EdgeADC

管理指南

内容

文件属性

文件编号：2.0.5.28.21.09.05

文件创建日期。2021年4月30日

文件最后编辑。May 28, 2021

文件作者。杰伊-萨沃尔

文件最后编辑者。

文件转介。 边缘ADC- 版本 4.2.7.1890

文件免责声明

由于您的产品发布版本的不同，本手册中的截图和图形可能与您的产品略有不同。Edgenexus公司确保他们做出一切合理的努力，以确保本文件中的信息是完整和准确的。Edgenexus公司对任何错误不承担任何责任。Edgenexus公司会在未来的版本中，在需要时对本文档中的信息进行修改和更正。

版权

商标

Edgenexus标志、Edgenexus、EdgeADC、EdgeWAF、EdgeGSLB、EdgeDNS都是Edgenexus有限公司的商标或注册商标。所有其他商标都是其各自所有者的财产，并得到承认。

埃德纳克斯支持

如果你有关于本产品的任何技术问题，请提出支持票：support@edgenexus.io

安装EdgeADC

EdgeADC（从现在开始称为ADC）产品可以用几种方法进行安装。每个平台目标都需要它的安装程序，而这些都是你可以使用的。

这些是现有的各种安装模式。

- VMware ESXi
- 科沃斯
- 微软Hyper-V
- 甲骨文虚拟机
- 用于裸机硬件的ISO

你将用于托管ADC的虚拟机的大小取决于用例场景和数据吞吐量。

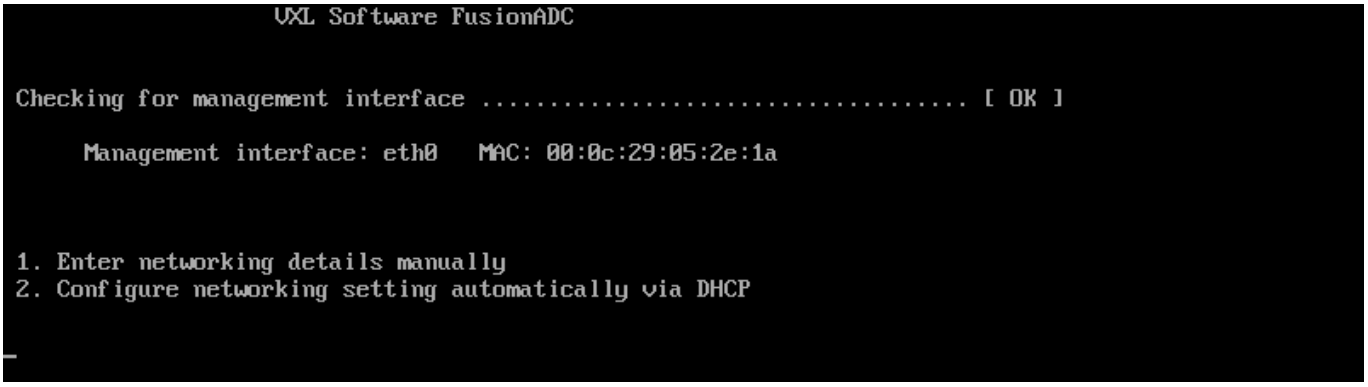
VMware ESXi

ADC可以安装在VMware ESXi是5.x及以上版本。

- 使用下载邮件中提供的适当链接下载ADC的最新安装OVA包。
- 下载后，请在你的ESXi主机或SAN上的一个合适的目录中解压。
- 在vSphere客户端，选择File: Deploy OVA/OVF Template。
- 浏览并选择你保存文件的位置；选择OVF文件并点击**下一步**
- ESX服务器要求提供设备名称。键入一个合适的名称，然后点击**NEXT**
- 选择数据存储，你的ADC设备将从那里运行。
- 选择一个有足够空间的数据存储，然后点击**下一步**
- 然后你将被告知有关产品的信息；点击**下一步**
- 点击 "**下一步**"。
- 一旦你把文件复制到数据存储，你就可以安装虚拟设备了。

启动你的vSphere客户端，查看新的ADC虚拟设备。

- 右键点击VA，进入电源>开机状态
- 然后，你的VA将启动，ADC启动屏幕将显示在控制台。



请参考 "首次启动配置 "一节，以便进一步操作。

安装VMXNET3接口

支持VMXnet3驱动程序，但您需要先对网卡设置进行修改。

注意 - 不要升级VMware-tools

在一个刚导入的VA上启用VMXNET3接口（从未启动）。

1. 从虚拟机中删除两个网卡
2. 升级虚拟机硬件 - -
   右键单击列表中的VA，选择升级虚拟硬件（不要启动VMware工具的安装或更新，只执行硬件升级）。
3. 添加两个网卡并选择它们为VMXNET3
4. 用标准方法启动VA。它将与VMXNET3一起工作

在已经运行的VA上启用VMXNET3接口

1. 停止虚拟机（CLI关机命令或GUI断电）。
2. 获取两个网卡的MAC地址（记住列表中网卡的顺序！）。
3. 从虚拟机中删除两个网卡
4. 升级虚拟机硬件（不要开始安装或更新VMware工具，只进行硬件升级
5. 添加两个网卡并选择它们为VMXNET3
6. 根据步骤2，为新的网卡设置MAC地址
7. 重新启动VA

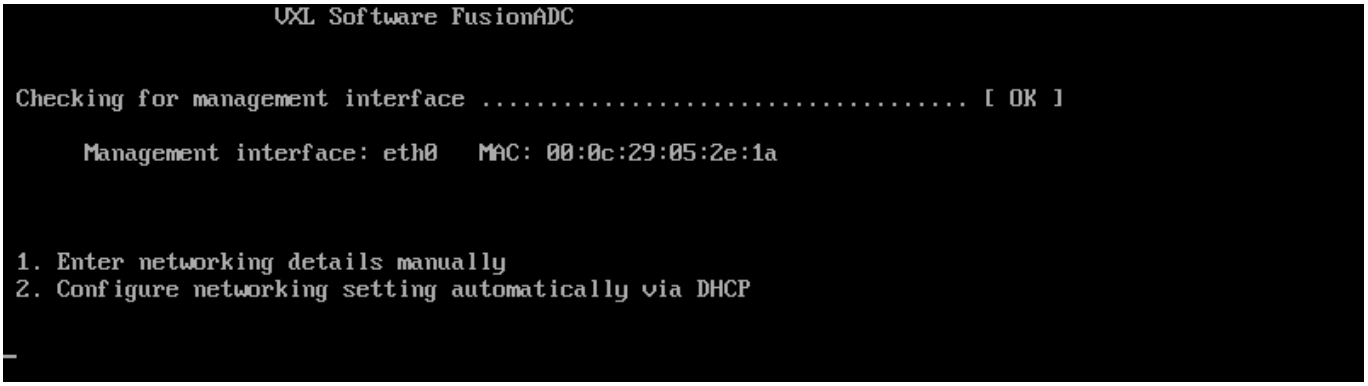
我们支持VMware ESXi作为生产平台。 为评估目的，你可以使用VMware Workstation和Player。

微软Hyper-V

ADC虚拟设备与安装在Microsoft Hyper-V服务器上兼容。

- 将Hyper-V ADC VA zip文件解压到你的本地机器或服务器。

- 打开Hyper-V管理器。
- 在你的Hyper-V管理器中，右击服务器，选择 **"导入虚拟机"。**
- 浏览到包含ADC Hyper-V文件的文件夹。
- 点击 **"复制虚拟机（创建一个新的唯一ID）"**
- 勾选 **"复制所有文件，以便可以再次导入相同的虚拟机"。**
- 点击 **"导入"。**
- 你的机器以 **"ADC ADC VA for Hyper-V "的**名称导入。
- 确保你在网卡上选择正确的网络
- 如果你要安装一个以上的虚拟设备，你将不得不为每个设备配置一个独特的MAC地址
- 右击你刚刚创建的虚拟机，点击 **"连接"。**
- 点击绿色的开始按钮或点击 **"ActionStart"。**
- 你的VA将启动，ADC控制台屏幕将显示。



- 一旦你配置了网络属性，VA将重新启动并呈现出登录VA控制台的状态。

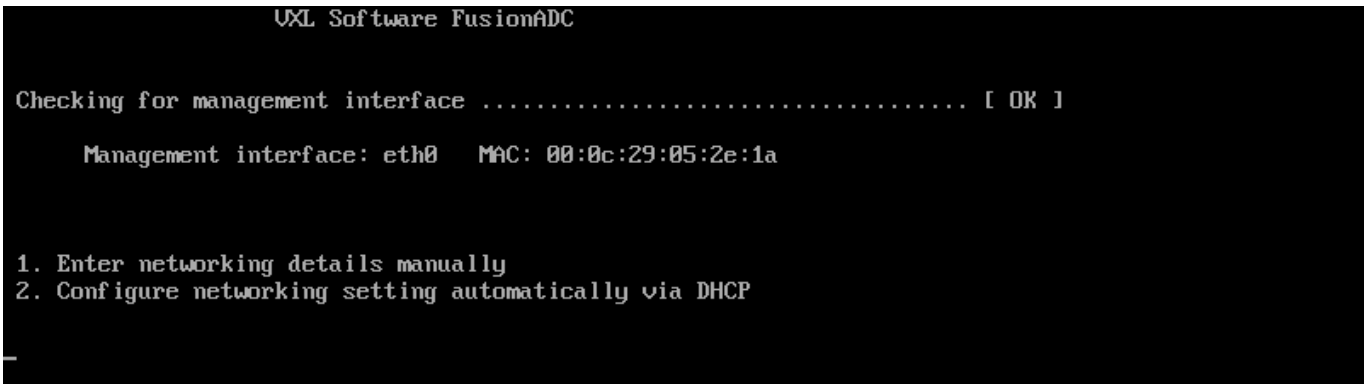
请参考 "首次启动配置 "一节，以便进一步操作。

Citrix XenServer

ADC虚拟设备可以安装在Citrix XenServer上。

- 将ADC OVA ALB-VA文件提取到你的本地机器或服务器。
- 打开Citrix XenCenter Client。
- 在XenCenter客户端，选择 **"文件：导入"。**
- 浏览并选择**OVA**文件，然后点击 **"Open Next"。**
- 当要求时，选择虚拟机创建位置。
- 选择您想安装的XenServer，然后点击 **"NEXT"。**
- 当询问时，选择存储库（SR）用于虚拟磁盘的放置。
- 选择一个有足够空间的SR，然后点击 **"NEXT"。**
- 绘制你的虚拟网络接口。两个接口都将显示Eth0；但是，请注意，最下面的接口是Eth1。
- 为每个接口选择目标网络，并点击**下一步**

- 不要勾选 "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，并将网络设置留在DHCP上。请注意，如果你没有工作的DHCP服务器，你必须为传输分配静态IP地址的详细信息。如果不这样做，将导致导入时连续显示连接失败。点击 **"下一步"**
- 审查所有信息，然后检查正确的设置。点击 **"完成"。**
- 您的虚拟机将开始传输虚拟磁盘 "ADC ADC"，一旦完成，将在您的XenServer下显示。
- 在XenCenter客户端，您现在可以看到新的虚拟机。
  右键点击VA，点击 "**START**"。
- 然后你的虚拟机将启动，ADC启动屏幕将显示。



- 一旦配置好，登录VA的过程就会呈现出来。

请参考 "首次启动配置 "一节，以便进一步操作。

首次启动配置

在第一次启动时，ADC VA显示以下屏幕，要求对生产操作进行配置。

第一次开机--手动网络细节

在第一次启动时，你将有10秒钟的时间来中断通过DHCP自动分配IP的细节

要中断这个过程，请点击进入控制台窗口并按任何键。然后你可以手动输入以下细节。

- IP地址
- 子网掩码
- 闸门
- DNS服务器

这些变化是持久性的，在重启后仍会存在，不需要在VA上再次配置。

第一次启动 - DHCP成功

如果你不中断网络分配过程，你的ADC将在超时后联系DHCP服务器，以获得其网络细节。如果联系成功，那么你的机器将被分配到以下信息。

- IP地址
- 子网掩码
- 默认网关
- DNS服务器

我们建议你不要使用DHCP地址来操作ADC VA，除非该IP地址与DHCP服务器内的VA的MAC地址永久链接。我们始终建议在使用VA时使用一个**固定的IP地址**。按照**改变管理IP地址**和后续章节中的步骤进行操作，直到完成网络配置。

第一次启动 - DHCP失败

如果您没有DHCP服务器或连接失败，将分配IP地址192.168.100.100。
该IP地址将以'1'递增，直到VA找到一个空闲的IP地址。同样地，VA将检查该IP地址是否正在使用，如果是，将再次递增并重新检查。

改变管理IP地址

你可以在任何时候使用**set greenside=n.n.n.n**命令改变VA的IP地址，如下所示。

```
Command:set greenside=192.168.101.1_
```

改变eth0的子网掩码

网络接口使用前缀 "eth"；基本网络地址被称为eth0。子网掩码或网络掩码可以用**set mask eth0 n.n.n.n**命令来改变。

```
Command:set mask eth0 255.255.255.0_
```

指定一个默认网关

VA需要一个默认网关来进行操作。要设置默认网关，请使用**route add default gw n.n.n.n.**命令，如下例所示。

```
Command:route add default gw 192.168.101.254_
```

检查默认网关值

要检查默认网关是否被添加并且是正确的，请使用**route**命令。该命令将显示网络路由和默认网关值。请看下面的例子。

```
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
```

现在你可以访问图形用户界面（GUI）来配置ADC的生产或评估使用。

访问网络界面

你可以使用任何带有Javascript的互联网浏览器来配置、监控和部署ADC，使其投入运行使用。

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

默认情况下，ADC使用一个自签名的SSL证书。你可以改变ADC以使用你自己选择的SSL证书。

一旦你的浏览器到达ADC，它就会向你显示登录屏幕。ADC的出厂默认凭证是。

默认用户名 = **admin** / 默认密码 = **jetnexus**

命令参考表

指挥部	参数1	参数2	描述	例子
日期			显示当前所配置的日期和时间	Tue Sept 3 13:00 UTC 2013
违约			为您的设备指定出厂默认设置	
退出			退出命令行界面	
帮助			显示所有有效的命令	
如果配置	[空白]		查看所有界面的界面配置	如果配置
	eth0		只查看eth0的接口配置	ifconfig eth0
机器码			该命令将提供用于许可ADC的机器ID。	EF4-3A35-F79
退出			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			重新启动ADC ADC虚拟服务	
航线	[空白]		查看路由表	航线
	增加	缺省gw	添加默认网关的IP地址	路由添加默认gw 192.168.100.254
设置	绿地		设置ADC的管理IP地址	设置greenside=192.168.101.1
	面罩		设置一个接口的子网掩码。接口名称是eth0, eth1....	设置掩码 eth0 255.255.255.0
显示			显示全局配置设置	
停业			终止所有连接并关闭ADC的电源 ADC	
身份			显示当前的数据统计	
顶部			查看进程信息，如CPU和内存	
查看日志	信息		显示原始的syslog消息	查看日志信息

请注意：命令是不分大小写的。没有命令历史记录。

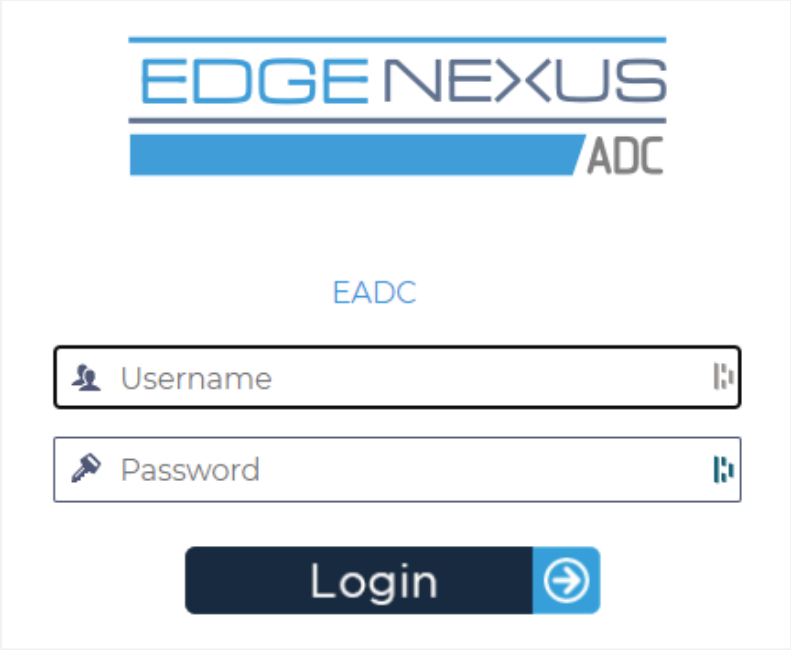
启动ADC Web Console

对ADC（也称为ADC）的所有操作都是通过网络控制台进行配置和执行的。可以使用任何带有Javascript的浏览器访问网络控制台。

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

https://adc.company.com

启动后，ADC的网络控制台如下图所示，允许你作为管理用户登录。



默认登录凭证

默认的登录凭证是。

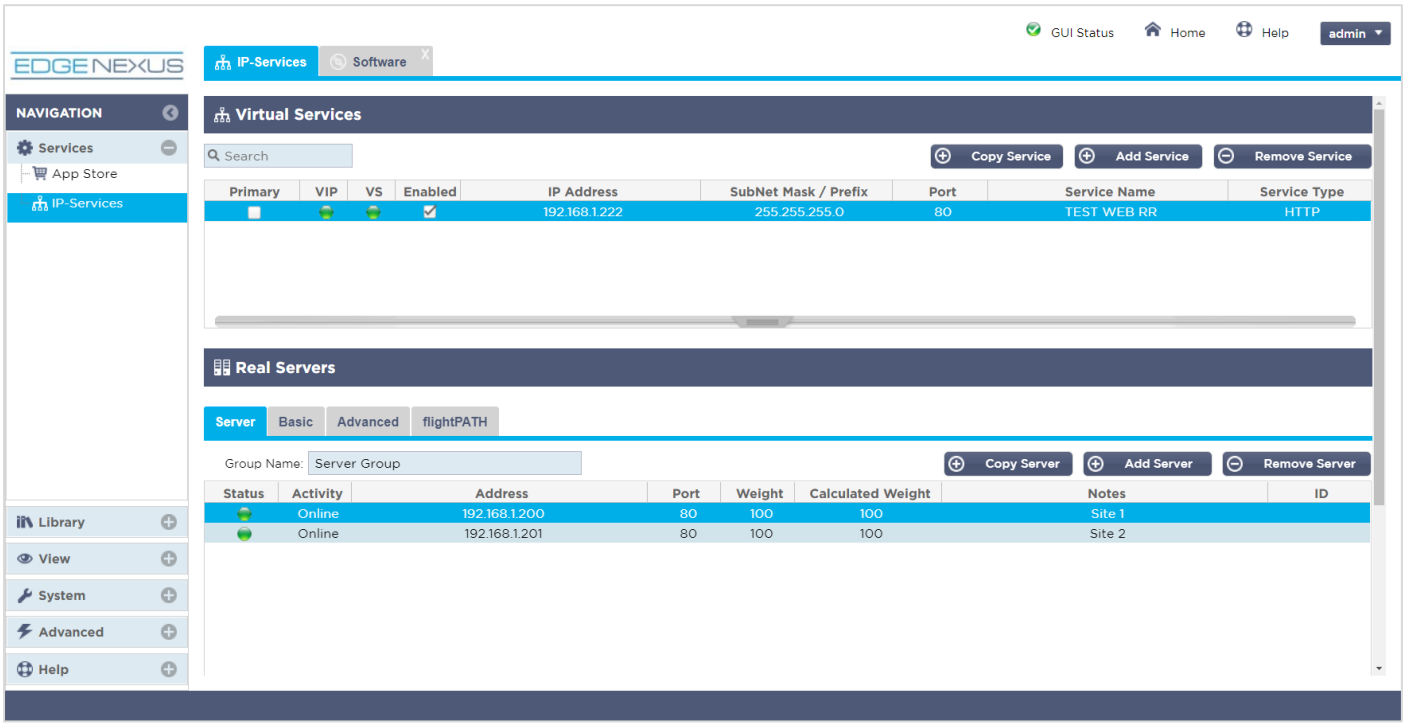
- 用户名: admin
- 密码: jetnexus

你可以在任何时候使用位于*系统>用户的*用户配置功能来改变这一点。

一旦你成功登录，就会显示ADC的主仪表板。

主仪表板

下面的图片说明了ADC的主要仪表板或 "主页
"的样子。由于改进的原因，我们可能会不时地做一些改变，但所有的功能都会保留。



为了尽可能简明扼要，我们将假设对屏幕部分的首次介绍将证明对ADC配置区的不同部分有足够的认识，因此我们在推进过程中不会对其进行详细描述，而是将重点放在配置性元素上。

从左到右，我们首先有导航。导航部分由ADC内的不同区域组成。当你点击导航中的一个特定选择时，这将在屏幕的右侧显示相应的部分。你还可以看到所选择的配置部分在屏幕顶部的标签，与产品标志相邻。这些选项卡能够更快地导航到ADC配置中预先使用的区域。

服务

ADC的服务部分在其内部有几个区域。当你点击服务项目时，这将扩大显示可用的选择。

知识产权服务

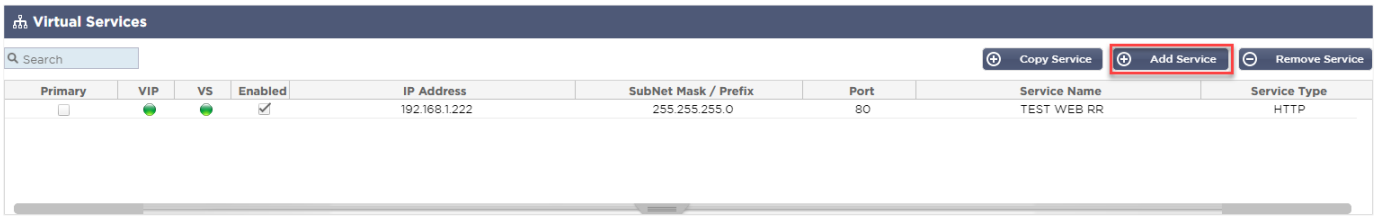
ADC的IP服务部分允许你添加、删除和配置你在特定使用情况下需要的各种虚拟IP服务。这些设置和选项分为以下几个部分。这些部分在应用屏幕的右侧。

虚拟服务

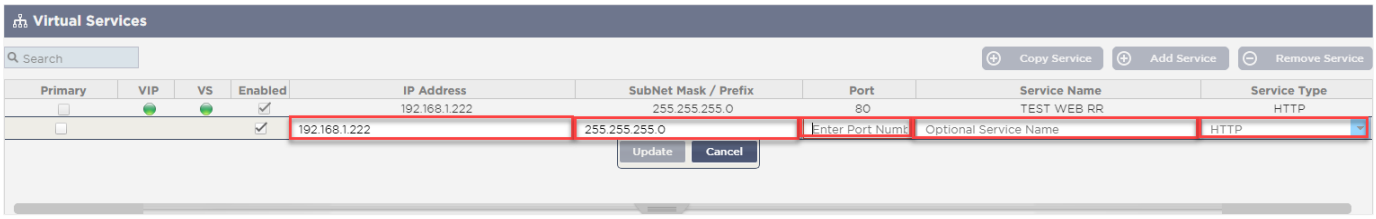
一个虚拟服务结合了一个虚拟IP（VIP）和一个ADC监听的TCP/UDP端口。到达虚拟服务IP的流量被重定向到与该服务相关的真实服务器之一。虚拟服务的IP地址不能与ADC的管理地址相同，即eth0、eth1等...。

ADC根据在 "真实服务器 "部分的 "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到服务器上。

使用一个新的VIP创建一个新的虚拟服务



- 如上所述，点击添加虚拟服务按钮。

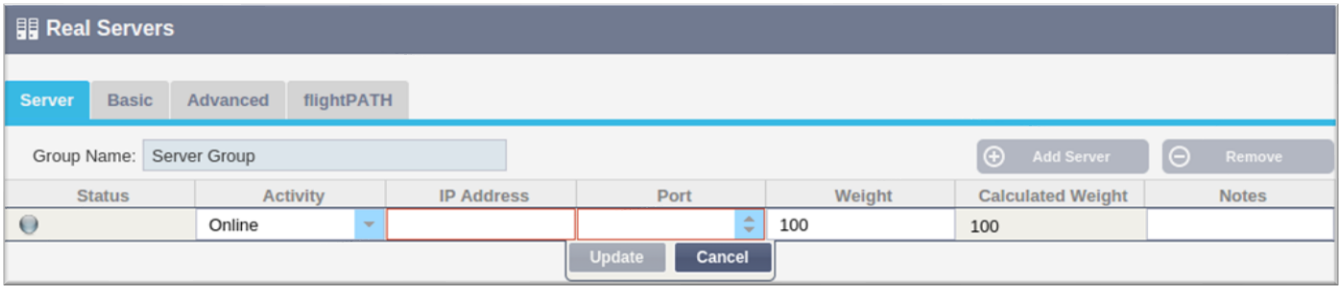


- 然后你将进入**编辑行**模式。
- 完成四个突出显示的字段以继续，然后点击更新按钮。

请使用TAB键在各字段中导航。

场地	描述
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。这个IP是用户或应用程序访问负载均衡应用程序的指向。
子网掩码/前缀	这个字段是与ADC所在的网络有关的子网掩码。
港口	访问VIP时使用的入口端口。如果你使用反向代理，这个值不一定要与真实服务器相同。
服务名称	服务名称是VIP的目的的文本表示。它是可选的，但我们建议你提供它以使之清晰。
服务类型	有许多不同的服务类型供你选择。第4层服务类型不能使用flightPATH技术。

现在你可以按更新按钮来保存这一部分，并自动跳到下面详细介绍的真实服务器部分。

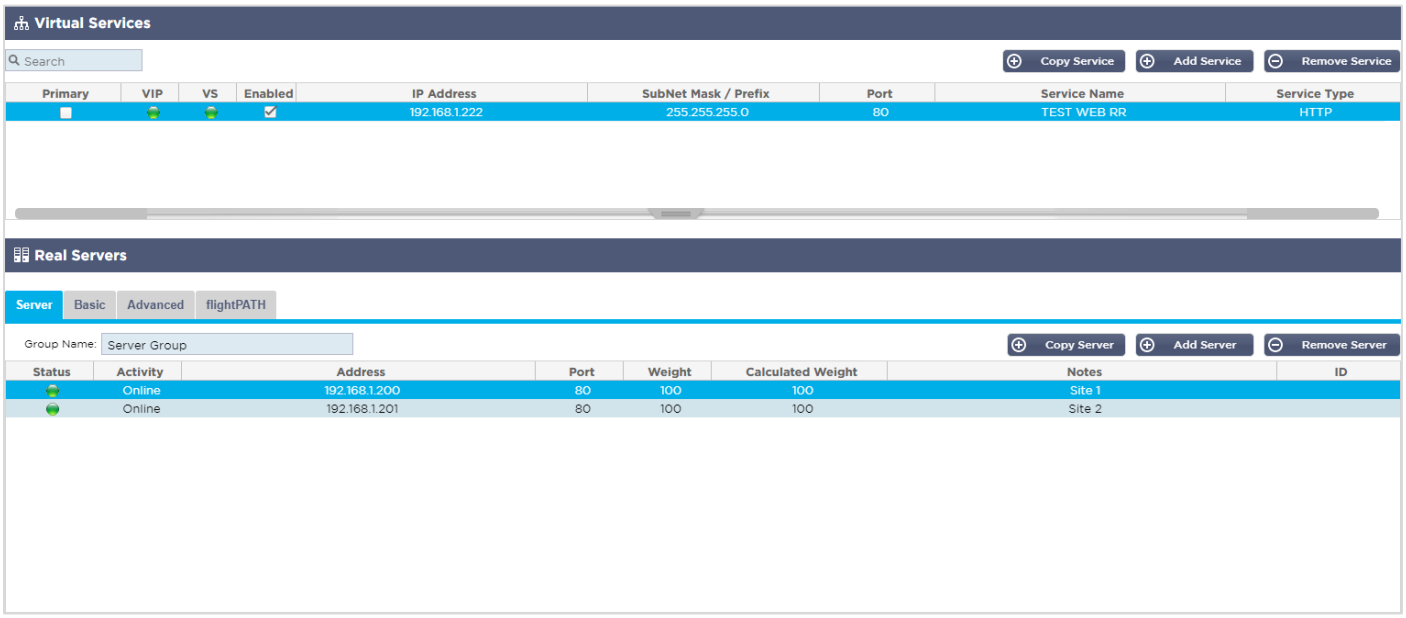


场地	描述
活动	活动字段可以用来显示和改变负载平衡的真实服务器的状态。 在线 - 表示服务器处于活动状态，正在接收负载平衡的请求。 离线 - 服务器处于离线状态，没有收到请求 Drain - 服务器已被置于drain模式，以便持久性可以冲刷，并将服务器转移到离线状态而不影响用户。 待机 - 服务器已被置于待机状态
IP地址	这个值是Real服务器的IP地址。它必须是准确的，不应该是DHCP地址。
港口	真实服务器上的目标访问端口。当使用反向代理时，这可能与VIP上指定的入口端口不同。
加权	这个设置通常是由ADC自动配置的。如果你想改变优先权的权重，你可以改变这个。

- 单击 "更新 "按钮或按回车键以保存您的更改。

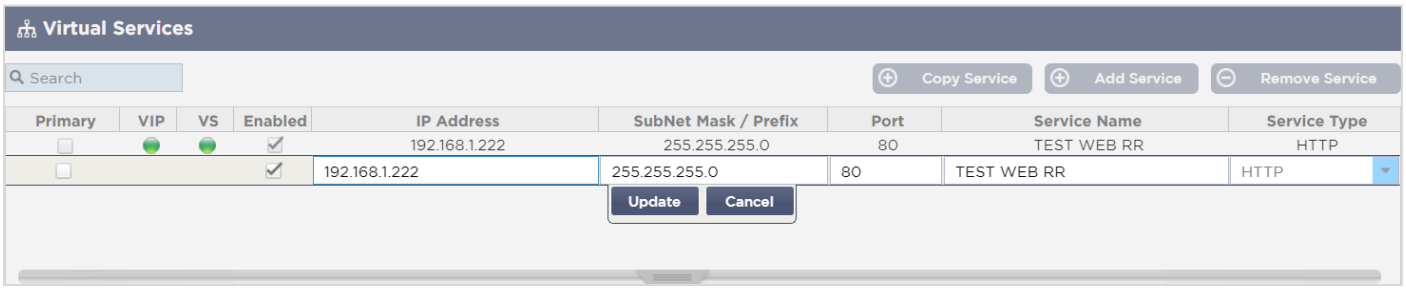
- 状态灯将首先变成灰色，如果服务器健康检查成功，则变成绿色。如果真实服务器监控失败，它将变成红色。
- 一个状态为红色的服务器将不会被负载平衡。

完成的虚拟服务的例子

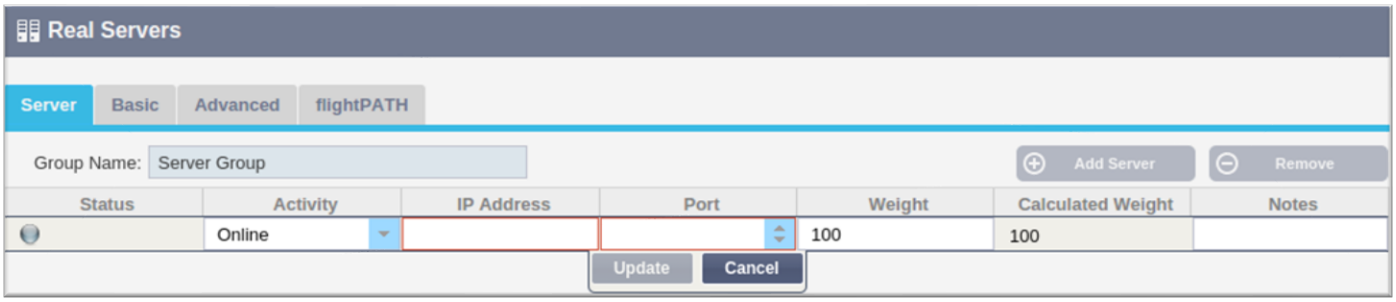


使用现有的VIP创建一个新的虚拟服务

- 突出显示你想复制的虚拟服务
- 点击添加虚拟服务，进入行编辑模式



- IP地址和子网掩码会自动复制过来
- 输入你的服务的端口号
- 输入一个可选的服务名称
- 选择一个服务类型
- 现在你可以按更新按钮保存这一部分，并自动跳到下面的真实服务器部分。

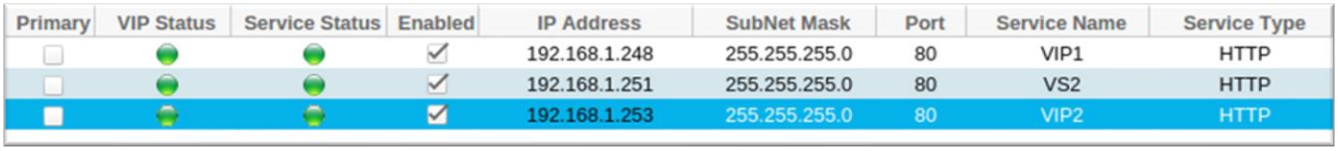


- 将服务器活动选项保留为在线 -
  这意味着如果它通过TCP连接的默认健康监测，它将被负载平衡。如果需要，以后可以改变这一设置。
- 输入一个真实服务器的IP地址
- 为真实服务器输入一个端口号
- 为真实服务器输入一个可选的名称
- 单击 "更新 "以保存您的更改
- 如果服务器健康检查成功，状态灯将首先变成灰色，然后变成绿色。如果真实服务器监控失败，它将变成红色。
- 一个有红色状态指示灯的服务器将不会被负载平衡

改变虚拟服务的IP地址

你可以在任何时候改变现有虚拟服务或VIP的IP地址。

- 突出显示你想改变其IP地址的虚拟服务



- 双击该服务的IP地址字段

- 将IP地址改成你想使用的那个地址
- 点击 "更新 "按钮，保存更改。

注意：改变一个虚拟服务的IP地址将改变与该VIP相关的所有服务的IP地址。

使用复制服务创建一个新的虚拟服务

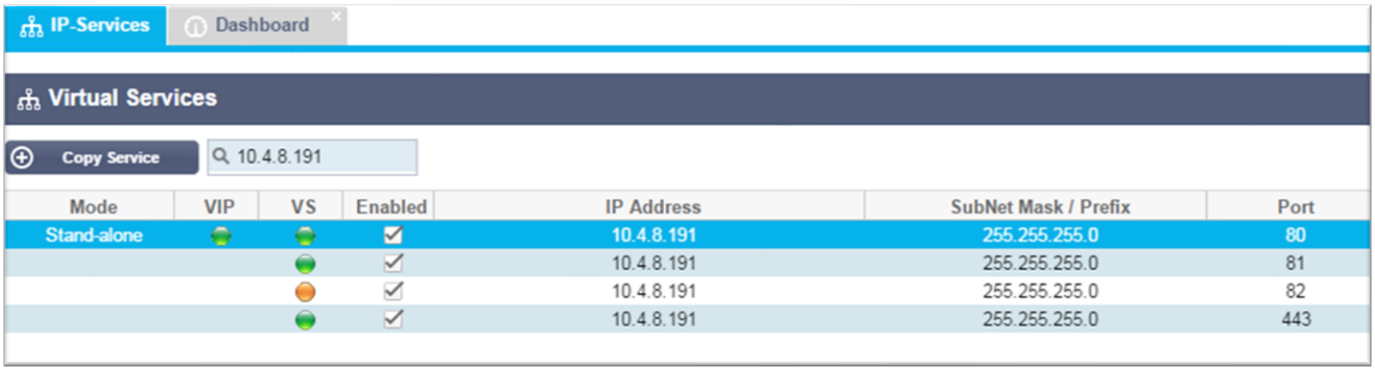
- 复制服务按钮将复制整个服务，包括所有真实服务器、基本设置、高级设置和与之相关的flightPATH规则。
- 突出显示你想复制的服务，并点击复制服务
- 行编辑器将出现，光标在IP地址列上闪烁。
- 你必须把IP地址改成唯一的，或者如果你想保留IP地址，你必须编辑端口，使其对该IP地址是唯一的。

如果你改变了一个设置，如负载平衡策略、Real服务器监视器或删除flightPATH规则，别忘了编辑每个标签。

筛选显示的数据

搜索一个特定的术语

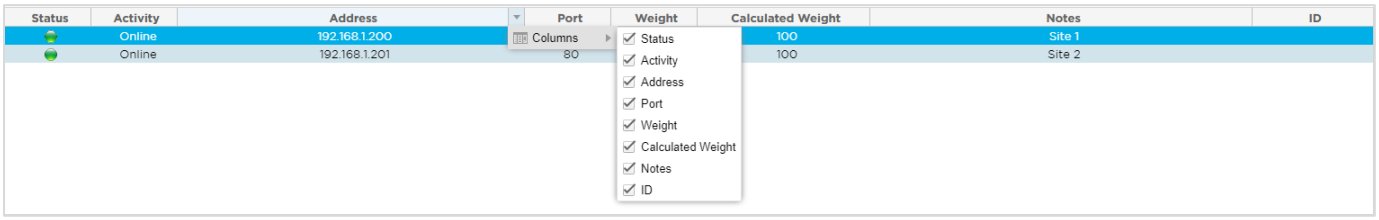
搜索框允许你使用任何数值搜索表格，如IP地址的八位数或服务名称。



上面的例子显示了搜索10.4.8.191这个特定IP地址的结果。

选择列的可见性

你也可以选择你希望在仪表板上显示的栏目。

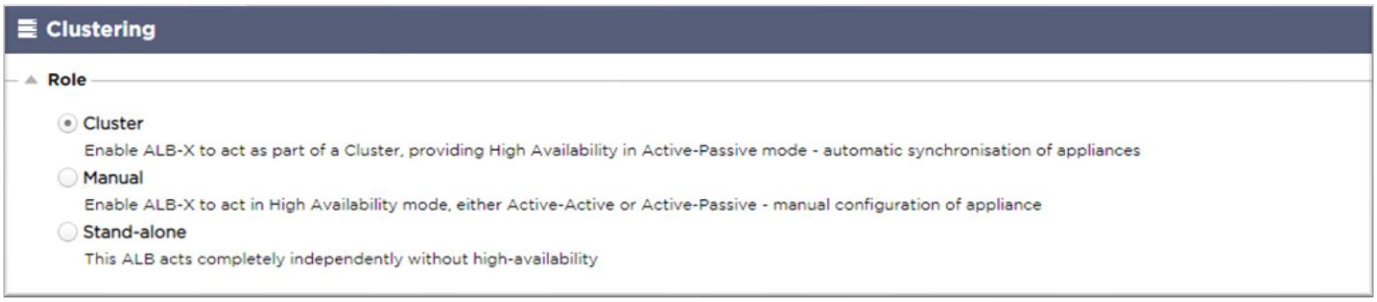


- 将鼠标移到任何一列上
- 你会看到列的右边出现一个小箭头
- 点击复选框可以选择你希望在仪表板上看到的栏目。

了解虚拟服务栏

主要/模式

Primary/Mode列表示为当前VIP选择的高可用性角色。使用系统 > 集群中的选项来配置这个选项。



选项	描述
群体	群集是ADC在安装时的默认角色，Primary/Mode列将显示它当前运行的模式。当你的数据中心有一对ADC设备的HA时，其中一个会显示主动，另一个显示被动
手册	手动角色允许ADC对不同的虚拟IP地址以主动-主动模式运行。在这种情况下，Primary列将包含一个方框，在每个独特的虚拟IP旁边，可以勾选主动，或不勾选被动。
单独的	ADC是作为一个独立的设备，不在高可用性模式下。因此，Primary（主要）一栏将显示Stand-alone（独立）。

负责人

这一栏提供了关于每个虚拟服务状态的视觉反馈。这些指标是用颜色编码的，具体如下。

LED	意义
●	在线
●	故障转移-待机。这个虚拟服务是热备用的
●	表示 "次要的 "正在为 "主要的 "拖后腿。
●	服务需要注意。该指示可能是由于Real服务器未能通过健康监测检查或被手动改为离线。流量将继续流动，但真实服务器的容量会减少。
●	离线。内容服务器无法到达，或没有启用内容服务器
●	查找情况
●	未被许可或被许可的虚拟IP数量超过了

已启用

这个选项的默认值是
"已启用"，复选框显示为勾选。你可以通过双击该行，取消勾选该复选框，然后点击更新按钮来禁用虚拟服务。

IP地址

添加你的IPv4地址（十进制点号）或一个IPv6地址。这个值是你的服务的虚拟IP地址（VIP）。例如IPv4"192.168.1.100"。例子 Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

子网掩码/前缀

添加你的子网掩码，以十进制点号表示。例如
"255.255.255.0"。或者对于IPv6，添加你的前缀。关于IPv6的更多信息，请参见**HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS。**

港口

添加与你的服务相关的端口号。该端口可以是一个TCP或UDP端口号。例如，TCP "80 "用于网络流量，TCP "443 "用于安全网络流量。

服务名称

添加一个友好的名称来识别你的服务。例如 "生产型网络服务器"。

服务类型

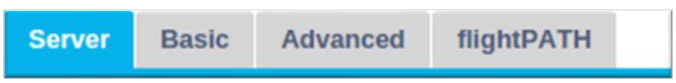
请注意，对于所有 "第4层
"服务类型，ADC不会与数据流进行交互或修改，因此flightPATH在第4层服务类型中不可用。第4层服务只是根据负载平衡策略对流量进行负载平衡。

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不会改变数据流中的任何信息，并将根据负载平衡策略执行标准的负载平衡流量。
第4层UDP	任何UDP端口	第4层	与第4层TCP一样，ADC不会改变数据流中的任何信息，并将根据负载平衡策略执行标准的负载平衡流量。
第四层TCP/UDP	任何TCP或UDP端口	第4层	如果你的服务有一个主要的协议，如UDP，但会回落到TCP，这是理想的。ADC不会改变数据流中的任何信息，并将根据负载平衡策略执行标准的负载平衡流量。

HTTP	HTTP或HTTPS协议	第7层	ADC可以使用flightPATH进行交互，操作和修改数据流。
FTP	文件传输协议协议	第7层	在客户端和服务器之间使用单独的控制和数据连接
SMTP	简单邮件传输协议	第4层	在负载平衡邮件服务器时使用
POP3	邮局礼仪	第4层	在负载平衡邮件服务器时使用
IMAP	互联网信息访问协议	第4层	在负载平衡邮件服务器时使用
RDP	远程桌面协议	第4层	在负载平衡终端服务服务器时使用
RPC	远程程序调用	第4层	在使用RPC调用的负载平衡系统时使用
RPC/ADS	Exchange 2010通讯录服务的静态RPC	第4层	在负载平衡Exchange服务器时使用
RPC/CA/PF	客户端访问和公共文件夹的Exchange 2010静态RPC	第4层	在负载平衡Exchange服务器时使用
DICOM	医学中的数字成像和通信	第4层	在使用DICOM协议的服务器进行负载平衡时使用

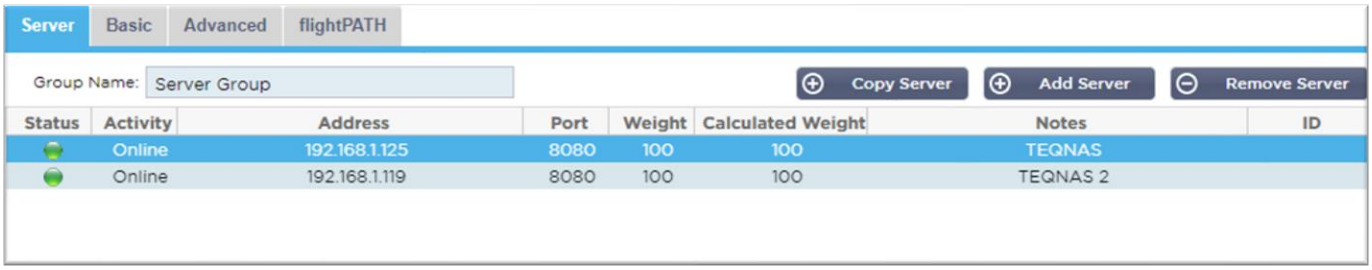
真实的服务器

在仪表板的真实服务器部分有几个标签。服务器，基本，高级，和flightPATH。



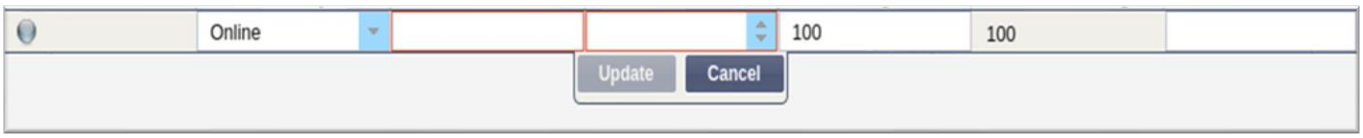
服务器

服务器选项卡持有与当前选择的虚拟服务配对的真实后端服务器的定义。你需要在真实服务器部分添加至少一个服务器。



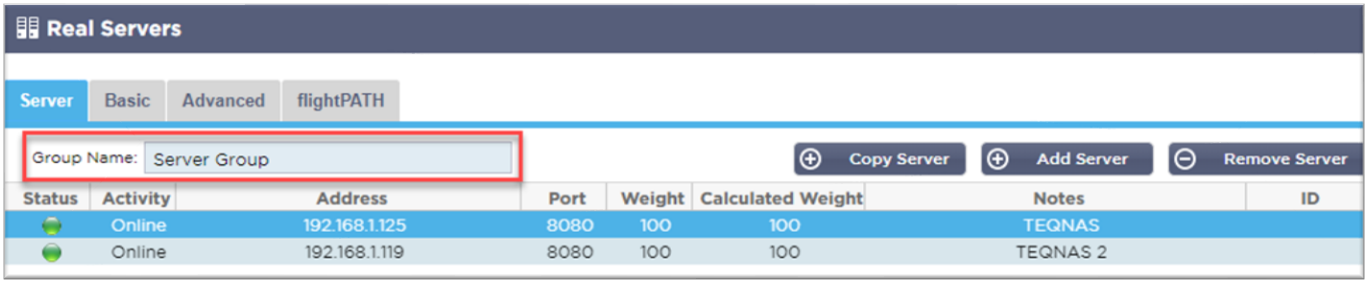
添加服务器

- 选择你以前定义的适当的VIP。
- 点击添加服务器
- 一个新的行将出现，光标在IP地址栏上闪烁。



- 输入你的服务器的IPv4地址，以十进制点号表示。真实服务器可以和你的虚拟服务在同一个网络上，也可以是任何直接连接的本地网络，或者是你的ADC可以路由的任何网络。例如 "10.1.1.1"。
- 标签到端口栏，输入服务器的TCP/UDP端口号。该端口号可以与虚拟服务的端口号相同，也可以是反向代理连接的其他端口号。ADC将自动翻译成这个号码。
- 在 "注释 "部分的标签中添加服务器的任何相关细节。例如。"IIS网络服务器1"

集团名称



当你添加了组成负载均衡组的服务器后，你还可以给它们附加一个组名。一旦你编辑了这个字段，内容就会保存，不需要按更新按钮。

真实服务器状态灯

你可以通过状态栏中的浅色看到一个真实服务器的状态。见下图。

LED	意义
●	已连接
◎	不受监控
●	排水
●	离线
●	待机
●	未连接
●	调查情况
●	未经许可或许可的真实服务器超过了

活动

你可以在任何时候通过使用下拉菜单来改变一个真实服务器的活动。要做到这一点，请双击真实服务器行，使其进入编辑模式。

选项	描述
在线	所有在线分配的真实服务器将根据基本选项卡内设置的负载平衡策略接收流量。
沥水	所有被指定为排空的真实服务器将继续为现有连接提供服务，但不接受任何新的连接。在排水过程中，状态灯将闪烁绿色/蓝色。一旦现有的连接自然关闭，真实服务器将离线，状态灯将是纯蓝色。你也可以通过浏览导航>监控>状态部分来查看这些连接。
离线	所有被设置为 "离线 "的真实服务器将立即下线，不会收到任何流量。

待机	所有设置为待机的真实服务器将保持离线，直到**所有**在线组的服务器不能通过其服务器健康监控检查。当这种情况发生时，流量将由待机组按照负载平衡策略接收。如果在线组中的一个服务器通过了服务器健康监控检查，这个在线服务器将接收所有的流量，而待机组将停止接收流量。

IP地址

这个字段是你的Real服务器的IP地址。例如 "192.168.1.200"。

港口

Real服务器为服务监听的TCP或UDP端口号。例如 "80 "用于网络流量。

重量

当有一个适当的负载平衡策略被指定时，这一栏将成为可编辑的。

真实服务器 的默认权重是100，你可以输入1-100的值。100的值意味着最大负荷，1意味着最小负荷。

三个服务器的例子可能看起来像这样。

- 服务器1重量=100
- 服务器2重量=50
- 服务器3重量=50

如果我们考虑负载平衡策略被设置为最小连接，并且共有200个客户连接。

- 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Round
Robin作为负载平衡方法，在负载平衡的服务器组中轮换请求，改变权重会影响服务器被选为目标的频率。

如果我们认为最快的负载平衡策略使用最短的时间来获取响应，调整权重会改变偏向，类似于最小连接。

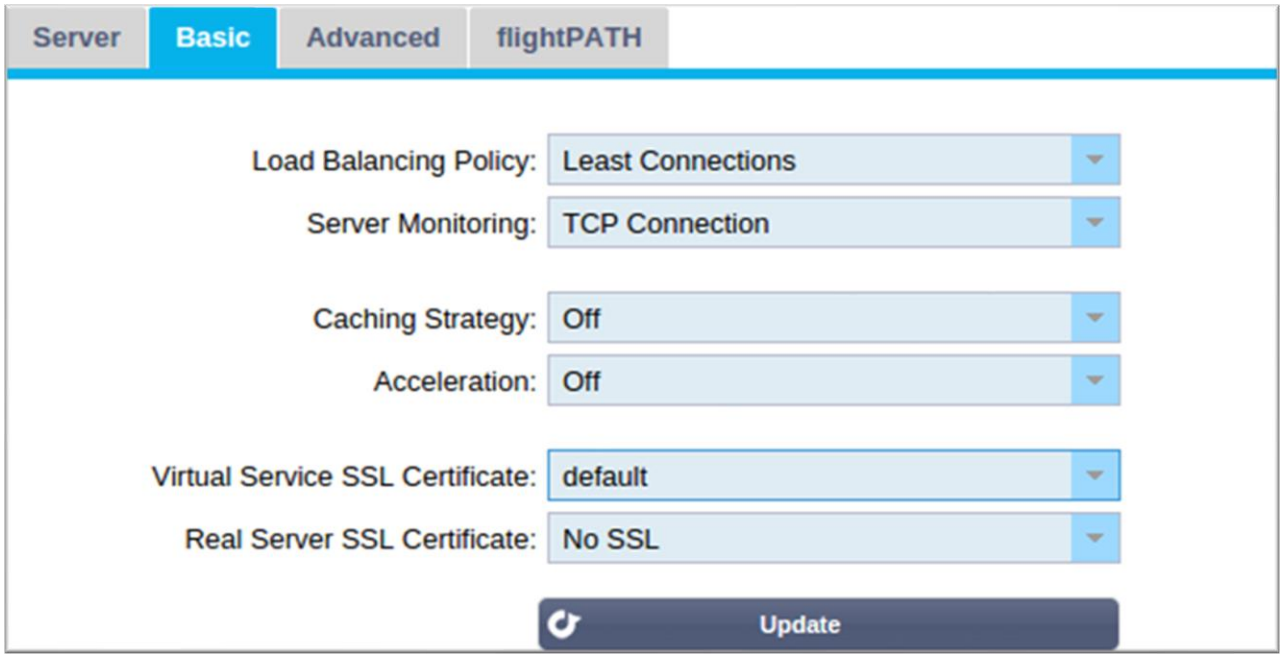
计算出的重量

每个服务器的计算权重可以动态查看，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加权。

笔记

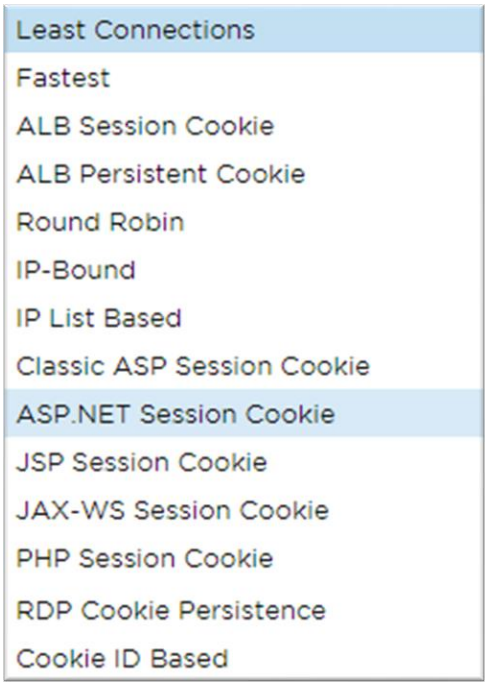
在 "注释 "栏中输入任何有助于描述所定义条目的特殊注释。例如 "IIS Server1 - London DC"。

基本



负载平衡政策

下拉列表显示了当前支持的可使用的负载平衡策略。下面是负载平衡策略的清单，以及解释。



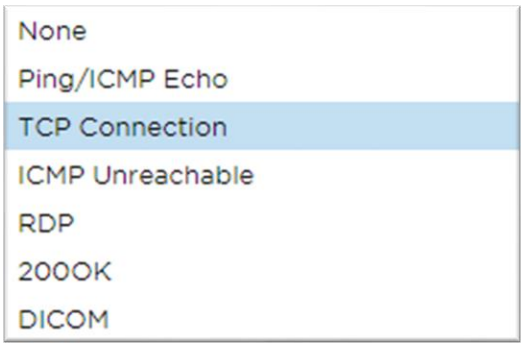
选项	描述
最快的	最快的负载均衡策略自动计算每台服务器所有请求的响应时间，并对时间进行平滑处理。计算权重栏包含自动计算的值。只有在使用这个负载平衡策略时，才可以手动输入。
循环赛	Round Robin通常用于防火墙和基本的负载平衡器，是最简单的方法。每个真实服务器依次接收一个新的

	请求。这种方法只有在你需要均匀地对服务器进行负载平衡的时候才合适；一个例子是查询网络服务器。然而，当你需要根据应用负载或服务器负载进行负载平衡时，甚至需要确保你在会话中使用同一台服务器时，Round Robin方法就不合适了。
最少的连接	负载平衡器将跟踪每个Real服务器的当前连接数。连接数最少的Real服务器会收到后续的新请求。
第三层会话亲和性/持久性--IP绑定	在这种模式下，客户的IP地址构成了选择哪个Real服务器将接收请求的基础。这个动作提供了持久性。HTTP和第4层协议可以使用这种模式。这种方法对于网络拓扑结构已知的内部网络很有帮助，而且你可以确信上游没有 "超级代理"。有了第四层和代理，所有的请求看起来都像是来自一个客户端，因此，负载不会是均匀的。有了HTTP，头信息（X-Forwarder-For）在出现时被用来应对代理。
第三层会话亲和性/持久性 - 基于IP列表	与Real服务器的连接使用 "最小连接 "启动，然后根据客户的IP地址实现会话亲和性。默认情况下，列表保持2小时，但这可以用jetPACK来改变。
第7层会话亲和性/持久性--ALB会话Cookie	这种模式是HTTP负载均衡中最流行的持久性方法。在这种模式下，ADC对每个第一个请求使用基于IP列表的负载均衡。它在第一个HTTP响应的头文件中插入一个cookie。此后，ADC使用客户端cookie将流量路由到同一后端服务器。当客户端每次都需要去同一个后端服务器时，这个cookie被用于持久性。一旦会话关闭，该cookie就会过期。
第7层会话亲和性/持久性 - ALB持久性Cookie	基于IP列表的负载平衡模式用于每个第一次请求。ADC在第一个HTTP响应的头文件中插入一个cookie。此后，ADC使用客户端cookie将流量路由到同一后端服务器。当客户端每次都必须去同一个后端服务器时，这个cookie用于持久性。该cookie将在2小时后过期，并且连接将根据基于IP列表的算法进行负载平衡。这个过期时间可通过jetPACK进行配置。
Session Cookie - 经典ASP Session Cookie	Active Server Pages（ASP）是微软的一项服务器端技术。选择这个选项后，如果检测到ASP cookie并在其已知的cookie列表中找到，ADC将保持会话持久性到同一服务器。在检测到一个新的ASP cookie时，它将使用最小连接算法进行负载平衡。
Session Cookie - ASP.NET	这种模式适用于**ASP.net。**选择这种模式后，如果检测到ASP.NET cookie并在其已知cookie列表中找到，ADC将保持对同一服务器的会话持久性。在检测到一个新的ASP cookie时，它将使用最小连接算法进行负载平衡。

Session Cookie	
Session Cookie - JSP Session Cookie	Java服务器页面（JSP）是一种Oracle服务器端技术。选择这种模式后，如果检测到一个JSP cookie并在其已知的cookie列表中找到，ADC将保持对同一服务器的会话持久性。在检测到一个新的JSP cookie时，它将使用最小连接算法进行负载平衡。
Session Cookie - JAX-WS Session Cookie	Java网络服务（JAX-WS）是一项Oracle服务器端技术。选择这种模式后，如果检测到JAX-WS cookie并在其已知cookie列表中找到，ADC将保持对同一服务器的会话持久性。在检测到一个新的JAX-WS cookie时，它将使用最小连接算法进行负载平衡。
Session Cookie--PHP Session Cookie	个人主页（PHP）是一种开源的服务器端技术。选择这种模式后，当检测到PHP cookie时，ADC将保持会话持久性到同一服务器。
Session Cookie - RDP Cookie的持久性	这种负载平衡方法使用微软创建的基于用户名/域名的RDP Cookie来提供对服务器的持久性。这种方法的优点是，即使客户端的IP地址发生变化，也可以保持与服务器的连接。
基于Cookie-ID	一个非常像 "PhpCookieBased "和其他负载平衡方法的新方法，但使用CookieIDBased和cookie RegEx h=[^;]+ 这个方法将使用Real Server的注释字段 "ID=X; "中设置的值作为cookie值来识别服务器。因此，这意味着它是一种类似于CookieListBased的方法，但使用不同的cookie名称，并存储一个独特的cookie值，不是加扰的IP，而是来自真实服务器的ID（在加载时读入。 默认值是CookieIDName="h"；但是，如果在虚拟服务器的高级设置配置中有一个覆盖值，就用这个值代替。**注意**：如果设置了这个值，我们会覆盖上面的cookie表达式，用新的值替换h=。 最后一点是，如果一个未知的cookie值到达并与真实服务器ID之一相匹配，就应该选择该服务器；否则，使用下一个方法（委托。

服务器监控

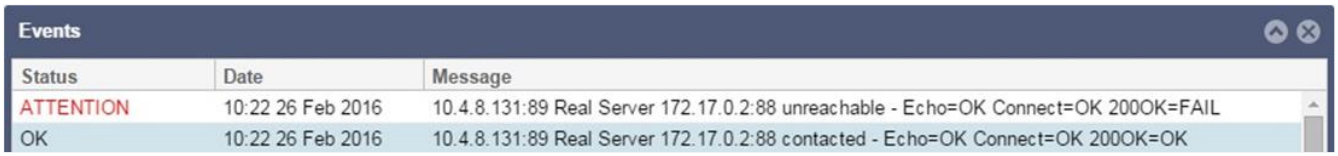
你的ADC包含以下六个标准的真实服务器监控方法。



选择你希望应用于虚拟服务（VIP）的监控方法。

为服务选择正确的监视器是至关重要的。例如，如果Real服务器是一个RDP服务器，那么200OK监视器就没有意义。如果你不确定该选择哪个监视器，默认的TCP连接是一个很好的开始。

你可以选择多个监视器，依次点击你想应用于服务的每个监视器。选定的监视器按照你选择的顺序执行；因此先从低层的监视器开始。例如，设置监视器Ping/ICMP Echo、TCP连接和200OK将在仪表板事件中显示，如下图所示。



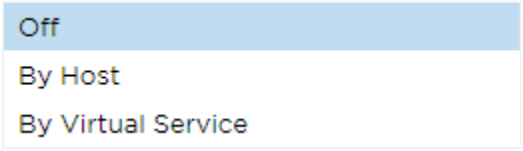
如果我们看最上面一行，我们可以看到第三层Ping和第四层TCP连接已经成功，但是第七层200OK却失败了。这些监测结果提供了足够的信息，表明路由没有问题，并且有一个服务在相关的端口上运行，但是网站没有对请求的页面做出正确的响应。现在是时候看一下网站服务器和库>真实服务器监控部分，看看失败的监控的细节。

选项	描述
无	在这种模式下，Real服务器不被监控，并且总是正确地启动和运行。无设置对于监控使服务器不安的情况和不应该加入ADC的故障转移行动的服务是有帮助的。它是托管不可靠的或遗留的系统的路线，这些系统对H/A操作并不主要。对任何服务类型使用这种监控方法。
平/ICMP回声	在这种模式下，ADC向内容服务器的IP发送一个ICMP回波请求。如果收到一个有效的回波响应，ADC认为真实服务器已经启动并运行，到服务器的流量吞吐量继续。它还会在H/A对上保持服务的可用性。这种监控方法可用于任何服务类型。
TCP连接	在这种模式下，一个TCP连接被建立到Real服务器上，并立即中断，不发送任何数据。如果连接成功，ADC就认为Real服务器已经启动并运行。这种监控方法可用于任何服务类型。UDP服务是目前唯一不适合于TCP连接监控的服务。
ICMP无法到	ADC将向服务器发送一个UDP健康检查，如果它收到一个ICMP端口不可达消息，就将Real服务器标记为不可用。当你需要检查服务器上的UDP服务端口是否可用时，这种方法会很有帮助，例如DNS端

达	口53。
RDP	在这种模式下，一个TCP连接初始化，就像ICMP不可到达方法中解释的那样。在连接初始化之后，请求一个第7层的RDP连接。如果该连接被确认，ADC认为Real服务器已经启动并运行。这种监控方法可用于任何微软终端服务器。
200 OK	在这种方法中，一个TCP连接初始化到Real服务器上。连接成功后，ADC向Real Server发送一个HTTP请求。等待一个HTTP响应并检查 "200 OK "响应代码。如果收到 "200 OK "响应代码，ADC认为Real Server已经启动并运行。如果ADC由于任何原因没有收到 "200 OK "响应代码，包括超时、连接失败和其他原因，ADC会将Real Server标记为不可用。这种监控方法只适用于HTTP和加速的HTTP服务类型。如果HTTP服务器使用的是第4层服务类型，如果SSL没有在真实服务器上使用，或者被 "内容SSL "设施适当处理，它是可以使用的。
DICOM	一个TCP连接在DICOM模式下初始化到Real服务器，并在连接时向Real服务器提出Echoscu "关联请求"。包括来自内容服务器的 "关联接受 "的对话，少量数据的传输，然后是 "释放请求 "和 "释放响应"，成功地结束了监测。如果由于任何原因，监控没有成功完成，那么真实服务器将被视为停机。
用户定义的	任何在真实服务器监控部分配置的监视器都会出现在列表中。

缓存策略

默认情况下，缓存策略是禁用的，设置为关闭。如果你的服务类型是HTTP，那么你可以应用两种类型的缓存策略。



请参考配置缓存页面来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，压缩的对象不会被缓存。

选项	描述
作者：主持人	每个主机的缓存是基于每个主机名的应用。每个域名/主机名会有一个单独的缓存。这种模式对于可以根据域名为多个网站提供服务的网络服务器来说非常理想。
通过虚拟服务	当你选择这个选项时，每个虚拟服务的缓存是可用的。对于通过虚拟服务的所有域名/主机名，将只存在一个缓存。这个选项是一个专业设置，用于一个网站的多个克隆。

加速

选项	描述
关闭	关闭虚拟服务的压缩功能
压缩	当选择时，该选项开启了对所选虚拟服务的压缩。ADC会根据请求动态地压缩数据流到客户端。这个过程只适用于包含content-encoding: gzip头的对象。示例内容包括HTML、CSS或Javascript。你也可以使用 "全局排除 "部分排除某些内容类型。

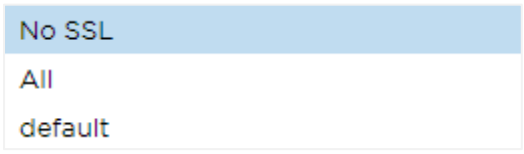
注意：如果对象是可缓存的，ADC将存储一个压缩的版本，并静态地（从内存中）提供这个版本，直到内容过期并重新验证。

虚拟服务SSL证书（客户端和ADC之间的加密）。

默认情况下，设置为无SSL。如果你的服务类型是 "HTTP "或 "Layer4 TCP"，你可以从下拉菜单中选择一个证书来应用于虚拟服务。已经创建或导入的证书将出现在这个列表中。你可以高亮显示多个证书以应用于一个服务。该操作将自动启用SNI扩展，以允许基于客户要求的 "域名"的证书。

服务器名称指示

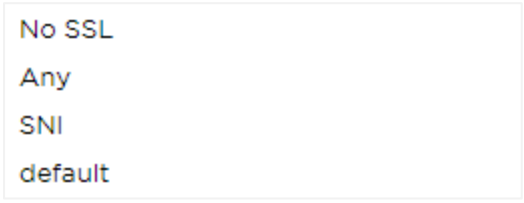
这个选项是对TLS网络协议的一个扩展，使用它，客户端在握手过程开始时表明它试图连接到什么主机名。这个设置允许ADC在同一个虚拟IP地址和TCP端口上展示多个证书。



选项	描述
没有SSL	从源头到ADC的流量是不加密的。
默认情况下	该选项的结果是将本地创建的名为 "默认 "的证书应用到通道的浏览器端。当没有创建或导入SSL时，使用该选项来测试SSL。
用户导入的SSL证书	你已经导入ADC的任何证书都将显示在这里。

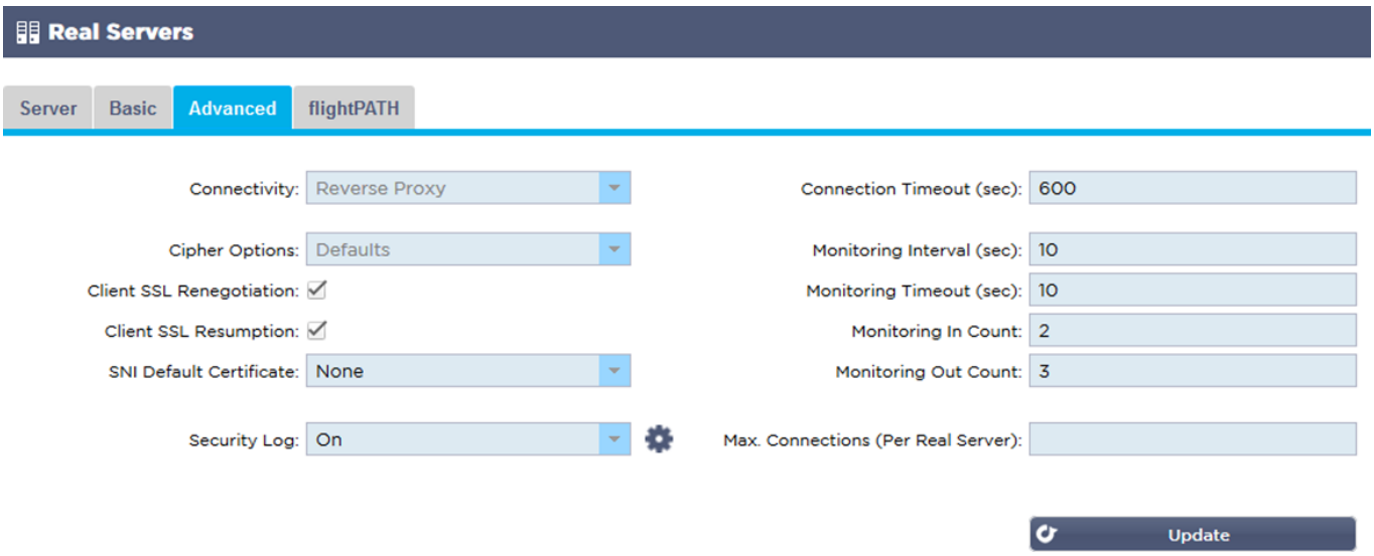
真实服务器SSL证书（ADC和真实服务器之间的加密）。

该选项的默认设置是无SSL。如果你的服务器需要一个加密连接，这个值必须是No SSL以外的其他值。已经创建或导入的证书将出现在这个列表中。



选项	描述
没有SSL	从ADC到真实服务器的流量是不加密的。在浏览器端选择证书意味着可以在客户端选择"无SSL "来提供所谓的 "SSL卸载"。
任何	ADC作为一个客户，将接受Real Server提供的任何证书。当选择该选项时，从ADC到真实服务器的流量是加密的。当在虚拟服务端指定一个证书时，使用 "任何 "选项，提供所谓的 "SSL桥接 "或 "SSL再加密"。
SNI	ADC作为一个客户，将接受Real Server提供的任何证书。如果选择了这个选项，从ADC到真实服务器的流量是加密的。当在虚拟服务端指定一个证书时，使用 "任何 "选项，提供所谓的 "SSL桥接 "或 "SSL再加密"。选择该选项可以在服务器端启用SNI。
用户导入的SSL证书	你已经导入ADC的任何证书都会出现在这里。

高级



连接性

你的虚拟服务可以配置四种不同的连接方式。请选择适用于该服务的连接模式。

选项	描述
反向代理	反向代理是默认值，在第七层工作，有压缩和缓存。而在第四层则没有缓存或压缩。在这种模式下

	，你的ADC作为一个反向代理，成为真实服务器看到的源地址。
直接服务器返回	直接服务器返回或DSR（在某些圈子里称为DR-直接路由）允许负载均衡器后面的服务器绕过响应的ADC直接响应客户端。DSR只适合用于第4层的负载平衡。因此，选择这个选项时，缓存和压缩是不可用的。 第7层的负载平衡不能与这个DSR一起工作。另外，除了基于IP列表外，没有持久性支持。用这种方法进行SSL/TLS负载均衡并不理想，因为源IP持久性支持是唯一可用的类型。DSR还需要对Real Server进行修改。请参考真实服务器变更部分。
闸门	网关模式允许你通过ADC路由所有流量，允许来自Real Servers的流量通过ADC的虚拟机或硬件接口被路由到其他网络。在多接口模式下运行时，将该设备作为Real服务器的网关设备是非常理想的。 使用这种方法的第7层负载平衡不起作用，因为除了基于IP列表外，没有持久性支持。这种方法要求Real服务器将其默认网关设置为ADC的本地接口地址（eth0、eth1等）。请参考Real Server变更部分。

密码选项

你可以在每个服务层面设置密码，这只与启用了SSL/TLS的服务有关。ADC执行密码的自动选择，您可以使用jetPACKS添加不同的密码。在添加适当的jetPACK时，你可以设置每个服务的密码选项。这样做的好处是，你可以创建几个具有不同安全水平的服务。请注意，旧的客户端与新的密码不兼容，以减少客户端的数量，服务越安全。

客户端SSL重新协商

如果你希望允许客户端发起的SSL重新协商，请勾选此框。禁用客户端SSL重新协商，以防止任何可能的针对SSL层的DDOS攻击，取消勾选该选项。

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。当客户提出重新使用一个会话时，服务器将尝试重新使用这个会话（如果找到的话）。如果不勾选恢复，客户端或服务器的会话缓存就不会发生。

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将呈现SNI默认证书。这方面的默认设置是
"无"，如果没有完全匹配，将有效地放弃连接。从下拉菜单中选择任何已安装的证书，以便在准确的SSL证书匹配失败时呈现。

安全日志

开
"是默认值，是在每个服务的基础上，启用将认证信息记录到W3C日志的服务。点击Cog图标将带你到系统>日志页面，在那里你可以检查W3C日志的设置。

连接超时

默认的连接超时是600秒或10分钟。这个设置将调整连接在没有活动时超时的时间。对于短暂的无状态网络流量，即通常为90秒或更短的时间，减少这个时间。对于有状态的连接，如RDP，将这个数字增加到7200秒（2小时）或更多，取决于你的基础设施。RDP超时的例子意味着，如果用户有一个2小时或更短的不活动期，连接将保持开放。

监测设置

这些设置与基本选项卡中的真实服务器监控器有关。配置中有一些全局条目，用来计算在服务器状态被标记为在线或失败之前成功或失败的监控次数。

间隔

间隔是指显示器之间的时间，单位是秒。默认的时间间隔是1秒。虽然1秒对大多数应用来说是可以接受的，但对其他应用或在测试期间增加这个时间可能是有益的。

监测超时

超时值是指ADC将等待服务器响应连接请求的时间。默认值是2s。对于繁忙的服务器，增加这个值。

监测计数

这个设置的默认值是2，值为2表示Real服务器在上线前必须通过两次成功的健康监控检查。增加这个数字将增加服务器可以提供流量的概率，但需要更长的时间来投入服务，这取决于间隔时间。降低这个数值将使你的服务器更快进入服务状态。

监测出数

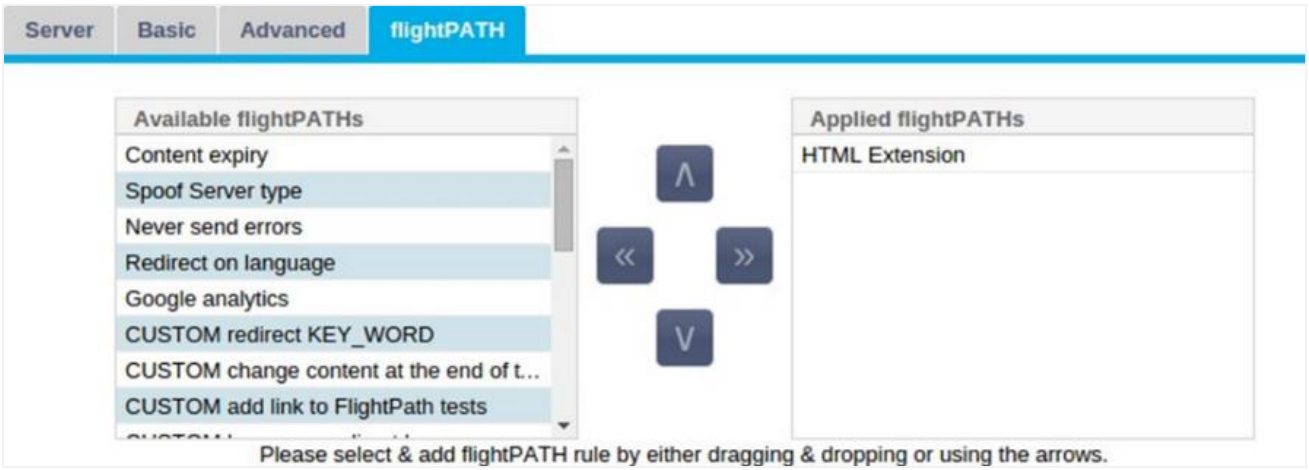
这个设置的默认值是3，意味着Real服务器监控必须失败三次，ADC才会停止向该服务器发送流量，并将其标记为红色和不可达。增加这个数字将导致更好和更可靠的服务，代价是ADC停止向该服务器发送流量的时间。

最大。连接方式

限制Real服务器的并发连接数，按服务设置。例如，如果你将其配置为1000，并且有两个Real Server，ADC就将每个Real Server限制为1000个并发连接。你也可以选择在所有服务器达到这个限制时，显示一个 "服务器太忙

"的页面，帮助用户了解为什么会出现任何不响应或延迟。如果是无限制的连接，请将此留空。你在这里设置的内容取决于你的系统资源。

飞行路线



flightPATH是一个由Edgenexus设计的系统，在ADC中独家使用。与其他供应商的基于规则的引擎不同，flightPATH不通过命令行或脚本输入控制台操作。相反，它使用一个GUI来选择不同的参数、条件和行动，以实现他们的需求。这些特点使flightPATH非常强大，允许网络管理员以非常有效的方式操纵HTTPS流量。

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

你可以从上面的图片中看到；左边有一个可用规则的列表，右边是应用于虚拟服务的规则。

添加一个可用的规则，方法是将规则从左边拖到右边，或者突出显示一个规则并点击右边的箭头，将其移到右边。

执行的顺序是至关重要的，从最上面的规则开始，先执行。要改变执行顺序，突出显示规则，用箭头向上和向下移动。

要删除一条规则，可以把它拖回左边的规则清单，或者突出显示该规则并点击左边的箭头。

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

图书馆

附加元件

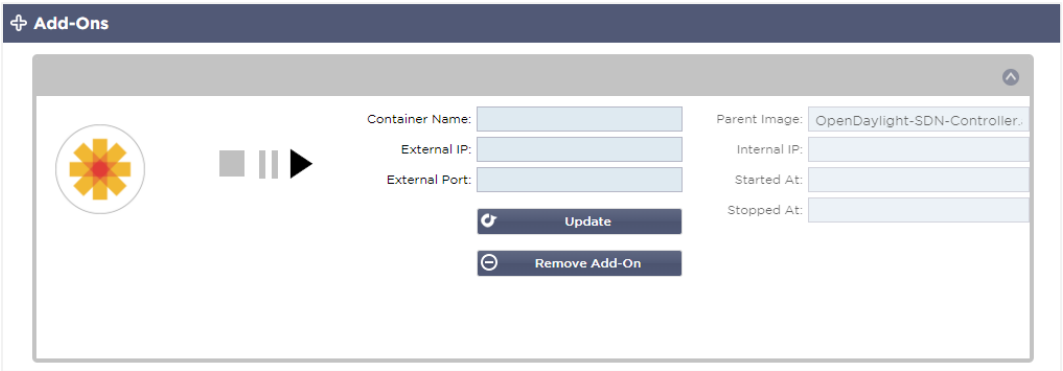
附加组件是基于Docker的容器，可以在ADC中以隔离的模式运行。附加组件的例子可以是一个应用防火墙，甚至是ADC本身的一个微型实例。

应用

附加组件中的应用程序部分详细介绍了你已经购买、下载和部署的应用程序。

如果没有应用程序，该部分将显示一条信息，提示你继续前往应用程序部分，下载并部署一个应用程序。

一旦你部署了一个应用程序，它将出现在应用程序区域。



购买附加组件

要购买一个应用程序，你需要在App Store注册。购买是通过ADC本身进行的。你会发现

导航到ADC仪表板的图书馆>应用程序页面。

在这里，你可以选择你想要下载的应用程序，然后进行安装。

如果你是在ADC仪表板上做这个，请只选择1个项目。你可能拥有多个ADC集，而应用程序需要与部署在其上的ADC关联。

如果你通过你的桌面和浏览器访问App Store，你可以下载你想要的数量。例如，WAF或GSLB的四个实例。它们将出现在你的ADC的已购应用程序区域，以便你可以下载它们。

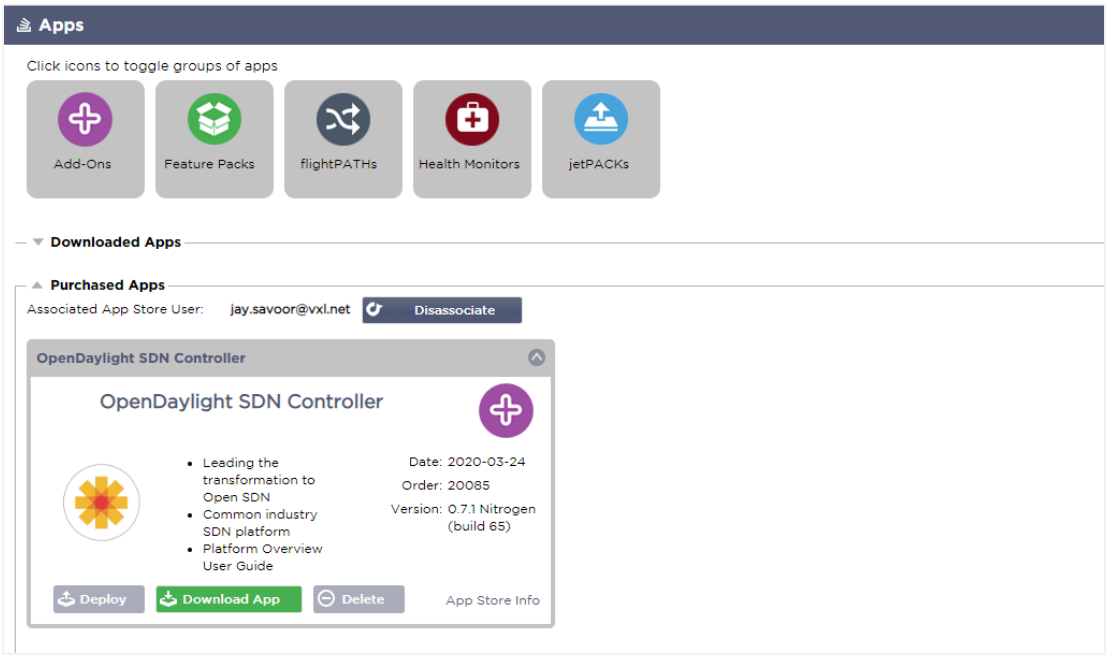
这些应用程序与你拥有并已注册的ADC相关联。

当你选择下载一个应用程序时，你会被要求提供机器ID，随后应用程序会被加密并与ADC机器ID链接。

App Store的链接是。

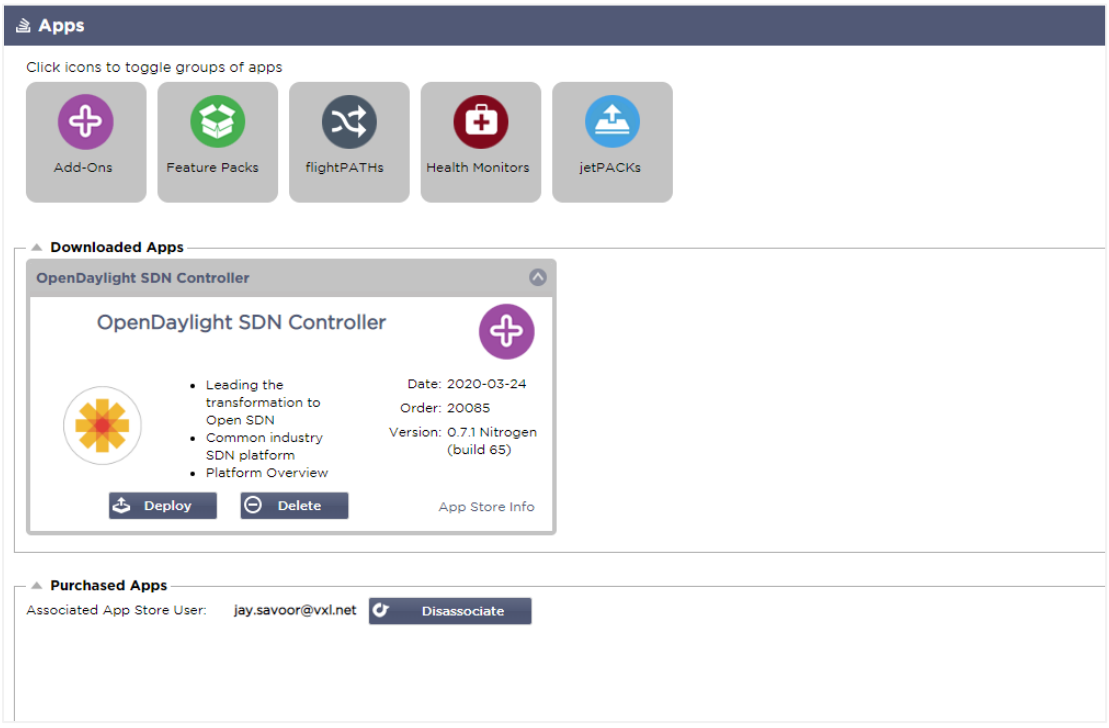
- 附加组件。**HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/。**

- 健康监测器。HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/。
- jetPACKS: HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/
- 功能包。HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/。
- flightPATH规则。HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/。
- 软件更新。HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/。



部署一个应用程序

一旦下载到ADC，该应用程序将被移到下载的应用程序部分，并使用部署按钮部署到ADC。这个过程需要一些时间，取决于ADC的可用资源。一旦部署，它将出现在下载的应用程序部分。



认证

库 >

认证页面允许你设置认证服务器并创建认证规则，有客户端Basic或Forms和服务器端NTLM或BASIC选项。

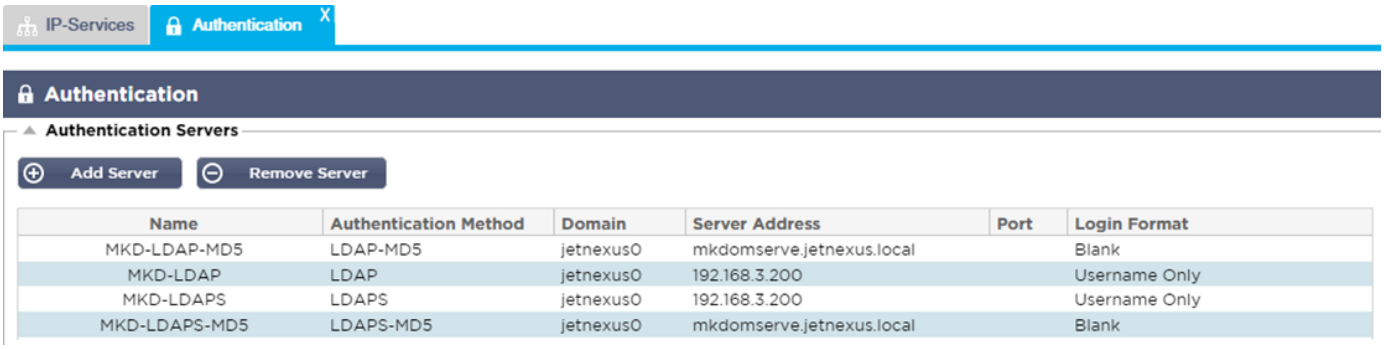
设置认证--一个工作流程

请至少执行以下步骤，将认证应用于你的服务。

1. 创建一个认证服务器。
2. 创建一个使用认证服务器的认证规则。
3. 创建一个使用认证规则的flightPATH规则。
4. 将flightPATH规则应用于一个服务

认证服务器

为了建立一个有效的认证方法，我们必须首先建立一个认证服务器。



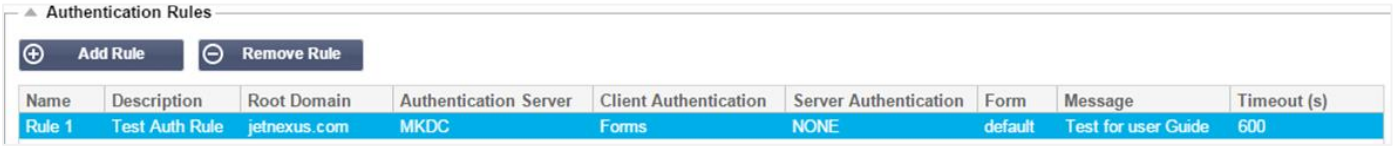
- 点击添加服务器按钮。
- 这个动作将产生一个空白行，准备完成。

选项	描述
命名	给你的服务器起个名字，以便于识别 - 这个名字在规则中使用
描述	添加描述
认证方法	选择一个认证方法 LDAP - 基本的LDAP，用户名和密码以明文形式发送到LDAP服务器。 LDAP-MD5 - 基本的LDAP，用户名为明文，密码为MD5散列以提高安全性。 LDAPS - LDAP over SSL。在ADC和LDAP服务器之间的加密隧道内，以明文形式发送密码。 LDAPS-MD5 - LDAP over SSL。在ADC和LDAP服务器之间的加密隧道中，密码是经过MD5散列的，以增加安全性。
领域	添加LDAP服务器的域名。
服务器地址	添加认证服务器的IP地址或主机名 LDAP - IPv4地址或主机名。

	LDAP-MD5 - 仅限主机名（IPv4地址不工作）。 LDAPS - IPv4地址或主机名。 LDAPS-MD5 - 只有主机名（IPv4地址不起作用）。
港口	默认情况下，为LDAP使用389端口，为LDAPS使用636端口。不需要为LDAP和LDAPS添加端口号。当其他方法可用时，你将能够在这里配置它们
搜索条件	搜索条件必须符合RFC 4515的规定。例子。 (MemberOf=CN=Phon- VPN,CN=Users,DC=mycompany,DC=local)。
搜索基地	这个值是在LDAP数据库中搜索的起点。 例子 *dc=mycompany,dc=local*
登录格式	使用你需要的登录格式。 用户名 - 选择这种格式后，你只需要输入用户名。用户输入的任何用户和域名信息都会被删除，而使用来自服务器的域名信息。 用户名和域 - 用户必须输入整个域和用户名的语法。例如：*mycompany\gchristie OR someone@mycompany*。在服务器一级输入的域名信息被忽略。 空白 - ADC将接受用户输入的任何信息，并将其发送到认证服务器。这个选项在使用MD5时使用。
密码锁	在这个版本中没有使用这个选项。
死亡时间	本版本中未使用

认证规则

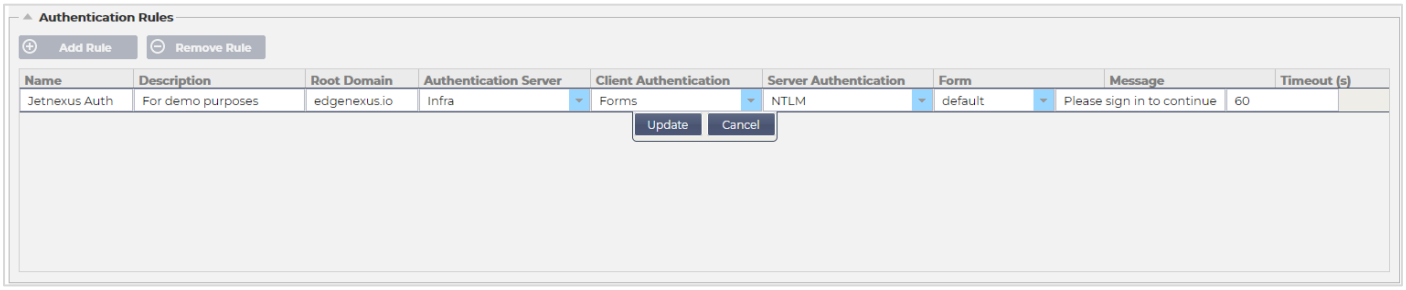
下一个阶段是创建认证规则，供服务器定义使用。



场地	**描述**
命名	为你的认证规则添加一个合适的名称。
描述	添加一个合适的描述。
根域	除非你需要跨子域的单点登录，否则这个选项必须留空。
认证服务器	这是一个下拉框，包含你已经配置的服务器。
客户端认证。	选择适合你的需求的价值。 基本（401）--该方法使用标准的401认证方法 表格 - 这将向用户展示ADC的默认表格。在表格中，你可以添加一条信息。你可以选择一个你已经上传的表格，使用下面的部分。

服务器认证	选择适当的值。 无 - 如果你的服务器没有任何现有的认证，选择此设置。这个设置意味着你可以向以前没有的服务器添加认证能力。 基本 - 如果你的服务器启用了基本认证(401)，那么选择基本。 NTLM - 如果你的服务器启用了NTLM认证，那么选择NTLM。
形状	选择适当的值 默认 - 选择该选项将导致ADC使用其内置形式。 自定义 - 你可以添加一个你所设计的表格，并在这里选择它。
留言	在表格中添加一条个人信息。
超时	在规则中添加一个超时，超时后用户需要再次进行认证。注意超时设置只对基于表单的认证有效。

单点登录



如果你希望为用户提供单点登录，请在根域名一栏中填写你的域名。在这个例子中，我们使用了edgenexus.io。我们现在可以有多个服务将使用edgenexus.io作为根域，而你只需要登录一次。如果我们考虑以下服务。

- 分享点.mycompany.com
- usercentral.mycompany.com
- appstore.mycompany.com

这些服务可以驻留在一个VIP上，也可以分布在三个VIP上。用户第一次访问usercentral.mycompany.com时，会看到一个表格，要求他们根据使用的认证规则登录。然后，同一个用户可以连接到appstore.mycompany.com，并将被ADC自动认证。你可以设置超时，一旦达到这个非活动期，将强制认证。

表格

本节将使你能够上传一个自定义表单。

如何创建你的自定义表格

尽管ADC提供的基本表格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。你可以创建你的自定义表格，在这种情况下，用户将被要求填写。这个表格必须是HTM或HTML格式。

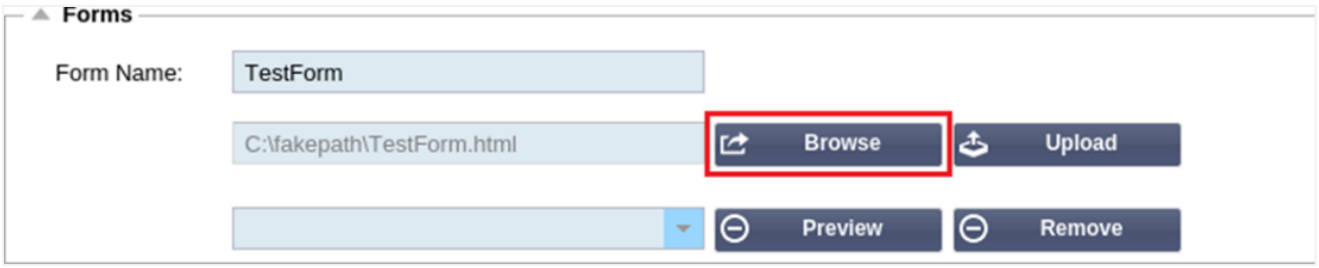
选项	描述
命名	表单名称 = loginform 行动=%JNURL% 方法 = POST
帐号	语法：name = "JNUSER"
密码。	名称="JNPASS"
可选信息1。	%JNMESSAGE%。
可选信息2。	%jnauthmessage%。
图片	如果你想添加图片，那么请使用Base64编码在行内添加它。

一个非常基本和简单的表格的HTML代码示例

```
<HTML>
<开头>
<title>示例认证表格</title>。
</HEAD>
<BODY>
%JNMESSAGE%[br>
<form name="loginform" action="%JNURL%" method="post"> USER: <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>
```

添加一个自定义表单

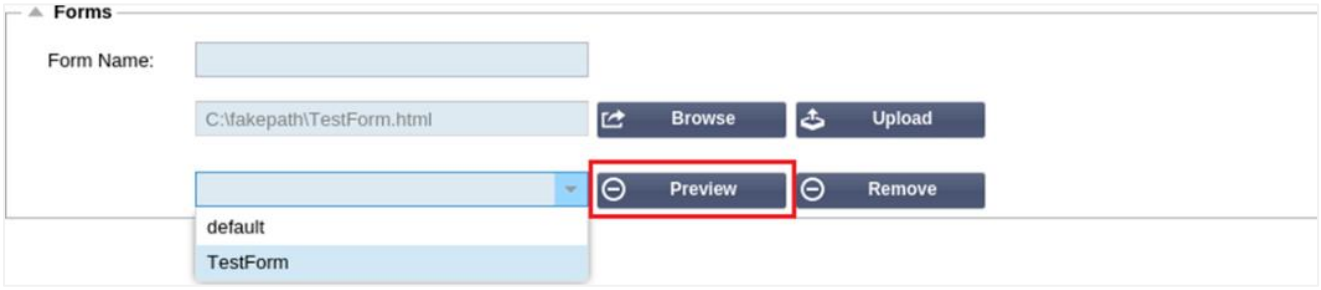
一旦你创建了一个自定义表单，你可以使用表单部分来添加它。



1. 为你的表格选择一个名称
2. 在本地浏览您的表格
3. 点击上传

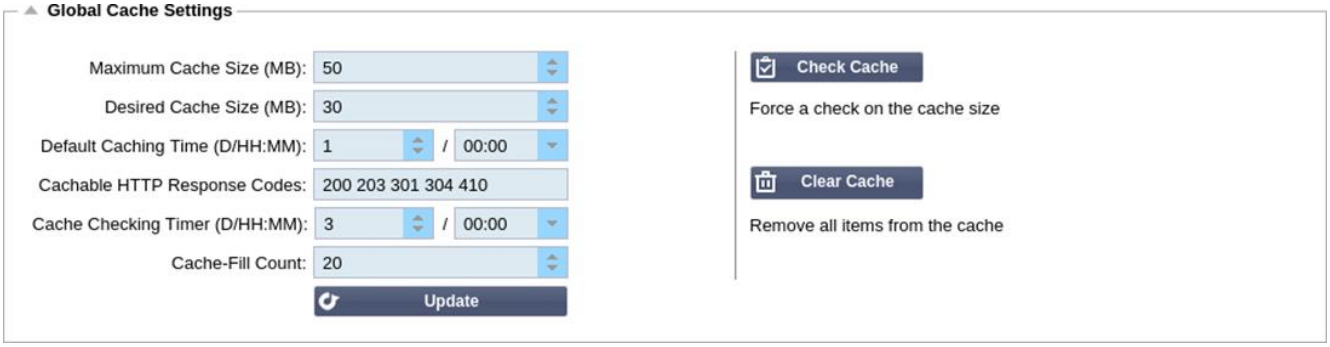
预览你的自定义表格

要查看你刚上传的自定义表格，你要选择它并点击预览。你也可以用这个部分来删除不再需要的表格。



缓存

ADC能够在其内部存储器中缓存数据，并定期将此缓存刷新到ADC的内部存储器中。管理这一功能的设置在本节中提供。



全局缓存设置

最大缓存大小（MB

这个值决定了Cache可以消耗的最大RAM。ADC缓存是一个内存中的缓存，也会定期刷新到存储介质中，以保持重启、重启和关机操作后的缓存持久性。这种功能意味着最大的缓存大小必须适合设备的内存空间（而不是磁盘空间），并且不应超过可用内存的一半。

希望的缓存大小（MB

这个值表示最佳的RAM，Cache将被修剪到这个值。虽然最大的缓存容量代表了缓存的绝对上界，但期望的缓存容量是指每当自动或手动检查缓存容量时，缓存应该尝试达到的最佳容量。最大缓存大小和期望缓存大小之间的差距是为了适应在定期检查缓存大小以裁减过期内容之间新内容的到来和重叠。再一次，接受默认值（30MB）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（D/HH:MM）。

这里输入的值代表没有明确过期值的内容的寿命。默认的缓存时间是指在流量头中没有 "不存储 "指令或明确过期时间的内容被存储的时间。

该字段的输入形式为 "D/HH:MM" - 所以输入
"1/01:01"（默认为1/00:00）意味着存储ADC将保持一天的内容，"01:00 "为一小时，"00:01 "为一分钟。

可缓存的HTTP响应代码

缓存的数据集之一是HTTP响应。缓存的HTTP响应代码是：。

- 200 - 成功的HTTP请求的标准响应
- 203 - 标题不是确定的，而是从本地或第三方的副本中收集的。
- 301 - 所请求的资源已经被分配了一个新的永久URL
- 304 - 自上次请求后未修改，应使用本地缓存的副本。
- 410 - 资源在服务器上不再可用，并且没有转发地址。

这个字段应该谨慎编辑，因为最常见的可缓存的响应代码已经被列出。

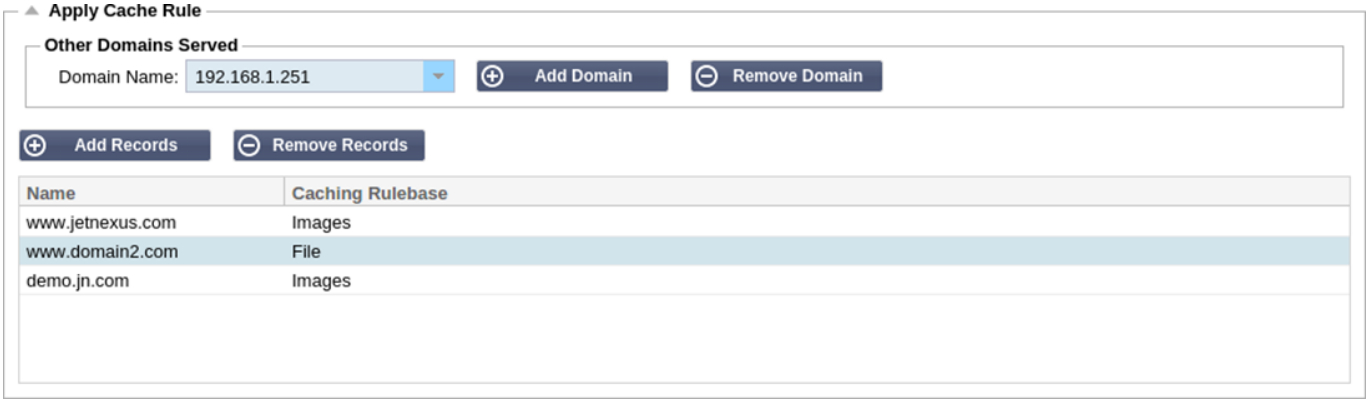
缓存检查时间（D/HH:MM）。

这个设置决定了缓存修剪操作的时间间隔。

缓存填充计数

这个设置是一个辅助工具，当检测到一定数量的304时，帮助填充缓存。

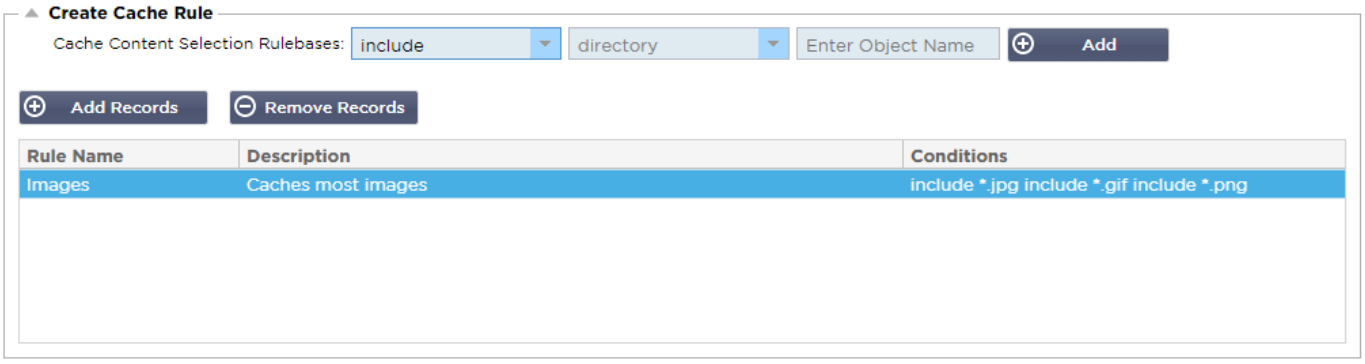
应用缓存规则



本节允许你对一个域应用缓存规则。

- 用 "添加记录
  "按钮手动添加域名。你必须使用一个完全合格的域名或一个点阵十进制的IP地址。例如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。
- 只要流量通过了虚拟服务，并且缓存策略已经应用于虚拟服务，该列表就会被填充。
- 通过双击缓存规则库列并从列表中选择你的缓存规则

创建缓存规则



这一部分允许你创建几个不同的缓存规则，然后可以应用于一个域。

- 点击添加记录，给你的规则一个名称和描述
- 你可以手动键入你的条件，或者使用 "添加条件"。

要使用选择规则库添加一个条件。

- 选择包括或不包括
- 选择所有JPEG图像
- 点击+添加符号
- 你会看到，"包括*.jpg "现在已经被添加到条件中。
- 你可以添加更多的条件。如果你选择手动操作，你需要在新的一行中添加每个条件。请注意，你的规则将显示在同一行，直到你点击条件框，然后它们将显示在一个单独的行中。

飞行路线

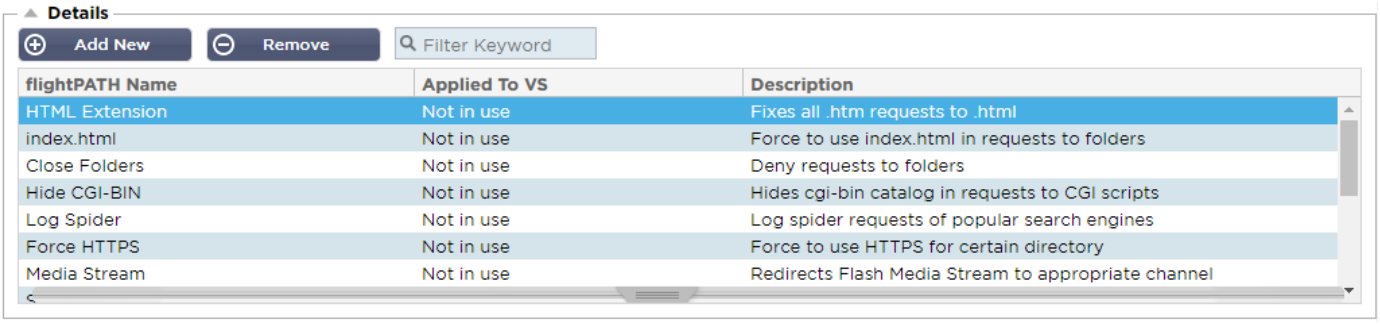
flightPATH是ADC内置的流量管理技术。flightPATH允许你实时检查HTTP和HTTPS流量，并根据条件执行行动。

在规则中使用IP对象时，flightPATH规则必须应用于VIP。

一个飞行路径规则由四个要素组成。

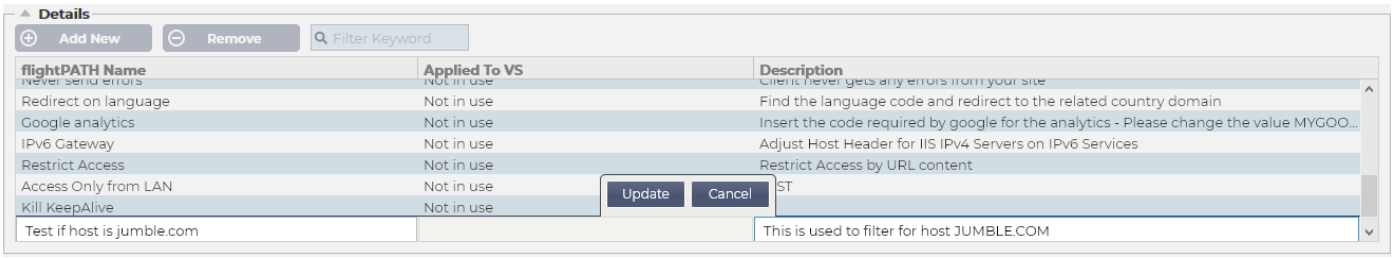
1. 详细信息，在这里你可以定义flightPATH名称和它所连接的服务。
2. 可以定义的导致规则被触发的条件。
3. 评价，允许定义可在行动中使用的变量。
4. 用于管理满足条件时应发生的事情的行动

详细内容



细节部分显示了可用的flightPATH规则。你可以在这部分添加新的flightPATH规则和删除已定义的规则。

添加一个新的flightPATH规则



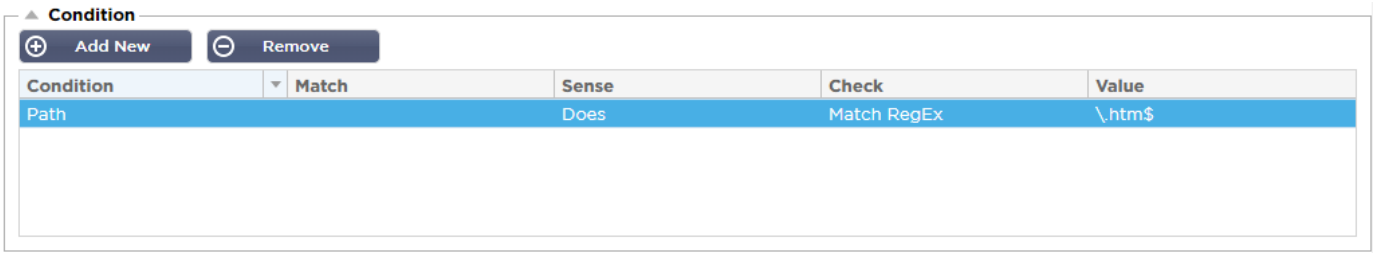
场地	描述
飞行路线名称	这个字段是为flightPATH规则命名的。你在这里提供的名称会出现在ADC的其他部分并被引用。
适用于VS	这一栏是只读的，显示应用flightPATH规则的VIP。
描述	代表为可读性而提供的描述的值。

添加flightPATH规则的步骤

1. 首先，点击位于细节部分的添加新按钮。
2. 为你的规则输入一个名称。例子 Auth2
3. 输入对你的规则的描述
4. 一旦规则被应用到一个服务上，你会看到应用到一栏自动填充了一个IP地址和端口值
5. 不要忘记点击 "更新 "按钮来保存你的变化，如果你犯了一个错误，只需点击 "取消 "即可恢复到以前的状态。

状况

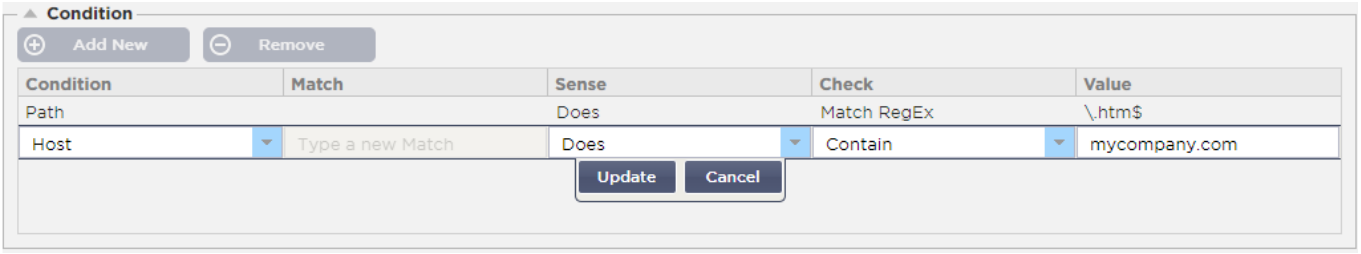
一个flightPATH规则可以有任何数量的条件。这些条件在AND的基础上工作，允许你设置触发行动的条件。如果你想使用OR条件，创建一个额外的flightPATH规则，并以正确的顺序将其应用于VIP。



你也可以通过在Check字段选择Match

RegEx，在Value字段选择RegEx值来使用RegEx。RegEx评估的加入极大地扩展了flightPATH的能力。

创建一个新的flightPATH条件



状况

我们在下拉菜单中提供了几个预定义的条件，涵盖了所有可预见的情况。当新的条件被添加时，这些条件将通过Jetpack的更新来提供。

可供选择的是。

状况	描述	例子
<表格>	HTML表格是用来向服务器传递数据的	例子 "表格没有长度0"
GEO位置	将源IP地址与ISO 3166国家代码相比较	GEO位置等于GB，或GEO位置等于德国
宿主	从URL中提取的主机	www.mywebsite.com 或 192.168.1.1
语言	从HTTP头的语言中提取的语言	这个条件将产生一个带有语言列表的下拉菜单
方法	HTTP方法的下拉菜单	下拉式，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Origin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|为多个IP的。
路径	网站的路径	/mywebsite/index.asp
帖文	POST请求方法	检查正在上传到网站的数据
查询	查询的名称和值，可以接受查询名称，也可以接受一个值	"Best=jetNEXUS"，其中匹配的是Best，值是edgeNEXUS。

查询字符串	在? 字符之后的整个查询字符串	
索取饼干	客户端要求的一个cookie的名称	MS-WSMAN=afYfn1CDqqCDqUD::
请求标题	任何HTTP标头	Referrer, User-Agent, From, Date
要求版本	HTTP版本	http/1.0或http/1.1
回应机构	响应体中的一个用户定义的字符串	服务器升级
响应代码	响应的HTTP代码	200 OK, 304 Not Modified
回应饼干	服务器发送的一个cookie的名称	MS-WSMAN=afYfn1CDqqCDqUD::
响应头	任何HTTP标头	Referrer, User-Agent, From, Date
回复版本	服务器发送的HTTP版本	http/1.0或http/1.1
来源于IP	起源IP，代理服务器IP，或其他一些聚合的IP地址	客户端 IP、代理IP、防火墙IP。也可以使用多个IP和子网。你必须转义点，因为这些是RegEX。例如10\.1\.2\.3是10.1.2.3

匹配

匹配字段可以是下拉式或文本值，可根据条件字段的值来定义。例如，如果Condition被设置为Host，Match字段就不可用。如果条件设置为<form>，则匹配字段显示为文本字段，如果条件为POST，则匹配字段显示为一个包含相关值的下拉式。

可供选择的是。

匹配	描述	例子
接受	可接受的内容类型	接受: text/plain
接受-编码	可接受的编码	Accept-Encoding: <compress | gzip | deflate | sdch | identity >。
接受语言	可接受的回应语言	Accept-Language: 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: bytes

授权书	用于HTTP认证的认证凭证	授权。Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
收费-目的	包含应用所申请方法的费用的账户信息	
内容-编码	使用的编码类型	Content-Encoding: gzip
内容-长度	响应体的长度，单位是八位数（8位字节）。	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: application/x-www-form-urlencoded
饼干	服务器之前用Set-Cookie发送的一个HTTP cookie（如下）。	Cookie: $Version=1; Skin=new;
日期	信息发出的日期和时间	Date = "Date" ":" HTTP-date
ETag	一个资源的特定版本的标识符，通常是一个消息摘要	ETag。"aed6bdb8e090cd1:0"
来自	提出请求的用户的电子邮件地址	来自: user@example.com
如果修改过-自	如果内容没有变化，允许返回304未修改。	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
最后修改时间	请求对象的最后修改日期，格式为RFC 2822	最后修改的。Tue, 15 Nov 1994 12:45:26 GMT
プラグマ	实施。具体的标头，在请求- 响应链的任何地方都可能产生各种影响。	Pragma: no-cache
推荐人	前一个网页的地址，从该网页链接到当前请求的页面。	推荐人: HTTP://www.edgenexus.io
服务器	服务器的一个名称	服务器。Apache/2.4.1 (Unix)
设置参数	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)
不尽相同	告诉下游代理如何匹配未来的请求头，以决定 是否可以使用缓存的响应，而不是 从源服务器 请求一个新的响应。	变化。用户代理
X-Powered-By	指定支持网络应用的技术（如ASP.NET、PHP、JBoss）。	X-Powered-By:PHP/5.4.0

感知

意义字段是一个下拉布尔字段，包含有 "有 "或 "无 "的选择。

检查

检查字段允许设置针对条件的检查值。

可用的选择是。包含, 结束, 平等, 存在, 有长度, 匹配RegEx, 匹配列表, 开始, 超过长度

检查	描述	例子
存在的	这不关心条件的细节，只关心它的存在/不存在。	宿主 - 确实 - 存在
开始	该字符串以 "值 "开始	路径 - Does - Start - /secure
结束	字符串以 "值 "结束。	Path - Does - End - .jpg
包含	该字符串确实包含了价值	请求头 - 接受 - 是否 - 包含 - 图像
平等	字符串确实等于值	主持人--是否--平等-- www.jetnexus.com
有长度	该字符串确实有一个长度的值	主机 - 是否 - 有长度 - 16 www.jetnexus.com = TRUE www.jetnexus.co.uk = FALSE
匹配RegEx	使你能够输入一个完整的与Perl兼容的正则表达式	起始IP - 是否 - 匹配Regex - 10\.* | 11\.*

添加一个条件的步骤

添加一个新的flightPATH条件是非常容易的。上面是一个例子。

1. 点击条件区域内的添加新按钮。
2. 从下拉框中选择一个条件。让我们以主机为例。你也可以在该字段中输入，ADC会在下拉框中显示该值。
3. 选择一种感觉。例如，是否
4. 选择一个检查。例如，包含
5. 选择一个值。例如，mycompany.com

上面的例子表明，有两个条件必须都是 "真"，才能完成规则

- 首先是检查所请求的对象是否是一个图像
- 第二个检查URL中的主机是否为www.imagepool.com

评价

添加可定义变量的能力是一种引人注目的能力。普通的ADC使用脚本或命令行选项来提供这种能力，这对任何人来说都不理想。ADC允许你使用一个易于使用的GUI来定义任何数量的变量，如下所示和描述。

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 - 可能的来源点的下拉列表
- 细节--从下拉菜单中选择数值或手动输入。
- Value - 变量持有的值，可以是一个字母数字值或用于微调的RegEx。

内置变量。

内置变量已经被硬编码，所以你不需要为这些变量创建一个评估条目。

你可以在行动部分使用下面列出的任何变量。

每个变量的解释都在上面的 "条件 "表中。

- 方法=$method$
- 路径 = $path$
- Querystring = $querystring$
- Sourceip = $sourceip$
- 响应代码（文本也包括 "200 OK"）= $resp$
- 主机=$host$
- 版本 = $version$
- 客户端口 = $clientport$
- Clientip = $clientip$
- 地理定位=$geolocation$"

行动	目标
行动 = 重定向 302	目标 = HTTPs://$host$/404.html
行动=记录	目标 = 一个来自$sourceip$:$sourceport$的客户刚刚提出了一个$path$页面请求

解释一下。

- 客户在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，用户被重定向到他们使用的原始主机名，但错误的路径被替换为404.html
- 一个条目被添加到Syslog中说："一个来自154.3.22.14:3454的客户刚刚请求了错误的.html页面"。

行动

这个过程的下一个阶段是添加一个与flightPATH规则和条件相关的行动。

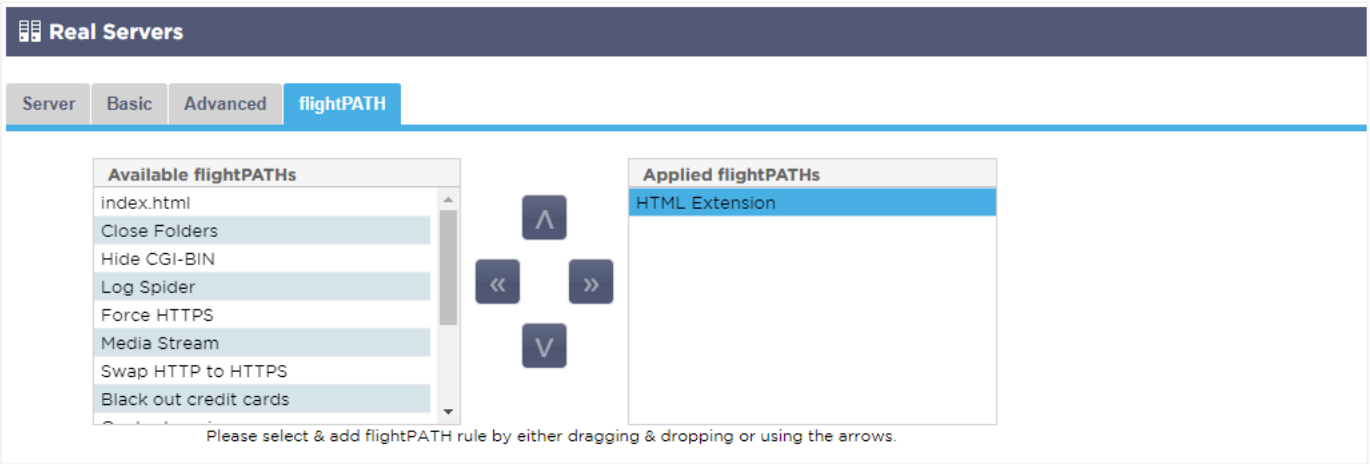
在这个例子中，我们要重写URL的路径部分，以反映用户输入的URL。

- 点击添加新的
- 从行动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

这个动作将在路径中加入/myimages，所以最终的URL变成了www.imagepool.com/myimages

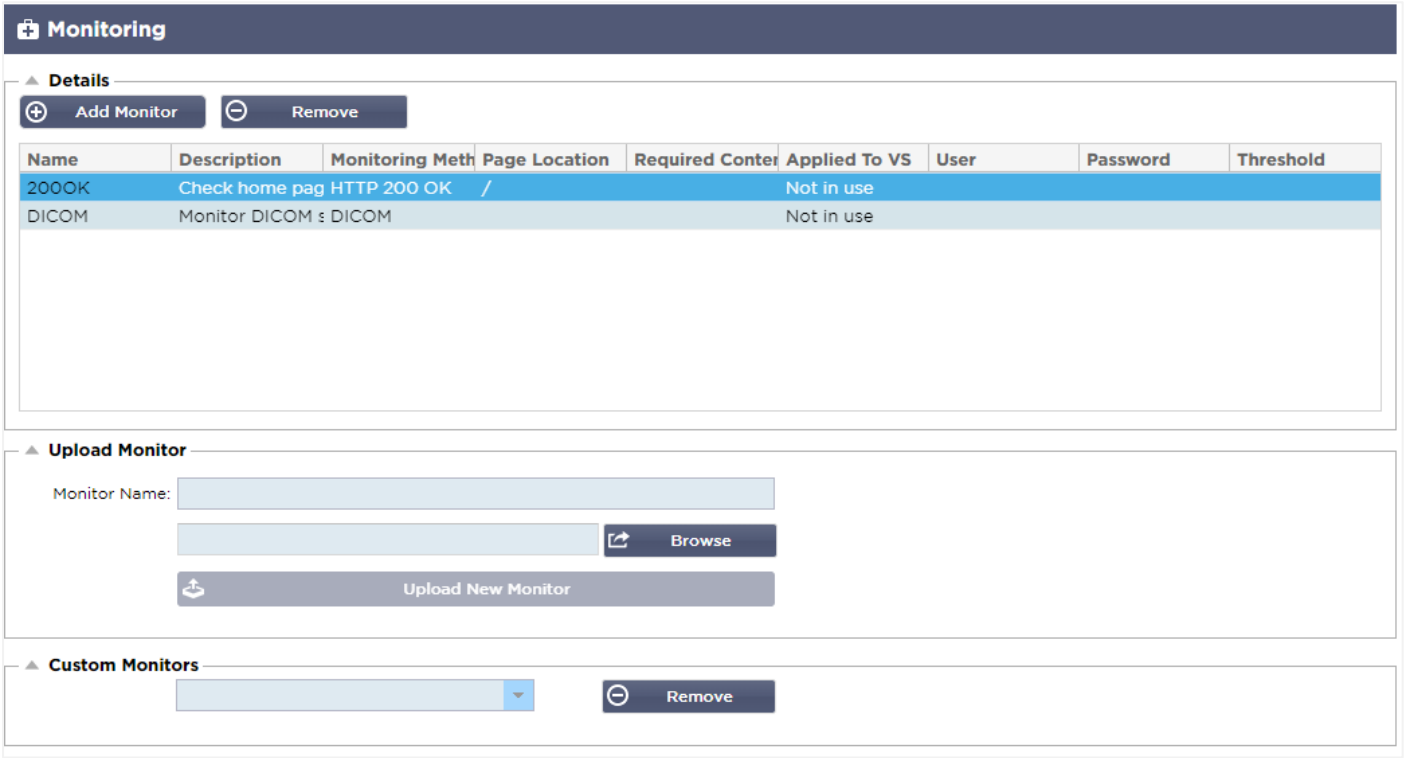
应用flightPATH规则

任何flightPATH规则的应用都是在每个VIP/VS的flightPATH标签中进行的。



- 导航到服务 > IP服务，并选择你想分配flightPATH规则的VIP。
- 你将看到如下所示的真实服务器列表
- 点击flightPATH标签
- 选择你已经配置的flightPATH规则或支持的预建规则之一。如果需要，你可以选择多个flightPATH规则。
- 将所选的集子拖放到Applied flightPATHs部分或点击>>箭头按钮。
- 该规则将被移至右侧并自动应用。

真实的服务器监控器



当设置了负载均衡后，监测真正的服务器和在其上运行的应用程序的健康状况是很有帮助的。例如，在Web服务器中，你可以设置一个特定的页面，你可以用它来监控状态，或者使用ADC的其他监控系统之一。

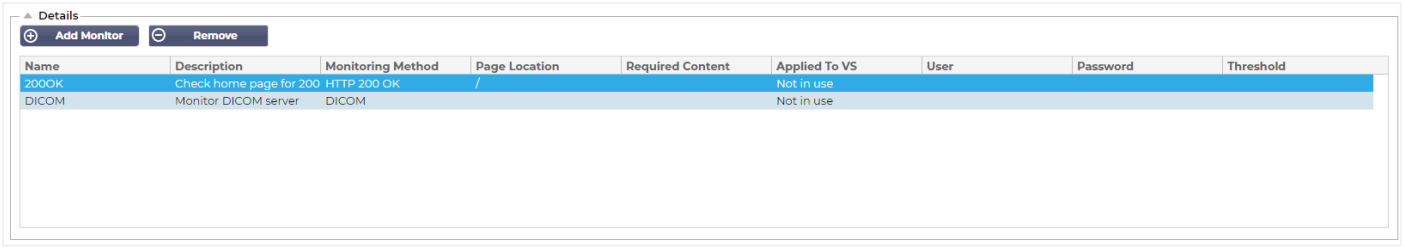
库>真实服务器监控页面允许你添加、查看和编辑自定义监控。这些是第7层的服务器"健康检查"，从你定义的虚拟服务的基本选项卡内的服务器监控领域选择它们。

真实服务器监控器页面分为三个部分。

- 详细内容
- 上传
- 定制显示器

详细内容

细节部分是用来添加新的监视器和删除任何你不需要的监视器。你也可以通过双击现有的显示器来编辑它。



命名

你为你的显示器选择的名称。

描述

本监测器的文字描述，我们建议最好是尽可能的描述性。

监测方法

从下拉列表中选择监测方法。可用的选择是。

监测方法	描述	例子
HTTP 200 OK	一个TCP连接被建立到真实服务器。连接建立后，向真实服务器发送一个简短的HTTP请求。等待来自服务器的HTTP响应，然后检查是否有 "200 OK "响应代码。如果收到 "200 OK "响应代码，则认为真实服务器已经启动并运行。如果由于任何原因，没有收到 "200 OK "响应代码，包括超时或连接失败，那么Real服务器就被视为停机和不可用。这种监控方法只能真正用于HTTP和加速的HTTP服务类型。然而，如果HTTP服务器使用的是第4层服务类型，那么如果SSL没有在Real Server上使用，或由 "内容SSL "设施适当处理，它仍然可以被使用。	名称。200 OK 描述。检查生产网站 监测方法。HTTP 200 OK 页面位置。/main/index.html 或 HTTP://www.edgenexus.io/main/index.html 需要的内容。不适用
HTTP响应	与Real服务器建立连接和HTTP请求/响应，并按照前一个例子的解释进行检查。但不是检查 "200 OK "的响应代码，而是检查HTTP响应的标头是否有自定义文本内容。该文本可以是一个完整的头，头的一部分，页面的一部分的一行，或者只是一个词。如果发现该文本，则认为Real服务器已经启动并运行。这种监控方法只能真正用于HTTP和加速的HTTP服务类型。但是，如果HTTP服务器使用的是第4层服务类型，如果SSL没有在Real Server上使用，或由 "内容SSL "设施适当处理，它仍然可以使用。	名称。服务器启动 描述。检查页面的内容，看是否有 "服务器启动。" 监测方法。HTTP响应 页面位置。/main/index.html 或 HTTP://www.edgenexus.io/main/index.html

		要求的内容。服务器启动
DICOM	我们使用所需内容栏中的 "源调用 "AE标题值来发送DICOM回声。你也可以在每台服务器的备注栏中设置 "目的地呼叫 "AE标题值。你可以在IP服务-中找到注释栏。 -虚拟服务--服务器页面。	名称。DICOM 描述。为DICOM服务进行L7健康检查 监测方法。DICOM 页面位置。不适用 必要的内容。AET价值
频带外的TCP	TCP Out of Band方法与TCP连接一样，只是你可以在所需内容栏中指定你想监控的端口。这个端口通常与流量端口不一样，当你想把服务绑在一起时使用	名称。乐队外的TCP 描述。监测带外/流量端口 页面位置。不适用 必要的内容。555
多端口TCP监控器	这个方法和上面的一样，只是你可以有几个不同的端口。只有在所需内容部分指定的所有端口都正确响应的情况下，监控才被视为成功。	名称。多端口显示器 描述。监控多个端口的成功 页面位置。不适用 要求的内容。135,59534,59535

页面位置

URL

一个HTTP监视器的页面位置。这个值可以是一个相对链接，如/folder1/folder2/page1.html。你也可以使用一个绝对链接，其中网站被绑定到主机名。

必要的内容

这个值包含监控器需要检测和利用的任何内容。这里所代表的值将根据所选择的监测方法而改变。

适用于VS

这个字段会自动填入监控器所应用的虚拟服务的IP/端口。你将不能删除任何已经与虚拟服务一起使用的监控器。

用户

一些自定义监视器可以使用这个值和密码字段一起登录到Real服务器。

密码

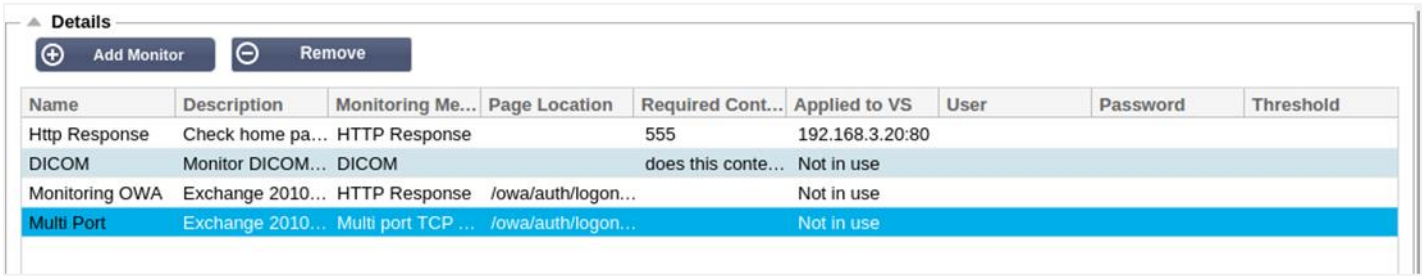
一些自定义监视器可以使用这个值和用户字段一起登录到Real服务器。

阈值

阈值字段是一个一般的整数，用于需要阈值（如CPU水平）的自定义监控。

注意：请确保从应用服务器返回的响应不是一个"分块"响应。

真实服务器监控实例



上传监控

在很多情况下，用户希望创建他们自己的自定义监视器，这一部分允许他们将其上传到ADC。

自定义监视器是用PERL脚本编写的，文件扩展名为.pl。

- 给你的监视器一个名字，以便你能在监测方法列表中识别它。
- 浏览.pl文件
- 点击上传新显示器
- 你的文件将被上传到正确的位置，并将作为一个新的监测方法可见。

定制显示器

在这个部分，你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
- 选择自定义显示器的名称
- 点击删除
- 你的自定义监控器将不再在监控方法列表中可见。

创建一个自定义监控器的Perl脚本

注意：本节是为具有使用和编写Perl语言经验的人准备的。

本节向你展示了你可以在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。如果你不包括这一行，那么你的脚本将不会被发现

以下是强制性的。

- #Monitor-Name
- 严格使用。
- 使用警告。

Perl脚本是在CHROOTED环境下运行的。它们经常调用另一个应用程序，如WGET或CURL。有时，这些程序需要针对特定的功能进行更新，如SNI。

动态价值

- my $host = $_[0]; - 这使用了IP Services--Real Server部分的 "地址"。
- my $port = $_[1]; - 这是使用IP服务--真实服务器部分的 "端口"。
- my $content = $_[2]; - 这使用了Library--Real Server Monitoring部分的 "Required Content "值。
- my $notes = $_[3]; - 这使用了IP服务中真实服务器部分的 "注释 "栏。
- my $page = $_[4]; - 这使用了Library--Real Server Monitor部分的 "页面位置 "值。
- my $user = $_[5]; - 这使用了Library--Real Server Monitor部分的 "User "值。
- my $password = $_[6]; - 这使用了Library--Real Server Monitor部分的 "密码 "值。

定制健康检查有两个结果

- 成功
  返回值 1
  向Syslog打印一条成功信息,
  标记真实服务器在线（提供IN COUNT匹配）。
- 不成功
  返回值 2
  向Syslog打印一条 "不成功 "的消息,
  标记真实服务器离线（如果OUT计数匹配）。

自定义健康监测器的例子

```
#Monitor-Name HTTPS_SNI
严格使用。
使用警告。
# 在可用健康检查的下拉菜单中显示上述监视器名称
# 有6个值传递给这个脚本（见下文）。
# 脚本将返回以下值
# 1是测试成功
# 2 如果测试不成功，子监控器
{
my Shost        = $_[0]; ###主机IP或名称
my Sport        = $_[1]; ### 主机端口
my Scontent     = $_[2]; ### 要寻找的内容（在网页和HTTP头文件中）。
my Snotes       = $_[3]; ### 虚拟主机名
my Spage        = $_[4]; ### 主机地址之后的URL部分
my Suser        = $_[5]:###域名/用户名称(可选)
my Spassword  = $_[6]; ###密码（可选）。
我的$resolve。
我的$auth       =;
如果 ($port)
{
        $resolve = "$notes:$port:$host":
}
否则 {
        $resolve = "$notes:$host";
}
如果（$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/)
        {
        print "HTTPs://$notes}${page} looking for - $content - Health check successful./n";
        返回(1)。
        }
否则
        {
        print "HTTPs://${notes}${page} looking for - $content - Health check failed.\n";
        返回(2)
        }
}
```

监控（@ARGV）。

注意：自定义监控--使用全局变量是不可能的。只能使用局部变量--在函数内部定义的变量

SSL证书

为了成功地与使用SSL加密连接的服务器使用第7层负载平衡，ADC必须配备目标服务器上使用的SSL证书。这一要求是为了使数据流能够被解密、检查、管理，然后在发送至目标服务器之前重新加密。

SSL证书的范围可以从ADC可以生成的自签名证书到受信任的供应商提供的传统证书（包括通配符）。你还可以使用从活动目录生成的域签名证书。

ADC对SSL证书做什么？

ADC可以根据数据包含的内容，执行流量管理规则（flightPATH）。这种管理不能在SSL加密的数据上执行。当ADC必须检查数据时，它首先需要解密，为此，它需要有服务器使用的SSL证书。一旦解密，ADC将能够检查并执行flightPATH规则。在这之后，数据将使用SSL证书重新加密，并被发送到最终的Real服务器上。

创建证书

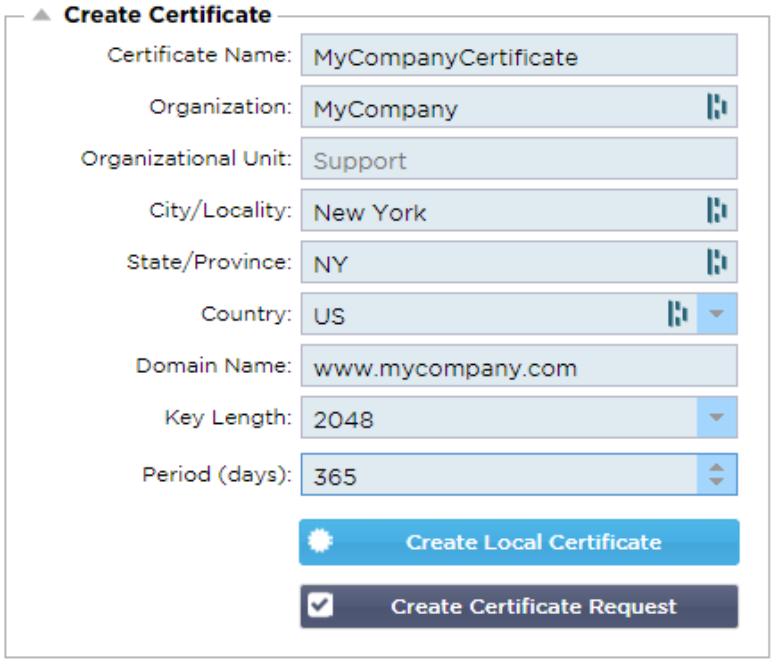
尽管ADC可以使用全球信任的SSL证书，但它可以生成一个自签名SSL证书。自签名SSL非常适合于内部负载平衡的要求。然而，你的IT政策可能需要一个受信任或域CA证书。

如何创建本地SSL证书

- 像上面的例子一样，填写所有细节
- 单击 "创建本地证书
- 一旦你点击了这一点，你就可以将证书应用于虚拟服务。

创建一个证书请求（CSR

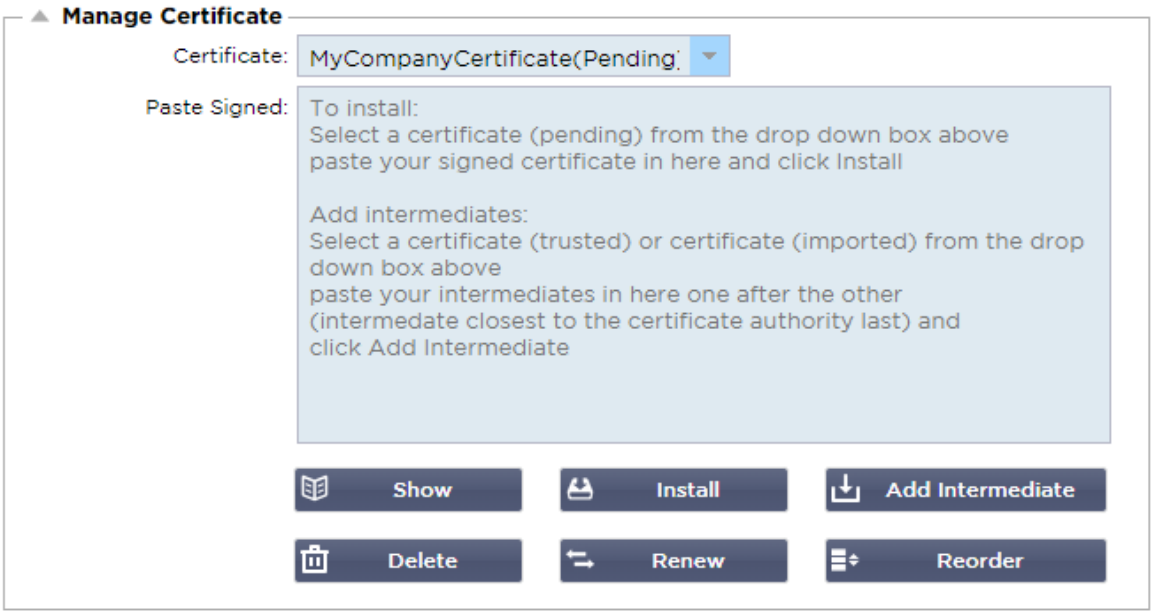
当你需要从外部供应商那里获得全球信任的SSL时，你将需要生成CSR来生成SSL证书。



如上图所示，在表格中填写所有相关数据，然后点击证书申请按钮。你将会看到与你提供的数据相对应的弹出窗口。

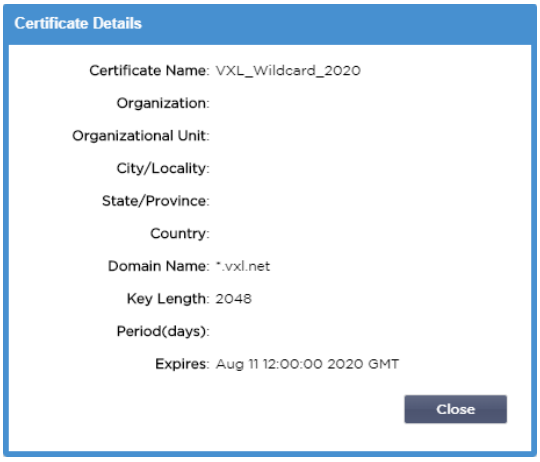
你需要将内容剪切并粘贴到一个文本文件中，并以CSR文件的扩展名命名，例如，*mycert.csr*。这个CSR文件将需要提供给你的证书颁发机构以创建SSL证书。

管理证书



该子部分包含各种工具，允许管理你在ADC内拥有的SSL证书。

显示

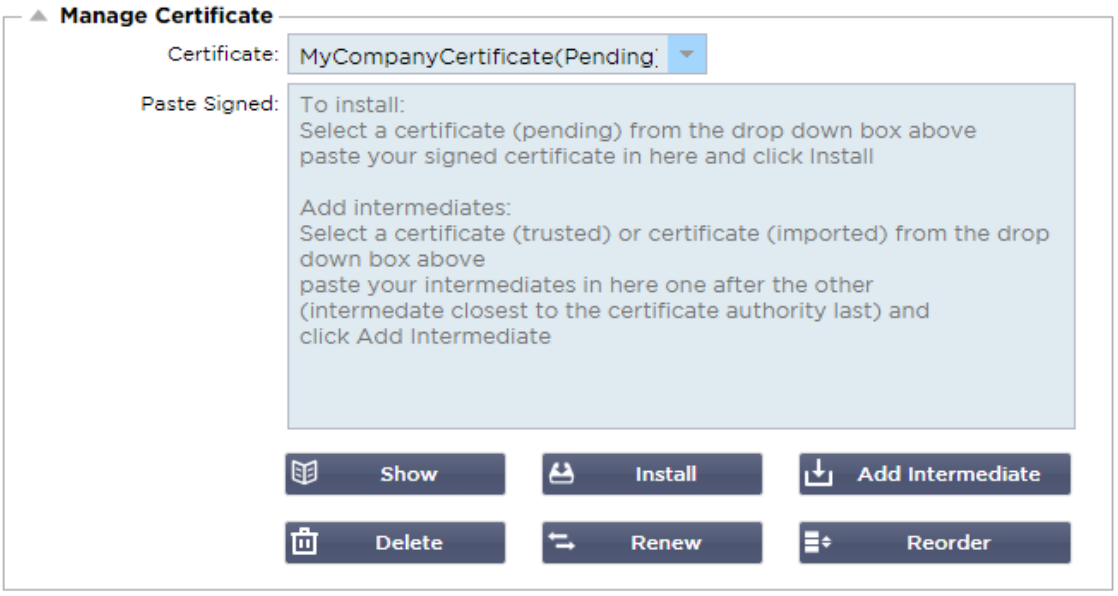


有时，你可能希望查看已安装的SSL证书的细节。

- 从下拉菜单中选择证书
- 单击 "显示 "按钮
- 下面显示的弹出窗口将显示证书的详细信息。

安装证书

一旦你从受信任的证书颁发机构获得证书，你将需要将其与生成的CSR相匹配，并在ADC内安装它。



- 选择你在上述步骤中生成的证书。该行项目将有一个固定的（Pending）状态。在这个例子中，MyCompanyCertificate显示在上面的图片中。
- 在一个文本编辑器中打开证书文件
- 将文件的全部内容复制到剪贴板上
- 将你从受信任机构收到的已签署的SSL证书的内容粘贴到标有 "已签署 "的字段中。

- 你也可以在这下面粘贴中间人，注意遵循正确的顺序。
    1. (TOP)　　你签署的证书
    2. (从头开始的第二项)　　中级1
    3. (从上到下第三位)　　中级2
    4. (底部)　　中级3
    5. 根证书机构　　不需要添加这个，因为它们存在于客户机上。
       (ADC也包含一个用于重新加密的根捆绑，在那里它充当Real服务器的一个客户端)
- 点击安装
- 一旦你安装了证书，你应该在你的证书旁边看到状态（受信任）。

如果你犯了一个错误或输入了错误的中间顺序，那么选择证书（受信任的）并按照正确的顺序再次添加证书（包括已签署的证书），然后点击安装。

添加中级

有时需要单独添加中间证书。例如，你可能已经导入了一个没有中间证书的证书。

- 突出显示一个证书（受信任的）或证书（已导入）。
- 一个一个地粘贴中间件，注意最接近证书授权的中间件要最后粘贴。
- 点击添加中级。

如果你犯了一个错误的顺序，你可以重复这个过程并再次添加中间物。这个动作将只覆盖之前的中间物。

删除一个证书

你可以使用删除按钮删除一个证书。一旦删除，该证书将完全从ADC中删除，并需要被替换，然后在需要时重新应用于虚拟服务。

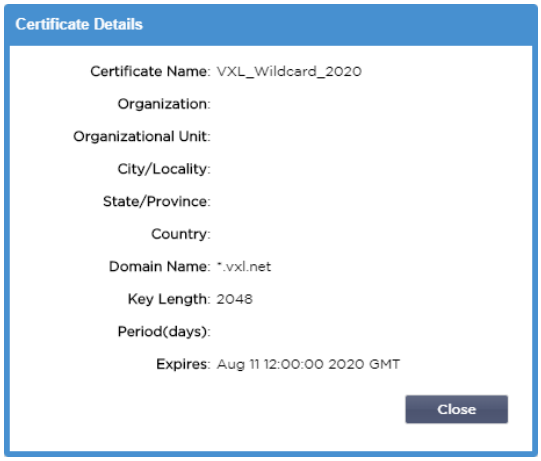
注意：在删除证书之前，请确保该证书没有附加到一个正在运行的VIP上。

更新证书

更新按钮允许你获得一个新的证书签名请求。当证书过期需要更新时，就需要进行这一操作。

- 从下拉列表中选择一个证书；你可以选择任何具有（待定）、（可信）或（已导入）状态的证书
- 点击更新
- 复制新的CSR细节，以便你能获得新的证书

- 当你获得新的证书时，请按照 "显示 "中详述的步骤操作。



- 有时，你可能希望查看已安装的SSL证书的细节。
- 从下拉菜单中选择证书
- 单击 "显示 "按钮
- 下面显示的弹出窗口将显示证书的详细信息。
- 安装证书。
- 新的和更新的证书现在将被安装到ADC中。

导入证书

在许多情况下，公司企业将需要使用他们的域名签名证书作为其内部安全制度的一部分。这些证书必须是PKCS#12格式，而密码必然会保护这些证书。

下面的图片显示了导入单个SSL证书的子部分。

- 给你的证书一个友好的名字。该名称可以在ADC中使用的下拉列表中识别它。它不需要与证书域名相同，但必须是没有空格的字母数字。除了 _ 和 - 之外，不允许使用其他特殊字符。
- 输入你用来创建PKCS#12证书的密码
- 浏览{证书名称}.pfx
- 点击导入。
- 你的证书现在将出现在ADC的相关SSL下拉菜单中。

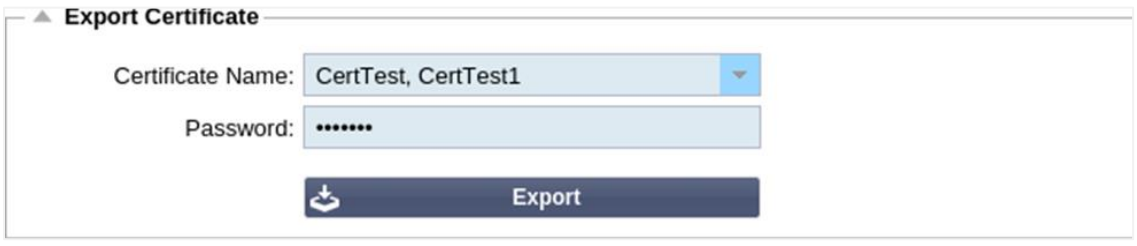
导入多个证书

本节允许你导入一个包含多个证书的JNBK文件。当导出多个证书时，JNBK文件会被ADC加密并产生。

- 浏览你的JNBK文件 - 你可以通过导出多个证书来创建一个这样的文件
- 输入你用来创建JNBK文件的密码
- 点击导入。
- 你的证书现在将出现在ADC的相关SSL下拉菜单中。

导出证书

有时，你可能希望导出ADC中持有的一个证书。ADC已经具备了这样的能力。



- 点击你想安装的证书。你可以点击全部选项来选择所有列出的证书。

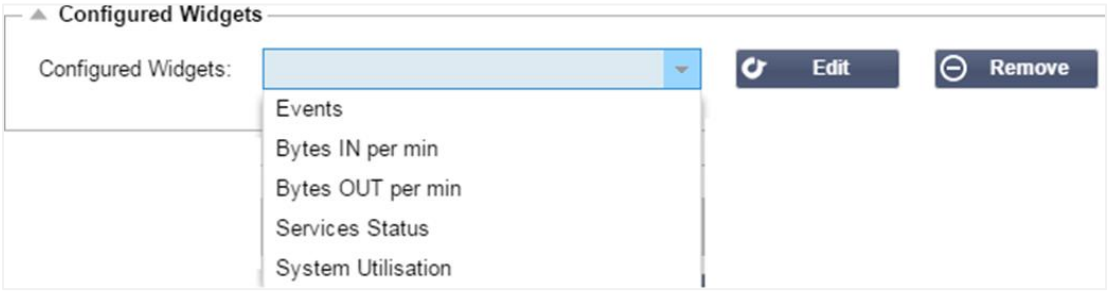
- 键入一个密码以保护导出的文件。密码必须至少有六个字符的长度。可以使用字母、数字和某些符号。以下字符是不能接受的： < > " ' ( ) ; \ | \A3 % &
- 点击出口
- 如果你要导出单个证书，生成的文件将被命名为sslcert_{certname}.pfx。例如，sslcert_Test1Cert.pfx
- 在多证书输出的情况下，产生的文件将是一个 JNBK 文件。文件名将是sslcert__pack.jnbk。

注意：JNBK文件是由ADC产生的加密容器文件，只对导入ADC有效。

小工具

库 > 小工具页面允许你配置显示在你的自定义仪表板中的各种轻量级视觉组件。

配置的小工具

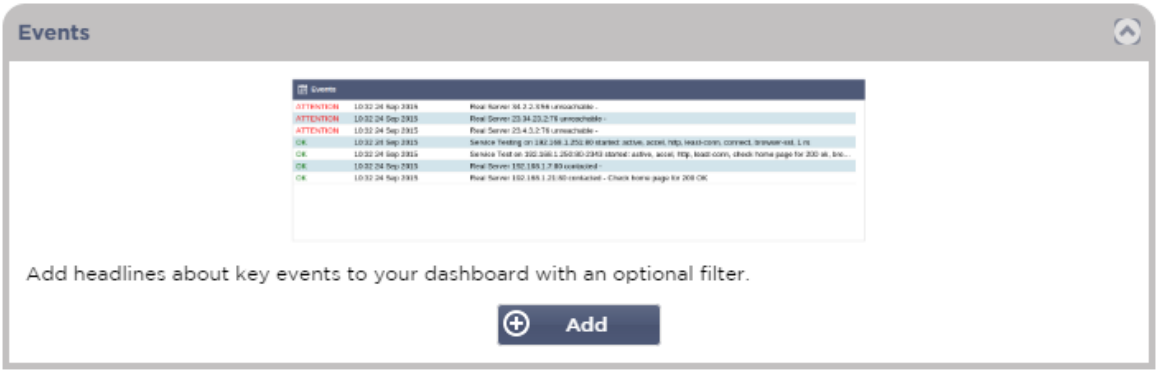


配置的小工具部分允许你查看、编辑或删除从可用小工具部分创建的任何小工具。

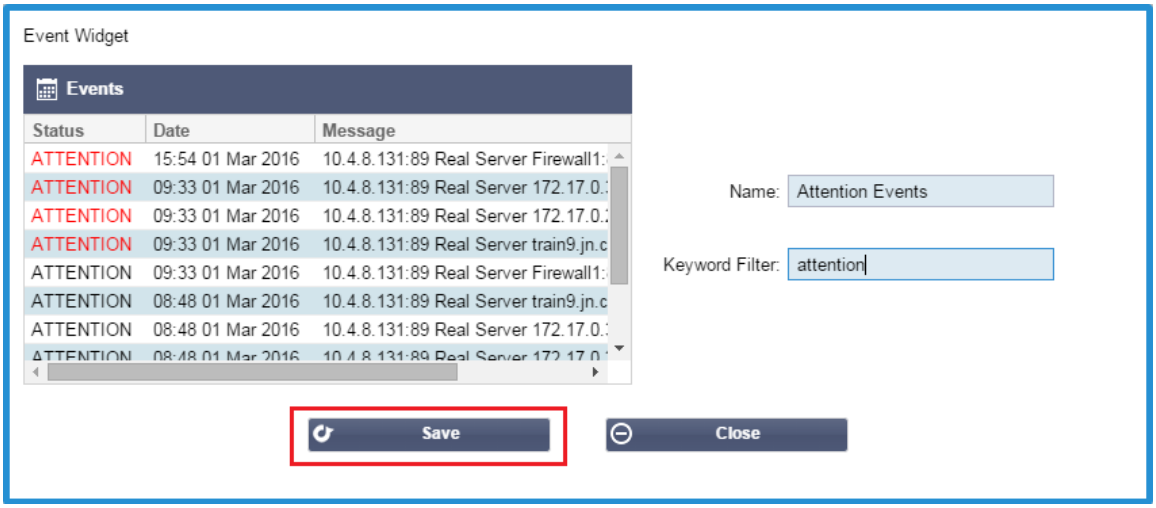
可用的小工具

ADC内提供了五个不同的部件，你可以根据你的要求对它们进行配置。

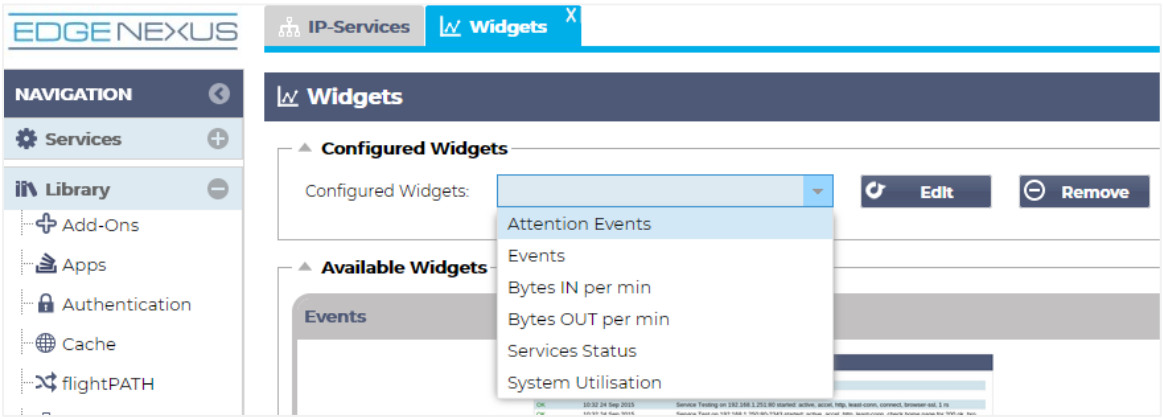
活动小工具



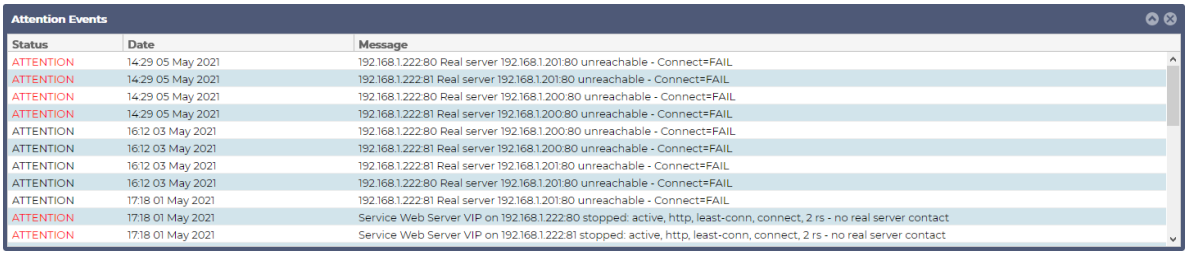
- 要添加一个事件到 "事件 "小组件，点击 "添加 "按钮。
- 为你的事件提供一个名称。在我们的例子中，我们添加了Attention Events作为事件名称。
- 添加一个关键词过滤器。我们还添加了Attention的过滤值



- 点击保存，然后关闭
- 现在你会在配置的小工具下拉菜单中看到一个额外的小工具，名为 "关注事件"。

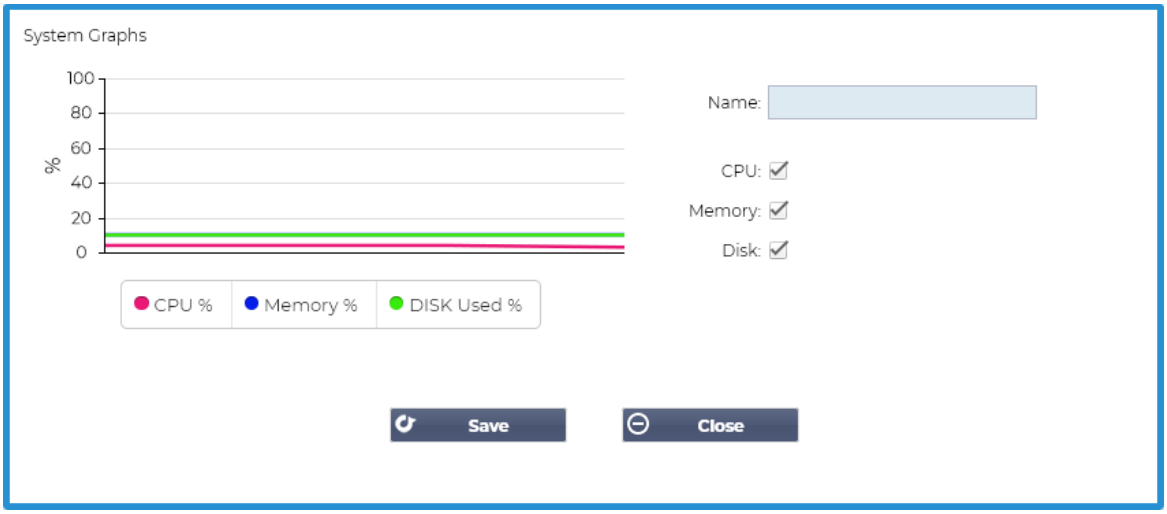


- 你可以看到我们现在已经在视图>仪表板部分添加了这个部件。
- 选择 "关注事件 "小组件，在仪表板内显示。见下文。



你也可以通过点击暂停实时数据按钮来暂停和重启实时数据传输。此外，你可以在任何时候通过点击 "默认仪表盘 "按钮恢复到默认仪表盘。

系统图表小工具

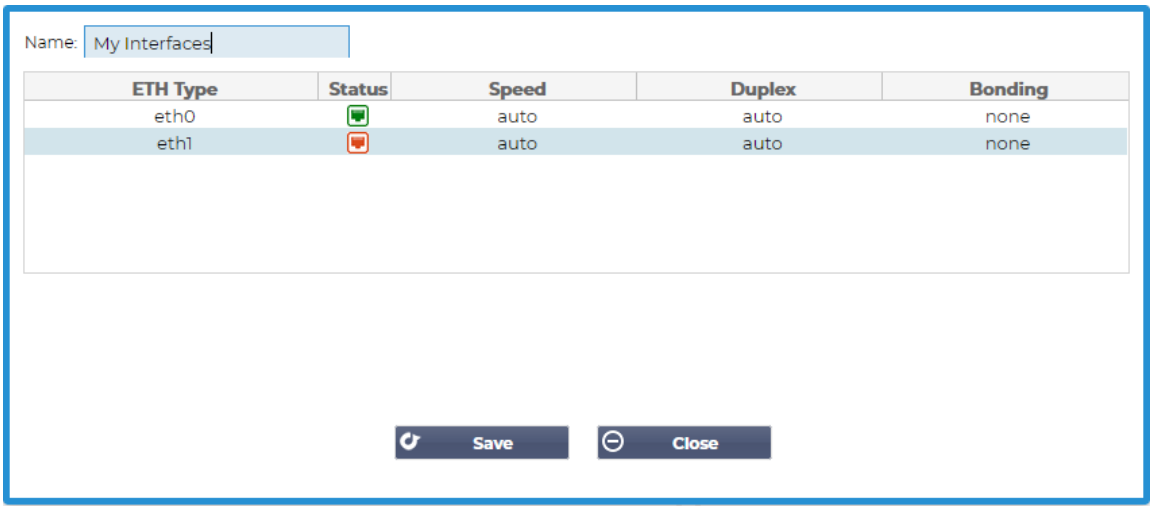


ADC有一个可配置的系统图表小组件。通过点击小组件上的添加按钮，你可以添加以下监测图表来显示。

- CPU
- 记忆
- 碟片

一旦你添加了它们，它们将在仪表板的小部件菜单中单独可用。

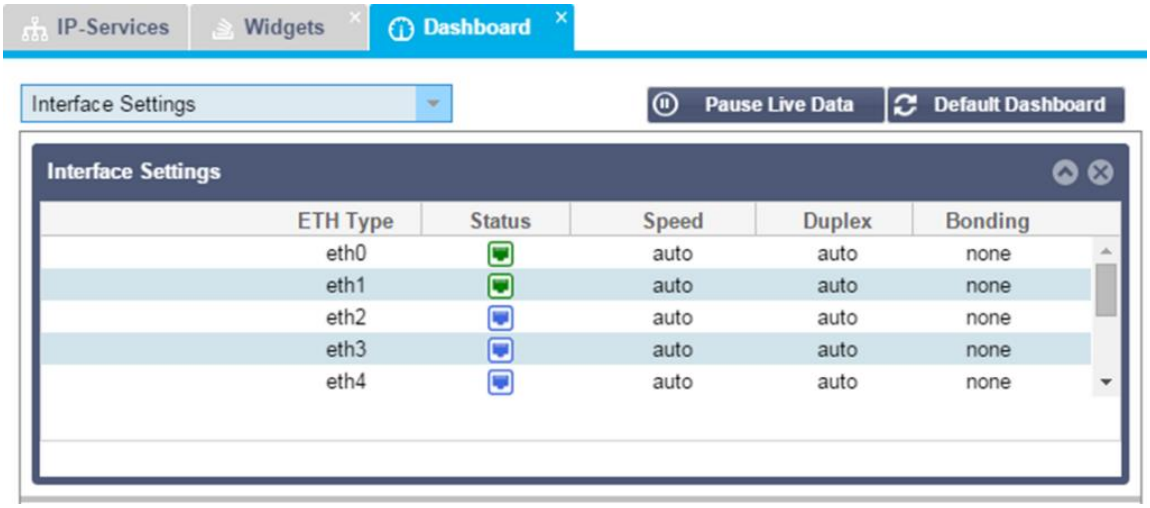
界面小工具



接口小组件允许你显示所选网络接口的数据，如ETH0、ETH1等。可供添加的接口数量取决于你为虚拟设备定义了多少个网络接口或在硬件设备内配置了多少个网络接口。

一旦你完成了，点击保存按钮，然后点击关闭按钮。

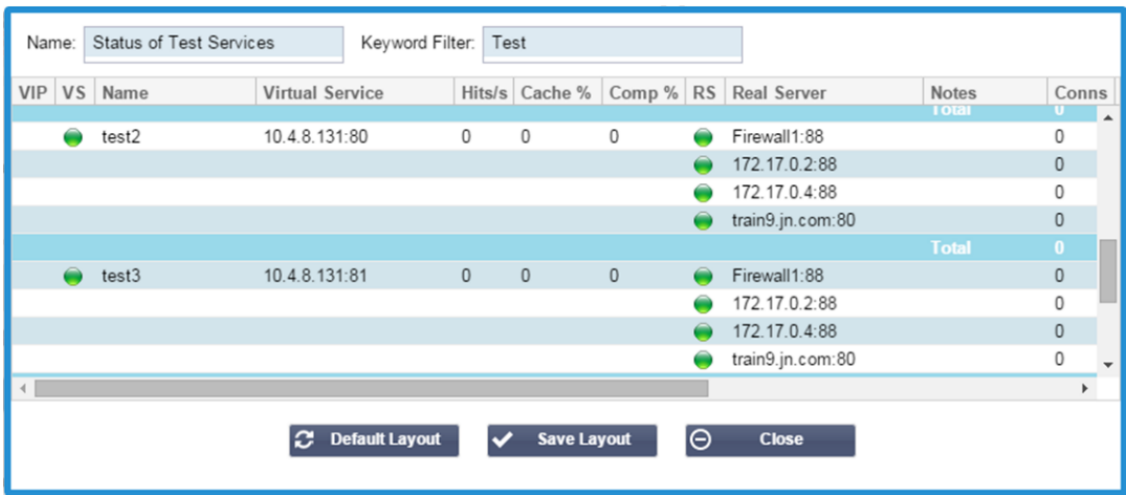
从仪表板内的小部件下拉菜单中选择你刚刚定制的小部件。你会看到一个像下面这样的屏幕。



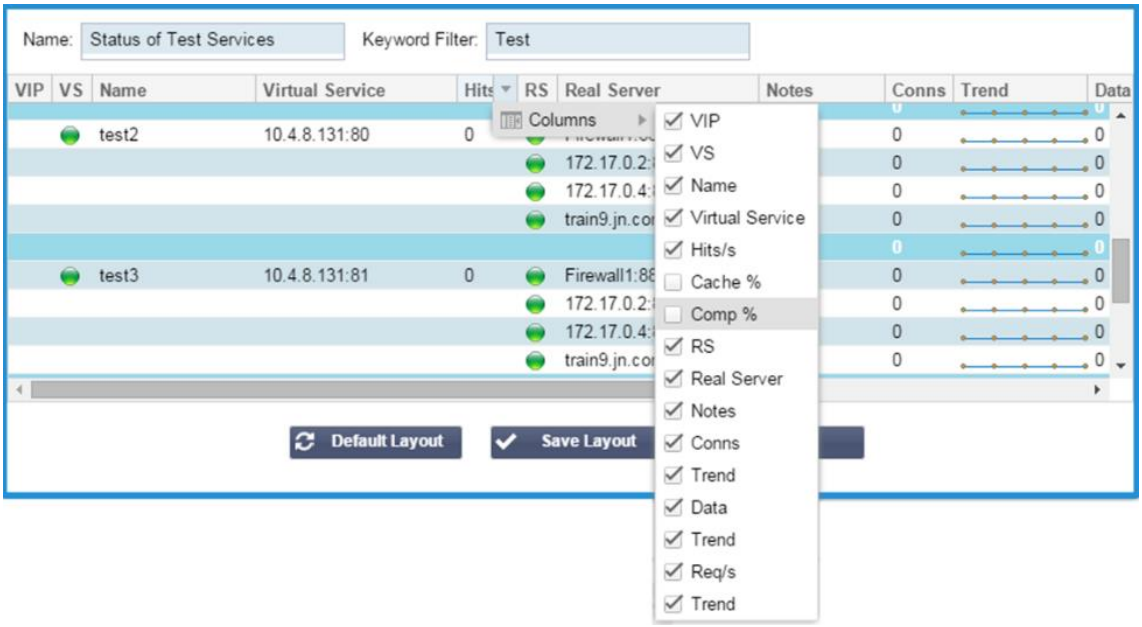
状态小工具

状态小组件允许你看到负载平衡的运作。你也可以过滤该视图以显示特定的信息。

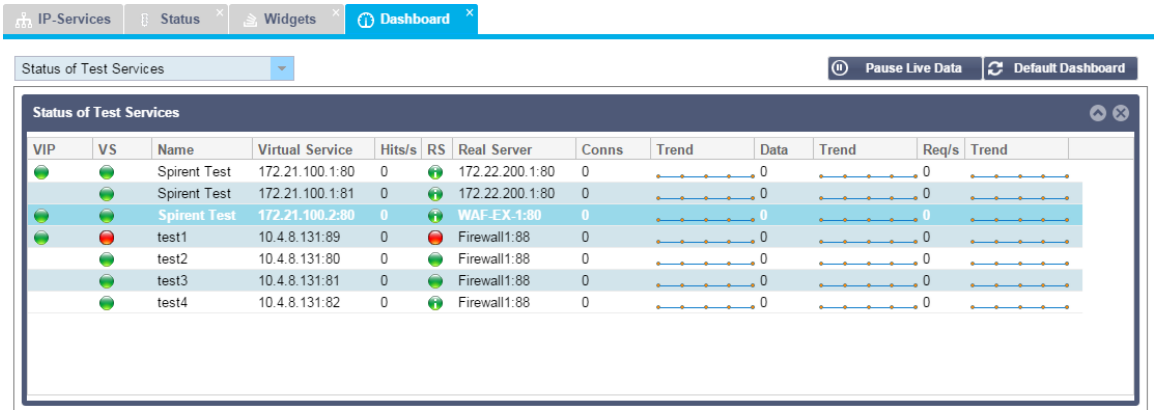
- 点击添加。



- 为你希望监测的服务输入一个名称
- 你还可以选择你希望在小组件中显示哪些列。

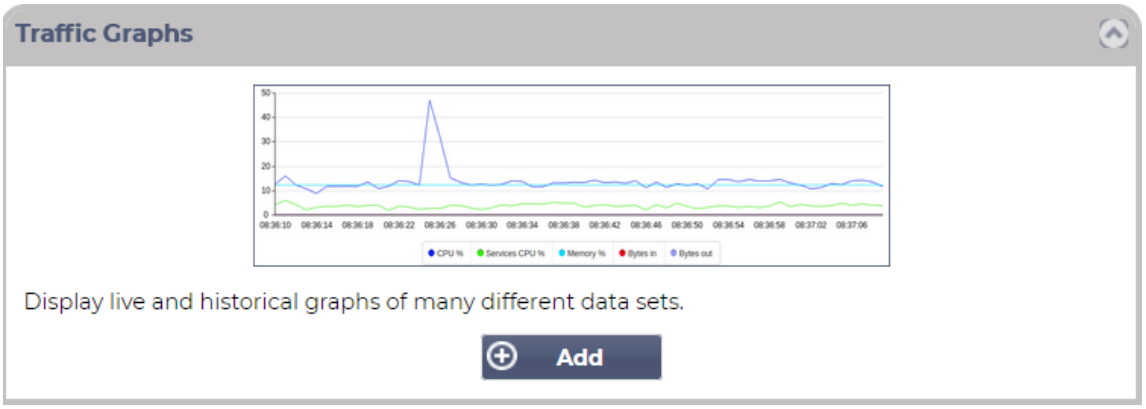


- 一旦你感到满意，点击保存，然后关闭。
- 所选择的状态小部件将在仪表板部分可用。



交通图形小工具

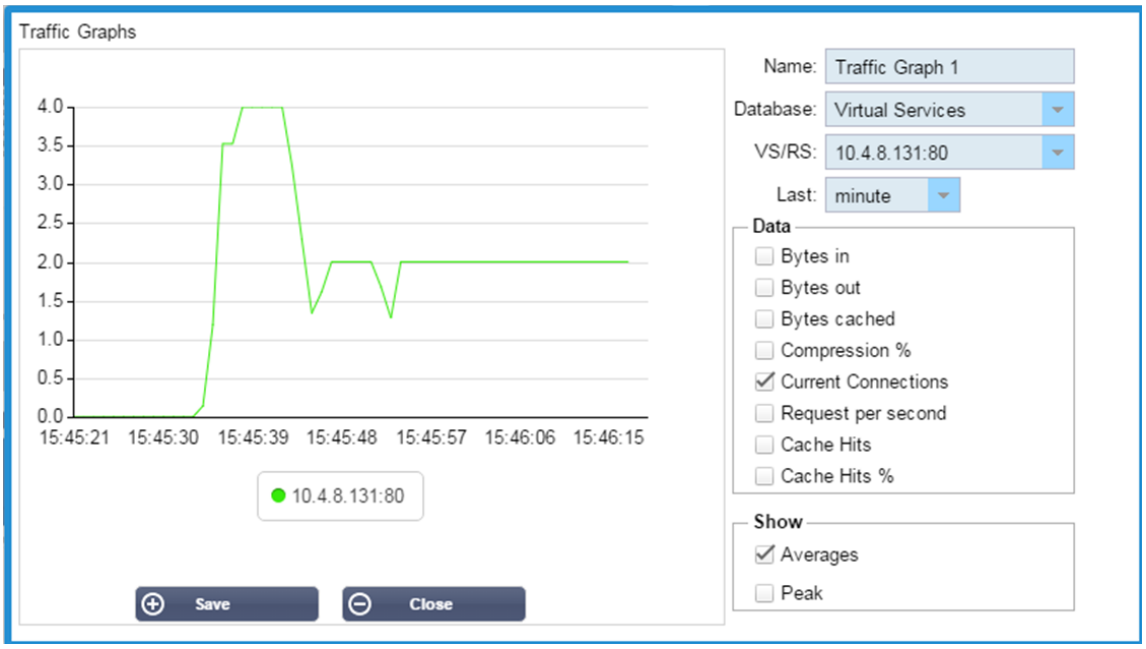
这个小组件可以被配置为显示每个虚拟服务和真实服务器的当前和历史流量数据。此外，你可以看到全球流量的整体当前和历史数据。



- 点击添加按钮

- 命名你的小部件。
- 从虚拟服务、真实服务器或系统中选择一个数据库。
- 如果你选择虚拟服务，你可以从VS/RS下拉菜单中选择一个虚拟服务。
- 从最后一个下拉菜单中选择一个时间范围。
    - 分钟 - 最后60分钟
    - 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--过去七天内每天的汇总数据
    - 月--过去七天里每周的汇总数据
    - 年份--过去12个月中每个月的汇总数据
- 根据你所选择的数据库，选择可用的数据
    - 虚拟服务数据库
    - 字节数在
    - 字节输出
    - 缓存的字节数
    - 压缩百分比
    - 当前连接
    - 每秒请求数
    - 缓存点击率
    - 缓存点击率百分比
- 真实的服务器
    - 字节数在
    - 字节输出
    - 当前连接
    - 每秒请求数
    - 响应时间
- 系统
    - CPU百分比
    - 服务 CPU
    - 记忆力%的人
    - 磁盘空闲百分比
    - 字节数在
    - 字节输出
- 选择显示平均值或峰值
- 一旦你选择了所有的选项，点击保存并关闭。

流量图示例



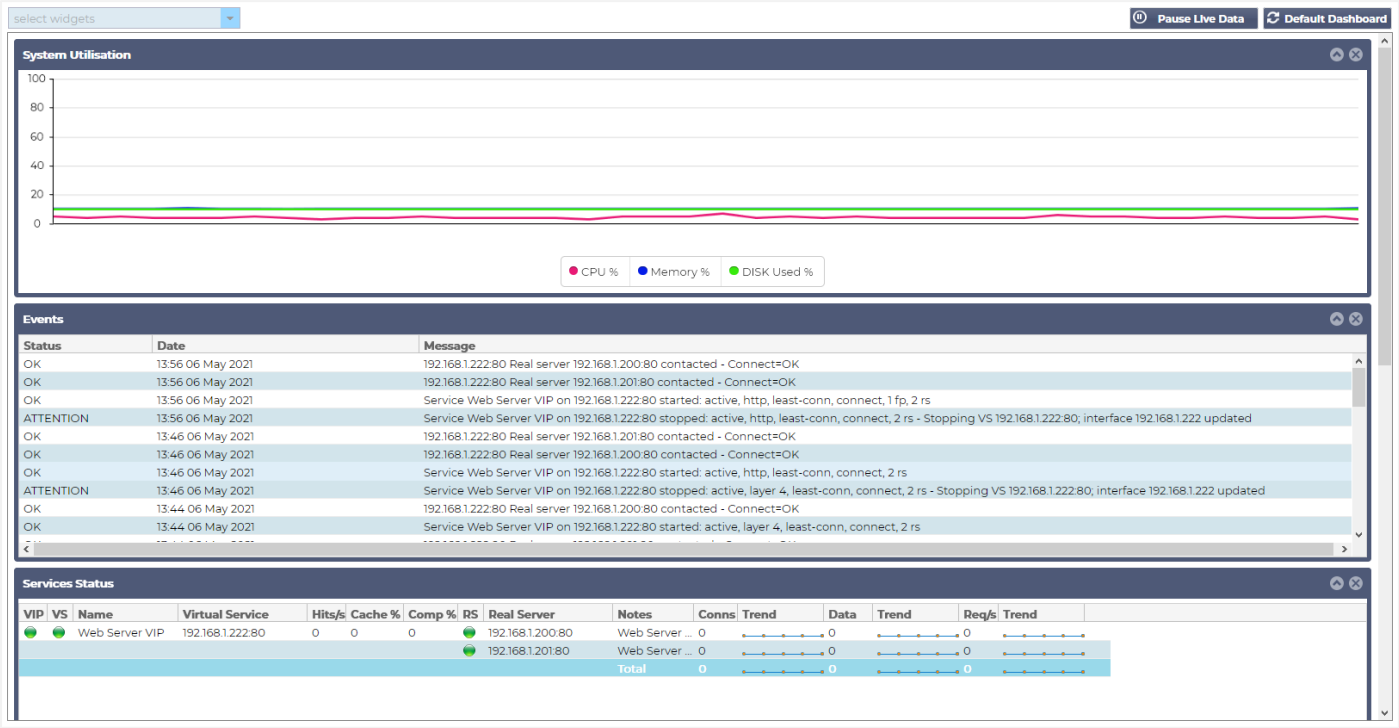
现在你可以将你的交通图部件添加到视图>仪表板。

查看

仪表板

像所有的IT系统管理界面一样，有很多时候，你需要查看ADC正在处理的性能指标和数据。我们为你提供了一个可定制的仪表盘，让你以一种简单而有意义的方式来做这件事。

仪表板可以通过导航面板的 "视图
"部分到达。当选择时，它显示几个默认的部件，并允许你选择任何你定义的自定义部件。



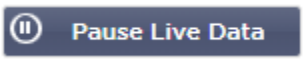
仪表板的使用

仪表板U有四个元素：小工具菜单、暂停/播放按钮和默认仪表板按钮。

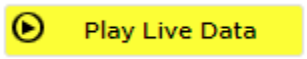
小工具菜单

位于仪表板左上方的小工具菜单允许你选择和添加任何你定义的标准或定制的小工具。要使用它，从下拉菜单中选择小工具。

暂停实时数据按钮



这个按钮允许你选择ADC是否应该实时更新仪表板。一旦暂停，就不会有仪表盘小部件被更新，允许你在闲暇时检查内容。一旦开始暂停，该按钮会改变状态，显示播放实时数据。



当你完成后，只需点击播放实时数据按钮，重新启动数据收集并更新仪表板。

默认的仪表板按钮

你可能希望将仪表板布局重置为默认值。在这种情况下，请按下Default Dashboard按钮。一旦点击，对仪表板所做的所有改变都将丢失。

调整大小、最小化、重新排序和删除小工具

调整一个小部件的大小

你可以非常容易地调整一个小组件的大小。点击并按住小组件的标题栏，把它拖到仪表板区域的左边或右边。你会看到一个点状的矩形，代表新的小组件尺寸。把小组件放到矩形里，然后放开鼠标按钮。如果你想把调整过的小组件放在以前调整过的小组件旁边，你会看到矩形出现在你想放在旁边的小组件附近。

最小化一个小部件

你可以在任何时候通过点击小组件的标题栏来最小化小组件。这个动作将最小化小组件，只显示标题栏。

移动小工具顺序

要移动一个小组件，你可以通过点击并按住标题栏和移动鼠标进行拖放。

移除一个小部件

你可以通过点击小组件标题栏的图标⊗来删除一个。

历史

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

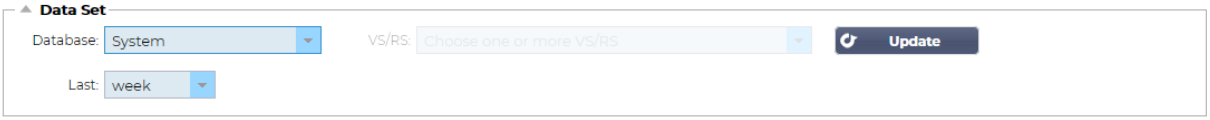
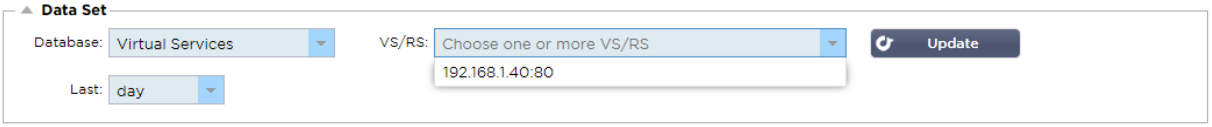
它还可以让你看到负载平衡的运行情况，并帮助捕捉任何需要调查的错误或模式。注意，你必须在"系统">"历史 "中启用历史记录，才能使用这一功能。

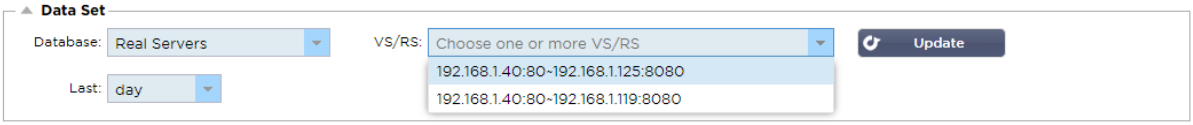
查看图形数据

数据集

以图表形式查看历史数据，请按以下步骤操作。

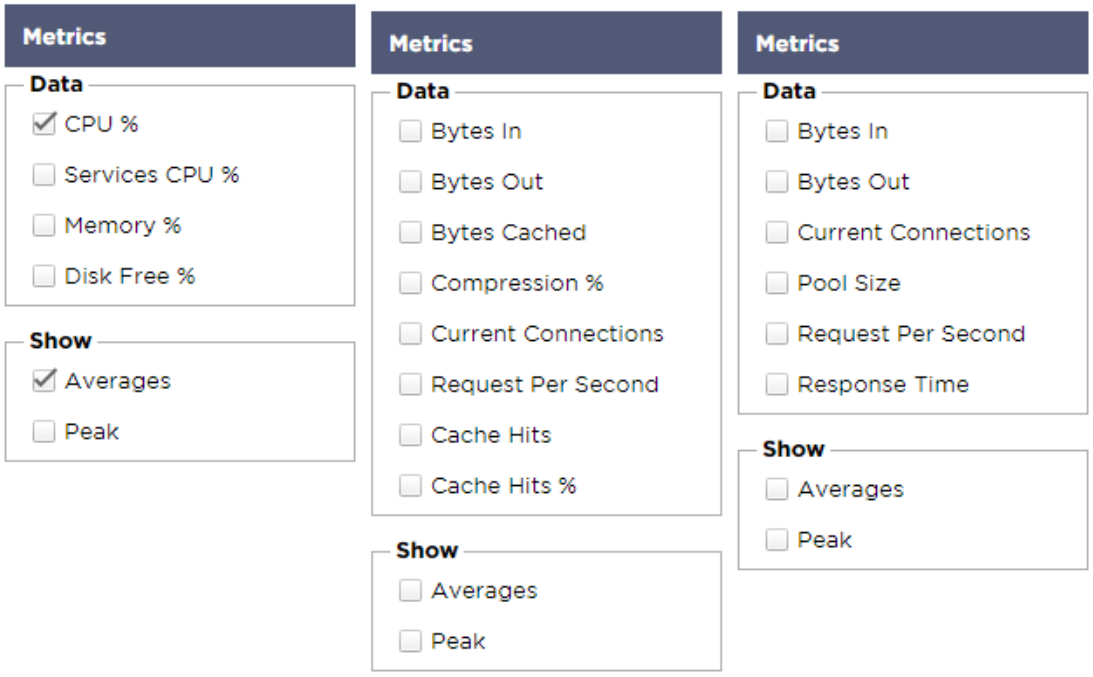
第一步是选择与你希望查看的信息有关的数据库和时期。你可以从最后一个下拉菜单中选择的时期是分钟、小时、日、周、月和年。

数据库	描述
系统	选择该数据库将允许你看到CPU、内存和磁盘驱动器空间随时间变化的情况 
虚拟服务	选择这个数据库将允许你选择数据库中从你开始记录数据时起的所有虚拟服务。你将看到一个虚拟服务的列表，你可以从中选择一个。 

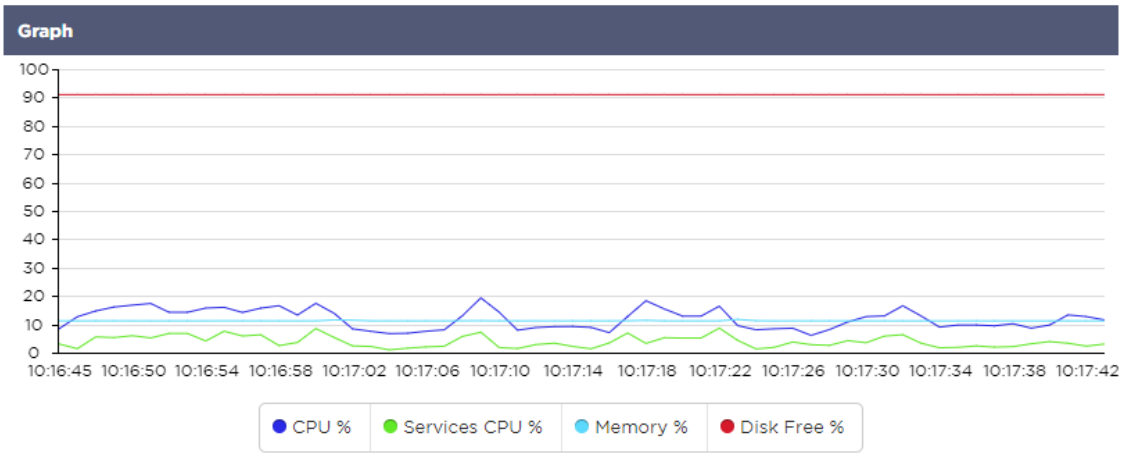
真正的服务	选择这个数据库将允许你选择数据库中从你开始记录数据时的所有Real Servers。你会看到一个Real Servers的列表，你可以从中选择一个。 

度量衡

一旦你选择了你要使用的数据集，就该选择你希望显示的指标了。下面的图片说明了可供管理员选择的指标：这些选择对应于系统、虚拟服务和真实服务器（从左到右）。



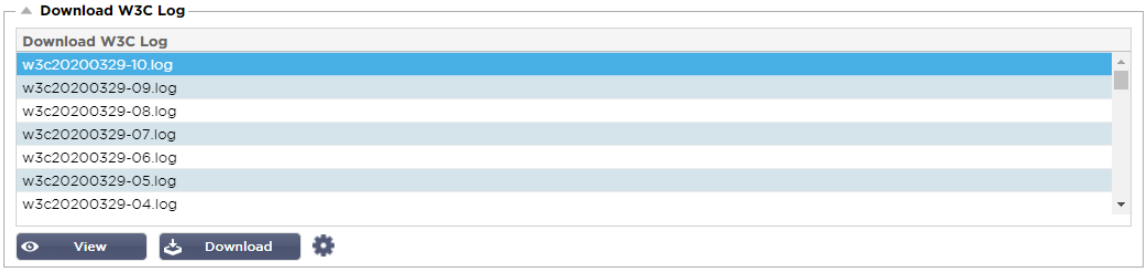
样品图



日志

查看部分的日志页面允许你预览和下载W3C和系统日志。该页面分为两个部分，详见下文。

下载W3C日志



W3C日志是在系统>日志部分启用的。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，包括源互联网协议（IP）地址、HTTP版本、浏览器类型、引用者页面和时间戳。W3C日志可以变得非常大，这取决于数据量和记录的日志类别。

从W3C部分，你可以选择你需要的日志，然后查看或下载它。

查看按钮

查看按钮允许你在文本编辑器窗口中查看所选的日志，如记事本。

下载按钮

这个按钮允许你将日志下载到你的本地存储，以便以后查看。

齿轮图标

点击这个图标可以进入位于系统>日志的W3C日志设置部分。我们将在本指南的日志部分详细讨论这个问题。

统计数据

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的全部目的是监测数据并将其引导到配置为接收数据的Real服务器。在ADC中提供压缩功能是为了提高ADC的性能。有时，管理员希望测试和检查ADC的数据压缩信息；这些数据由统计中的压缩面板提供。

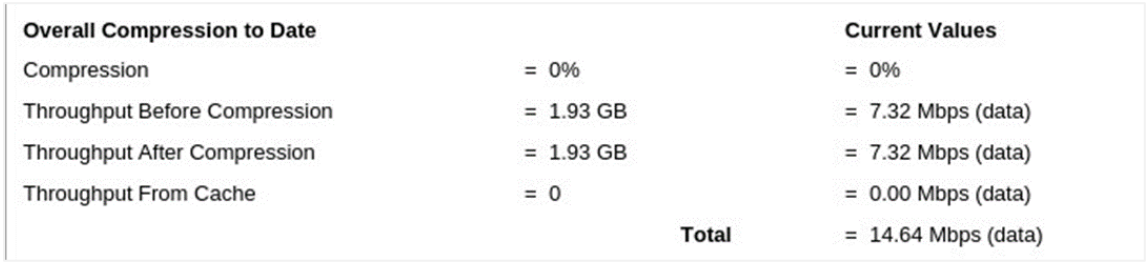
迄今为止的内容压缩

Compression Statistic

Content Compression to Date	
Compression	= 0%
Throughput Before Compression	= 0
Throughput After Compression	= 0

本节中显示的数据详细说明了ADC在可压缩内容上实现的压缩水平。60-80%的数值是我们所称的典型值。

迄今为止的总体压缩情况



Overall Compression to Date			Current Values
Compression	= 0%		= 0%
Throughput Before Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput After Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput From Cache	= 0		= 0.00 Mbps (data)
		Total	= 14.64 Mbps (data)

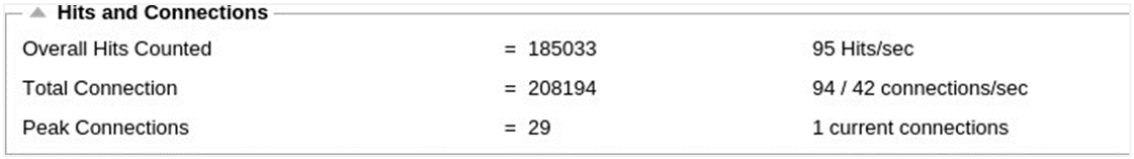
本节中提供的数值报告了ADC在所有内容上实现了多少压缩。这方面的典型百分比取决于你的服务中包含多少预压缩的图像。图像的数量越多，整体的压缩百分比就可能越小。

总投入/产出

Total Input	= 2.13 GB	Input/s	= 9.10 Mbps
Total Output	= 2.18 GB	Output/s	= 9.24 Mbps

总输入/输出数字表示进入和离开ADC的原始数据量。测量单位将随着规模从kbps到Mbps到Gbps的增长而变化。

点击率和联系



Hits and Connections

Overall Hits Counted	= 185033	95 Hits/sec
Total Connection	= 208194	94 / 42 connections/sec
Peak Connections	= 29	1 current connections

点击和连接部分包含了通过ADC的点击和交易的总体统计数据。那么，点击率和连接数是什么意思？

- Hit被定义为第7层事务。通常用于网络服务器，这是对一个对象（如图像）的GET请求。
- 一个连接被定义为第四层的TCP连接。在一个TCP连接上可以发生许多交易。

计算的总体点击率

本节中的数字显示了自上次重置以来非缓存点击的累积数量。在右侧，数字将显示当前每秒的点击数。

连接总数

总连接值表示自上次重置以来TCP连接的累积数量。第二栏中的数字表示每秒向ADC发出的TCP连接。右侧一栏中的数字是每秒钟向真实服务器发出的TCP连接数。例如6/8个连接/秒。在所示例子中，我们每秒有6个TCP连接到虚拟服务，每秒有6个TCP连接到真实服务器。

峰值连接

连接数的峰值代表向ADC进行的TCP连接的最大数量。最右边一栏的数字表示当前活动的TCP连接数。

缓存

你会记得，ADC同时配备了压缩和缓存。本节显示了应用于一个通道时与缓存有关的总体统计数据。如果缓存没有被应用到一个通道并被正确配置，你将看到0缓存内容。

Caching

Content Caching	Hits	Bytes
From Cache	= 0 / **0.0%**	= 0 / **0.0%**
From Server	= 495799 / **100.0%**	= 1.97 GB / **100.0%**
Cache Contents	= 0 entries	= 0 / **0.0%**

来自缓存

点击率。第一栏给出了自上次重置以来从ADC缓存中获得的交易总数。还提供了总交易量的百分比。

字节。第二列给出了从ADC缓存中提供的以千字节为单位的数据总量。还提供了总数据的百分比。

来自服务器

点击率。第1栏给出了自上次重置以来，从真实服务器上提供的交易总数。还提供了总交易量的百分比。

字节。第二列给出了从真实服务器提供的以千字节为单位的数据总量。还提供了总数据的百分比。

缓存内容

点击量。这个数字给出了ADC缓存中包含的对象的总数。

字节。第一个数字给出了ADC缓存对象的总体大小，单位是兆字节。还提供了最大缓存大小的百分比。

硬件设施

无论你是在虚拟环境中还是在硬件中使用ADC，本节将为你提供关于设备性能的宝贵信息。

Hardware

Disk Usage	= 22%
Memory Usage	= 18.9%(277.5MB of 1465.1MB)
CPU Usage	= 11.0%

磁盘使用情况

第2列中提供的数值给出了当前使用的磁盘空间的百分比，并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器上。

内存使用情况

第二列给出了当前使用的内存的百分比。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的内存。

CPU使用率

提供的关键值之一是ADC目前使用的CPU的百分比。这是很自然的波动。

状况

视图 >

状态页面显示你所定义的虚拟服务在ADC中穿越的实时流量。它还显示每个真实服务器的连接数和数据，因此你可以实时体验负载平衡。

虚拟服务细节

贵宾专栏

该灯的颜色表示与一个或多个虚拟服务相关的虚拟IP地址的状态。

状况	描述
🟢	在线
🔵	故障转移-待机。这个虚拟服务是热备用的
🟡	表示 "被动 "的人在为 "主动 "的人拖延时间
🔴	离线。真实服务器无法到达，或没有启用真实服务器
⚪	查找情况
🟣	未被许可或被许可的虚拟IP数量超过了

VS状态栏

该灯的颜色表示虚拟服务的状态。

状况	描述
●	在线
●	故障转移-待机。这个虚拟服务是热备用的
●	表示 "被动 "的人在为 "主动 "的人拖延时间
●	服务需要注意。这种状态指示可能是由于Real服务器未能通过健康监测或被手动改为离线。流量将继续流动，但真实服务器的容量会减少。
●	离线。真实服务器无法到达，或没有启用真实服务器
●	查找情况
●	未被许可或被许可的虚拟IP数量超过了

命名

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。

命中率/秒

在客户端每秒进行第7层交易。

缓存百分比

这里提供的数字代表了从ADC的RAM缓存中获得服务的对象的百分比。

压缩率%。

这个数字表示在客户端和ADC之间被压缩的对象的百分比。

RS状态（远程服务器

下表概述了与VIP相连的真实服务器状态的含义。

状况	描述
●	已连接
●	未监测
●	排水或脱机
●	待机
●	未连接
●	查找情况
●	未被许可或被许可的虚拟IP数量超过了

真实服务器

真实服务器的IP地址和端口。

笔记

这个值可以是任何有用的说明，使其他人了解该条目的目的。

Conns (连接)

表示每个Real服务器的连接数，让你看到负载平衡的作用。对于验证你的负载平衡策略是否正常工作非常有帮助。

数据

这一栏中的数值显示了被发送到每个真实服务器的数据量。

Req/Sec（每秒的请求）。

每秒发送到每个真实服务器的请求数。

系统

ADC用户界面的 "系统 "部分允许你访问和控制ADC的所有系统范围方面。

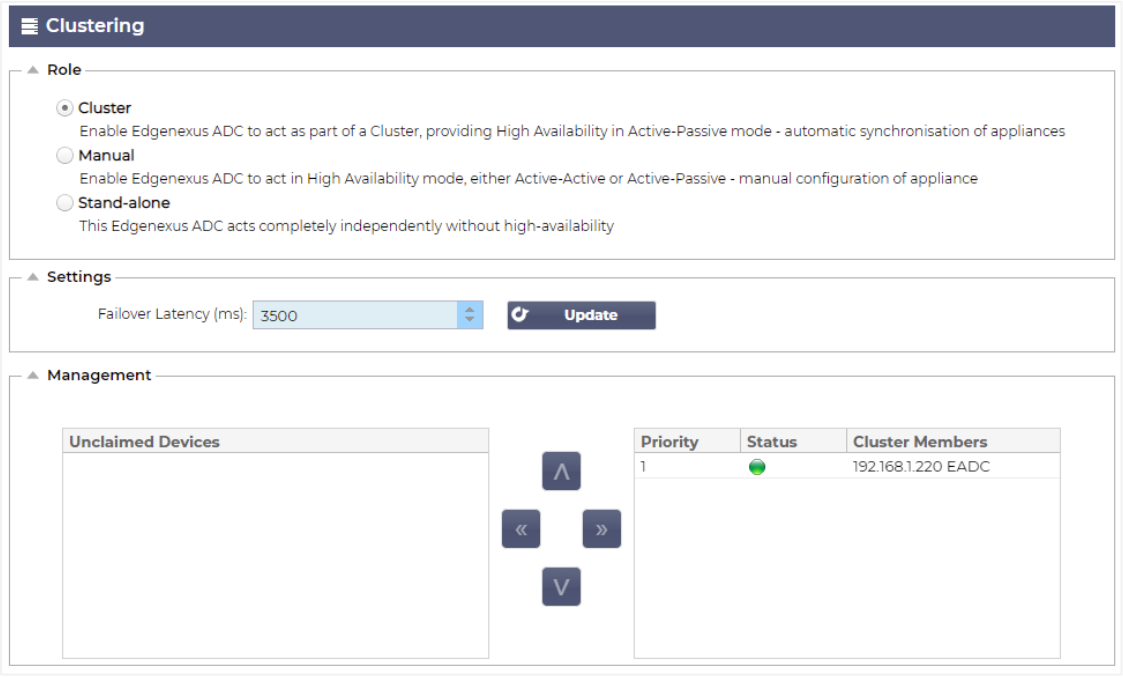
聚类

ADC可以作为一个单一的独立设备使用，而且它可以很好地完成这个任务。然而，当人们考虑到ADC的目的是对各组服务器进行负载平衡时，对ADC本身进行集群的需要就变得很明显。ADC易于浏览的用户界面设计使集群系统的配置变得简单明了。

系统 > 集群页面是您配置 ADC 设备高可用性的地方。这一部分被组织成几个部分。

重要说明

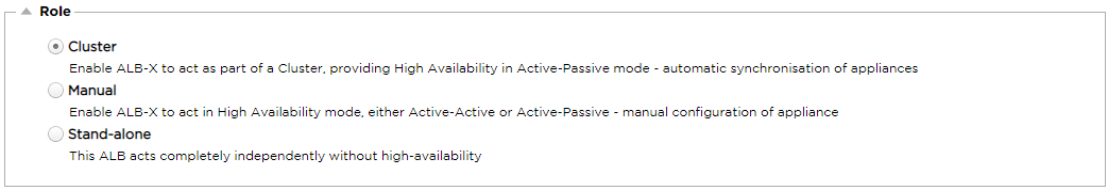
- 不需要在ADC对之间使用专用电缆来维持高可用性的心跳。
- 心跳与需要高可用性的虚拟服务在同一网络上进行。
- ADC设备之间不存在有状态的故障转移。
- 当在两个或多个ADC上启用高可用性时，每个盒子将通过UDP广播它被配置为提供的虚拟服务。
- 高可用性故障转移使用单播消息和Gratuitous ARP来通知新的Active负载平衡器交换机。



角色

当你为高可用性配置ADC时，有三种集群角色可用。

群体



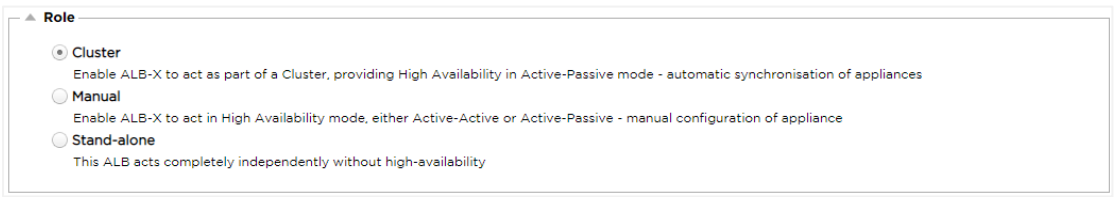
- 默认情况下，一个新的ADC将使用集群角色开机。在这个角色中，每个集群成员都有相同的"工作配置"，因此，在任何时候集群中只有一个ADC是活跃的。
- 一个 "工作配置
  "意味着所有的配置参数，除了需要唯一的项目，如管理IP地址、ALB名称、网络设置、接口细节等。
- 处于优先级1的ADC，也就是集群成员框中最上面的位置，是集群所有者和主动负载平衡器，而所有其他ADC是被动成员。
- 你可以编辑集群中的任何ADC，并且这些变化将同步到所有集群成员。
- 当你从集群中删除一个ADC时，所有的虚拟服务都将从该ADC中删除。
- 你不能把群集的最后一个成员删除到无主设备。要删除最后一个成员，请将角色改为手动或独立。
- 以下对象是不同步的。
    - 手动日期和时间部分 - (NTP部分是同步的)
    - 故障切换延迟（毫秒
    - 硬件部分
    - 家电部分
    - 网络部分

集群所有者的失败

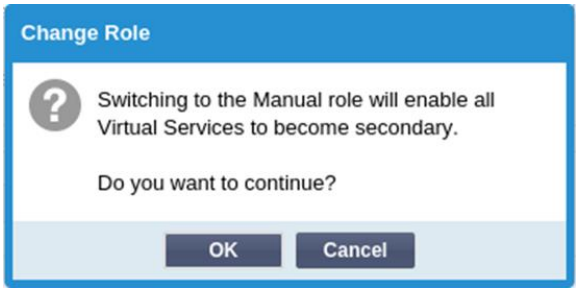
- 当集群所有者失败时，其余成员之一将自动接管并进行流量的负载平衡。
- 当集群所有者返回时，它将恢复负载平衡流量并接管所有者角色。
- 让我们假设所有者失败了，一个成员已经接管了负载平衡。如果你想让那个接管负载均衡流量的成员成为新的所有者，突出显示该成员，并点击向上的箭头，将其移到优先级1的位置。
- 如果你编辑剩下的群集成员之一，而群集的拥有者已经停机，那么被编辑的成员将自动晋升为拥有者，而不会有流量损失。

将角色从集群角色改为手动角色

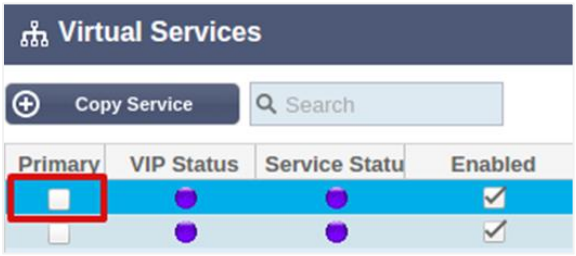
- 如果您希望将角色从集群改为手动，请点击手动角色选项旁边的单选按钮。



- 在你点击单选按钮后，你会看到以下信息。



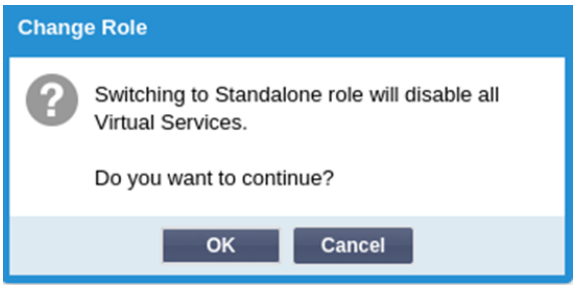
- 点击 "确定 "按钮
- 检查虚拟服务部分。你会发现，Primary一栏现在显示了一个未勾选的方框。



- 这是一个安全功能，意味着如果你有另一个具有相同虚拟服务的ADC，那么将不会中断流量。

从集群到独立的角色转变

- 如果你想把角色从集群改为单机，点击单机选项旁边的单选按钮。
- 你将被提示以下信息。



- 单击 "确定 "来改变角色。
- 检查你的虚拟服务。你会看到主栏的名称变成了独立的。
- 你还会看到，出于安全原因，所有的虚拟服务都被禁用（未被选中）。
- 一旦你确信同一网络上没有其他ADC有重复的虚拟服务，你就可以依次启用每一个虚拟服务。

手册作用

手动角色的ADC将与其他手动角色的ADC一起工作，以提供高可用性。与群集角色相比，主要的优势是能够为一个虚拟IP设置哪个ADC是活动的。缺点是，ADC之间没有配置同步。任何变化都必须通过GUI在每个盒子上手动复制，或者对于大量的变化，你可以从一个ADC创建一个jetPACK并将其发送到另一个。

- 要使一个虚拟IP地址 "激活"，请在主栏中勾选复选框（IP服务页）。

- 要使一个虚拟IP地址成为 "被动"，请在主栏中把复选框留空（IP服务页）。
- 在这种情况下，一个主动服务会失败到被动服务上。
    - 如果两个主要栏目都被勾选，那么就会发生一个选举过程，最低的MAC地址将被激活。
    - 如果两者都没有被选中，那么就会发生同样的选举过程。此外，如果两者都没有被选中，就不会自动返回到原来的活跃ADC。

独立的角色

处于独立角色的 ADC 将不会与任何其他 ADC
就其服务进行通信，因此所有的虚拟服务将保持绿色状态并连接。你必须确保所有的虚拟服务都有唯一的IP地址，否则在你的网络上会出现冲突。

设置

在设置部分，你可以设置故障转移延迟，以毫秒为单位，被动ADC在主动ADC故障后接管虚拟服务之前所要等待的时间。

我们建议将其设置为10000ms或10秒，但你可以根据你的网络和要求减少或增加这个值。可接受的值在1500 ms和20000ms之间。如果你在较低的延迟下遇到集群的不稳定，你应该增加这个值。

管理层

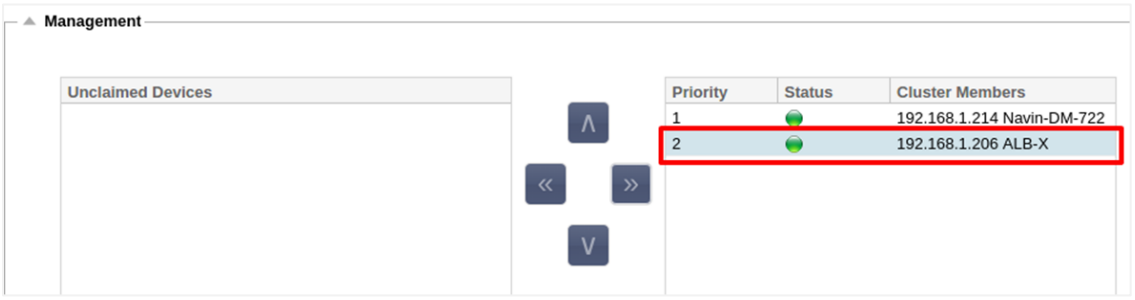
在这一部分，你可以添加和删除集群成员，同时也可以改变集群中一个ADC的优先级。该部分由两个面板和中间的一组方向键组成。左边的区域是无主设备，而最右边的区域是群集本身。

将一个ADC添加到集群中

- 在将ADC添加到集群中之前，你必须确保所有的ADC设备都已经在系统>网络部分提供了一个唯一的名称设置。
- 你应该看到ADC的优先级为1，状态为绿色，其名称在管理部分的群集成员栏下。这个ADC是默认的主设备。

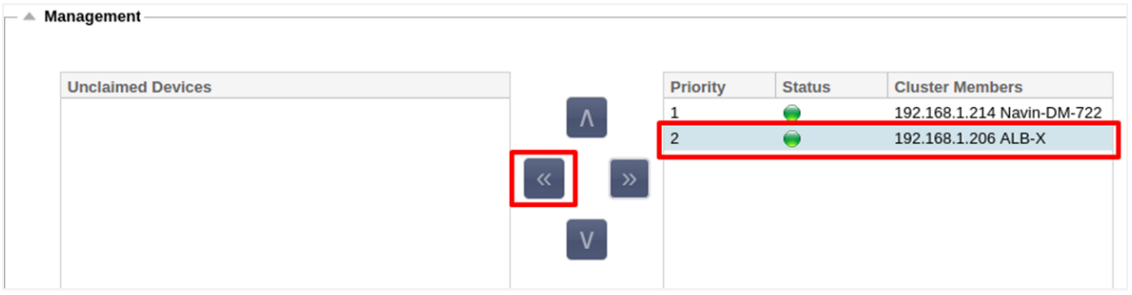
- 所有其他可用的 ADC
  将显示在管理部分的无主设备窗口中。无人认领的设备是指在群集角色中被分配的ADC，但没有配置虚拟服务。
- 突出显示无主设备窗口中的ADC，并点击右箭头按钮。
- 现在你将看到以下信息。

- 单击 "确定"，将ADC推广到集群中。
- 你的ADC现在应该在集群成员列表中显示为优先级2。



删除一个集群成员

- 突出显示你想从集群中删除的集群成员。
- 点击左边的箭头按钮。



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

改变一个ADC的优先级

有时，你可能希望改变成员名单中某个ADC的优先级。

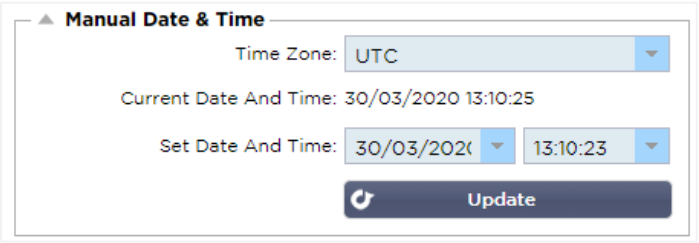
- 在集群成员列表顶部的ADC被赋予优先权1，是所有虚拟服务的活动ADC。

- 列表中排名第二的ADC被赋予优先级2，是所有虚拟服务的被动ADC。
- 要改变哪个ADC是活动的，只需选中该ADC并点击向上的箭头，直到它位于列表的顶部

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所处的时区。与时区一起，日期和时间在与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

你在这个字段中设置的值代表ADC所在的时区。

- 点击时区的下拉框，开始输入你的位置。
  例如，伦敦
- 当你开始输入时，ADC将自动显示包含字母L的位置。
- 继续输入 "Lon"，以此类推--列出的地点将被缩小到包含 "Lon "的地点。'
- 如果你在，比如说，伦敦，那么选择欧洲/伦敦来设置你的位置

如果在上述更改后，日期和时间仍然不正确，请手动更改日期。

设置日期和时间

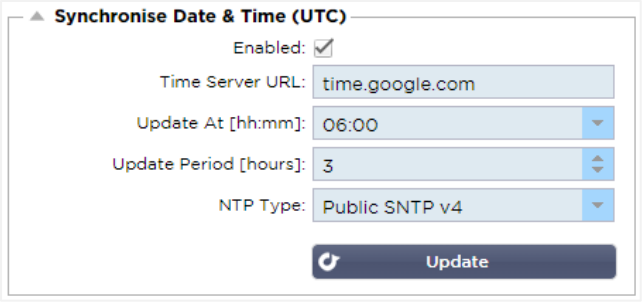
该设置代表实际的日期和时间。

- 从第一个下拉菜单中选择正确的日期或。
  或者，你也可以按以下格式输入日期：DD/MM/YYYY
- 加入以下格式的时间，hh: mm: ss，例如，06:00:10表示上午6点和10秒。
- 一旦你输入正确，请点击更新来申请。

- 然后，你应该看到新的日期和时间的粗体字。

同步日期和时间（UTC

你可以使用NTP服务器来准确同步你的日期和时间。NTP服务器位于全球，当你的基础设施对外部访问有限制时，你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）。如果该服务器是位于互联网上的全球服务器，我们建议使用FQDN。

在[hh:mm]更新

选择你希望ADC与NTP服务器同步的计划时间。

更新期[小时]。

选择你希望同步发生的频率。

NTP类型。

- 公共SNTP V4 - 这是目前与NTP服务器同步时的首选方法。**RFC 5905**
- NTP v1 Over TCP - 通过TCP的传统NTP版本。**RFC 1059**
- NTP v1 Over UDP - 通过UDP的传统NTP版本。**RFC 1059**

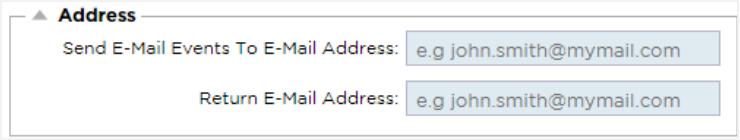
注意：请注意，同步只在UTC下进行。如果你想设置一个本地时间，只能手动完成。这一限制将在以后的版本中被改变，以便能够选择一个时区。

电子邮件活动

ADC是一个重要的设备，像任何重要的系统一样，它配备了通知系统管理部门任何可能需要注意的问题的能力。

系统 >
电子邮件事件页面允许你配置一个电子邮件服务器连接，并向系统管理员发送通知。该页面被组织成以下几个部分。

地址



发送到电子邮件事件到电子邮件地址

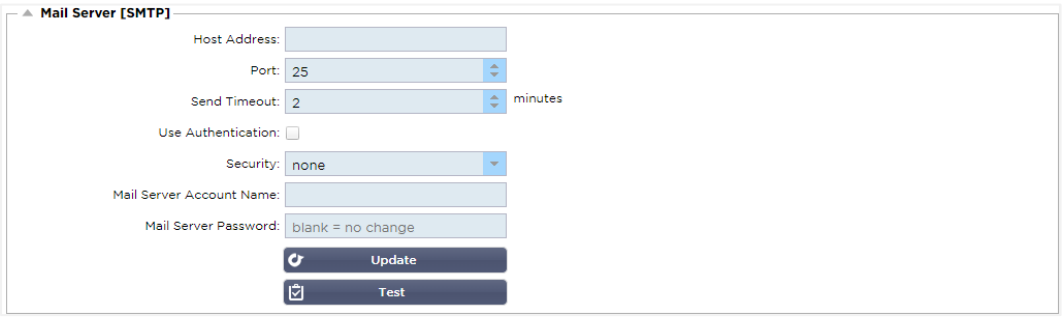
添加一个有效的电子邮件地址来发送警报、通知和事件。例如**SUPPORT@DOMAIN.COM**。

返回电子邮件地址。

加入一个将出现在收件箱中的电子邮件地址。例如**ADC@DOMAIN.COM**。

邮件服务器（SMTP

在这一部分，你需要添加用于发送电子邮件的SMTP服务器的详细信息。请确保你用于发送的电子邮件地址已被授权。



主机地址

加入你的SMTP服务器的IP地址。

港口

加入你的SMTP服务器的端口。SMTP的默认端口是25，如果你使用SSL，则为587。

发送超时

加入SMTP超时。默认设置为2分钟。

使用认证

如果你的SMTP服务器需要认证，请勾选该方框。

安全问题

- 无
- 默认设置为无。
- SSL - 如果你的SMTP服务器需要安全套接字层验证，请使用此设置。
- TLS - 如果你的SMTP服务器需要传输层安全认证，请使用此设置。

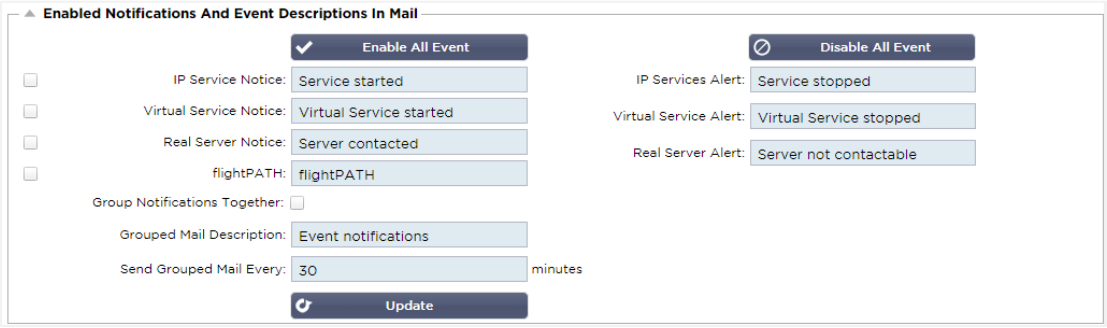
主服务器账户名称

加入认证所需的用户名。

邮件服务器密码

加入认证所需的密码。

通知和警报



有几种类型的事件通知，ADC将向配置为接收这些通知的人发送。你可以勾选并启用应该发送的通知和警报。当联系到真实服务器或启动通道时，就会发出通知。当Real Servers不能被联系到，或者通道停止工作时，就会发出警报。

IP服务

当任何虚拟IP地址在线或停止工作时，IP服务通知会通知你。这一操作是针对属于VIP的所有虚拟服务进行的。

虚拟服务

通知收件人一个虚拟服务是在线的或已经停止工作。

真实服务器

当一个真实服务器和端口被连接或无法联系时，ADC将发送真实服务器通知。

飞行路线

这个通知是当一个条件被满足时发出的电子邮件，并且有一个配置的动作指示ADC以电子邮件形式发送该事件。

团体通知

勾选将通知分组。勾选后，所有的通知和警报将被汇总到一封邮件中。

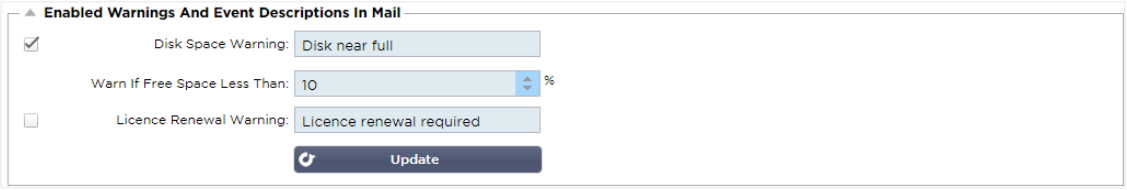
群发邮件描述

指定团体通知邮件的相关主题。

群组发送间隔

规定你希望在发送团体通知邮件前等待的时间。最短的时间是2分钟。

警告



有两种类型的警告邮件，都不应该被忽视。

磁盘空间

设置自由磁盘空间的百分比，在这之前发送警告。当达到这个百分比时，将向你发送电子邮件。

许可证过期

此设置允许你启用或禁用向系统管理员发送的许可证过期警告电子邮件。当达到这一点时，你将会收到电子邮件。

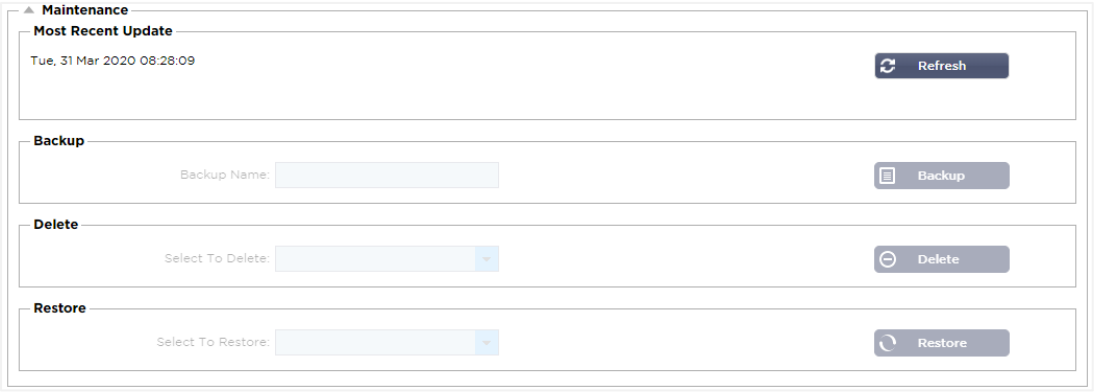
系统历史

在系统部分，有一个系统历史选项，允许提供诸如CPU、内存、每秒请求和其他功能的历史数据。一旦启用，你可以通过 "查看>历史
"页面以图形形式查看结果。这个页面也将允许你备份或恢复你的历史文件到本地ADC。

收集数据

- 要启用数据收集，请勾选该复选框。
- 接下来，设置你希望ADC收集数据的时间间隔。这个时间值可以在1-60秒之间。

维护



如果你已经启用了历史日志记录，这部分将是灰色的。请取消 "收集数据 "部分的 "已启用 "复选框，并单击 "更新 "以允许维护历史日志。

备份

给你的备份一个描述性的名字。点击备份，将所有文件备份到ADC上

删除

从下拉列表中选择一个备份文件。单击 "删除 "从ADC中删除备份文件。

恢复

选择一个以前存储的备份文件。单击 "恢复"，从该备份文件中填充数据。

许可证

ADC的使用许可取决于你的购买参数和客户类型，可以使用以下模式之一。

许可证类型	描述
永久的	你，客户，有权永久使用ADC和其他软件。这并不排除你必须购买支持以获得援助和更新。
SaaS	SaaS或软件即服务（Software-as-a-Service）意味着你基本上是以持续或随用随付的方式租用软件。在这种模式下，你每年为软件支付租金。你没有永久使用该软件的权利。
MSP	管理服务提供商可以将ADC作为一项服务来提供，并按每个VIP购买许可证，每年收费和支付。

许可证详情

每个许可证包括与购买它的个人或组织有关的具体细节。

许可证编号

这个许可证ID与机器ID和其他特定于你的购买和ADC的细节直接相关。这一信息是至关重要的，当你希望从App Store检索更新和其他项目时，需要这一信息。

机器ID

机器ID是使用虚拟ADC设备的eth0 IP地址和基于硬件的ADC的MAC ID生成的。如果你改变虚拟ADC设备的IP地址，许可证将不再有效。你将不得不联系支持部门寻求帮助。我们建议你的虚拟ADC设备有固定的IP地址，并说明不要改变它们。可以通过在HTTPs://edgenexus.io上开票来获得技术支持。

注意：你不能改变你的ADC设备的IP地址或MAC ID。如果你是在一个虚拟化的框架中，那么请固定MAC ID和IP地址。

发给

该值包含与ADC的机器ID相关的购买者名称。

联系人

该值包含与机器ID相关的客户公司的联系人。

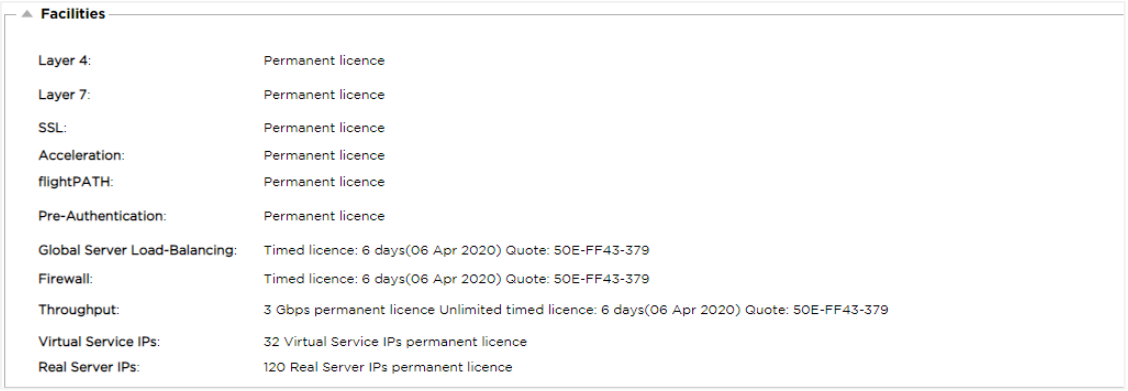
日期问题

许可证的签发日期

命名

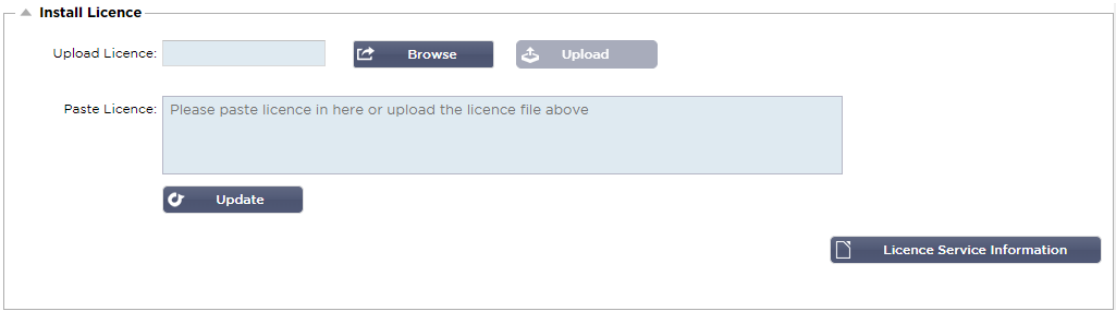
此值显示你所提供的ADC设备的描述性名称。

设施



设施部分为您提供关于ADC内哪些功能已被许可使用以及许可有效期的信息。同时显示的还有ADC已被授权的吞吐量和真实服务器的数量。这些信息取决于你所购买的许可证。

安装许可证



- 安装一个新的许可证非常简单。当您从Edgenexus收到您的新许可证或替换许可证时，它将以文本文件的形式发送。您可以打开该文件，然后将其内容复制并粘贴到粘贴许可证字段中。
- 如果复制/粘贴对你来说不是一个选项，你也可以把它上传到ADC。
- 一旦你完成了这些，请点击更新按钮
- 许可证现在已经安装完毕。

许可证服务信息

点击 "许可证服务信息 "按钮将显示许可证的所有信息。这个功能可用于将细节发送给支持人员。

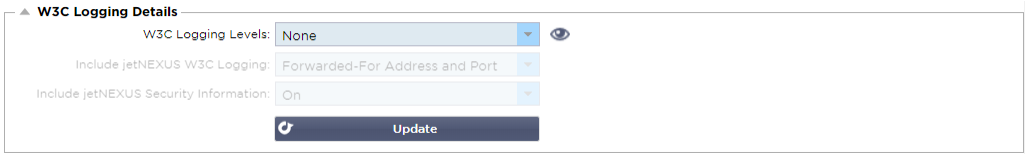
伐木

在 "系统">"日志
"页面，你可以设置W3C的日志级别，并指定自动输出日志的远程服务器。该页面分为以下四个部分。

万维网联盟记录细节

启用W3C日志将使ADC开始记录一个W3C兼容的日志文件。W3C日志是Web服务器的访问日志，其中生成的文本文件包含关于每个访问请求的数据，包括源互联网协议（IP）地址、HTTP版本、浏览器类型、引用者页

面和时间戳。该格式是由万维网联盟（W3C）开发的，该组织旨在促进网络发展的标准。该文件是ASCII文本，以空格分隔的列。该文件拥有以#字符开头的注释行。这些注释行之一是表明字段（提供列名）的行，以便数据可以被挖掘出来。有单独的文件用于HTTP和FTP协议。



W3C日志级别

有不同的记录级别，根据服务类型，提供的数据也不同。

价值	描述
无	W3C的记录是关闭的。
简介	#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）.
全程	这是一种与处理器更兼容的格式，有独立的日期和时间字段。关于这些字段的含义，请参见下面的字段摘要。现在的字段是。#Fields: date time 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).
场地	这种格式与 "完整 "非常相似，但有一个额外的字段。关于这些字段的含义，请看下面的字段摘要。存在的字段是。#Fields: date time 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) referer 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) 。
诊断性	这种格式充满了与发展和支持人员有关的各种信息。关于这些字段的含义，请参见下面的字段摘要。 存在的字段有：。#Fields:日期 时间 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-imes(new,rcon,rqf,rql,tqf,tql,rsf,tsf,tsl,dis,log) x-closed-by x-compress-action x-sc(Content-Type) x-cache-action X-finish

下表描述了W3C HTTP的日志级别。

下表描述了W3C FTP的日志记录级别。

价值	描述
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
全程	#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
诊断性	#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

价值	描述
客户的网络地址和端口	这里显示的值显示实际的客户端IP地址和端口。
客户的网络地址	这个选项将包括并只显示实际的客户IP地址。
转发的地址和端口	该选项将显示XFF头中的细节，包括地址和端口。
转发的地址	这个选项将显示XFF头中的细节，只包括地址。

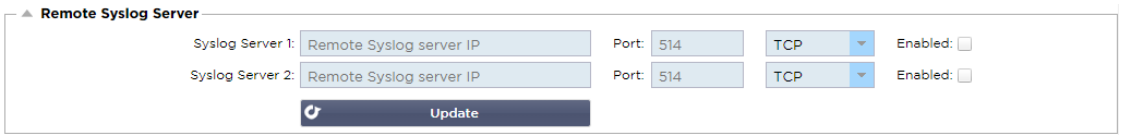
这个选项允许你设置哪些ADC信息应该包括在W3C日志中。

包括安全信息

价值	描述
在	这个设置是全局的。当设置为 "开 "时，当任何虚拟服务使用认证并启用W3C日志时，用户名将被追加到W3C日志中。
关闭	这将在全局范围内关闭将用户名记录到W3C日志的能力。

该菜单由两个选项组成。

远程Syslog服务器



在本节中，你可以配置两个外部Syslog服务器来发送所有的系统日志。

- 添加你的Syslog服务器的IP地址
- 添加端口
- 选择TCP或UDP

- 勾选方框
- 点击更新

远程日志存储

所有的W3C日志都以压缩的形式每小时存储到ADC上。当磁盘空间剩余30%时，最旧的文件将被删除。如果你希望将这些文件导出到远程服务器上保存，你可以使用SMB共享来配置。请注意，在文件完成和压缩之前，W3C日志不会传输到远程位置。由于日志是每小时写一次，这在虚拟机设备中可能需要两个小时，在硬件设备中可能需要五个小时。

Col1	Col2
远程日志存储	勾选方框，启用远程日志存储
IP地址	指定你的SMB服务器的IP地址。这应该是十进制的点号。例如：10.1.1.23
股份名称	指定SMB服务器上的共享名称。例如：w3c。
指南	指定SMB服务器上的目录。例如。/log。
帐号	指定SMB共享的用户名。
密码	指定SMB共享的密码

我们将在未来的版本中包括一个测试按钮，以提供一些反馈，证明你的设置是正确的。

现场总结

状况	描述
日期	非本地化=总是YYY-MM-DD（GMT/UTC）。
时间	非本地化 = HH:MM:SS 或 HH:MM:SS.ZZZ (GMT/UTC) * 注意-- 不幸的是，这有两种格式（Site
	没有.ZZZ毫秒）。)
x-mil	只有网站格式=时间戳的毫秒数
c-ip	客户端IP可以从网络或X-Forwarded-For头中得到最好的信息

c-port	从网络或X-Forwarded-For报头中可以得到的最好的客户端口
cs-username	客户的用户名请求字段
s-ip	ALB的监听端口
s-port	ALB的聆听贵宾
x-xff	X-Forwarded-For头的值
x-xffcustom	配置命名的X-Forwarded-For类型请求头的值
cs-host	请求中的主机名称
x-r-ip	使用的Real服务器的IP地址
x-r-port	使用的真实服务器的端口
cs-方法	HTTP请求方法 *除简要格式外
方法	* 只有简短的格式使用此名称的cs-方法
cs-uri-stem	所请求的资源的路径 *除简要格式外
cs-uri-query	对所请求的资源进行查询 * 除简要格式外
uri	*简短的格式记录了一个组合的路径和查询-字符串
状况	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	引荐页（由客户发送
x-c-version	客户端请求的HTTP版本
x-r-version	内容-服务器的响应 HTTP版本
cs-bytes	来自客户端的字节，在请求中
sr-bytes	转发给Real服务器的字节，在请求中
rs-bytes	来自Real服务器的字节，在响应中
编码	发送给客户端的字节，在响应中
x-percent	压缩百分比 * = 100 * (1 - 输出/输入) 包括头文件
所需时间	真实服务器花了多长时间（秒）？
x-trip-times 新 pcon	从连接到在 "新手名单 "上发帖的毫秒时间 从连接到放置连接到真实服务器的毫秒时间
acon	从连接到完成与真实服务器的连接的毫秒。

ĂĂĂ	从连接到建立真实服务器连接的毫秒时间
ĂĂĂ	从连接到接收到客户端的第一个字节的请求的一毫秒
rql	从连接到收到客户端最后一个字节的请求的毫秒数
tqf	从连接到向真实服务器发送第一个字节的请求的毫秒。
tql	从连接到向真实服务器发送最后一个字节的请求的毫秒。
ĂĂĂ	从连接到收到来自真实服务器的第一个字节的响应的毫秒。
rsl	从连接到接收来自真实服务器的最后一个字节的响应的毫秒。
tsf	从连接到向客户发送第一个字节的响应的毫秒。
tsl	从连接到向客户发送最后一个字节的响应的毫秒。
弃权	从连接到断开的毫秒（双方--最后一个断开的）。
原木	从连接到此日志记录的毫秒，通常紧随其后的是（负载平衡政策和推理）。
x-round-trip-time	ALB用了多长时间（秒）？
x-closed-by	什么行动导致连接被关闭（或保持开放）？
x-compress-action	如何进行压缩，或防止压缩
x-sc(Content-Type)	响应的内容-类型
x-cache-action	缓存是如何反应的，或被阻止的
x-finish	引起该日志行的触发器

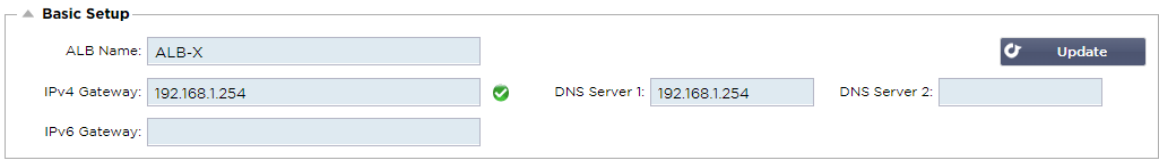
清除日志文件

这项功能允许你清除ADC中的日志文件。你可以从下拉菜单中选择你想删除的日志类型，然后点击清除按钮。

网络

库中的网络部分允许对ADC的网络接口及其行为进行配置。

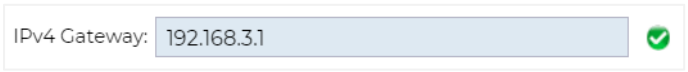
基本设置



ALB名称

为你的 ADC 设备指定一个名称。请注意，如果集群中有不止一个成员，则不能改变这个名称。请参阅 "集群"一节。

IPv4网关



指定IPv4网关地址。这个地址将需要与现有的适配器在同一个子网中。如果你添加的网关不正确，你会看到一个红圈中的白叉。当你添加一个正确的网关时，你会在页面底部看到一个绿色的成功标语，在IP地址旁边的绿色圆圈里有一个白色的勾。

IPv6网关

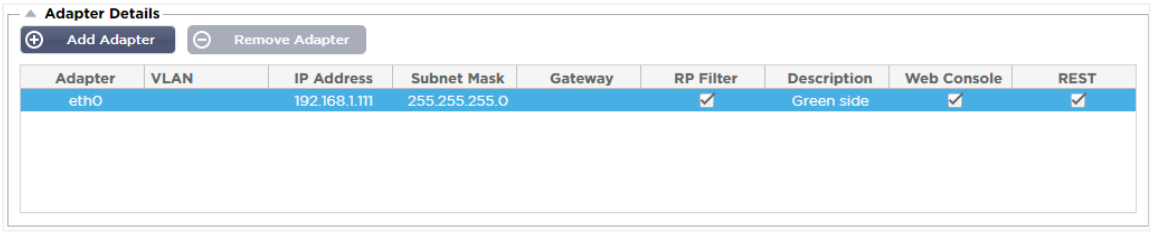
指定IPv6网关地址。这个地址将需要与现有的适配器在同一个子网中。如果你添加的网关不正确，你会看到一个红圈中的白叉。当你添加一个正确的网关时，你会看到页面底部有一个绿色的成功标语，在IP地址旁边的绿色圆圈里有一个白色的勾。

DNS服务器1和DNS服务器2

加入你的第一个和第二个（可选）DNS服务器的IPv4地址。

适配器详细信息

网络面板的这一部分显示安装在ADC设备中的网络接口。你可以根据需要添加和删除适配器。

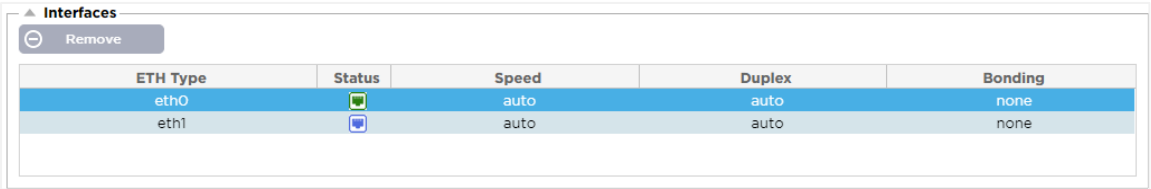


栏目	描述
适配器	这一栏显示设备上安装的物理适配器。通过点击从可用的适配器列表中选择一个适配器--双击将使列表行进入编辑模式。
VLAN	双击来添加适配器的VLAN ID。VLAN是一个虚拟局域网，它创建了一个独特的广播域。VLAN具有与物理局域网相同的属性，但

	它允许终端站在不在同一网络交换机上的情况下更容易地被分组到一起。
IP地址	双击来添加与适配器接口相关的IP地址。你可以在同一个接口上添加多个IP地址。这应该是一个IPv4的32位数字，采用四点十进制的符号。例如192.168.101.2
子网掩码	双击来添加分配给适配器接口的子网掩码。这应该是一个IPv4的32位数字，采用四点十进制的符号。例如255.255.255.0
闸门	为该接口添加一个网关。当添加了这个后，ADC将设置一个简单的策略，允许从这个接口发起的连接通过这个接口返回到指定的网关路由器。这使得ADC可以安装在更复杂的网络环境中，而不需要手动配置复杂的基于策略的路由。
描述	双击来为你的适配器添加描述。例如公共接口。 注意：ADC将自动命名第一个接口为绿色面，第二个接口为红色面，第三个接口为第三面等。 请随时根据你自己的选择改变这些命名惯例。
网络控制台	双击这一栏，然后勾选方框，将该接口指定为图形用户界面Web Console的管理地址。在改变Web Console要监听的接口时，请非常小心。你需要有正确的路由设置，或者与新的接口在同一个子网中，以便在改变后到达Web Console。唯一的办法是进入命令行，发出set greenside命令，把它改回来。这将删除除eth0以外的所有接口。

接口

网络面板内的接口部分允许配置与网络接口有关的某些元素。你也可以通过点击移除按钮从列表中移除一个网络接口。当你使用一个虚拟设备时，你在这里看到的接口是由底层虚拟化框架限制的。



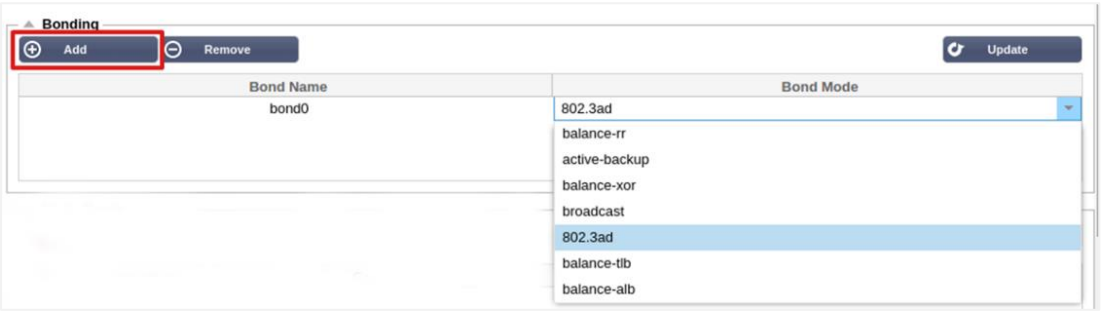
栏目	描述
ETH类型	这个值表示操作系统对网络接口的内部参考。这个字段不能被定制。数值从ETH0开始，并根据网络接口的数量依次进行。
状况	这个图形指示显示了网络接口的当前状态。绿色状态显示接口已连接并正常。其他状态指示器显示如下。 **适应性提高** 适配器下移 适配器拔掉 适配器缺失
速度	默认情况下，该值被设置为自动协商速度。但你可以将接口的网络速度改为下拉菜单中的任何数值（10/100/1000/AUTO）。
复式	这个字段的值是可定制的，你可以在自动（默认）、全双工和半双工之间进行选择。
粘合	你可以选择你所定义的粘合类型之一。更多细节请参见 "结合 "一节。

粘合

许多名称被用来命名网络接口绑定。端口中继、通道绑定、链路聚合、网卡组队，以及其他。绑定将多个网络连接合并或聚合成一个通道绑定的接口。绑定允许两个或多个网络接口作为一个，增加吞吐量，并提供冗余或故障转移。

ADC的内核有一个内置的Bonding驱动，用于将多个物理网络接口聚合成一个逻辑接口（例如，将eth0和eth1聚合成bond0）。对于每个绑定的接口，你可以定义模式和链接监控选项。有七个不同的模式选项，每个选项都提供特定的负载平衡和容错特性。如下图所示。

注意：绑定只能为基于硬件的ADC设备进行配置。



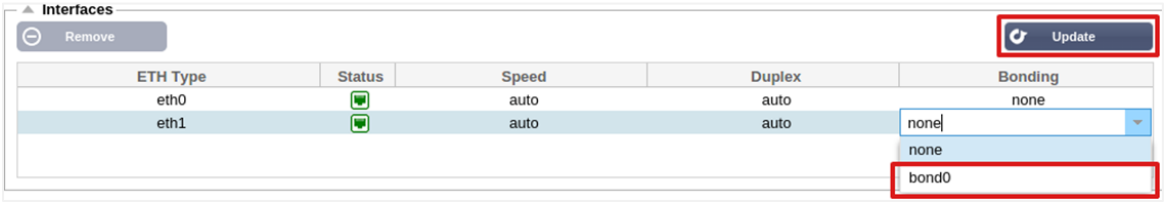
创建一个绑定的配置文件

- 点击 "添加 "按钮，添加一个新的债券
- 为绑定配置提供一个名称

- 选择你希望使用的粘合模式

然后从 "接口 "部分，从网络接口的 "粘合 "下拉字段中选择你想使用的粘合模式。

在下面的例子中，eth0、eth1和eth2现在是bond0的一部分。而Eth0仍然作为管理接口独立存在。

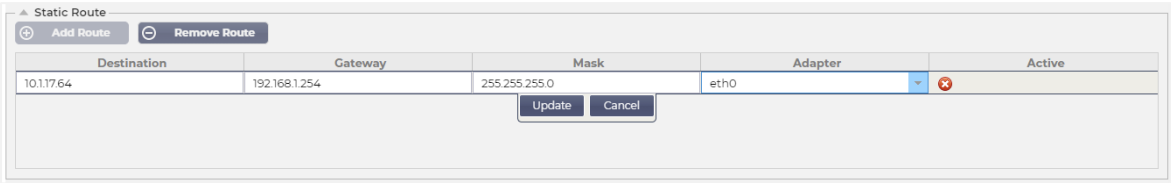


粘合模式

粘合模式	描述
平衡-rr。	数据包按顺序逐一通过每个接口传输/接收。
主动备份。	在这种模式下，一个接口将处于活动状态，第二个接口将处于待机状态。这个次要的接口只有在第一个接口上的活动连接失败时才会变成活动的。
平衡-xor。	根据源MAC地址与目的MAC地址XOR的方式进行传输。该选项为每个目标MAC地址选择相同的从属设备。
播报。	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规范利用活动聚合器中的所有从机。
balance-tlb。	自适应传输负载平衡绑定模式。提供不需要任何特殊交换机支持的通道绑定。传出的流量根据每个从站的当前负载（相对于速度计算）进行分配。当前的从属设备接收传入的流量。如果接收的从属设备发生故障，另一个从属设备将接管故障接收从属设备的MAC地址。
平衡-alb。	自适应负载平衡绑定模式：也包括平衡-TLB和IPV4流量的接收负载平衡（rlb），不需要任何特殊的交换机支持。接收负载平衡是通过ARP协商实现的。绑定驱动程序拦截本地系统发出的ARP回复，并以绑定中的一个从机的唯一硬件地址覆盖源硬件地址，这样，不同的对等体对服务器使用不同的硬件地址。

静态路线

有时，你需要为你的网络中的特定子网创建静态路由。ADC为你提供了使用静态路由模块来实现这一功能的能力。



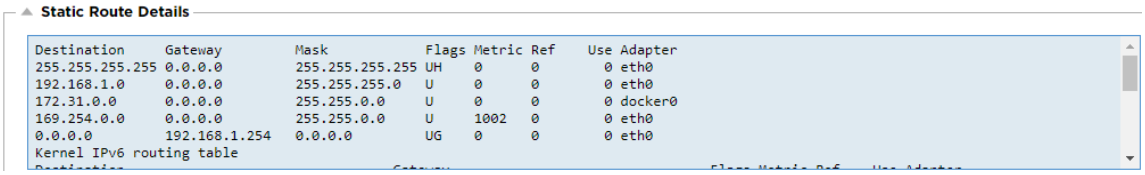
添加静态路由

- 点击添加路线按钮
- 以下表中的详细资料为指导，填写该领域。
- 完成后点击更新按钮。

场地	描述
目的地	以十进制点号输入目的网络地址。例如：123.123.123.5
闸门	以十进制点号输入网关的 IPv4 地址。例子 10.4.8.1
面罩	以十进制点号输入目标子网掩码。例如：255.255.255.0
适配器	输入可以到达网关的适配器。例如eth1。
活跃	一个绿色的钩框将表示可以到达网关。红叉表示在该接口上不能到达网关。请确保你已经在与网关相同的网络上设置了一个接口和IP地址。

静态路由详细信息

本节将提供关于ADC上配置的所有路由的信息。



高级网络设置

Nagle是什么？

Nagle的算法通过减少需要在网络上发送的数据包数量来提高TCP/IP网络的效率。参见**维基百科关于NAGLE的文章**

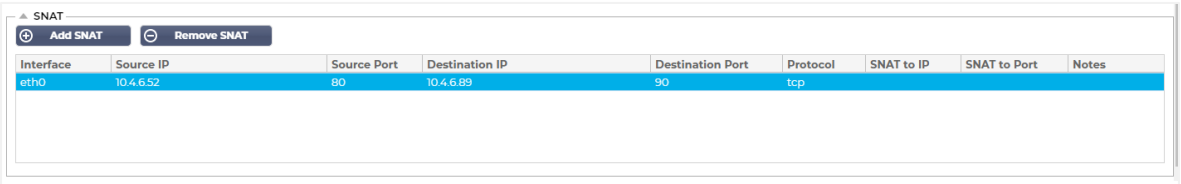
服务器 Nagle

勾选此框，以启用服务器Nagle设置。Server 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网络效率的手段。这个设置适用于交易的服务器端。由于Nagle和延迟ACK可能会严重影响性能，所以必须对服务器设置加以注意。

客户 Nagle

勾选方框，启用客户Nagle设置。同上，但适用于交易的客户端。

SNAT



SNAT是源网络地址转换的意思，不同的供应商对SNAT的实现有轻微的差异。对EdgeADC SNAT的一个简单解释如下。

在正常情况下，入站请求将被引导到VIP，VIP会看到请求的源IP。例如，如果一个浏览器端点的IP地址是81.71.61.51，这对VIP来说是可见的。

当SNAT生效时，请求的原始源IP将从VIP那里隐藏，相反，它将看到SNAT规则中提供的IP地址。SNAT可以在第4层和第7层负载平衡模式下使用。

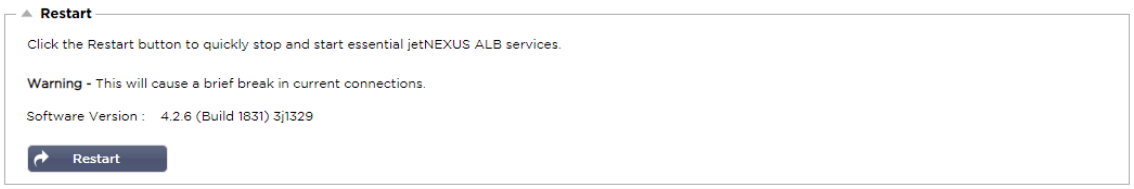
场地	描述
来源于IP	源IP地址是可选的，它可以是一个网络IP地址（带/掩码）或一个普通IP地址。掩码可以是一个网络掩码，也可以是一个普通数字，指定网络掩码左边的1的数量。因此，/24的掩码相当于255.255.255.0。
目的地IP	目的地IP地址是可选的，它可以是一个网络IP地址（带/掩码）或一个普通IP地址。掩码可以是一个网络掩码，也可以是一个普通数字，指定网络掩码左边的1的数量。因此，/24的掩码相当于255.255.255.0。
源港	源端口是可选的，它可以是一个单一的数字，在这种情况下，它只指定该端口，或者它可以包括一个冒号，这指定了一系列的端口。例如。80或5900:5905。
目的地港口	目标端口是可选的，它可以是一个单一的数字，在这种情况下，它只指定该端口，或者它可以包括一个冒号，这指定了一系列的端口。例如。80或5900:5905。
议定书	你可以选择是在单个协议上使用SNAT，还是在所有协议上使用。我们建议要具体一点，以便更精确。
SNA	SNAT到IP是一个强制性的IP地址或一系列的IP地址。例如。10.0.0.1或10.0.0.1-10.0.0.3。

T转IP	
SNAT to Port	SNAT到端口是可选的，它可以是一个单一的数字，在这种情况下，它只指定该端口，或者它可以包括一个破折号，这指定了一个端口范围。例如。80或5900-5905。
笔记	用这个来放一个友好的名字来提醒自己为什么会有这些规则存在;-)。这对于在Syslog中进行调试也很有用。

权力

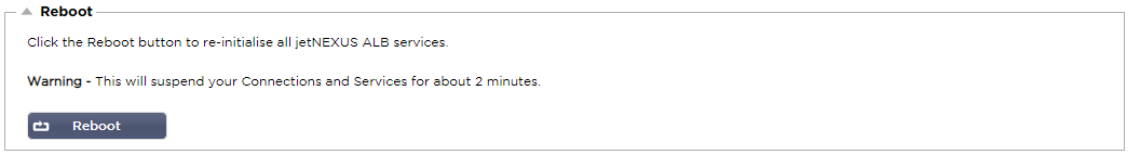
这个ADC系统功能还允许你在你的ADC上进行一些与电源有关的任务。

重新启动



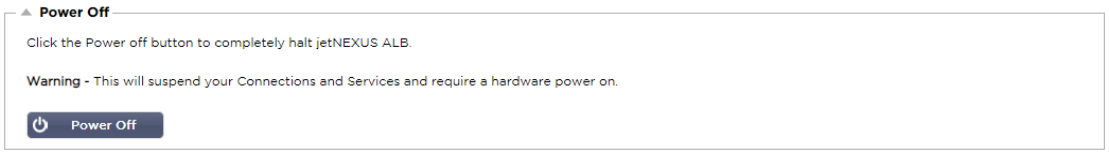
这个设置启动了所有服务的全局重启，因此中断了所有当前活动的连接。所有的服务将在短时间内自动恢复，但时间将取决于配置了多少个服务。将会显示一个弹出窗口，要求确认重启行动。

重新启动



点击 "重启
"按钮将对ADC进行电源循环，并自动使其恢复到活动状态。将会显示一个弹出窗口，要求确认重启行动。

关闭电源



点击 "关闭电源
"按钮将关闭ADC。如果这是一个硬件设备，你将需要对该设备进行物理访问，以使其重新启动。将显示一个弹出窗口，要求确认关机操作。

安全问题

这一部分允许你改变网络控制台的密码，并启用或禁用安全壳访问。它还允许启用REST API功能。

SSH

选项	描述
安全外壳远程连接	如果你希望使用SSH访问ADC，请勾选该方框。"Putty "是一个很好的应用程序，可以做到这一点。

网络控制台

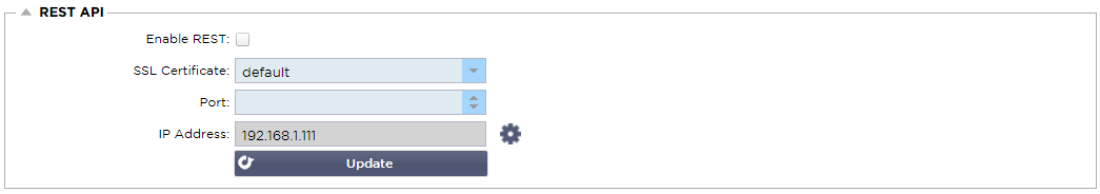
SSL证书

从下拉列表中选择一个证书。你选择的证书将用于保护你与ADC的网络用户界面的连接。你可以在ADC中创建一个自签名的证书，或者从**SSL证书**部分导入一个。

选项	描述
安全端口	网络控制台的默认端口是TCP 443。如果你出于安全原因希望使用一个不同的端口，你可以在这里改变它。

REST API

REST API，也被称为RESTful API，是一个符合REST架构风格的应用编程接口，允许配置ADC或从ADC提取数据。REST一词代表表征性状态转移，是由计算机科学家罗伊-菲尔丁创造的。



选项	描述
启用REST	勾选此框以启用使用REST API的访问。注意，你还必须配置启用REST的哪个适配器。见下面Cog链接的说明。
SSL证书	为REST服务选择一个证书。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。使用443以外的端口是一个好主意。

IP地址	这将显示REST服务所绑定的IP地址。你可以点击Cog链接，进入网络页面，改变REST服务启用的适配器。
齿形链接	点击这个链接将带你到网络页面，在那里你可以为REST配置一个适配器。

REST API的文档

关于如何使用REST API的文档有：**jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

注意：如果你在Swagger页面上遇到错误，这是因为他们在支持查询字符串方面有问题。
滚动到jetNEXUS REST API的错误处。

实例

使用CURL的GUID。

- 指挥部

```
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

许可证详情

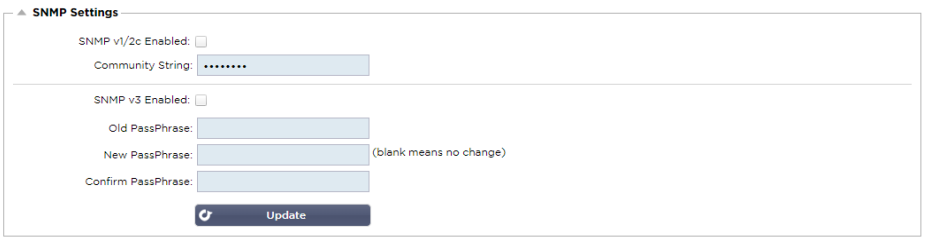
- 指挥部

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

SNMP

SNMP部分允许配置驻留在ADC内的SNMP
MIB。然后，MIB可以由能够与配备SNMP的设备进行通信的第三方软件进行查询。

SNMP设置



选项	描述
SNMP v1 / V2C	勾选该复选框以启用V1/V2C MIB。 SNMP v1符合RFC-1157的规定。SNMP V2c符合RFC-1901-1908。

SNMP v3	勾选复选框以启用V3 MIB。RFC-3411-3418。 V3的用户名是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，由管理器用来检索SNMP信息。默认的社区字符串是jetnexus
句式	这是启用SNMP v3时需要的密码，必须至少有8个字符或更多，仅包含字母Aa-Zz和数字0-9。默认的口令是**jetnexus。**

SNMP MIB

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

MIB下载

该MIB可以在这里下载。

ADC OID

ROOT OID

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

我们的OIDs

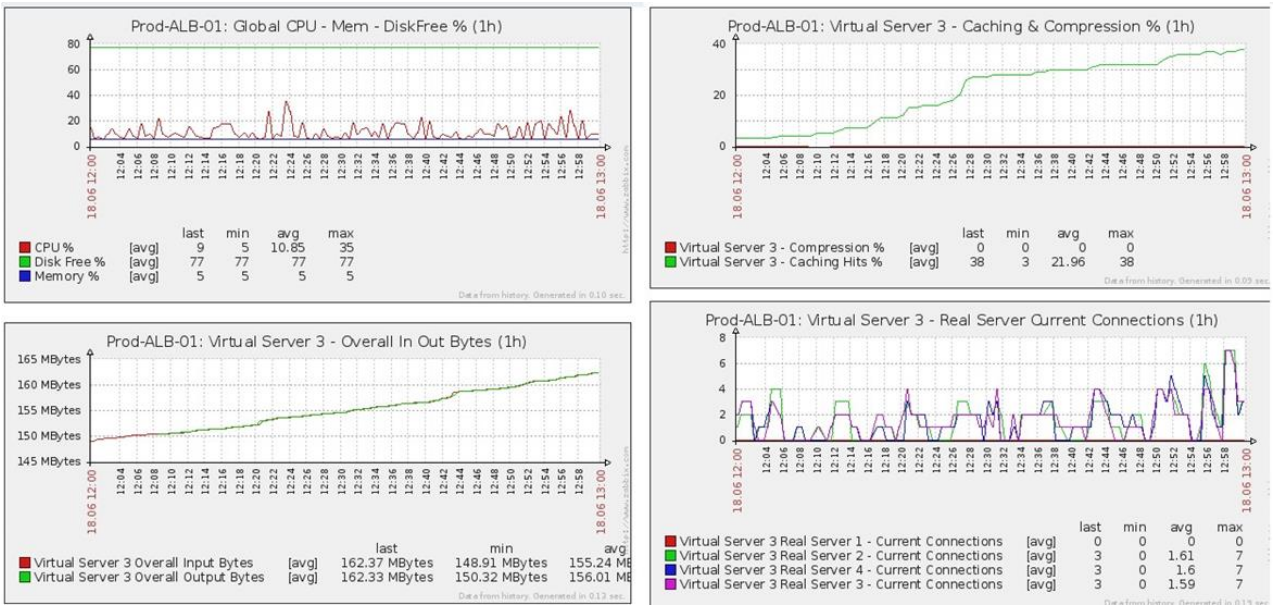
.....38370个jetnexusMIB
.1 **jetnexusData** (1.3.6.1.4.1.38370.1)
.1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
.2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
.3 **jetnexusServers** (1.3.6.1.4.1.38370.1.3)
.1 **jetnexusGlobal**（1.3.6.1.4.1.38370.1.1）。
.1 **jetnexusOverallInputBytes** (1.3.6.1.4.1.38370.1.1.1.0)
.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**（1.3.6.1.4.1.38370.1.1.**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（1.3.6.1.4.1.38370.1.1.11）。

历史图表

ADC的自定义SNMP
MIB的最佳用途是能够将历史图表卸载到你选择的管理控制台。下面是Zabbix的一些例子，这些例子对ADC的上述各种OID值进行轮询。



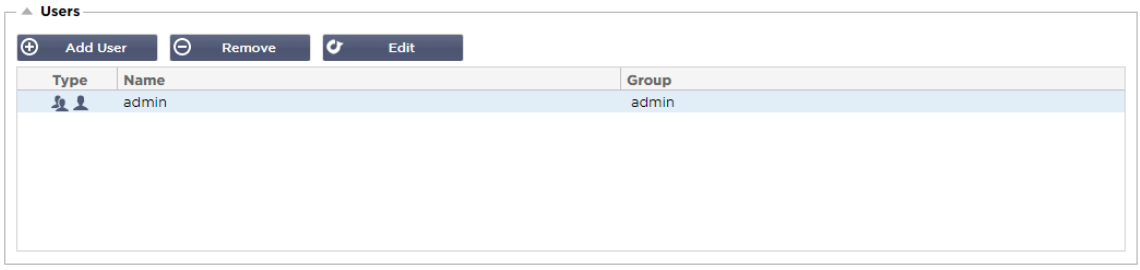
用户和审计日志

ADC提供了拥有一套内部用户的能力，以配置和定义ADC的工作。在ADC内定义的用户可以执行各种操作，这取决于附属于他们的角色。

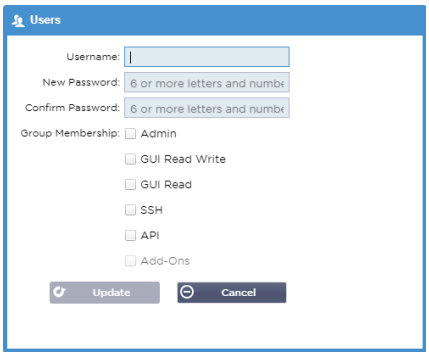
在第一次配置ADC时，有一个叫**admin的**默认用户，你可以使用它。admin的默认密码是**jetnexus**。

用户

用户部分提供给你创建、编辑和删除ADC中的用户。



添加用户



点击上图所示的添加用户按钮，弹出添加用户对话框。

参数	描述/用途
帐号	输入一个你选择的用户名 该用户名必须遵守以下规定。 • 最小字符数 1 • 最大字符数 32 • 字母可以是大写和小写 • 可以使用数字 • 不允许使用符号
密码	输入一个符合以下要求的**强**密码 • 最小字符数 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 • 符号是允许的，但以下例子中的符号除外 **£, %, & , < , >**
确认密码	再次确认密码以确保其正确性
集团成员	勾选你希望用户所属的组别。 • 管理员 - 这个组可以做任何事情 • GUI 读写 - 该组的用户可以访问 GUI，并通过 GUI 进行更改。 • GUI读取 - 该组的用户可以访问GUI，只查看信息。不能做任何改变 • SSH - 该组的用户可以通过安全壳访问ADC。这个选择将允许访问命令行，它有一组最小的可用命令 • API - 该组的用户将可以访问SOAP和REST的可编程接口。REST将从软件版本4.2.1开始提供。

用户类型

本地用户

单机或手动H/A角色中的ADC将只创建本地用户

默认情况下，一个名为 "admin

"的本地用户**是管理员组的成员。为了向后兼容，这个用户永远不能被删除。**

你可以改变这个用户的密码或将其删除，但你不能删除最后一个本地管理员。

集群用户

群集中的ADC角色将只创建群集用户

群集用户在群集的所有ADC中同步。

对集群用户的任何改变都会在集群的所有成员上发生改变。

如果你以集群用户的身份登录，你将无法将角色从集群切换到手动或单机。

集群和本地用户

任何在独立或手动角色下创建的用户都将被复制到群集。

如果ADC后来离开了集群，那么只有本地用户会保留下来

用户最后配置的密码将是有效的

删除一个用户

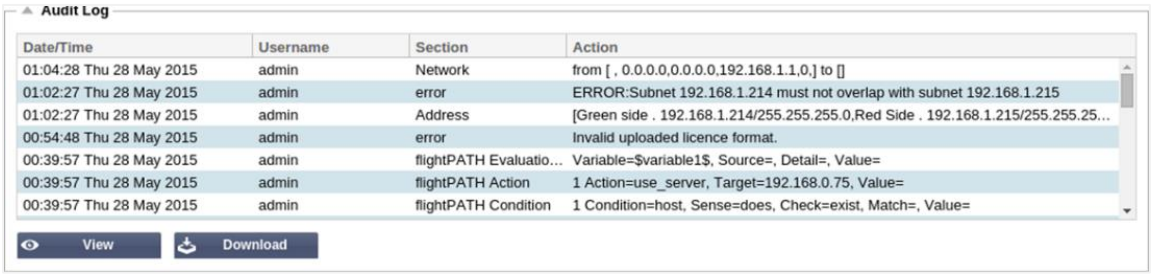
- 突出一个现有的用户
- 点击删除
- 你将无法删除目前已登录的用户
- 你将无法删除管理组中的最后一个本地用户
- 你将无法删除管理员组中最后剩下的集群用户
- 为了向后兼容，你将不能删除管理员用户。
- 如果你从集群中移除ADC，除本地用户外的所有用户将被删除

编辑一个用户

- 突出一个现有的用户
- 点击编辑
- 你可以通过勾选适当的方框和更新来改变用户的组别成员资格。
- 你也可以改变用户的密码，只要你有管理权限

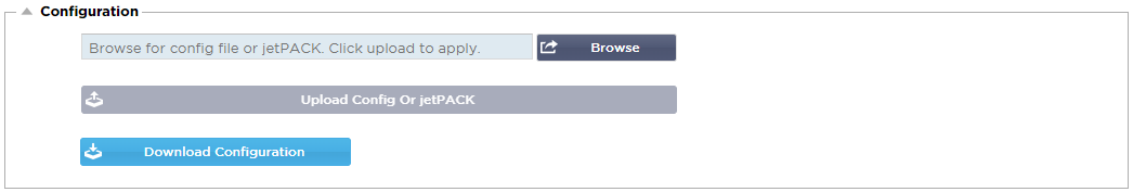
审计日志

ADC会记录个人用户对ADC配置所做的更改。审计日志将提供所有用户进行的最后50个操作。你也可以在日志部分看到所有条目。例如。



高级

配置



一旦ADC完全设置好并按要求工作，下载并保存其配置始终是最佳做法。你可以使用配置模块来下载和上传配置。

Jetpacks是标准应用程序的配置文件，由Edgenexus提供，以简化你的工作。这些也可以使用配置模块上传到ADC。

配置文件本质上是一个基于文本的文件，因此，您可以使用文本编辑器（如Notepad++或VI）进行编辑。一旦按要求编辑完毕，就可以将配置文件上传到ADC。

下载一个配置

- 要下载ADC的当前配置，请按下载配置按钮。
- 将出现一个弹出窗口，要求你打开或保存.conf文件。
- 保存到一个方便的位置。
- 你可以用任何文本编辑器打开它，如Notepad++。

上传配置

- 你可以通过浏览保存的.conf文件来上传保存的配置文件。
- 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。如果它没有自动刷新浏览器，请点击浏览器上的刷新。
- 完成后，你将被转到仪表板页面。

上传一个JetPACK

- JetPACK是对现有配置的一组配置更新。
- jetPACK可以小到改变TCP超时值，大到Microsoft Exchange或Microsoft Lync等完整的特定应用配置。
    - 你可以从本指南末尾所示的支持门户获得jetPACK。
- 浏览jetPACK.txt文件。
- 点击上传。
- 上传后，浏览器会自动刷新。

- 完成后，你将被转到仪表板页面。
- 对于更复杂的部署，如Microsoft Lync等，导入可能需要更长的时间。

全球设置

全局设置部分允许你改变各种元素，包括SSL加密库。

主机缓存定时器

Host Cache Timer是一个设置，当域名被用来代替IP地址时，它可以在一定时期内存储Real服务器的IP地址。缓存在真实服务器故障时被刷新。将此值设置为零将防止缓存被刷新。这个设置没有最大值。

沥水

对于与虚拟服务相联系的每个真实服务器，Drain功能是可配置的。默认情况下，Drain清除持久性设置是启用的，允许被置于Drain模式下的服务器优雅地结束会话，以便它们可以被下线维护。

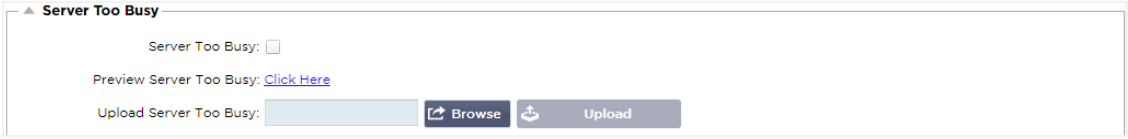
SSL

这个全局设置允许根据需要改变SSL库。ADC使用的默认SSL加密库是来自OpenSSL。如果你想使用一个不同的加密库，可以在这里改变。

议定书

协议部分是用来设置HTTP协议的许多高级设置。

服务器太忙



假设你已经限制了对你的真实服务器的最大连接数；你可以选择在达到这个限制后呈现一个友好的网页。

- 用你的信息创建一个简单的网页。你可以包括与其他网络服务器和网站上的对象的外部链接。另外，如果你想在你的网页上有图像，那么使用内联base64编码的图像
- 浏览你新创建的网页HTM（L）文件
- 点击上传
- 如果你想预览该页面，你可以通过点击这里的链接来实现。

转寄对象

转发是识别通过第7层负载均衡器和代理服务器连接到网络服务器的客户源IP地址的事实上的标准。

转发的输出

选项	描述
关闭	ADC不改变转发的头。
添加地址和端口	这个选择将把连接到ADC的设备或客户端的IP地址和端口附加到转发的头中。
添加地址	这个选择将把连接到ADC的设备或客户端的IP地址附加到转发的头中。
替换地址和端口	这个选择将用连接到ADC的设备或客户端的IP地址和端口替换转发请求头的值。
替换地址	这个选择将用连接到ADC的设备或客户端的IP地址替换转发请求头的值。

转发的标头

这个字段允许你指定给转发的头的名称。通常情况下，这是 "X-Forwarded-For"，但在某些环境下可能会被改变。

IIS的高级日志 - 自定义日志

你可以通过安装IIS高级日志64位应用程序获得X-Forwarded-For信息。下载后，用下面的设置创建一个名为X-Forwarded-For的自定义日志域。

从类别列表中的源类型列表中选择默认，在源名称框中选择请求头，并输入X-Forwarded-For。

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

Apache HTTPd.conf的变化

你要对默认格式做几个修改，以记录X-Forwarded-For客户的IP地址，如果X-Forwarded-For头不存在，则记录实际客户的IP地址。

这些变化见下文。

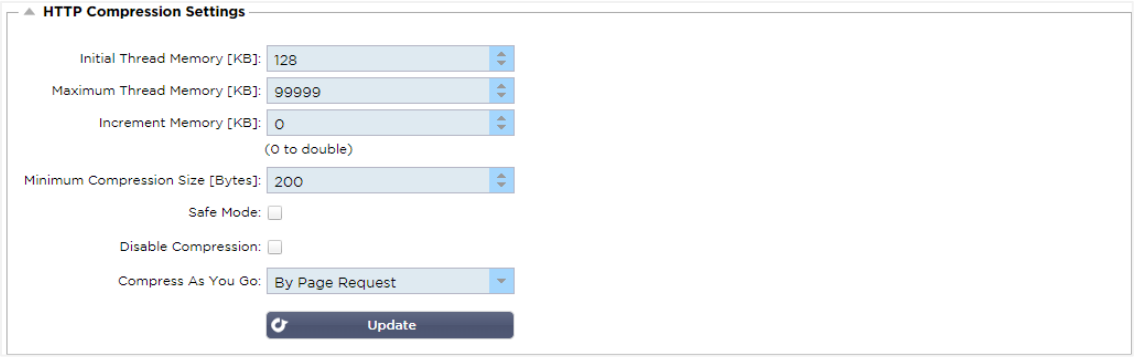
类型	价值
日志格式。	"%h %l %u %t %>s %b %{Referator}i\" "%{Referator}i\""%{User-Agent}i"" 结合起来
日志格式。	"%{X-Forwarded-For}i %l %u %t\"%r\" %>s %b\"%{Refer}i\""%{User-Agent}i"" 代理 SetEnvIf X- Forwarded-For "^.*\.*.*\.*" 转发。
习惯日志。	"logs/access_log" 结合env=!forwarded
习惯日志。	"logs/access_log" proxy env=forwarded

这种格式利用了Apache对基于环境变量的条件性日志的内置支持。

- 第1行是默认的标准组合日志格式化字符串。
- 第2行用从X-Forwarded-For头中提取的值替换%h（远程主机）字段，并将此日志文件模式的名称设置为 "代理"。
- 第3行是对环境变量 "forwarded"的设置，它包含一个匹配IP地址的松散的正则表达式，在这种情况下是可以的，因为我们更关心X-Forwarded-For报头中是否存在一个IP地址。
- 另外，第3行可以理解为。"如果有一个X-Forwarded-For值，请使用它。"
- 第4行和第5行告诉Apache要使用哪种日志模式。如果存在一个X-Forwarded-For值，就使用 "代理"模式，否则就使用请求的 "组合"模式。为了便于阅读，第4行和第5行没有利用Apache的旋转日志（piped）日志功能，但我们假设几乎每个人都会使用它。

这些变化将导致为每个请求记录一个IP地址。

HTTP压缩设置



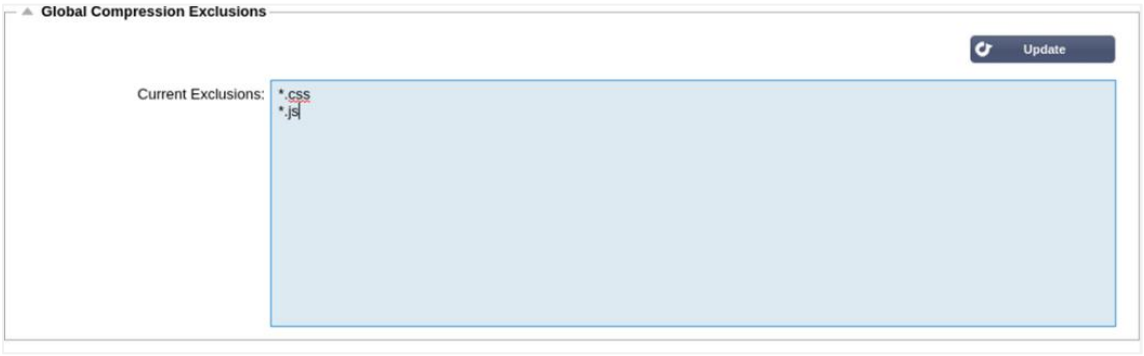
压缩是一个加速功能，在IP服务页面上为每个服务启用。

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

选项	描述
初始线程内存[KB]	这个值是ADC收到的每个请求最初可能分配的内存量。为了获得最有效的性能，这个值应该被设置为刚好超过网络服务器可能发送的最大的未压缩HTML文件的值。
最大线程内存[KB]	这个值是ADC在一次请求中所分配的最大内存量。为了获得最大的性能，ADC通常在内存中存储和压缩所有内容。如果处理的内容文件特别大，超过这个数量，ADC将写入磁盘并在那里压缩数据。
递增内存[KB]	该值设置当需要更多的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，当数据超过当前的分配（例如，128Kb，然后是256Kb，然后是512Kb，等等）时，ADC将加倍分配，直到每线程最大内存使用量设定的限制。这在大多数页面大小一致但偶尔有较大文件的情况下是有效的。例如，大多数页面是128Kb或更小，但偶尔的响应是1Mb大小）。在有大的可变大小的文件的情况下，设置一个重要大小的线性增量是更有效的（例如，响应的大小是2Mb到10Mb，初始设置为1Mb，增量为1Mb会更有效）。
最小压缩量[字节]	这个值是以字节为单位的大小，在这个大小下，ADC不会尝试进行压缩。这很有用，因为任何低于200字节的文件都不会被很好地压缩，甚至可能由于压缩头的开销而增大尺寸。
安全模式	勾选这个选项可以防止ADC对JavaScript的样式表进行压缩。这样做的原因是，即使ADC知道哪些浏览器可以处理压缩的内容，其他一些代理服务器，即使它们声称符合HTTP/1.1标准，也无法正确传输压缩的样式表和JavaScript。如果通过代理服务器的样式表或JavaScript出现了问题，那么使用这个选项来禁用这些类型的压缩。然而，这将减少内容的整体压缩量。
禁用	勾选此选项以停止ADC压缩任何响应。

压缩	
边走边压缩	ON - 在这个页面上使用边走边压缩。这将把从服务器收到的每个数据块压缩成一个离散的小块，并可完全解压缩。 OFF - 不要在这个页面上使用边走边压缩。 By Page Request - 根据页面请求使用 "边走边压缩"。

全局压缩排除法



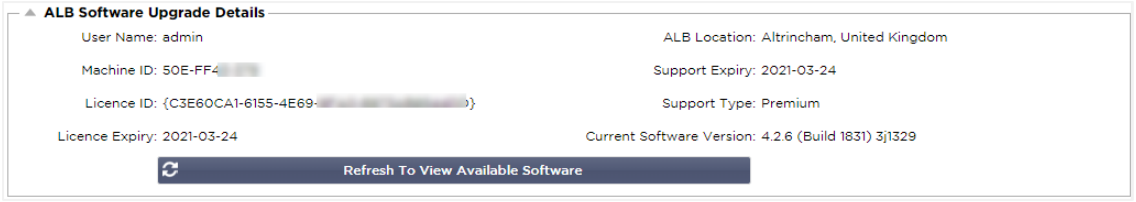
任何在排除列表中添加了扩展名的页面将不会被压缩。

- 键入单个文件名。
- 点击更新。
- 如果你想添加一个文件类型，只需输入 "*.css"，所有层叠样式表就会被排除。
- 每个文件或文件类型应添加在一个新行中。

软件

在软件部分，你可以更新ADC的配置和固件。

软件升级细节



如果你有一个正常的互联网连接，本节中的信息将被填充。如果你的浏览器没有链接到互联网，这部分将是空白。一旦连接，你将收到下面的横幅信息。

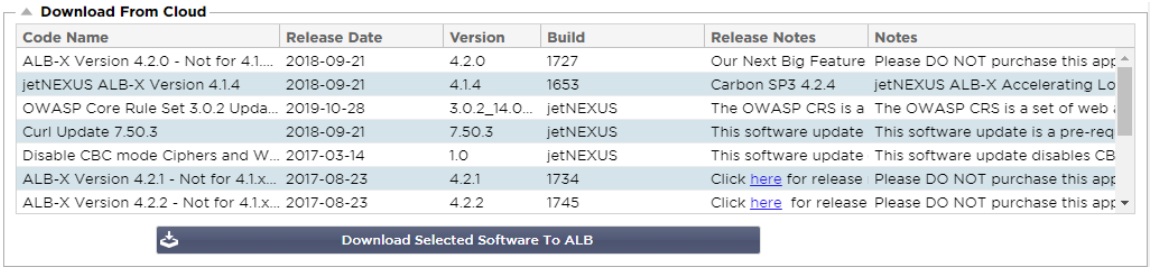
下面显示的 "从云端下载
"部分将被填充信息，显示你在支持计划下可获得的更新。你应该注意支持类型和支持到期日期。

注意：我们使用您的浏览器的互联网连接来查看Edgenexus云的可用内容。只有在ADC有互联网连接的情况下，您才能下载软件更新。

要检查这一点。

- 高级--故障排除--Ping
- IP地址 - appstore.edgenexus.io
- 点击平移
- 如果结果显示 "ping: unknown host appstore.edgenexus.io."
- ADC将不能从云端下载任何东西

从云端下载



如果你的浏览器连接到互联网，你会看到云中可用软件的详细信息。

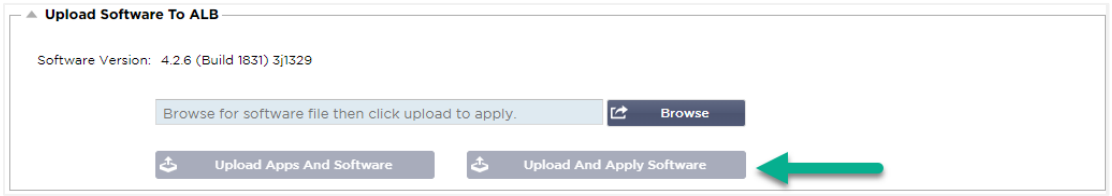
- 突出显示你感兴趣的那一行，并点击 "下载所选软件到ALB。"按钮
- 点击后，所选的软件将下载到你的ALB上，可以在下面的 "应用ALB上存储的软件 "部分进行应用。

注意：如果ADC没有直接的互联网接入，你会收到一个类似下面的错误。

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

上传软件到ALB

应用上传

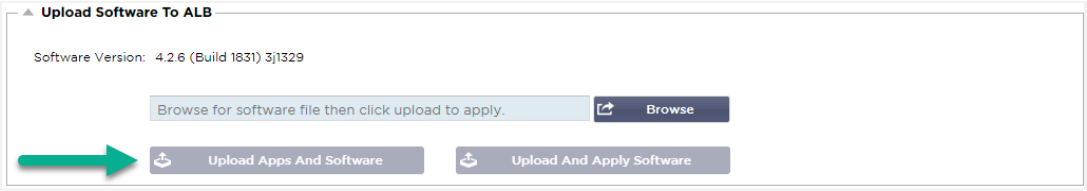


如果你有一个以<apptype>.alb结尾的App文件，你可以使用这个方法来上传它。

- 有五种类型的应用程序
  - <appname>flightpath.alb
  - <appname>.monitor.alb
  - <appname>.jetpack.alb
  - <appname>.addons.alb

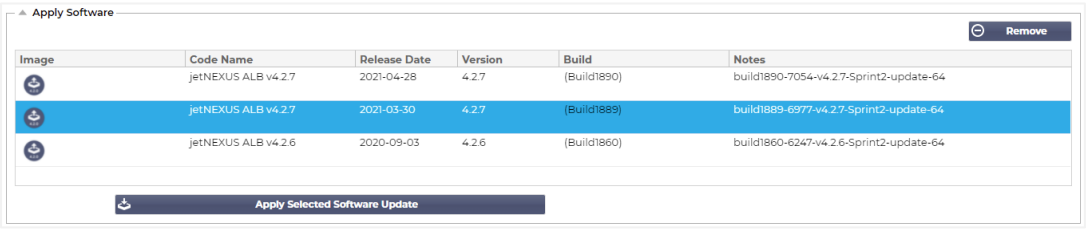
    - <appname>.featurepack.alb
- 一旦上传，每个应用程序将在图书馆>应用程序部分找到。
- 然后，你必须单独部署该部分的每个应用程序。

软件



- 如果你希望上传软件而不应用它，那么请使用突出显示的按钮。
- 软件文件是<softwarename>.software.alb。
- 然后它将显示在 "存储在ALB上的软件 "部分，在那里你可以在你方便的时候应用它。

应用存储在ALB上的软件



这一部分将显示存储在ALB上的所有软件文件，可供部署。该列表将包括更新的Web应用防火墙（WAF）签名。

- 突出显示你有兴趣使用的软件行。
- 点击 "从所选软件中应用"。
- 如果这是一个ALB软件更新，请注意它将上传，然后重新启动ALB来应用。
- 如果你应用的更新是OWASP签名更新，它将自动应用而不需要重新启动。

故障排除

总有一些问题需要排除故障，以找到根本原因和解决方案。本节允许你这样做。

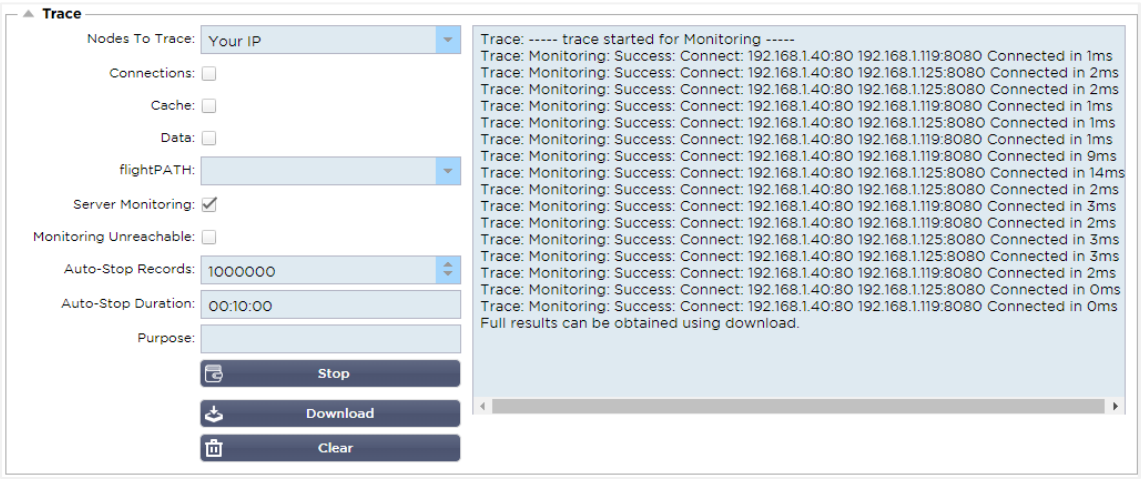
支持文件

如果你遇到ADC的问题，需要开一张支持票，技术支持部门往往会要求从ADC设备中获得几个不同的文件。这些文件现在已经汇总成一个单一的.dat文件，可以通过本节下载。

- 从下拉菜单中选择一个时间范围。你可以选择3天、7天、14天和全天。

- 点击 "下载支持文件"
- 将会下载一个格式为Support-jetNEXUS-yymmddhh-NAME.dat的文件。
- 在支持门户网站上提出支持票，详情见本文件末尾。
- 请确保你彻底描述问题，并将.dat文件附在票据上。

追踪



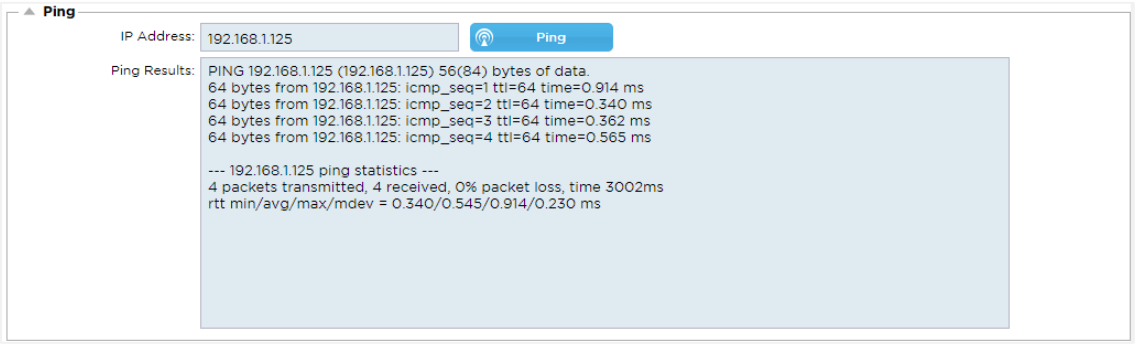
追踪部分将允许你检查信息，以便对问题进行调试。所提供的信息取决于你从下拉菜单和复选框中选择的选项。

选项	描述
要追踪的节点	**你的IP**：这将过滤输出，使用你访问GUI的IP地址（注意不要为监控选择这个选项，因为监控将使用ADC接口地址）。 **所有IP**：将不应用过滤器。应该注意的是，在一个繁忙的盒子上，这将对性能产生不利的影响。
连接	这个复选框被勾选后，将显示有关客户端和服务器端连接的信息。
缓存	勾选这个复选框将显示关于缓存对象的信息。
数据	当这个复选框被选中时，它将包括由ADC处理的输入和输出的原始数据字节。
飞行路线	flightPATH菜单允许你选择一个特定的flightPATH规则来监控或所有flightPATH规则。
服务器监控	这个复选框被选中后，将显示ADC上活跃的服务器健康监测器及其各自的结果。
监控无法到达	勾选这个选项与上面一样，只是它只显示失败的监视器，所以就像一个过滤器，只针对这些信息。
自动停止	默认值是1,000,000条记录，此后跟踪功能将自动停止。这是一项安全防范措施，以防止Trace意外地被打开而影响ADC的性能。

记录	
自动停止时间	默认时间被设置为10分钟，之后跟踪设施将自动停止。这是一项安全防范措施，以防止Trace意外地被打开而影响ADC的性能。
开始	点击手动启动跟踪设施。
停止	在达到自动记录或时间之前，点击手动停止追踪设施。
下载	虽然你可以在右侧看到实时查看器，但信息的显示速度可能太快。你可以下载Trace.log来查看当天各种跟踪过程中收集的所有信息。这基本上是一个经过过滤的跟踪信息列表。如果你想查看前几天的跟踪信息，那么你可以下载当天的syslog，但必须手动过滤。
清楚	清除跟踪记录

平

你可以使用Ping工具检查与服务器和基础设施中其他网络对象的网络连接情况。



输入你想测试的主机的IP地址，例如，使用点状十进制符号的默认网关或IPv6地址。一旦你按下 "Ping "按钮，你可能需要等待几秒钟才能得到结果反馈。

如果你已经配置了一个DNS服务器，那么你可以输入完全合格的域名。你可以在**DNS服务器1和DNS服务器2**部分配置一个DNS服务器。一旦你按下 "Ping "按钮，你可能需要等待几秒钟才能得到结果反馈。

捕获

要捕获网络流量，请遵循以下简单的指示。

- 完成表格中的选项
- 单击 "生成"。

- 一旦捕获运行，你的浏览器将弹出并询问你希望将文件保存在哪里。它的格式是"jetNEXUS.cap.gz"。
- 在支持门户网站上提出支持票，详情见本文件末尾。
- 请确保你彻底描述问题，并将文件附在票据上。
- 你也可以用Wireshark查看内容

选项	描述
适配器	从下拉菜单中选择你的适配器，通常是eth0或eth1。你也可以用 "any "捕捉所有的接口
包裹	这个值是捕获数据包的最大数量。通常情况下，99999
时间	选择捕获的最长时间。对于高流量的网站，典型的时间是15秒。在捕获期间，GUI将无法访问。
地址	该值将对输入框中的任何IP地址进行过滤。留空表示不过滤。

为了保持性能，我们将下载文件限制在10MB。如果你发现这不足以捕获所有需要的数据，我们可以增加这个数字。

注意：这将对实时网站的性能产生影响。要增加可用的捕获尺寸，请应用全局设置jetPACK来增加捕获尺寸。

什么是JetPACK

jetPACKs是一种为特定应用即时配置ADC的独特方法。这些易于使用的模板预先配置并完全调整了所有特定应用的设置，你需要从你的ADC享受优化的服务交付。一些jetPACKs使用flightPATH来操作流量，你必须有flightPATH许可证才能使用这个元素。要了解你是否有flightPATH的许可证，请参考许可证页面。

下载JetPACK

- 下面的每个jetPACK都是以包含在jetPACK标题中的唯一虚拟IP地址创建的。例如，下面第一个jetPACK的虚拟IP地址是1.1.1.1。
- 您可以按原样上传jetPACK，并在GUI中修改IP地址，或者用文本编辑器（如Notepad++）编辑jetPACK，用虚拟IP地址搜索并替换1.1.1.1。
- 此外，每个jetPACK都有2个IP地址为127.1.1.1和127.2.2.2的真实服务器。同样，你可以在上传后或事先用记事本++改变这些。
- 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	它的作用是什么？	包括哪些内容？
交易所2010	jetPACK-1.1.1.1-Exchange-2010	这个jetPACK将添加基本设置以实现Microsoft Exchange 2010的负载平衡。包括一个flightPATH规则，将HTTP服务的流量重定向到HTTPS，但这是一个选项。如果你没有flightPATH的许可证，这个jetPACK仍然可以工作。	全局设置。服务超时2小时 监测器。用于Outlook网络应用的第7层监视器，以及用于客户端访问服务的第4层带外监视器。 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-Exchan	与上述相同，但它将在反向代理连接中添加一个端口25的SMTP服务。SMTP服务器将看到ALB-X接口地址作为源IP。	全局设置。服务超时2小时 监测器。Outlook网络应用的第7层监视器。用于客户端访问服务的第4层带外监视器 虚拟服务IP：1.1.1.1

	ge-2010-SMTP-RP		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-2010-SMTP-DSR	和上面一样，除了这个jetPACK将配置SMTP服务使用直接服务器返回连接。如果您的SMTP服务器需要看到客户的实际IP地址，就需要这个jetPACK。	全局设置。服务超时2小时 监测器。Outlook网络应用的第7层监视器。用于客户端访问服务的第4层带外监视器 虚拟服务IP：1.1.1.1 虚拟服务端口。80, 443, 135, 59534, 59535, 25（服务器直接返回）。 真实服务器。127.1.1.1 127.2.2.2 flightPATH: 增加了从HTTP到HTTPs的重定向
2013年交流会	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	这种设置为HTTP和HTTPS流量增加了1个VIP和两个服务，需要的CPU最少。 可以向VIP添加多个健康检查，以检查每个单独的服务是否正常。	全局设置。 监测器。用于OWA、EWS、OA、EAS、ECP、OAB和ADS的第7层监视器。 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	这种设置为每个服务使用一个独特的IP地址，因此比上面使用更多资源。你必须将每个服务配置为一个单独的DNS条目，例如owa.jetnexus.com、ews.jetnexus.com等。每个服务的监视器将被添加并应用于相关服务	全局设置。 监测器。对OWA、EWS、OA、EAS、ECP、OAB、ADS、MAPI和PowerShell的第7层监控。 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

- Resource		虚拟服务端口。80, 443 真实服务器。127.1.1.1 127.2.2.2 flightPATH: 增加了从HTTP到HTTPs的重定向
jetPACK-2.2.2.3-Exchange2013-Hlgh-Resource	这个jetPACK将添加一个唯一的IP地址和几个不同端口的虚拟服务，然后flightPATH将根据目标路径进行上下文切换，以获得正确的虚拟服务。这个jetPACK需要最多的CPU来进行上下文切换。	全局设置。 监测器。对OWA、EWS、OA、EAS、ECP、OAB、ADS、MAPI和PowerShell的第7层监控。 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

微软Lync 2010/2013

反向代理	前端	内部边缘	外部边缘
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

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

微软远程桌面

jetPACK-5.5.5.1-Remote-Desktop

DICOM - 医学中的数字成像和通信

jetPACK-6.6.6.1-DICOM

甲骨文e-Business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

全球设置

- GUI安全端口443 - 这个jetPACK将把你的GUI安全端口从27376改为443。HTTPs://x.x.x.x

- GUI超时1天 - GUI将要求你每20分钟输入一次密码。这个设置将把这个请求增加到1天
- ARP刷新10 -
  在HA设备之间的故障切换期间，此设置将增加**无偿ARP的**数量，以便在过渡期间协助交换机。
- 捕获大小16MB - 默认捕获大小为2MB。这个值将增加到最大16MB的大小

密码选项

- 强密码 - 这将增加从密码选项列表中选择 "强密码 "的能力。
  - 密码 = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- 反野兽 - 这将增加从密码选项列表中选择 "反野兽 "的能力。
  - 密码 = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:！MD5:！aNULL:！EDH
- 无SSLv3 - 这将增加从密码选项列表中选择 "无SSLv3 "的能力。
  - 密码 = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:！MD5:！aNULL:！EDH:！RC4
- No SSLv3 no TLSv1 No RC4 - 这将增加从密码选项列表中选择 "No-TLSv1 No-SSLv3 No-RC4 "的能力。
  - 密码 = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:！MD5:！aNULL:！EDH:！RC4
- NO_TLSv1.1 -这将增加从密码选项列表中选择 "NO_TLSv1.1 "的能力。
  - 密码= 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

飞行路线

- X-Content-Type-Options - 如果这个头不存在，则添加这个头，并将其设置为 "nosniff" - 防止浏览器自动 "MIME-Sniffing"。
- X-Frame-Options - 如果这个标题不存在，请添加它，并将其设置为 "SAMEORIGIN" - 你的网站上的页面可以包含在框架中，但只能在同一网站的其他页面上。
- X-XSS-Protection - 如果不存在，请添加此标题并将其设置为 "1; mode=block" - 启用浏览器跨站脚本保护。
- Strict-Transport-Security - 如果不存在，则添加头，并将其设置为 "max-age=31536000 ; includeSubdomains" - 确保客户端应遵守所有链接都是HTTPs://的最大年龄。

应用JetPACK

您可以按任何顺序应用任何jetPACK，但要注意不要使用具有相同虚拟IP地址的jetPACK。这种行为将导致配置中出现重复的IP地址。如果你错误地这样做，你可以在GUI中进行修改。

- 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
- 一旦浏览器屏幕变成白色，请点击刷新并等待仪表板页面出现

创建JetPACK

jetPACK的好处之一是你可以创建你自己的。你可能已经为一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，从你现有的ALB-X中复制当前的配置。
  - 高级
  - 更新软件
  - 下载当前配置
- 用Notepad++编辑这个文件
- 打开一个新的txt文件，将其称为 "yourname-jetPACK1.txt"
- 从配置文件中复制所有相关部分到 "yourname-jetPACK1.txt"。
- 完成后保存

重要提示：每个jetPACK都被分成不同的部分，但所有jetPACK都必须在页面顶部有#！jetpack。

建议编辑/复制的部分列在下面。

0节。

```
#！jetpack
```

这一行需要在jetPACK的顶部，否则你当前的配置将被覆盖。

第1节。

```
[jetnexusdaemon]
```

本节包含全局设置，一旦改变，将适用于所有服务。其中一些设置可以从网络控制台中改变，但其他设置只在这里可用。

例子。

```
ConnectionTimeout=600000
```

这个例子是以毫秒为单位的TCP超时值。这个设置意味着一个TCP连接在不活动10分钟后将被关闭

```
内容服务器CustomTimer=20000
```

这个例子是内容服务器健康检查之间的延迟，以毫秒为单位，用于自定义监视器，如DICOM

jnCookieHeader="MS-WSMAN"

这个例子将把用于持久性负载平衡的cookie头的名称从默认的 "jnAccel "改为 "MS-WSMAN"。Lync 2010/2013的反向代理需要这种特殊的改变。

第2节。

[jetnexusdaemon-Csm-Rules] 。

本节包含自定义的服务器监控规则，这些规则通常从web控制台这里配置。

例子。

[jetnexusdaemon-Csm-Rules-0]。

内容="服务器启动"

描述="监视器1″。

方法="CheckResponse"

名称="健康检查-服务器是否正常"

Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"

第3节。

[jetnexusdaemon-LocalInterface]。

本节包含IP服务部分的所有细节。每个接口都有编号，包括每个通道的子接口。如果你的通道应用了flightPATH规则，那么它也将包含一个路径部分。

例子。

[jetnexusdaemon-LocalInterface1]。

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-LocalInterface1.1]。

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″""

AddressResolution=0

缓存端口=0

CertificateName="default"

ClientCertificateName="无SSL"

压缩=1

连接限制=0

DSR=0

DSRProto="tcp"

已启用=1

LoadBalancePolicy="CookieBased"

最大连接数=10000

监测政策="1"。

穿透=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-Path]。

这一部分包含所有的flightPATH规则。数字必须与已经应用于接口的内容相匹配。在上面的例子中，我们看到flightPATH规则 "6 "已经被应用到通道上，包括下面这个例子。

例子。

[jetnexusdaemon-Path-6] 。

Desc="强制对某些目录使用HTTPS"

名称="Gary-强制HTTPS"

[jetnexusdaemon-Path-6-Condition-1] 。

检查="包含"

条件="路径"

匹配=

感官="确实"

值="/secure/"

[jetnexusdaemon-Path-6-Evaluate-1] 。

详细=

来源="主机"

价值=

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

行动="重定向"

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

价值=

flightPATH简介

什么是flightPATH？

flightPATH是由Edgenexus开发的一个智能规则引擎，用于操作和路由HTTP和HTTPS流量。它是高度可配置的，非常强大，但又非常容易使用。

尽管flightPATH的一些组件是IP对象，如源IP，但flightPATH只能应用于等于HTTP的**服务类型**。如果你选择任何其他服务类型，那么IP服务中的flightPATH标签将是空白的。

一个flightPATH规则有三个组成部分。

选项	描述
状况	设置多个标准来触发flightPATH规则。
评价	允许使用可在行动区使用的变量。
行动	一旦规则被触发后的行为。

flightPATH能做什么？

flightPATH可以用来修改传入和传出的HTTP（）内容和请求。

除了使用简单的字符串匹配，例如 "开始于 "和
"结束于"，还可以使用强大的与Perl兼容的正则表达式（RegEx）实现完全控制。

关于RegEx的更多信息，请看这个有用的网站https://www.regexbuddy.com/regex.html。

此外，还可以在**行动**区创建和使用自定义变量，实现许多不同的可能性。

状况

状况	描述	例子
<表格>	HTML表格是用来向服务器传递数据的	例子 "表格没有长度0"
GEO位置	这是将源IP地址与ISO 3166国家代码进行比较。	GEO位置等于GB或GEO位置等于德国
宿主	这是从URL中提取的主机	www.mywebsite.com 或 192.168.1.1
语言	这是从language的HTTP头中提取的语言。	这个条件将产生一个带有语言列表的下拉菜单
方法	这是一个下拉式的HTTP方法	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Origin地址。	客户端IP。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|为多个IP的。
路径	这是网站的路径	/mywebsite/index.asp
帖文	POST请求方法	检查正在上传到网站的数据
查询	这是一个查询的名称和值，因此它可以接受查询名称或一个值。	"Best=jetNEXUS"，其中匹配的是Best，值是edgeNEXUS。
查询字符串	在? 字符之后的整个查询字符串	
索取饼干	这是客户要求的一个cookie的名称。	MS-WSMAN=afYfn1CDqqCDqUD::
请求标题	这可以是任何HTTP头	Referrer, User-Agent, From, Date
要求版本	这是HTTP版本	http/1.0或http/1.1
回应机构	响应体中的一个用户定义的字符串	服务器升级
响应代码	响应的HTTP代码	200 OK, 304 Not Modified
回应饼干	这是由服务器发送的cookie的名称	MS-WSMAN=afYfn1CDqqCDqUD::
响应头	这可以是任何HTTP头	Referrer, User-Agent, From, Date
响应版本	服务器发送的HTTP版本	http/1.0或http/1.1
来源于IP	这要么是源头IP、代理服务器IP，要么是其他一些聚合的IP地址	客户端 IP、代理IP、防火墙IP。也可以使用多个IP和子网。你 必须摆脱点，因为这些是RegEX。例如10\.1\.2\.3是10.1.2.3

匹配	描述	例子
接受	可接受的内容类型	接受: text/plain
接受-编码	可接受的编码	Accept-Encoding: <compress | gzip | deflate | sdch | identity >。
接受语言	可接受的回应语言	Accept-Language: en-US

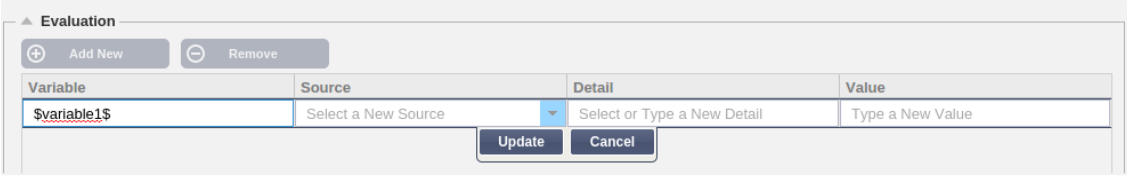
接受范围	该服务器支持哪些部分内容范围类型	接受-范围: bytes
授权书	用于HTTP认证的认证凭证	授权。Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
收费-目的	包含应用所申请方法的费用的账户信息	
内容-编码	数据上使用的编码类型。	Content-Encoding: gzip
内容-长度	响应体的长度，单位是八位数（8位字节）。	内容-长度: 348
内容-类型	请求正文的mime类型（用于POST和PUT请求）。	Content-Type: application/x-www-form-urlencoded
饼干	服务器之前用Set-Cookie发送的一个HTTP cookie（如下）。	Cookie: $Version=1; Skin=new;
日期	信息发出的日期和时间	Date = "Date" ":" HTTP-date
ETag	一个资源的特定版本的标识符，通常是一个消息摘要	ETag。"aed6bdb8e090cd1:0"
来自	提出请求的用户的电子邮件地址	来自: user@example.com
如果修改过-自	如果内容没有变化，允许返回304未修改。	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
最后修改时间	请求对象的最后修改日期，格式为RFC 2822	最后修改的。Tue, 15 Nov 1994 12:45:26 GMT
プラグマ	具体实施的标头可以在请求-响应链的任何地方产生各种影响。	Pragma: no-cache
推荐人	这是前一个网页的地址，从这个网页上可以链接到当前请求的页面。	推荐人: HTTP://www.edgenexus.io
服务器	服务器的一个名称	服务器。Apache/2.4.1 (Unix)
设置参数	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)
不尽相同	告诉下游代理如何匹配未来的请求头，以决定是否可以使用缓存的响应，而不是从源服务器请求一个新的响应。	变化。用户代理
X-Powered-By	指定支持网络应用的技术（如ASP.NET、PHP、JBoss）。	X-Powered-By:PHP/5.4.0

检查	描述	例子
存在的	这不关心条件的细节，只关心它的存在/不存在。	宿主 - 确实 - 存在
开始	该字符串以 "值 "开始	路径 - Does - Start - /secure
结束	字符串以 "值 "结束。	Path - Does - End - .jpg
包含	该字符串确实包含了价值	请求头 - 接受 - 是否 - 包含 - 图像
平等	字符串确实等于值	主持人 - 是否 - 平等 - www.jetnexus.com
有长度	该字符串确实有长度的值	主机 - 是否 - 有长度 - 16 www.jetnexus.com = TRUE www.jetnexus.co.uk = FALSE
匹配RegEx	这使你能够输入一个完全与Perl兼容的正则表达式	起始IP - 是否 - 匹配Regex - 10\.* | 11\.*

例子

- 这个例子有两个条件，而且必须满足这两个条件才能执行行动
- 首先是检查所请求的对象是否是一个图像
- 第二种是检查一个特定的主机名

评价



添加变量是一个引人注目的功能，它将允许你从请求中提取数据并在行动中利用它。例如，你可以记录一个用户的用户名，或者在有安全问题时发送一封电子邮件。

- 变量。这必须以$符号开始和结束。例如，$variable1$
- 来源。从下拉框中选择变量的来源
- 细节。相关时从列表中选择。如果Source=Request Header，细节可以是User-Agent
- 值。输入文本或正则表达式，对变量进行微调。

内置变量。

- 内置变量已经被硬编码了，所以你不需要为这些变量创建一个评估条目。
- 你可以在你的行动中使用下面列出的任何变量
- 每个变量的解释都在上面的 "条件 "表中。
    - 方法=$method$
    - 路径 = $path$
    - Querystring = $querystring$
    - Sourceip = $sourceip$
    - 响应代码（文本也包括 "200 OK"）= $resp$
    - 主机=$host$
    - 版本 = $version$
    - 客户端口 = $clientport$
    - Clientip = $clientip$
    - 地理定位=$geolocation$"

示例行动。

- 行动 = 重定向 302
    - 目标 = HTTPs://$host$/404.html
- 行动=记录
    - 目标 = 一个来自$sourceip$:$sourceport$的客户刚刚提出了一个$path$页面请求

解释一下。

- 客户端访问不存在的页面时，通常会出现一个浏览器404页面
- 在这种情况下，用户被重定向到他们使用的原始主机名，但错误的路径被替换为404.html。
- 在syslog中添加了一个条目："一个来自154.3.22.14:3454的客户刚刚对wrong.html页面进行了请求"

来源	描述	例子
饼干	这是该cookie头的名称和值	MS-WSMAN=afYfn1CDqqCDqUD::其中名称为MS-WSMAN，值为afYfn1CDqqCDqUD:。
宿主	这是从URL中提取的主机名	www.mywebsite.com 或 192.168.1.1
语言	这是从Language HTTP头中提取的语言。	这个条件将产生一个带有语言列表的下拉菜单。
方法	这是一个下拉式的HTTP方法	下拉菜单将包括GET、POST
路径	这是网站的路径	/mywebsite/index.html
帖文	POST请求方法	检查正在上传到网站的数据

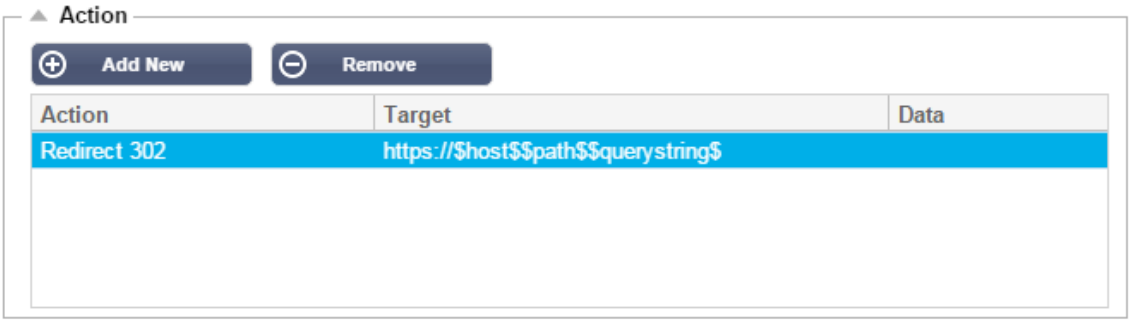
查询项目	这是一个查询的名称和值。因此，它既可以接受查询的名称，也可以接受一个值。	"Best=jetNEXUS"，其中匹配的是Best，值是edgeNEXUS。
查询字符串	这是在? 字符之后的整个字符串	HTTP://server/path/program?query_string
请求标题	这可以是客户端发送的任何标头	Referrer, User-Agent, From, Date...
响应头	这可以是服务器发送的任何标头	Referrer, User-Agent, From, Date...
版本	这是HTTP版本	HTTP/1.0或HTTP/1.1

详情	描述	例子
接受	可接受的内容类型	接受: text/plain
接受-编码	可接受的编码	Accept-Encoding: <compress | gzip | deflate | sdch | identity >。
接受语言	可接受的回应语言	Accept-Language: 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: bytes
授权书	用于HTTP认证的认证凭证	授权。Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
收费-目的	包含应用所申请方法的费用的账户信息	
内容-编码	数据上使用的编码类型。	Content-Encoding: gzip
内容-长度	响应体的长度，单位是八位数（8位字节）。	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: application/x-www-form-urlencoded
饼干	服务器之前用Set-Cookie发送的一个HTTP cookie（如下）。	Cookie: $Version=1; Skin=new;
日期	信息发出的日期和时间	Date = "Date" ":" HTTP-date
ETag	一个资源的特定版本的标识符，通常是一个消息摘要	ETag。"aed6bdb8e090cd1:0"
来自	提出请求的用户的电子邮件地址	来自: user@example.com
如果修改过-自	如果内容没有变化，允许返回304未修改。	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
最后修改时	请求对象的最后修改日期，格式为RFC 2822	最后修改的。Tue, 15 Nov 1994 12:45:26 GMT

间		
プラグマ	具体实施的头文件，可能在请求- 响应链的任何地方产生各种影响。	Pragma: no-cache
推荐人	这是前一个网页的地址，从这个网页上可以链接到当前请求的页面。	推荐人: HTTP://www.edgenexus.io
服务器	服务器的一个名称	服务器。Apache/2.4.1 (Unix)
设置参数	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)
不尽相同	告诉 下游代理如何匹配未来的请求头，以决定 是否可以使用缓存的响应，而不是 从源服务器 请求一个新的响应。	变化。用户代理
X-Powered-By	指定支持网络应用的技术（如ASP.NET、PHP、JBoss）。	X-Powered-By:PHP/5.4.0

行动

行动是指一旦条件得到满足就启用的一项或多项任务。



行动

双击行动栏，查看下拉列表。

目标

双击目标栏，查看下拉列表。列表将根据行动的不同而改变。

你也可以用一些动作手动打字。

数据

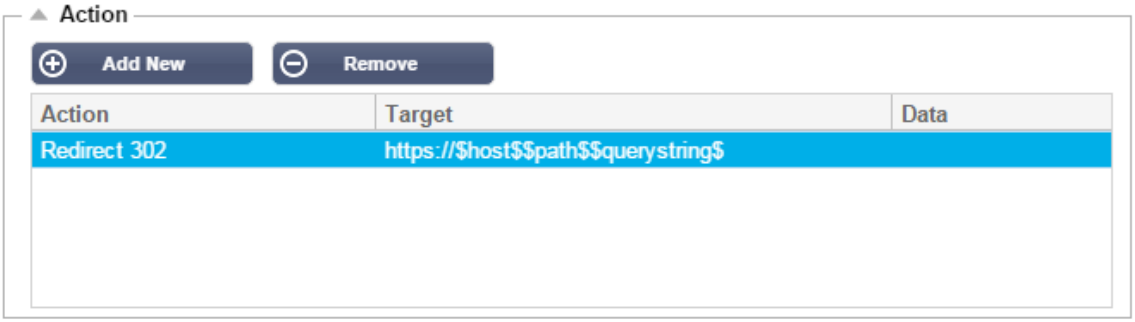
双击数据栏，手动添加你想添加或替换的数据。

所有行动的清单详见下文。

行动	描述	例子
添加请求Cookie	在目标部分添加详细的请求cookie，并在数据部分添加值	目标= 饼干 数据= MS-WSMAN=afYfn1CDqqCDqCVii
添加请求标题	在数据部分添加一个带有数值的目标类型的请求头	目标=接受 数据= image/png
添加响应Cookie	在目标部分添加详细的响应Cookie，并在数据部分添加值。	目标= 饼干 数据= MS-WSMAN=afYfn1CDqqCDqCVii
添加响应头	在目标部分添加详细的请求头，并在数据部分添加值	目标= Cache-Control 数据= max-age=8888888
身体全部更换	搜索响应主体并替换所有实例	目标= HTTP:// (搜索字符串) 数据= HTTPs:// (替换字符串)
首先更换车身	搜索响应主体，仅替换第一种情况	目标= HTTP:// (搜索字符串) 数据= HTTPs:// (替换字符串)
身体更换最后一个	搜索响应主体，仅替换最后一个实例	目标= HTTP:// (搜索字符串) 数据= HTTPs:// (替换字符串)
跌落	这将放弃连接	目标= 不适用 数据= 不适用
电子邮件	将发送一封电子邮件到电子邮件事件中配置的地址。你可以使用一个变量作为地址或信息	目标="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	目标= "flightPATH在系统日志中记录了这一点" 数据= 不适用
重定向301	这将发出一个永久的重定向	目标= HTTP://www.edgenexus.ioData= 不适用
重定向 302	这将发出一个临时重定向	目标= HTTP://www.edgenexus.ioData= 不适用
移除要求的Cookie	移除目标部分中详述的请求cookie	目标= 饼干 数据= MS-

		WSMAN=afYfn1CDqqCDqCVii
移除请求标头	移除目标部分中详述的请求标头	目标=服务器 数据=N/A
移除响应的Cookie	移除目标部分中详述的响应cookie	目标=jnAccel
移除响应标头	移除目标部分中详述的响应头	目标= Etag 数据= 不适用
替换请求饼干	用数据部分的值替换目标部分的详细请求cookie	目标= 饼干 数据= MS-WSMAN=afYfn1CDqqCDqCVii
替换请求标头	用数据值替换目标中的请求头	目标=连接 数据= keep-alive
替换响应饼干	用数据部分的值替换目标部分中详述的响应cookie	目标=jnAccel=afYfn1CDqqCDqCViiDate=MS-WSMAN=afYfn1CDqqCDqCVii
替换响应头	用数据部分的值替换目标部分的详细响应头	目标=服务器 数据= 为安全起见不公开
重写路径	这将允许你根据条件将请求重定向到新的URL。	目标=/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=192.168.101:443Data=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
加密饼干	这将对cookies进行3DES加密，然后对其进行base64编码	目标= 输入要加密的cookie名称，你可以在最后使用*作为通配符 Data= 输入加密的密码短语。

例子。



下面的动作将向浏览器发出一个临时重定向到一个安全的HTTPS虚拟服务。它将使用与请求相同的主机名、路径和查询词。

常见用途

应用防火墙和安全

- 阻止不需要的IP
- 强制用户对特定（或所有）内容使用HTTPS
- 阻止或重定向蜘蛛
- 防止和提醒跨站脚本攻击
- 防止和提醒SQL注入
- 隐藏内部目录结构
- 重写饼干
- 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
- 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
- 修复破损的URL
- 日志和电子邮件提醒404响应代码
- 防止目录访问/浏览
- 向蜘蛛发送不同的内容

预先建立的规则

HTML扩展

将所有的.htm请求改为.html

状况。

- 条件=路径
- 感知 = 感受
- 检查 = 匹配RegEx
- 值 = \.htm$

评价。

- 空白

行动。

- 行动=重写路径
- 目标=$path$l

索引.html

在对文件夹的请求中强制使用index.html。

条件：这个条件是一个一般条件，将与大多数对象相匹配。

- 条件 = 主机
- 感知 = 感受
- 检查=存在

评价。

- 空白

行动。

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

关闭文件夹

拒绝对文件夹的请求。

条件：这个条件是一个一般条件，将与大多数对象相匹配。

- 条件=这需要适当的思考
- 感官=
- 检查=

评价。

- 空白

行动。

- 行动=
- 目标=

隐藏CGI-BBIN。

在对CGI脚本的请求中隐藏cgi-bin目录。

条件：这个条件是一个一般条件，将与大多数对象相匹配。

- 条件 = 主机
- 感知 = 感受
- 检查 = 匹配RegEX
- 值 = \.cgi$

评价。

- 空白

行动。

- 行动=重写路径
- 目标 = /cgi-bin$path$

日志蜘蛛

记录流行搜索引擎的蜘蛛请求。

条件：这个条件是一个一般条件，将与大多数对象相匹配。

- 条件=请求头
- 匹配 = 用户代理
- 感知 = 感受
- 检查 = 匹配RegEX
- 值=Googlebot|Slurp|bingbot|ia_archiver

评价。

- 变量=$crawler$
- 来源=请求头
- 细节=用户代理

行动。

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

强制HTTPS

对某些目录强制使用HTTPS。在这种情况下，如果客户正在访问任何包含/secure/目录的东西，那么他们将被重定向到所请求的HTTPs版本的URL。

状况。

- 条件=路径
- 感知 = 感受
- 检查=包含
- 值=/secure/

评价。

- 空白

行动。

- 行动 = 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。

状况。

- 条件=路径
- 感知 = 感受
- 检查=结束
- 值=.flv

评价。

- 空白

行动。

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

将HTTP换成HTTPS

将任何硬编码的HTTP://改为HTTPS://

状况。

- 条件=响应代码

- 感知 = 感受
- 检查 = 平等
- 值=200 OK

评价。

- 空白

行动。

- 行动 = 替换所有车身
- 目标 = HTTP://
- 数据 = HTTPs://

空白的信用卡

检查回复中是否有信用卡，如果发现有信用卡，则将其清空。

状况。

- 条件=响应代码
- 感知 = 感受
- 检查 = 平等
- 值=200 OK

评价。

- 空白

行动。

- 行动 = 替换所有车身
- 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-xxxx

内容过期

在页面上添加一个合理的内容过期日期，以减少请求和304的数量。

条件：这是一个通用的条件，作为一个总括。建议将这个条件集中在你的

- 条件=响应代码
- 感知 = 感受
- 检查 = 平等
- 值=200 OK

评价。

- 空白

行动。

- 行动=添加响应头
- 目标 = 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改为其他类型。

条件：这是一个通用的条件，作为一个总括。建议将这个条件集中在你的

- 条件=响应代码
- 感知 = 感受
- 检查 = 平等
- 值=200 OK

评价。

- 空白

行动。

- 行动 = 替换响应头
- 目标=服务器
- 数据 = 秘密

永不发送错误

客户从未从你的网站上得到任何错误。

状况

- 条件=响应代码
- 感知 = 感受
- 检查=包含
- 值=404

评价

- 空白

行动

- 行动 = 重定向 302
- 目标 = HTTP//$host$/

关于语言的重定向

找到语言代码并重定向到相关国家的域名。

状况

- 条件=语言
- 感知 = 感受
- 检查=包含
- 价值=德语（标准

评价

- 变量=$host_template$
- 来源 = 主机
- 值=.*/。

行动

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

谷歌分析

插入谷歌分析所需的代码 - 请将MYGOOGLECODE的值改为你的谷歌UA ID。

状况

- 条件=响应代码
- 感知 = 感受
- 检查 = 平等
- 值=200 OK

评价

- 空白

行动

- 行动 = 替换最后的正文
- 目标=</body>
- Data = <
  scripttype='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); }(); </p> <p)(); </script> </body>

IPv6网关

调整IPv6服务上的IIS IPv4服务器的主机头。 IIS

IPv4服务器不喜欢在主机客户端请求中看到IPV6地址，所以这条规则用一个通用名称代替。

状况

- 空白

评价

- 空白

行动

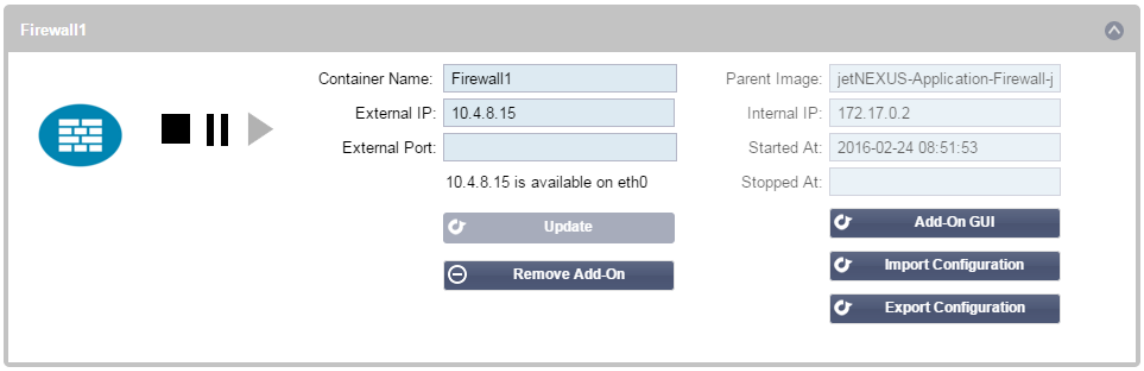
- 行动 = 替换请求头
- 目标=主机
- 数据=ipv4.host.header

网络应用防火墙(edgeWAF)

网络应用防火墙（WAF）可根据要求提供，并按年度收费许可。WAF的安装是通过ADC中内置的应用程序部分完成的。

运行WAF

在Docker容器中运行，WAF需要在启动前设置一些网络参数。

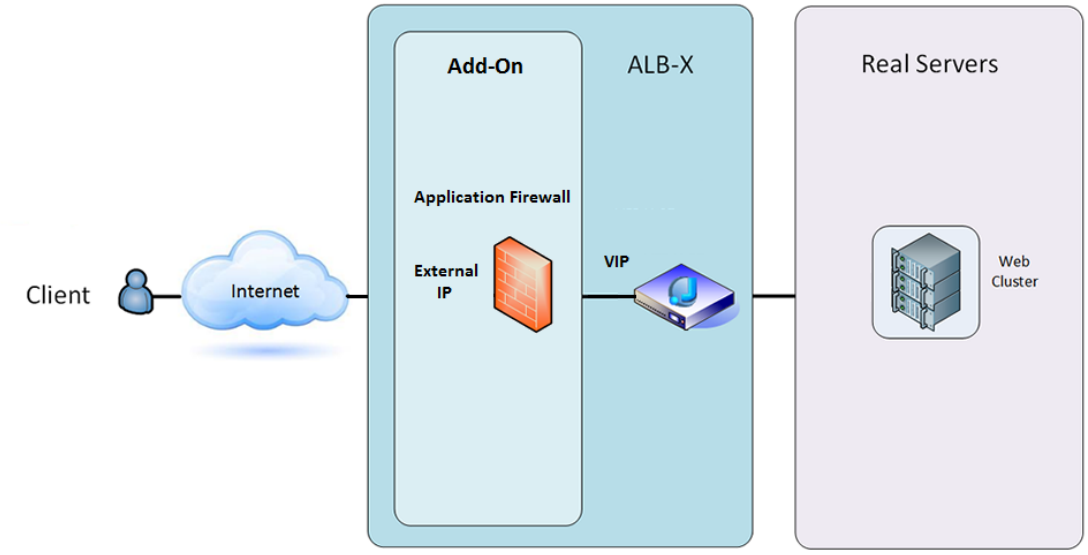


选项	描述
停止	在启动Add-On实例之前，它将是灰色的。按下这个按钮可以停止Docker实例。
暂停	这个按钮将暂停该插件。
播放	它将以当前的设置启动该插件。
容器名称	给你的容器起个名字，以便从其他容器中识别出来。这必须是唯一的。如果你愿意的话，你可以用这个名字作为Real服务器的名字，它将自动解析为实例的内部IP地址。
外部IP	在这里你可以设置一个外部IP来访问你的附加组件。这可能是为了访问附加组件的GUI以及通过附加组件运行的服务。在防火墙插件的情况下，这是你的HTTP服务的IP地址。然后，防火墙可以被配置为访问一个服务器或一个包含多个服务器的负载平衡的ALB-X VIP。
外部端口	如果你留空，那么所有的端口将被转发到你的防火墙。要限制这一点，只需在逗号分隔的端口列表中添加。例如80、443、88。注意防火墙的GUI地址将是**HTTP//[外部IP]88/waf。**因此，如果你限制端口列表，要么把外部端口设置留空，要么加入端口88来访问GUI。
更新	你只能在一个插件停止后更新它的设置。一旦你的实例停止，你可以改变容器名称、外部IP和外部端口设置。
移除附加组件	将完全从附加组件页面中删除附加组件。你将需要到图书馆-应用程序页面再次部署该插件。
父母形象	表示该插件所使用的Docker镜像。防火墙可能有几个版本，或者完全是另一种类型的插件，所以这将有助于区分它们。本节仅用于提供信息，因此是灰色的。

内部IP	Docker会自动创建内部IP地址，因此，不能编辑。如果你停止Docker实例并重新启动，一个新的内部IP地址将被发布。正是由于这个原因，你应该为你的服务使用一个外部IP地址，或者你使用容器名称作为你的服务的真实服务器地址。
开始于	这将说明该插件启动的日期和时间。例如 2016-02-16 155721
停在了	这将说明该插件被停止的日期和时间。例如 2016-02-24 095839

建筑实例

使用外部IP地址的WAF

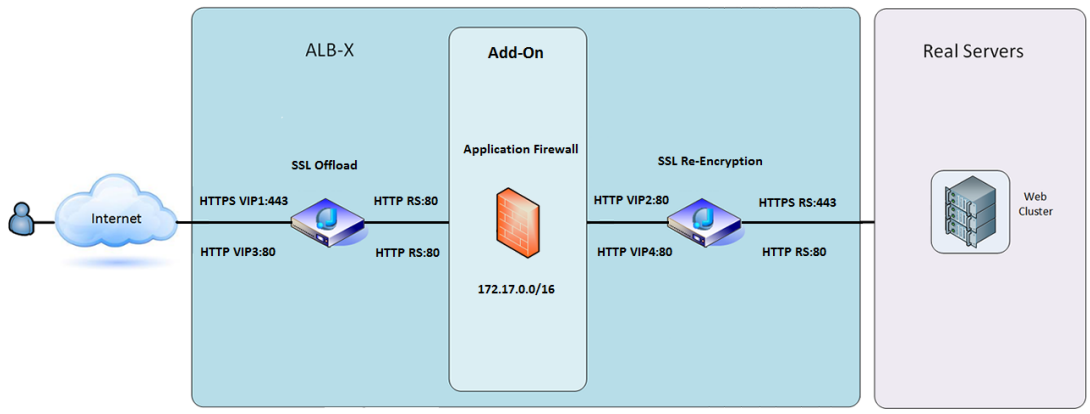


在这种结构中，只有HTTP可以用于你的服务，因为防火墙不能检查HTTPS流量。

需要对防火墙进行配置，以便将流量发送到ALB-X VIP上。

反过来，ALB-X VIP将被配置为负载平衡流量到你的网络集群。

使用内部IP地址的WAF



在这个架构中，你可以指定HTTP和HTTPS。

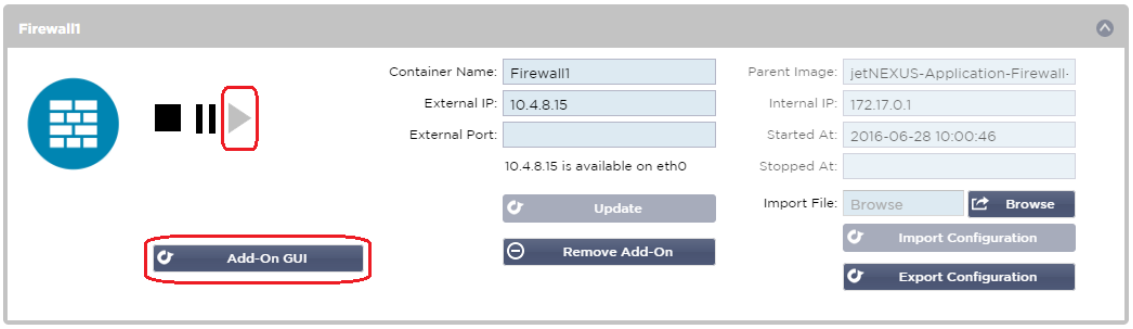
HTTPS可以是端到端的，从客户端到ALB-X的连接是加密的，从ALB-X到真实服务器的连接也是加密的。

从ALB-X到防火墙的内部IP地址的流量需要解密，以便能够被检查。

一旦流量通过了防火墙，它就会被转发到另一个VIP，然后可以对流量进行重新加密，并对安全服务器进行负载平衡，或者干脆通过HTTP对不安全的服务器进行负载平衡。

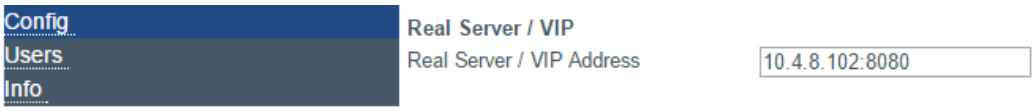
访问您的WAF插件

- 填写你的防火墙的详细信息
- 你可以将你的端口限制在你需要的范围内，或者留空以允许所有端口。
- 点击播放按钮
- 将会出现一个插件GUI按钮

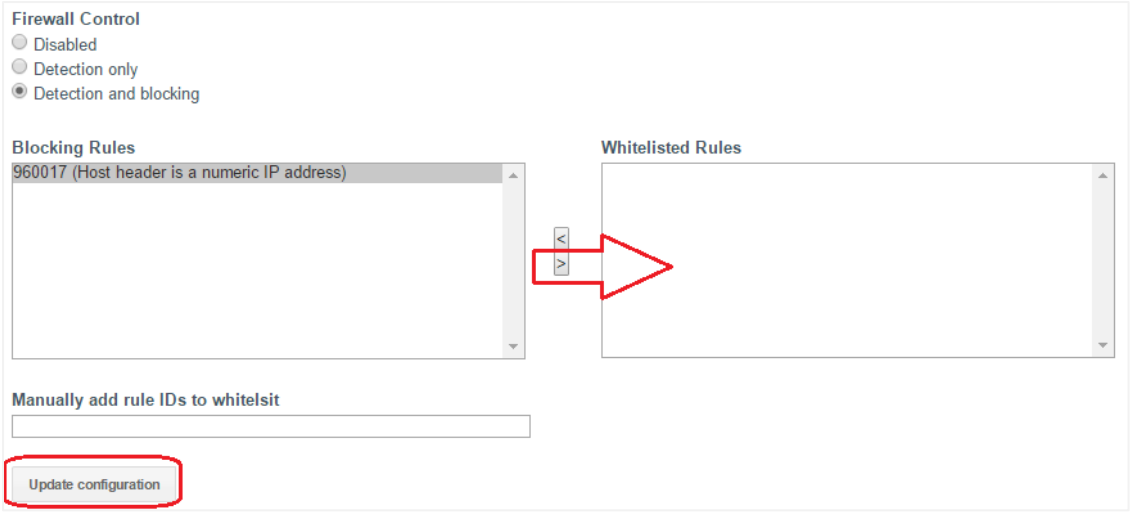


- 点击这个按钮，它将打开一个HTTP://[外部IP]:88/waf的浏览器。
- 在这个例子中，它将是HTTP:/10.4.8.15:88/waf
- 你将会看到一个登录对话框。
- 输入你的ADC的凭证。
- 在完成成功登录后，您将看到WAF的主页。

- 主页显示事件的图形概览，即应用防火墙执行的过滤行动。
- 当你第一次打开网页时，图表很可能是空白的，因为不会有通过防火墙的访问尝试。
- 你可以配置你想在防火墙过滤后将流量发送到的IP地址或网站域名。
- 这可以在管理 > 配置部分进行更改



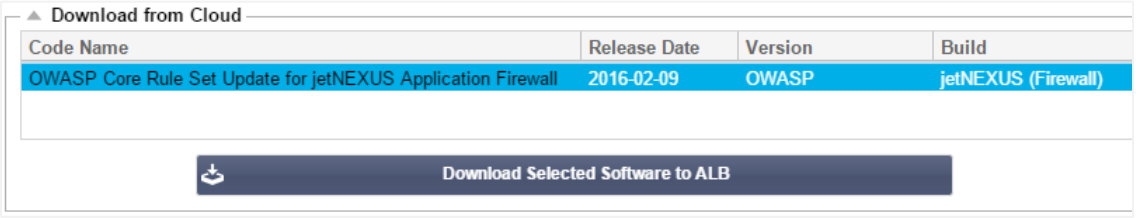
- 防火墙将检查流量，然后将其发送到这里的Real Sever IP或VIP地址。你也可以在输入IP地址的同时输入一个端口。如果你单独输入一个IP地址，那么该端口将被假定为80端口。点击 "更新配置 "按钮，保存这个新设置。
- 当防火墙阻止一个应用程序资源时，阻止流量的规则将出现在 "白名单 "页面的 "阻止规则 "列表中。
- 为了防止防火墙阻断有效的应用资源，请将阻断规则移到白名单规则部分。



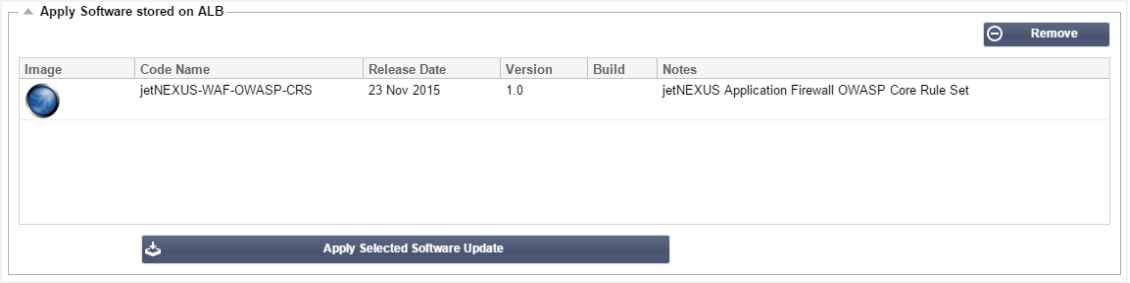
- 当你把所有的规则从封堵部分转移到白名单部分时，按更新配置。

更新规则

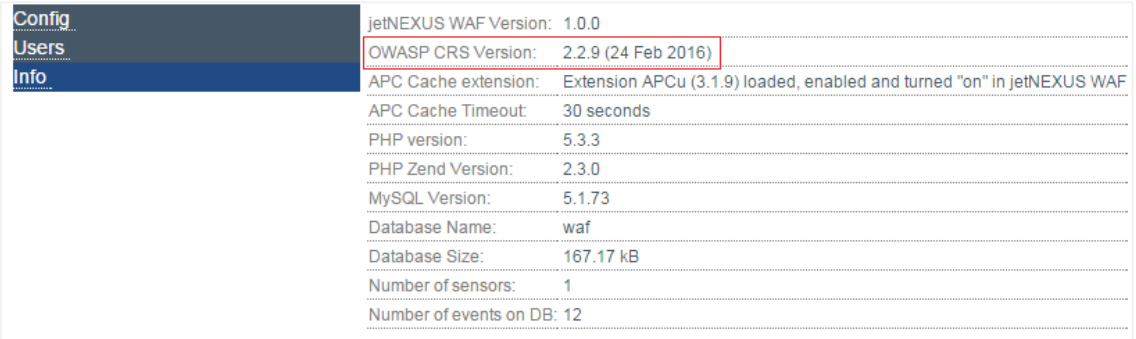
- 应用防火墙规则可以通过访问高级-软件部分进行更新
- 单击 "刷新 "以查看软件升级细节部分的可用软件按钮
- 现在显示了一个名为从云端下载的附加框
- 检查是否有OWASP核心规则集可用



- 如果是这样，你可以选中并点击下载选定的软件到ALB-X
- 然后，这个动作将把智能文件下载到存储在ALB上的应用软件中。



- 突出显示jetNEXUS-WAF-OWASP-CRS并点击应用所选软件更新并点击应用
- 防火墙将自动检测更新的规则集，加载并应用它。
- 白名单规则的ID将被保留。然而，新的规则可能开始阻止有效的应用程序资源。
- 在这种情况下，请检查白名单页面的阻止规则列表。
- 你也可以检查防火墙GUI的管理信息部分，了解OWASP CRS的版本



全球服务器负载平衡edgeGSLB)

简介

全球服务器负载平衡（GSLB）是一个术语，用于描述在互联网上分配网络流量的方法。GSLB与服务器负载平衡（SLB）或应用负载平衡（ALB）不同，因为它通常用于在多个数据中心之间分配流量，而传统的ADC/SLB则用于在单个数据中心内分配流量。

GSLB通常在以下情况下使用。

复原力和灾难恢复

你有多个数据中心，你希望以主动-
被动的方式运行它们，这样，如果一个数据中心发生故障，流量将被发送到另一个数据中心。

负载平衡和地理定位

你想根据特定的标准，如数据中心的性能、数据中心的能力、数据中心的健康检查和客户的物理位置（这样你就可以把他们送到最近的数据中心）等，在主动-主动的情况下在数据中心之间分配流量。

商业考虑

确保来自特定地理位置的用户被送至特定的数据中心。确保向其他用户提供不同的内容（或阻止），这取决于几个标准，如客户所在的国家，他们所请求的资源，语言等。

域名系统概述

GSLB可能很复杂；因此，值得花时间去了解神秘的域名服务器（DNS）系统是如何工作的。

DNS由三个关键部分组成。

- DNS解析器，即，客户端：解析器负责发起查询，最终导致所需资源的完全解析。
- 名称服务器：这是客户最初连接的名称服务器，以执行DNS解析。
- 权威名称服务器。包括顶级域（TLD）的名称服务器和根名称服务器。

一个典型的DNS交易解释如下。

- 用户在网络浏览器中输入 "example.com"，该查询进入互联网并被DNS递归解析器接收。
- 然后，解析器查询一个DNS根名称服务器（.）。
- 然后，根服务器用顶级域名（TLD）DNS服务器（如.com或.net）的地址来响应解析器，该服务器为其域名存储信息。当搜索example.com时，我们的请求被指向.com TLD。
- 然后，解析器请求.com TLD。

- 然后，顶级域名服务器以该域名的名称服务器（example.com）的IP地址作出回应。
- 最后，递归解析器向域名的名称服务器发送查询。
- 然后，IP 地址，例如 example.com，将从名称服务器返回给解析器。
- 然后，DNS解析器用最初请求的域名的IP地址来响应网络浏览器。
- 一旦DNS查询的八个步骤返回了IP地址，比如example.com，浏览器就可以请求网页。
- 浏览器向该IP地址发出**HTTP**请求。
- 该IP的服务器返回网页，在浏览器中进行渲染。

这个过程可以进一步复杂化。

缓存

解析名称服务器缓存响应可以向许多客户发送相同的响应。客户端解析器和应用程序可能有不同的缓存策略。

注意：为了测试，我们在操作系统的服务部分中停止并禁用Windows DNS客户端。
DNS名称将继续被解析；但是，它不会缓存结果或注册计算机的名称。你的系统管理员需要决定这是否是你的环境的最佳选择，因为它可能影响其他服务。

活着的时间

解析的名称服务器可以忽略生存时间（TTL），即响应的缓存时间。

GSLB概述

GSLB以DNS为基础，使用与上述非常相似的机制。

ADC可以根据本指南后面描述的几个因素来改变响应。ADC通过访问资源本身，利用监视器检查远程资源的可用性。然而，为了应用任何逻辑，系统必须首先接收DNS请求。

有几种设计允许这样做。第一种是GSLB作为权威的命名服务器。

第二种设计是最常见的实现方式，与权威性名称服务器配置类似，但使用子域。主要的权威性DNS服务器并没有被GSLB取代，而是委托一个子域进行解析。无论是直接委托名字还是使用CNAME，都允许你控制GSLB处理和不处理的内容。在这种情况下，对于不需要GSLB的系统，你不必将所有的DNS流量路由到GSLB。

提供冗余，以便在一个名称服务器（GSLB）出现故障时，远程名称服务器自动向另一个GSLB发出请求，防止网站瘫痪。

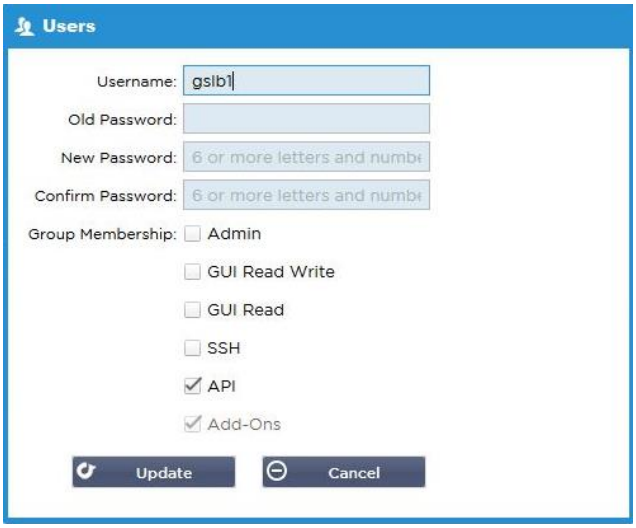
GSLB配置

下载GSLB插件后，请通过访问ADC GUI的Library > Apps页面并点击 "Deploy "按钮进行部署，如下所示。

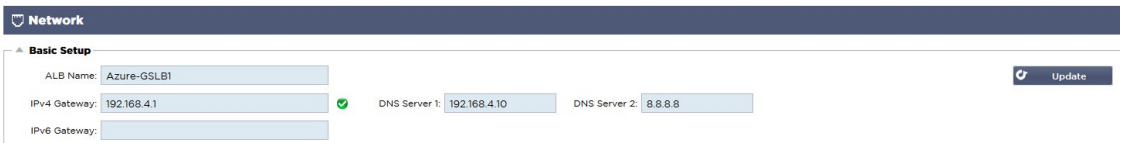
安装完成后，请在ADC GUI的Library > Add-Ons页面配置GSLB Add-On的详细信息，包括容器名称、外部IP和外部端口，如下图所示。

- 容器名称是一个运行中的插件实例的唯一名称，由ADC托管，它被用来区分同类的多个插件。
- 外部IP是你网络上的IP，它将被分配给GSLB。
- 如果你想做出基于GEO的决定，你必须配置GSLB有一个外部IP地址，因为这将使GSLB能够查看客户的真实IP地址。
- 外部端口是GSLB的TCP和UDP端口列表，可由其他网络主机访问。
- 请在外部端口输入框中输入 "53/UDP, 53/TCP, 9393/TCP "以允许DNS（53/UDP, 53/TCP）和edgeNEXUS GSLB GUI通信（9393/TCP）。
- 在配置完附加组件的细节后，请点击更新按钮。
- 点击运行按钮，启动GSLB插件。

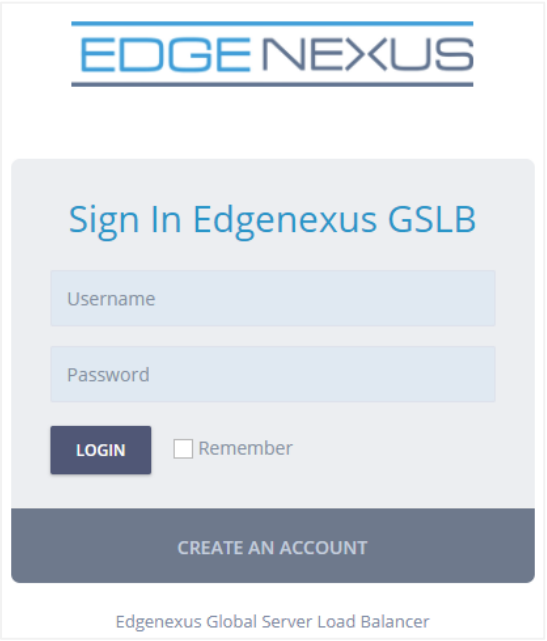
- 下一步是允许edgeNEXUS GSLB插件读取和改变ADC配置。
- 请访问ADC GUI的 "系统">"用户 "页面，编辑一个与你所部署的GSLB插件同名的用户，如下图所示。
- 编辑 "gslb1 "用户并勾选API，然后点击更新--在后来的软件版本中可能已经默认勾选了。



- 只有当你为测试或评估目的而配置GSLB，不想修改互联网上的任何DNS区域数据时，才需要进行下一步。
- 在这种情况下，请指示ADC使用GSLB Add-On作为其主要的DNS解析服务器，方法是在ADC GUI的系统>网络页面中改变 "DNS服务器1"，如下图所示。
- DNS服务器2一般可以配置为你的本地DNS服务器或互联网上的服务器，如Google 8.8.8.8。

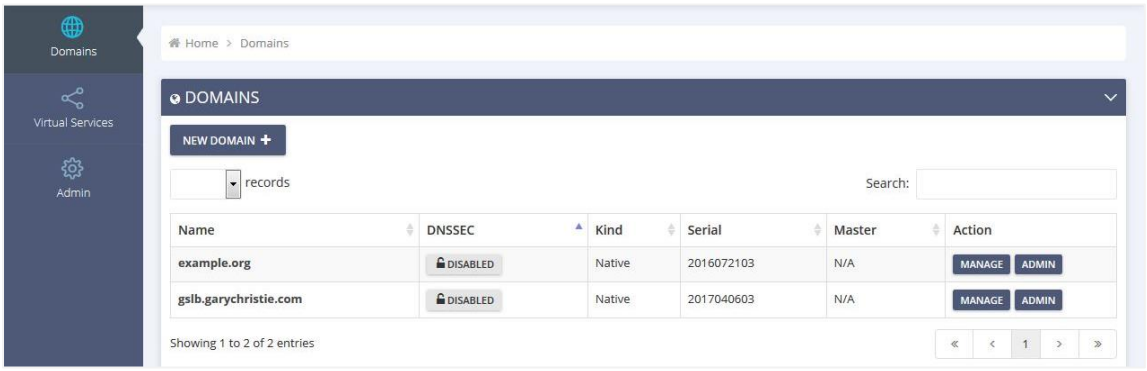


- 现在是登录GSLB GUI的时候了。
- 请导航到ADC GUI的Library > Add-Ons页面，并点击Add-On GUI按钮。
- 点击将打开一个新的浏览器标签，呈现GSLB GUI登录页面，如下图所示。

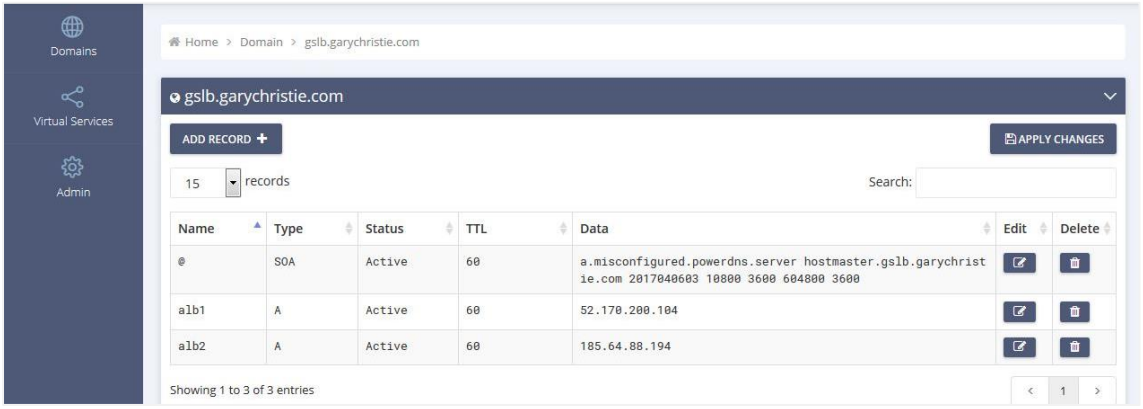


- 默认的用户名是admin，默认的密码是jetnexus。请不要忘记在GSLB GUI的管理员>我的资料页面上修改密码。
- 配置顺序的下一步是在PowerDNS名称服务器中创建一个DNS区，它是GSLB的一部分，使其成为 "example.org "区的权威名称服务器或子域区，如上面 "基于DNS的GSLB概述 "部分提到的 "geo.example.org "子域。
- 关于DNS区域配置的深入细节，请参见**PowerDNS名称服务器文档**。图6中显示了一个区域的例子。

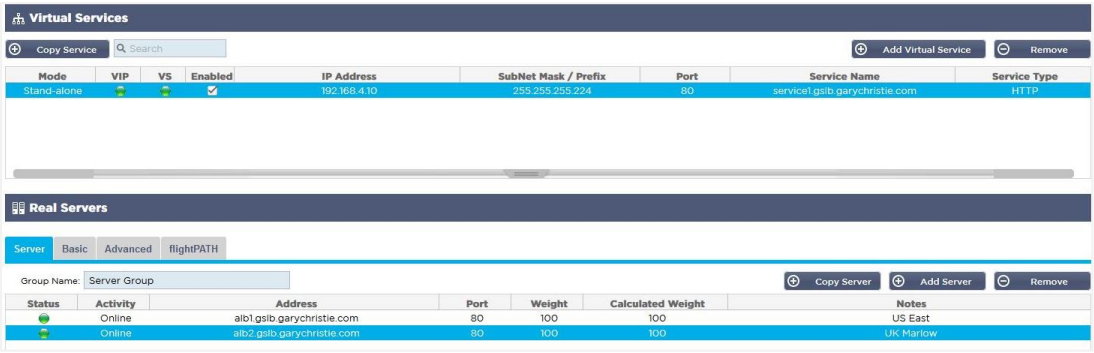
* edgeNEXUS GSLB GUI是基于一个开源项目PowerDNS-Admin。



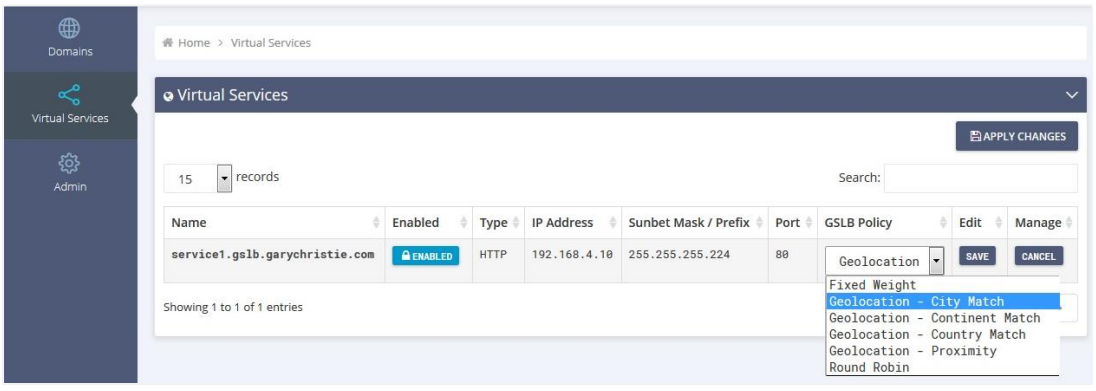
- 创建DNS区域后，请点击 "管理 "按钮，向该域添加主机名，如下图所示。
- 在GSLB GUI内编辑任何现有记录后，请按 "保存 "按钮。
- 在您完成创建主机名记录后，请点击 "应用更改 "按钮。如果你不点击 "应用"，然后修改页面，你将失去你的变化。
- 下面我们创建的记录是IPv4地址记录。
- 请确保你为你希望解决的所有记录创建一个记录，包括IPv6地址的AAAA记录。



- 现在，让我们回到ADC GUI，定义一个虚拟服务，与我们刚刚创建的DNS区域相对应。



- 虚拟服务将被用于GSLB域中服务器的健康检查。
- GSLB利用ADC的健康检查机制，包括自定义监视器。它可以与ADC支持的任何服务类型一起使用。
- 请浏览ADC GUI的服务>IP服务页面，并创建一个虚拟服务，如下图所示。
- 请确保在服务名称中配置你希望在GSLB中使用的正确域名。GSLB将通过API读取这个信息并自动填充到GSLB GUI中的虚拟服务部分。
- 请在上图的真实服务器部分添加GSLB域中的所有服务器。
- 你可以通过域名或IP地址指定服务器。
- 如果你指定了域名，那么它将使用在你的GSLB上创建的记录。
- 你可以在基本和高级选项卡中选择不同的服务器健康监测方法和参数。
- 你可以将一些服务器的活动设置为待机，以实现主动-被动方案。
- 在这种情况下，如果一个 "在线 "服务器未能通过健康检查，而有一个健康的备用服务器，Edgenexus EdgeGSLB将把域名解析为备用服务器的地址。
- 关于配置虚拟服务的细节，请参考虚拟服务部分。
- 现在，让我们转到GSLB GUI。
- 导航到虚拟服务页面，为从ADC虚拟服务部分检索的API的域选择一个GSLB策略。
- 这在下图中显示。



- GSLB支持以下政策。

政策	描述
固定重量	GSLB选择权重最高的服务器（服务器权重可由用户指定）。在多个服务器拥有最高权重的情况下，G

	SLB将随机选择其中一个服务器。
加权循环赛	一个接一个地选择服务器，排成一排。具有较高权重的服务器比具有较低权重的服务器被更多地选择。
地理定位	接近性 - 利用地理经纬度数据选择离客户所在地最近的服务器。与客户在同一国家的服务器是首选，即使它们比邻国的服务器更远。
地理定位	城市匹配 - 选择一个与客户相同城市的服务器。如果在客户所在城市没有服务器，则选择客户所在国家的服务器。如果在客户所在的国家没有服务器，则选择同一大洲的服务器。如果这是不可能的，就用地理经纬度数据选择一个离客户所在地最近的服务器。
地理定位	国家匹配 - 选择一个与客户相同国家的服务器。如果没有同一国家的服务器，则尝试同一大洲，然后尝试最近的地点。
地理定位	大陆匹配 - 选择一个与客户相同大陆的服务器。如果在同一大洲没有服务器，则尝试最近的位置。

- 在你选择了一个GSLB政策后，请不要忘记点击 "应用更改 "按钮。
- 现在你可以通过点击管理按钮审查和调整虚拟服务的细节。
- 这将呈现一个如下所示的页面。
- 如果你选择了基于权重的策略之一，你可能需要调整服务器GSLB的权重。
- 如果你选择了基于地理位置的GSLB策略之一，你可能需要为服务器指定地理数据。
- 如果你没有为服务器指定任何地理数据，GSLB将使用MaxMind的GeoLite2数据库提供的数据。
- 你也可以在这个页面上修改服务器名称、端口和活动。
- 当你点击 "应用变化 "按钮时，这些变化将与ADC同步。

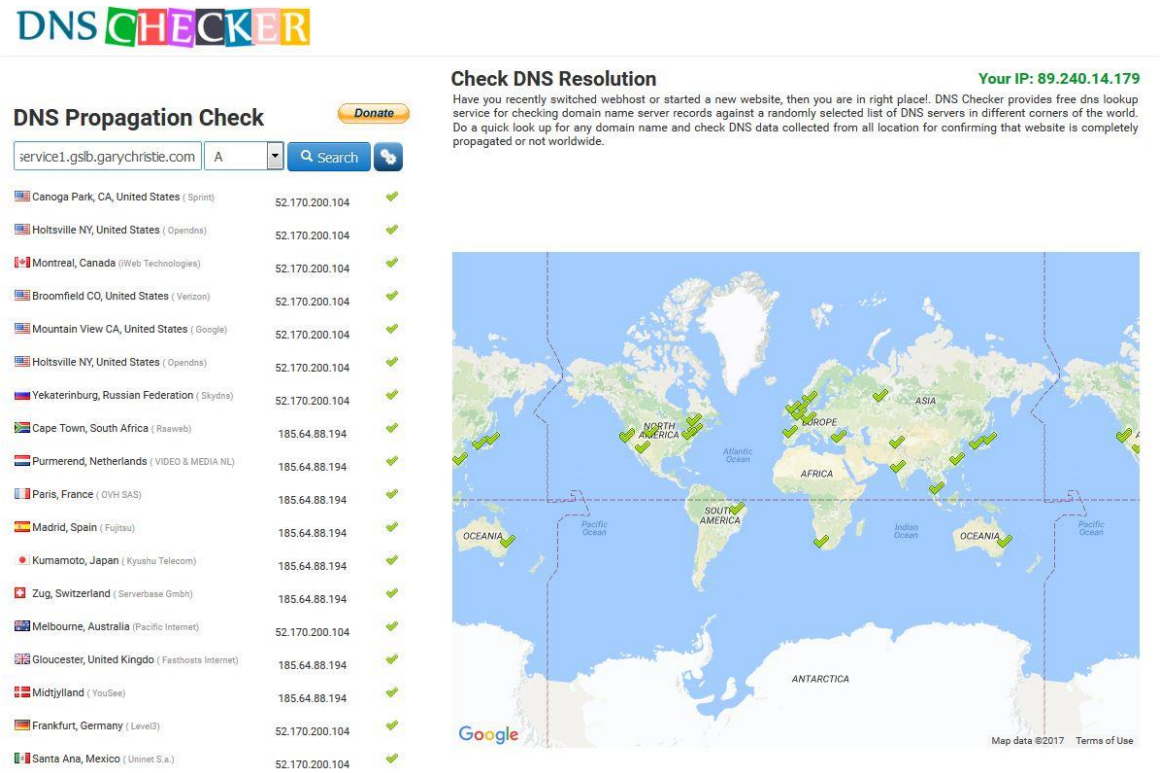
- 检查GSLB将发送什么答案给客户的一个好方法是使用NSLOOKUP。
- 如果你使用的是Windows，命令如下。

```
NSLOOKUP service1.gslb.garychristie.com 192.168.4.10
```

- 其中service1.gslb.garychristie.com是你希望解决的域名。
- 其中192.168.4.10是你的GSLB的外部IP地址。
- 要检查互联网上将返回什么IP地址，你可以使用谷歌的DNS服务器8.8.8.8。

  Nslookup service1.gslb.garychristie.com 8.8.8.8。

- 或者，你可以使用HTTPs://dnschecker.org这样的东西。
  例如HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com。
- 结果的例子见下文。



自定义地点

私人网络

GSLB也可以被配置为使用自定义位置，这样你就可以在内部 "私人
"网络上使用它。在上面的方案中，GSLB通过将客户的公共IP地址与数据库交叉引用来确定客户的位置。它还从同一数据库中计算出服务IP地址的位置，如果负载平衡策略被设置为GEO策略，它将返回最近的IP地址。这种方法对公共IP地址非常有效，但对于符合RFC 1918的IPv4地址和RFC
4193的IPv6地址的内部私有地址，却没有这种数据库。

请参阅解释私有寻址的维基百科页面 **HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK**

它是如何工作的

通常，将我们的GSLB用于内部网络的想法是，来自特定地址的用户将根据他们所处的网络收到不同的服务答案。因此，让我们考虑两个数据中心，北方和南方，分别提供一个名为north.service1.gslb.com和south.serv

ice1.gslb.com的服务。当一个来自北方数据中心的用户查询GSLB时，我们希望GSLB用与north.service1.gslb.com相关的IP地址进行响应，前提是该服务工作正常。或者，如果一个来自南方数据中心的用户查询GSLB，我们希望GSLB再次使用与south.service1.gslb.com相关的IP地址进行响应，前提是服务正常运行。

那么，我们需要做什么来实现上述情景？

- 我们需要至少有两个自定义地点，每个数据中心一个。
- 将各种专用网络分配给这些地点
- 将每项服务分配到各自的位置

我们如何在GSLB上配置这个外观？

为北方数据中心增加一个地点

- 点击左侧的 "自定义位置"。
- 点击添加位置
- 命名
  - 北方
- 为你的北方网络添加一个私有IP地址和子网掩码。在这个练习中，我们将假设服务和客户的IP地址是在同一个专用网络中
  - 10.1.1.0/24
- 添加 "大陆 "代码
  - 欧盟
- 添加国家代码
  - 英国
- 添加城市
  - 恩菲尔德
- 添加纬度 - 从谷歌获得
  - 51.6523
- 添加经度 - 从谷歌获得
  - 0.0807

注意，请使用正确的代码，可以从这里获得。

为南方数据中心增加一个地点

- 点击左侧的 "自定义位置"。
- 点击添加位置
- 命名
  - 南方
- 为你的南方网络添加一个私有IP地址和子网掩码。在这个练习中，我们将假设服务和客户的IP地址是在同一个专用网络中。

    - 192.168.1.0/24
- 添加 "大陆 "代码
    - 欧盟
- 添加国家代码
    - 英国
- 添加城市
    - 克罗伊登
- 添加纬度 - 从谷歌获得
    - 51.3762
- 添加经度 - 从谷歌获得
    - 0.0982

注意，请使用正确的代码，可以从这里获得。

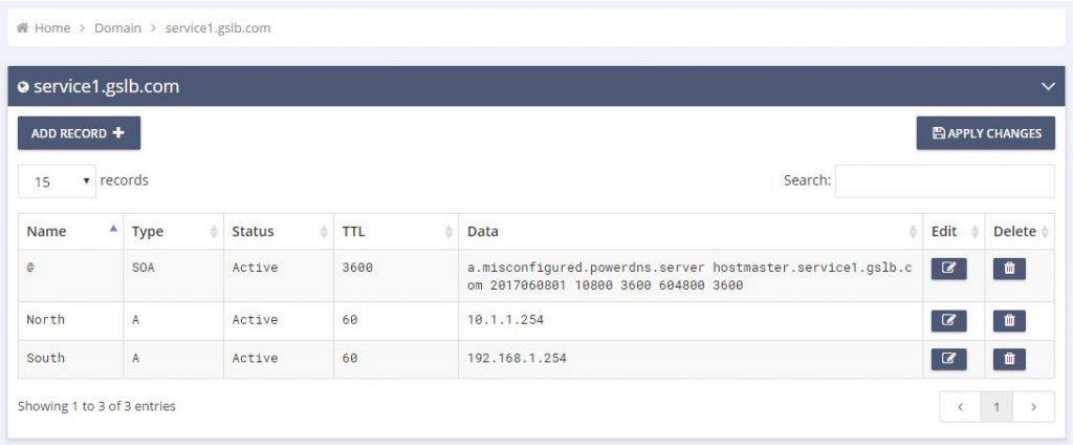
为north.service1.gslb.com添加一个A记录

- 点击域名service1.gslb.com
- 点击添加记录
- 添加名称
    - 北方
- 类型
    - A
- 状况
    - 活跃
- TTL
    - 1分钟
- IP地址
    - 10.1.1.254（注意这与恩菲尔德的位置在同一网络中）。

为south.service1.gslb.com添加一个A记录

- 点击域名service1.gslb.com
- 点击添加记录
- 添加名称

    - 南方
- 类型
    - A
- 状况
    - 活跃
- TTL
    - 1分钟
- IP地址
    - 192.168.1.254 (注意这与克罗伊登的位置在同一网络中)



交通流

例子1--北方数据中心的客户

- 客户端IP 10.1.1.23查询GSLB的service1.gslb.com。
- GSLB查找IP地址10.1.1.23并与自定义位置Enfield 10.1.1.0/24相匹配。
- GSLB查看service1.gslb.com的A记录，并匹配north.service1.gslb.com，因为它也在网络10.1.1.0/24中。
- GSLB以service1.gslb.com的IP地址10.1.1.254来响应10.1.1.23。

例2--南方数据中心的客户

- 客户端IP 192.168.1.23查询GSLB的service1.gslb.com。
- GSLB查找IP地址192.168.1.23，并与自定义位置Croydon 192.168.1.0/24相匹配。
- GSLB查看service1.gslb.com的A记录，匹配south.service1.gslb.com，因为它也在192.168.1.0/24网络中。
- GSLB以192.168.1.254的IP地址响应192.168.1.23，用于service1.gslb.com。

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。

如果您对edgeADC、edgeWAF或edgeGSLB有一个有效的支持和维护合同，我们将通过技术支持提供所有支持。

要提出支持票，请访问。

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