

客户从不会从你们的网站上看到任何错误。

条件

- 条件 = 响应代码
- 感觉 = 是否
- 检查 = 包含
- 值 = 404

评估

- 空白

行动

- 操作 = 重定向 302
- 目标 = HTTP//$host$/

语言重定向

查找语言代码并重定向到相关国家域名。

条件

- 条件 = 语言
- 感觉 = 是否
- 检查 = 包含
- 值 = 德语（标准）

评估

- 变量 = $host_template$
- 来源 = 主机
- 值 = .*\.

行动

- 操作 = 重定向 302
- 目标 = HTTP//$host_template$de$path$$querystring$

谷歌分析

插入 Google 分析所需的代码 - 请将 MYGOOGLECODE 更改为您的 Google UA ID。

条件

- 条件 = 响应代码
- 感觉 = 是否
- 检查 = 相同
- 值 = 200 OK

评估

- 空白

行动

- 操作 = 正文 最后替换
- 目标 = </body>
- 数据 = <script type='text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); } }.)(); </script> </body> </body

IPv6 网关

调整 IPv6 服务上 IIS IPv4 服务器的主机标头。IIS IPv4 服务器不喜欢在主机客户端请求中看到 IPV6 地址，因此这条规则用一个通用名称来替代。

条件

- 空白

评估

- 空白

行动

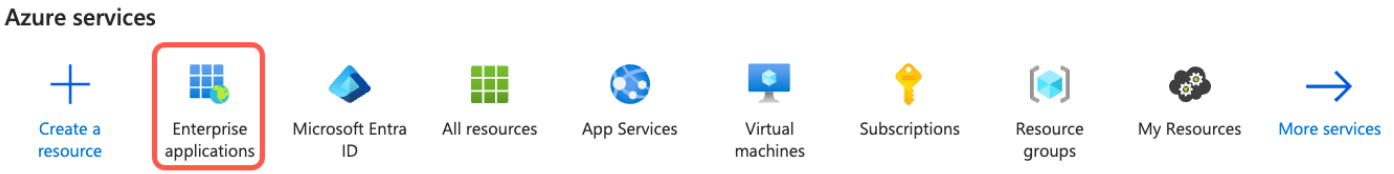
- 操作 = 替换请求标头
- 目标 = 主机
- 数据 =ipv4.host.header

SAML 和 Entra ID

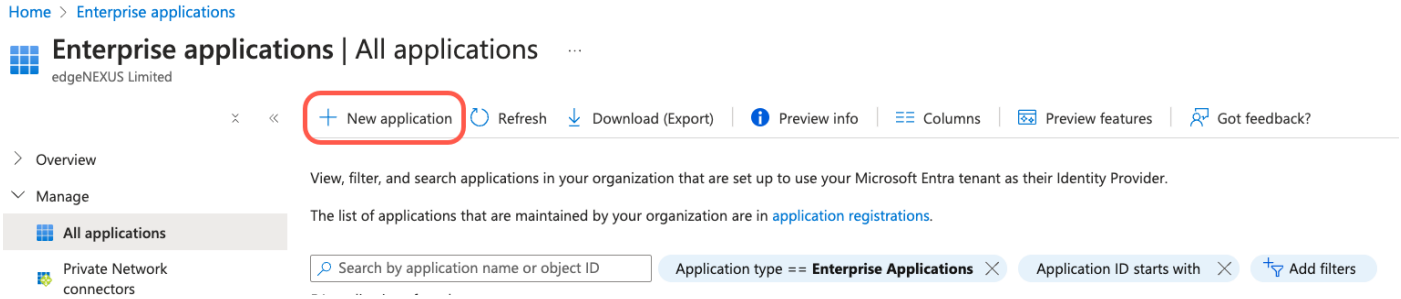
在 Microsoft Entra 中设置 Entra ID 身份验证应用程序

为了使 SAML 身份验证成功运行，您需要在 Microsoft Entra 管理门户中设置企业应用程序。这是一项简单的任务，可以为 SAML 身份验证请求和令牌以及配置 XML 数据提供所需的签名证书。

为此，首先应登录 Microsoft Entra Portal (https://portal.azure.com)，并确保您位于 Azure 服务页面，在该页面顶部有一个图标列表（见下图）。

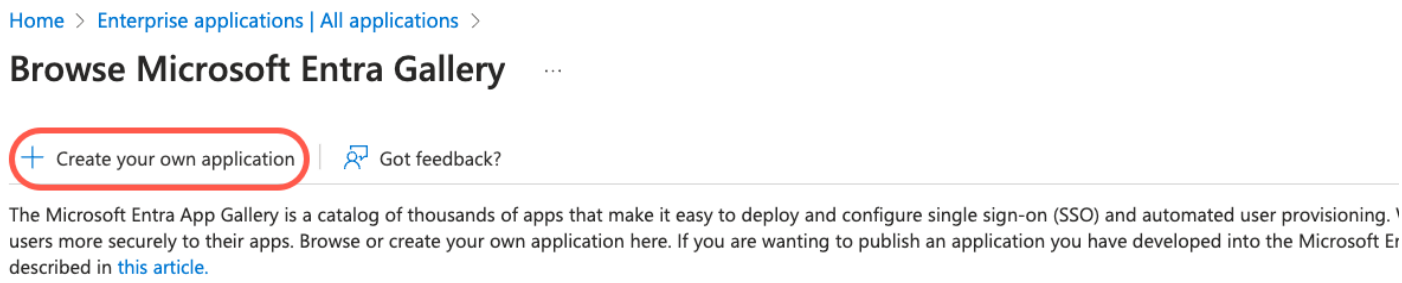


- 单击企业应用程序。如果在图标列表中看不到企业应用程序，可以在顶部的搜索栏中输入名称。您将看到如下所示的页面。

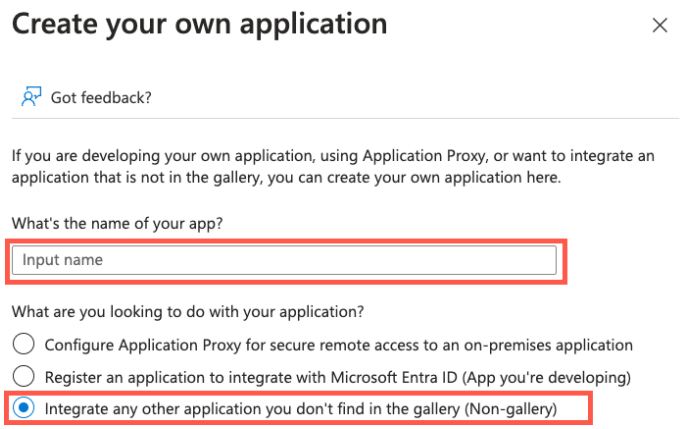


点击*新申请*

在下一页，点击*创建自己的应用程序*。

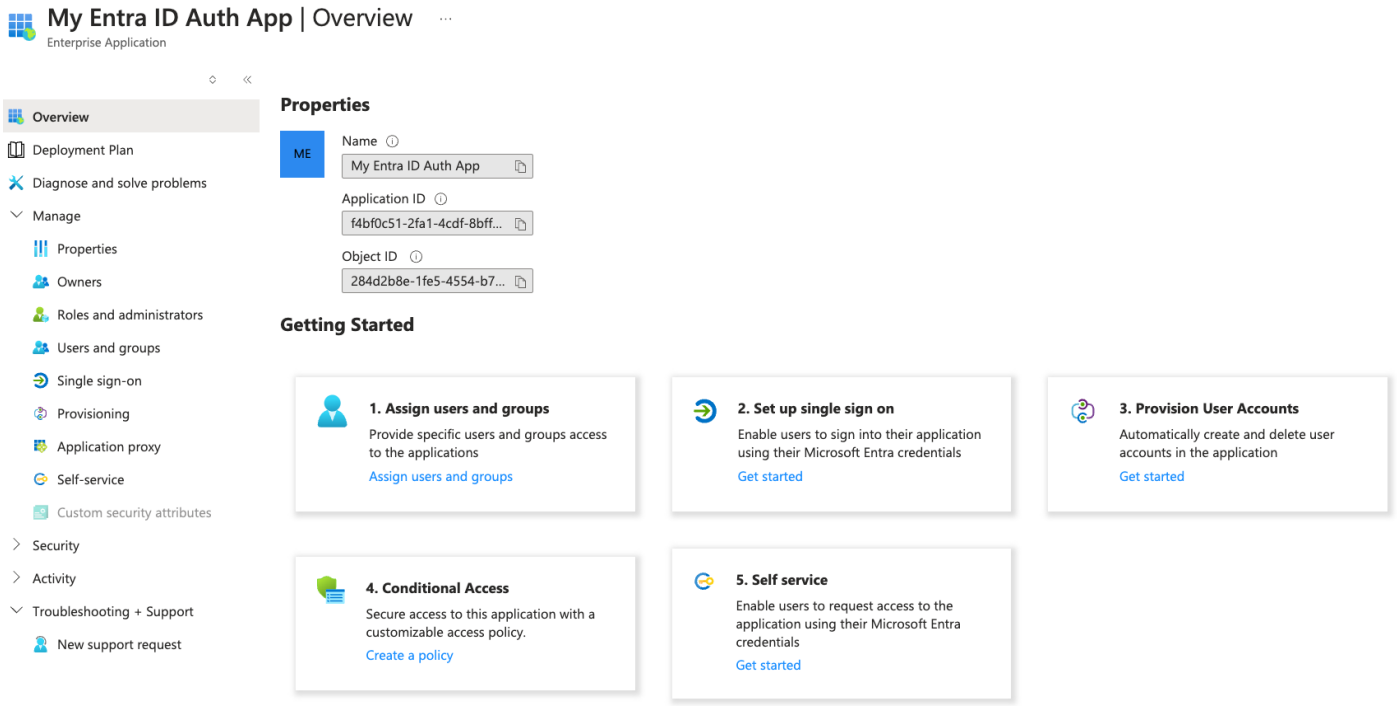


- 页面右侧将打开一个标题为 "*创建自己的应用程序*"的部分。

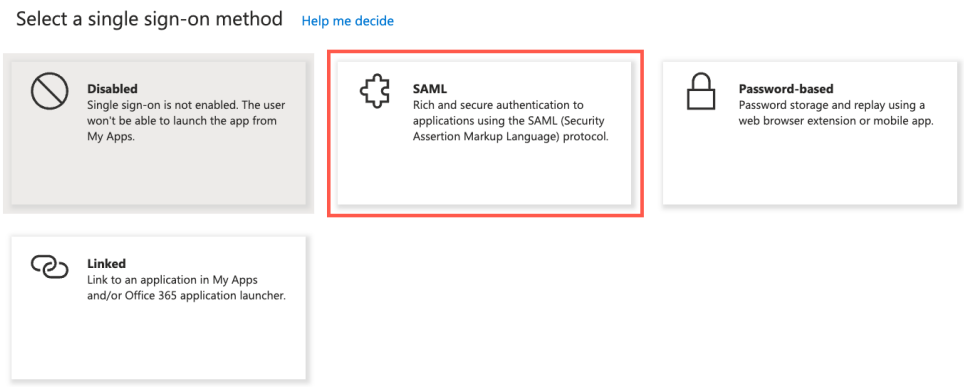


- 为你的应用程序命名，例如 "我的 Entra ID Auth 应用程序"。您可以选择任何您想要的名称。
- 单击 "*整合图库（非图库）中没有的任何其他应用程序* "单选按钮选项。
- 单击 "*创建* "按钮。

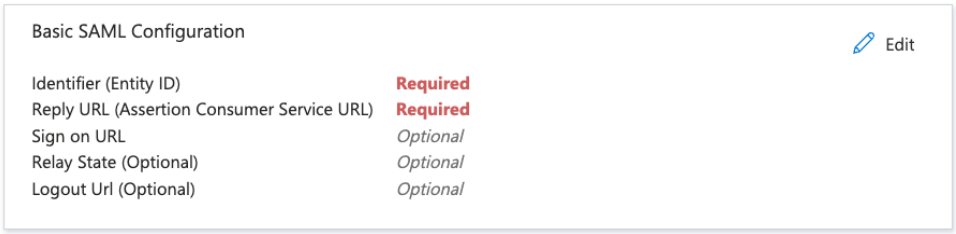
现在您将看到一个类似下图的页面。



- 点击左侧导航栏中的单点登录选项。
- 选择 SAML 框



- 现在您将看到一个包含基本 SAML 配置部分的页面。



- 在基本 SAML 配置区域填写
    - 标识符（实体 ID）
    - 回复 URL（断言消费者服务 URL）
    - 登录 URL
    - 注销 URL（可选）
- 保存配置并测试应用程序。

有关更详细的指导，请参阅 Microsoft 网站上的 "为企业应用程序启用单点登录 "文档。

技术支持

我们根据公司的标准服务条款为所有用户提供技术支持。

如果您拥有 EdgeADC、EdgeWAF 或 EdgeGSLB 的有效支持和维护合同，我们将提供技术支持。

要提出支持请求，请访问

https://www.edgenexus.io/support/