NetScaler Intelligent Traffic Management

Machine translated content

Disclaimer

Contents

新增功能

April 29, 2022

新的特性/增强功能	版本
警报 -此功能监视来自全球最终用户网络的已配置平台的性能问题或异常情况。	2022.02.15
本地持久性 -此功能在启用时提供决策粘性功能。这些请求使用 IP 子网掩码进行标识，其长度是可配置的。例如，当客户端在特定时段（Persistence TTL）内向同一个应用程序重复请求时，原始决策将被送回。	2021.12.09
AWS ELB Connector - 这个新的连接器通过 Fusion 从 AWS ELB 提取 `HealthyHostCount`、`UnHealthyHostCount` 和 `Load Balancer Capacity Units (LCUs)` 指标。它为客户提供了集成的负载平衡体验，并可以了解其 Openmix 应用程序中提供的 Fusion 指标。	2019.08.16
更改平台类型（私有到社区）：此新功能允许客户更改其私有平台或 GSLB 的当前设置以引用社区平台。对于私有平台托管在公共数据中心或云区域的客户，此功能非常有用。	2019.07.03
新控制板 -新的 ITM 控制面板现在可操作、信息密集、可定制，总体上比以前的版本更有用。在新的控制面板中，您可以查看“雷达会话”、“雷达性能”、“Openmix 流量管理决策”和“声纳监视状态”图表。您可以创建多个控制板，每个控制板都针对您关心的视图进行定制。您还可以选择将 ITM Visualizer 或控制板设为默认登录页面。	2019.06.27
融合隔离：如果失败的 Fusion 数据馈送失败或轮询间隔小于 24 小时，此功能可隔离客户失败的 Fusion 数据馈送。Fusion 应用隔离逻辑来阻止这些失败的源运行，以节省资源（CPU/内存）并避免影响其他良好或有效的 Fusion 数据源。	2019.06.19
启用/禁用适用于 Openmix 的平台 - 现在可以通过在“平台设置”中打开或关闭已启用 **Openmix** 按钮来为 Openmix 启用或禁用平台。如果 Openmix 禁用了某个特定平台，则在 Openmix 决策中不会考虑该平台。	2019.04.09

新的特性/增强功能	版本
平台地理 位置-此功能允许客户查看和管理分配给平台的地理位置。默认情况下，没有分配给专用平台的 **Geo** 位置。当用户创建私有平台并配置 Radar 探测时，我们使用探测 URL 对平台进行地理定位。或者，用户可以手动分配 Geo，而不依赖于 Radar URL 路径。对于 GSLB 和 F5 配置导入，我们地理定位公有 IP 并将其用作平台的 **Geo** 。社区平台默认继承平台的原始位置。	2019.04.09
Visualizer：向下钻取到州级：活动警报，其中包含有关云、数据中心、CDN 和其他服务的性能和可用性的信息。这些警报是在美国境内的州一级进行测量和查看的。	2019.04.01
可视化工具：F5 和 GSLB 导入 - F5 和 GSLB 导入：您现在可以通过 GSLB 或 F5 配置导入平台。基本站点信息（IP 和名称）作为 ITM 平台导入。ITM 对站点进行地理定位，并允许在可视化工具上显示平台以进行性能分析。	2019.03.29
G-Core 清除适配器 -G-Core CDN 清除适配器现已添加到 ITM 支持运行清除的适配器列表中。	2019.03.29
面向所有社区提供商的 Radar DSA 3 —为了不断改进 Radar 社区和基准测试的准确性，我们最近发布了新的动态内容基准测试。这个新的基准具有一个动态的 HTML 页面和一个签名，用来验证测量结果。	2019.03.21
可视化工具 —ITM 可视化工具是一种直观而智能的工具，可让您监视和分析 ISP 和服务的全球性能。ITM Visualizer UI 提供主动警报，其中包含有关云、数据中心、CDN 和其他服务的性能和可用性的信息。ITM 社区在全球范围内衡量这些警报。ITM Radar 通过 Radar 社区从全球的真实用户那里收集了数十亿份测量结果。它使用众包模型来衡量这些警报。	2019.03.08
现在，**ITM** 演示门户网站提供可视化展台和 **Openmix** 的导游（演练）。您可以通过 ITM 门户内的帮助图标访问演示门户。在演示门户 的右下角，您可以看到一个启动导游的图标。	2019.03.08

第三方声明

September 22, 2023

NetScaler Intelligent Traffic Management 第三方通知 (PDF)

词汇表

September 22, 2023

术语	说明
应用程序	Openmix 应用程序是一种可以在门户中配置的负载平衡逻辑规范。该应用程序将针对向 Openmix 发出的每个请求进行处理，并将根据指定的逻辑做出路由决策。可以将这些应用程序用于一种或多种类型的内容。客户可能将一个应用程序用于一种具有高业务价值的内容类型，将另一个应用程序用于价值较低且必须以不同的方式进行路由的内容。例如，客户可能有一个应用程序用于处理向所有用户显示的内容，该应用程序专注于路由到最快的提供程序，而不考虑成本。客户可能还有另一个应用程序用于处理很少显示的内容，该应用程序专注于针对低价值内容在提供程序之间进行成本优化。在上述场景中，客户将有两个 Openmix 应用程序。
社区测量	社区测量是通过众包模型获得的，该模型为客户提供了全球地理和逻辑层面的供应商绩效和可用性视图。参与的社区成员可以免费使用社区测量（需要安装 JavaScript 标记）。未做出贡献（即，未进行 JS 集成）的组织访问社区数据需要付费。
决策	Openmix 决策被指定为向 NetScaler 的负载均衡器之一发出的单个请求。对于 DNS，它是向 DNS 负载均衡器发出的单个 DNS 请求。对于 HTTP，它是向 Openmix HTTP 端点发出的 GET 或 HEAD 请求。
测量	测量涉及 Radar 和从最终用户那里收集的有关服务应用程序性能的数据。有关社区测量，请参阅“社区测量”。
平台	平台是客户想在 Radar 内监控的或者想在 Openmix 应用程序中使用的 CDN、云、数据中心或其他端点。

术语	说明
私有测量	Radar 私有测量是指如下所述的测量或遥测（在流媒体情况下）：将反馈最终用户的体验，但不与社区共享该信息。这可以适用于客户正在寻找测量的地方：+ 他们自己的数据中心架构 /s + 使用他们自己的测试对象或页面 + 使用他们与供应商的合同 + 音频/视频最终用户体验的质量

Radar 数据定义

April 27, 2020

已部署 Radar 标签的 Benchmark 合作伙伴和 Radar 社区成员可以选择访问其 Radar 测量结果。对于基准合作伙伴，无论在哪个页面上部署 Radar 标签，也无论何时进行测量，我们都会分享该合作伙伴的测量结果。社区成员可以看到他们的网站访问者采取的所有测量结果，无论是哪个基准合作伙伴。

客户 Radar 数据共享

当 Radar 标签部署程序在其 Web 站点上进行 Radar 测量时，可以选择访问我们从 Radar 客户端接收的字段的子集。在生成报告之前，用户 IP 地址是匿名的。有关日志描述，请参阅网络视图 (NEM) 文档。

原始 Radar 测量

原始 Radar 测量包含我们在进行 Radar 测量时从 Radar 客户端接收的字段的子集。在生成报告之前，用户 IP 地址是匿名的。

这些报告可以每天或实时提供，在 5 分钟内提供测量数据。

这些文件可以采用制表符分隔、CSV 或 JSON 格式。有关日志描述和报告，请参阅 Netscope 文档。

Autonomous System Numbers

https://s3-eu-west-1.amazonaws.com/community-radar/ref/asns.json.gz

社区（公共）提供商 ID

https://s3-eu-west-1.amazonaws.com/community-radar/ref/providers.json.gz

探头类型（测量类型）

https://s3-eu-west-1.amazonaws.com/community-radar/ref/probetypes.json.gz

---

响应代码

密码	模块	说明	值
0	全部	成功	测量值
1	远程探测	HTTP 请求超时	0
2	远程探测	RTMP 连接失败	0
3	远程探测	未找到 RTMP 流	0
4	远程探测	HTTP 无效文件	0
5	导航定时	不支持导航计时 API	0

市场代码

密码	名称	ISO 缩写
0	未知	XX
1	北美洲	不适用
2	大洋洲	OC
3	欧洲	欧盟
4	亚洲	作为
5	非洲	AF
6	南美洲	SA

国家/地区代码

根据ISO 3166 -1 Alpha 2

https://s3-eu-west-1.amazonaws.com/community-radar/ref/countries.json.gz

地区代码

我们所知道的区域没有 ISO 标准。此外，我们的 GEO 提供商仅为少数国家提供区域。根据他们的文件，“区域”的目标是将某些国家细分为大于国家的区域。例如“美国-西南”

首先，我们提供了我们自己的数字“区域 ID”和映射：https://s3-eu-west-1.amazonaws.com/community-radar/ref/regions.json.gz

> 注意：我们保留更改该文件格式的权利。创建要在这些映射中加载的任何代码都必须牢记这一点。长期来看，将会有一个 API 调用来下载这些映射。

州代码

有适用于各州的 ISO 标准 3166-2。我们正在评估该标准是否符合我们的需求。所以开始，我们正在使用我们自己的数字字符串映射。与区域类似，格式可能会改变https://s3-eu-west-1.amazonaws.com/community-radar/ref/states.json.gz

城市代码

我们正在使用我们自己的数字来字符串映射。与区域类似，格式可能会改变，我们最终可能会将这些映射作为 API 调用提供。https://s3-eu-west-1.amazonaws.com/community-radar/ref/cities.json.gz

Visualizer

September 22, 2023

简介

ITM 可视化工具是一款直观、智能的工具，可让您监视和分析 ISP 和服务的全球性能。ITM Visualizer UI 提供主动警报，其中包含有关云、数据中心、CDN 和其他服务的性能和可用性的信息。ITM 社区在全球范围内衡量这些警报。ITM Radar 通过 Radar 社区从全球的真实用户那里收集了数十亿份测量结果。它使用众包模型来衡量这些警报。

对于新用户，可视化工具页面打开，其中包含地图上所有可用的社区警报。ITM Radar 可测量性能异常，并在全球几乎每个网络和每个位置生成警报。

Visualizer 地图上的四个磁贴显示以下数据。

处于活动状态的 **Radar** 警报

主动 Radar 警报是最新的和持续的。

Radar 警报

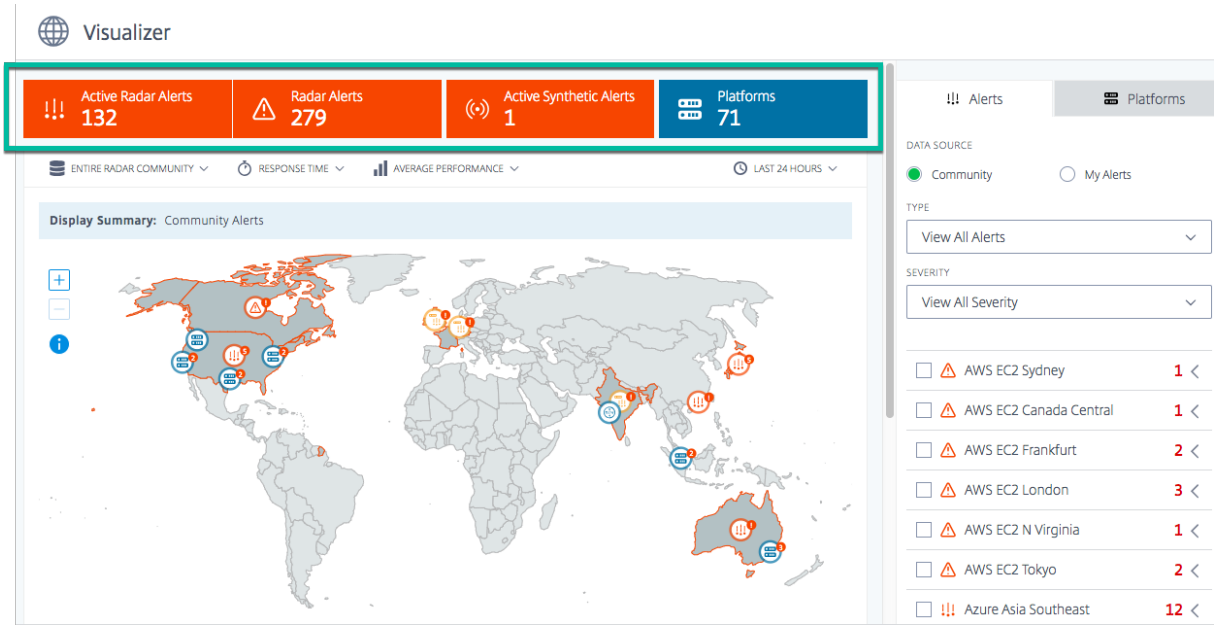
主动 Radar 警报是最新的和持续的。默认情况下，此磁贴显示过去 24 小时内的所有警报，但会根据用户选择的时间段而变化。

活动合成警报

这些警报是实时发生的。Sonar 是我们的综合监视系统，用于测量服务或数据中心的全球可用性，它会生成这些警报。

平台

客户帐户中配置的平台的数量。



查看选项

您可以使用以下条件在地图上查看警报和平台：

整个 **Radar** 社区或者仅限您的访客

选择 **Radar** 社区，查看整个 Radar 社区中平台的性能。或者，要仅针对经由您的私有平台的访客查看性能，请选择仅限您的访客。

响应时间或可用性

单击地图或列表中的任意平台，基于可用性或响应时间查看其性能。

最佳性能或平均性能

选择平均性能或“最佳性能”，查看您的平台将获得的平均/最佳性能。

平均性能 类似于在您的平台之间进行轮询，最佳性能是我们通过使用 ITM 获得的性能。

当您选择最佳性能时，您会在地图上看到基于最佳性能平台的性能。例如，如果您要查看特定国家/地区的性能，并且选择了两个平台，则最佳性能会根据这两个平台中对于该国家/地区具有最佳性能（可用性最高或响应时间最短）的那个平台为国家/地区地图着色。

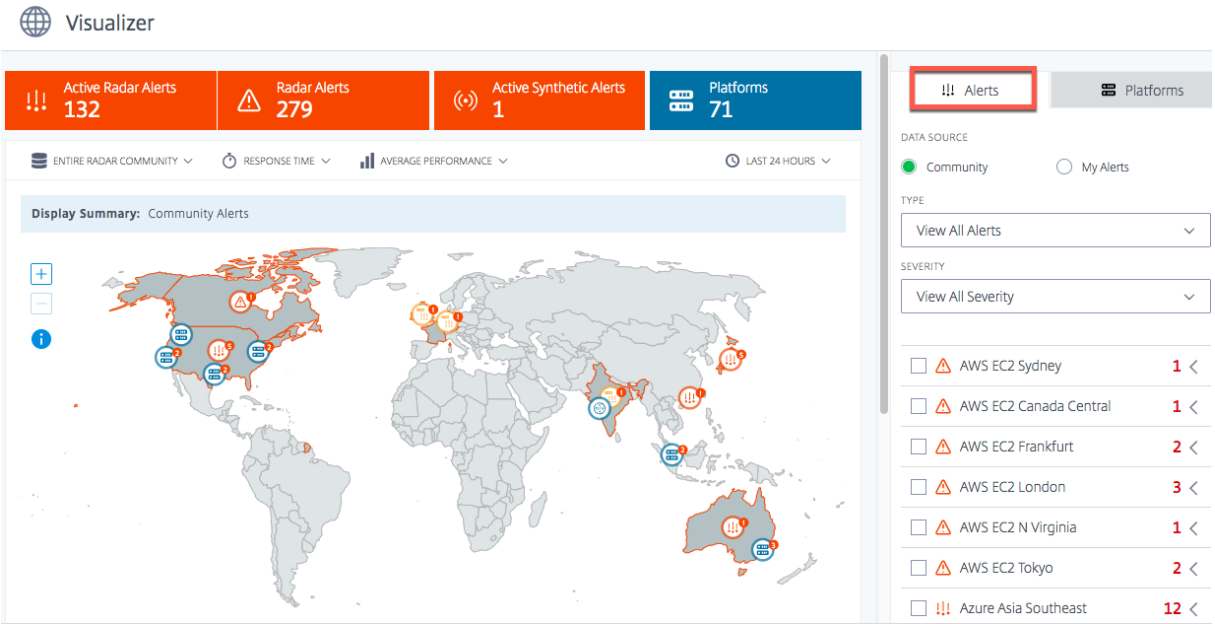
或者，如果选择“平均性能”，则可以在地图上看到基于所有选定平台的平均值的性能。它使用两个平台的平均可用性（或响应时间）为国家/地区地图着色。

时间周期

可以为以下时段生成地图上的警报：过去 **60** 分钟、过去 **24** 小时、过去 **48** 小时、过去 **7** 天、过去 **30** 天，或自定义范围。默认视图为“过去 24 小时”。每次更改时间段时，它都会刷新地图上的数据，并向您显示该时间段内触发的警报。

警报

警报选项卡是您登陆 Visualizer 页面时显示的默认选项卡。对于没有自己的警报的新用户，显示的默认数据源是社区。这意味着您作为新用户在地图上查看的所有警报均为社区警报。即使您已设置警报，但没有任何活动或持续警报，您的视图也会默认为社区警报。但是，如果您已设置警报，并且有持续有效的警报，则默认视图是您自己的警报。有关警报的更多信息，请参阅警报。



社区

社区警报是 ITM Radar 在 ITM 社区中发生的性能问题或异常。这些警报通过来自全球的最终用户网络进行测量。当您首次以新用户身份打开 可视化 工具时，您会在地图上看到所有社区警报。设置您自己的警报后，您会看到这些警报，而不是社区警报。

但是，如果您设置了私有平台和警报，则您自己的警报会显示为我的警报（默认视图）。

我的提醒

这些警报是您的私有平台的性能问题或异常情况。它使用遍布全球的最终用户网络来衡量这些警报。

作为新用户，如果您没有看到任何警报，这意味着您没有设置任何警报。您可以从左侧边栏转到“警报”页面，为您的平台性能设置警报。但是你需要先设置你的私有平台。要设置平台，您可以从左侧边栏转到 平台 页面，或通过 平台 选项卡即时执行。

警报详细信息

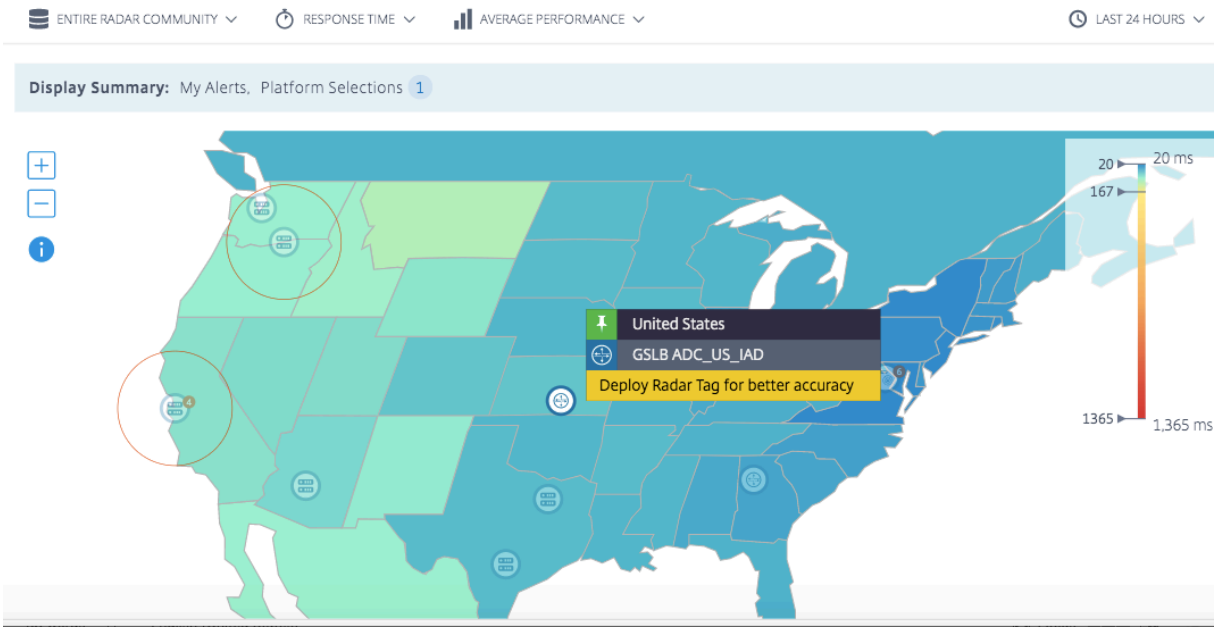
您可以将鼠标悬停在地图上的警报上，以查看触发警报的国家/地区和服务。有关特定警示的更多详细信息，请

1. 单击地图上的警报图标以选中服务触发警报的复选框，并在列表中突出显示该警报。
2. 单击所选平台或服务右侧的箭头以显示警报的详细信息，包括

    a) 数据源的可用性 或 响应时间
    b) 警报的持续时间

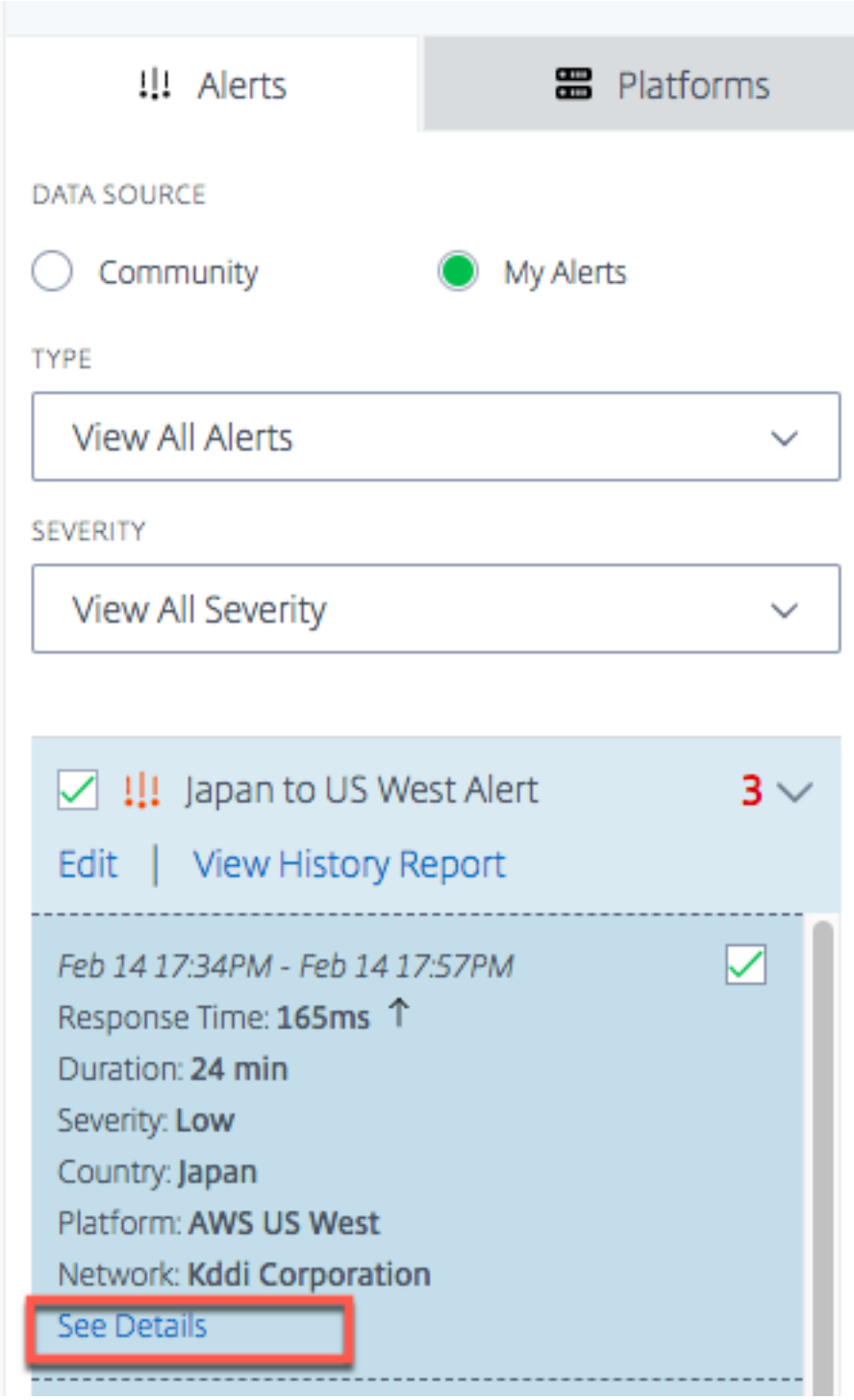
c) 警报的严重性
d) 检测到问题的网络所在的国家/地区
e) 触发了警报的平台的名称。
f) 从中测量问题的 网络 名称。

状态级警报：活动警报，其中包含有关云、数据中心、CDN 和其他服务的性能和可用性的信息。这些警报是在美国境内的州一级进行测量和查看的。



要更深入地了解警报的详细信息，请单击查看详细信息以转至警报页面。

> 注意：您只能看到自己的警报的查看详细信息链接。

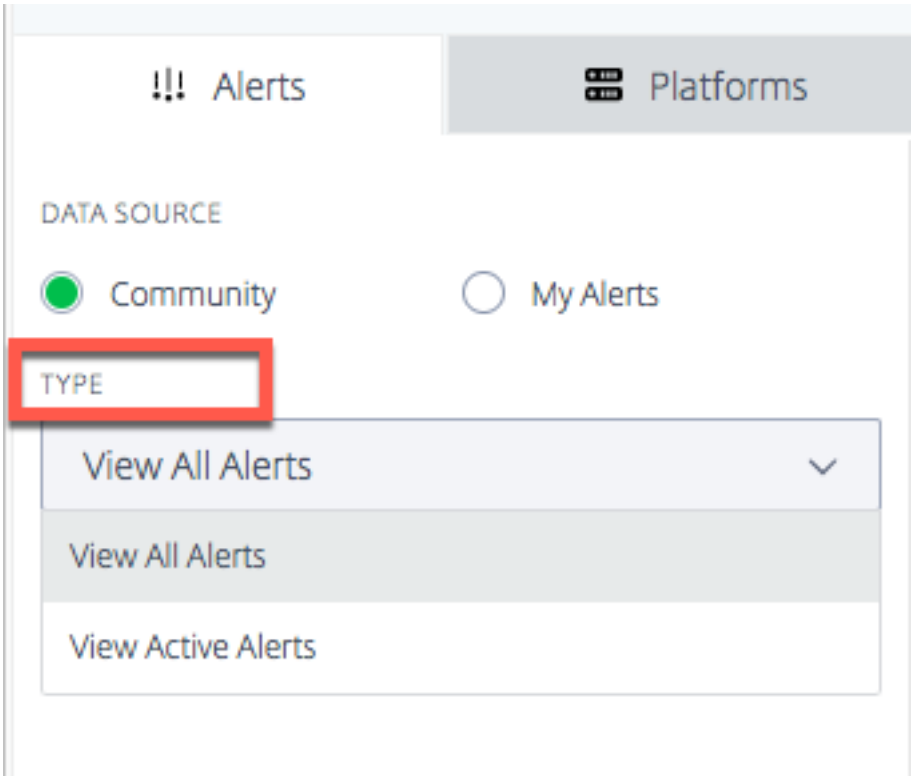


警报类型

类型菜单允许您查看以下类型的警报。

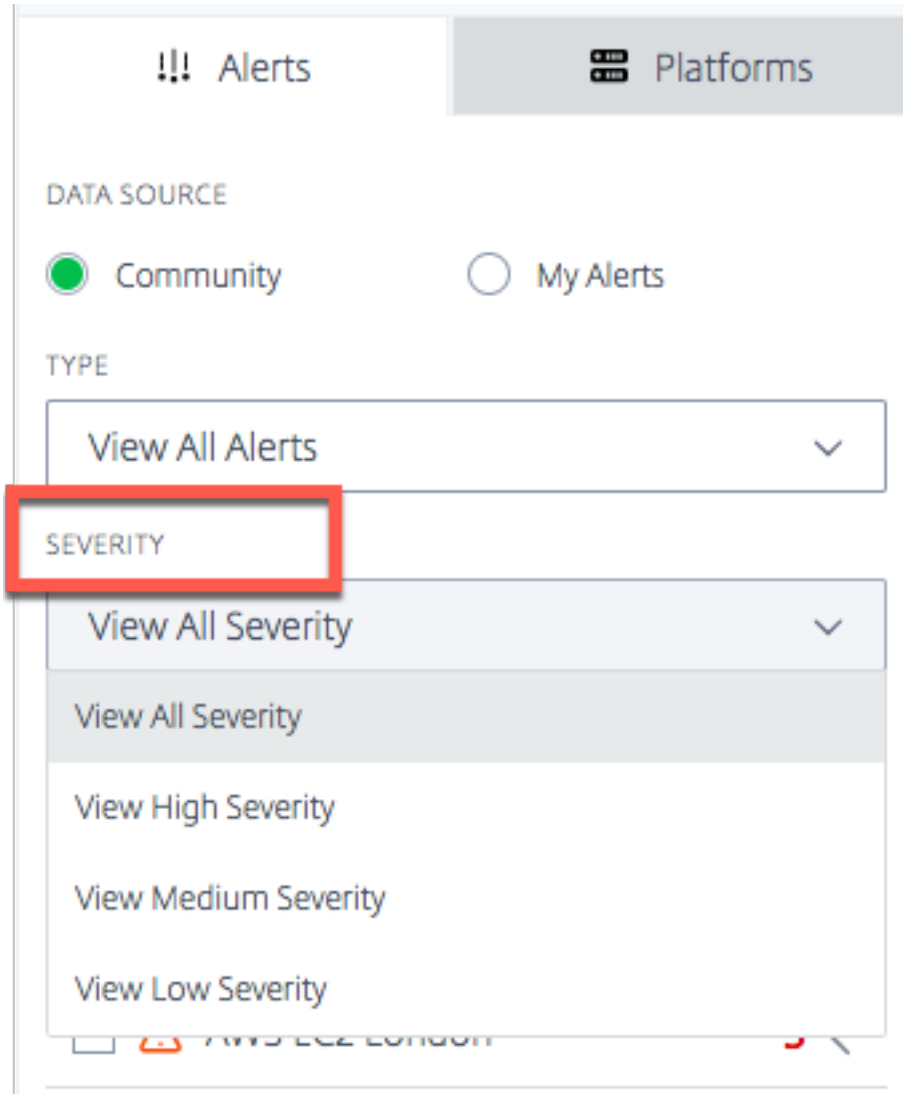
所有警报　所有警报包括处于活动状态的警报和历史警报。历史警报是在所选时段内较晚生成的警报。

处于活动状态的警报　处于活动状态的警报包括正在进行的警报。它们在用户指定的时段内是有效和最新的。



警报严重性

可以根据高、中和低严重性来过滤警报。“所有严重性”是默认显示。



严重性逻辑　对于可用性：

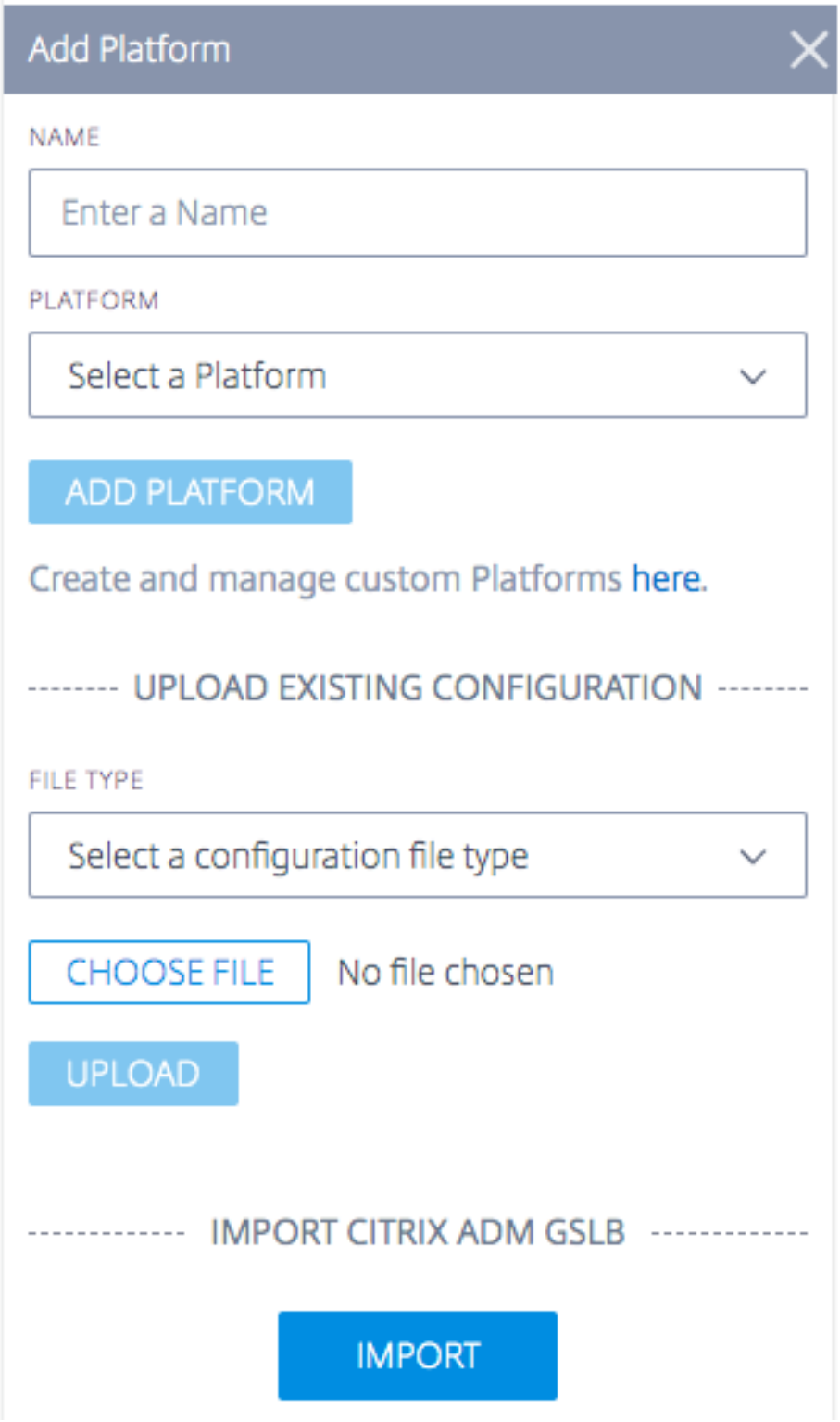
- 如果比阈值低 50% 以上 -> 严重性为高
- 如果比阈值低 25% 以上但 50% 以下 -> 严重性为中
- 如果比阈值低 25% 以下 -> 严重性为低

对于响应时间：

- 如果比阈值高 200% 以上 -> 严重性为高
- 如果比阈值高 100% 以上但 200% 以下 -> 严重性为中
- 如果比阈值高 100% 以下 -> 严重性为低

平台

选择平台选项卡时，您会看到您已添加的平台的列表。但是，如果您是新用户并且尚未设置任何平台，则可以在此处即时添加社区平台，也可以通过单击在此处创建和管理自定义平台链接来设置私有平台。



添加社区平台

1. 要添加社区平台，请单击添加平台栏旁边的 + 图标。
2. 为平台指定一个名称，然后从平台菜单中的社区平台列表中选择该平台。
3. 单击添加平台。

添加自定义/私有平台

1. 要添加私有平台，请单击“添加平台”栏旁边的 + 图标。
2. 单击“在此处创建和管理自定义平台”链接，该链接将转到“平台”页面，您可以在其中添加新的私有平台。或者，您可以从左侧边栏转到 平台 页面。

上传现有配置：**NetScaler** 和 **F5 BIG-IP DNS**

此选项允许您选择 NetScaler 或 F5 BIG-IP DNS 配置文件并直接导入配置（现有平台的）。它会自动为您的 NetScaler 或 F5 BIG-IP DNS 配置创建私有平台。

从 **ADM Service** 导入 **Citrix GSLB**

此选项允许您直接导入在 ADM 服务中配置的所有 GSLB。

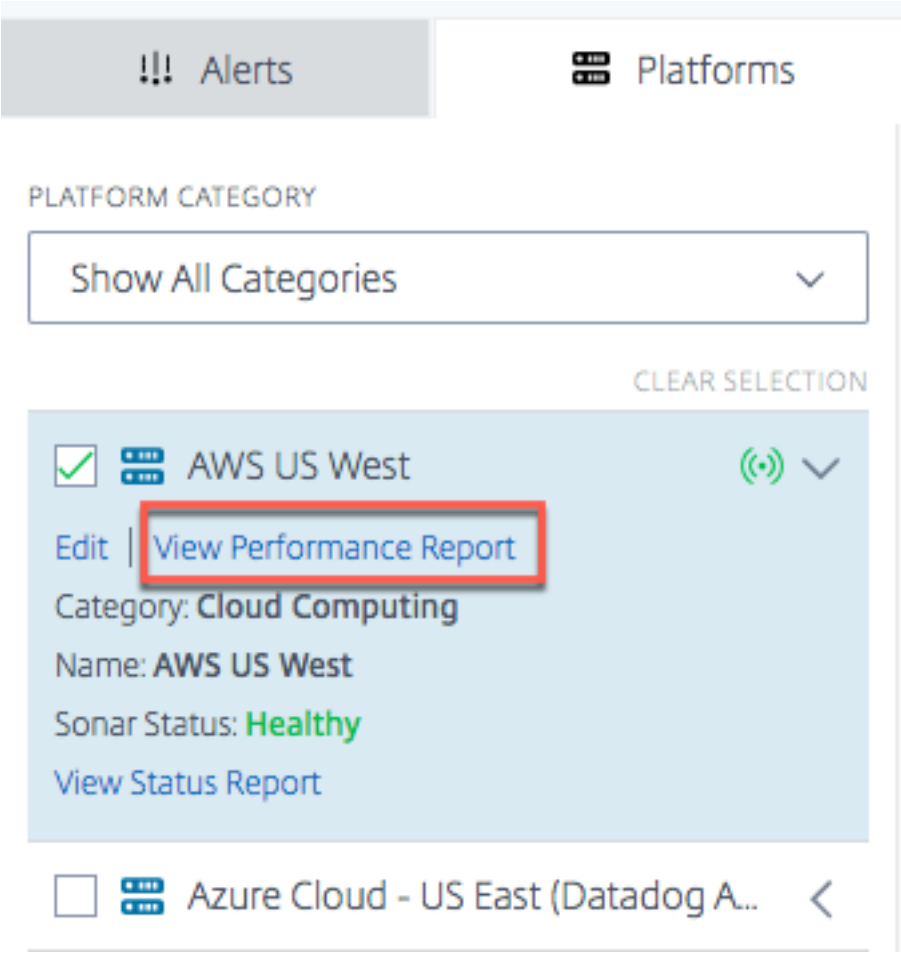
如果您使用的是 Citrix Cloud ADM Service，则可以导入在该位置配置的 GSLB。基本站点信息-IP 和名称作为 ITM 平台导入。ITM 对站点进行地理定位，并允许平台显示在可视化工具上以进行性能分析。

绩效报告

“雷达性能报告”提供了有关特定平台、触发的警报以及测量它的每个网络的详细信息。该报告显示“响应时间”或“可用性”度量，以及所测量问题的时间段。它包含了在 可视化工具中应用的所有过滤器。

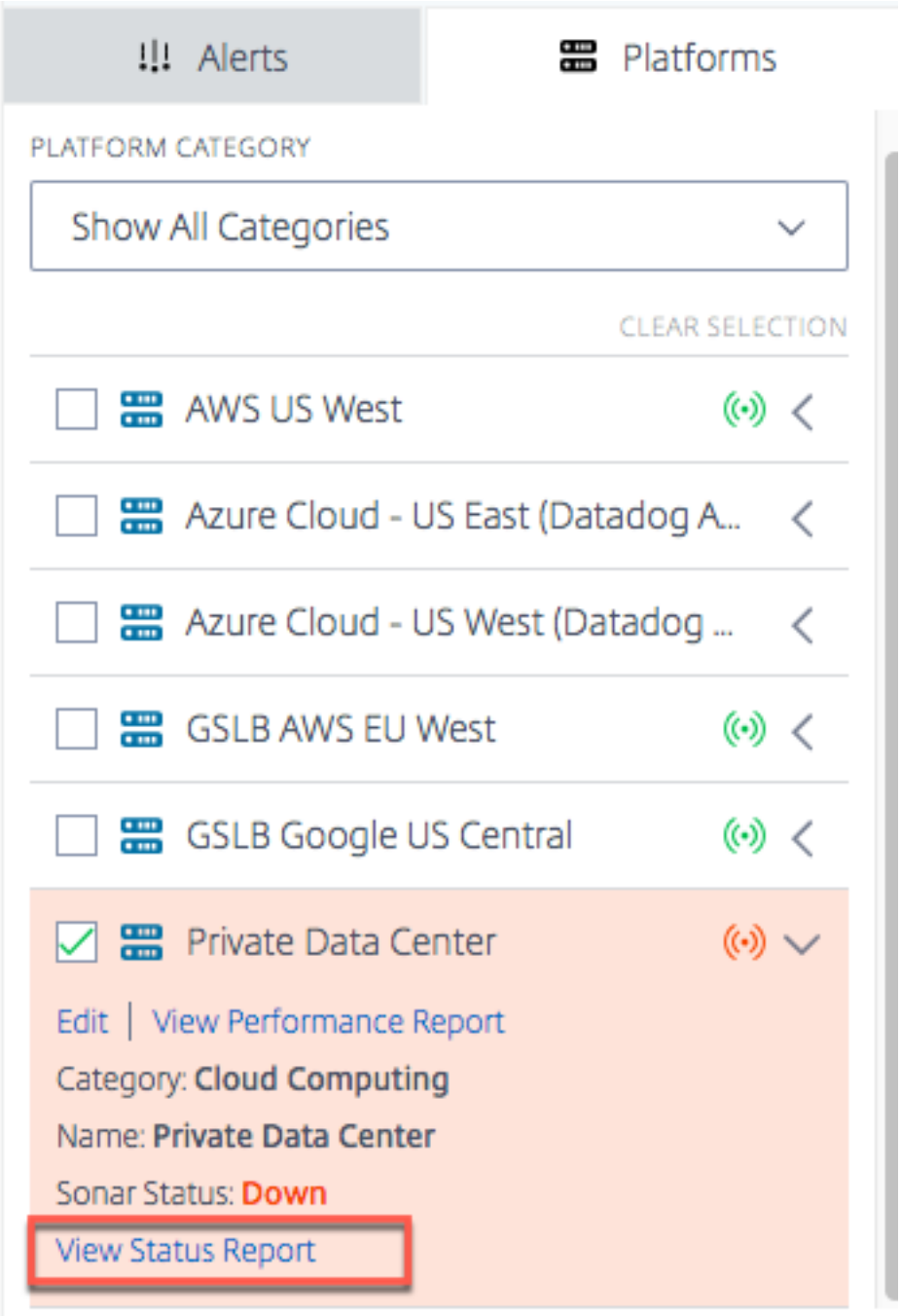
要查看已触发警报的特定平台的性能详细信息，请执行以下操作。

1. 单击地图上的平台图标或警报图标将其突出显示，然后选中右侧列表中的复选框。
2. 单击平台旁边的箭头或警报以展开它。
3. 单击“查看性能报告”链接可转到“Radar 性能报告”页面。

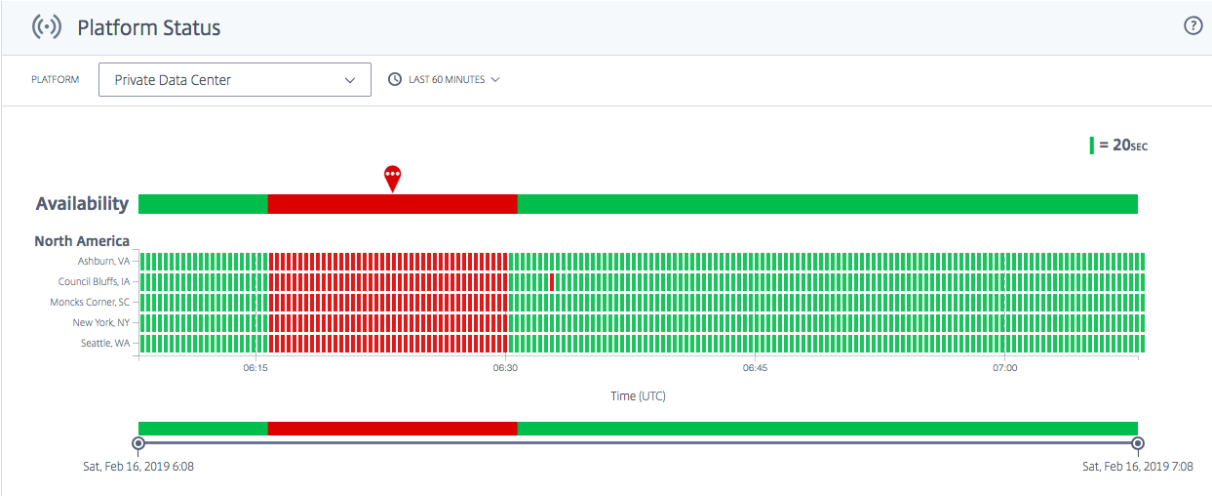


状态报告

对于综合监控警报，您可以通过展开平台来查看详细信息并单击查看状态报告来查看警报详细信息。



查看状态报告链接会将您带到 Sonar 平台状态页面，并根据实时综合监控检查结果提供您的平台运行状况的详细信息。



Radar

September 22, 2023

概述

Radar 是数据收集方法的支柱。Radar 使用嵌入在内容页面或应用程序提供商页面中的 JavaScript 脚本来收集有关数据中心或交付平台的性能和可用性的信息。

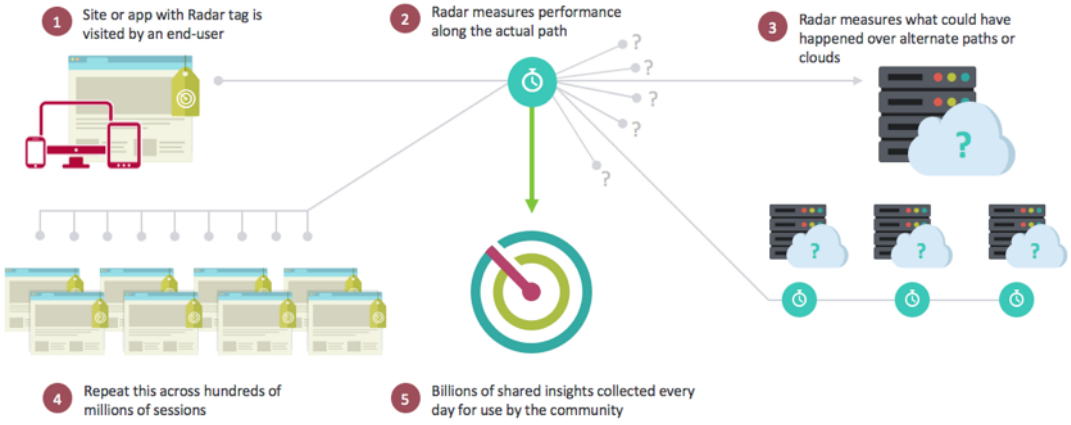
Radar 客户端是一个 JavaScript 应用程序，可在客户网页上和移动应用程序内运行。其核心用途是收集网络性能数据供 Openmix 用来推动智能路由决策，并提供可选插件以启用其他 NetScaler Intelligent Traffic Management 服务，例如页面加载时间、页面资源计时和视频播放指标。

Radar 客户端功能齐全，但轻巧且不显眼。该客户端等待大多数页面资源下载完毕后才执行其大部分工作，并且所有网络通信都尽可能以异步方式执行。这些说明指定了在会话期间接下来要测量的平台，这些平台是从社区平台和特定于该社区成员的任何私有平台中挑选出来的。它们还指出了要执行的测量类型，其中可能包括可用性、往返时间、吞吐量或其他指标集合。

为了使其尽可能小，编译该 JavaScript 时使用了 Google Closure Compiler 的高级优化功能。高级可选功能以插件形式提供，供客户选择使用。

Radar 社区

Radar 采用独特的基于社区的方法，为全球最大的公共基础结构（从云计算和存储到内容和应用程序交付网络）的全球性能和可用性提供了无与伦比的透明度。使用 Radar，客户可以快速查明对每位访客而言性能最佳和最差的平台。



Radar 是互联网的第一个云监控合作社。成为社区成员意味着可以不受限制地访问我们的历史报告数据库，包括按提供商、国家/地区和网络进行的细分。

成为 Radar 社区成员还会获得一套丰富的工具，用于捕捉内部和外部内容交付基础结构提供的服务级别。Radar 的独特之处在于能够利用您的网站访客来评估他们将从企业当前未使用的平台上获得的体验。同样的方法可用于在云平台的整个生命周期中对其进行客观评估，包括相对于 SLA 对其性能进行持续评估。

通过向您的网页添加简单的 JavaScript 标记或向移动应用程序添加 SDK，客户可以将每位访客变成虚拟的“测试代理”。Radar 通过以下方式触发基于设备的测量：下载参考对象，并比较网站或 Web 应用程序的实际最终用户所看到的内部和外部基础结构、数据中心、交付网络和云平台。

参与的主要好处

Radar 通过其监控和数据收集方法解决了多个 Web 交付难题。加入 Radar 社区的主要好处是：

- 大规模的测试环境，每个网络的最终用户分布在每个位置（到目前为止，已识别的网络已超过 42,000 个）。
- 在试用前获得有关服务提供商的重要信息，以便做出更明智的决策。
- 透明地了解当前提供商的表现，以及他们在您有用户和没有用户的地理区域的行为。
- 重点关注对网络和移动用户有真正影响的指标（性能、可用性和 QoS）。
- 全球（190 多个国家/地区）可以不受限制地查看国家、网络、区域和州/省/市/自治区级别的信息。
- 真实、无偏见的数据，通过利用最终用户，Radar 数据是“真实世界”的信息，而不是合成的测试或最佳猜测。
- 所有用户都不一样：可以了解不同的计算机、连接和设备。
- 可以了解实际页面的性能。

基准

ITM Radar 提供了 3 个主要基准：

- 社区基准
- 私有基准

- 页面加载基准

CDN、云和数据中心的社区基准

社区测量是通过众包模型获得的，该模型为客户提供了全球地理和逻辑层面的供应商绩效和可用性视图。通过社区衡量，可以对最终用户的供应商体验质量进行比较，并允许在评估供应商和供应商的内容和应用程序分发时进行“假设”分析。通过使用众包模型，ITM 客户在评估和监控供应商绩效时获得了更高级别的数据粒度和质量，从而受益，即使在客户可能没有高密度用户或根本没有任何用户的地方也是如此。

测量本身使用位于不同云和 CDN 供应商的一组标准对象，最终用户在内容所有者的网站或应用程序上执行 Radar JavaScript 客户端或移动 SDK 逻辑时会下载这些对象。

然后，以下指标将被报告给 ITM，并显示在门户或 API 报告界面中：

- 可用性—对象是否加载。
- 响应时间—建立连接的所有干扰信息完成后，服务器需要多长时间来响应后续请求。这是从浏览器到提供程序的 TCP 往返时间 (RTT) 的近似值。
- 吞吐量—这是连接的数据速率，以千比特/每秒为单位，基于一个 100 KB 对象的检索进行测量。

私有基准

作为 Radar 标记部署的一部分，ITM 使客户能够创建自己的“基准”测试，这些测试由客户的访客进行测量。这可能适用于数据中心或他们自己的 CDN 和云合同。与社区基准测量一样，提供了相同的指标–可用性、响应时间和吞吐量，使客户能够有效地评估现有的内容交付策略。

这些私有信息仅供客户使用，不会共享。
示例用途包括：

- 他们自己的数据中心架构
- 使用他们自己的测试对象或页面
- 使用他们自己与特定供应商或一组供应商设定的合同和帐户

Radar 页面加载基准

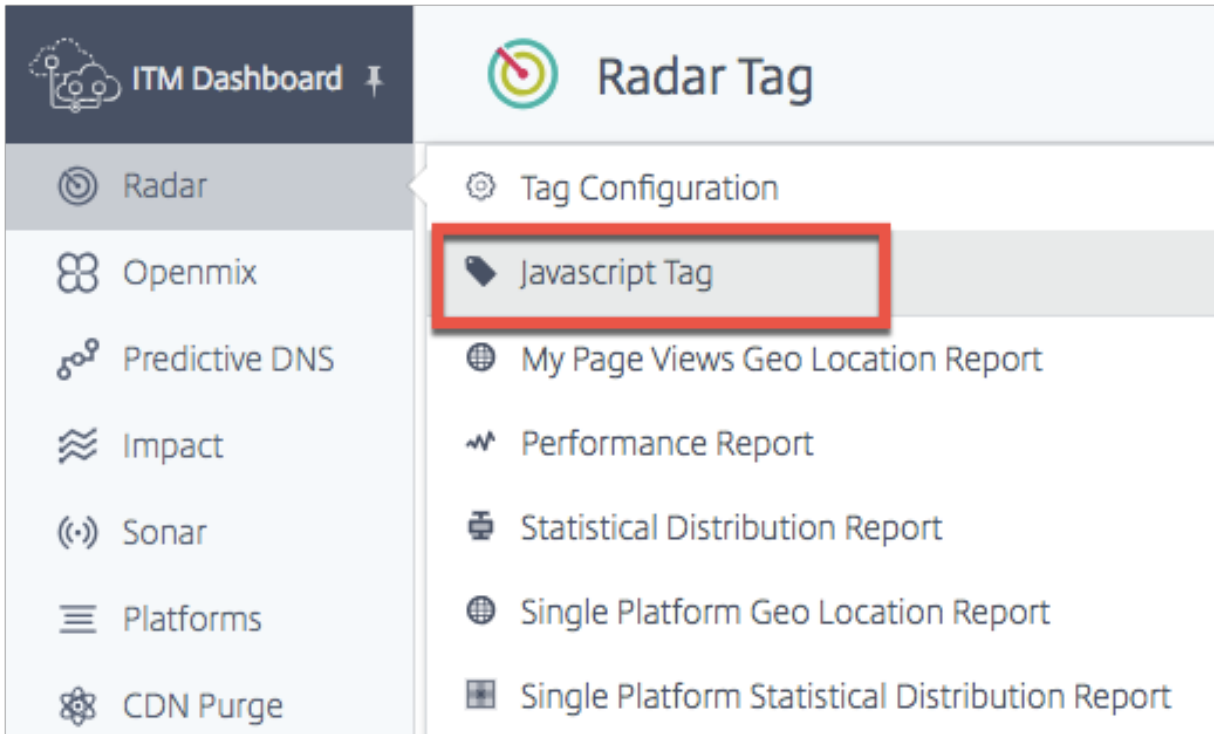
在 Radar 中，ITM 使客户能够详细了解实施了该标记的页面的下载性能。ITM 提供的信息使您能够查看实际最终用户在与您的网页交互时所体验到的性能。这些数据是通过许多新版本浏览器支持的导航计时 API 提供的。

Radar 标记

可以使用 JavaScript 代码片段来集成 Radar 标记。要导航到 **Radar** 标记页面，请执行以下操作：

1. 登录到 NetScaler Intelligent Traffic Management 门户。

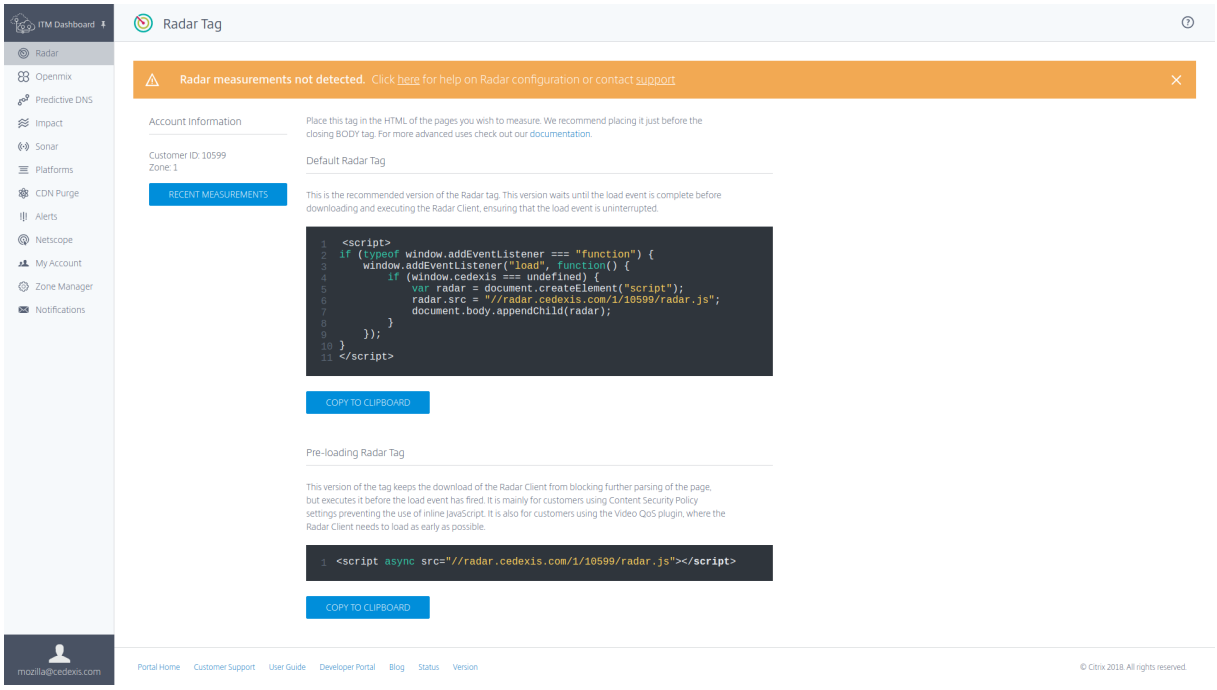
2. 从左侧导航菜单中，选择 **Radar > Javascript** 标记。



Radar 标记 页面随即打开。

如果您尚未配置 Radar 标记，则会在屏幕顶部看到一个橙色的水平条，告诉您未检测到 Radar 测量值。

如果此标记的配置不正确，也会出现此橙色条。



相反，如果 Radar 标记按预期工作，则您会看到一个绿色的水平条，告诉您已成功获得 Radar 测量值。

在此页面上，您可以选择适用于您的使用情况的标记版本并将其复制到剪贴板。

注意：请勿更改此 JavaScript 代码片段。该代码包含重要信息，如果更改这些信息，可能会导致意外或不可靠的行为。

集成 **Radar** 标记

集成 Radar 标记相当简单。您只需要将下面的 JavaScript 代码片段之一添加到你的站点标记中。将其放在您要测量的页面的 HTML 中。我们建议您将其放在页面底部的结束正文标记 </body> 之前。

默认 **Radar** 标记

这是建议使用的 Radar 标记版本。此版本会等到加载事件完成后再下载并执行 Radar 客户端，从而确保加载事件不被中断。

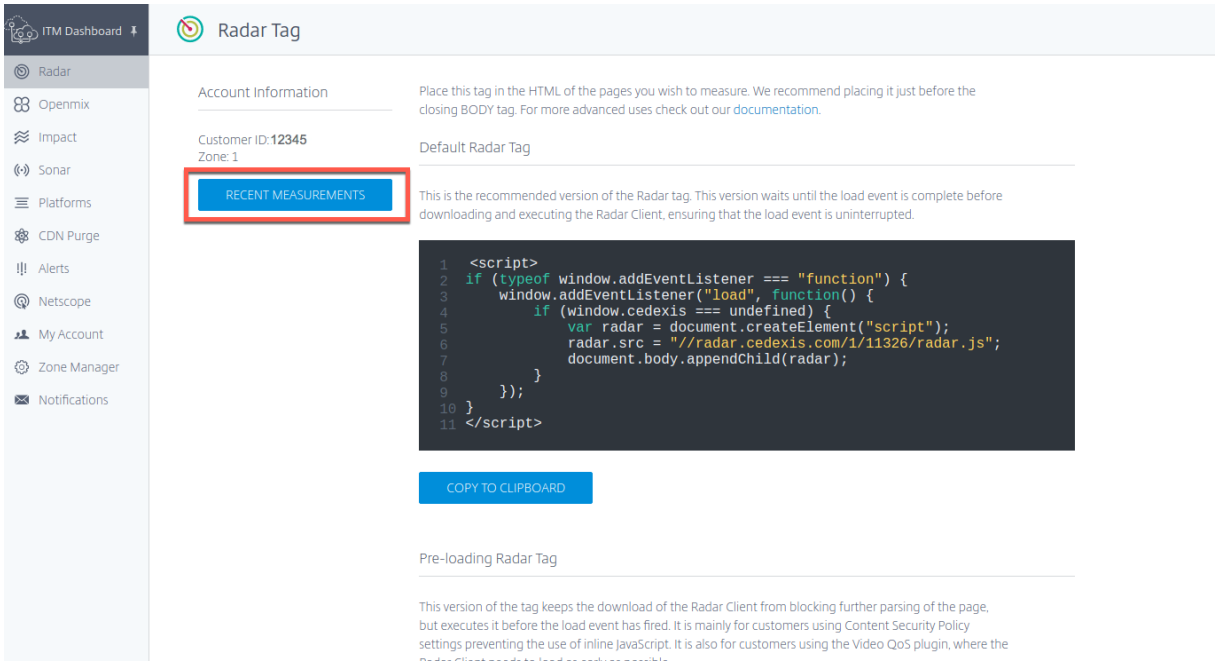
```
<script>
if (typeof window.addEventListener === "function") {

    window.addEventListener("load", function() {

        if (window.cedexis === undefined) {

            var radar = document.createElement("script");
            radar.src = "//radar.cedexis.com/1/54621/radar.js"; //
                replace with user specific value
            document.body.appendChild(radar);
         }

     }
 );
 }

</script>
<!--NeedCopy-->
```

此版本的标记可以防止 Radar 客户端的下载阻止页面的进一步解析，但会在加载事件触发之前执行该客户端。它主要用于使用的内容安全策略设置阻止使用内联 JavaScript 的客户。它也适用于使用视频 QoS 插件的客户，其中需要尽早加载 Radar 客户端。

```
<script src="//radar.cedexis.com/1/54621/radar.js" async></script>
<!--NeedCopy-->
```

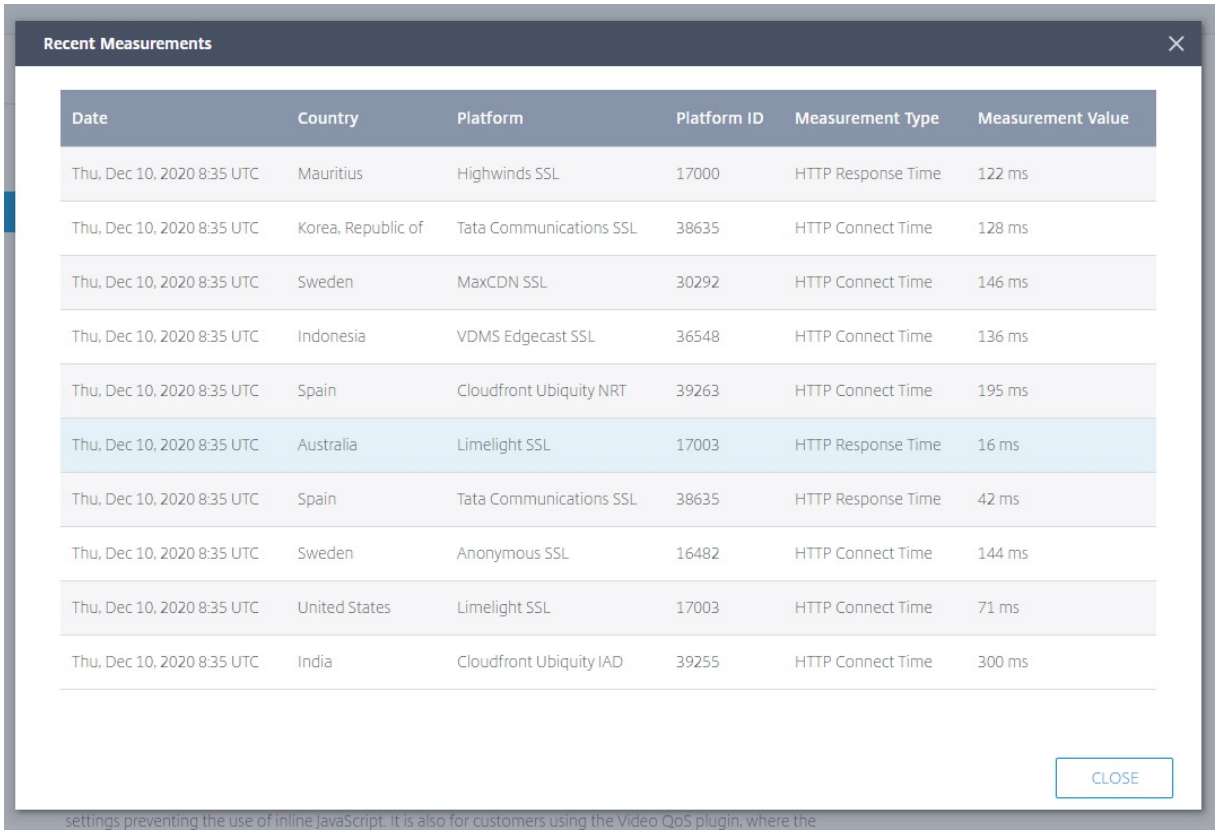
最近的测量

最近的测量表允许您查看使用 Radar 进行的最新测量。



单击最近的测量按钮。它为您提供以下信息：

- 进行测量的日期和时间 (UTC)。
- 进行测量的国家/地区。
- 用于进行测量的平台。
- 平台的 ID。
- 测量类型，即连接时间（以毫秒为单位）、响应时间（以毫秒为单位）或吞吐量（以千比特/每秒为单位）
- 以毫秒为单位（对于连接时间和响应时间）或以千比特/每秒为单位（对于吞吐量）的实际测量值。



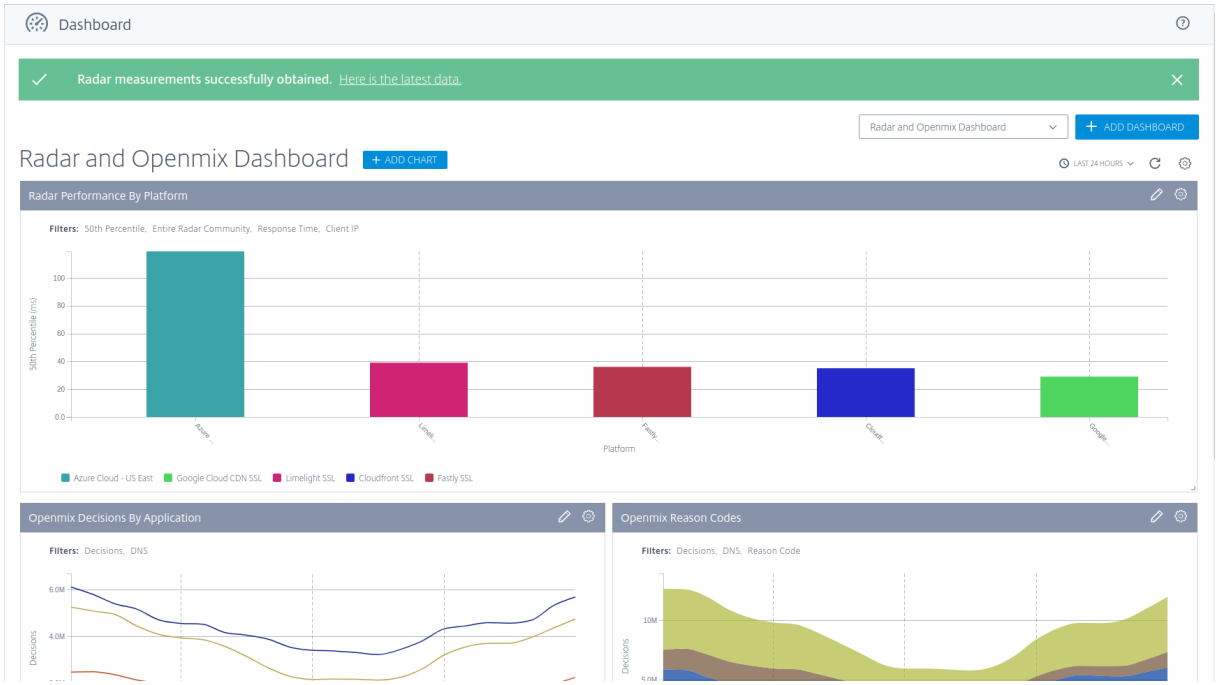
Recent Measurements

Date	Country	Platform	Platform ID	Measurement Type	Measurement Value
Thu, Dec 10, 2020 8:35 UTC	Mauritius	Highwinds SSL	17000	HTTP Response Time	122 ms
Thu, Dec 10, 2020 8:35 UTC	Korea, Republic of	Tata Communications SSL	38635	HTTP Connect Time	128 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	MaxCDN SSL	30292	HTTP Connect Time	146 ms
Thu, Dec 10, 2020 8:35 UTC	Indonesia	VDMS Edgecast SSL	36548	HTTP Connect Time	136 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Cloudfront Ubiquity NRT	39263	HTTP Connect Time	195 ms
Thu, Dec 10, 2020 8:35 UTC	Australia	Limelight SSL	17003	HTTP Response Time	16 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Tata Communications SSL	38635	HTTP Response Time	42 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	Anonymous SSL	16482	HTTP Connect Time	144 ms
Thu, Dec 10, 2020 8:35 UTC	United States	Limelight SSL	17003	HTTP Connect Time	71 ms
Thu, Dec 10, 2020 8:35 UTC	India	Cloudfront Ubiquity IAD	39255	HTTP Connect Time	300 ms

CLOSE

settings preventing the use of inline JavaScript. It is also for customers using the Video QoS plugin, where the

首次登录 ITM 门户时，Radar 测量栏也将出现在 Radar 仪表板页面中。



与移动应用程序的集成

与移动应用程序的集成是使用运行该 JavaScript 客户端的隐藏 Web 视图的包装器实现的。这样可以确保在浏览器和移动应用程序中收集的数据是一致的。

将 **Radar** 与 **iOS** 应用程序集成的说明
以下 GitHub 存储库包含用于将 Radar 与 iOS 应用程序集成的包装器代码和分步说明：

iOS 版 Radar Runner

将 **Radar** 与 **Android** 集成的说明
Android Radar 是一个可以轻松地将 Radar 集成到 Android 应用程序中的客户端库。可以在这里找到它：

AndroidRadar 库

与 **NetScaler** 的集成

Radar 标记很重要，因为它为 Openmix 提供了测量值，使 Openmix 能够做出更好的路由决策。使用该标记的网页越多，路由决策就越好。

使用以下方法，您可以使用 NetScaler 将 Radar JavaScript 标记放入您的网页中。您可以使用命令行或 NetScaler 配置实用程序。

这些方法允许您在响应中注入 Radar 标记。要注入 Radar 标记，您需要使用重写。重写分为三个步骤：创建操作、配置策略和绑定策略。

命令行配置

命令行配置重写操作　模板：

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-pattern <expression> | -search <expression>] [-refineSearch <string>] [-comment <string>]
<!--NeedCopy-->
```

示例：

```
add rewrite action radar_tag action insert_after HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).BEFORE_STR("</body>") '"<script async src=\\"//radar.cedexis.com/1/<customer_id>/radar.js\\"></script>"'
<!--NeedCopy-->
```

注意：请在显示了 `<customer_id>` 的位置插入您自己的客户 ID

命令行配置重写策略　模板：


```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <string>] [-logAction <string>]
<!--NeedCopy-->
```

示例：

```
add rewrite policy radar_tag_policy HTTP.RES.HEADER("Content-Type").TO_LOWER.CONTAINS("text/html") radar_tag_action
<!--NeedCopy-->
```

命令行绑定重写策略　模板 1：

```
bind vpn vserver <name> [-policy <string> [-priority <positive_integer>] [-secondary] [-groupExtraction] [-gotoPriorityExpression <expression>] [-type <type>]] [-intranetApplication <string>] [-nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <netmask> ] [-staServer <URL> [-staAddressType ( IPV4 | IPV6 )]] [-appController <URL>] [-sharefile <string>]
<!--NeedCopy-->
```

示例 1：

```
bind vpn vserver <name_of_vserver> -policy radar_tag_policy -type RESPONSE -priority 10
<!--NeedCopy-->
```

模板 2：

```
bind cs vserver <name> (-lbvserver <string> | -vServer <string> | (-policyName <string> [-targetLBVserver <string>] [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] ) | (-domainName <string> [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>] [-cookieDomain <string>] [-cookieTimeout <mins>] [-sitedomainTTL <secs>]))
<!--NeedCopy-->
```

示例 2：

```
bind cs vserver <name_of_vserver> -policyName radar_tag_policy -type RESPONSE -priority 10
<!--NeedCopy-->
```

模板 3：

```
bind lb vserver <name>@ (<serviceName>@ [- weight <positive_integer>]) | <serviceGroupName>@ | (- policyName <string>@ [-priority <positive_integer>] [- gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] )
<!--NeedCopy-->
```


示例 3：

```
bind lb vserver <name_of_vserver> -policyName radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

模板 4：

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
    [-type <type>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

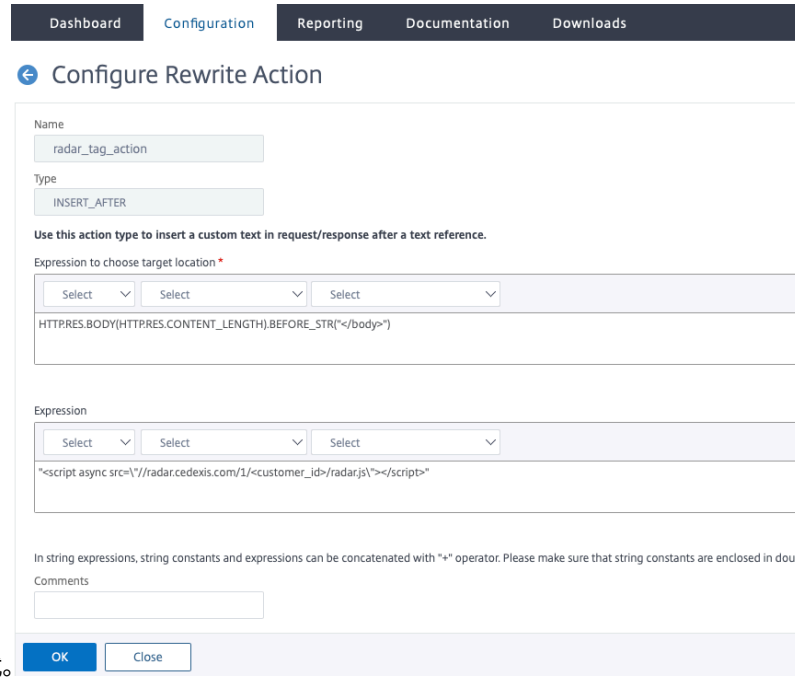
示例 4：

```
bind rewrite global radar_tag_policy 100 -type RES_DEFAULT
<!--NeedCopy-->
```

GUI 实用程序的配置

GUI 重写操作

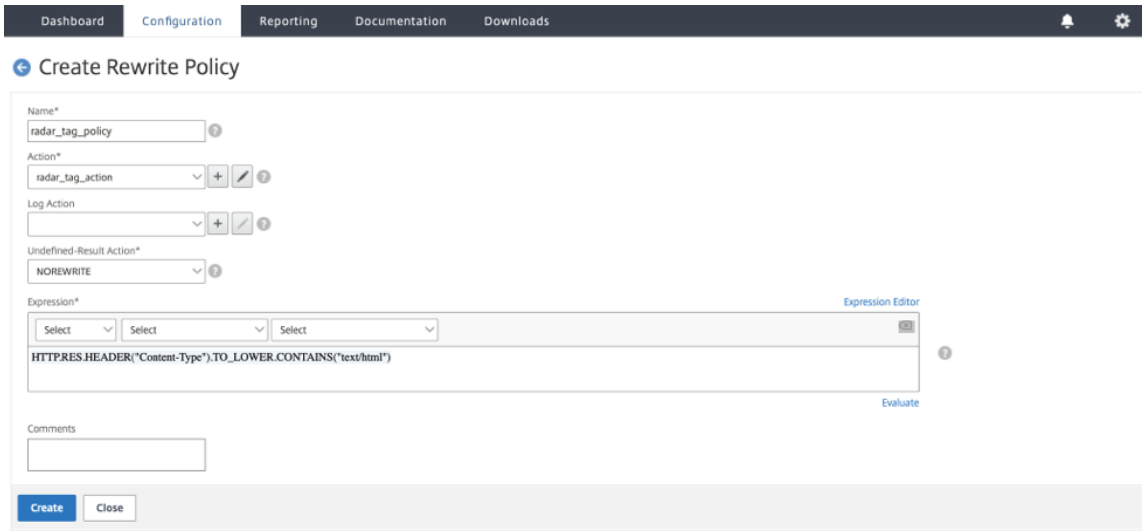
1. 从 **NetScaler** 配置页面上的左侧导航菜单中，导航到 **AppExpert** -> 重写 -> 重写操作
2. 选择添加按钮。



3. 在配置重写操作页面中，输入如示例所示的表达式。
4. 在 Radar 脚本中，在标有 `<customer_id>` 的空白处输入您的客户 ID。
5. 选择确定。您已完成重写操作的创建。

GUI 重写策略

1. 从 **NetScaler** 配置页面上的左侧导航菜单中，导航到 **AppExpert** -> 重写 -> 重写策略
2. 选择添加按钮。
3. 在配置重写策略页面上，输入如示例所示的表达式。

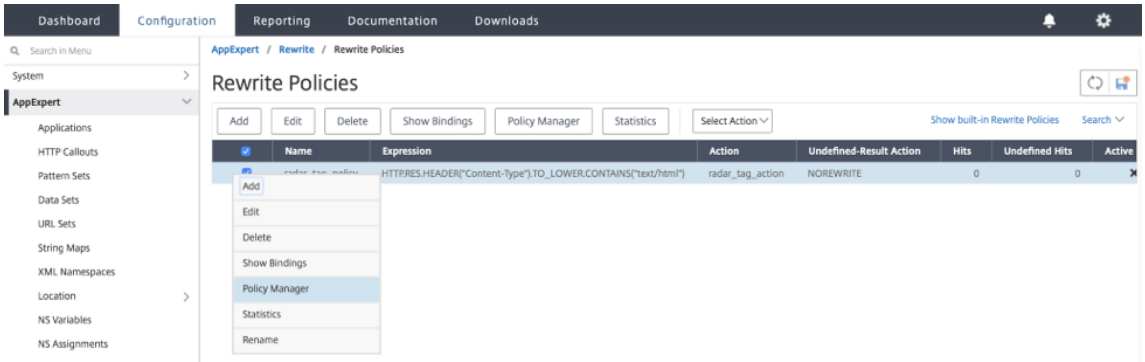


4. 单击创建。

您已完成重写策略的配置。

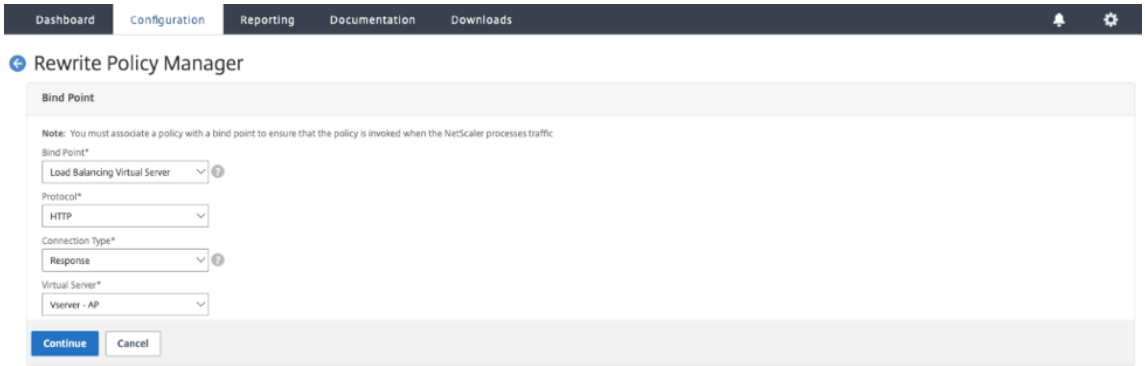
GUI 绑定重写策略　配置完策略后，最后一步是使用策略管理器来绑定策略。

1. 转至重写策略页面。
2. 选择您为 Radar 标记创建的重写策略。
3. 转至策略管理器。

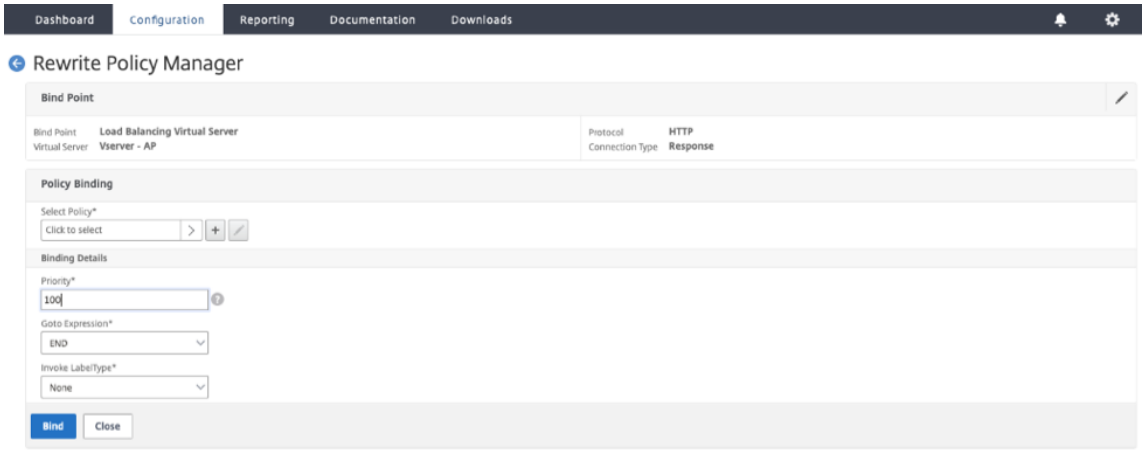


4. 在策略管理器页面中，您可以通过执行以下操作来绑定策略。
   - 对于绑定端口，您可以选择覆盖全局、**VPN** 虚拟服务器、内容交换虚拟服务器或负载平衡虚拟服务器。
   - 对于协议，请选择 **HTTP**。

- 在连接类型中选择响应。
- 对于虚拟服务器，请使用您自己的虚拟服务器名称。



- 单击继续。
- 在下一页上，选择您之前创建的重写策略。
- 添加绑定详细信息。
- 单击绑定。

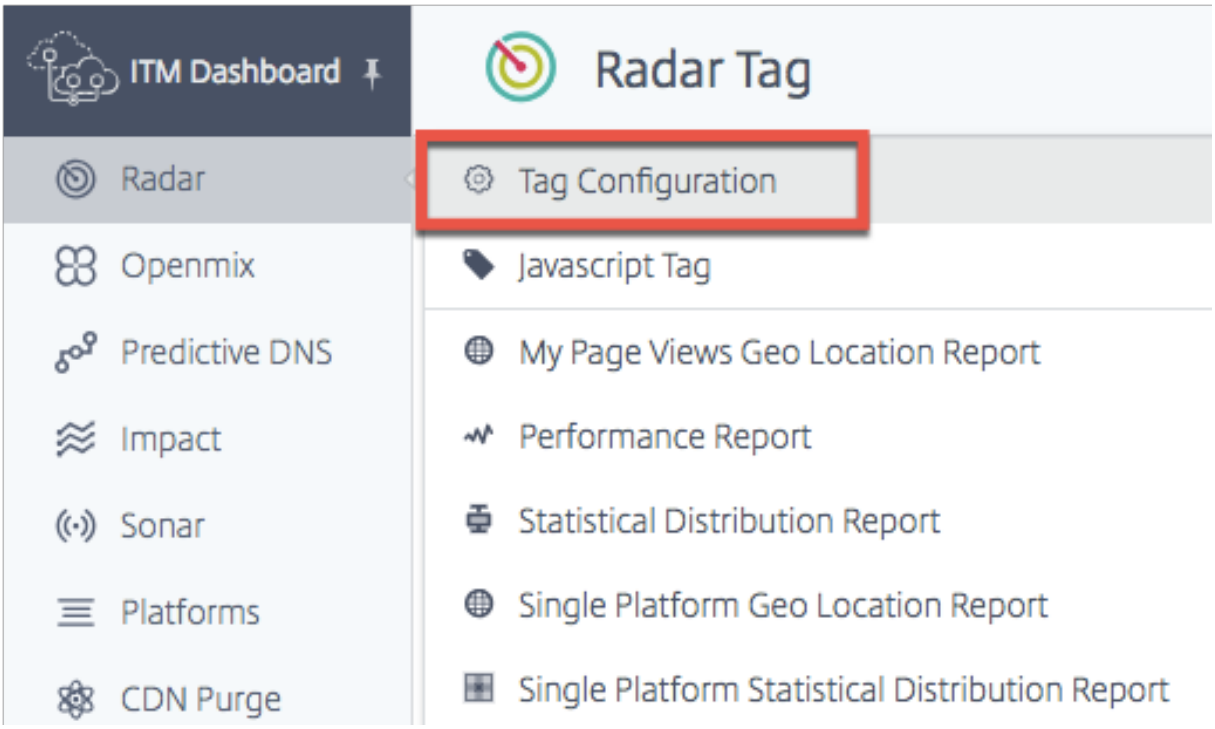


使用上述方法，您可以将 Radar 标记插入到您的网页中。但是，必须注意的是，这是一个基本的实现。可以进行进一步的过滤，以更好地控制已实施了该标记的页面。

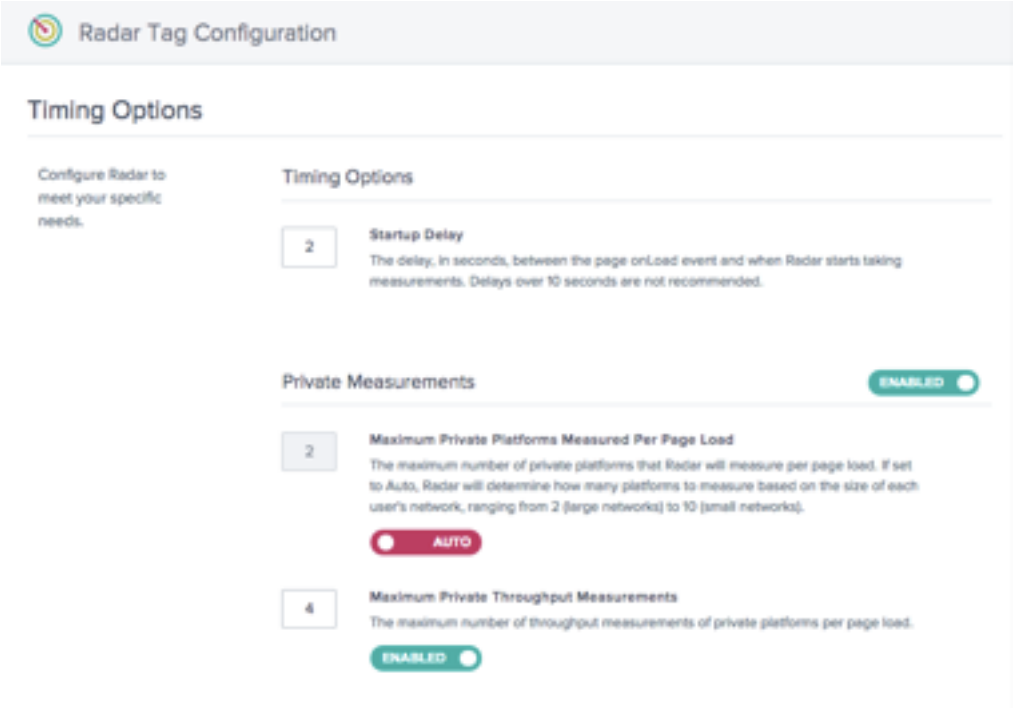
Radar 标记配置

您可以在 **Radar** 标记配置页面上配置 Radar。

1. 登录到 NetScaler Intelligent Traffic Management 门户。
2. 从左侧导航菜单中，选择 **Radar >** 标记配置。



“Radar 标记配置”页面随即打开。在这里，您可以设置各种选项来自定义 Radar 测量。您可以对 Radar JavaScript 的参数进行自定义来调整计时和延迟元素；最终用户为社区和私有测量完成的测试数量；以及用于测量可用性的超时值，等等



下表提供的信息介绍了各个配置选项的用途以及每个选项的默认设置。进行更改时，请务必单击屏幕底部的更新 **Radar** 设置以应用更改。

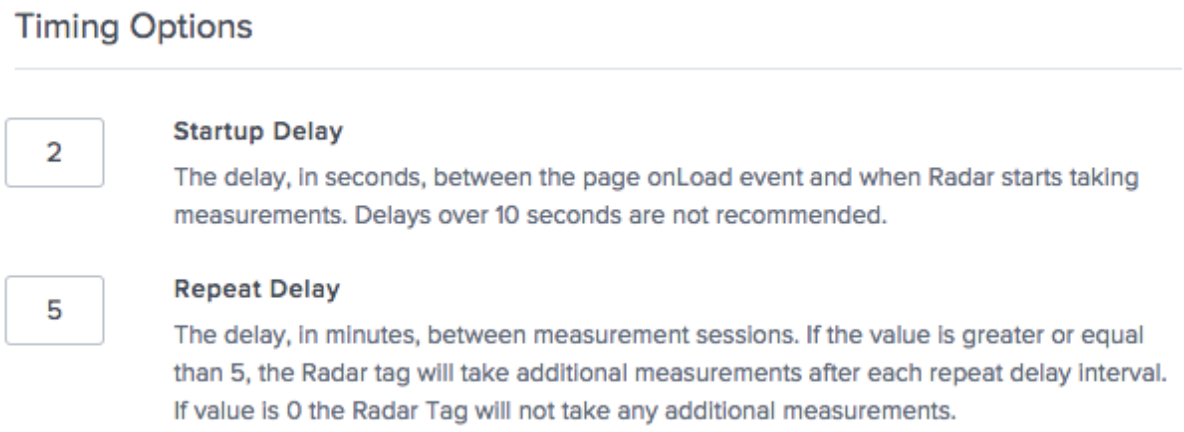
功能	参数	说明	默认设置
计时选项	启动延迟	页面 onLoad 事件与 Radar 开始记录导航计时数据之间的延迟（以秒为单位）。	2 秒
	重复延迟	测量会话之间的延迟（以分钟为单位）。如果该值大于或等于 5，则 Radar 标记在每个重复延迟间隔后将进行更多测量。如果该值为 0，则 Radar 标记将不会进行任何额外测量。	5 分钟
协议选项	始终允许私人 HTTPS 测量	允许 Radar 客户端进行 HTTPS 测量，甚至是从 HTTP 网站进行测量。	对具有与 Radar 客户端运行的页面匹配的 URL 协议的平台进行测量。
	允许对 HTTPS 连接进行私有 HTTP 测量。	允许 Radar 客户端从 HTTPS 网站进行 HTTP 测量。	对具有与 Radar 客户端运行的页面匹配的 URL 协议的平台进行测量。
采样率	Radar 采样率	激活 Radar 标签以进行测量的页面的百分比。	已禁用
私有测量	每次页面加载的最大私有测量数	Radar 将测量的每页加载量的最大私有平台数量。**	自动 *
	最大私有吞吐量测量数	每页加载私有平台的最大吞吐量测量数量。**	4
社区测量	每页加载的最大社区测量	Radar 将测量每页加载量的最大社区平台数量。**	自动 *
	最大社区吞吐量测量	每页加载社区平台的最大吞吐量测量数量。**	4

*“自动”表示 NetScaler Intelligent Traffic Management 根据最终用户的位置确定必须为某个会话测量多少个平台。对于数据稀疏的小型网络，我们尝试在每个会话中测量更多的平台，而对于数据密集的大型网络，则无需这样做。

** 这是为每个会话尝试的最大测量次数。例如，Radar 可以在每个会话中测量 4 个私有平台，所有这些平台都配置为同时测量 RTT 和吞吐量。但是，如果“最大私有吞吐量测量数”设置为 2，则在测量前 2 个私有平台后，客户端将停止吞吐量测量。对于最后两个平台，它将只测量 RTT。

计时选项允许您设置 Radar 在开始测量之前必须等待的时间长度。

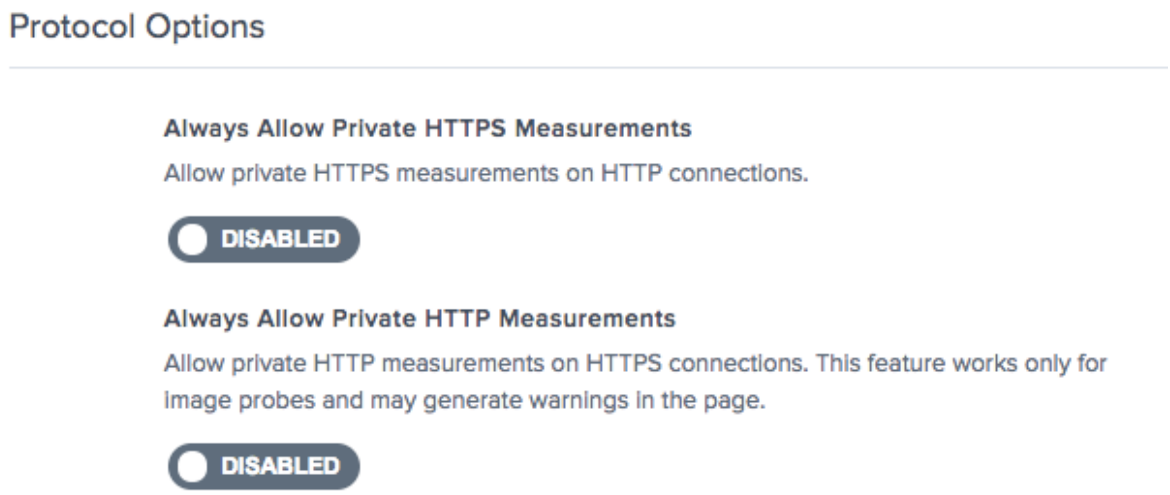
注意：启动延迟以秒为单位，而重复延迟以分钟为单位。



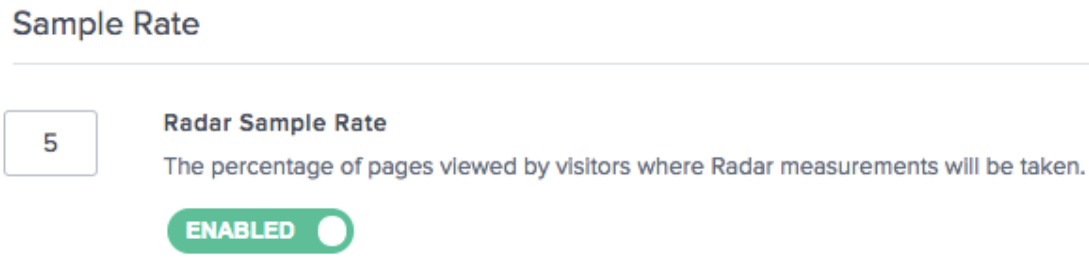
协议选项

通常，Radar 客户端仅测量符合以下条件的平台：其 URL 的协议与运行该客户端的页面的协议相匹配的平台。这些选项允许您在私有平台上覆盖该行为。例如，启用“始终允许私有 HTTPS 测量”允许客户端测量 `http://example.com` 中的 `https://myprovider.com/r20.png`，而“始终允许私有 HTTP 测量”则允许客户端测量 `https://example.com` 中的 `http://myprovider.com/r20.png`。

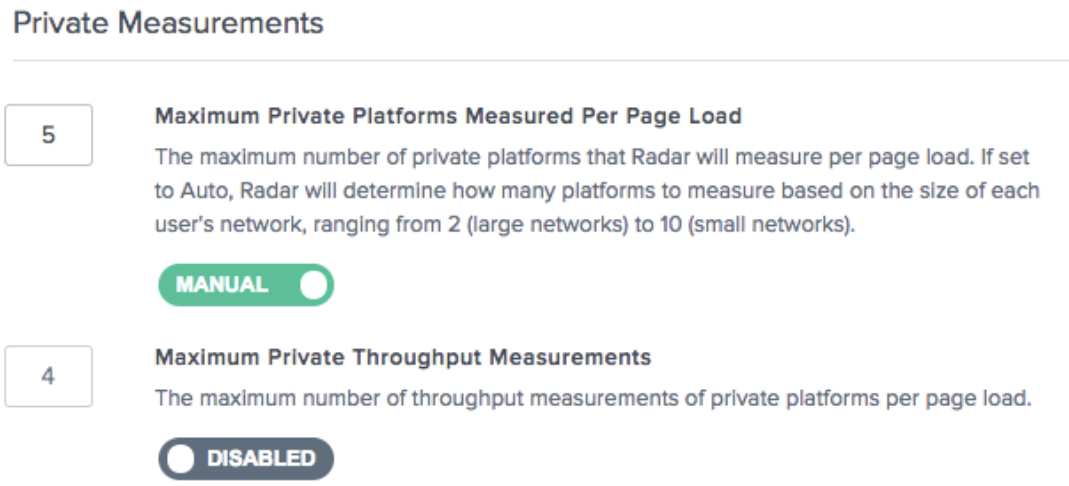
除极端用例外，通常必须避免使用这些选项。确保获得足够的私有测量密度的最佳方法是将您的平台配置为测量您在生产中实际使用的平台和协议（仅此而已），并在尽可能多的生产页面上部署 Radar 标记。我们有时将其称为“将 Radar 放在需要的地方。”



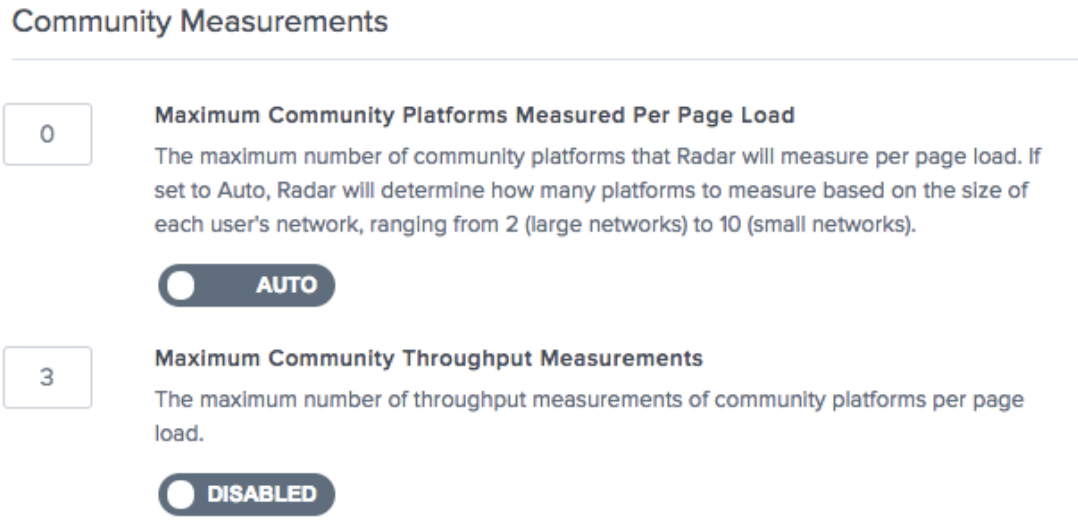
使用采样率，您可以设置要从中收集测量值的网页（被用户查看的）所占百分比。例如，如果您的网站每天的页面查看次数为 100,000，并且您设置了 5%的采样率，那么 Radar 将仅从 100,000 次页面查看的 5%中收集测量值。



私有测量　这些设置适用于您的私有平台的测量。私有平台是您在平台部分中设置的用于测量特定 CDN、云提供商和基础结构的其他部分的平台。有关更多信息，请参阅平台部分。



此选项允许您配置在向社区提供信息时 Radar 的行为。

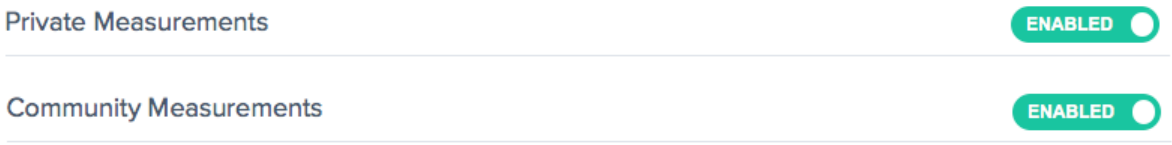


关闭 **Radar** 测试

如果在发生意外情况时需要快速关闭 Radar 测量，则可以在门户中这样做，以避免紧急更改您的站点的代码。

在“Radar 标记配置”页面上，通过将启用开关按钮切换为“禁用”，关闭私有测量、社区测量或关闭两者。

单击保存 **Radar** 配置以确认更改。这些更改可能需要花费一两分钟进行传播，之后 Radar 测量就会停止。



Radar 客户端方法

客户端行为的一个基本维度是会话。客户端发送的所有数据都与会话相关联。会话是通过调用 NetScaler ITM 服务器（称为初始化请求）来创建的。会话过期相当快，这有助于确保只接受有效的 Radar 数据。由于此特征，Radar 测量始终是分批进行的，这些批次与其会话事务 ID 相关联，我们经常提及“Radar 会话”来描述与之关联的测量。

Radar 会话

Radar 会话是客户端执行的主要工作单元。它包括向 NetScaler ITM 服务器发送请求来获取客户配置和要测量的一组平台，然后请求测量这些平台并报告结果。这些操作以异步和序列化的方式进行，因此一次只发生一个请求。一个典型的会话在 10 秒内完成。

探测类型

客户端发送的每份报告都有一个关联的探测类型，它告诉系统这是什么类型的测量以及如何处理它。它还指出了要执行的测量类型，其中可能包括可用性、往返时间、吞吐量或其他指标集合。

可用性与性能探测（例如往返时间和吞吐量）之间存在着重要的关系。在任何特定的测量会话中，始终会首先测量特定资源的可用性。只有当可用性测量成功时，才可以在同一会话中对同一资源进行其他性能测量。

如果速度特别慢的网络出现可用性中断，这可能导致包括该网络的报告的总体性能实际上会提高。这只是一个报告非自然信号，因为 NetScaler Intelligent Traffic Management 始终使用最精细的、特定于网络的性能数据进行实时决策。

可用性　可用性也称为冷启动探测，旨在允许服务对其缓存进行预热。尽管有一个与此探测关联的测量值。我们使用可用性探测来确定提供程序是否可用。

如果平台未配置为执行冷启动探测，我们会使用 RTT 探测的结果代替冷启动报告来提供可用性指标。

类似地，对于测量站点加速服务的动态对象，客户端会将小型测试对象下载一次并报告冷启动和响应时间的测量值。

测试对象	定义
标准	使用资源计时时间戳：responseStart - requestStart
动态	使用资源计时时间戳：responseEnd - domainLookupStart

RTT

测试对象	时间间隔	API	说明
标准	responseStart - requestStart	资源计时	为响应 HTTP 请求而返回单个数据包的时间。
动态	responseEnd - domainLookupStart	资源计时	为请求提供服务的时间，包括 DNS 查询时间、连接时间和响应时间。

吞吐量

测试对象	时间间隔	API	说明
标准	文件大小（千字节）* 8 / (responseEnd - requestStart)	资源计时	基于大型测试对象下载为整个请求和响应测量到的吞吐量（千比特/每秒）。
动态	文件大小（千字节）* 8 / (responseEnd - domainLookupStart)	资源计时	基于大型测试对象下载为整个请求和响应测量到的吞吐量（千比特/每秒）。如果 RTT 测试对象已经下载，这通常不包括连接时间或 DNS 查询时间。

测试对象

测试对象是托管在平台上并由客户端下载以生成测量值的文件。本部分介绍了客户端支持的各种类型的测试对象。并非所有对象类型都适用于每个平台。

所需标头：

为了允许 JavaScript 访问资源计时 API 提供的低级别计时数据，需要使用 Timing-Allow-Origin 响应标头。推荐的设置是 `Timing-Allow-Origin: *`，这表示必须向在任何域上运行的 JavaScript 授予访问资源计时数据的权限。

标准　标准测试对象是媒体，客户端通过在图像对象上设置 `src` 属性来下载媒体。下载后，客户端使用资源计时 API 来收集性能数据。
这些测试对象必须与 Timing-Allow-Origin 响应标头一起提供。有关更多信息，请参阅 **Timing-Allow-Origin** 标头部分。

标准小型　标准小型测试对象是单像素图像文件，在客户端需要发出轻量级网络请求时使用。

标准小型测试对象用于以下用例：

- 非动态冷启动探测
- 非动态往返时间探测

标准大型　标准大型测试对象是一个 100KB 的图像文件，用于测量平台的吞吐量。

大型对象命名：要计算吞吐量，客户端需要知道测试对象的大小。客户端通过在文件名中的某处查找 KB 来确定文件名，例如 `r20-100KB.png`。客户可以测量不同大小的图像文件，只要名称以相同的方式包含文件大小即可，例如 `myimage-2048kb.jpg`。

动态　动态测试对象用于测量与站点加速服务相关的性能。
每个对象都是一个包含 JavaScript 的 HTML 文件，该 JavaScript 能够从导航计时 API 收集时间戳并将其发布到父级页面。客户端使用 iframe 下载测试对象并获取这些时间戳，并使用它来计算测量值。

安全与验证　该测试对象是一个 40KB 的对象。该测试对象的一项新功能是 HMAC（基于哈希的消息验证码），该功能基于查询参数和服务器可以访问的密钥提供。此 HMAC 随我们的测量值一起发回，这使我们能够验证 Radar 客户端是否能够访问测试对象，并且没有缓存任何内容。

动态测试对象与标准测试对象的区别：

对于标准 Radar 测量，我们尝试仅隔离与下载测试对象相关的主要请求活动，而对于站点加速服务，我们的目标是测量更多的活动。因此，还包括 DNS 查询和连接时间。
此外，动态测量旨在测量当请求被定向到服务源头（而不仅仅是边缘缓存）时的请求性能。

在门户中，您可以通过执行以下操作来选择此方法：

- 从左侧导航菜单中，转至平台。
- 单击页面右上角的添加平台图标。
- 转至私有平台 **>** 类别 **>** 动态内容。
- 在 **Radar** 测试对象对话框中，单击自定义探测复选框。
- 输入响应时间 URL，然后从对象类型 下拉列表中选择 **Web** 页面动态。

动态小型测试对象用于测量可用性和往返时间，并且对各项站点加速服务使用相同的探测。

iNav iNav 测试对象是一个静态 HTML 文件，其中包含能够执行许多任务的 JavaScript。客户端通过在用于将 HTML 文件加载到 iframe 的 URL 中包括查询字符串参数来指示要执行的任务。
iNav 测试对象支持以下用例：
iNav 冷启动
iNav 往返时间

iUNI iUNI 测试对象用于检测与平台的一组 Radar 测量关联的 UNI 值（另一种方法是 CORS AJAX，它不需要单独的测试对象）。

AJAX GET AJAX GET 方法通常可以用于客户想要测量的任何 URL，前提是该 URL 与 **Timing-Allow-Origin** 标头和相应的 **Access-Control-Allow-Origin** 标头一起提供。
在门户中，您可以通过执行以下操作来选择此方法：

- 从左侧导航菜单中，转至平台。
- 单击页面右上角的添加平台图标。
- 转至私有平台 **>** 类别 **>** 动态内容。
- 在 **Radar** 测试对象对话框中，单击自定义探测复选框。
- 输入响应时间，然后从对象类型下拉列表中选择 **AJAX (GET)**。

Timing-Allow-Origin 标头 为了允许 JavaScript 访问资源计时 API 提供的低级别计时数据，需要使用 Timing-Allow-Origin 响应标头。
推荐的设置是 `Timing-Allow-Origin: *`，这表示必须向在任何域上运行的 JavaScript 授予访问资源计时数据的权限。

Radar API

Radar 针对操作功能和数据检索功能都提供了 API。

- 操作 API —添加/编辑/删除 Radar 帐户，并提供通过 API 运行您的帐户的控制机制
- Radar 数据 API –ITM Radar 数据 API 提供 Radar 公共社区和私有测量数据的聚合。数据会持续更新，大约每 60 秒批处理一次，以供 API 检索。提供数据 API 是为了让客户将 Radar 数据集成到自己的报告和控制板中。对于每个平台，调用一次 API 可以为所有国家/地区和最多 30 个所关注的 ASN 提供 Radar 四分位值或测量平均值。

Radar 报告

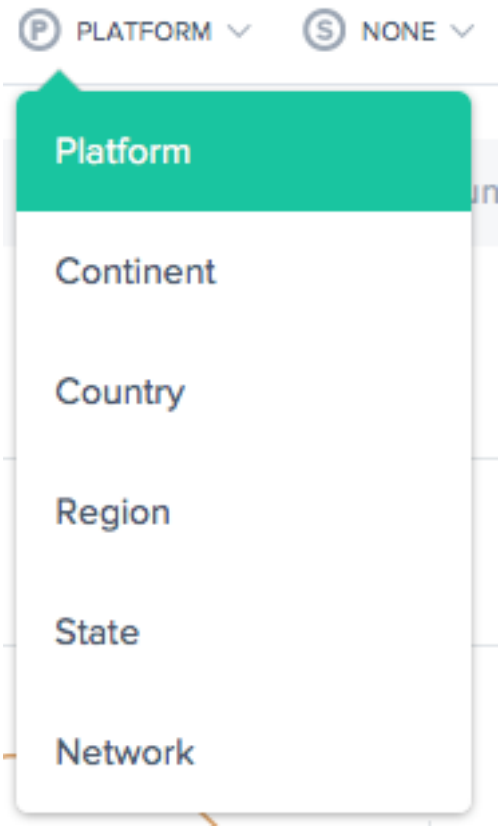
Radar 报告对通过 Radar 标记收集的动态数据提供了强大的洞察力。

Radar 成员可以访问通过直观的交互式图表提供的丰富数据集。收集的数据集包含了数十亿次测量的完整公共数据集，以及从客户的 Radar 标记或移动 SDK 部署中收集的私有数据，并且公共数据充当私有数据的背景。页面加载时间信息是通过客户自己的标记捕获的，有助于深入了解您的网站和移动应用程序最终用户的实际性能体验。

除了性能指标外，Radar 报告还能深入洞察最终用户受众的许多方面，包括：数量、地理位置、用户代理、操作系统类型以及他们使用您的网站或移动应用程序的时间。

每个报告的定义如下，但下面是所有报告的重要方面：

主要和次要维度

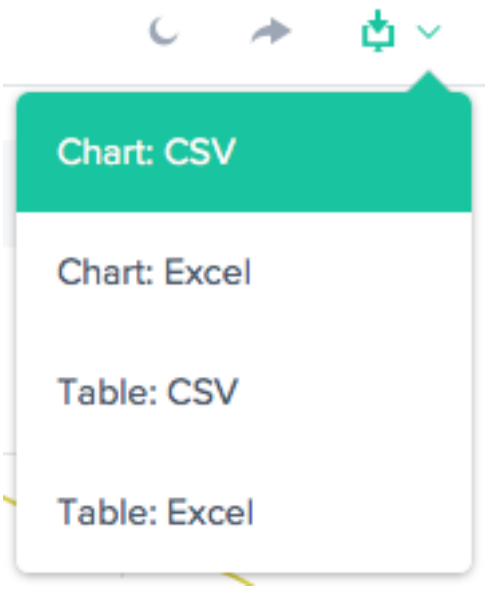


图表的主要维度是通过图表上方的选择列表选择的。使用它作为报告的强大透视视图。还可以选择次要维度来进一步优化报告。

可视化背景切换

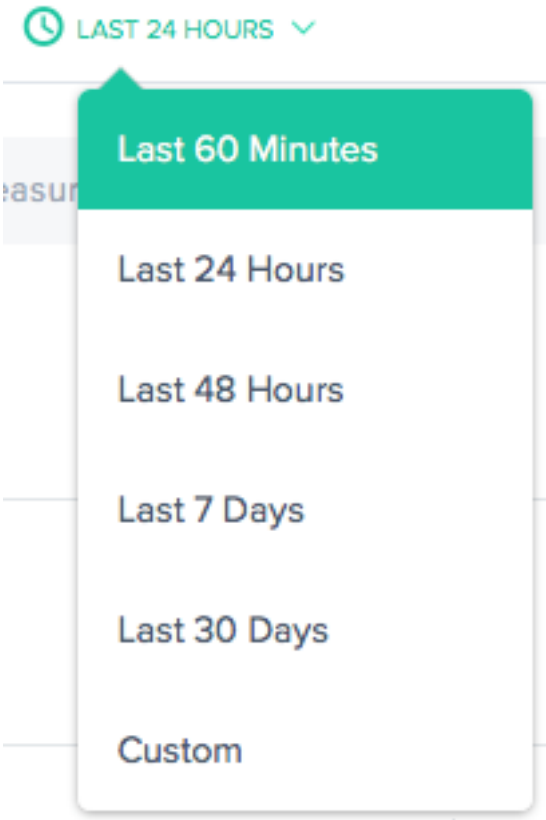
默认情况下，图表设置为白色背景。可以使用背景切换将背景切换为适合高对比度显示器的深色。

数据导出



此外，最终用户可以通过报告顶部的下载链接下载图表和表格数据。

过滤器：报告时间范围



可以为以下时间范围生成雷达报告：过去 60 分钟、过去 24 小时、过去 48 小时、过去 7 天、过去 30 天，或自定义范围。默认视图为“过去 24 小时”。

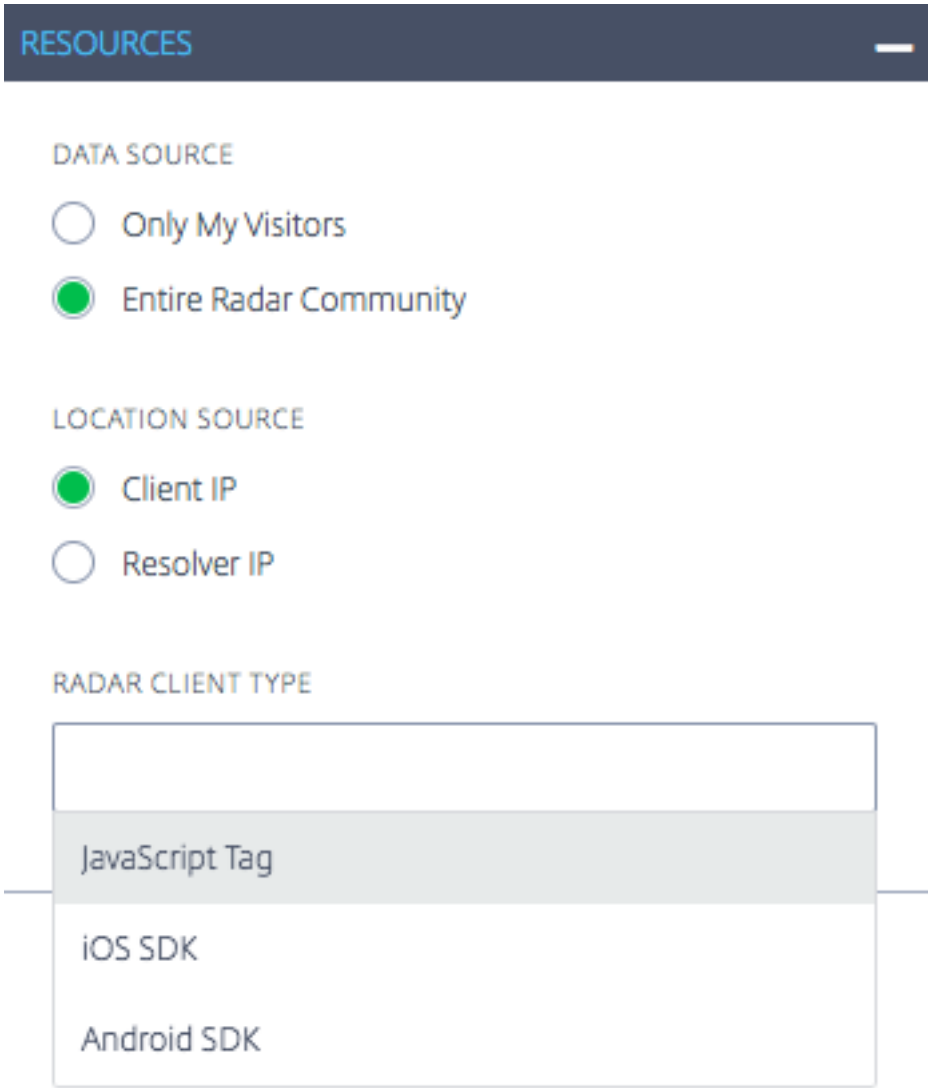
过滤器：平台和位置

适用于报告的过滤器根据数据情况可能略有不同。以下是最常见的：

- 平台—选择要包括的一个或多个平台（提供商）。
- 大陆—选择要包括的一个或多个大洲。
- 国家/地区—选择要包括的一个或多个国家/地区。
- 区域—选择一个或多个要包括的地理区域（如果适用）。
- 州—选择一个或多个要包括的地理州（如果适用）。
- 网络—选择要包括的一个或多个网络 (ASN)。

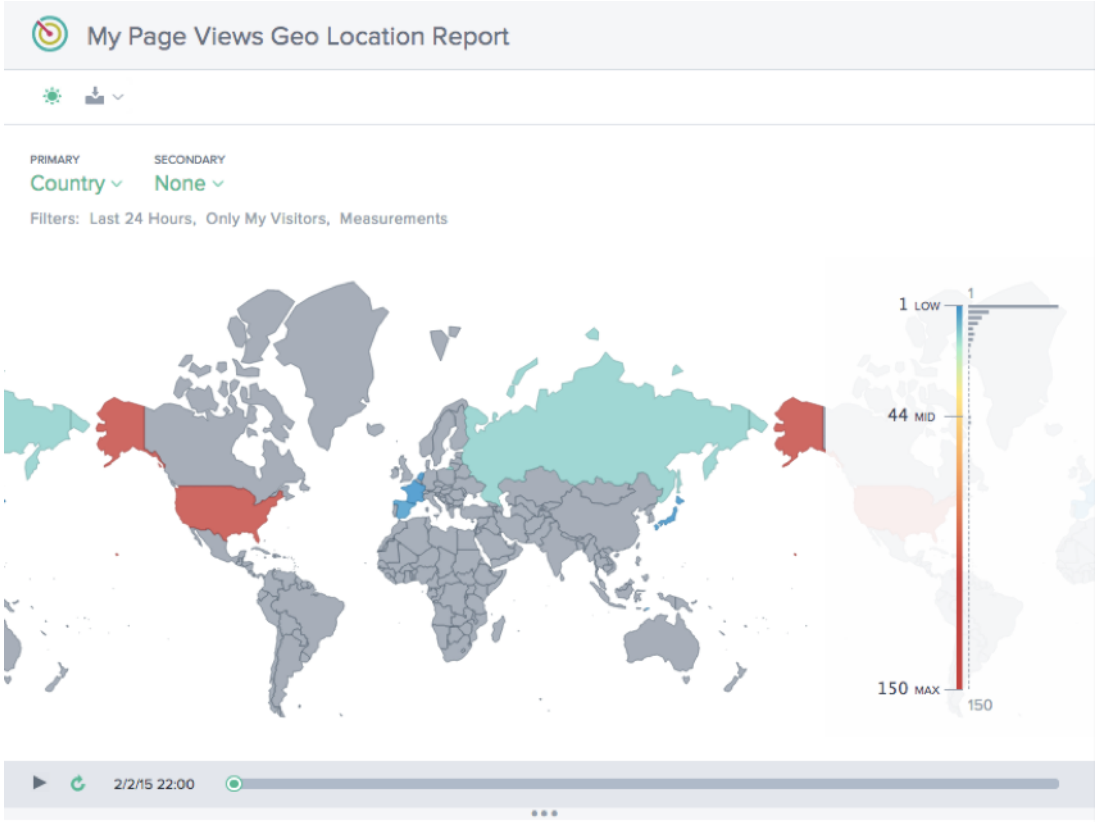
过滤器：资源

- 数据源 -包括来自整个 Radar 社区或仅来自您的网站访问者的数据。
- 位置来源 - 选择客户端 IP 或解析器 IP 作为您的位置来源。
- **Radar** 客户端类型 - 选择 JavaScript 标记、iOS SDK 或 Android SDK 作为 Radar 客户端类型。



我的页面查看地理位置报告

此报告显示每个国家/地区的页面查看量。通过选择图表底部的播放按钮，可以随着时间的推移查看此地图视图（基于为报告选择的时间范围）。

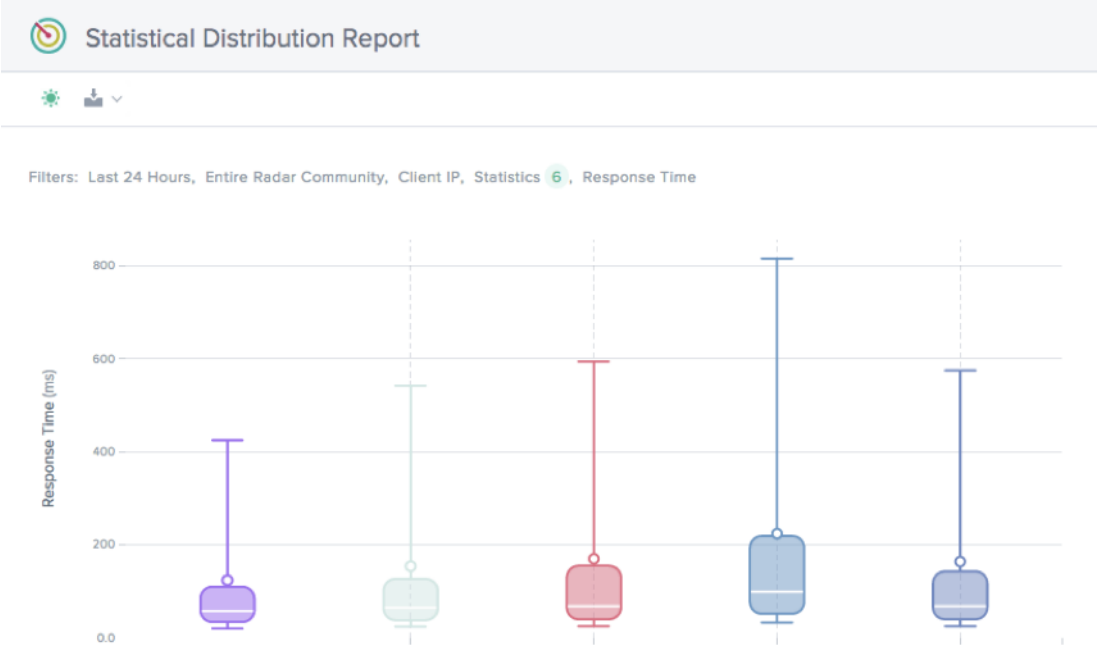


绩效报告

此报告显示所定义的每个平台的性能趋势。

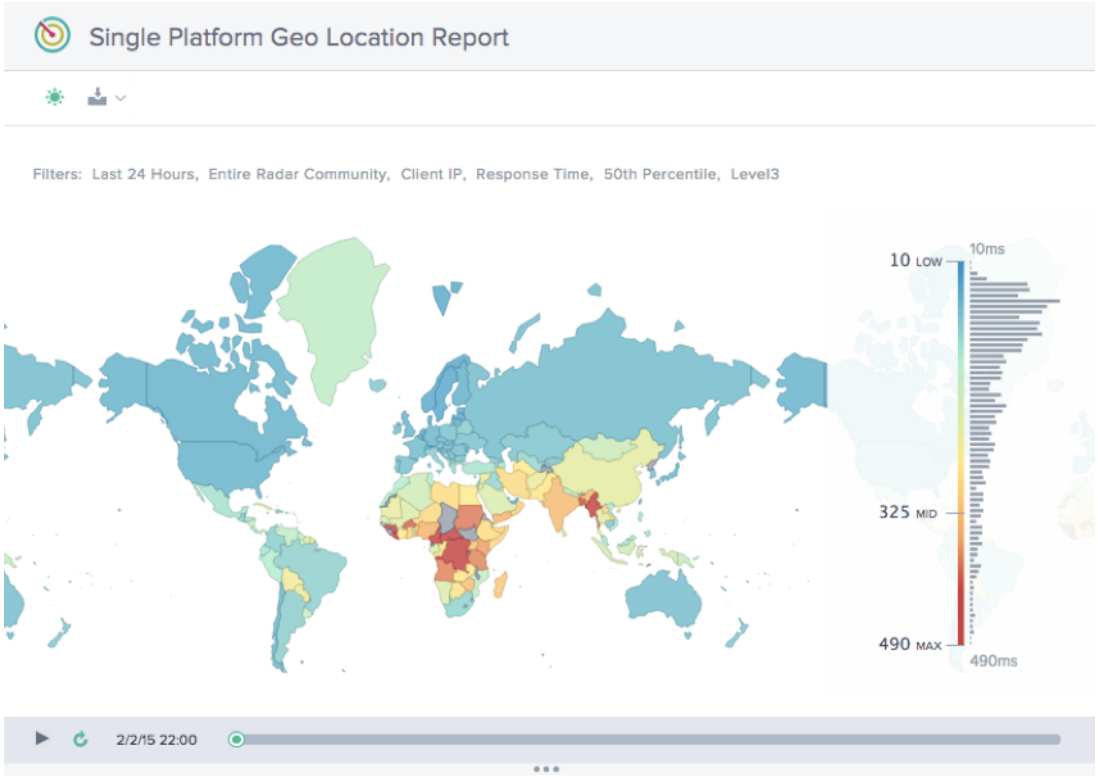
统计分布报告

此报告显示为帐户定义的每个平台的统计明细。



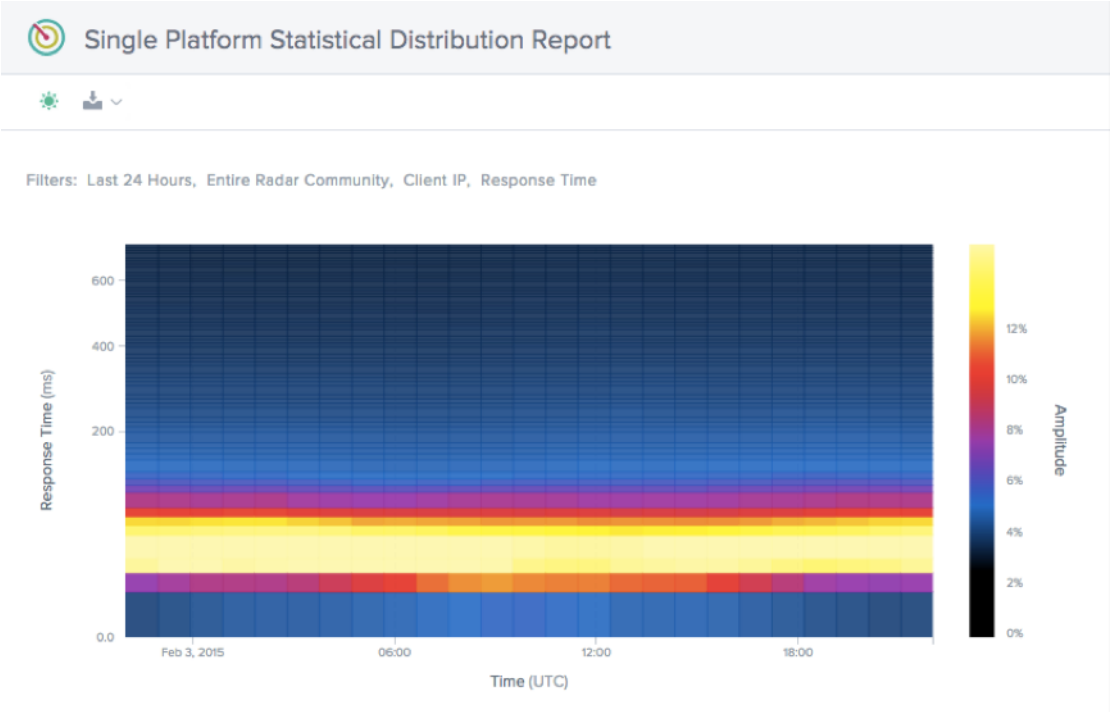
单平台地理位置报告

此报告一次为一个平台显示按国家/地区划分的 Radar 流量随时间推移的分布情况。



单平台统计分布报告

此报告按响应时间显示 Radar 流量随时间推移的分布情况。

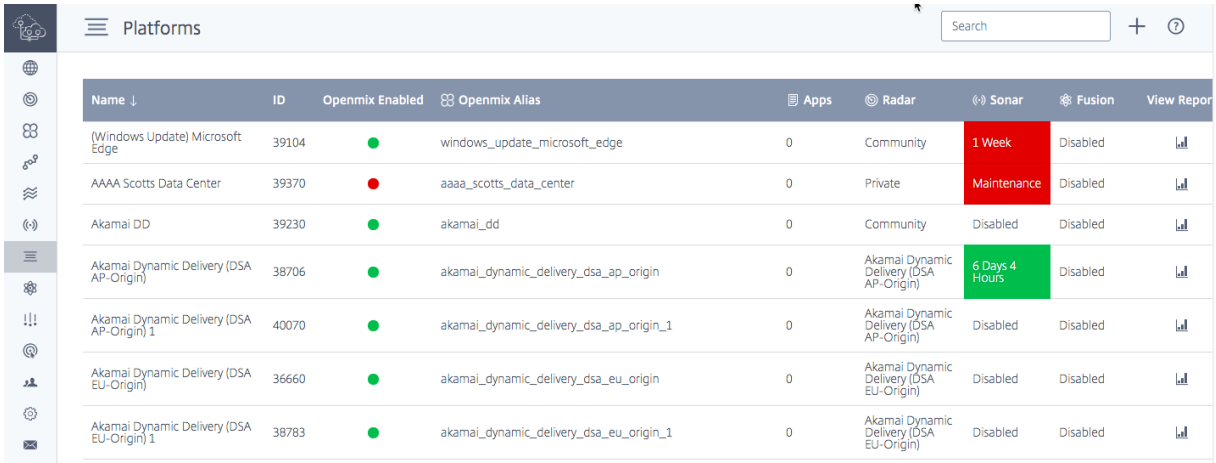


平台

June 7, 2021

“平台”页面是客户指定必须与 Openmix 一起监视和使用的 CDN、云、数据中心或其他终端点的位置。必须为要报告的每个路由终端点设置平台。如果使用适用于 GSLB 的 Openmix，平台通常表示 CDN、云区域或单个实例。

点击此菜单项后，客户会看到以下屏幕。



此屏幕显示了为报告、Radar 测量或 Sonar 和 Fusion 服务配置的所有平台的完整列表。

下表显示：

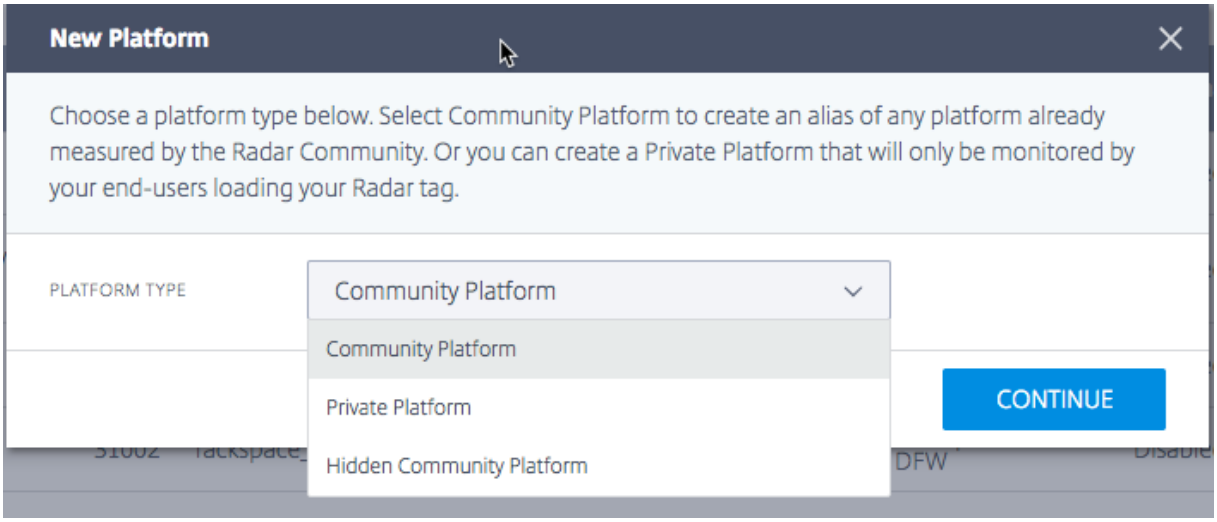
标题	说明
名称	平台的用户定义名称。
ID	为平台生成的 ID，用于 API 访问和报告。
Openmix 别名	从 Openmix 应用程序中引用平台的别名。
应用程序	使用该平台的 Openmix 应用程序的数量。
Radar	该平台是否设置为使用社区或私人 Radar 测量。
Sonar	Sonar 是否在此平台上激活。
Fusion	是否在此平台上激活 Fusion。

创建平台

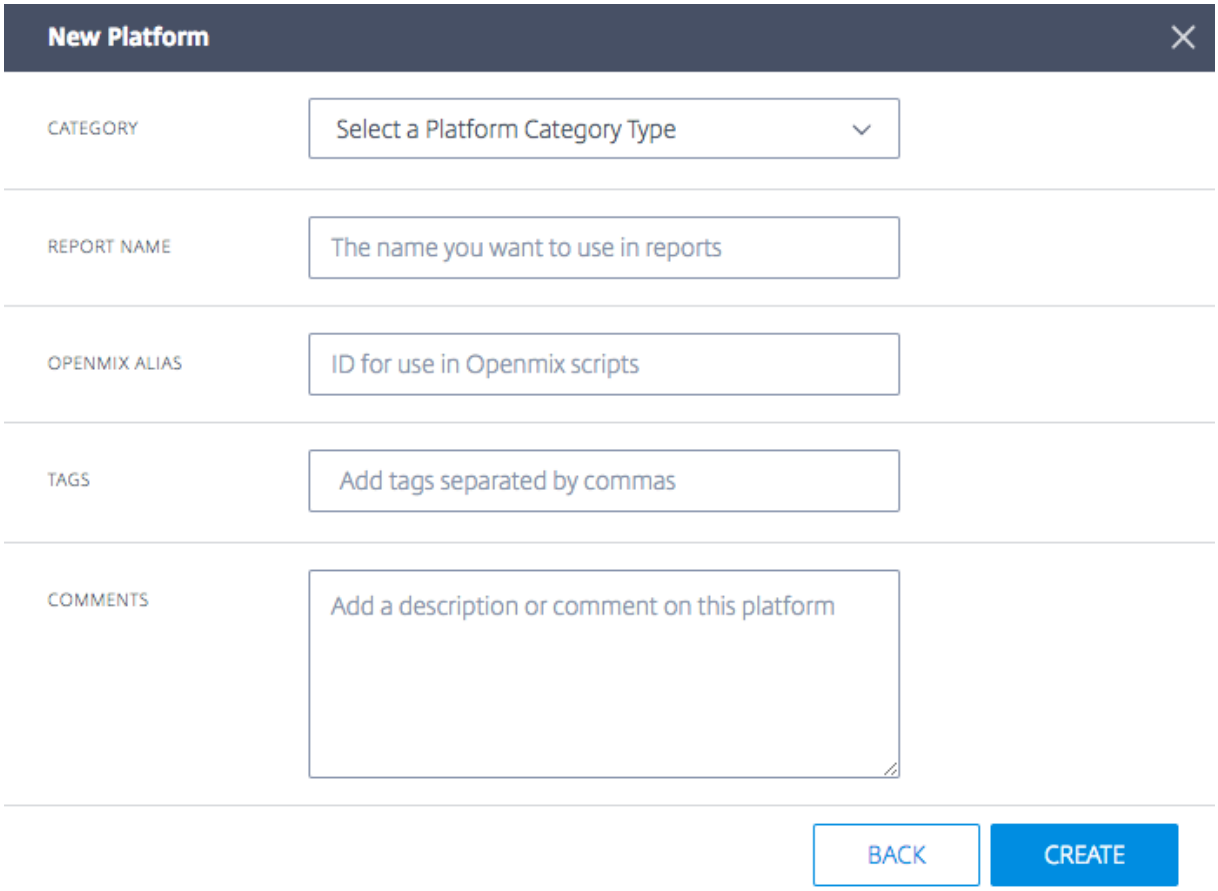
要添加平台，请单击平台页面顶部的 **+** 按钮。

新平台

单击“添加平台”后，您将看到以下页面，您可以在其中选择要配置的平台类型。



选择 平台类型后，您可以为平台提供一个名称，该名称将用于显示信息并在 ITM 提供的其他服务（如 Openmix）中使用。

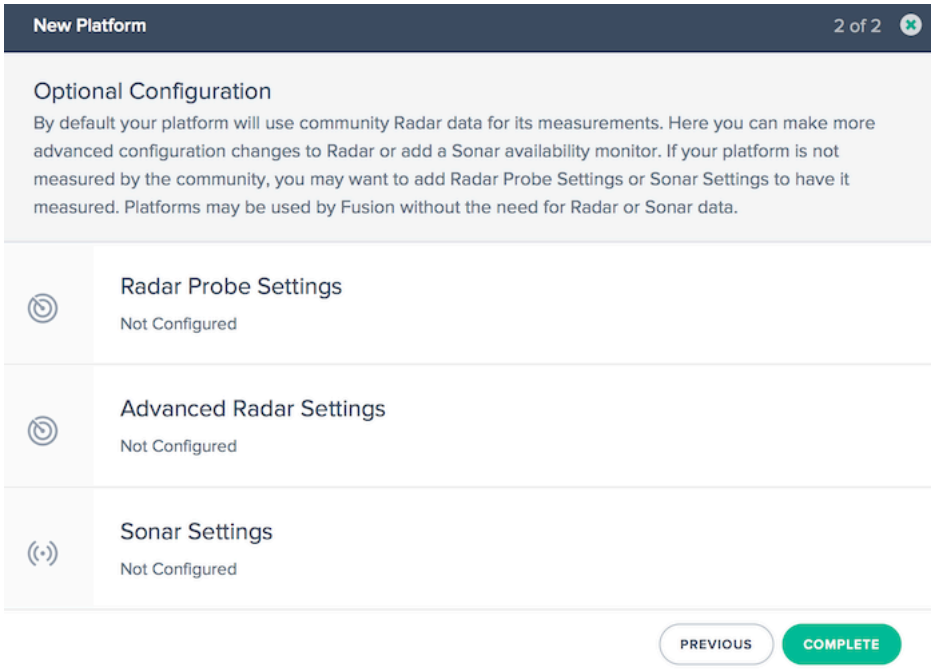


在 平台设置中，输入以下信息：

输入项目	说明
类别	平台所代表的服务类型。根据不同的类型，Radar 和 Openmix 平台的处理方式不同。可用的平台类别包括：云计算、动态内容、交付网络、云存储、安全对象交付和托管 DNS。对于 私 有平台，还有一个可用的类别是 数据中心。注意：所有导入的 GSLB 都是作为数据中心创建的。
平台	选择要测试的平台，例如 Akamai、Amazon、Azure 等
报告名称	显示和报告中使用的平台的名称。
Openmix 别名	Openmix 应用程序用于识别平台的别名。
标记	标签可以分配给平台，以便它们可以根据需要进行组织。

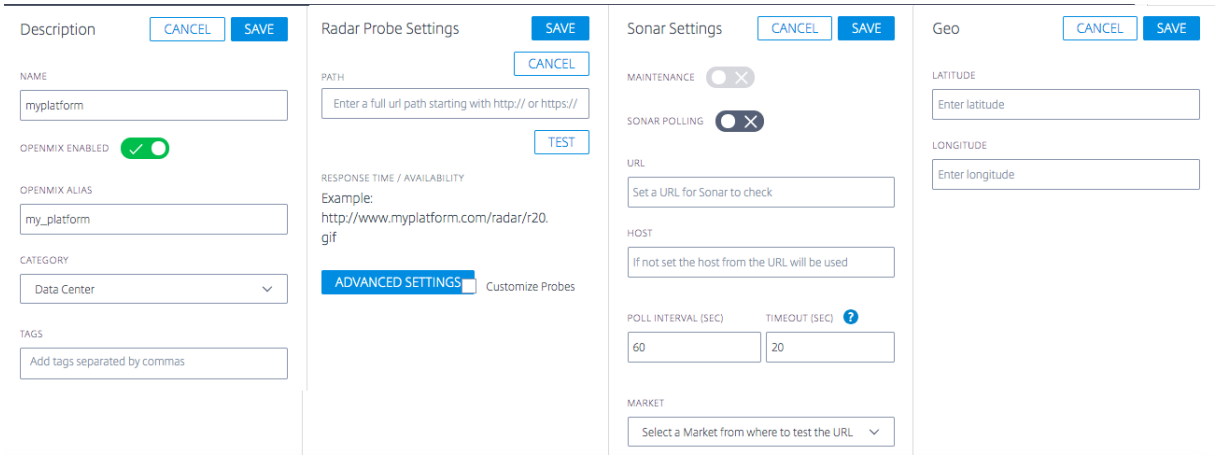
当您选择一个现有平台时，报表名称和 **Openmix** 别名 字段将被填写。您可以将这些字段保留为默认值，也可以根据需要对其进行修改。

单击“下一步”继续进行可选配置。完成可选配置后，单击“完 成”添加平台。



编辑平台

编辑平台与单击表格中的平台行并单击 编辑 按钮一样简单。



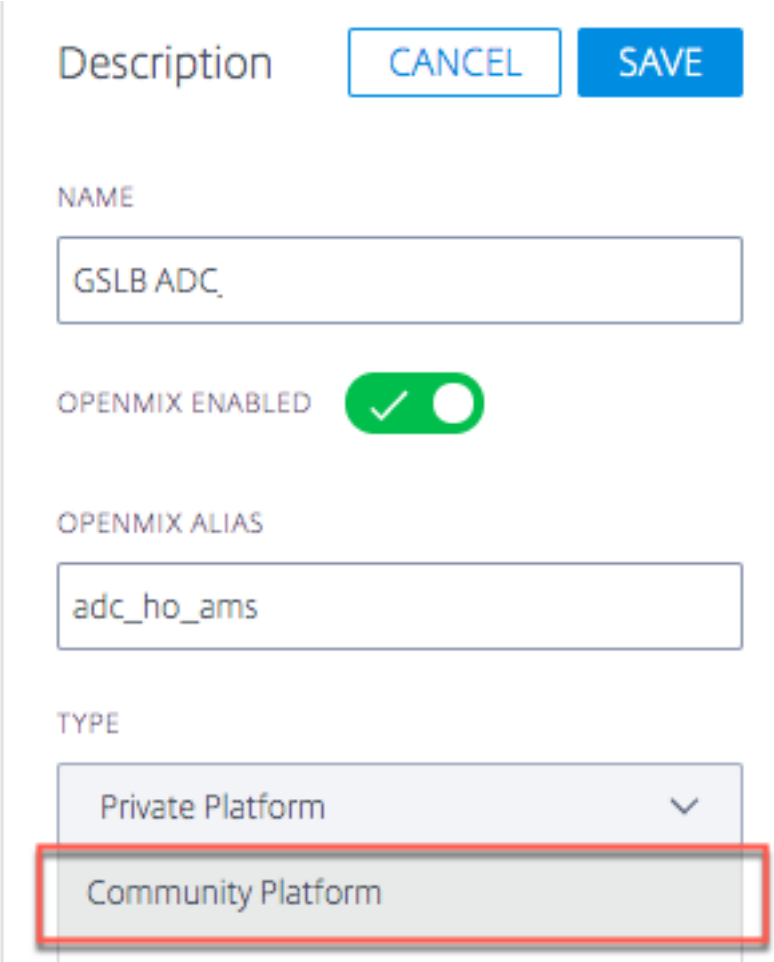
更改配置后，只需点击“保 存”，就像使用新应用程序一样，这将带您回到平台屏幕，并保存您的更改。

更改平台类型

此功能对于私有平台托管在由 Radar 社区（例如 AWS）测量的公共数据中心或云区域中并希望继承该社区平台的 Radar 数据的客户非常有用。例如，当客户将 GSLB 导入 ITM 门户时，它们将作为私有数据中心导入，但实际上可能位于公有云区域。要继承社区平台的 Radar 数据，客户可以更改私人平台或 GSLB 的当前设置以引用社区平台。

要将平台类型（如 GSLB 或私有数据中心）更改为公共社区平台（如果需要，则从社区更改为私有），请执行以下操作。

1. 单击平台表中的 平台 行。
2. 在 平台设置 部分，单击编 辑 按钮。
3. 转到 类型。如果要将私有 平台更改为社区 平台，请从列表中选择社区平台。
4. 转到 “类别”。从列表中选择一个平台类别。
5. 转到 平台。从平台下拉列表中选择要更改为的 平台。
6. 单 击平台设置 部分右上角的保存。您将看到一条确认消息，告诉您您私有平台的 Radar 探测器设置将被删除并替换为社区平台的设置。
7. 单击 确认。

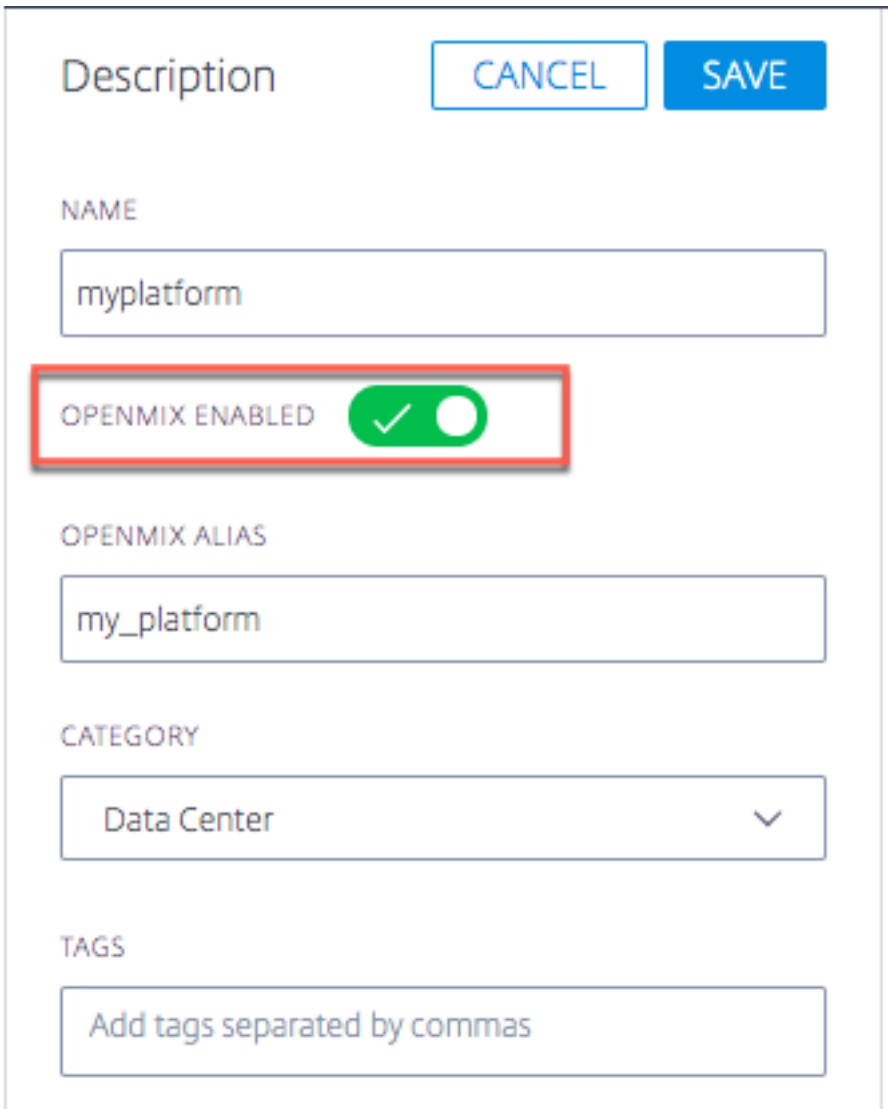


注意：如果您决定从社区更改为私有平台，则需要重新配置 Radar 探测器设置。

用于 **Openmix** 的启用平台

通过在平台设置中打开或关闭启用 **Openmix** 按钮，可以为 **Openmix** 启用 或禁 用平台。

- 单击平 台设置 中的 编辑按钮
- 选择 启用 **Openmix** 的按钮以打开它。



如果 Openmix 禁用了某个特定的平台，那么 Openmix 决策中将不再考虑该平台。这意味着不会为该特定平台生成 Radar 分数。

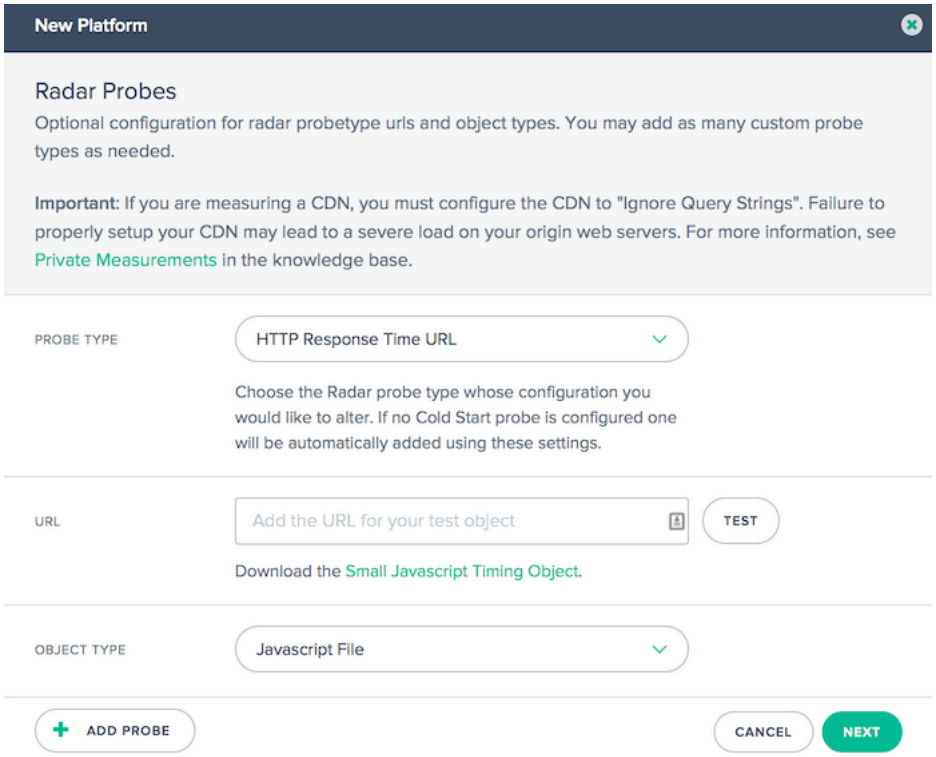
在快速入门应用程序中，平台（如果在 UI 中禁用）不会显示为要选择的选项。

但是，对于自定义应用程序，如果平台硬编码到应用程序逻辑中，则有可能会被拾取（即使该平台在 UI 中为 Openmix 禁用）。为了避免这种情况发生，自定义应用程序的编写方式必须始终包含一个用于获取 Radar 分数的逻辑。当 Openmix 平台被禁用时（在 UI 中），将不再为其生成 Radar 分数，因此应用程序会自动忽略该平台。

如果特定平台出现问题，并且客户希望在该问题期间将其从所有应用程序中提取出来，则此操作可用作开/关开关。

Radar 探头设置

可为每个平台指定 Radar 探头。通常，只有在您设置用于 Radar 监视的私有平台时才需要这样做。公共平台提供社区收集的数据，可用于大多数用途。



对于所收集的每种类型的数据都有一个探测器，例如：HTTPS 响应时间、HTTP 吞吐量、HTTPS 冷启动（针对可用性）等，大多数 Radar 设置至少具有冷启动和响应时间的探测器，在某些情况下具有吞吐量。

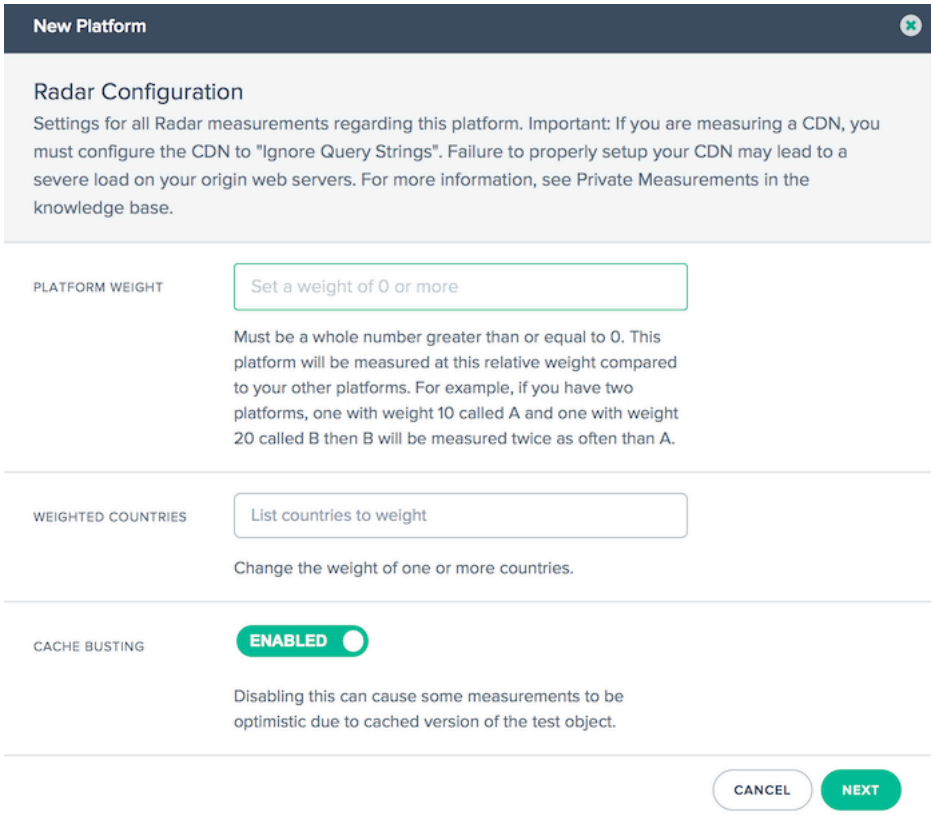
每个探头都有以下设置：

输入项目	说明
探头类型	应报告数据的值。针对每个协议 (HTTP/HTTPS) 和将收集的数据类型（冷启动、往返时间、吞吐量等）都有单独的探测。
URL	探测对象的 URL。
对象类型	用于进行测量的文件类型。在大多数情况下，您想从对话框中的链接下载“定时对象”并选择“图像文件”。对于 DSA 服务的探测，您通常会选择“网页（动态）”。

单击对话框左下角的 添加探测器，并为每个探测器添加信息。输入所有探测器后，单击“保存”。

高级 **Radar** 设置

您可以控制平台 Radar 检查的行为。只有当您了解对 Openmix 应用程序的影响时，才能更改这些内容。



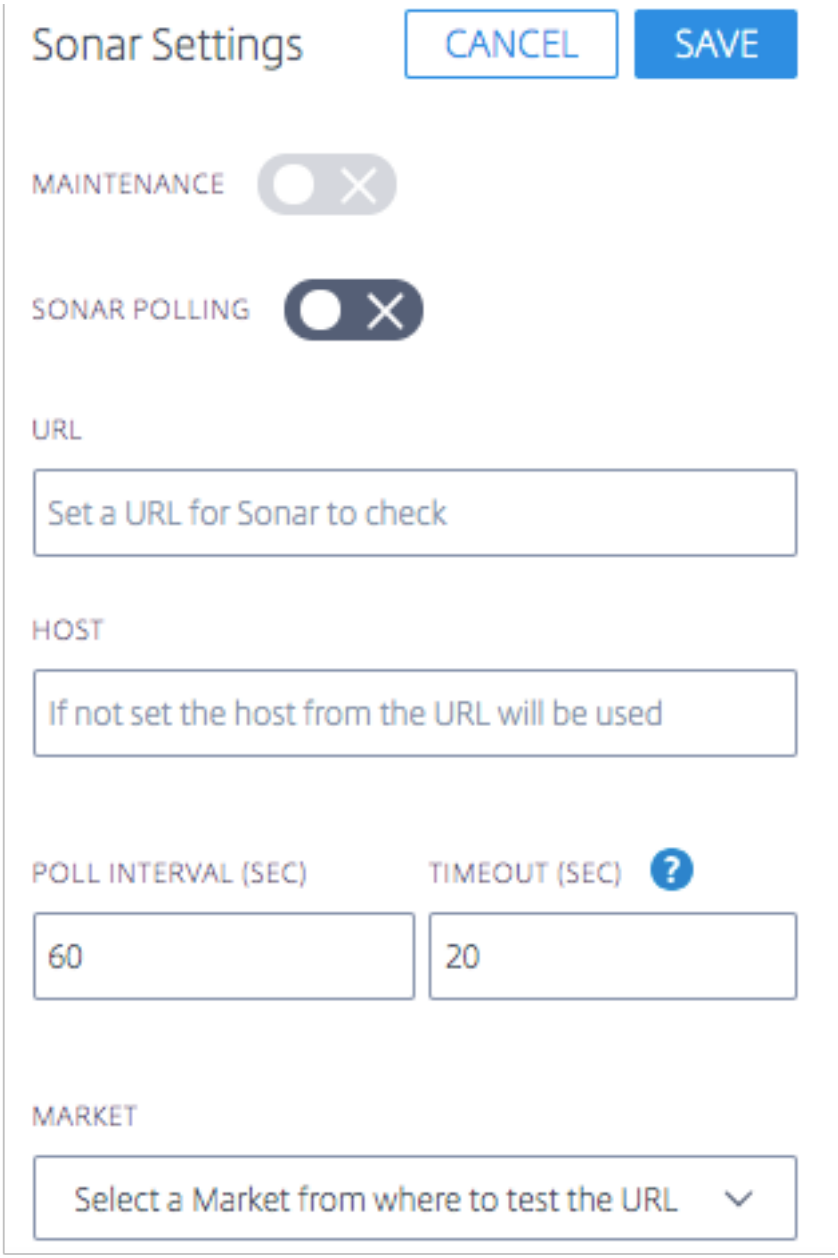
以下选项可用：

输入项目	说明	默认值
平台重量	Radar 使用权重系统来帮助客户确定自定义测试的优先级，数量越高，此专用测试的优先级越高。通常情况下，如果您只配置一个测试，则将其保留为默认测试，则会在您有多个自定义测试时使用此选项。	10，无权重
加权国家	您可以通过输入所需国家/地区来覆盖某些国家/地区的平台重量。使用 ISO 国家/地区代码指定国家/地区。	0，无权重
国家/地区权重	如果指定了加权国家/地区，则此权重将应用于国家/地区，并覆盖平台重量。如果权重设置为零，则不会在指定国家/地区测量该平台。	
缓存破坏	由于报告了测试对象的缓存版本，禁用此设置可能会导致某些测量值感到乐观。	已启用

Sonar 设置

Sonar 是一种活性检查服务，可用于监视基于 Web 的服务的可用性。Sonar 的工作原理是从世界各地的多个存在点向您指定的 URL 发出 HTTP 或 HTTPS 请求。

Sonar 在平台配置中已启用。请参阅用Sonar户指南了解更多信息。



平台地理

平台 **Geo** 是分配给平台的位置（纬度和经度）。地理信息使您能够在 可视化 工具中准确地将平台放置在地图上。

注意：**Geo** 仅适用于具有一个物理位置（如数据中心或云区域）的平台。

适用于私有平台

默认情况下，没有分配给专用平台的 **Geo** 位置。当用户创建私有平台并配置 **Radar** 探测器时，我们使用探测器对其进行地理定位。这意味着，当您向 **Radar** 设置添加 URL 时，我们会对找回的 IP 进行地理定位，并将其分配为私有平台的 **Geo** 。如有必要，您可以编辑此 **Geo** 。或者，您可以手动为您的平台分配 **Geo** ，而不依赖于 Radar URL 路径。

设置 **Geo** 后，它不会自行重置。即使您更改了 **Radar** URL，它也不会更改平台的 **Geo** 。您需要手动编辑 **Geo** 才能对其进行修改。

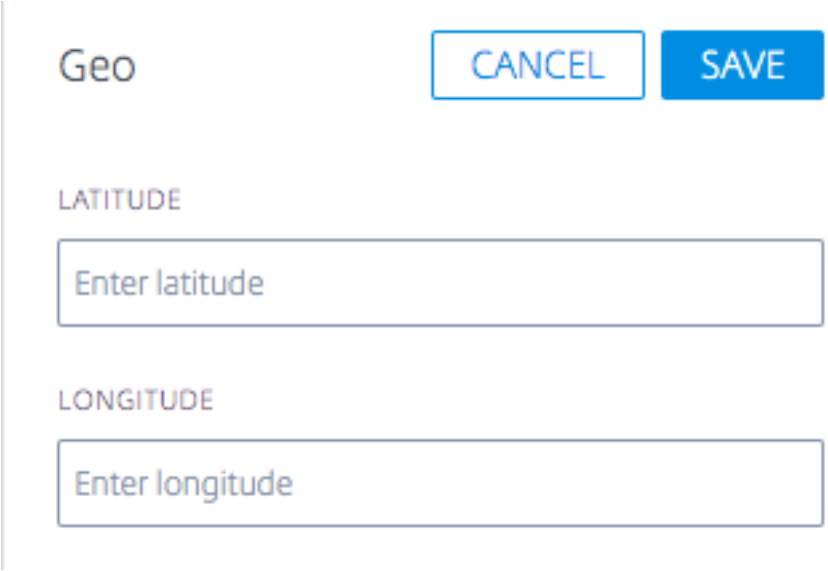
注意：并非所有私有平台都会分配 **Geo** 值。Geos 仅适用于具有一个物理位置的平台。

用于导入的平台

如果您通过 GSLB 或 F5 配置导入平台，我们会从该配置定位公有 IP，并将其用作平台的 **Geo** 。

适用于社区平台

当客户向其帐户添加社区平台时，默认情况下，此平台将继承 社区平台的原始地理位置。但是，客户可以编辑此平台的地理位置。通常情况下，客户不必对其进行编辑。但是，如果客户选择编辑此 **Geo** 并输入新的纬度和经度，则客户的设置（针对社区平台）将覆盖 社区平台 的原始 **Geo** 。



Openmix

September 22, 2023

概述

NetScaler Intelligent Traffic Management (ITM) Openmix 提供了一种革命性的方法来执行全局流量管理/全局服务器负载平衡 (GTM/GSLB)。对于传统的全局流量管理，ITM 提供了一种基于 DNS 的负载平衡方法。ITM 使用 DNS CNAME 或记录，根据所需的业务逻辑实时更改 DNS 响应。Openmix 可以通过多种方式集成到视频工作流程和交付中。

GTM 或 GSLB 工具和服务依靠专有、不可扩展的静态规则引擎来定义和控制一组狭窄的固定策略，用于故障转移、轮询和地理位置定位。NetScaler ITM 的使命是实现基于实时数据馈送的下一代云战略。Openmix 平台提供了一种非常稳健的方法，可以从各种来源提取实时数据。它将元数据公开为环境“变量”，可以在每个请求中对其进行评估。

Openmix：主要优势

- 消除单一供应商依赖关系并确保 100% 可用性
- 控制性价比权衡，消除与多来源相关的麻烦
- 消除传统性能工具的不确定性，有选择地和战略性地减轻流量
- 将特定供应商应用于个别市场

Openmix 如何运作

客户登录 Citrix ITM 门户以部署其第一个应用程序。提供了一个示例应用程序库来帮助 入门 ，还有一个分步向导工具可帮助创建具有最常见路由逻辑的应用程序。ITM Openmix 应用程序可以支持两种协议用于指导流量：DNS 或 HTTP。

应用程序定义的控制

全球分布式按需的 Openmix 平台让 GTM/GSLB 决策更贴近您的应用程序受众。每个主机都可以拥有自己的自定义 Openmix 应用程序，该应用程序考虑当前的指标和变量，从而为任何路由请求提供最佳优化。

Openmix 脚本是用 JavaScript 编程的，这是大多数 Web 程序员和网络管理员都可以访问的语言。而这种基于脚本的方法几乎可以用最小的编码复杂度实现任何业务逻辑，以此作为真正动态流量管理策略的基础。由于我们客户社区的协作性质，ITM 还提供“快速入门应用程序”，这些应用程序是不需要代码的标准应用程序。

何时使用 **HTTP** 或 **DNS** 服务

ITM Openmix 实现了广泛的内容交付优化。您使用哪种方法来启用 Openmix 在很大程度上取决于您的用例的具体情况。DNS 方法易于实施，对客户端大多是透明的，并且可以在各种内容中使用。但是，切换提供商的能力受到 DNS 响应上设置的 TTL 的限制，并且某些内容无法在中途切换到其他提供商。HTTP 提供了更大的集成灵活性，当它最适合客户端时，可以做出优化决策。这种更大的灵活性需要更多的工作来与 CMS 或客户端集成。

下表总结了 DNS 和 HTTP 接口的客户使用案例。

	Openmix DNS	Openmix Web Services (HTTP)
Typical Use	Webpage Optimization Mobile App Optimization Player or Game Download Initial Video/Game Request Mid-Stream Requests (TTL expiration)	Initial Video Request Initial Game Server Selection Mid-Stream Requests Mid-Play Gaming Client Requests
Radar Tag / SDK & Fusion Data Collection	Cedexis Radar RUM CDN & Cloud Performance Monitoring CDN & Cloud Costs data, 3rd Party Monitoring Metrics: Player, Server or App Health, Synthetic Process Monitoring, etc.	
Client Data Collection	Video Player Performance Metrics	
Cedexis Billing	Per Millions of DNS Queries	Per Millions of HTTP Requests

Openmix：DNS

CNAME 委派　ITM 客户最简单的集成是使用 DNS CNAME 委派。CNAME 委派的工作原理是让客户将面向最终用户的主机名（在以下示例中为 `www.acme.com`）指向 ITM 主机名

```
www.acme.com  600  IN  CNAME  2-02-123d-000d.cdx.cedexis.net.
<!--NeedCopy-->
```

在收到来自最终用户的 DNS 请求后，ITM 系统会实时做出决策。该决策基于 Radar 数据、应用程序中的业务逻辑和任何第三方信息。这个决定要么是另一个 CNAME 记录（在 acme.cdn1.net 下面的示例中），要么是 A 记录，例如 111.222.111.222。

通过提供 CNAME 记录，ITM 将最终用户“指向”所选的 CDN、云或数据中心。路由最终用户使用该提供商而不是另一个提供商。

```
2-02-123d-000d.cdx.cedexis.net.  19  IN  CNAME acme.cdn1.net.
<!--NeedCopy-->
```

一旦提供了 CDN 或 Cloud CNAME，最终用户的机器就会继续解析链。它请求一个 CDN 名称服务器，直到收到节点或服务器的 IP 地址。在下载内容的过程开始的位置。

如果记录作为逻辑的一部分提供，则最终用户的机器将接收 IP 地址。它直接连接到服务器并启动内容下载。

```
acme.cdn1.net.  132  IN  A  111.222.222.111
<!--NeedCopy-->
```


区域委派　此外，权威 DNS 区域委派是实施 Openmix 的一个选项。客户创建一个 DNS 区域并委派到在 ITM 门户中创建的预测 DNS 区域。在委派区域中创建主机名。将其配置为使用 Openmix 应用程序或动态预测 DNS 记录来生成响应。

此选项的优点是无需在主机名和来自 ITM 平台的动态响应之间进行 CNAME 委派。使用前面的示例 `www.acme.com`，主机名直接解析为最佳 CDN、Cloud 或数据中心的配置值。

```
www.acme.com. 19 IN CNAME acme.cdn1.net.
```

也可以使用 A/AAAA 记录来代替 CNAME，并且主机名将直接解析为最佳目的地的记录。

```
www.acme.com. 19 IN A 111.222.222.111
```

DNS 和生存时间的影响　我们会仔细考虑诸如生存时间 (TTL) 值之类的因素，为内容设置适当的时间，以及用户必须如何做出决策。在大多数情况下，ITM 建议用于页面和对象内容的 20 秒 TTL。对于视频内容，ITM 顾问与客户合作，根据区块长度和集成方法找到最合适的平衡。

Openmix：HTTP

DNS 的替代方法是使用 HTTP API。Openmix 使用 HTTP 请求通知客户端（例如视频播放器或 CMS）在任何时间点使用哪个平台。

```
http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision
< HTTP/1.1 200 OK
< Content-Type: application/json
< Date: Mon, 22 Apr 2015 20:25:24 GMT
< Connection: keep-alive
< Content-Length: 177
<
{

  "providers" : [
    {

    "provider" : "cdn2",
    "host" : "foo.cdn2.net"
     }
 ,
    {

    "provider" : "cdn1",
    "host" : "acme.cdn1.net"
     }

  ]
 }

<!--NeedCopy-->
```


HTTP Openmix 服务使用与其基于 DNS 的服务相同的应用程序逻辑。它还包括一些额外的扩展，允许对客户端计算机进行进一步的性能分析。例如，使用 HTTP Openmix，可以查看用户代理字符串、X-Forwarded-For 和 Referer 的标头。使用查询字符串参数提供 IP 覆盖。

由于 HTTP Openmix 的有效负载比 DNS 更具可扩展性，因此也可以以不同的方式提供 CDN、云或服务器决策选择。到目前为止，最常见的是从首选平台到最低平台的有序列表（如上所述）。完整列表允许将决策等级提供给 CMS 或客户端，但仍允许在选择提供商时使用内部启发式方法。

CMS 集成

有些客户更喜欢在服务器端处理提供商选择，而不是在每个客户端中实现提供商选择。HTTP API 可用于在客户端请求时从 Openmix 检索优化决策。它可用于填充从 CMS 返回给客户端的文件。

默认情况下，Openmix HTTP 端点使用调用方的 IP 作为地理位置和决策标准。如果您从位于最终用户客户端和 Openmix 之间的 CMS 或其他系统调用，则可以将 IP 指定为决策中使用的参数。

```
http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision?ip=1.2.3.4
< HTTP/1.1 200 OK
< Content-Type: application/json
< Date: Mon, 22 Apr 2015 20:25:24 GMT
< Connection: keep-alive
< Content-Length: 177
<
{

  "providers" : [
    {

    "provider" : "cd1",
    "host" : "acme.cdn1.net"
     }
 ,
    {

    "provider" : "cdn2",
    "host" : "foo.cdn2.net"
     }

  ]
 }

<!--NeedCopy-->
```

此方法允许您使用 CMS 集成从 Openmix 中提取决策。您还可以为最终用户获得地理位置和 ISP 路由优化的好处。然后将从 Openmix 返回的主机名打包到响应中，例如视频清单文件，并由 CMS 返回给客户端。客户端无需任何修改即可使用优化的决策来支持 Openmix 优化。

Openmix 应用程序

Openmix 快速入门应用程序是负载平衡和流量管理应用程序。这些应用程序根据一组规则向最佳提供商提供实时流量路由。

针对向 Openmix 提出的每个请求都会处理应用程序，并根据指定的逻辑做出路由决定。客户可以对具有较高业务价值的内容使用一个应用程序，而对价值较小的内容使用另一个应用程序。这些请求是单独路由的。

调用应用程序时，会向 Citrix 的其中一个负载均衡器发出一个请求。对于 DNS，它是向 DNS 负载均衡器发出的单个 DNS 请求。对于 HTTP，它是对 Openmix HTTP 端点的 GET 或 HEAD 请求。

目前可通过 NetScaler Intelligent Traffic Management 门户使用以下应用程序。

- 静态路由
- 故障转移
- 轮询
- 最佳往返时间 (ORTT)
- 吞吐量
- 静态接近

Openmix 自定义 JavaScript 应用程序由专门的 Openmix 服务器根据脚本中的逻辑来响应 DNS 或 HTTP 请求。脚本的部署是通过配置和发布应用程序的客户门户完成的。有关如何创建自己的 JavaScript 脚本的更多信息，请参阅我们的 Developer Exchange 中的信息。

在设置应用程序之前，了解以下概念非常重要：

可用性阈值

可用性阈值是平台在考虑路由时必须达到的最低可用性分数。所有应用程序的默认最低可用性阈值为 80%。但是，您可以修改此百分比并将其设置为适合您的位置、网络可用性和可靠性的值。

注意：如果没有平台满足此最低可用性阈值（默认值为 80%，或您设置的值），则会对轮询、ORTT 和吞吐量应用程序执行随机路由。

回退

如果 Openmix 应用程序因任何原因未能成功运行，则会返回回退响应。或者，如果 Sonar 确认没有可用的平台。因此，必须指定有效的备用 CNAME/A/AAAA 记录或 IP（或 HTTP 中的路径），Openmix 可以用它进行响应。此备用 URL 或 CNAME 记录可以用于 Openmix 中预先配置的平台。
在以下情况下，有时也会发生回退：

- 在应用程序版本之间切换时，您上传并发布新脚本。在新脚本初始化并删除旧脚本之前，需要短暂的毫秒回退时间。

- 如果出现过载（这种情况很少发生），Openmix 会使用后备 CNAME/A/AAAA 进行响应，因为回退会抵消服务的负载。

要进行回退，必须在 DNS 中输入有效的主机名（CNAME/A/AAAA 记录）或 IP 地址，以及有效的 URI（可以是 HTTP 格式的 `scheme:[//host[:port]][/path][?query][#fragment])`）。

TTL

在 Openmix 中，应用程序的 DNS 生存时间（TTL）告诉解析者在再次询问 Openmix 之前，他们必须保留多长时间的决定。
TTL 用于控制 Openmix 应用程序获得的流量。它还控制应用程序对所处理的数据变更的敏感程度。
默认 TTL 为 20 秒。尽管您可以修改此值，但不建议这样做。如果降低 TTL，则会获得更多的流量和更多的实时 DNS 查询。这可能会导致成本增加和性能降低，因为 DNS 查询需要在客户端上花费时间。因此，最好不要更改 TTL 的默认值。

> 注意：生存时间适用于快速入门应用程序、自定义 JS 应用程序（如果代码中未指定 TTL）以及所有备用响应

重量（用于轮询）

您可以为全球和/或市场或国家/地区的每个平台的优先级和选择分配权重。

例如，假设您为应用程序选择了三个平台-P1、P2 和 P3。您给他们权重：分别为 60、50 和 10。循环应用程序将这些值转换为百分比，例如 P1= 50%、P2= 42% 和 P3= 8%，加起来等于 100%。这些百分比意味着 50% 的时间用户通过 P1 进行路由，42% 的时间通过 P2 进行路由，8% 的时间通过 P3 进行路由。

您赋予平台的权重加起来不必等于 100。它们可以是介于 0 和 1,000,000 之间的任何整数。当转换为百分比（由后端的应用程序）时，赋予平台的权重加起来为 100%。如果所有选定的平台都具有相同的权重，则流量将随着时间的推移在它们之间均匀分布。如果您有一个平台，那么无论您给它多少权重，该平台都会百分之百地被使用。

权重仅用于根据 Radar 和 Sonar 可用性检查认为可用的平台，具体取决于应用程序的配置。不可用的平台会导致分布与配置的权重不匹配。例如，如果 P1 的重量为 100，P2 的重量为 0，但 P1 未通过 Radar 可用性检查，则所有流量都将流向 P2。

让分（用于 **ORTT** 和吞吐量）

让分是一个百分比值，可以应用于平台来修改 RTT 和吞吐量的 Radar 分数，也就是说，人为地增加响应时间（以毫秒为单位）或降低吞吐量（以 kbps 为单位）。增加或减少这些值会降低平台的性能，从而降低平台被选中的可能性。让分可以在全球平台上添加，也可以针对特定市场或国家单独添加。
如果某个平台在特定市场或国家/地区价格昂贵，并且您希望在同等提供商的表现接近时降低其被选中的可能性。您可以将让分值作为乘数来增加响应时间的值或减少吞吐量的值。因此，它降低了平台被选中的可能性。

以下是让分在后端的运行方式：

- 应用让分的平台 RTT = RTT（以毫秒为单位的往返时间）*（1 + 让分）或
- 应用让分的平台吞吐量 =（以 kbps 为单位的吞吐量）*（1 —让分）

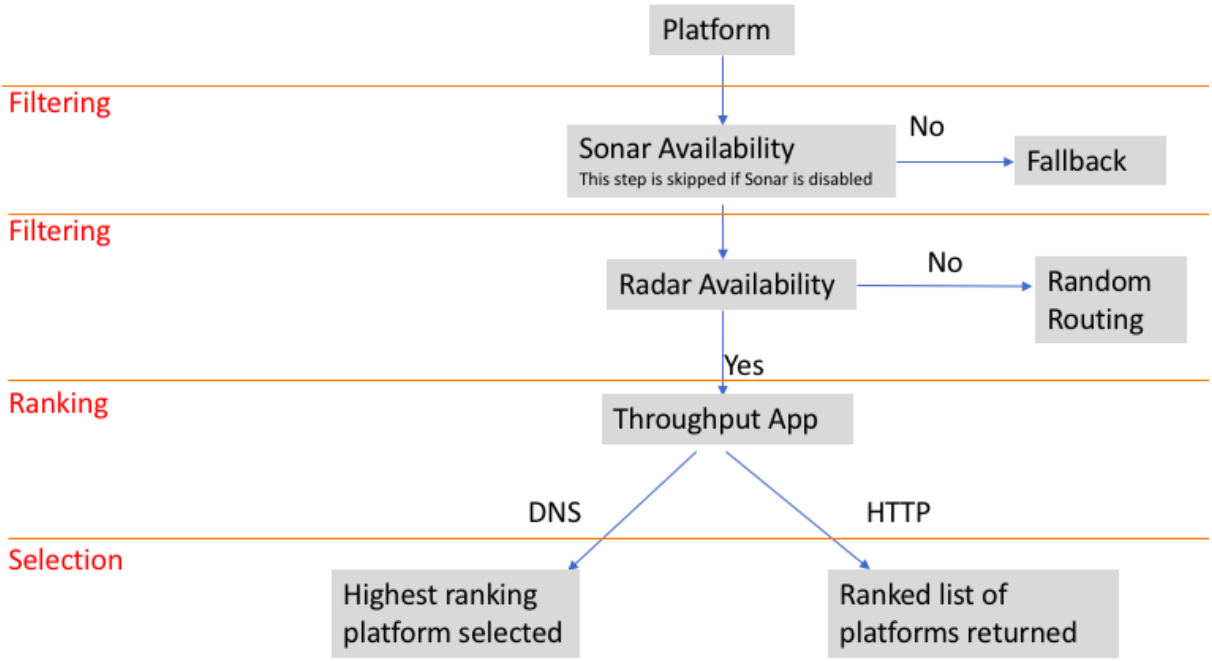
注意：平台的 RTT 和吞吐量值是来自 Radar 数据的分数。

下表显示了让分如何影响两个平台——P1 和 P2。以及让分如何降低 P1 被选中的可能性。

	P1	P2
不带让分的 RTT	50 毫秒	60 毫秒
RTT P1 的让分为 50% (0.5)，P2 为 0% (0)	50 (1+0.5) = 75 毫秒	60 (1+0) = 60 毫秒
无让分吞吐量	3000 kbps	2800 kbps
P1 的吞吐量为 50% (0.5) 个让分，P2 为 0% (0)	3000 (1-0.5) = 1500 kbps	2800 (1-0) = 2800 kbps

过滤、排名和选择工作流

吞吐量应用程序的示例流程图



平台选择标准

Openmix 快速入门应用程序使用以下标准作为第 1、2 和 3 级过滤器来排名和选择最佳平台。

过滤级别	选择标准	ORTT	吞吐量	轮询	故障转移	静态路由	静态接近
第 1 级	声纳可用性检查（如果启用）	X	X	X	X	X	X
第 2 级	Radar 可用性检查（如果启用）	X	X	X	X	X	不适用
第 3 级	权重（用户定义）	不适用	不适用	X	不适用	不适用	不适用
第 3 级	往返时间（以毫秒为单位）	X	不适用	不适用	不适用	不适用	不适用
第 3 级	吞吐量（以 kbps 为单位）	不适用	X	不适用	不适用	不适用	不适用

原因代码报告

原因代码提供决策原因的可见性，还可以了解应用程序代码的哪一部分正在运行。在执行过程中，应用可以随时在原因代码字段中添加一些内容。
原因代码对每个快速入门应用程序的含义各不相同。每个应用程序的原因代码之间有一些共同点，但并不全面。

注意：要正确显示原因代码，它们不得超过 200 个字符的最大字符限制。如果超过此限制，原因代码将显示为“未知”。如果用户尚未添加原因代码，则会显示“未知”。

以下是快速入门应用程序的原因代码：

原因代码	说明	最佳 RTT	轮询	静态路由	吞吐量	静态接近	故障转移
最佳利用率	业绩最佳的提供商现已上线，并已被选中。	X	不适用	不适用	X	不适用	X

原因代码	说明	最佳 RTT	轮询	静态路由	吞吐量	静态接近	故障转移
Optimal Unavail-Radar	表现最佳的提供商不可用；根据雷达的说法，已经选择了另一家符合条件的提供商	X	不适用	不适用	X	不适用	X
Optimal Unavail-Radar+Sonar	由于雷达和/或声纳的原因，性能最佳的供应商不可用。	X	不适用	不适用	X	不适用	X
All Unavail-Radar	根据雷达，所有符合条件的平台都不可用。请求已路由到后备设备	X	X	不适用	X	不适用	X
All Unavail-Sonar	根据声纳，所有符合条件的平台都不可用。请求已路由至后备设备。	X	X	不适用	X	不适用	X
数据问题	表示缺少一个或多个平台的雷达测量结果。因此，平台是随机选择的	X	X	不适用	X	不适用	X
地理默认	默认的地理设置已生效	X	X	不适用	X	X	X
地理覆盖国家/地区	该决定实行国家优先权	X	X	不适用	X	X	X

原因代码	说明	最佳 RTT	轮询	静态路由	吞吐量	静态接近	故障转移
地理覆盖市场	此决定已生效的市场优先权	X	X	不适用	X	X	X
全部可用	所有符合条件的平台均可通过声纳和雷达获得	X	X	不适用	X	不适用	不适用
近端可用	最近的地理平台可用且已被选中	X	不适用	不适用	不适用	X	不适用
Eligible Unavail-Radar	根据雷达，对于轮询，符合条件的提供商不可用	不适用	X	不适用	不适用	不适用	不适用
永久应用程序	该决策提供了缓存的响应，没有执行任何逻辑	X	X	X	X	X	X
请求地理位置不可用	无法建立请求的地理位置。请求已路由到后备设备	X	不适用	不适用	不适用	X	不适用
全部不可用提供商	所有提供商都不可用。请求已路由到后备设备	X	不适用	不适用	不适用	X	不适用
无效提供者	未找到任何提供商的邻近分数。请求已路由到后备设备	X	不适用	不适用	不适用	X	不适用

Openmix 快速入门应用程序

1. 登录到 NetScaler Intelligent Traffic Management 门户。

2. 从左侧导航菜单中，导航到 **Openmix >** 应用程序配置。
3. 如果您是首次配置 Openmix 应用程序，则单击 Op **enmix >** 应用程序配置 时会看到“入门”页面。
4. 要配置新应用程序，请单击页面右上角的 G **et** Starte **d** 按钮或添加 按钮。如果之前已配置 Openmix 应用程序，则您将在此页面上看到应用程序列表。

以下部分将引导您完成在门户中配置 Openmix 应用程序的过程。

静态路由

这种类型的应用程序不使用任何评估逻辑来决定必须向最终用户提供哪个 DNS 响应。应用程序始终在此处选择由用户指定的单个平台。因此，该应用程序仅使用单个 DNS CNAME 或 IP 地址响应。静态路由应用程序可以通过应用程序配置页面上的门户进行 配置。

注意：在配置应用程序之前，请确保首先配置了您的平台。有关 平台 配置，请参阅平台页面。

导航

1. 导航到 **Openmix >** 应用程序配置。
2. 点击右上角的 添加 按钮

将打开“基本信息”对话框。

基本信息　请按照以下步骤输入 基本信息：

1. 对于 协议，从列表中选择 DNS 或 HTTP。
2. 对于 应用程序类型，选择静态路由。或者，如果您正在配置其他类型的应用程序，请从列表中选择它。
3. 为应用程序指定名称（必填字段）；添加说明（可选字段）和标签（可选字段）。
4. 单击“下一步”进行 配置。

配置　要配置应用程序，请执行以下操作：

1. 从平台列表中选择关联的 平台。它是您在平台页面中设置的 平台 ，代表 CDN、云或数据中心。
2. 输入 **CNAME/A/AAAA** 记录（用于 DNS）或 **URL**（用于 HTTP）。所选平台的 DNS CNAME 或 HTTP URL 必须指向有效的 IP 地址或主机名。
3. 对于 **CORS**，在 HTTP 协议中，为 CORS 选择无、全部或自定义。CORS 允许您控制从其他站点访问您的站点。您可以完全限制从其他站点访问您的站点（通过单击“无”），允许所有其他站点的访问（通过单击“全 部”），或者仅允许从特定站点进行访问（通过单击“自定义”）。
4. 输入响应的 **TTL** （生存时间）。默认值为 20 秒，但可以覆盖。
5. 单击“完成”。
6. 在确认弹出窗口中，单击“完成”或“发布”以查看 Openmix 应用程序页面中列出的应用程序。如果单击“发布”，您的应用将立即上线并显示为绿色状态。这意味着应用程序正在生产中。如果单击“完成”，您的应用程序仍会列在应用程序页面上，但未发布，状态为红色。

故障转移

故障转移应用程序支持简单的路由逻辑，根据平台的排列位置和可用性来选择平台。客户可以创建一个故障转移链，用于决定首先选择哪个平台、其次选择哪个平台，等等。创建此故障转移链既可以在全球范围内使用，也可以在各个市场和国家/地区使用。

可以在“应用程序 配置”页面上的门户内配置 故障转移 应用程序。

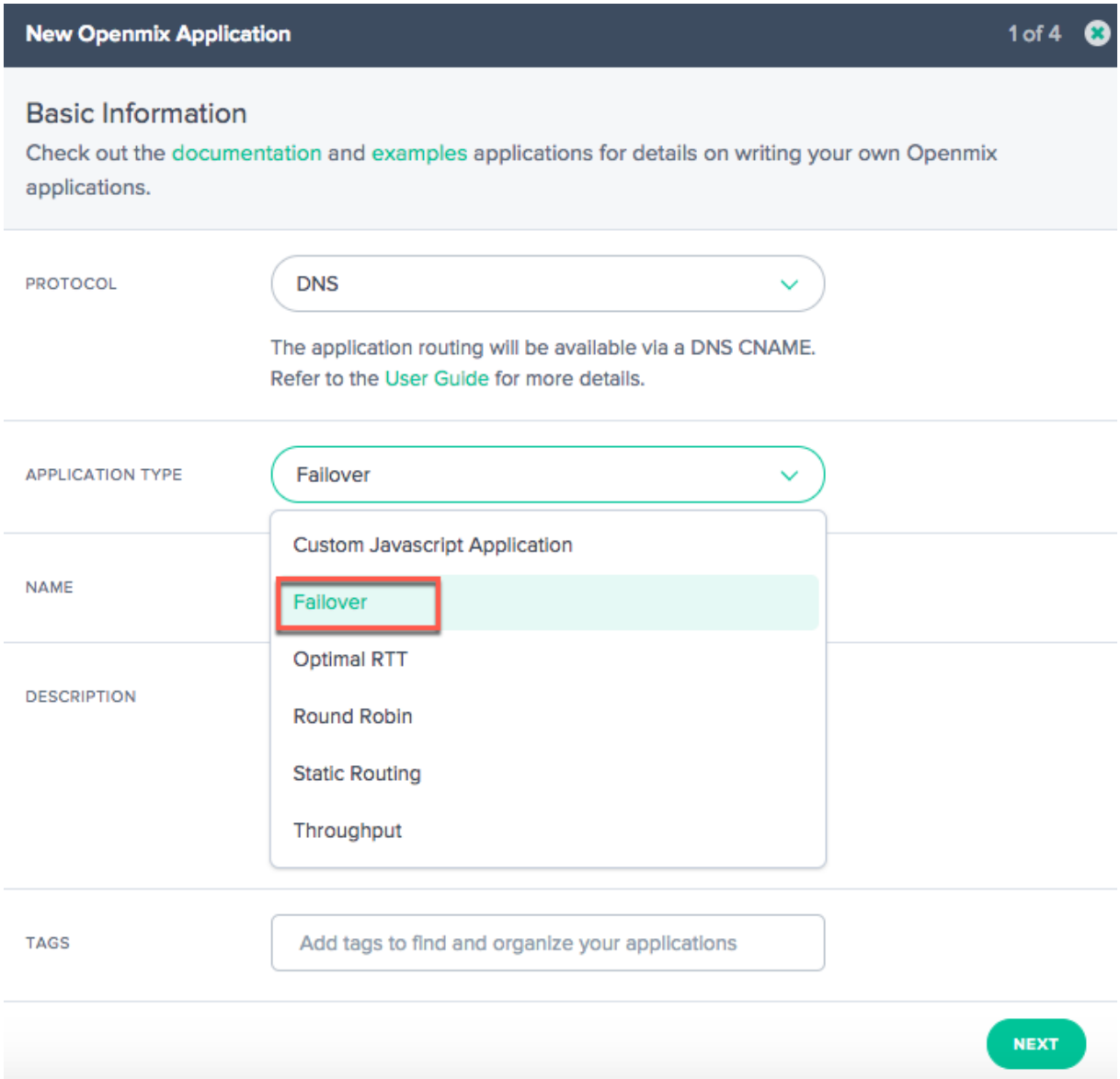
注意：在配置应用程序之前，请确保先配置平台。有关 平台 配置，请参阅平台页面。

导航

1. 登录门户。
2. 从左侧导航菜单中，导航到 **Openmix >** 应用程序配置。
3. 单击右上角的“添加”按钮，进入“新建 Openmix 应用程序”，基本信息对话框。

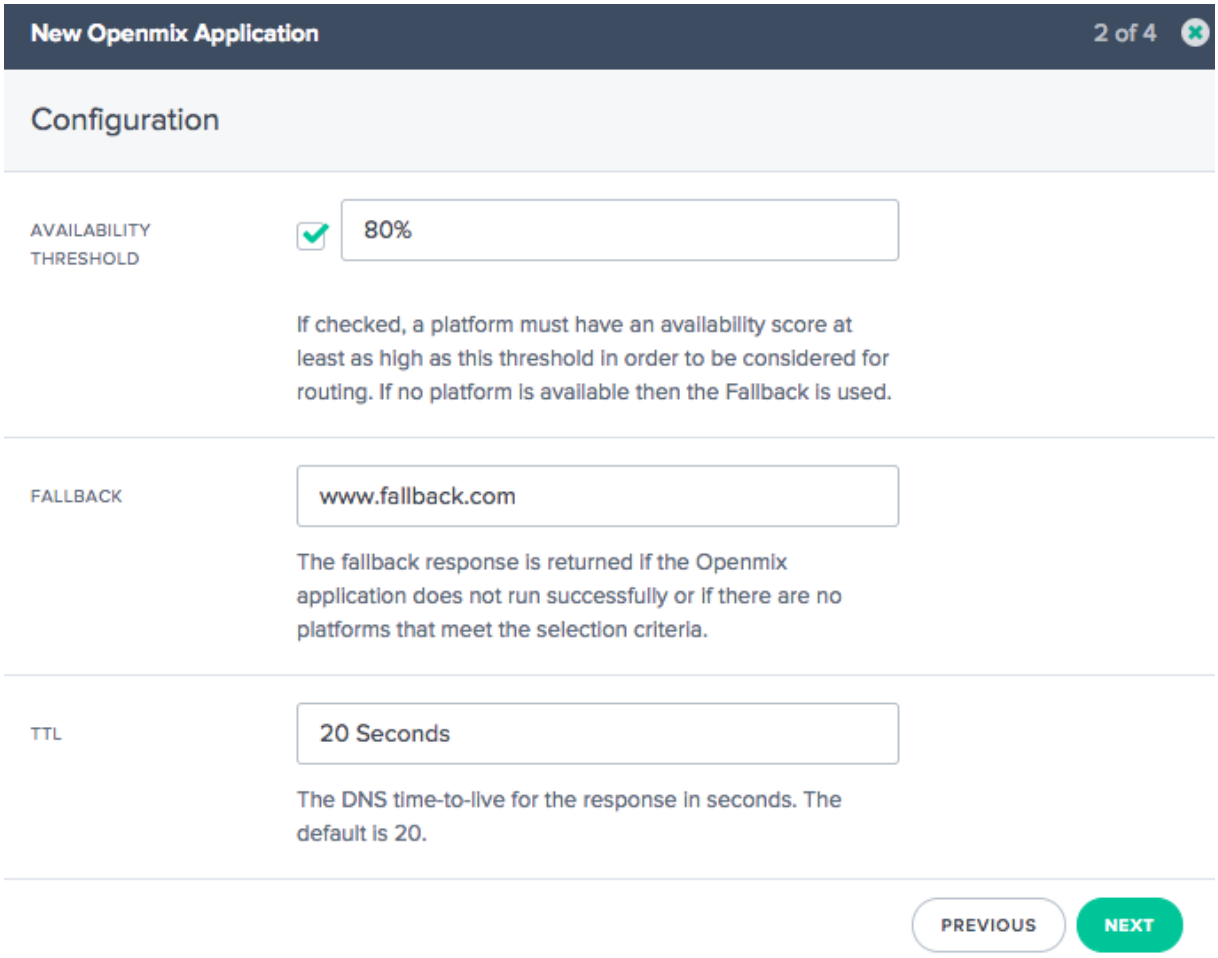
基本信息

1. 从“协议”列表中选择 **DNS** 。
2. 从“应用程序类型”列表中，选择“故障转移”。
3. 为应用程序指定名称（必填字段）；添加说明（可选字段）和标签（可选字段）。
4. 完成后，单击“下一步”。



配置

1. 在“配置”对话框中，选中“可用性阈值”复选框。可用性阈值 的默认值为 80%。平台的可用性分数必须至少与该阈值一样高，才能考虑进行路由。
   - 如果要修改默认可用性阈值，只需输入一个新值来替换默认值。
   - 如果没有平台的可用性分数等于或大于指定阈值，则使用回退 CNAME 或 A 或 AAAA 或 IP 地址。
   - 如果未选中该复选框，则平台将假定可用性阈值为零。这意味着此平台上没有 Radar 可用性检查。
2. 输入 CNAME/A/AAAA 或 IP 地址进行回退。如果应用程序遇到问题或错误，通常使用备用 CNAME/A/AAAA 或 IP。
3. 输入响应的 **TTL** （生存时间）。默认值为 20 秒。如有必要，您可以覆盖此值。



平台信息

1. 在“平台信息”对话框中，从列表中选择一个 平台。
    - 您可以使用“添加平台”按钮选择多个平台。这个想法是选择适用于全球和地理（市场和国家/地区）路由的所有可用平台。
    - 此列表中的平台是您在门户的 平台 页面中设置的平台，代表您的 CDN、云或数据中心。
    - 所有 Openmix 应用程序都需要事先设置一个关联的平台。如果您未在列表中找到平台，则可以在门户的平台页面中进行设置。
2. 输入平台的 **CNAME/A/AAAA** 记录。
3. 在移动到下一步之前，确保 已 选中“已启用”复选框（表示平台已启用）。
4. 如果配置了 **Sonar** ，并且您希望使用 Sonar 数据来帮助进行初始决策过程，请务必单击“使用 **Sonar** 获取平台可用性”复选框。注意：只有在该平台上启用了 Sonar 时，才会显示 Sonar 复选框。
5. 单击“下一步”进行 位置配置。

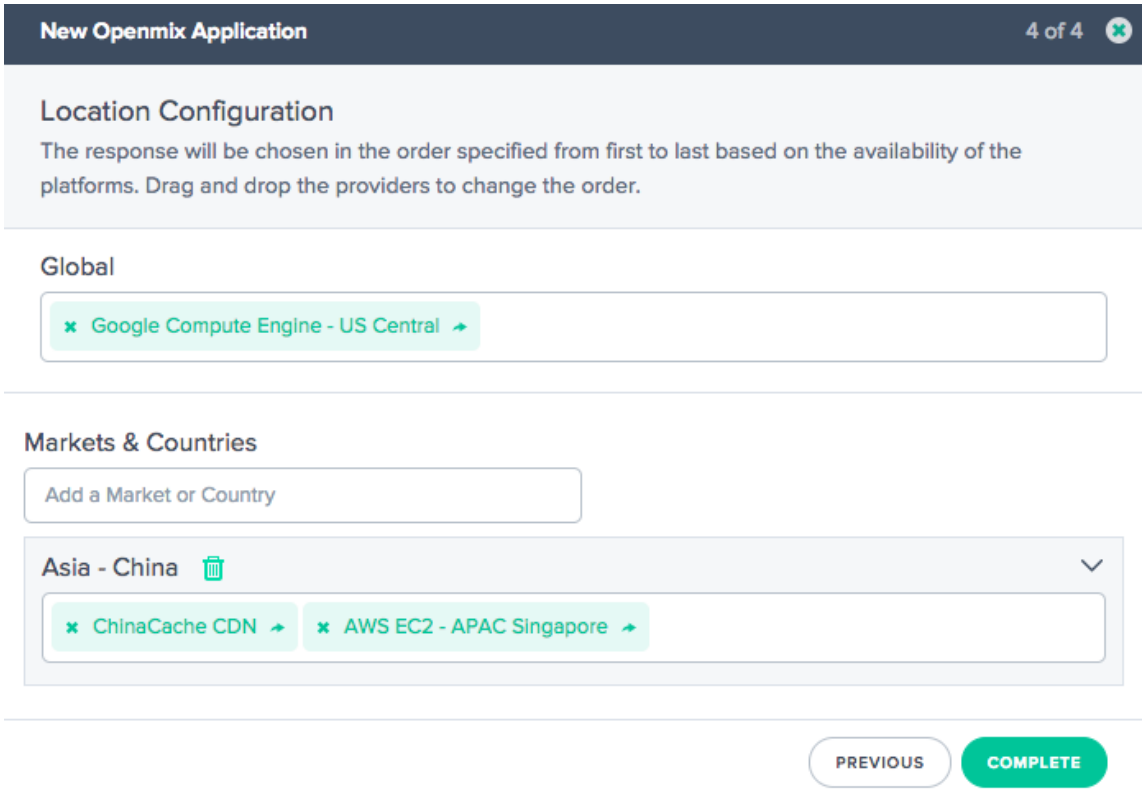
位置配置

1. 在“位置配置”对话框中，选择 全局 路由所需的平台。

   - **Global** 表示您正在为全局路由设置一系列平台。
   - 当您在“全局”字段内单击时，会出现一个列表，显示您在“平台 信息”步骤中选择的所有平台。
   - 从列表中选择基于可用性的全局路由所需的平台。
   - 在此字段中放置平台名称的顺序决定了其选择的优先级。例如，如果列表中的第一个平台不可用，则会选择第二个平台。如果列表中的任何平台都不可用，则使用回退。
   - 您可以拖动平台名称以更改其优先级顺序。

2. 如果您想设置本地地理路径的平台，请点击 市场和国家/地区。

   - 当您在“市场和国家/地区”字段中单击时，列表将显示您在平台 信息步骤中选择的所有平台。
   - 为每个地理位置（市场/国家/地区）分别选择本地地理位置路由平台。
   - 在此字段中放置平台名称的顺序决定了其选择的优先级。例如，在中国，您想先使用中国 POP，只有当它不可用时，您才会希望使用您的新加坡 POP，然后再放一行，依此类推。
   - 您可以拖动平台名称以更改其优先级顺序。



3. 点击 完成，完成应用的配置。

4. 在确认弹出窗口中，单击“完成”或“发布”以查看 **Openmix** 页面上列出的应用程序。

   - 如果单击“发布”，您的应用将立即上线并显示为绿色状态。您的应用程序已投入生产。
   - 如果单击“完成”，您的应用仍会在 Openmix 页面上列出，但未发布，状态为红色。

轮询

此应用程序遵循轮询的典型全局服务器负载平衡方法，在发出 DNS 请求时，每个 CNAME 交替返回给最终用户。然后，它使用 Sonar 数据（如果启用了 Sonar）和平台可用性 阈值来评估请求用户的最佳平台。每个平台都是根据轮询分配方法选择的。例如，如果平台 P1、P2 和 P3 达到可用性阈值，则第一个请求将路由到 P1，第二个路由到 P2，第三个请求路由到 P3。第四个请求再次路由到 P1，依此类推。

要配置新的轮询应用程序，请单击 Openmix 页面右上角的添加按钮。将打开“基本信息”对话框。

导航

1. 登录门户。
2. 从左侧导航菜单中，导航到 Openmix > 应用程序配置。
3. 单击右上角的“添加”按钮，进入“新建 Openmix 应用程序”，基本信息对话框。

基本信息

1. 在“基本信息”对话框中，选择“DNS”作为轮询协议。注意：对于轮询应用程序，路由只能通过 DNS CNAME 进行。
2. 从列表中选择 应用程序类型。为应用程序提供名称（必填字段）、说明（可选字段）和标记（可选字段）。
3. 单击下一步进行配置。

配置

1. 可用性阈值 的默认值为 80%。要修改此值，只需键入一个新值来替换默认值。
2. 输入 CNAME/A/AAAA 或 IP 地址进行回退。如果应用程序遇到问题或错误，通常使用备用 CNAME/A/AAAA 或 IP。
3. 输入响应的 TTL （生存时间）。默认值为 20 秒，但如有必要，可以覆盖此值。
4. 单击“下一步”获取平台信息。

平台信息

1. 从“平台”列表中选择一个 平台。注意：所有 Openmix 应用都需要事先设置相关的平台。如果您未在列表中找到平台，则可以在门户的平台页面中进行设置。
2. 点击“添加平台”按钮，选择更多平台。
3. 输入此平台的 CNAME 或 A/AAAA 记录或 IP（在 DNS 中）或 URL（以 HTTP 格式输入）。它必须是有效的 URL、主机名或 IP 地址。它的形式可以是：`scheme:[//host[:port]][/path][?query][#fragment]`。
4. 在移动到下一步之前，确保 已 选中“已启用”复选框（表示平台已启用）。
5. 如果 Sonar 可用，并且您希望使用 Sonar 数据来帮助初始决策过程，请务必单击“使用 **Sonar** 获取平台可用性”复选框。
6. 单击“保存”转到第 4 步，为每个平台分配适当的权重。

位置配置

1. 为全球和/或按市场或国家/地区划分每个平台的优先级和选择分配 权重。
2. 要分别为市场或国家/地区分配平台权重，请在市场和国家/地区搜索框中输入名称，然后从列表中进行选择。
3. 单击“完成”以创建您的应用程序。
4. 在确认弹出窗口中，单击完成或发布，即可在 Openmix 页面上看到您的应用列出。如果单击“发布”，您的应用将立即上线并显示为绿色状态。您的应用程序已投入生产。如果单击“完成”，您的应用仍会在 Openmix 页面上列出，但未发布，其状态为红色。

最佳往返时间 **(ORTT)** 应用程序

ORTT 应用程序使用 Radar 响应时间、声纳数据（如果已启用 Sonar）和平台可用性阈值来评估请求用户的最佳平台。可用性阈值是平台必须满足的最低可用性（默认值为 80%）。此外，ORTT 应用程序还使用让分，该值允许客户在全球或本地影响最终用户的路由方式。

前三个步骤（基本信息、配置和平台信息）的输入方式与其他应用程序相同。

按照以下步骤配置位置信息，并为每个平台、全球或按位置/市场输入让分值。

位置配置

1. 在位置配置对话框中，为一个或所有选定平台的让分输入一个值。您可以输入介于 0 和 6000 之间的让分值。让分的用途是在成本或便利性方面有更好的平台可用时，手动降低选择特定平台进行路由的机会。让分越多，平台被选中的机会就越小。如果需要，可以通过关闭平台 选择按钮来取消选择平台。
2. 点击 市场和国家**/**地区，从列表中选择一个特定的市场或国家/地区，并分别为每个关联平台输入让分值。
3. 点击 完成，完成应用的配置。
4. 在确认弹出窗口中，单击“完成”或“发布”以查看 Openmix 应用程序列表页面上列出的应用程序。如果单击“发布”，您的应用将立即上线并显示为绿色状态。您的应用程序已投入生产。如果单击“完成”，您的应用程序仍会列在“应用程序”页面上，但未发布，其状态为红色。

吞吐量

吞吐量 应用程序根据声纳数据（如果启用了 Sonar）、最高吞吐量（使用 Radar 数据）和平台可用性阈值（默认情况下为 80%）来选择平台。此外，此应用程序允许您添加让分值，以降低特定平台的吞吐量并影响最终用户的路由方式。这个可选的让分值可以在全球和/或本地（针对特定市场或国家/地区）分配。

前三个步骤（基本信息、配置和平台信息）的输入方式与其他应用程序相同。位置配置 的输入方式与在 ORTT 应用程序中的输入方式相同。

完成后，单击“完成”以返回 Openmix 应用程序列表页。最后，单击“发 布”以在您准备上线时发布您的应用程序。

申请的状态

应用程序的状态显示其当前配置。

- 红色代表未发布。完成配置后，如果单击“完成”，应用程序页面中将以红点列出您的应用程序，表示该应用程序尚未发布。
- 绿色代表已发布。如果单击“发布”，您的应用程序将立即上线，并用绿点表示，表示该应用程序已投入生产。
- 黄色代表未发布的最新版本。黄点表示应用程序已创建和编辑，上次修改的设置尚未发布。

静态接近

静态邻近应用程序响应位于请求用户纬度和经度附近的平台。

> 注意：
>
> 所有 Openmix 应用程序都需要事先设置一组关联的平台。如果未在列表中找到平台，则可以在门户的平台页面中进行设置。

导航

1. 登录到 NetScaler Intelligent Traffic Management 门户。
2. 从左侧导航菜单中，导航到 **Openmix >** 应用程序配置。
3. 点击右上角的加号按钮“添加 **Openmix** 应用程序”。
4. 选择“快速启动应用程序”。

基本信息

1. 在“基本信息”对话框中，选择 **DNS** 作为协议。
2. 选择“静态邻近”作为“应用程序类型”。为应用程序提供名称（必填字段）、说明（可选字段）和标记（可选字段）。
3. 单击下一步进行配置。

配置

1. 如果启用，可用性阈值 的默认值为 80%。输入新值以替换默认值。
2. 输入 CNAME/A/AAAA 或 IP 地址进行回退。如果应用程序遇到问题或错误，通常使用备用 CNAME/A/AAAA 或 IP。此字段不能为空。
3. 为响应输入 **TTL**（生存时间）。默认值为 20 秒，但如有必要，可以覆盖此值。
4. 单击“下一步”查看持久性控制。

持久性控制　设置 本地持久性。有关更多信息，请参阅 本地持久性。单击“下一步”获取平台信息。

平台信息　每个平台都必须通过“平台”页面设置其纬度和经度。社区平台的别名最初是从社区平台继承地理信息，但在创建别名后您可以更改它们。私有平台需要在创建时或之后通过其配置窗格进行设置。要查看配置窗格，只需单击表的平台条目即可。

只有属于以下类别的平台才能拥有地理信息并成为 opx 应用答案列表的一部分：

- 云计算
- 云端存储
- 数据中心

1. 从“平台”列表中选择一个 平台。
2. 输入平台的 CNAME、A/AAAA 记录或 IP（在 DNS 中）或 URL（在 HTTP 中）。它必须是有效的 URL、主机名或 IP 地址。它的形式可以是：

   ```
   scheme:[//host[:port]][/path][?query][#fragment]
   ```

3. 确保选中“已启用”复选框，表示平台已启用，然后再进行下一步。
4. 如果 Sonar 可用于此平台，并且您希望在 DNS 解析过程中考虑使用 Sonar 数据，请务必单击“使用 **Sonar** 获取平台可用性”复选框。
5. 您可以通过单击“添加平台”来 添加更多平台。
6. 单击“下一步”进行 位置配置。

位置配置

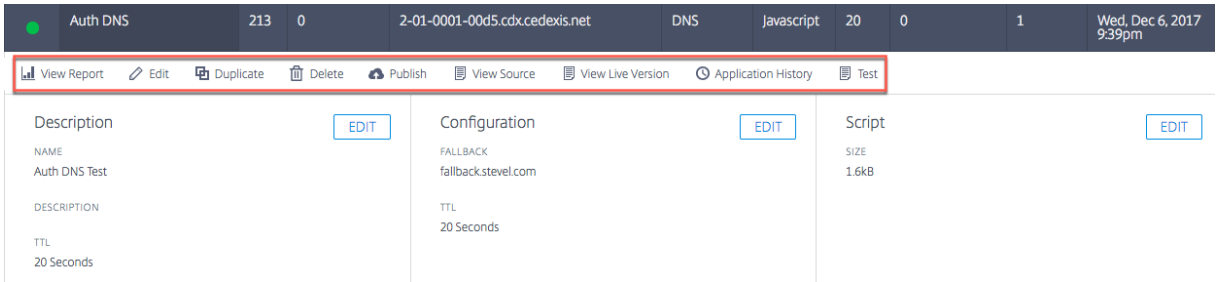
1. 在“位置配置”对话框的“全局”部分中，可以为全局路由设置平台链。您可以全局启用或禁用对每个平台的选择。
2. 在市场和国家/地区中，您可以为每个市场或国家/地区创建不同的设置，从而有效地为它们制定地理围栏规则。
3. 单击“完成”以创建应用程序。

在确认弹出窗口中，单击“发布”、“添加另一个”或“完成”：

- 如果单击“发布”，您的应用将立即上线，并且状态为绿色。这意味着该应用程序已投入生产。
- 如果单击“完成”，您的应用程序将在 Openmix 页面上列出，但未发布，状态为红色。
- 如果单击“添加另一个”，则应用程序的状态与“完成”相同，但您需要重新启动相同的过程来创建新应用程序。

管理快速入门应用程序

使用应用程序管理器面板中的顶部选项卡编辑、复制、删除、测试、查看报告、查看源代码和查看应用程序的版本历史记录。在 Openmix 应用程序列表页中单击您的应用程序以展开应用程序管理器。



查看报告

查看报告 将带您进入 Openmix 决策报告页面，在该页面中，您可以查看每个应用程序、平台和地理位置的 Openmix 决策趋势。

编辑

要编辑您的 Openmix 应用程序，只需单击应用程序管理器面板顶部的 编辑 图标即可。您还可以通过单击面板中的“编辑”按钮，分别对基本信息、配置、平台或位置信息执行单独的 编辑，如图所示。完成编辑后，单击“完成”以列出处于未发布状态的应用程序（稍后可进行更多编辑），或单击“发布”立即上线。

重复

单击“复制”可 复制 当前应用程序的配置并使用新名称进行保存。

Delete

单击“删除”以删除不再需要的应用程序。

发布

单击“发布”直接从 Openmix 应用程序管理器发布应用程序。仅当应用程序尚未发布时，此选项才可见。

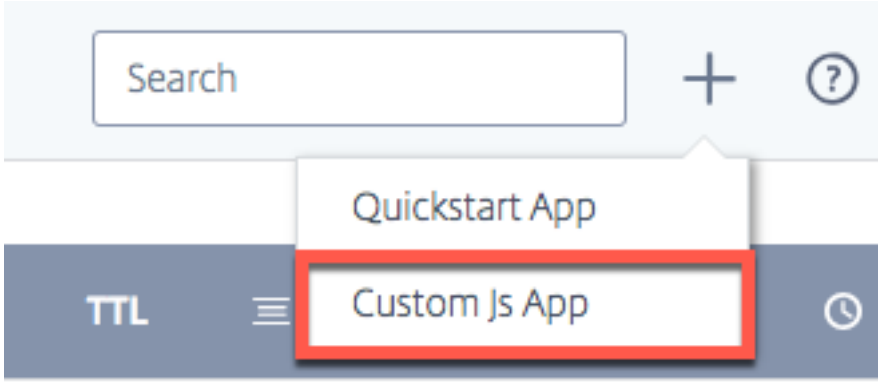
Openmix 自定义 JavaScript 应用程序

Openmix JavaScript 应用程序是带有可自定义的 Java 您可以使用 ITM 门户中的 UI 进行创建、配置、测试和发布。

注意：本指南不涵盖自定义脚本的实际创建（语法、变量等）。有关创建自定义 JavaScript 的更多信息，请参阅 开发者交易平台。

导航

1. 登录 ITM 门户。
2. 从左侧的导航菜单中，转到 **Openmix**。
3. 选择 应用程序配置。
4. 要配置新的 Openmix 应用程序，请单击右上角的添加图标。
5. 选择 自定义 **JS** 应用程序。
6. 此时 将打开 **Openmix** 应用程序配置 页面。



基本信息

1. 应用程序名称：为您的应用程序命名。
2. 说明: 在此处为应用程序提供说明或添加发行说明。这是一个可选字段。
3. 标签：如有必要，请输入相应的标签。标签有助于识别和整理您的应用。这是一个可选字段。
4. 协议：选择 DNS 或 HTTP 作为协议。
   - **DNS**：如果选择 DNS，则必须输入 TTL 值。
   - **HTTP**：如果选择 HTTP，则可以启用 安全访问。
5. **TTL**：输入应用程序的 DNS 生存时间。建议的值为 20 秒。注意：如果自定义 JS 应用程序未设置 TTL 或者响应是后备值，则此 TTL 适用。
6. 回退:输入 CNAME/A/AAAA 或 IP 地址进行回退。如果应用程序遇到问题或错误，通常使用备用 CNAME/A/AAAA 或 IP。
7. 安全访问：如果启用了 安全访问，则 HTTP API 在调用时必须要求客户端提供 Oauth 访问密钥。要了解更多信息，请参阅 保护 Openmix HTTP API。

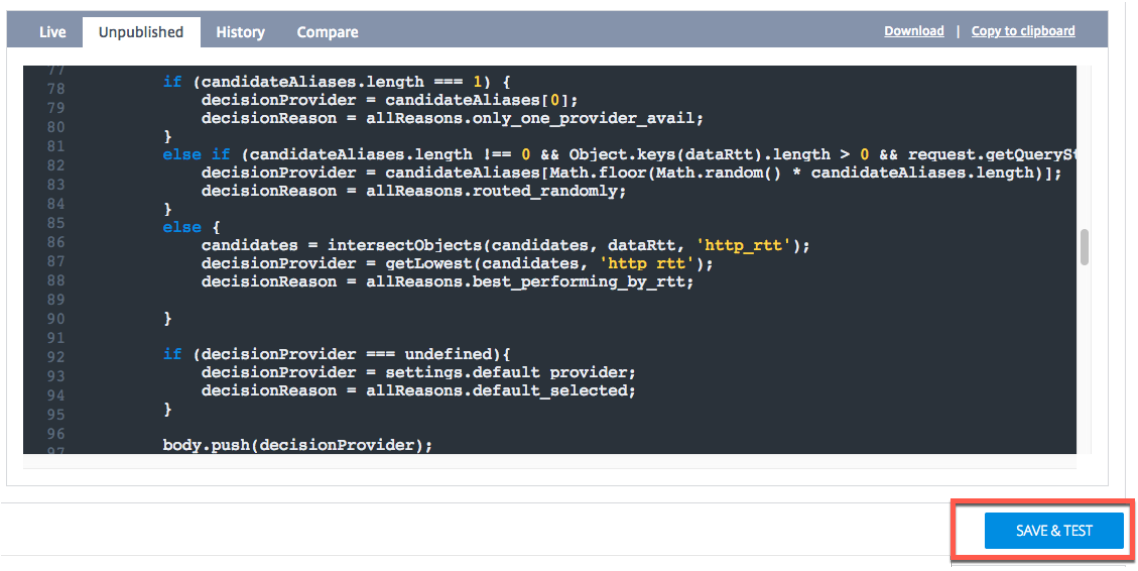
   注意：启用安全访问后，Openmix 首页上应用程序列表中的应用程序名称旁边会显示一个锁形图标。

自定义 **JavaScript**

输入配置信息后，您就可以上传自定义 JavaScript 了。

1. 单击“选择文件”按钮，然后选择要上传的 JavaScript 文件。您可以随时上传新文件以覆盖现有文件。
2. 单击“保存并测试”以保存您的应用程序。

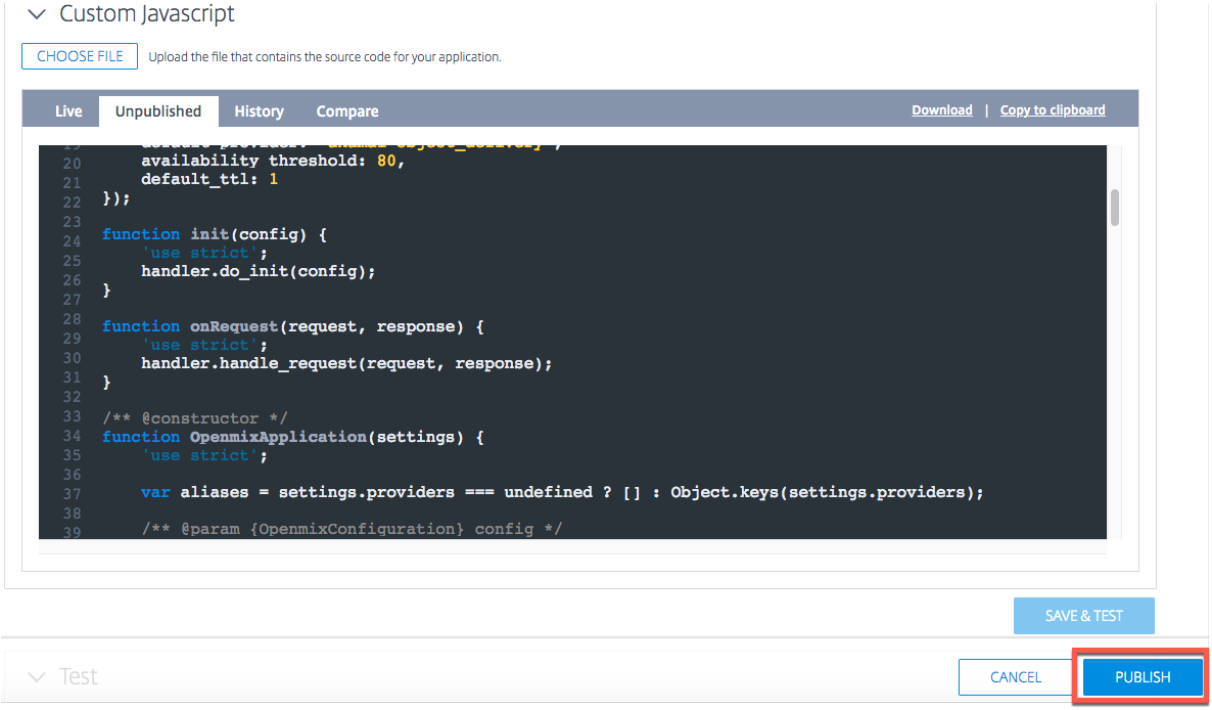
   注意：应用程序在上传和保存时，会使用应用程序检查器自动对其进行测试。如果存在错误，应用程序检查器会显示错误信息和错误的位置。有关应用程序检查器中可用数据的更多信息，请参阅 应用程序验证 部分。



3. 单击“取消”返回“Openmix 应用程序”页面，如果应用程序已准备就绪，请单击“发布”。

   注意：如果单击“发布”，您的应用将立即上线并显示为绿色状态。您的应用程序正在生产中。

   如果单击“取消”，您的应用程序将列在应用程序页面上，但未发布，状态为红色。要了解有关状态的更多信息，请参阅应用程序状态部分。



分阶段部署应用程序

您可以通过新版本（有时称为 Canary Deployment）发送一小部分网络流量，从而管理应用程序的推出。ITM 允许您将指定百分比的流量发送到新版本的应用程序，以确保应用程序逻辑按预期运行。您可以报告现有版本和新版本的行为，以评估在实时环境中对应用所做的更改。此选项允许您修复在通过新编辑的应用程序路由 100%的网络流量之前发生的任何问题或异常情况。验证所需的行为后，您可以增加流量到最新版本的百分比，或者将应用程序部署到所有用户。

要暂存应用程序部署并发布新修改的应用程序的测试版本，请执行以下操作：

- 单击应用程序名称（在 Openmix 应用程序列表页中）。应用程序管理器面板随即打开。
- 单击“编辑”图标以编辑您的应用程序。
- 修改现有应用程序，进行所有必要的更改。
- 完成编辑后，单击“保存并测试”。
- 使用“取消”和“发布”按钮在页面底部向下滚动。输入您希望流经此新修改版本的 Web 流量百分比（1% 到 99%）。
- 选中此复选框以通过此新版本的应用程序分配部分流量。剩余的流量将发送到以前的实时版本。
- 单击“发布”。该应用程序的这个新测试版本现在显示在 **Openmix** 配置 页面的应用程序列表中，并带有新的 状态 图标。新的 状态 图标表示只有部分网络流量通过此版本进行实时流动。

您可以将流量修改为测试版本并更改流量百分比以查看性能。

```
![Canary](/en-us/citrix-intelligent-traffic-management/media/openmix-jsapp-edit-canary.png)
```


要查看应用的性能，请前往 Openmix 决策报告。选择“应用程序”作为主要维，选择“版本”作为辅助维。从列表中选择您的应用程序后，单击“应用过滤器”。该图表显示了应用程序的不同版本的性能。

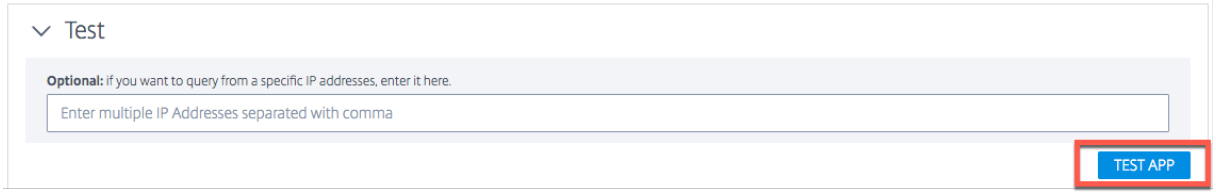
一旦您对这个版本的应用程序的性能感到满意，您可以通过点击“上线”按钮继续通过它路由 **100**%的网络流量。

此版本将当前的上线版本替换为新编辑的版本。

如果您不想使用此版本，请单击“取消发布”。您的更改将被保存，并在 **Openmix** 配置 页面的应用程序列表中显示为未发布的应用程序。现在，您的 100% 网络流量都通过应用的当前上线版本流动。

测试

您可以在发布之前或之后使用“测试 应用程序”按钮测试 您的 JavaScript 应用程序。

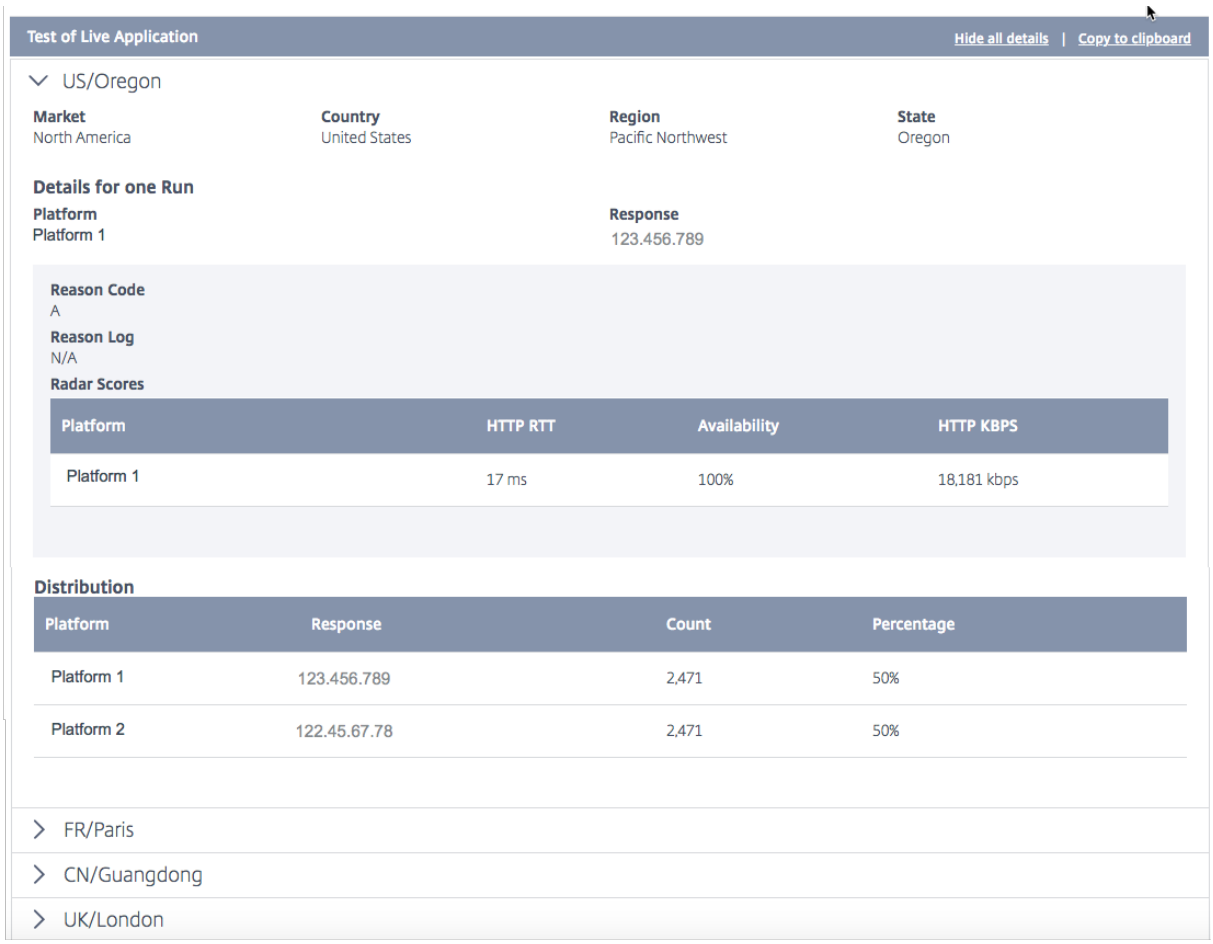


它使您能够查看特定市场、国家、地区和州的测试结果。您可以从特定 IP 地址查询应用程序。

测试结果包括：应用程序选择的平台、收到的响应、原因代码、原因日志、**Radar** 分数、分布等

此功能还允许您查看不同平台之间的决策分布。例如，如果使用两个平台进行路由，则可以查看每个平台的决策数量和收到的响应。

点击 显示所有详细信息 链接，查看应用的测试结果。



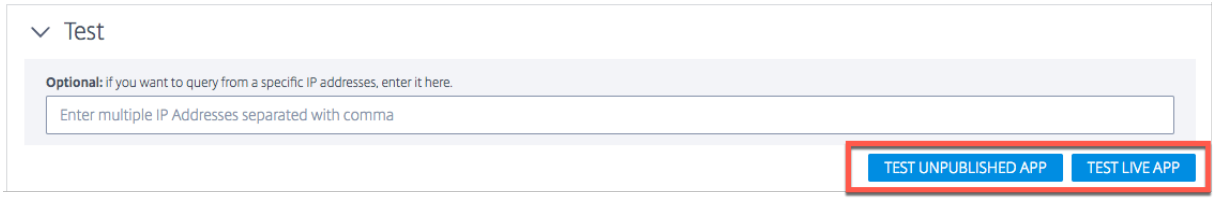
以下值显示为测试结果：

字段	说明
市场、国家、地区和州	测试应用程序的位置。
平台	应用程序选择的平台。
回应	应用程序选择的平台的 CNAME 或 IP 地址。
原因代码	说明决策背后的原因。
原因日志	来自应用程序的客户定义输出。使客户能够记录有关应用程序决策的信息。
Radar 得分	为平台记录的 响应时间 **(RTT)**、可用性和吞吐量 测量值。
版本	应用为每个测试位置选择的平台分布。计数 表示选择平台的次数。百分比 是平台选择总计数的百分比。

注意：您可以在上线应用程序或未发布的版本（即应用程序尚未发布）上运行此测试。

发布应用后，您可以选择通过单击“测试上线应用程序”选项来 测试上线应用程序。如果您编辑了应用程序或上传了新

版本，则可以在发布前点击 测试未发布的应用程序 按钮对其进行测试。



应用程序验证

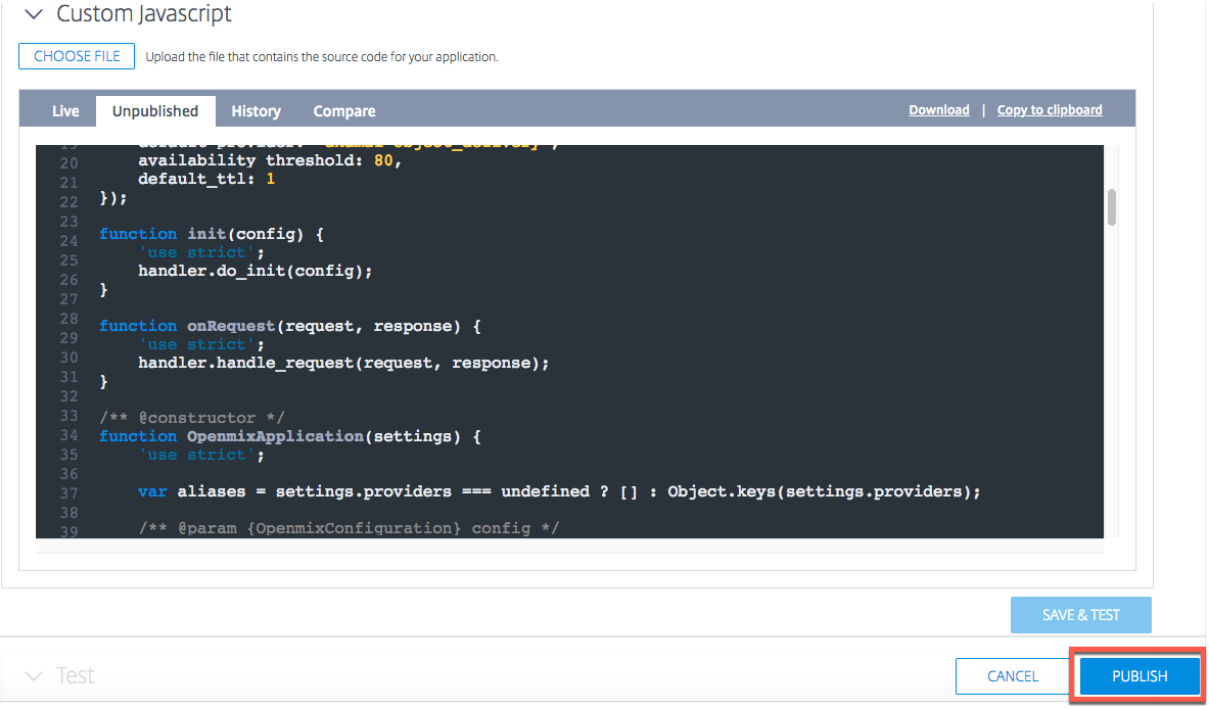
为确保自定义 JavaScript 应用程序按预期运行，请在将应用程序上传到 ITM 门户时通过代码和逻辑验证器运行该应用程序。应用程序验证程序通过具有合成流量的决策服务器运行应用程序，以测试应用程序是否成功编译和运行。

如果应用程序运行没有错误，则验证程序将提供有关决策分布和执行特征的信息。另一方面，如果决策服务器在运行应用程序时遇到错误，则验证程序会提供有关错误的信息。我们建议应用程序在发布之前必须没有错误。

如果出现错误，您可以在本地修复 JavaScript 文件，然后单击“选择文件”按钮将其重新上传到门户。

发布

要发布您的应用并使其上线，请点击 发布 按钮。如果应用程序尚未保存或已发布，则此选项将显示为灰色。当应用上线时，它将显示在 Openmix 应用程序管理器页面中为绿色状态。要了解有关应用程序状态的更多信息，请参阅应用程序状态部分。

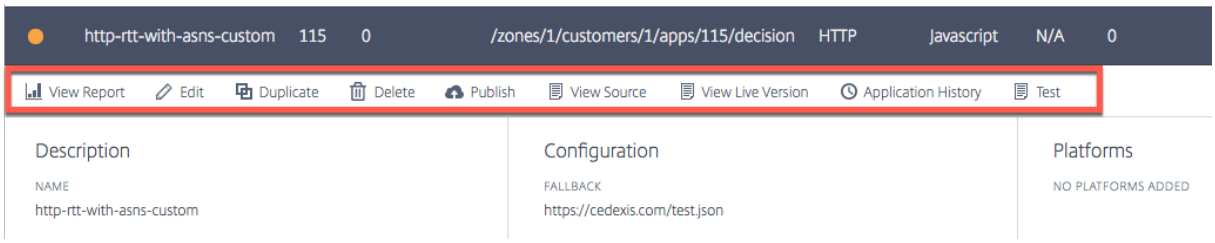


注意：如有必要，应用程序发布时会出现错误。

管理自定义 **JavaScript**

使用应用程序管理器面板中的顶部选项卡查看报告、编辑、复制、删除、发布、查看源代码、查看实时版本、查看历史记录。

在 Openmix 应用程序列表页中单击您的应用程序以展开应用程序管理器面板。

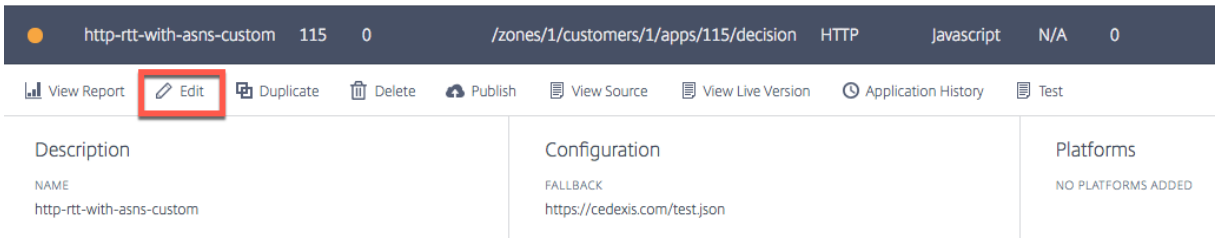


查看报告

查看报告 将带您进入 **Openmix** 决策报告 页面，在该页面中，您可以查看每个应用程序、平台和地理位置的 Openmix 决策趋势。

编辑

要编辑 Openmix 自定义 Javascript 应用程序，请单击应用程序名称（在 Openmix 应用程序列表页中）。应用程序管理器面板随即打开。可以通过单击“编辑”图标对配置进行更改和更新。



查看源代码

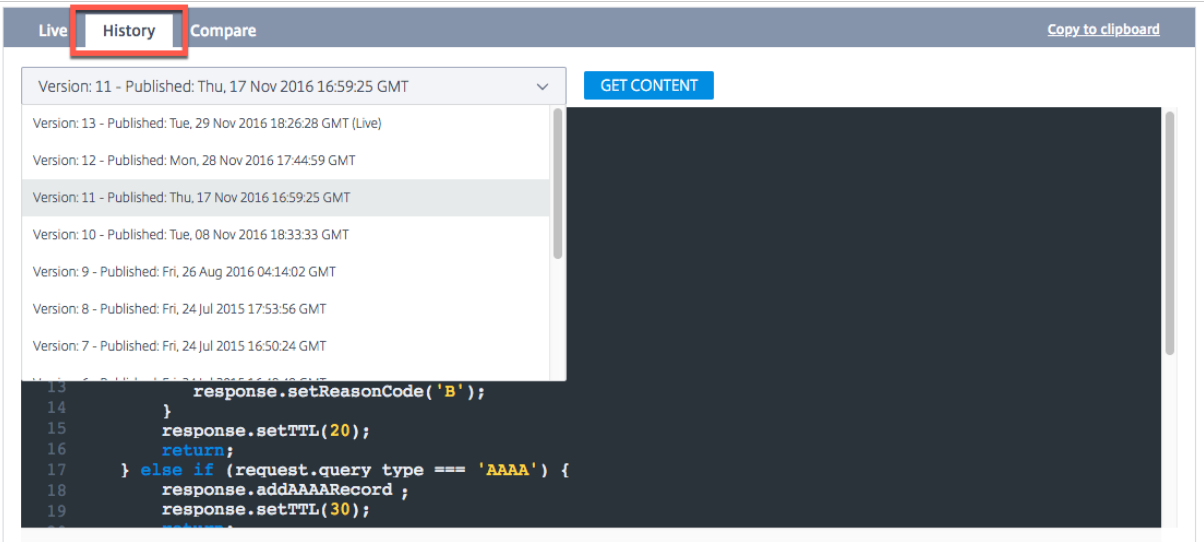
查看源代码 允许您查看应用程序的 JavaScript 源代码，即应用程序的最新版本是否已发布。此选项仅适用于自定义 JavaScript 应用程序。

查看直播版

您可以查看、复制和下载最新发布的应用程序版本。此选项仅适用于自定义 JavaScript 应用程序。

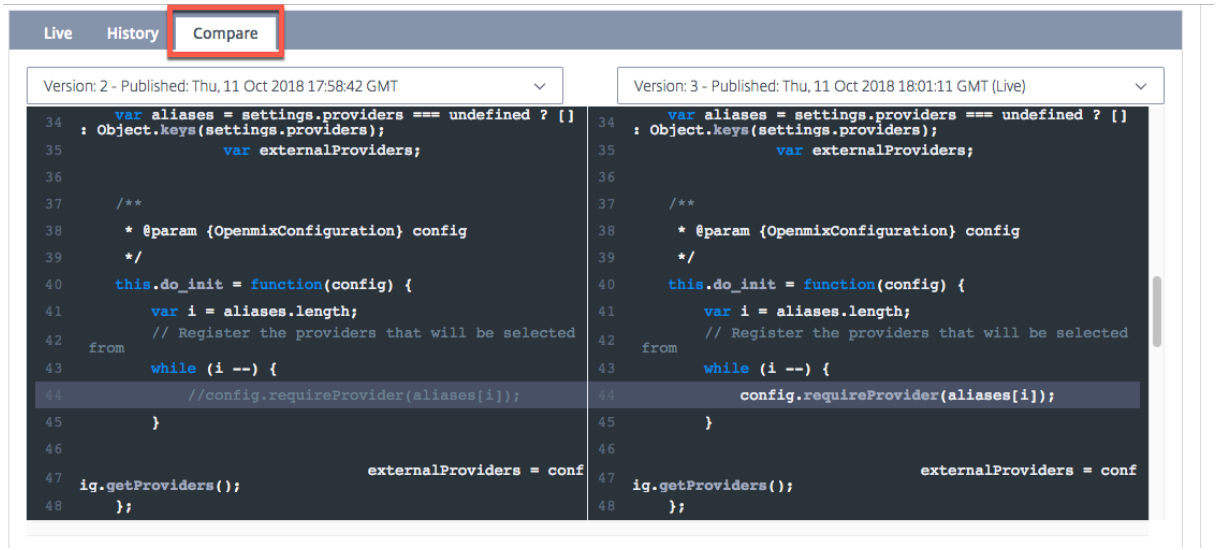
申请历史记录

应用程序历史记录 允许您查看应用程序的不同版本。您可以使用“选择版本”列表从实时版本切换到旧版本。单击“获取内容”以切换到旧版本。此选项仅适用于自定义 JavaScript 应用程序。



比较

“比较”功能允许您比较不同版本的 JavaScript 文件。您可以看到您的应用程序的两个版本之间的差异，并用突出显示的脚本行清楚地显示。



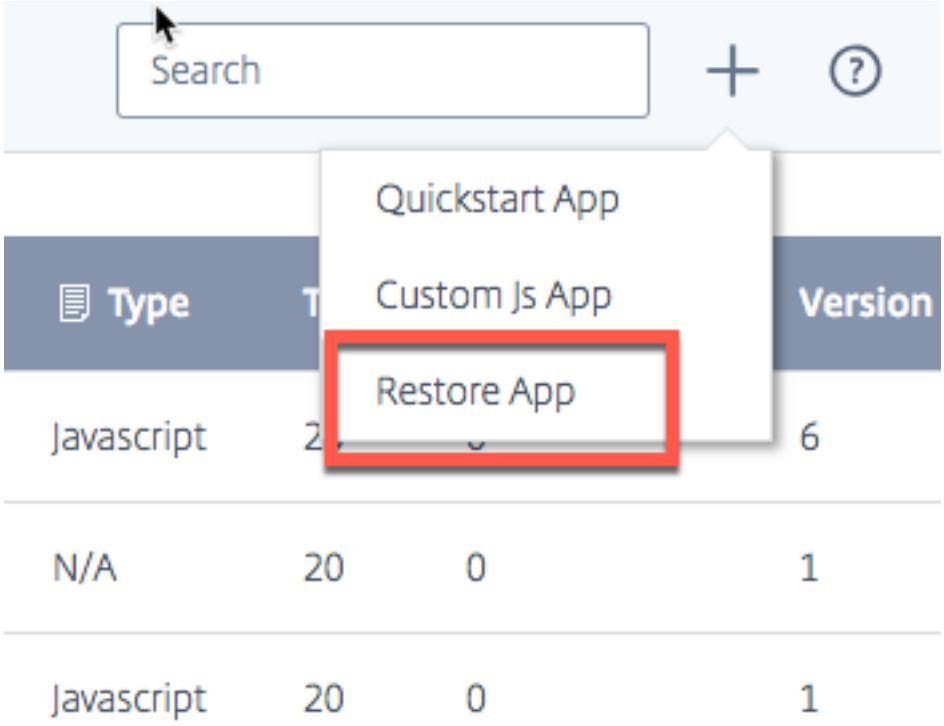
Delete

要删除 Openmix 应用程序，请单击应用程序名称（在 Openmix 应用程序列表页中）。应用程序管理器面板随即打开。单击“删除”图标，然后在确认对话框中选择“删除”按钮。该应用程序将从列表中消失。

还原应用程序

“还原应用程序”功能允许您在应用程序被删除后重新启用该应用程序。
要还原应用程序，请执行以下操作：

1. 单击页面右上角的 添加 **+** 图标。
2. 从下拉菜单中选择“还原应用程序”。将打开“还原应用程序”窗口。



3. 从列表中找到要重新启用的应用程序，然后单击其对应的“还原”按钮。

该应用程序将以相同的状态放回 Openmix 页面的列表中。

局部持久性

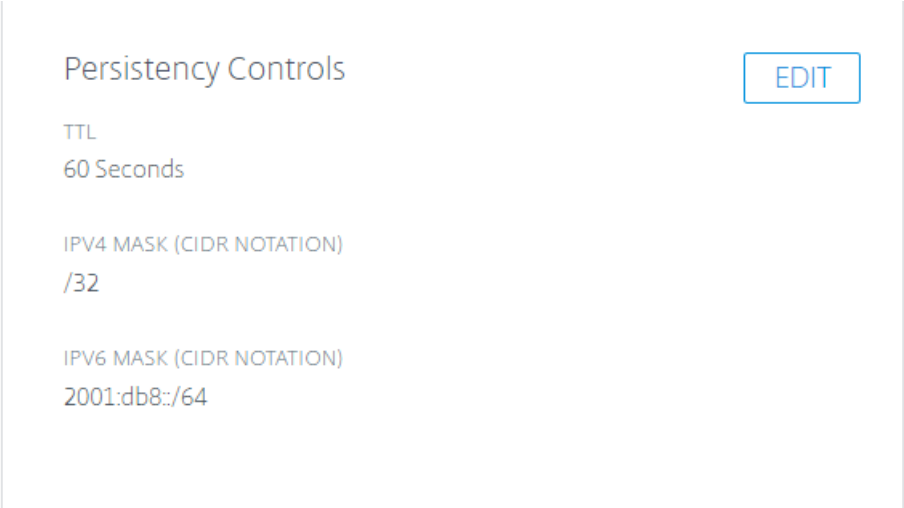
当为 Openmix 应用程序启用本地持久性功能时，该功能可提供决策粘性。这些请求使用 IP 子网掩码进行标识，其长度是可配置的。例如，当客户端在特定时段内向同一应用程序重复请求时，原始决策将被送回。当要求客户在特定会话期间不要在不同的决策之间跳动时，它可能是一项必不可少的功能。它可用于 DNS 或 HTTP Openmix 应用程序。

由于该机制的潜在自然限制，不能保证 100% 的请求都具有持久性。相反，采用了尽力而为的方法。测试表明，预期的持久性精度在 95-97%之间。

> 注意：
>
> 要为您的帐户启用“本地持久性”功能，请开立支持票证或联系您的客户成功经理。此外，还需要一个预测型 DNS 区域，该区域配置了名称服务器 `ns5.cedexis.net` 和 `ns6.cedexis.net`。考虑一下 DNS 区域更新可能需要很长时间才能在 Internet 上传播。

配置

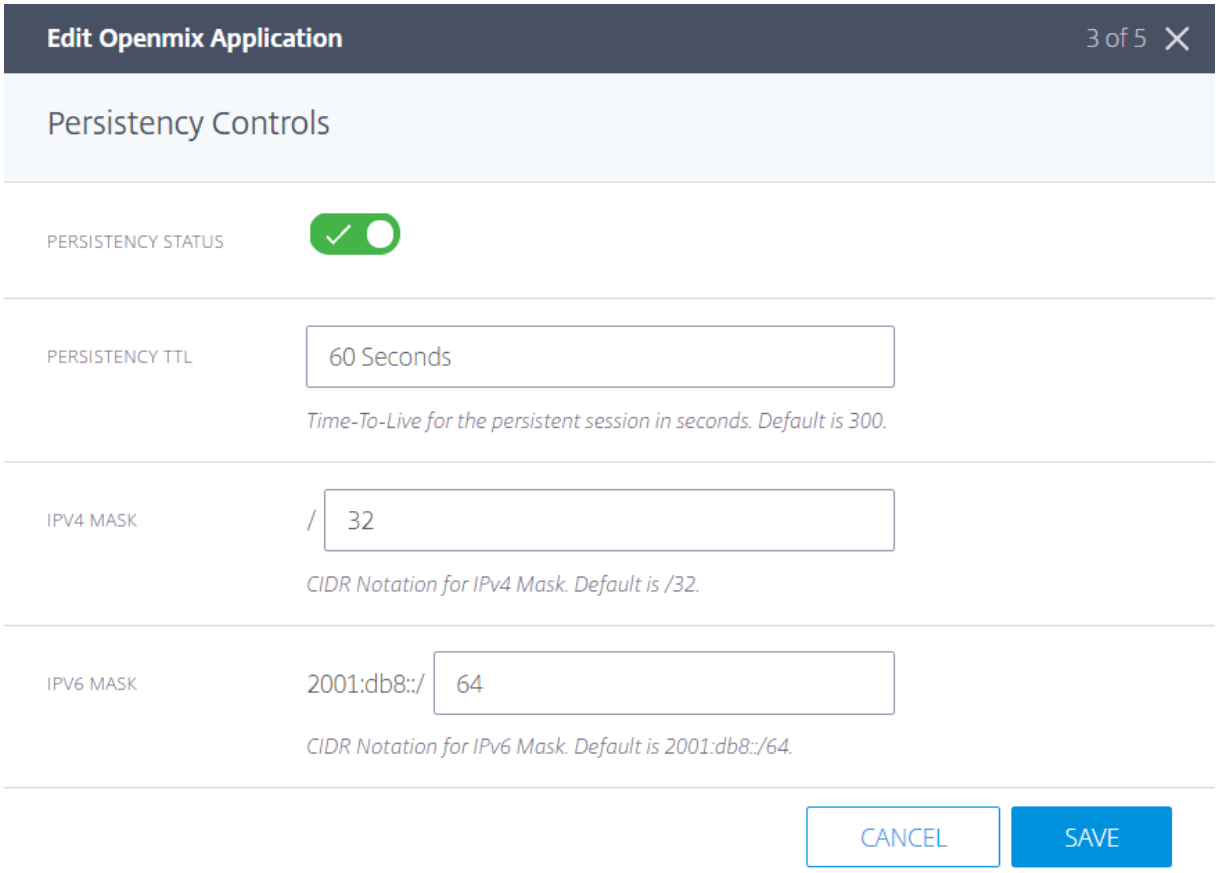
要启用本地持久性，请在 Openmix 应用程序选项下选择“持久性控制” > “编辑”。



可用设置如下所示：

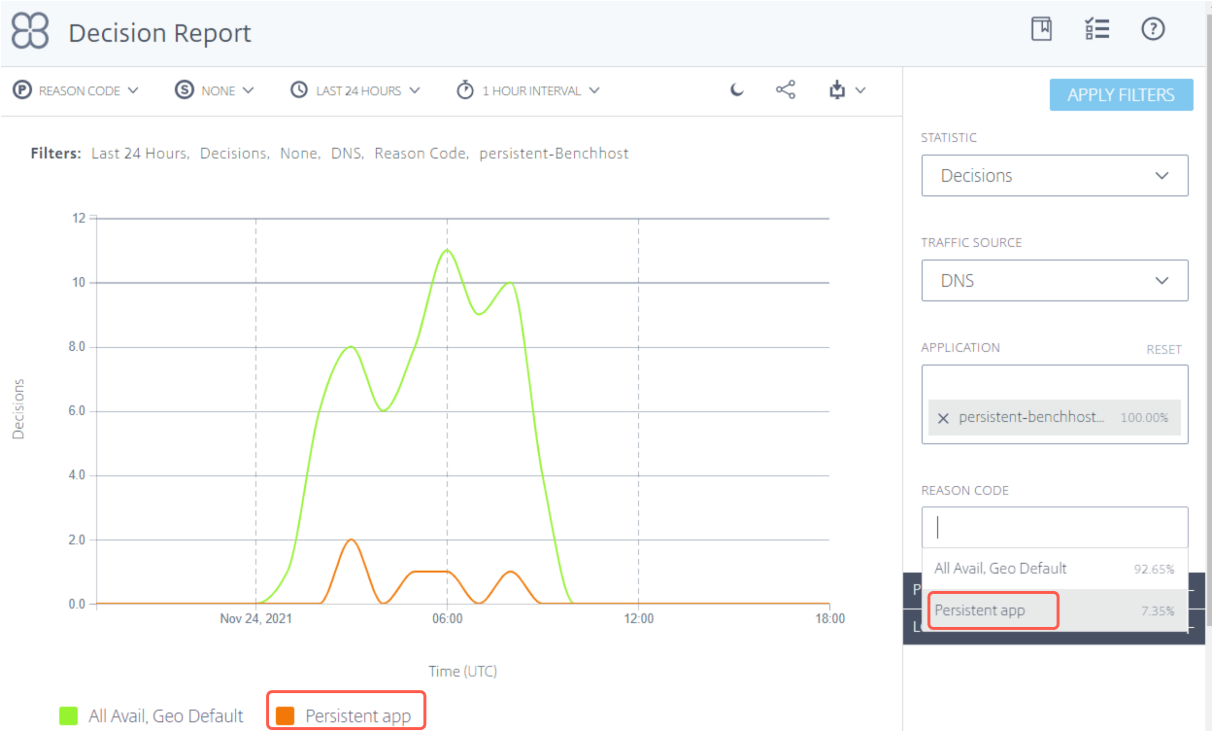
1. 在“配置”对话框中，输入“持久性 **TTL**”。默认选项为 300 秒。允许值介于 60 和 1440 之间。发出初始请求后，所提供的 DNS 决策最多保留 300 秒。如果另一个请求在到期前来自系统中的同一 IP 子网范围，则会做出同样的决定。
2. IPv4 和 IPv6 掩码均用于设置持久性粘性的粒度。IPv4 和 IPv6 的默认值分别为“/32”和“/64”。允许的值有：
   - /8 到 /32, 对于 IPv4
   - /32 到 /64, 适用于 IPv6

   对客户端 IP 地址的这种屏蔽决定了内部数据存储中使用的持久性密钥。例如，如果两个（或多个）客户端 IP 映射到同一个屏蔽的 IP 地址，则它们将获得相同的持久决策。



同样的设置在预测应用程序设置下也可用。

通过内部数据存储提供的 Openmix 决策在决策报告中使用原因代码 Pers **istent** 应用程序 进行报告。



运行状况检查

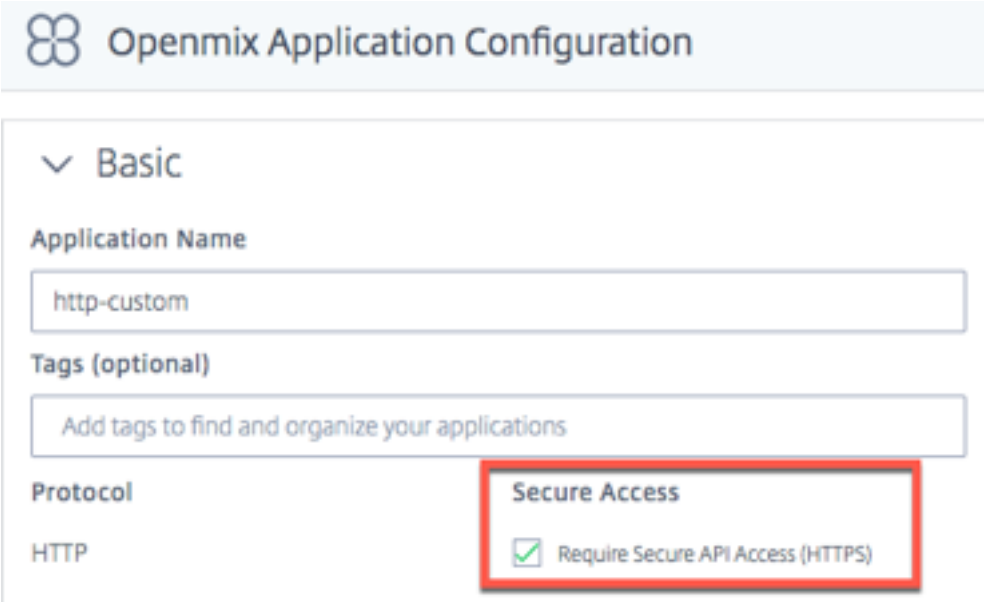
从持久性缓存中提供的决策在提供之前需要进行额外的运行状况检查：

1. 如果应用程序配置了 **Sonar** 可用性检查，则在执行缓存决策之前会检查 Sonar 可用性运行状况。如果 Sonar 报告平台“关闭”，则会忽略缓存的决定，并再次运行 OpenMix 应用程序。
2. 如果应用程序配置了 **Radar** 可用性检查，则在执行缓存决策之前会检查 Radar 可用性运行状况。如果平台的可用性低于配置的阈值，则会忽略缓存的决定。

> 注意：
>
> 对于持久性，Radar 可用性运行状况的最大阈值设置为固定的 10%。

保护 **Openmix HTTP API**

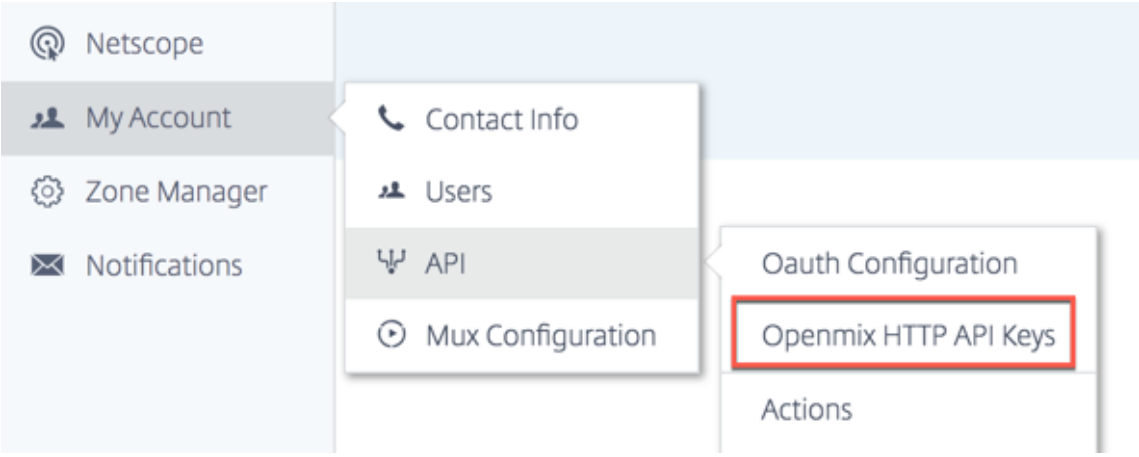
Openmix 可通过 DNS 或 HTTP API 获得，用于集成到非 DNS 工作流中。默认情况下，HTTP API 是通过纯 HTTP 调用的。也可以通过 TLS 和密钥身份验证来保护 API。通过选中“需要安全 **API** 访问 **(HTTPS)**”复选框即可通过 UI 完成。



创建 **API** 密钥

要启用密钥身份验证，请执行以下操作。

1. 在 Op **enmix** 应用程序配置 页面中选中 要求安全 **API** 访问 **(HTTPS)** 复选框，为每个应用程序启用安全访问。
2. 要生成安全访问密钥，请导航到 我的帐户 -> **API** -> **Openmix HTTP API** 密钥



3. 如果您是初次使用的用户，系统会提示您输入客户端 ID 以开始使用。在“新建客户端”对话框中输入您的客户端 **ID**，然后单击“完成”。
4. 在 **Openmix HTTP API** 身份验证配置页面上，客户端密钥显示在客户端 **ID** 旁边。
5. 现在，您可以使用基本身份验证向 Openmix 应用程序发出请求。使用您的客户端 **ID** 作为用户名，使用客户端密钥作为密码在浏览器上调用应用程序。

   要使用命令行调用应用程序，请使用以下 cURL 命令：


```
curl https://hopx.cedexis.com/zones/<zone>/customers/<customer_id
    >/apps/<app_id>/decision --user <client_key>:<client_secret>
<!--NeedCopy-->
```

注意：通过您创建的密钥，您可以访问任何 Openmix 应用程序。

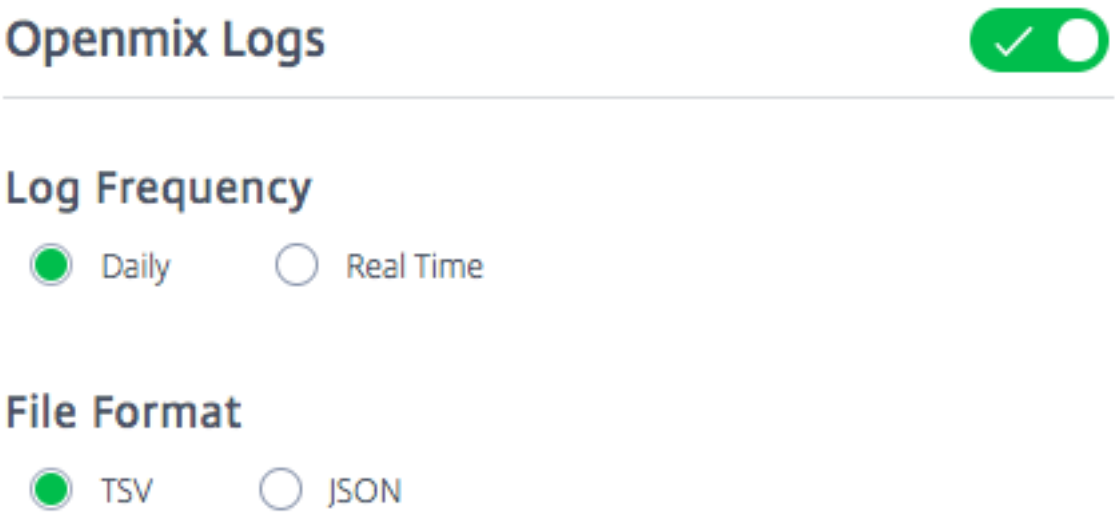
有关调用 Openmix HTTP API 的更多信息，请参阅 Openmix HTTP API 使用文档。

删除 **API** 密钥

1. 要删除密钥，请导航到 **Openmix HTTP API** 身份验证配置 页面。
2. 单击“客户端 **ID**”。
3. 在列表中选择“删除”。密钥已从系统中移除。它对身份验证或安全访问 Openmix 应用程序无效。

访问日志

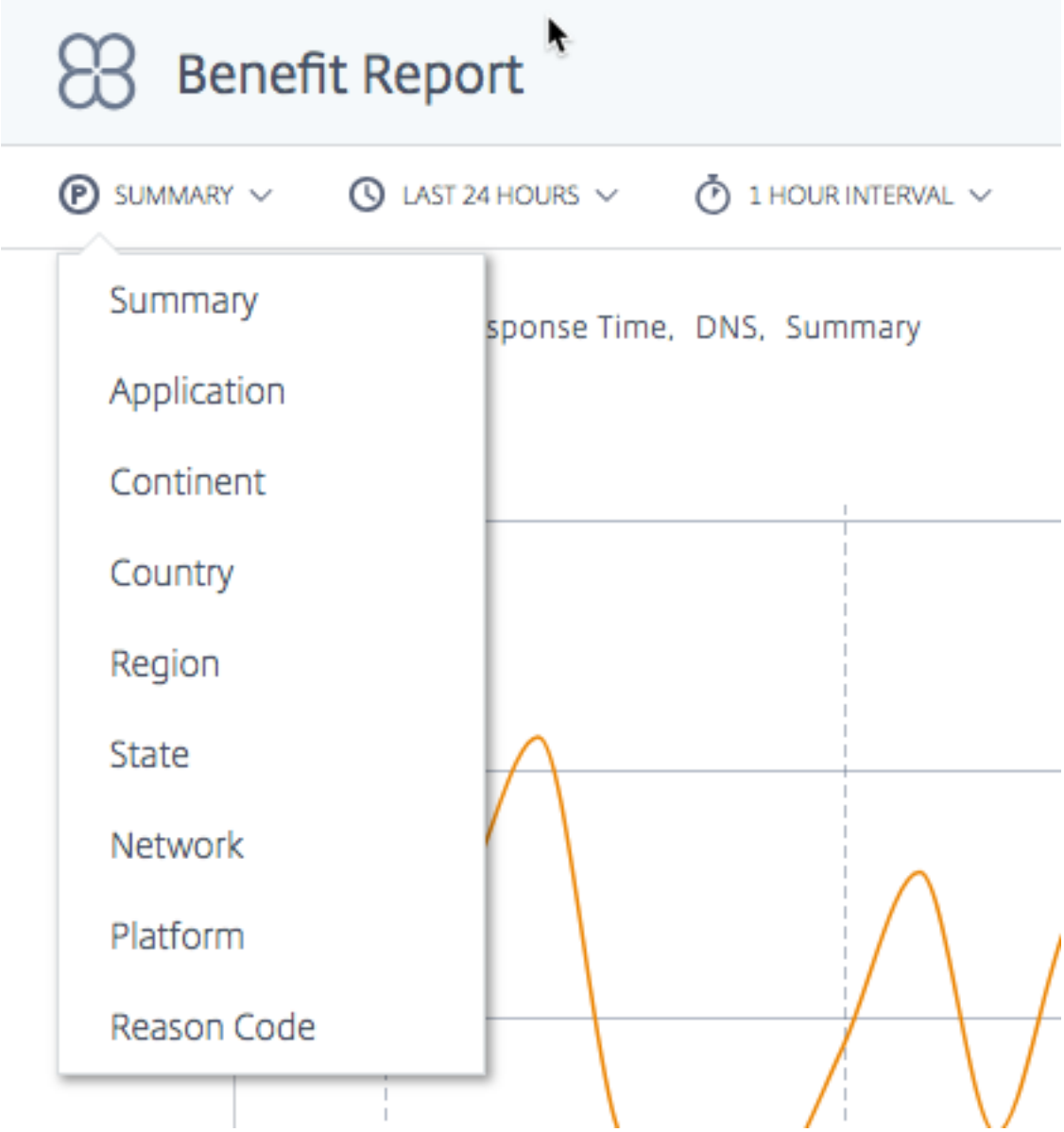
Openmix 制作的决策日志可以收集并可供安全下载。这些日志可以帮助您分析 Openmix 应用程序做出的决策和调试请求行为。日志可以在帐户级别打开/关闭并保护。有关如何启用和下载 Openmix 日志以及日志说明的详细信息，请访问 Netscope。



Openmix 报告

Openmix 报告为您的 DNS 或 HTTP 流量所做的 Openmix 决策提供了强大的可见性。每个报告都在以下部分中定义，但下面是有关报告的一些重要方面：

主要和次要维度

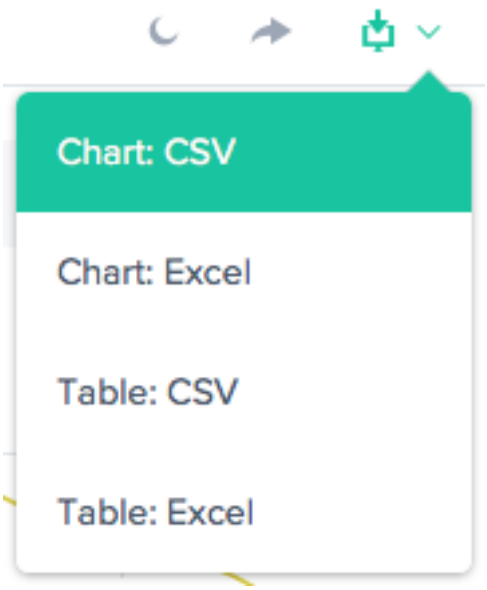


图表的主要维度是通过图表上方的列表选择的。使用它作为报告的强大透视视图。也可以选择次要维度来进一步完善报告。

可视化背景切换

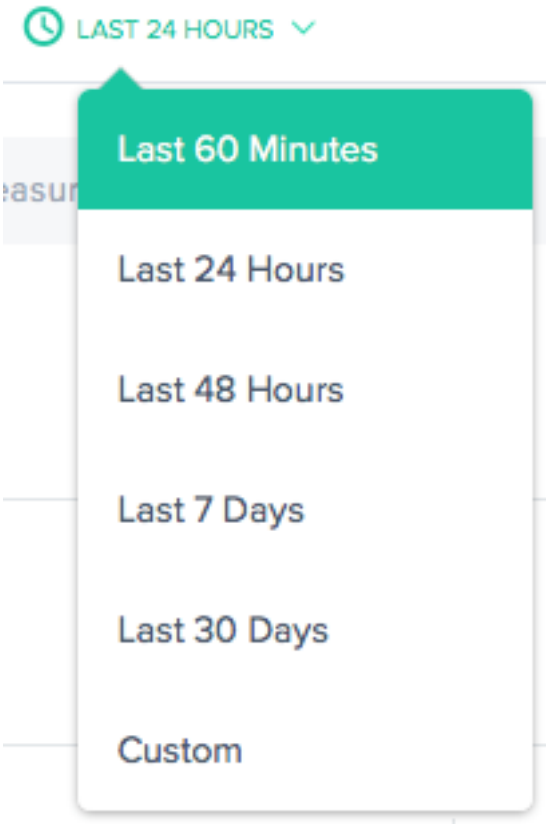
默认情况下，图表设置为白色背景。可以使用背景切换将背景切换为适合高对比度显示器的深色。

数据导出



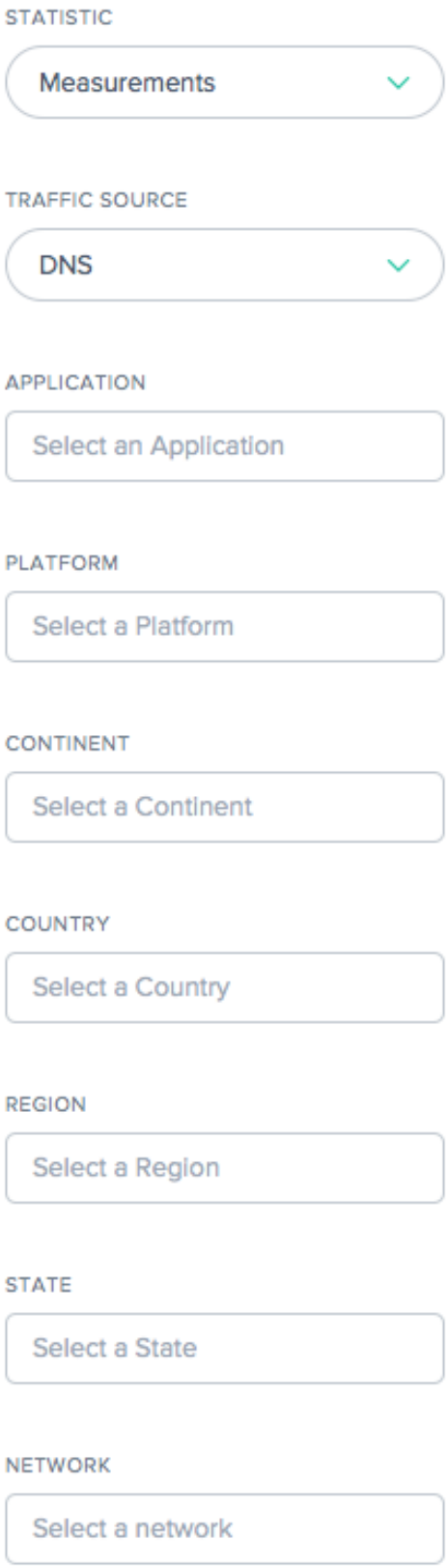
此外，最终用户可以通过报告顶部的下载链接下载图表和表格数据。

过滤器：报告时间范围



您可以生成时间范围为过去 60 分钟、24 小时、48 小时、7 天、30 天或自定义范围的报告。默认视图为“过去 24 小时”。

过滤器：强大的向下钻取功能



适用于报告的过滤器根据数据情况可能略有不同。以下是最常见的：

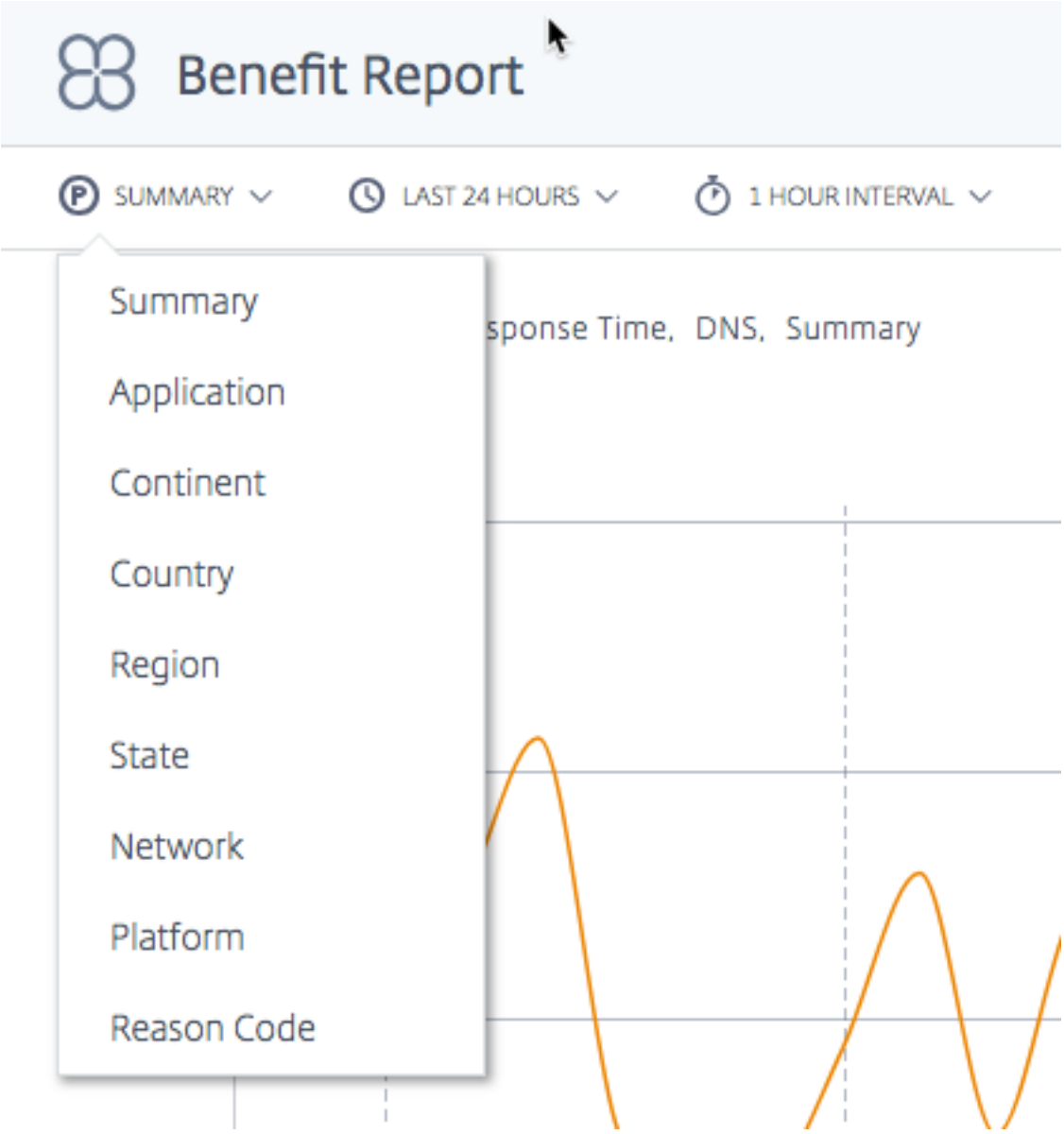
- 统计数据 -选择图表中显示的值，通常是决策数。
- 流量来源—选择要显示的流量类型：DNS 或 HTTP。
- 应用程序—选择一个或多个要显示的 Openmix 应用程序。
- 平台—选择要包括的一个或多个平台（提供商）。
- 大陆—选择要包括的一个或多个大洲。
- 国家/地区—选择要包括的一个或多个国家/地区。
- 区域—选择一个或多个要包括的地理区域（如果适用）。
- 州—选择一个或多个要包括的地理州（如果适用）。
- 网络—选择要包括的一个或多个网络 (ASN)。

福利报告

“益处”报告提供当使用 NetScaler Intelligent Traffic Management (ITM) 服务时，您的应用程序交付性能的总体改进。收益显示为响应时间和吞吐量提高的百分比。从候选平台池中选择一个特定的平台来生成报告。

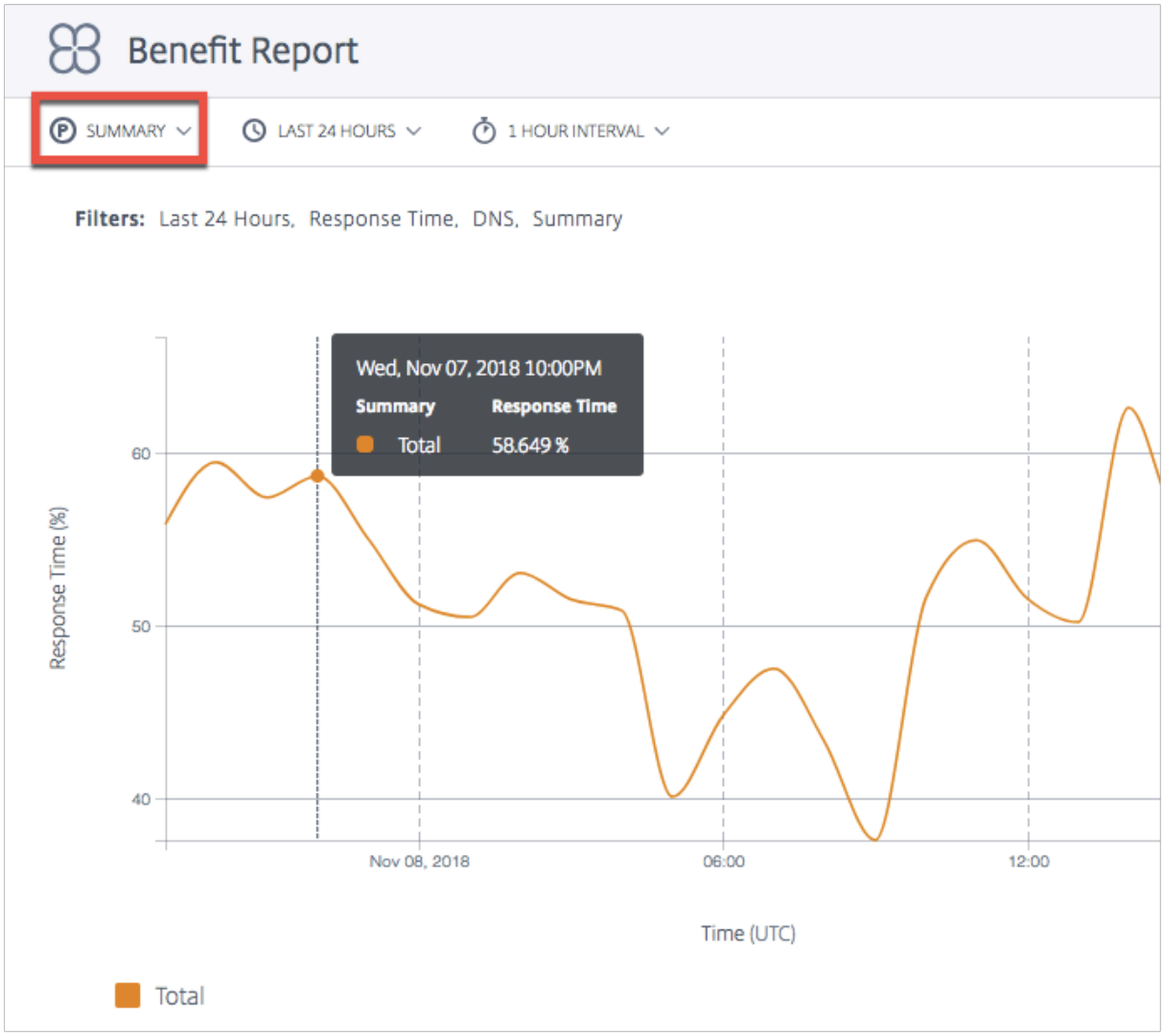
福利报告的主要维度

主要维度是显示收益报告的独立度量。以下各节详细描述了这些主要维度。



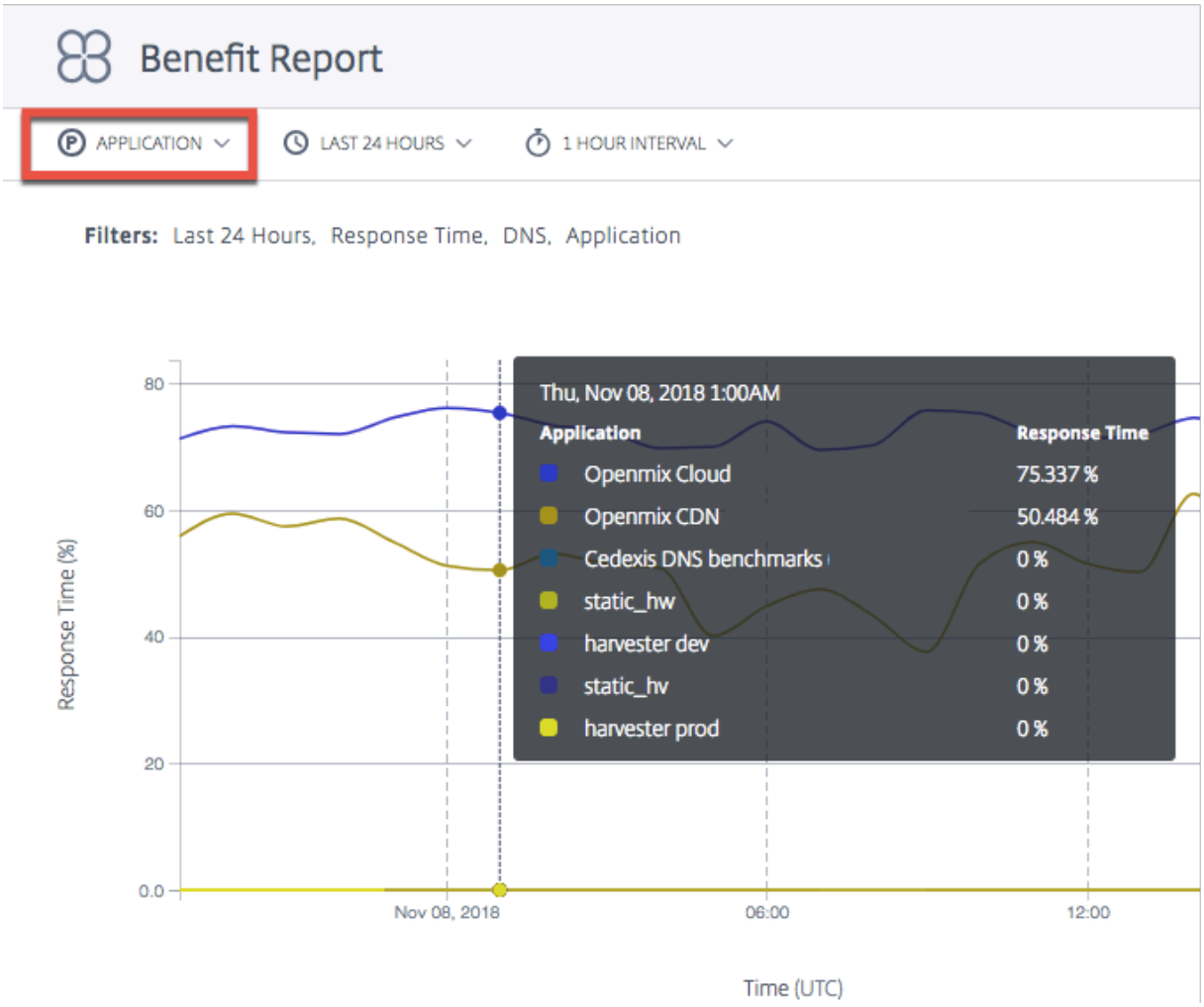
总结　摘要 是默认的主要维度。摘要图表显示了从所有应用程序获得的总收益百分比（以响应时间或吞吐量而言）的平均值。

注意：您可以使用 统计数据 过滤器在 响应时间 或 吞吐量 方面显示的优势之间切换。



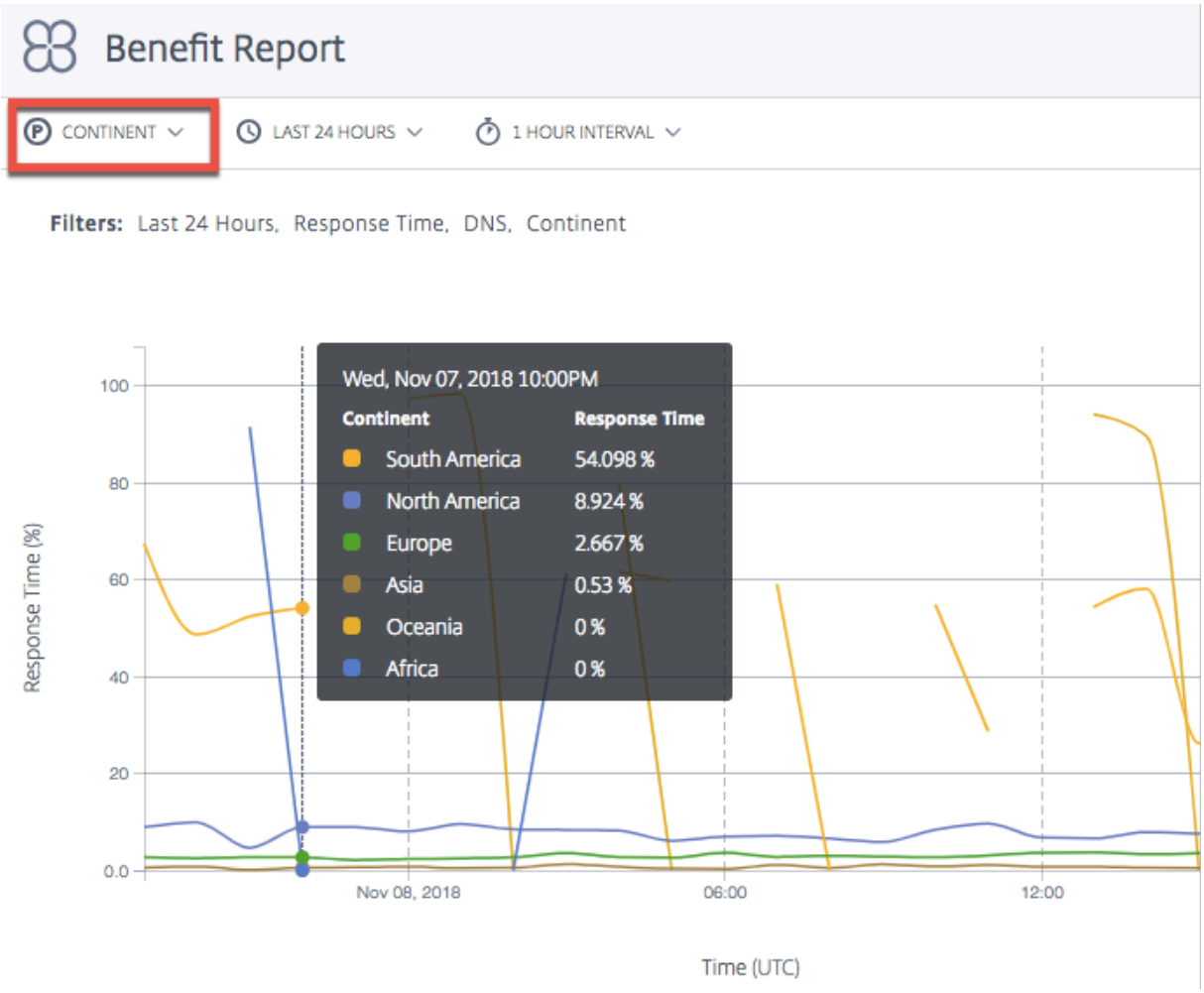
应用程序　当选择 应用程序 作为主要维度时，图表将显示每个应用程序和相应的性能（以响应时间或吞吐量而言），以选择某个平台优于其他候选平台的百分比收益。

注意：0% 表示选择一个特定平台而不是另一个平台没有额外的好处或改进。

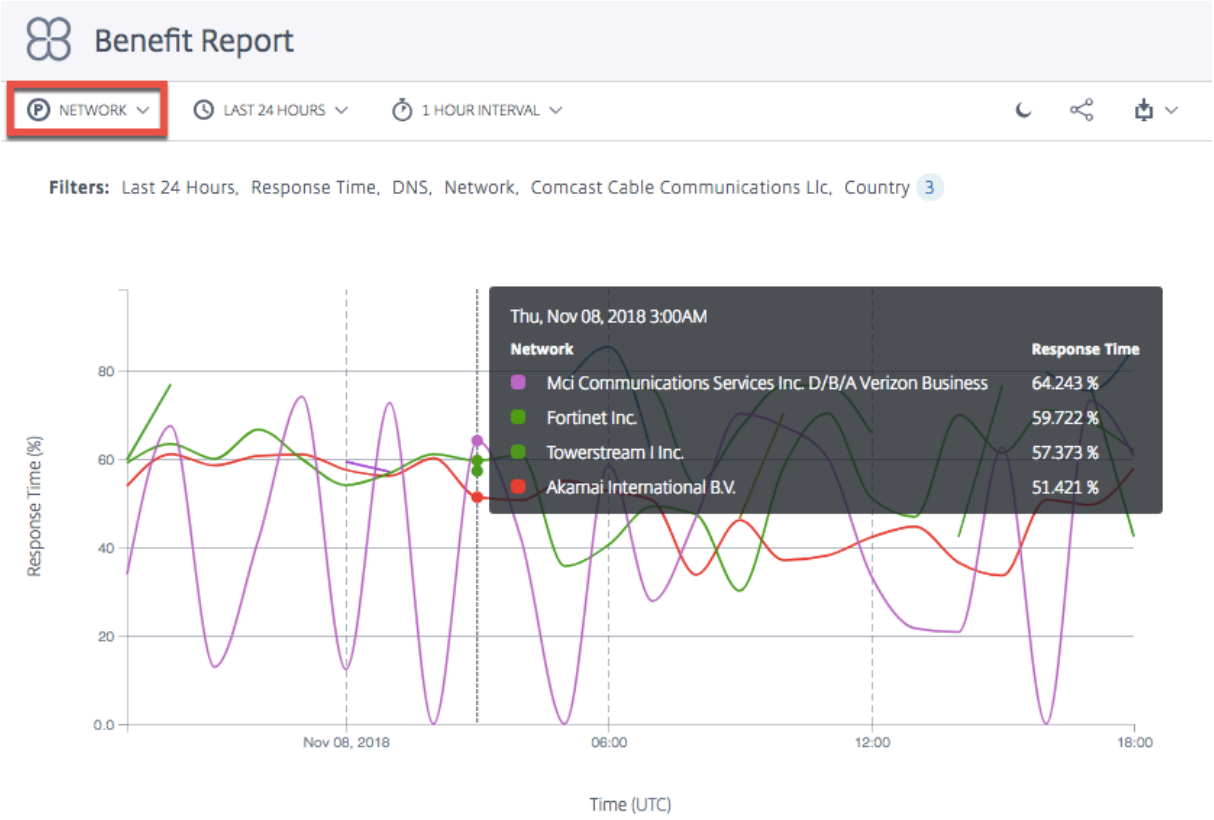


地点（大陆、国家、地区、州）　选择地点（大陆、国家、地区或 州）作为主要维度时，收益报告将显示每个地点的绩效改善总百分比（以响应时间或吞吐量而言）的平均值。您可以按大陆、国家、地区或州选择位置。

注意：由于地理位置规则或任何其他原因而不符合选择条件的平台不计入计算中。但是，将针对相关位置进行地理围栏的平台计算在内。

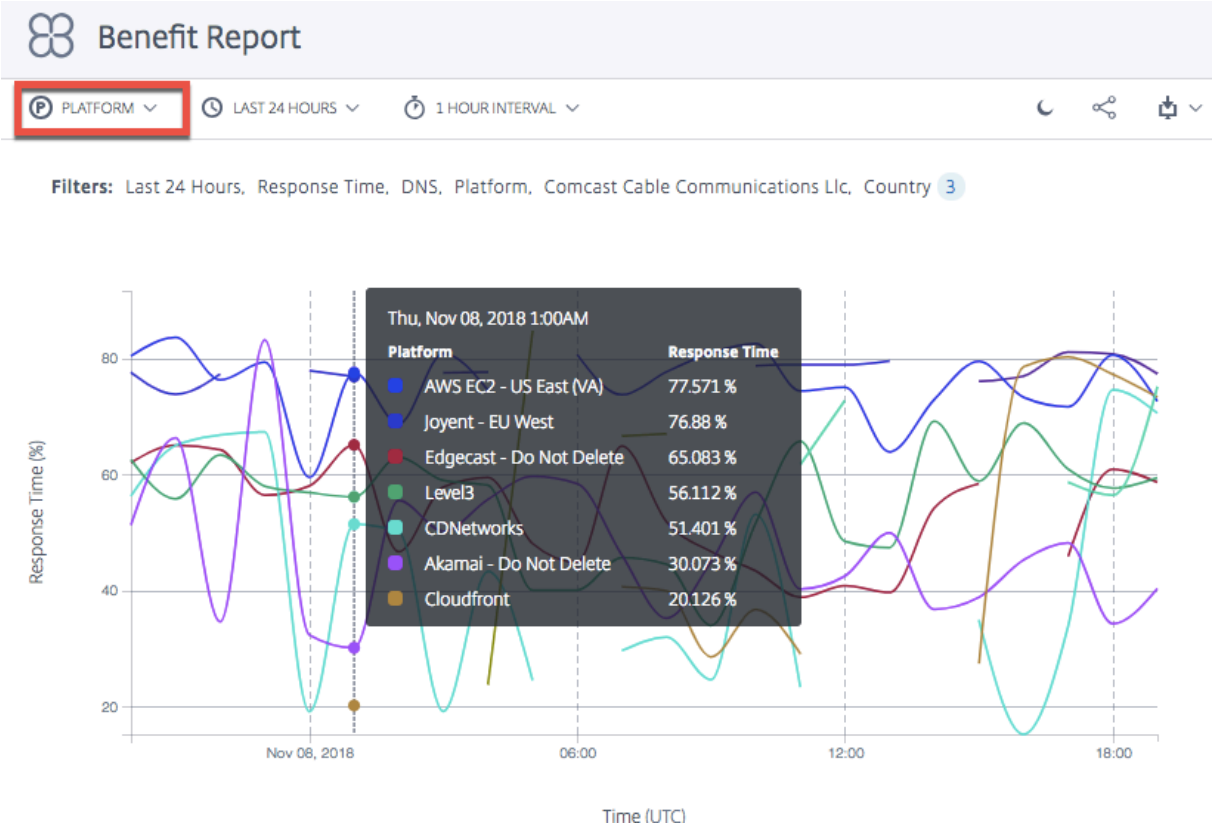


网络　选择“网络”作为主要维度时，您会看到分组到用户访问 ITM 的特定网络（或服务提供商）中的用户的性能提高百分比。它可以帮助您了解哪些用户组在来自这些特定网络时看到了性能优势。

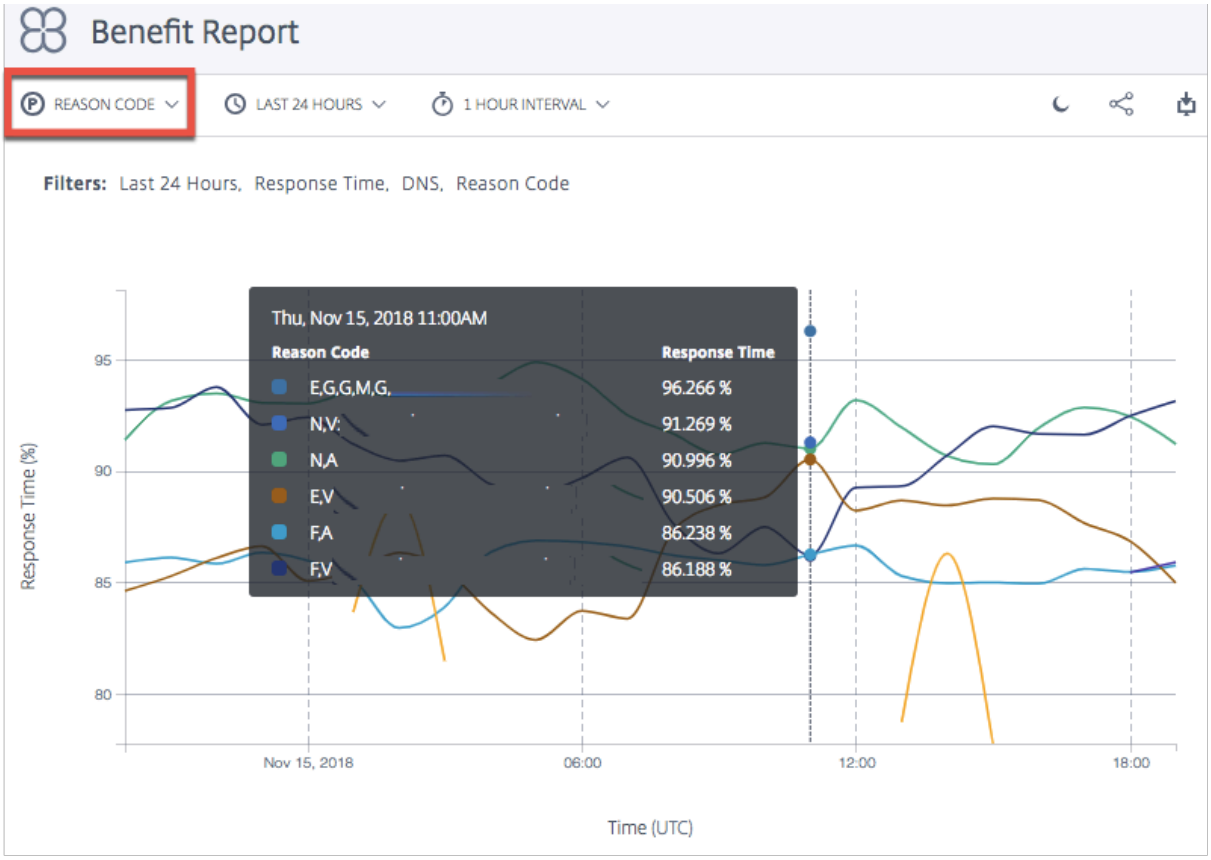


平台　当您选择 **Platform** 作为主要维度时，您会看到由不同应用选择的各个平台以及选择它们时相应的性能提高。改进的性能或优势在于响应时间或吞吐量（百分比）。

注意：应用选择该平台时显示的性能改善百分比。图表上的列表不一定表示这些平台之间的性能排名。



原因代码　选择 原因代码 作为主要维度时，图表中显示的百分比是针对特定原因代码做出决策时的总体平均收益。



忽略福利报告中的平台

为了提高收益报告的 **Openmix** 决策的准确性，您可以选择忽略某些平台，并将应用程序设置为仅从最适合比较的平台中进行选择。

例如，您的应用程序有五个平台可供比较——三个在欧洲用于欧洲流量，两个在美国用于美国流量。地理位置规则规定，欧洲流量必须通过欧洲平台，而美国的流量必须通过美国平台。

为确保使用三个欧洲平台进行计算，您可以将应用程序设置为忽略其他两个非欧洲平台。在您的 JavaScript 中使用 `ignoredProvider()` 方法。

该方法采用提供程序的别名（例如 `provider-1`、`provider-2`）作为输入参数（与 requireProvider() 方法非常相似）。每个别名必须调用一次 API。

在 `onRequest` 函数的 JavaScript 文件中使用以下示例代码：

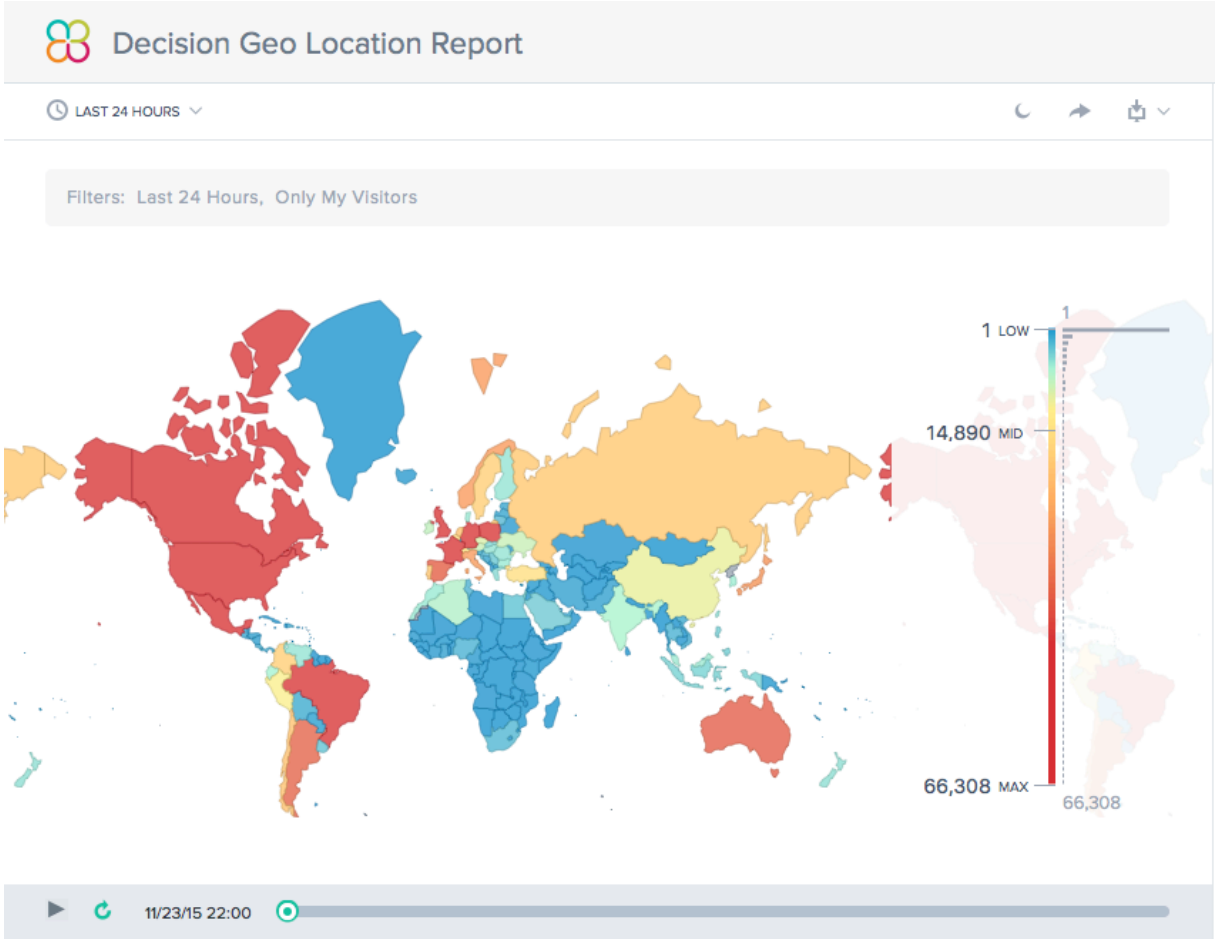
```
function onRequest(request, response) {

  response.ignoredProvider('provider-1');
  response.ignoredProvider('provider-2');
  response.setReasonCode('Ignoring provider-1 and provider-2');
  response.setTTL(this.__defaultTTL);
  response.respond('provider-3', 'cmg.test.fake.cname');
```



```
 }

<!--NeedCopy-->
```

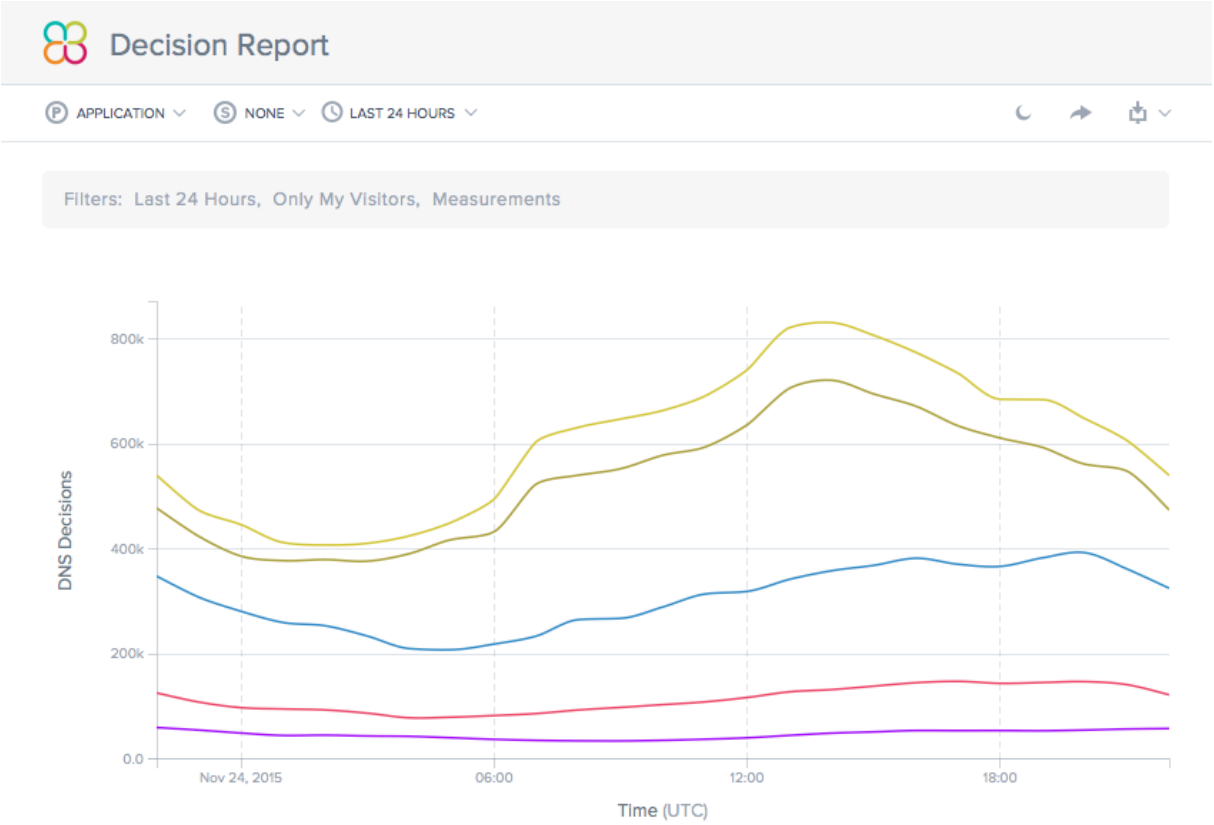
决策地理位置报告

此报告显示了每个国家/地区的 Openmix 决策量。通过选择图表底部的“播放”按钮，可以随时间查看此地图视图（基于为报告选择的时间范围）。



决策报告

此报告显示了每个应用程序、平台和地理区域的 Openmix 决策趋势。



预测性 **DNS**

September 22, 2023

概述

Predictive DNS 是一个基于机器学习的权威 DNS 平台，可管理您的区域并根据实时服务可用性做出路由决策。它具有高可用性，具有多个任播网络，可提供灵活可靠的路由规则。它是一款企业级产品，面向注重 DNS 决策流程质量的高级 DNS 客户。它适用于需要在可靠、高性能的基础结构上运行数据驱动的、智能的全局流量管理策略的客户。

Predictive DNS 支持创建主要区域和辅助区域。区域导入还支持最常用的记录类型，例如 A（IPV4 版本）、AAAA（IPV6 版本）、NS、SOA、CNAME、MX、PTR、SRV、SPF 和 TXT。我们还通过 Openmix 应用程序记录为 Openmix 客户提供无缝集成。一个区域中任意数量的 A/AAAA/CNAME 记录可以随时完全实现 OpenMix 智能化。客户还可以使用我们的 API 来驱动配置，在双主环境中运行 Predictive DNS。

Predictive DNS 和 **Openmix** 集成亮点

1. 在静态记录与复杂的数据驱动型流量管理策略之间无缝过渡，停机时间为零。
2. 完全可配置的流量管理策略（轮询、分布式、基于地理位置、基于网络，等等）。
3. 增加了对全球互联网流量、端点运行状况、基础结构状态、第三方供应商状态等的实时数据感知
4. 易于预配或修改流量管理。
5. 对请求活动进行深入分析和报告。

设置和委派区域的步骤

在登录 NetScaler Intelligent Traffic Management 之前，可查看下面的概要步骤，以帮助您了解如何设置和委派区域。

第 **1** 步：定义并创建您的区域

首先，创建一个与您公司的域名同名的区域。区域表示单个包含记录集合的父级域。它提供有关您希望如何为您的域及其子域进行流量路由的信息。如果您有来自当前 DNS 提供商的区域文件，请将其导入。使用导入的区域文件，您可以快速为您的区域创建所有记录。

第 **2** 步：添加并测试您的记录

您可以在 NetScaler Intelligent Traffic Management 门户的 Predictive DNS 控制台上手动创建记录，也可以导入包含所有记录的区域文件。当您导入区域文件时，Predictive DNS 会复制您的原始区域定义，迁移其中的所有现有记录。

您还可以使用 Predictive DNS API 以编程方式创建区域和记录。可以在门户中的我的帐户 **> API >** 配置 **> authdns** 下找到该 API。

Openmix 客户可以通过 Openmix 应用程序记录类型将现有 Openmix 应用程序映射到 CNAME 或 A/AAAA 记录。一个区域中任意数量的 A/AAAA/CNAME 记录可以随时完全实现 OpenMix 智能化。

要测试区域中的记录，您可以使用名为 dig 的工具来直接查询 DNS 服务器。使用您的区域名称作为参数运行 dig。例如：

```
dig @ns1.ourdomain.net NS mydomain.com
```

```
dig @ns1.ourdomain.net A host.mydomain.com
```

`@ns1.ourdomain.net` 告诉 dig 发出 NetScaler Intelligent Traffic Management DNS 基础结构请求，记录类型（NS 或 A）指示要请求哪个记录。NS 命令将请求 `mydomain.com` 区域的 NS 记录，第二个命令 `@ns1.ourdomain.net A host.mydomain.com` 将是 `mydomain.com` 区域中主机的 A 记录。

第 **4** 步：通过更新您的名称服务器，将 **NetScaler Intelligent Traffic Management** 分配为权威 **DNS**

要将我们指定为权威 DNS 来管理您的域名，请将负责响应您的 DNS 查询的名称服务器更新为我们的名称服务器。然后，新的 NetScaler ITM 名称服务器将负责为您的公司进行权威响应。

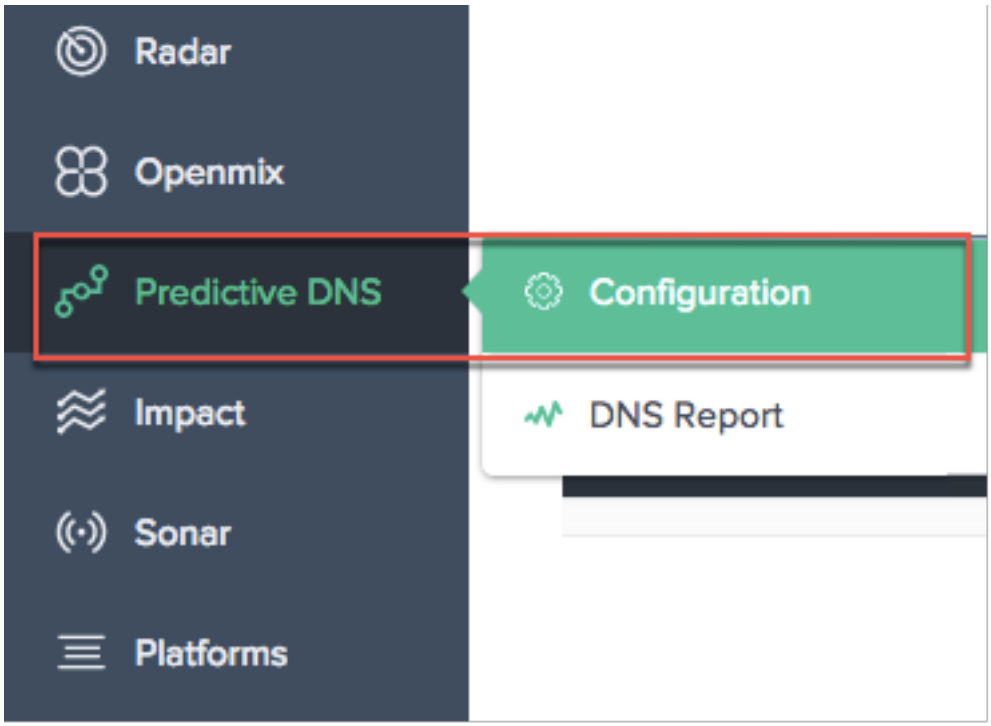
第 **5** 步：正确验证通信流

最初，您会看到在两个系统（您之前的 DNS 服务与 Citrix Predictive DNS）之间运行的流量，具体取决于先前系统中 TTL 的长度。流量可能需要一段时间才能完全迁移。如果您在迁移过程中遇到任何错误，请返回由之前的 DNS 服务提供的名称服务器，然后确定出了什么问题。如果您看到流量按预期流动，则表示您已成功迁移到 Citrix Predictive DNS。此处的默认 TTL 为 3600 秒。您可能需要先降低 TTL，直到确保迁移成功。在您对流量感到满意后，可以根据需要将 TTL 延长为更长的持续时间。

导航

要导航到 Predictive DNS 控制台，请执行以下操作：

1. 登录到 NetScaler Intelligent Traffic Management 门户。
2. 从左侧导航菜单中，选择 **Predictive DNS >** 配置。



这会将您带到添加区域页面，您可以在其中开始创建区域。

主要区域和辅助区域

区域表示单个包含记录集合的父级域。
您可以在 Predictive DNS 中将您的区域设置为主区域或辅助区域。主要 DNS 和辅助 DNS 是一种在 DNS 中创建冗余的方法。主要 DNS 有时被称为主 DNS，而辅助 DNS 有时被称为从 DNS。这是因为主要 DNS 拥有区域数据的主副本，而辅助 DNS 只是定期或在主要 DNS 发出提示时通过区域传输来克隆这些数据。

此过程通常也称为区域传输或 AXFR 传输。如果您在设置主要区域时启用了区域传输，则对该区域所做的所有更改都会自动传播到所有辅助服务器。作为辅助服务器输入的每个 IP 都会收到此更新。同样，您也可以设置辅助区域。

创建区域时，会自动为该区域创建名称服务器 (NS) 记录和授权起始 (SOA) 记录。您可以使用 Predictive DNS 用户界面添加、编辑、复制或删除区域。

注意：这些操作（编辑、复制或删除）会影响整个区域，包括对区域内任何记录的所有响应。必须极其谨慎地执行这些操作。

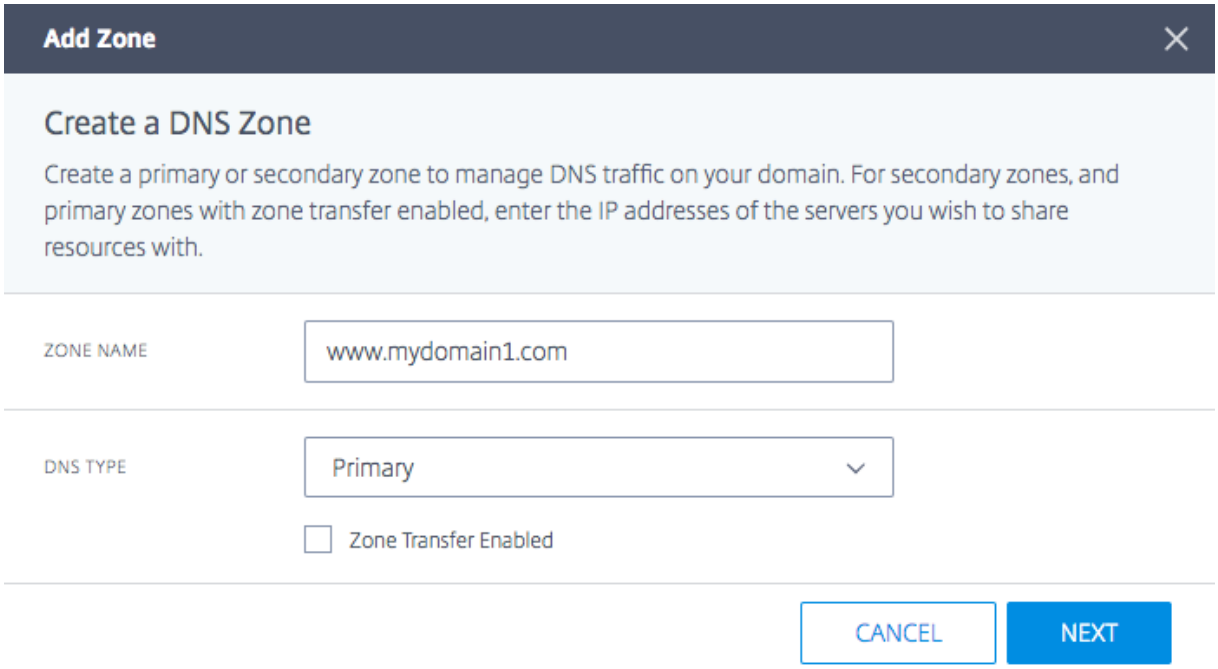
添加区域

要添加或创建区域，请执行以下操作：

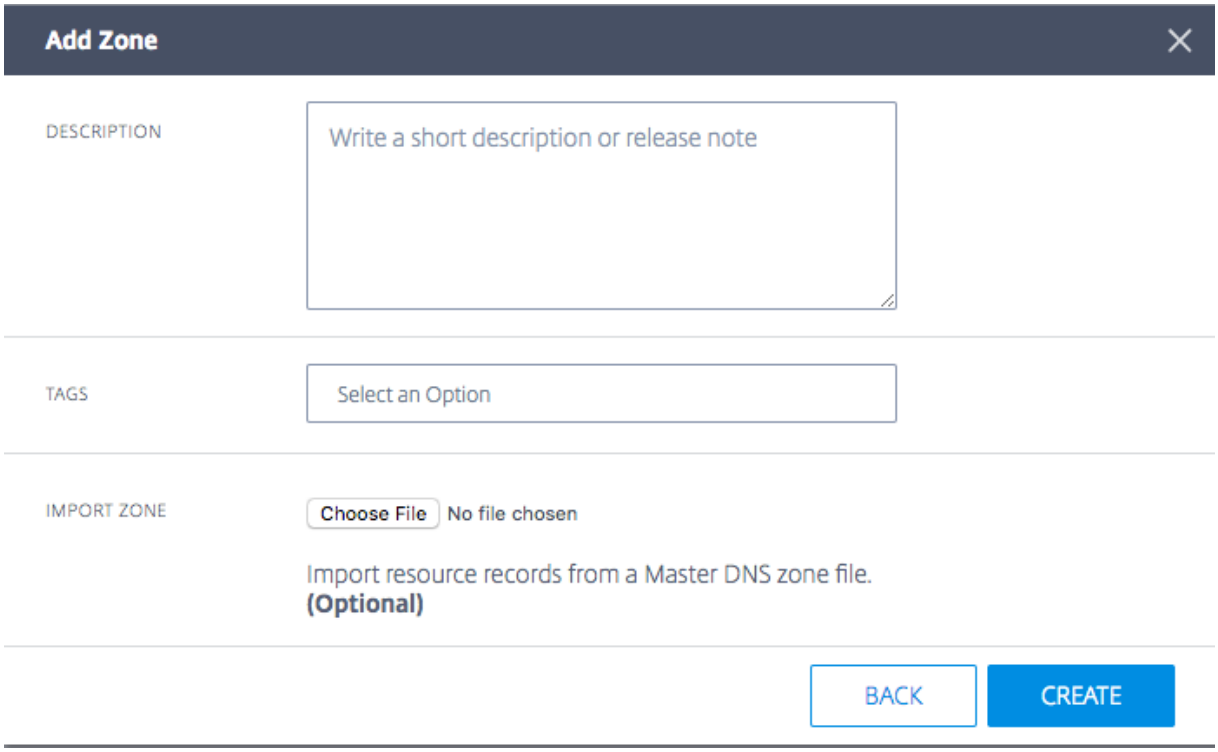
1. 如果这是您第一次执行此操作，则会显示启动屏幕，您可以在其中单击添加区域以开始操作。
2. 这会将您带到添加区域对话框，您可以在其中为您的域创建区域。

如果这不是您第一次执行此操作，则会看到为您公司的域创建的现有区域（域名）列表以及与每个域名相关联的记录数量。

1. 单击页面右上角的添加图标以开始创建区域。
2. 添加区域对话框随即打开。

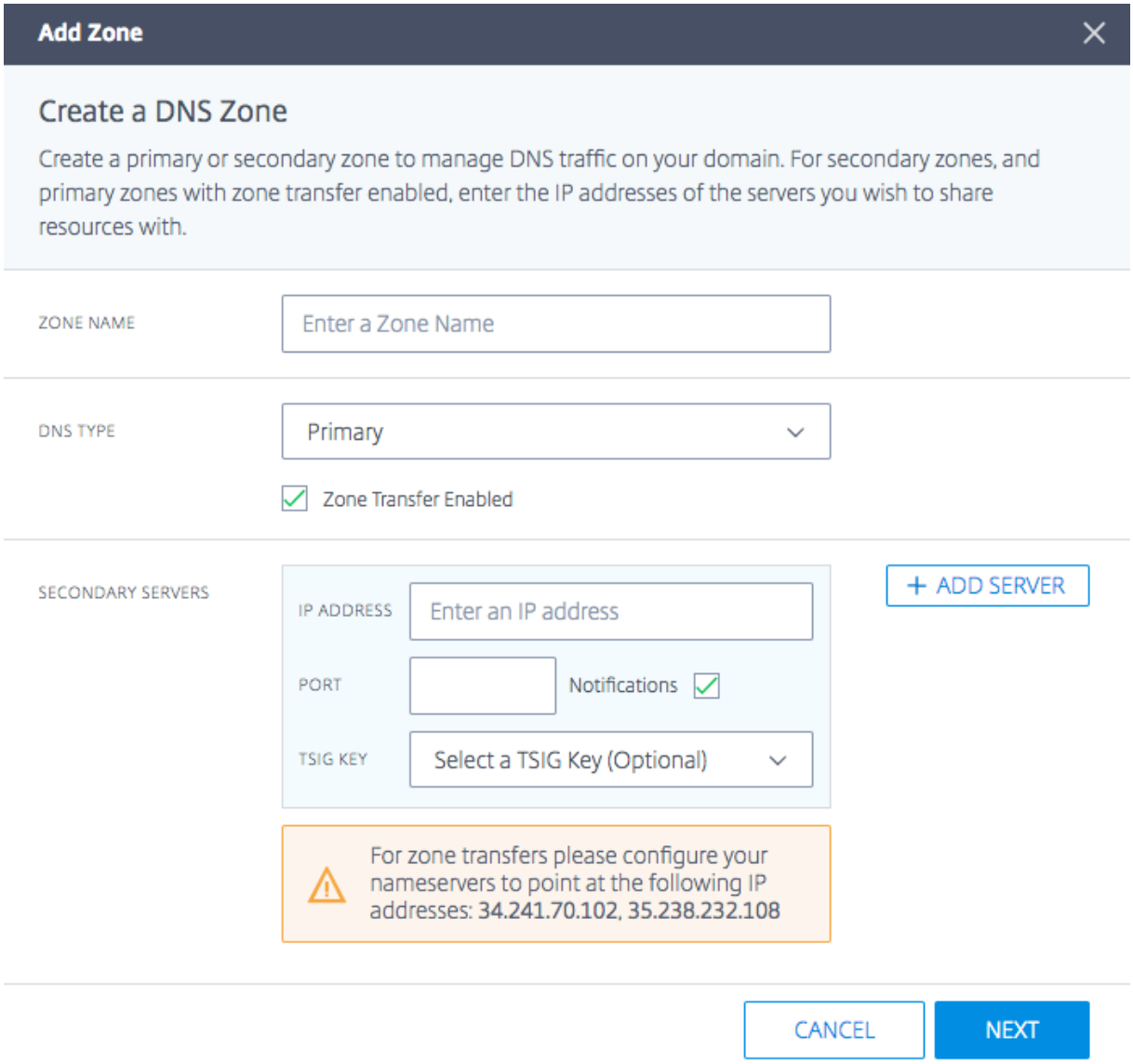


1. 输入您的域名作为区域名称。例如 `www.mydomain.com`。区域名称必须全局唯一，这意味着您不能创建已存在的区域名称，该名称甚至不能与现有区域名称部分重叠。但是，如果存在您需要创建可能与现有区域名称重叠的区域名称的有效方案，或者您无法为自己拥有的域创建区域，请联系支持人员。
2. 选择主要或辅助作为 **DNS** 类型。
3. 单击启用区域传输复选框以启用区域传输，然后输入主要服务器或辅助服务器的信息。有关详细信息，请参阅服务器信息 。
4. 单击下一步以输入区域信息，例如描述和标记。
5. 选择选择文件以从您的计算机导入区域文件（如果可用）。
6. 单击创建以完成新区域的添加。



创建新区域后，它们会出现在区域页面上的列表中。

服务器信息



IP 地址　输入主要或辅助服务器的 IP。

Port（端口）　输入与服务器关联的端口号。此字段为可选字段。只能为辅助服务器配置此设置。如果留空，则默认为 53。

通知　如果您希望当有更新发生时主要 DNS 通知 辅助 DNS，请选中“通知”复选框来启用通知。如果未选中该复选框，则主要 DNS 的更新将按固定的 60 分钟时间间隔发送到辅助 DNS。

添加服务器　可以使用添加服务器按钮为区域传输配置多台服务器。

TSIG 密钥　您可以从列表中选择一个 **TSIG** 密钥。此列表包含您在“TSIG 密钥”部分创建和管理的密钥。这是一个可选字段，用于提高安全性。有关更多信息，请参阅 TSIG 密钥 。

说明　添加有关您要创建的区域的简短描述或注释。这是一个可选字段，完全取决于您自己的需求。它不会以任何方式影响实际的 DNS 响应。

标记　标记允许您在列表中对区域进行排序和过滤。这也是一个可选字段。

导入区域　如果您有包含您的区域配置的区域导入文件，则可以在此处将其导入。要导入区域文件，请先创建一个与要导入的文件同名的区域。下面是导入要求：

- 区域文件中区域的名称必须与您正在创建的区域的名称相匹配。
- 区域文件为记录使用标准的 BIND 格式。
- 导入的文件必须采用 RFC 定义的区域文件格式。
- 您最多可以导入 5000 条记录。如果您需要导入 5000 条以上的记录，请联系支持人员。

要导入区域文件，请执行以下操作：

1. 在添加区域对话框中，转至导入区域。
2. 单击 **Choose File**（选择文件）。
3. 选择要用来填充区域的区域文件。
4. 单击创建以完成该过程。

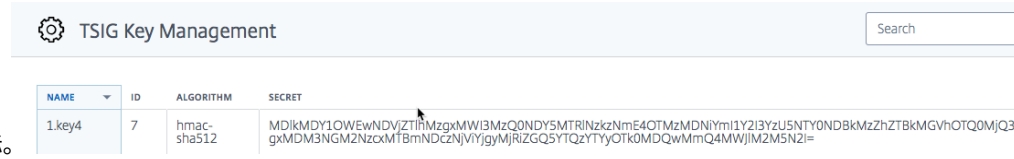
TSIG 密钥

TSIG 密钥为在主要服务器与辅助服务器之间共享信息提供了额外的安全层。密钥的机密必须在两台服务器（主要服务器和辅助服务器）上都可用，才能成功握手。

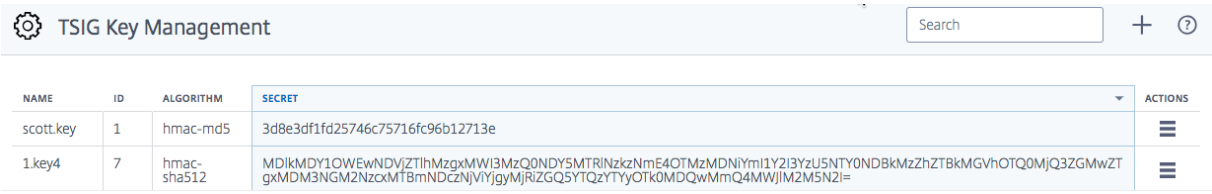
要生成和管理 TSIG 密钥，请执行以下操作：

1. 从左侧导航菜单中，选择 **Predictive DNS**。
2. 单击 **TSIG** 密钥管理。

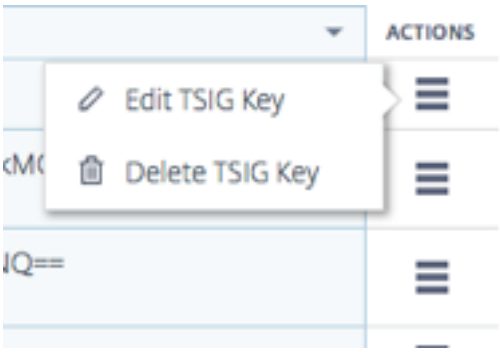
3. “TSIG 密钥管理”页面随即打开。



4. 点击页面右上角的添加图标。
5. 添加 **TSIG** 密钥对话框随即打开。
6. 为 TSIG 输入一个名称。
7. 从列表中选择一种算法。
8. 对于机密，您可以在字段中输入任何单词或句子。只要您输入的内容长度为 32 个字符（不含空格）并采用 base64 编码，就可以原样接受。否则，将根据您选择的算法对其进行哈希处理。注意：机密值和算法值在主要系统与辅助系统之间需要匹配。机密的值必须采用 base64 编码，字符长度必须为 32 个字符。只有尚未存在哈希值时，“生成哈希”按钮才可以帮助生成哈希。
9. 单击创建以完成密钥的生成。新创建的 TSIG 将在 **TSIG** 密钥管理页面上列出。

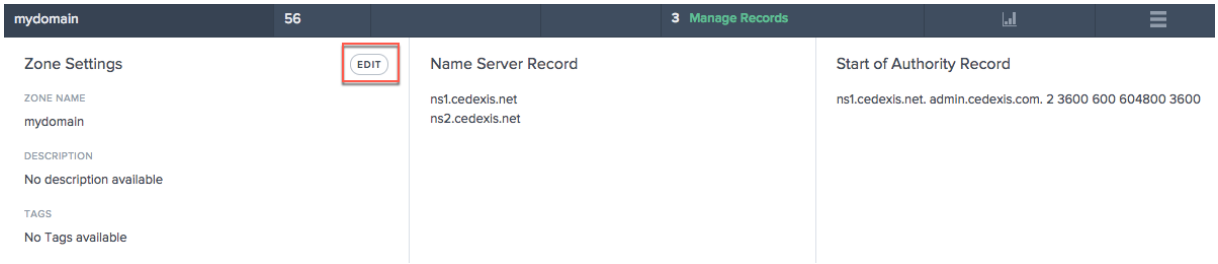


要编辑或删除 **TSIG** 密钥，请单击操作列。选择编辑进行修改或选择删除以删除密钥。



编辑区域

1. 单击要编辑的区域的名称。
2. 编辑抽屉随即打开。
3. 单击编辑按钮以更改区域名称、描述和标记。
4. 单击保存以保存更改。

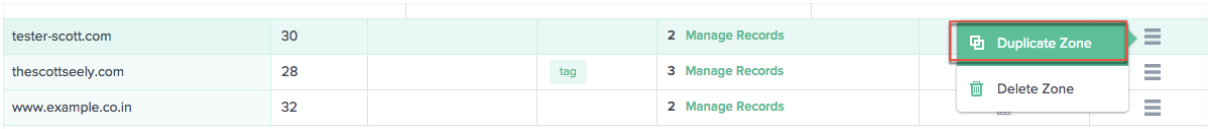


重要说明：编辑区域名称时要小心。由于区域中的所有记录实际上都以区域名称为后缀，因此重命名区域会更改每个请求。

复制区域

复制区域意味着只需使用现有区域中的信息创建另一个区域，但使用不同的区域名称。

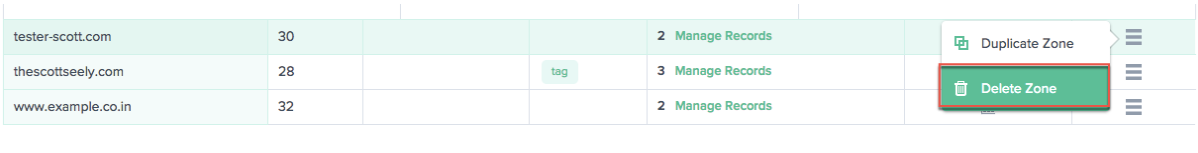
1. 要复制区域，请单击操作列中的图标。
2. 选择复制区域。
3. 添加区域对话框随即打开，其中包含来自原始区域的信息。
4. 给该区域指定一个新名称并根据需要更改任何信息。
5. 单击创建以完成该过程。
6. 使用在原始区域中找到的记录和信息创建了一个新区域。



注意：您可以自行决定是否更改新区域内的任何信息。但是您必须至少更改区域名称才能创建重复的区域。不允许使用重复的区域名称。

删除区域

1. 要删除区域，请单击操作列中的图标。
2. 选择 删除区域。
3. 单击确认。



注意：此操作会影响整个区域，包括对区域内任何记录的所有响应。必须极其谨慎地执行此操作。

记录

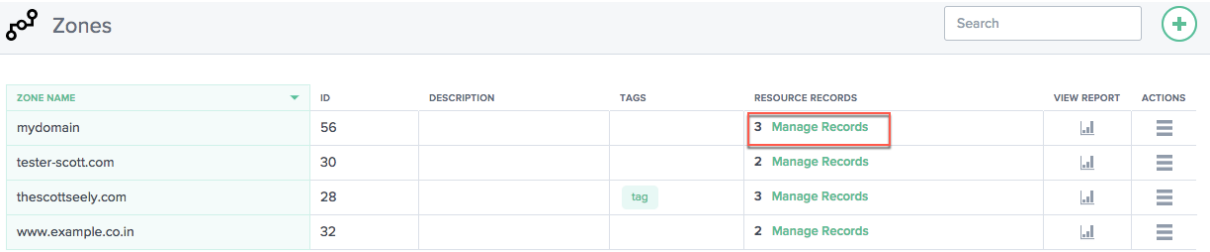
为您的域创建区域（例如 mydomain.com）后，您可以向该区域添加记录。您添加的每条记录都将包含名称、记录类型以及适用于该记录类型的其他信息。

区域内的所有记录都必须以该区域的域名作为后缀。例如，如果 mydomain.com 是区域，则它可以包含名为 www.mydomain.com 和 www.portal.mydomain.com 的记录，但不能包含名为 www.mydomain.co.in 的记录，也就是说，每条记录的名称都附有该区域的名称。

注意：创建区域时，会自动为该区域创建名称服务器 (NS) 记录和授权起始 (SOA) 记录类型。

管理记录

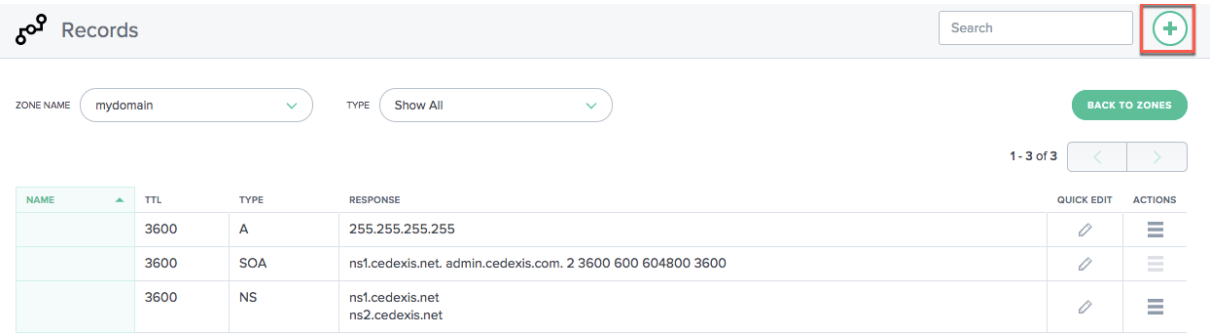
要进入“记录”页面并管理您的记录，请单击您的区域的资源记录列中的管理记录。记录页面随即打开，其中会显示所选区域下的记录列表。即使您尚未创建任何记录，您也可以在“资源记录”下看到您创建的一个或多个区域的至少两种记录类型。这些是首次创建区域时默认创建的 NS 和 SOA 记录。



此页面允许您添加、编辑、删除或复制记录。它还列出了每个子域或记录的 TTL、记录类型和响应。

添加记录

1. 在区域页面上，单击管理记录。这将转至记录页面。
2. 要添加新记录，请单击记录页面右上角的添加按钮。
3. 添加记录对话框随即打开。



名称　输入记录的名称。如果将此字段留空，则会在区域的顶点创建一条记录。例如，如果您的区域是 mydomain.com 并且您希望在此域的根中有一条 A 记录，则可以将其指定为 mydomain.com 区域中的无名记录。某些其他规

范和供应商将其称为 @ 记录。

TTL 输入 TTL 的值。TTL 是您希望 DNS 递归解析器缓存有关此记录的信息的时间长度（以秒为单位）。如果您指定更大的值（例如 172,800 秒或两天），则解析器将重复使用之前的响应，并降低向权威 DNS 服务器发送请求的频率。但是，这意味着对记录的更改需要更长的时间才能生效，因为递归解析器会在较长期间内使用缓存中的值，而不是请求最新信息。

类型 选择要创建的记录类型。有关各种记录类型的更多信息，请参阅记录类型部分。

响应类型 输入与记录类型值相适合的响应。对于除 CNAME 之外的所有类型，您可以输入多个响应值。单击添加图标输入多个响应值。如果输入了多个值，则会为该类型和名称的每个请求返回所有指定的响应。

单击创建以添加记录。新添加的记录将传播到 DNS 服务器，并且进行更改时将实时提供。

列出记录

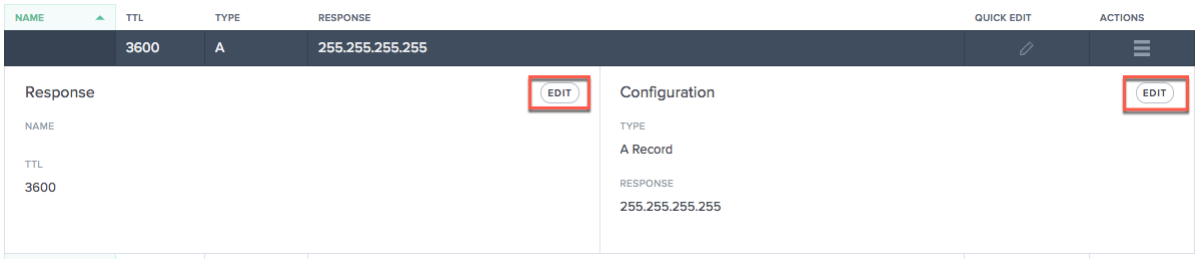
添加新记录时，该记录将在“记录”页面上列出。此页面列出您在特定区域名称下创建的所有记录，以及这些记录的 **TTL**、记录类型和响应。

此页面上的所有记录都属于记录页面左上角的区域名称列表中显示的某个特定区域。此列表列出已为您的公司创建的区域。您可以通过从列表中选择其他区域来切换到其他区域（并查看其自己的记录）。

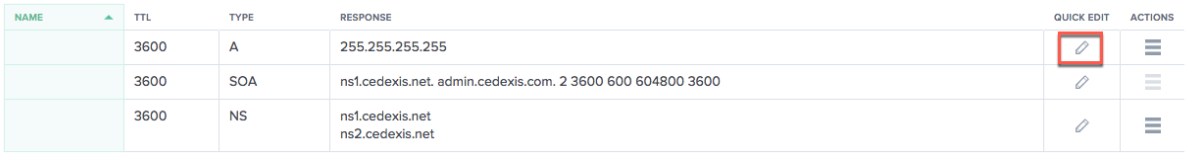
您还可以使用记录类型列表根据记录类型来过滤此列表。

编辑记录

有两种编辑记录的方法：详细编辑和快速编辑。要执行详细编辑，请在列表中单击记录（在记录页面上）。该记录将打开以显示带有编辑按钮的记录详细信息。单击编辑按钮以显示记录信息。完成编辑后，单击保存以保存您的更改。

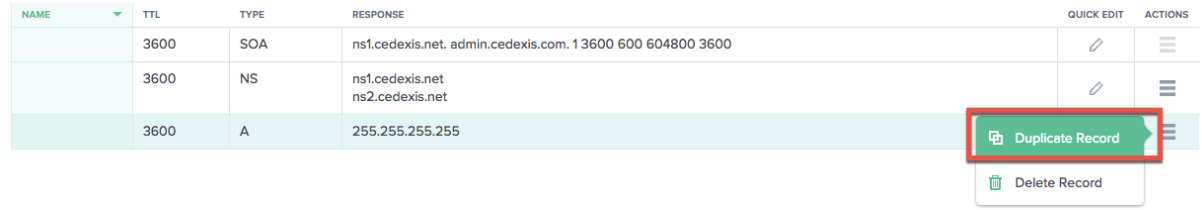


要使用快速编辑，只需单击要编辑的记录的编辑图标（在快速编辑列中）。您将能够编辑该记录的 TTL 和响应。完成编辑后，单击“保存”（对号标记）图标以保存编辑内容，或单击“取消”以撤消编辑。



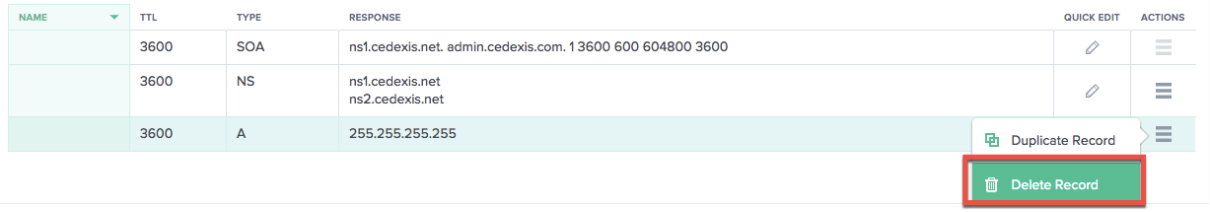
复制记录

要复制记录，请单击操作列中的图标。选择“复制记录”。“添加记录”对话框随即打开，其中包含要复制的记录中的信息。单击“创建”以使用原始记录中的信息创建记录。请注意，要创建新记录，必须至少更改记录名称或类型。
注意：SOA 记录不能复制。



删除记录

要删除记录，请单击操作列中的图标。选择“删除记录”。此操作会删除记录，Predictive DNS 将不再响应对该记录的查询。要删除记录中的特定响应，请使用“快速编辑”选项



注意：NS 和 SOA 记录是默认记录类型，无法删除。只有删除区域本身时，才会删除这些记录。

记录类型

NS 记录

NS 或名称服务器记录负责将 DNS 区域委派给权威服务器。我们创建了一条名称服务器 (NS) 记录，该记录在你创建区域时自动分配，例如 ns1.ourdomain.net 和 ns2.ourdomain.net。这些是您要在注册商中配置的名称服务器，以便可以将 DNS 查询路由到您的区域。
这些名称服务器用于确认可用于该区域的服务请求的服务器集，确保委派请求中返回的名称服务器集和委派服务器返回的名称服务器集相匹配。您也可以编辑名称服务器以确保它们匹配。

我们还允许您编辑您创建的名称服务器，以便您可以将您的任何域指向另一家公司的名称服务器，这些服务器可能存放着您的 DNS 区域并在那里管理您的记录。

注意：NS 记录可以编辑，但无法删除。

SOA 记录

授权起始 (SOA) 记录标识有关该区域的权威信息。SOA 资源记录是在创建区域时默认创建的。您可以根据需要修改该记录。

注意：用户无法创建 SOA 记录，但可以编辑某些参数。

SOA 记录的格式如下：`[MNAME] [RNAME] [Serial Number] [Refresh Time] [Retry Interval] [Expire Time] [Minimum TTL]`

下面是一个示例：`ns1.ourdomain.net admin.mydomain.com.314 3600 600 604800 10`

SOA 记录的元素包括：

- **MNAME**：主要名称服务器的域名，例如上例中的 `ns1.ourdomain.net`。
- **RNAME**：管理员的电子邮件地址，格式中的 @ 符号将替换成句点，例如上例中的 `admin.mydomain.com`。
- 序列号：当您更改区域文件并将更改分发到 DNS 服务器时，要递增的修订号。一个无符号的 32 位整数，例如上例中的 314。
- 刷新时间：DNS 服务器在查询 SOA 记录以检查更改之前等待的刷新时间（以秒为单位）。以秒为单位的一个无符号 32 位整数时间间隔，例如上例中的 3600。
- 重试间隔：辅助服务器在重试失败的区域传输之前等待的重试间隔（以秒为单位），例如上例中的 600（10 分钟）。通常，重试时间小于刷新时间。
- 过期时间：辅助服务器不断尝试完成区域传输的过期时间（以秒为单位），例如上例中的 604800（一周）。
- 最小 **TTL**：以秒为单位的最短存活时间 (TTL)，例如上例中的 10 秒。

A —**IPv4** 地址

IPv4 格式的 IP 地址，例如 `192.0.2.235`。A 记录的值是以点分十进制表示法表示的 IPv4 地址。

AAAA —**IPv6** 地址

IPv6 格式的 IP 地址，例如 `2001:0db8:85a3:0:0:8a2e:0370:7334`。AAAA 记录的值是 RFC 4291/5952 表示形式中指定的以冒号分隔的十六进制格式的 IPv6 地址。

CNAME —规范名称

这是您希望 Predictive DNS 在响应对此记录的 DNS 查询时返回的完全限定的域名（例如 `www.mydomain.com`）。CNAME 值元素的格式与域名的格式相同。

重要说明：DNS 协议不允许您为区域的根创建 CNAME 记录，也就是说，我们不允许创建无名 CNAME 记录。例如，如果您的区域是 `mydomain.com`，则您无法为 `mydomain.com` 创建 CNAME 记录。但是，您可以为 `www.mydomain.com`、`portal.mydomain.com` 等等创建 CNAME 记录。
此外，如果您为子域创建 CNAME 记录，则无法为该子域创建任何其他记录。例如，如果您为 `www.mydomain.com` 创建 CNAME 记录，则无法创建名称为 `www.mydomain.com` 的其他记录类型。
注意：如果某个子域有一条 Openmix 应用程序记录，则同一个子域中不能有 A、AAAA 或 CNAME 记录。

MX —邮件交换

这是用于将请求路由到邮件服务器的记录。例如：`1 mail.mydomain.com`

MX 记录的每个值都包含两个值：

1. 邮件服务器的优先级，可以是大于 0 的任何 16 位整数。
2. 邮件服务器的域名。

如果您指定多台服务器，则为优先级指定的值将指示您希望首先将电子邮件路由到哪台邮件服务器，其次路由到哪台服务器，等等。例如，如果您有两台邮件服务器，并且您将优先级值指定为 1 和 2，则电子邮件将始终发送到优先级为 1 的服务器，除非该服务器不可用。如果将值指定为 1 和 1，则电子邮件将大致均等地路由到这两台服务器。

Openmix (A/AAAA/CNAME)

Openmix 应用程序客户现在可以使用同一组服务管理区域中的整个记录集（包括静态记录）并为其提供服务。这允许客户使他们的任何主机实现 Openmix 智能化。因此，每当将 CNAME 附加到 Openmix 应用程序时，它就会获得与 Openmix 相同的由数据驱动的、动态、完全可编程的功能。

例如，您可以在 Openmix 应用程序后面设置多台 Web 应用程序服务器来存放您的“www”记录，而 Openmix 应用程序将使用其内置的智能逻辑决定使用哪个 CNAME 进行响应。

注意：Openmix 应用程序可以返回 CNAME、A 或 AAAA 记录，因此您不能同时拥有多个使用相同名称且具有任何这些记录类型的 Openmix 应用程序。

PTR —指针记录

PTR 记录用于将 IP 映射到域名，主要用于反向 DNS。正确配置的 PTR 记录对于安全场景可能很重要，例如验证电子邮件发件人的可信度或在 SSH 会话建立时执行的反向 DNS 查询。PTR 记录值的格式与域名的格式相同。例如，`hostname.mydomain.com`。

SPF —发件人策略框架

SPF 记录标识允许哪些邮件服务器代表您的域发送电子邮件。它以 v=spf 开头，例如，v=spf1 ip 4:192.168 .0.1/16-all。

SRV —服务定位器

SRV 记录由 Voice over IP、即时消息协议、服务发现和其他应用程序使用。SRV 记录值元素包含四个以空格分隔的值。前三个值是分别表示优先级、权重和端口的十进制数字。第四个值是域名。

SRV 记录的格式是：

```
[priority] [weight] [port] [domain name]
```

例如：

```
1 10 5269 xmpp-server.example.com
```

TXT —文本

文本记录可以包含任意文本，也可以用来定义机器可读的数据，例如安全或防滥用信息。它还经常用于域所有权验证（例如，您可以获取证书、注册第三方工具以代表您的域进行操作等）。
它只需要包含文本，例如“示例文本输入”。

预测记录 (A/AAAA/CNAME)

预测记录为基于实时服务可用性的全局流量管理提供了各种配置选项。预测记录允许您跨地址池应用路由配置，并针对不同的位置、网络或 IP/CIDR 块分别定义行为。该服务组合了故障转移和轮询路由逻辑，可确保跨平台实现最高可用性、零停机时间和无缝的数据驱动的流量管理。

Predictive DNS 客户可以将预测记录类型用于 CNAME、A 或 AAAA 响应类型。

作为 Predictive DNS 客户，在向区域中添加记录时，请从记录类型列表中选择预测 **(A/AAAA/CNAME)**。

导航

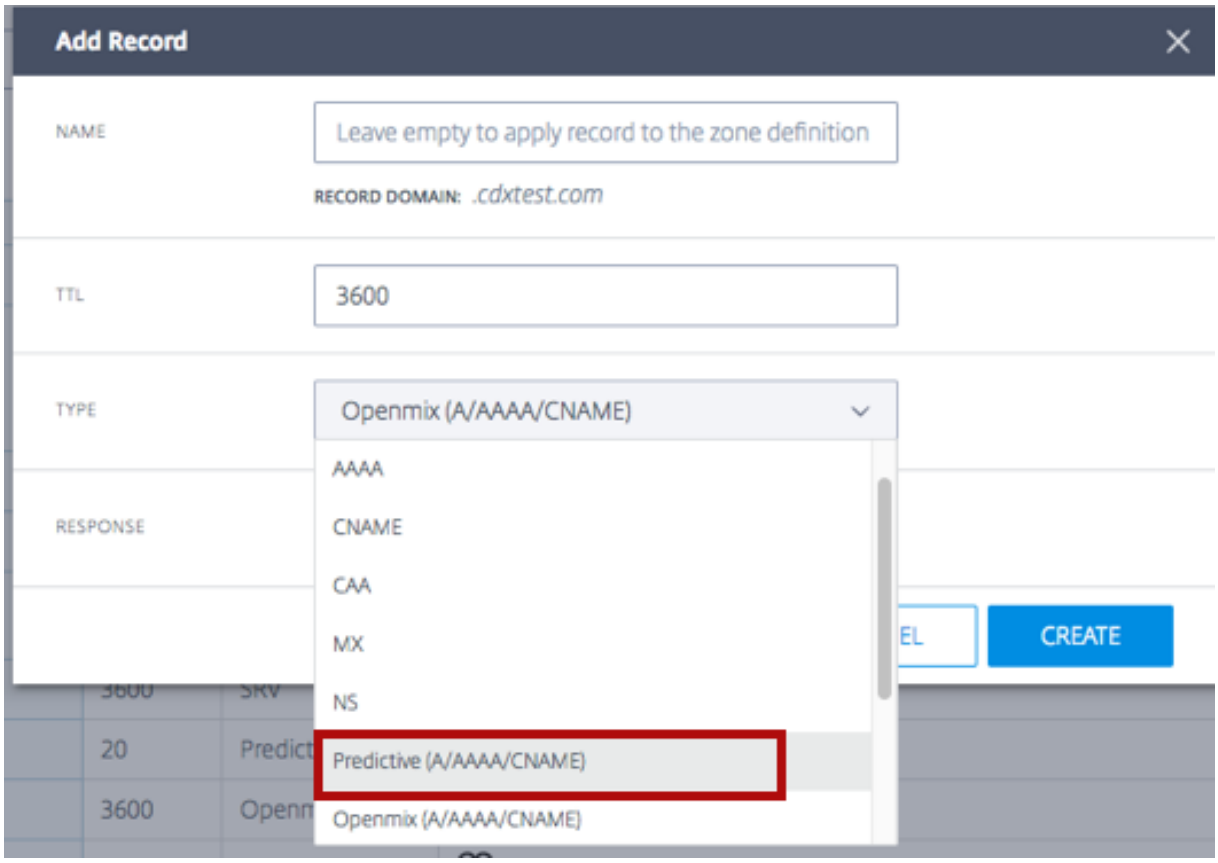
1. 转至您的区域的记录页面。
2. 单击“记录”页面上的添加记录按钮。要详细了解如何添加记录，请参阅添加记录部分。
3. 添加记录对话框随即打开。

添加预测记录

在添加记录对话框中，输入以下内容：

1. 名称：输入记录的名称。如果留空，则记录将自动具有区域定义。您也可以在名称最左侧使用一个星号 `*` 作为通配符，以匹配所有不存在的子域的请求。例如，您可以使用 `*`、`*.example.com` 或 `*.something.example.com`。但是，`*.` 无效，也就是说，不允许星号后只有一个点。我们支持 RFC 中定义的通配符功能。

2. **TTL**：您可以保留默认 TTL 不变，也可以根据需要对其进行修改。注意：DNS 生存时间 (TTL) 告诉解析器在再次请求更新之前，它们必须将决策保留多长时间。TTL 用于控制流量，也用于控制它作用于的数据的变更灵敏度。默认 TTL 为 20 秒。如果降低 TTL，则会获得更多的流量和更多的实时 DNS 查询。但是，这可能会导致成本增加和性能降低（因为 DNS 查询需要在客户端上花费时间）。因此，建议不要更改 20 秒的默认值。
3. 类型：单击类型列表，然后选择“预测 (A/AAAA/CNAME)”。
4. 响应类型：单击响应类型列表，然后将您的响应类型选择为 A、AAAA 或 CNAME。
5. 回退：输入回退响应。必须为回退指定有效的 CNAME、A、AAAA。回退在应用程序处理失败的情况下使用。注意：如果您在上一步中选择的响应类型为 CNAME，则回退响应必须是有效的 CNAME。如果选择的响应类型为 A，则回退响应必须是 CNAME 或 IPv4 地址。或者，如果选择的响应类型为 AAAA，则回退响应必须是 CNAME 或 IPv6 地址。
6. 单击创建并定义路由。
7. 预测配置页面随即打开。



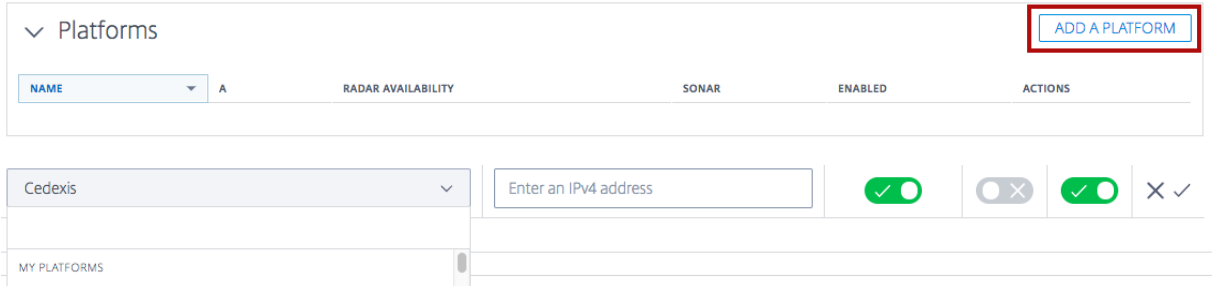
配置步骤

此页面顶部有一个常规部分，其中显示了您在添加记录对话框中所做的设置。它还具有可选字段，用于向预测记录添加标记或描述。

按照以下步骤配置记录。

第 **1** 步：选择所有可用平台　配置预测记录的第一步是选择您希望可用于不同位置、网络或 IP/CIDR 块的所有平台。如果您在列表中找不到您的平台，则可以在平台页面中添加它。

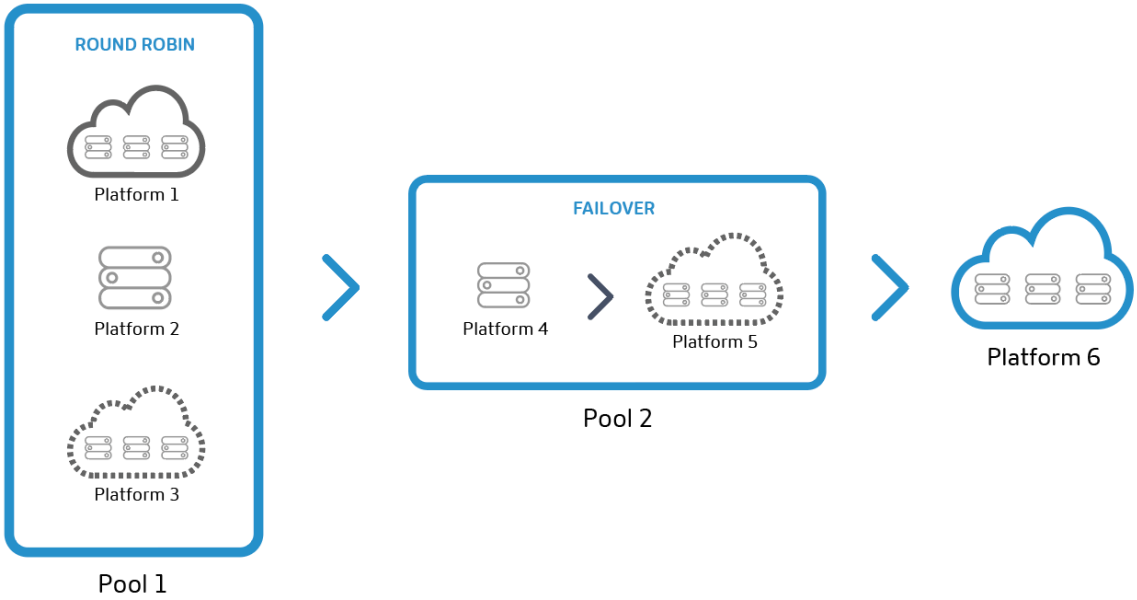
1. 点击本部分右上角的添加平台。
2. 添加您希望可用于路由的所有平台，包括需要添加到地址池中的平台。为此，您可以单击选择平台字段，然后从列表中分别选择各个平台。
3. 根据您在添加记录列表中选择的响应类型 (A、AAAA 或 CNAME)，输入平台的 IPv4 地址、IPv6 地址或 CNAME。如有必要，您可以返回到常规部分来编辑响应类型。
4. 选择平台并输入响应类型后，您可以通过单击“启用”切换按钮来启用或禁用平台。您还可以使用类似的切换按钮打开/关闭“**Radar** 可用性”和“**Sonar**”。
5. 在操作列中，选择对号图标以保存您的更改，或选择叉号图标以取消。



第 **2** 步：添加并定义地址池

地址池　地址池是遵循用户指定的路由方法的平台的集合。地址池的用途是使您能够定义可用于任何特定路由方法的平台的逻辑组。您可以指定轮询或故障转移路由方法，供池中的平台遵循。

您可以在每个池中添加任意数量的平台，也可以为每个地理位置添加任意数量的池。例如，您可以拥有一个欧盟池（包含主要为欧盟地区提供服务的平台）、一个亚洲池（包含位于中国、印度和新加坡的平台）和一个美国池（包含位于美国的平台）。

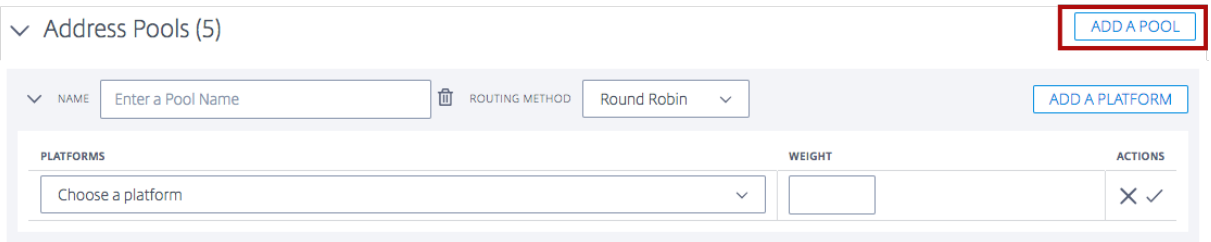


注意：地址池是可选的。您也可以使用单独的平台，并将它们添加到路由配置中。

轮询路由方法　此路由类型遵循典型的全局服务器负载平衡方法（即轮询），采用此方法时，当有 DNS 请求发出时，每个 CNAME/A/AAAA 将交替返回给最终用户。例如，如果平台 P1、P2 和 P3 满足可用性阈值，则第一个请求路由到 P1、次路由到 P2、第三个路由到 P3、第四个路由到 P1，依此类推。您还可以在全局并且/或者按市场或国家/地区为每个平台分配优先级权重和选择权重。

故障转移路由方法　此路由方法支持一种简单的路由逻辑，该逻辑根据平台的排队位置和可用性阈值来选择平台。您可以创建故障转移链来决定首先选择哪个平台、其次选择哪个平台，等等。可以创建这种故障转移链，使其在全球和/或个别市场和国家/地区生效。

添加地址池　要添加地址池，请执行以下操作：



1. 单击本部分右上角的添加池按钮。
2. 为池输入一个名称。名称可用于标识池的用途。
3. 选择一种路由方法。您可以选择轮询或故障转移。

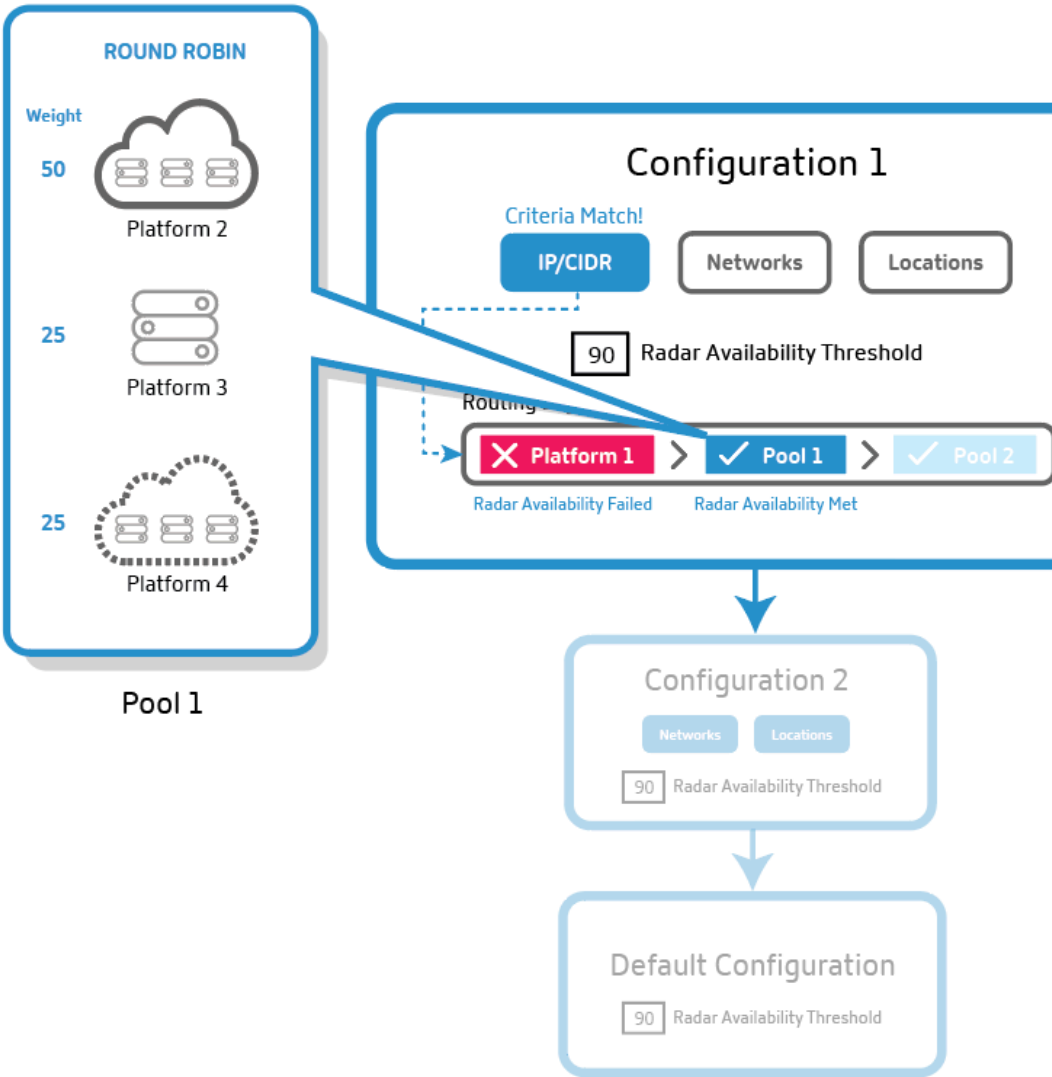
4. 从您在上一步中创建的列表中选择一个平台。
5. 您可以根据需要向此池中添加任意数量的平台，方法是单击添加平台按钮。
6. 对于您选择的每个平台，输入合适的权重。权重的用途是对用于流量分发的平台进行优先级排序和选择。您分配给各个平台的权重加起来不必等于 100。它们可以是介于 0 和 1,000,000 之间的任何整数。当这些权重转换为百分比时（在后端），它们加起来将等于 100%。如果所有选定的平台都具有相同的权重，则流量将随着时间的推移在它们之间均匀分布。如果你只有一个平台，那么无论您为其分配多大的权重，都会始终使用这个平台。
7. 完成后，选择对号图标以保存您的更改，或选择叉号图标以取消。
8. 然后，您可以通过在操作列中选择相应的图标来编辑或删除您的平台选择。

第 **3** 步：配置故障转移　故障转移应用于整组地址池和/或个别平台。它支持一种简单的验证方法，将根据以下条件评估是否可将个别平台或池用于路由：

- 位置、网络和/或 IP/CIDR。至少需要具体说明其中一个标准。

  > 注意：
  >
  > 故障转移的位置标准不应包含大陆和国家/地区的混合，但您可以使用路由逻辑创建多个故障切换。

- Sonar 和 Radar 可用性（如果配置），以及
- 排队位置

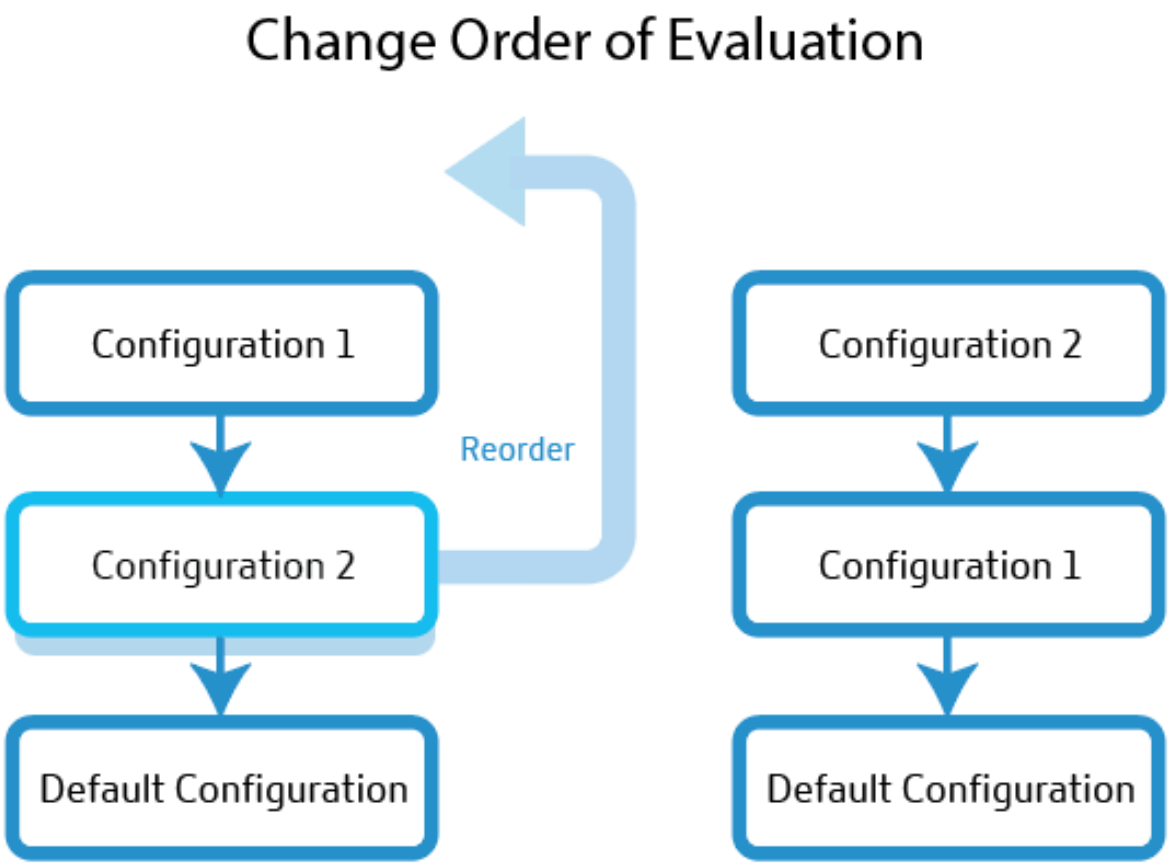


针对预测记录的故障转移

1. 预测记录根据所需条件（位置、网络和/或 IP）评估第一个配置块。如果第一个路由配置块不满足所需的条件，则它会移至队列中的第二个路由配置块，依此类推。
2. 满足所有必需条件的配置块将被选定用于流量分发。
3. 在选定的配置块中，将根据地址池或平台的排队位置和可用性阈值（Radar 和 Sonar）对其进行评估。
4. 将选择地址池内（或地址池外）第一个满足可用性阈值的平台进行流量分发。然后，轮询或故障转移路由逻辑开始发挥作用。

注意：如果池中只有一个平台，则会始终选择该平台，轮询逻辑将不适用于该平台。

作为用户，您可以按照以下方式排列路由配置块：优先级最高的配置块排在第一位，依此类推。可以通过将每个池或平台拖到队列中它需要处于的位置，手动进行重新排列。



默认配置　您必须在默认路由配置块中设置至少一个平台或池。它必须包含当所有其他选项都不符合指定的条件时，预测记录将使用的一个或多个平台或池。默认值没有任何要指定的条件，它匹配所有请求。如果平台可用性不满足 Radar 可用性阈值，则响应会返回回退。

配置故障转移的步骤　要定义配置，请执行以下操作：

1. 输入一个名称。此名称有助于识别您的路由配置块。
2. 您可以保留默认 TTL 不变，也可以根据需要对其进行修改。
3. 确保选中 **Radar** 可用性。您可以将 Radar 可用性阈值设置为所需的级别。取消选中此选项将为该组池或平台禁用 Radar。
4. 选择位置、网络和/或 **IP/CIDR**。例如，如果您的路由配置适用于大洋洲区域，则您可以指定该区域中平台或池的位置、网络和/或 IP 地址。
5. 故障转移配置字段允许您为所有池和平台设置选择优先级。您放置这些池或平台的顺序将决定在路由时对它们的选择。并且流量将根据上一步中指定的方法（轮询或故障转移）进行路由。
6. 要删除某个配置块，请单击名称字段旁边的垃圾桶图标。

DNS 报告

可以使用 DNS 报告根据指定域或主机名的各种条件深入了解 DNS 请求量。它们显示特定记录类型被查询的频率，并提供完全不同的向下钻取级别。这种精细度使 Predictive DNS 用户能够了解特定区域、主机名、请求类型、市场、国家/地区、区域、州/省/市/自治区和网络的趋势和查询量。

这些报告主要用于增强可见性和分析功能。它们提供每个区域或主机名的流量并帮助诊断与 DNS 相关的问题。它们还通过按记录类型和地理位置细分请求量来揭示异常情况，例如请求激增或其他违规行为。

您还可以通过了解哪些区域的流量最多来过滤不必要的干扰信息，并且只关注您关心的区域或记录类型。

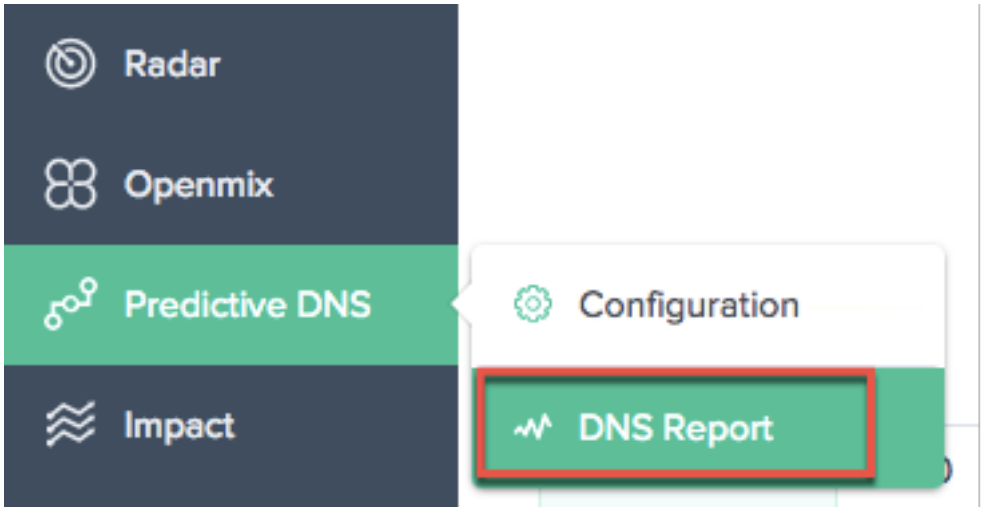
DNS 与 Openmix 报告

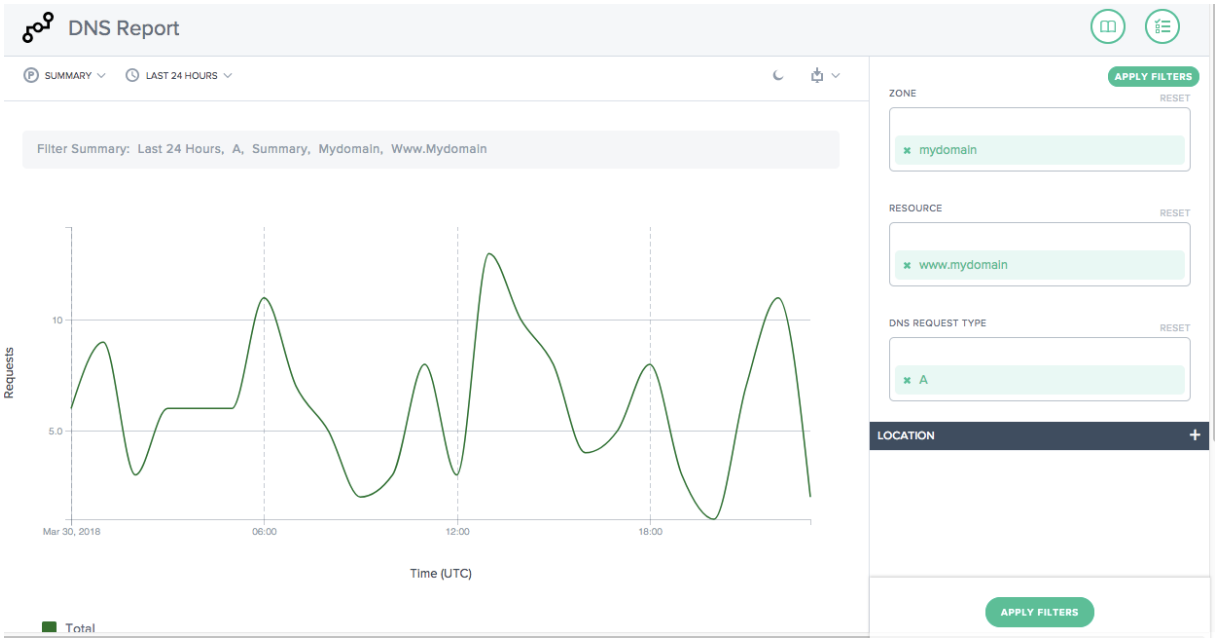
对于 Openmix 客户，报告会显示在 DNS 报告和 Openmix 决策报告中。DNS 报告提供有关向我们的权威区域发出的请求的信息，而 Openmix 则通过 Openmix 应用程序记录或直接向 Openmix CNAME 提供有关何时使用 Openmix 智能平台来满足请求的报告。

导航

要导航到 **DNS** 报告部分，请执行以下操作：

1. 在左侧导航菜单中单击 **Predictive DNS**。
2. 导航到 **DNS** 报告。
3. **DNS** 报告页面随即打开。



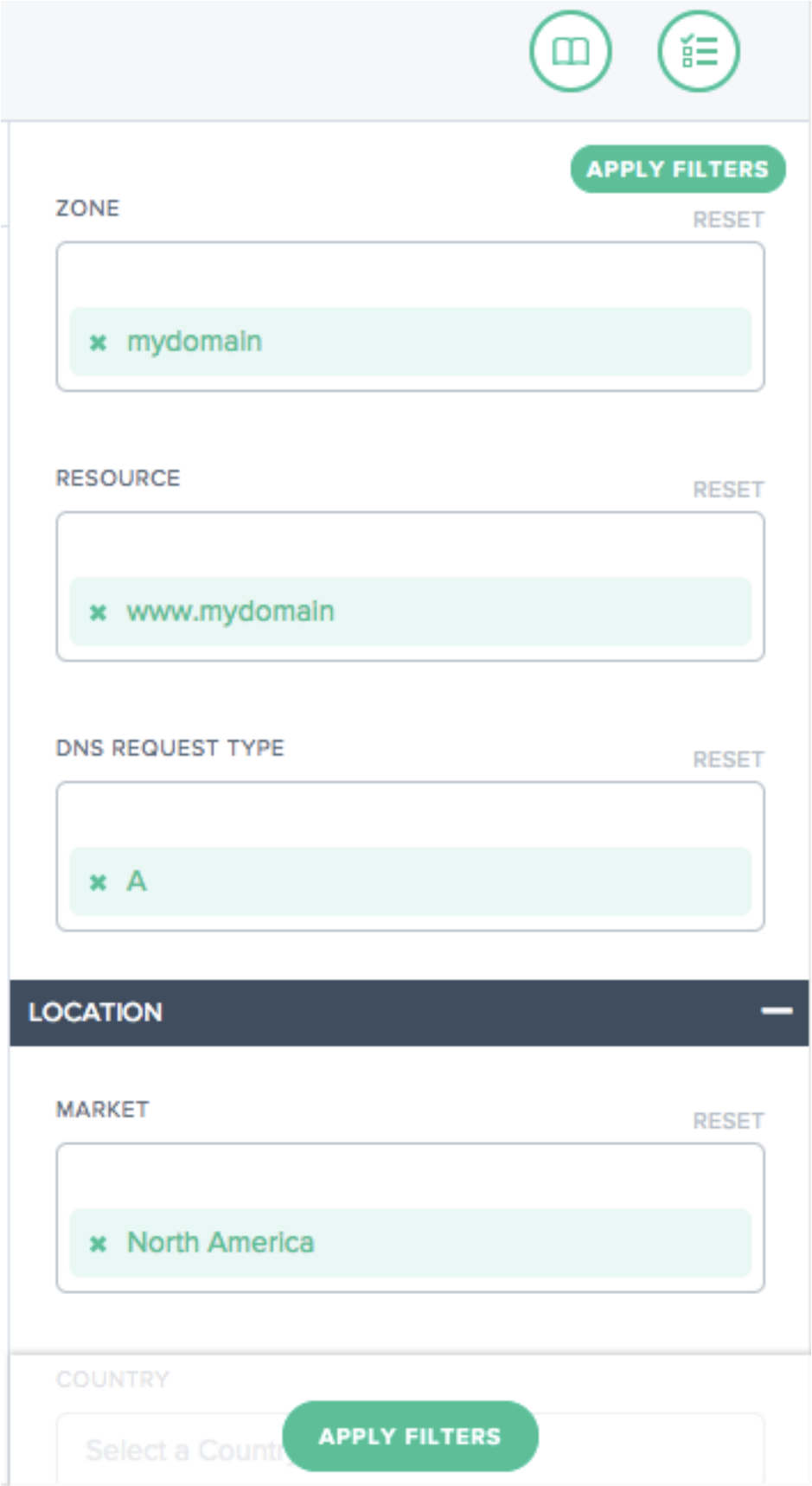


应用过滤器

右侧的应用过滤器面板可帮助您仅选择和查看要在报表上显示的数据。

您可以根据下列项进行过滤：

- 区域–选择要包括的一个或多个区域。
- 资源–选择要包括的一个或多个主机名。
- **DNS** 请求类型–选择要包括的一个或多个 DNS 请求类型。
- 位置–选择要包括的一个或多个地理位置（市场、区域、州/省/市/自治区或网络）。



主要维度

主要维度是通过图表上方的列表选择的。您可以使用它作为报告的强大透视视图。

总结　摘要为您提供请求总数并应用了完整的过滤器组。

按预设时间范围过滤

可以选择相对的预设时间范围作为额外的过滤器，以进一步优化报告。

为报告添加书签

根据过滤条件生成报告后，您可以通过为报告添加书签来保存所应用的过滤器。每当您访问此书签时，都会根据所有选定的过滤条件生成更新的报告。
要为报告添加书签，请执行以下操作：

- 点击页面右上角的书签图标。
- 在“添加新书签”对话框中，为书签指定合适的名称，然后单击“创建”。
- 新书签现已创建。您可以通过单击书签图标（在每个报表页面的右上角）并选择书签来访问书签。

Sonar

June 7, 2021

Sonar 是一种活性检查服务，可用于监视基于 Web 的服务的可用性。Sonar 的工作原理是从世界各地的多个存在点向您指定的 URL 发出 HTTP 或 HTTPS 请求。

Sonar 基础知识

根据以下标准，Sonar 测试的端点被视为向上或向下：

- 导致 HTTP 2xx 的请求被视为成功，任何其他结果（包括网络问题和超时）都被视为失败。
- Sonar 遵循重定向响应，返回 3xx 状态码，最多 6 个重定向，直到它收到非 3xx 响应或发生错误。
- 终端节点状态根据报告位置的仲裁决定。Sonar 报告大多数存在点返回的任何结果（成功或失败）。

Sonar 检查从世界各地的多个测试位置进行。这些地点包括：

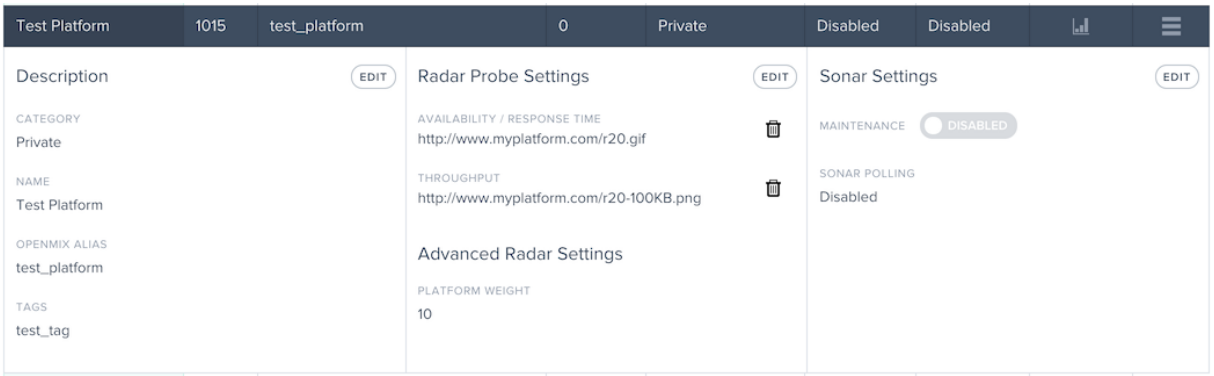
- 新加坡
- 南卡罗来纳州, 美国

- 日本東京
- 圣吉斯兰 (比利时)
- 华盛顿, 美国
- 纽约, 美国
- 伦敦 (英格兰)
- 香港特别行政區
- 法兰克福
- 都柏林
- 爱荷华州
- 維吉尼亞州
- 阿姆斯特丹

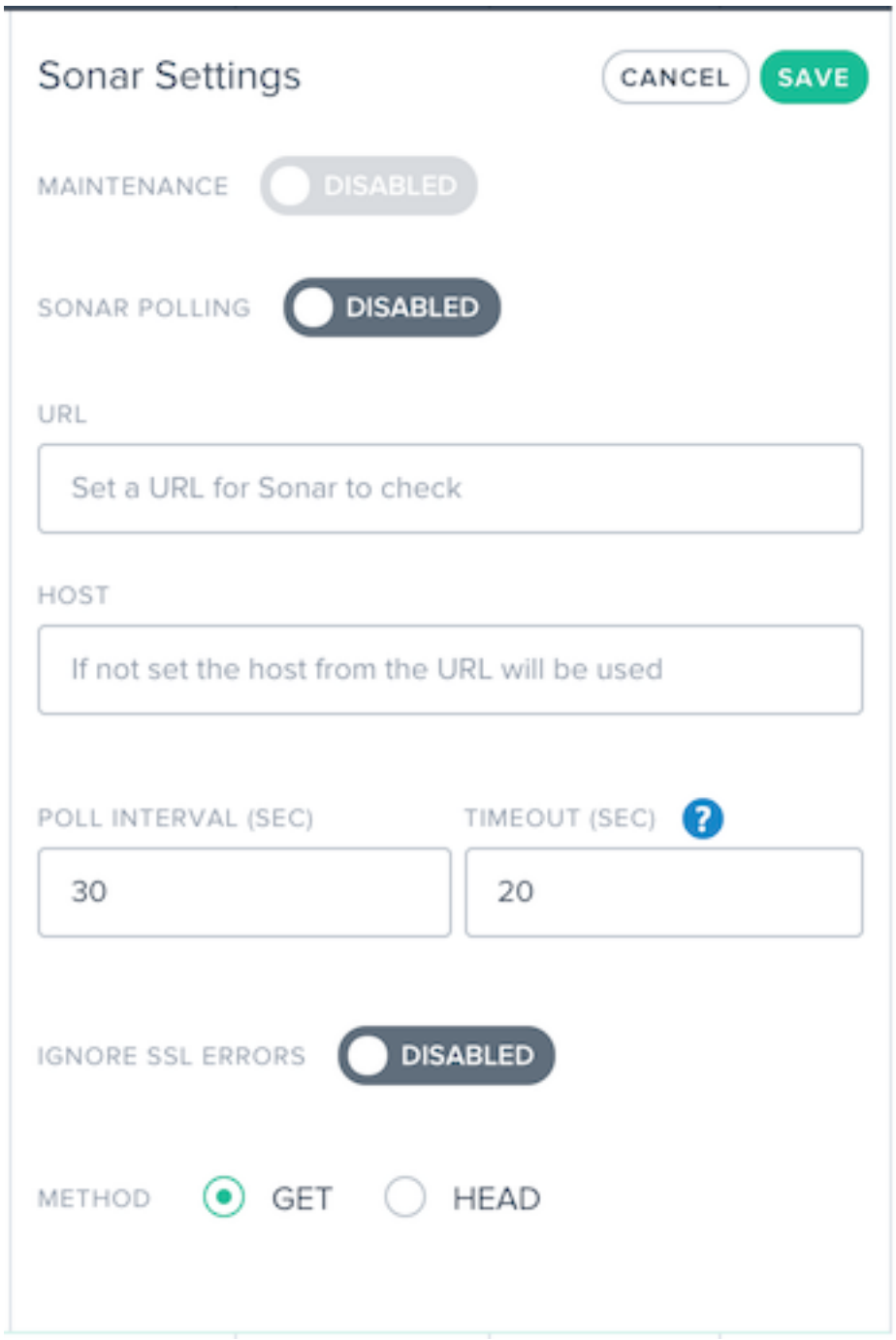
Sonar 平台与全球 Radar、Fusion 和 Openmix 平台服务紧密集成。Sonar 数据实时馈送到世界各地的所有 Openmix 节点，用作决策的额外输入。

平台 **Sonar** 配置

Sonar 为平台页面中的每个平台配置。单击列表中的平台以查看 **Sonar** 设置 部分。



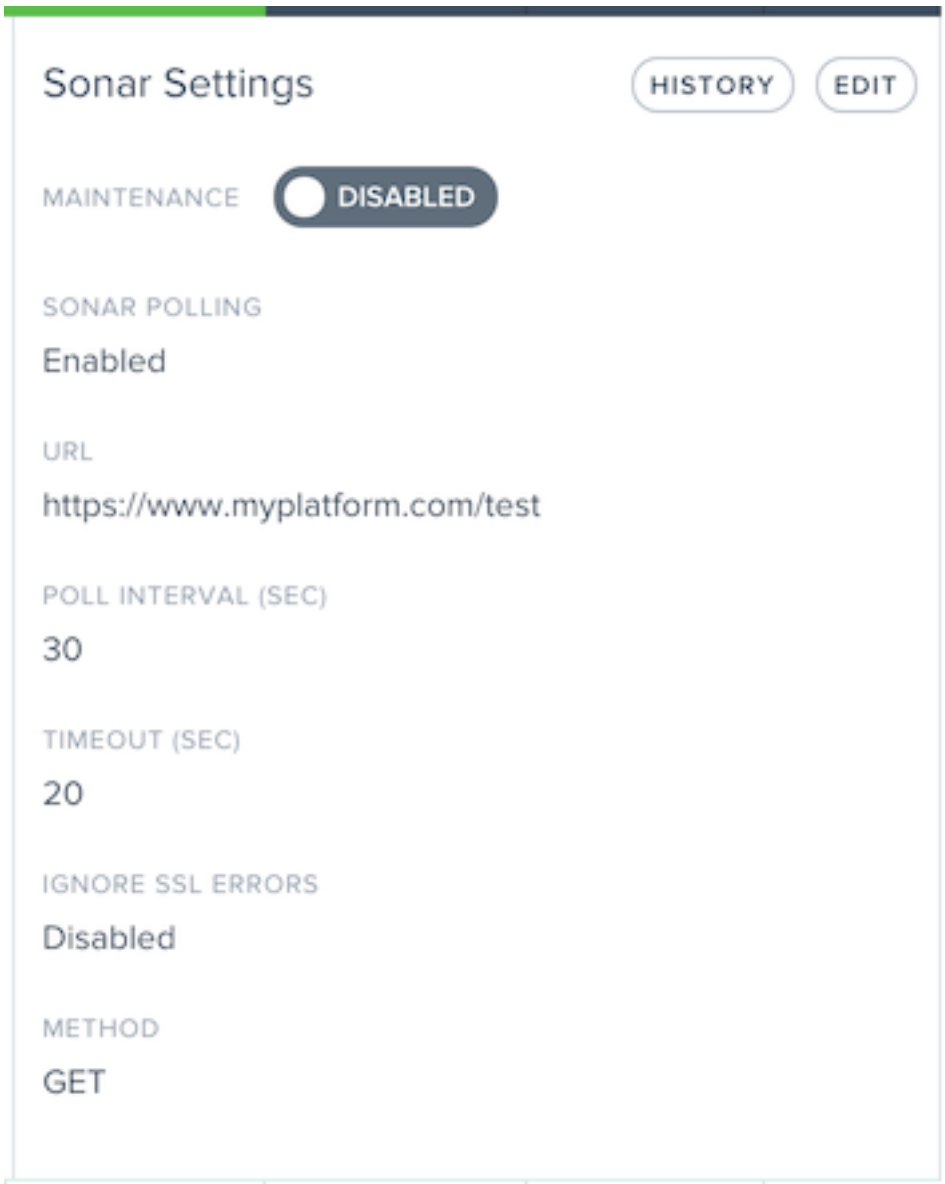
要将 Sonar 监视添加到平台，请单击 **Sonar** 设置 部分中的 编辑 按钮。



这些字段的描述如下：

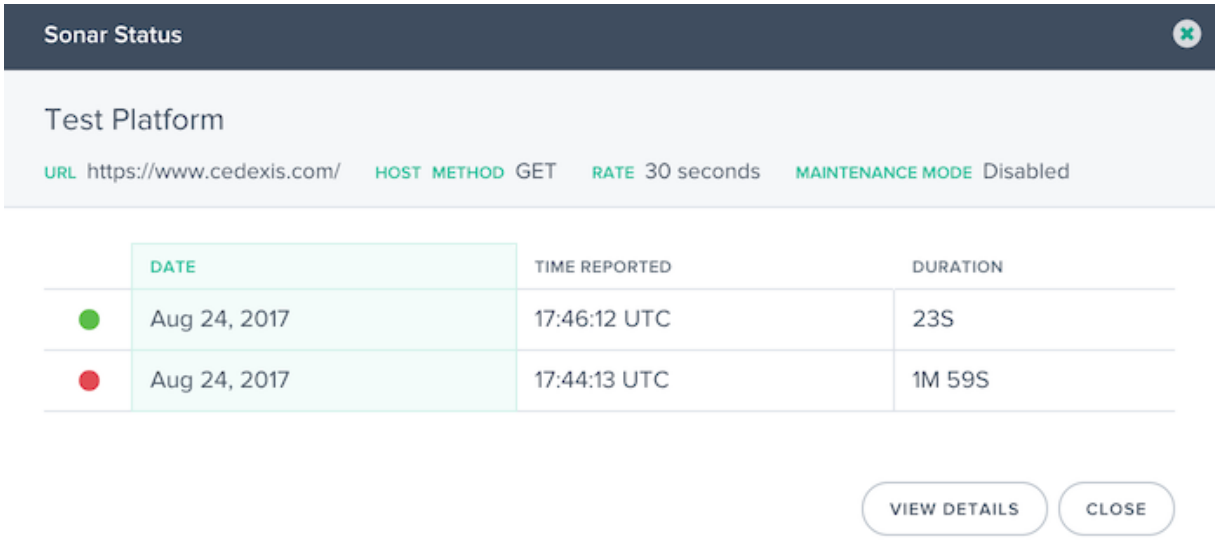
输入项目	说明	默认值
维护	启用后，无论实际状态如何，Sonar 都会将服务报告为关闭状态。这在希望从 Openmix 路由中移除平台以预期停机时非常有用。	已禁用
Sonar 民意测验	如果启用，Sonar 将对配置的 URL 进行检查。	已禁用
URL	URL Sonar 调用来检查服务的可用性。	
主机	必须用于请求中的主机标头值的值。	v
投票间隔	指定测试服务可用性的频率（以秒为单位）。支票的间隔最短可以是每 1 秒钟，最多 300 秒（5 分钟）。	60 v
超时	假定服务检查失败之前，指定等待响应的时间（以秒为单位）。检查的最小超时时间为 1 秒，最多可达 30 秒。对于较短的轮询间隔（例如 5 秒以下），超时限制为 4 秒。	20
忽略 **SSL** 错误	启用后，Sonar 将忽略请求期间发生的 SSL 错误，例如错误配置的 SSL 证书。	已禁用
方法	用于检查的 HTTP 方法：GET 或 HEAD。	

要打开 Sonar，请将 **Sonar** 轮询 切换为 已启用 并输入服务 URL。单击“保存”，检查将开始。



启用 Sonar 时，“设置”将显示当前 Sonar 设置。

启用 Sonar 后，您可以单击声 纳设置 部分中的“历史记录”按钮，查看最近的状态变化和持续时间。单击查 看详细信息 按钮转到 Sonar 平台状态页面，了解更多详细信息和长期状态报告。



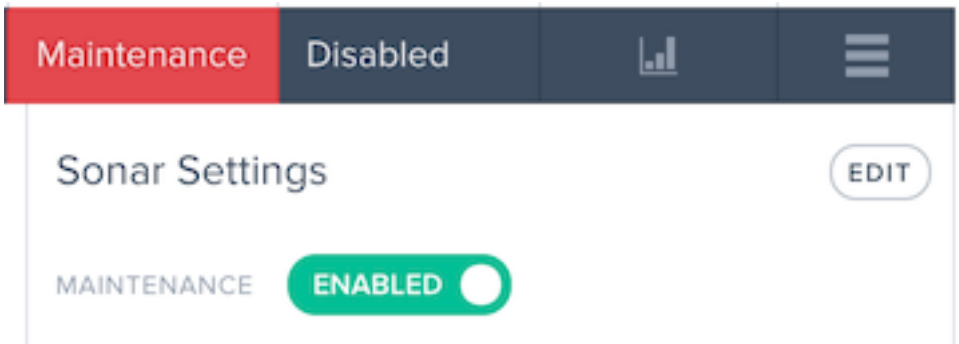
Sonar 状态

当为平台启用 Sonar 时，Sonar 状态会显示在 **Sonar** 列的平台列表中。当 Sonar 监视对平台进行检查时，列单元格为绿色，显示平台可到达的时间。

如果平台监视检查失败，**Sonar** 单元格为红色，将显示平台无法访问的时间。

维护模式

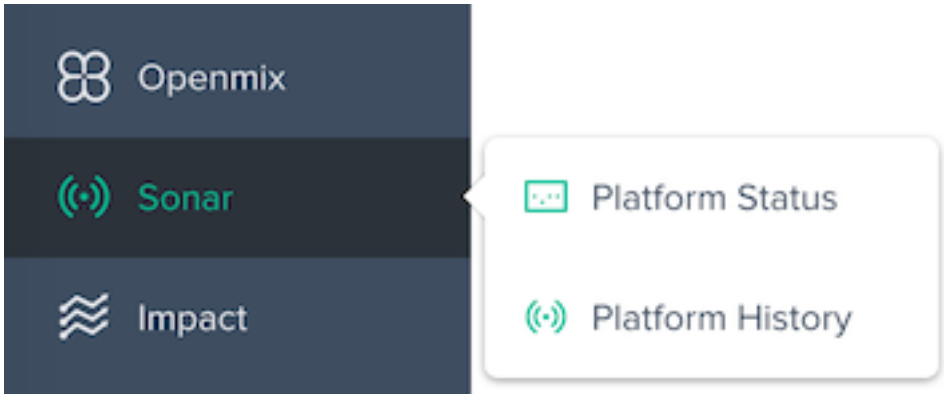
Sonar 状态根据综合检查的成功或失败显示服务的可用性。如果您希望将平台标记为关 闭，即使它可以访问，例如，在预期平台上的维护情况下，您可以启用维护模式。此模式将平台报告为 Openmix 应用程序中不可用的平台，并将自动阻止在任何启用 Sonar 的 Openmix 应用程序中将流量传输到平台。



启用维护模式，将 维护 选项切换为 已启用。

启用后，平台列表项将 Sonar 状态显示为 维护。

Sonar 菜单



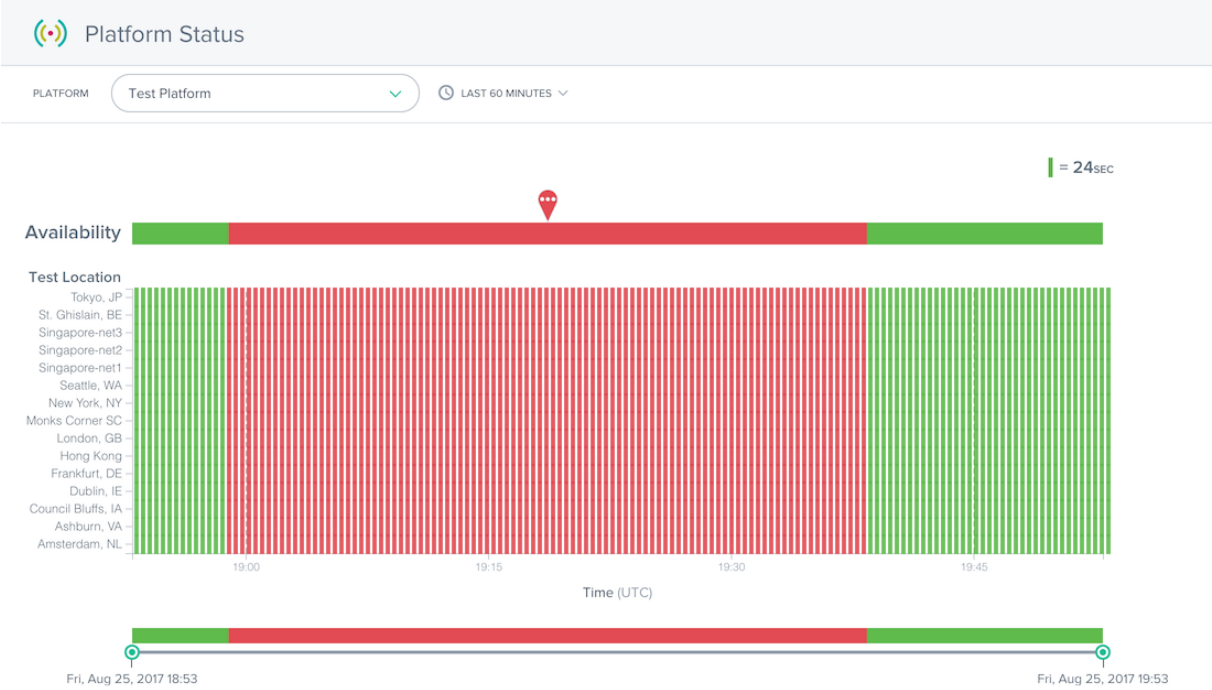
Sonar 菜单由以下选项组成：

1. 平台状态—每个测试位置的详细结果和整体可用性状态。
2. 平台历史记录—过去三个月的可用性状态概述。

平台状态

Sonar 平台状态报告显示了每个测试位置完成的检查的详细信息，以及根据聚合数据计算出的总体状态。

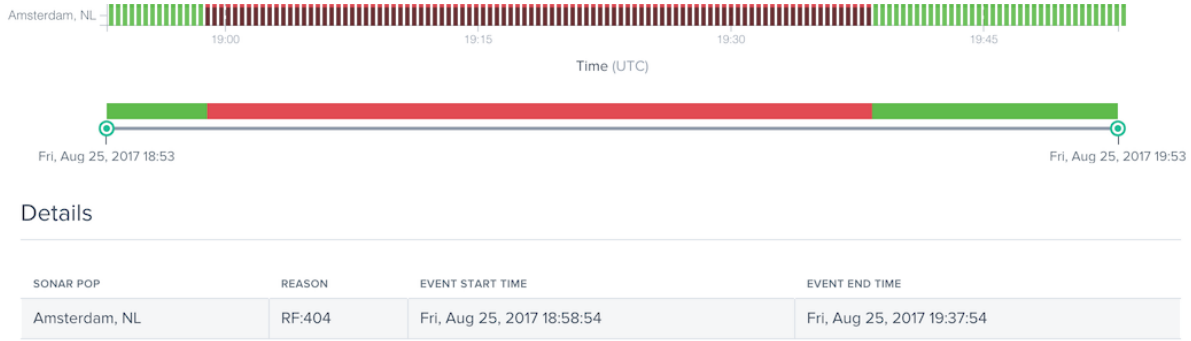
要获取有关特定平台的信息，请在 平台菜单中选择一个平台。



状态报告包含以下部分：

- 可用性：报告顶部是根据各个测试位置的汇总结果向 Openmix 报告的可用性。这是在指定的时间内在 Openmix 应用程序中使用的 Sonar 状态。
- 测试位置：显示每个测试位置的结果。
- 时间滑块：时间滑块允许您轻松钻取详细的时间段。拖动时间滑块以调整报表的时间段，并查看更详细的时间间隔。

通过单击测试位置行中的红色标记，可以查看失败检查的详细信息。测试失败的详细信息将显示在报告下方的 详细信息部分。

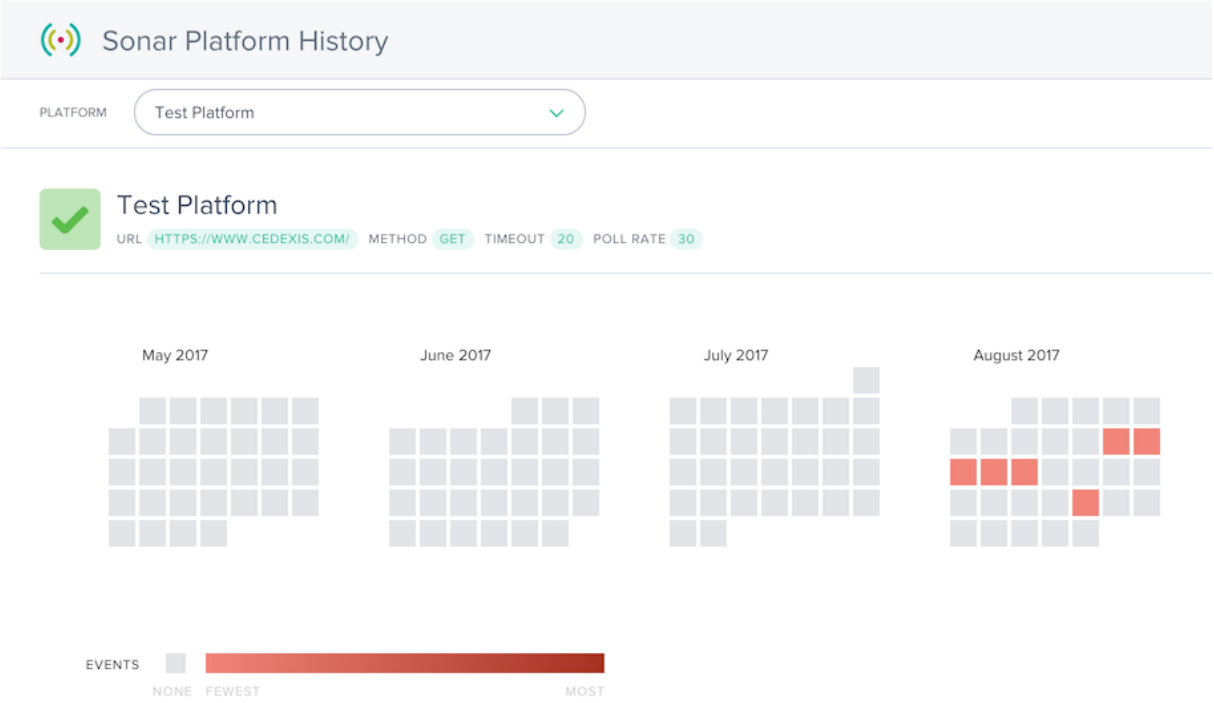


“原因”列提供详细信息，例如在该测试位置发生的 Sonar 检查返回的错误代码。

平台历史记录

Sonar 平台历史记录报告显示了过去几个月中每个测试位置进行的汇总检查的可用性状态。

要获取有关特定平台的信息，请在 平台菜单中选择一个平台。



历史记录报表显示过去几个月的日历。服务中断的天数以红色渐变显示。当天发生的更多可用性事件，它显示的红色。

日历下方是发生的服务中断的列表以及有关事件的一些基本详细信息。

Details

DATE	OUTAGES	START TIME - FIRST OUTAGE	END TIME - LAST OUTAGE	DURATION
2017-08-11	1	21:29:35	23:59:59	2 hours, 30 minutes, 25 seconds
2017-08-12	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-13	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-14	1	00:00:00	21:21:18	2 days, 23 hours, 51 minutes, 43 seconds
2017-08-15	3	14:50:00	15:50:05	0 hours, 4 minutes, 3 seconds
2017-08-24	3	17:44:12	18:03:21	0 hours, 15 minutes, 25 seconds

您可以单击“详细信息”列中的日历日或日期加载状态报告，了解有关服务中断的更多详细信息。

影响

June 7, 2021

Impact 提供了一个强大的视图，以了解访客在您的网站上收集的性能和业务 KPI 数据。单击您感兴趣的报告数据链接以查看更多详细信息。

云平台可视化报告

“影响”菜单由以下选项组成：

1. 导航计时数据 —页面级别的性能详细信息，也称为我们的页面加载时间报告。
2. 视频播放数据 —体验质量和视频交付数据。
3. 资源计时数据 —页面上个别资源的性能详细信息。

导航计时数据

September 22, 2023

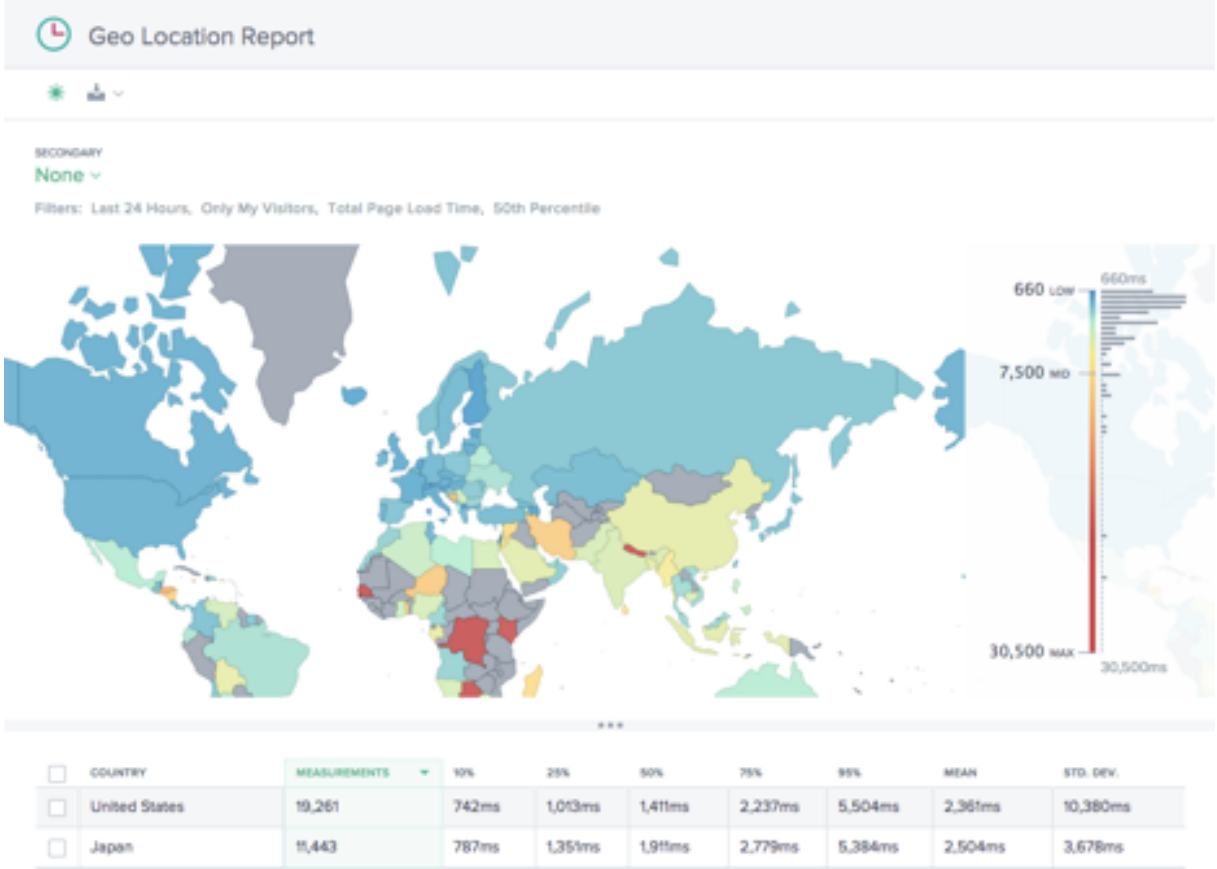
导航计时报告提供了一个强大的视图，可以用来查看当访客在您的网站上时收集的丰富的页面加载和事件性能数据。在报告的简要描述之后，详细介绍了如何透视、过滤和自定义导航计时报告。

导航计时报告

导航计时菜单包括以下报告：

1. 地理位置报告–按地理维度划分的导航计时报告。
2. 性能报告–一段时间内的导航计时测量数据。
3. 统计分布报告 -通过统计分布报告视图查看导航计时数据。

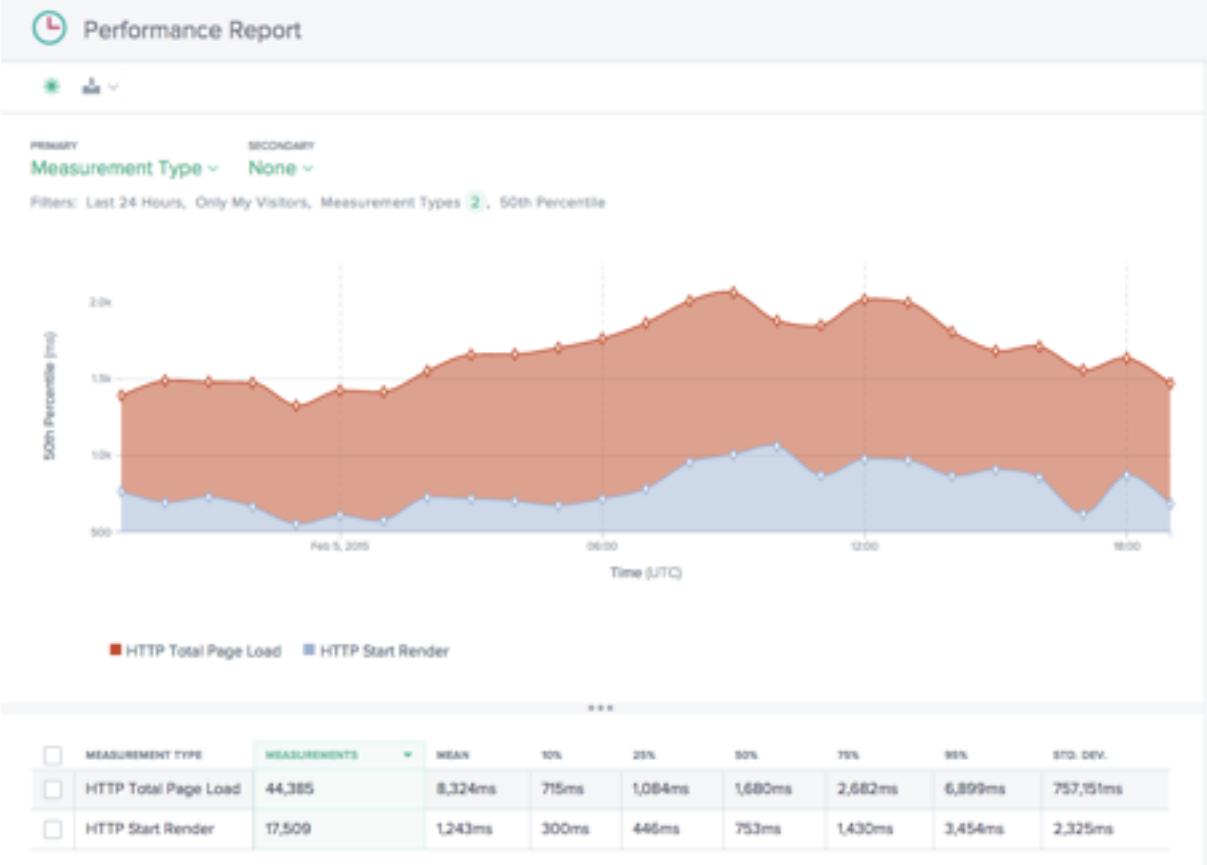
地理位置报告



此报告显示了每个国家/地区的页面加载时间表现。可以根据需要放大地图以查看更大的粒度。

该表列出了每个国家/地区及其关联的页面加载时间表现，以及测量次数（页面查看数）。

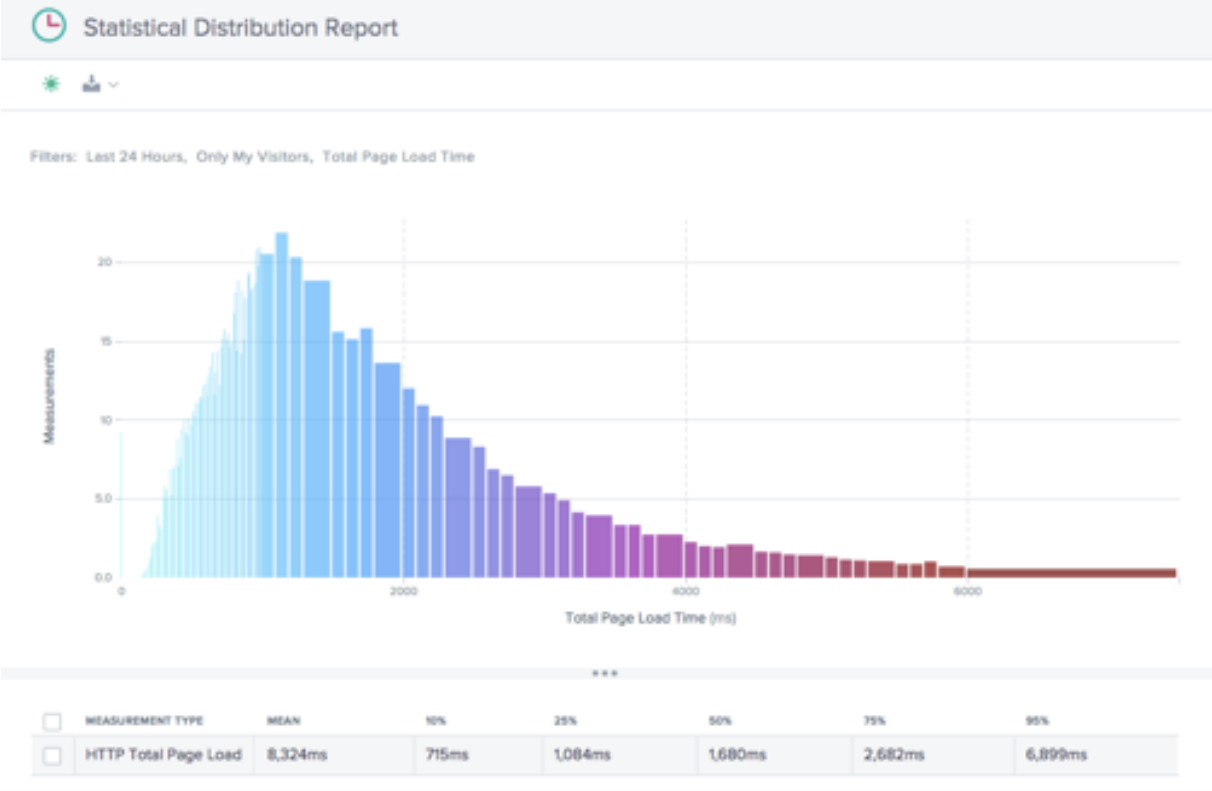
绩效报告



此报告显示了按测量类型细分的导航计时 KPI 在一段时间内的表现。

默认情况下，“开始呈现”和“页面加载时间总计”处于选中状态。可以根据需要添加其他测量类型。

统计分布报告



此报告显示导航计时和页面加载时间值的统计分布。

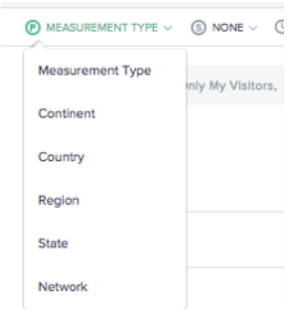
可以通过此报告深入了解针对每个页面加载时间值收集了多少测量值（页面查看数）。

使用导航计时报告

要根据特定的报告需求优化和自定义报告视图，请在导航计时报告中使用以下功能。

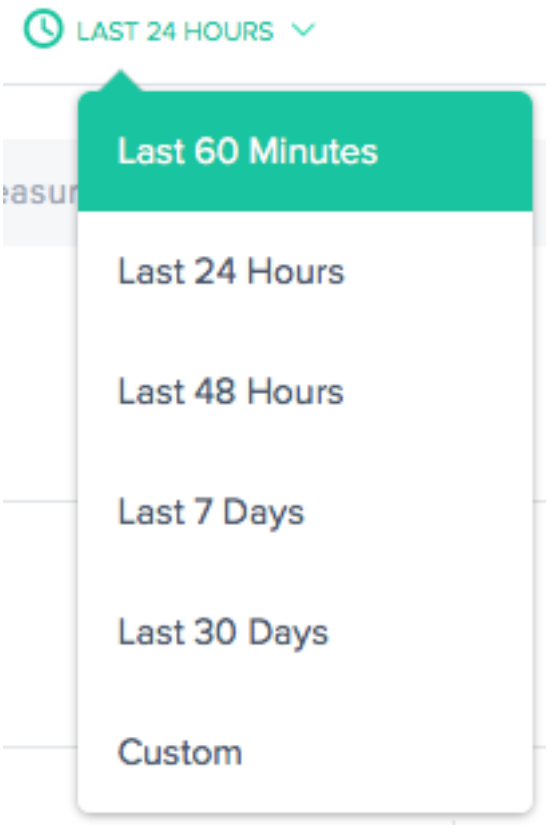
除了报告的标准功能（例如报告共享、背景切换、数据导出等）外，还提供了以下功能：

主要和次要维度



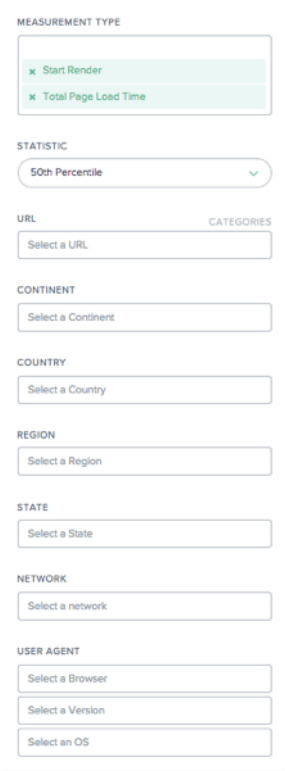
图表的主要维度是通过图表上方的选择列表选择的。使用它作为报告的强大透视视图，按测量类型（默认）、洲、国家/地区、区域、州/省/市/自治区或网络 (ASN) 来呈现数据。还可以选择一个次要维度来进一步优化报告。

过滤器：报告时间范围



可以为以下时间范围生成报告：过去 60 分钟、过去 24 小时、过去 48 小时、过去 7 天、过去 30 天，或自定义范围。默认视图为“过去 24 小时”。

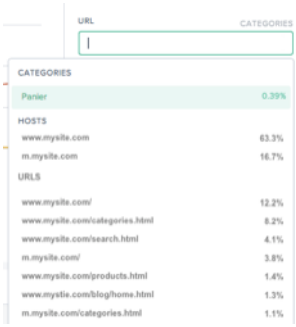
过滤器：强大的向下钻取功能



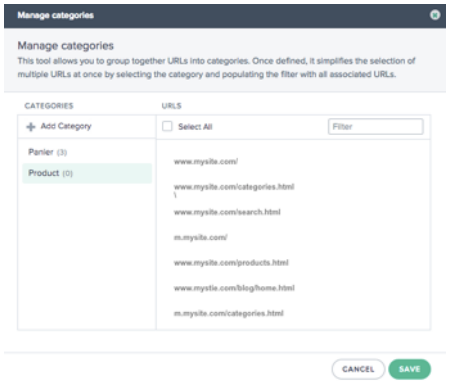
适用于报告的过滤器根据数据情况可能略有不同。导航计时报告中提供了以下过滤器：

- 测量类型–选择一种或多种测量类型进行查看。默认情况下，“开始呈现”和“页面加载时间总计”处于选中状态。
- 统计数据–选择一个统计度量来查看数据。
- **URL** –选择一个或多个 URL 进行查看。此外，您还可以选择主机名或 URL 类别（见下文）。
- 洲–选择要包括的一个或多个大洲
- 国家/地区–选择一个或多个要包括的国家/地区
- 区域–选择一个或多个要包括的地理区域（如果适用）
- 州/省/市/自治区–选择一个或多个要包括的地理州/省/市/自治区（如果适用）
- 网络–选择要包括的一个或多个网络 (ASN)
- 用户代理–选择一个或多个浏览器、浏览器版本和/或操作系统以进一步优化报告数据。

URL 类别



导航计时报告可以按 URL、主机或类别进行过滤。在 **URL** 搜索框中键入内容，可快速查找一个或多个感兴趣的项目。



要创建类别，请单击 **URL** 框右侧的类别。管理类别对话框随即显示。

选择添加类别以创建类别并根据需要对其进行命名。然后为新类别选择感兴趣的 URL。要查找 URL，只需在搜索框中开始输入，将根据搜索文本对 URL 列表进行过滤。

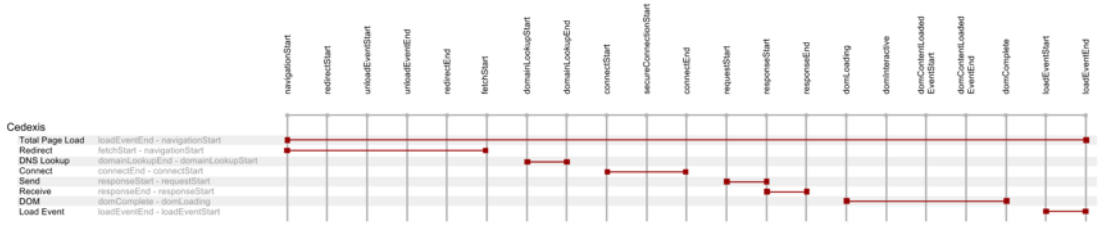
为类别选择了所有 URL 后，单击保存按钮以完成类别定义。

导航计时和页面加载时间数据

Radar 标记能够为实施了该标记的页面收集有关下载性能的详细信息。来自 NavTiming API 的性能信息是从支持该 API 的浏览器（Chrome 6.5+、Firefox 8+、IE9+）收集的。

NetScaler 在客户的门户中显示此信息，允许他们查看实际最终用户在与您的网页进行交互时所体验的性能。

下面是 Radar 通过导航计时提供的每项页面加载指标的图表和描述：



测量	说明	导航计时计算
页面总加载量	网页及其相应组件的完整下载。	`loadEventEnd - navigationStart`
重定向	重定向到页面所用的初始时间。	`fetchStart - navigationStart`
DNS 查询	完成基本页面 URI 的 DNS 解析所需的时间。	`domainLookupEnd - domainLookupStart`
连接	建立 TCP 连接的时间，如果使用 SSL，则包括 SSL。	`connectEnd - connectStart`
发送	初始基本页面的 HTTP 请求和响应时间，不包括任何消息正文。这是用于测量后端服务器延迟的一个良好指标。	`responseStart - requestStart`
接收	接收基本文档的正文 HTML 所花费的时间。	`responseEnd - responseStart`
DOM	下载从基本 HTML 调用的所有媒体、对象并将其加载到浏览器中所花费的时间。	`domComplete - domLoading`
加载事件	执行任何 JavaScript 并在浏览器中呈现页面所花费的时间。	`loadEventEnd - loadEventStart`
开始渲染	“开始呈现”时间是屏幕上显示某些内容的第一个时间点。	作为导航时间 API 的扩展，Chrome/IE 添加了更多的时间。

视频播放数据

June 7, 2021

云平台可视化收集最相关的视频网络交付性能和体验数据的质量，用于报告。视频体验质量直接由视频块交付的质量驱动。Openmix 基于 Radar 网络交付指标进行优化，为用户提供可能的最佳查看体验。在简要描述报表后，详细介绍了如何透视、筛选和自定义报表。

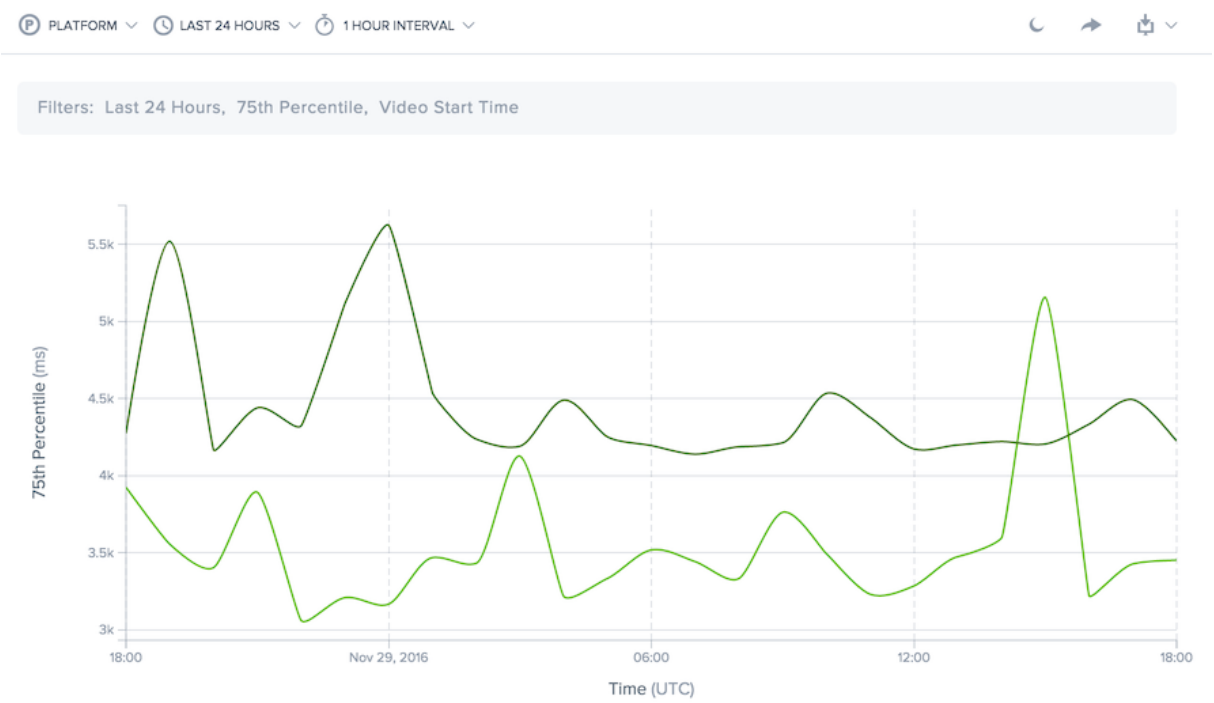
视频播放报告

“视频播放数据”菜单包括以下报告：

1. 绩效报告—随时间推移的视频体验和交付数据。

2. 统计分布报告—视频观看体验随着时间的推移变化。
3. 直方图比较报告 -将视频块传输数据与体验 KPI 质量进行比较。

绩效报告



此报告显示了随时间推移的视频观看体验。它允许您可视化随时间推移的交付趋势，查看正在观看的视频数量，以及查看体验的总体质量。

可以使用允许对多个值进行比较的维度来查看数据。例如，可以按域查看数据，以比较跨多个视频域的传输性能。

报告的时间段可以自定义，从最近的 60 分钟到最近 13 个月内的 30 天。
数据可以按用于提供内容或视频块的内容、主机名和路径、地理位置、网络或查看器用户代理的平台进行筛选。

统计分布报告

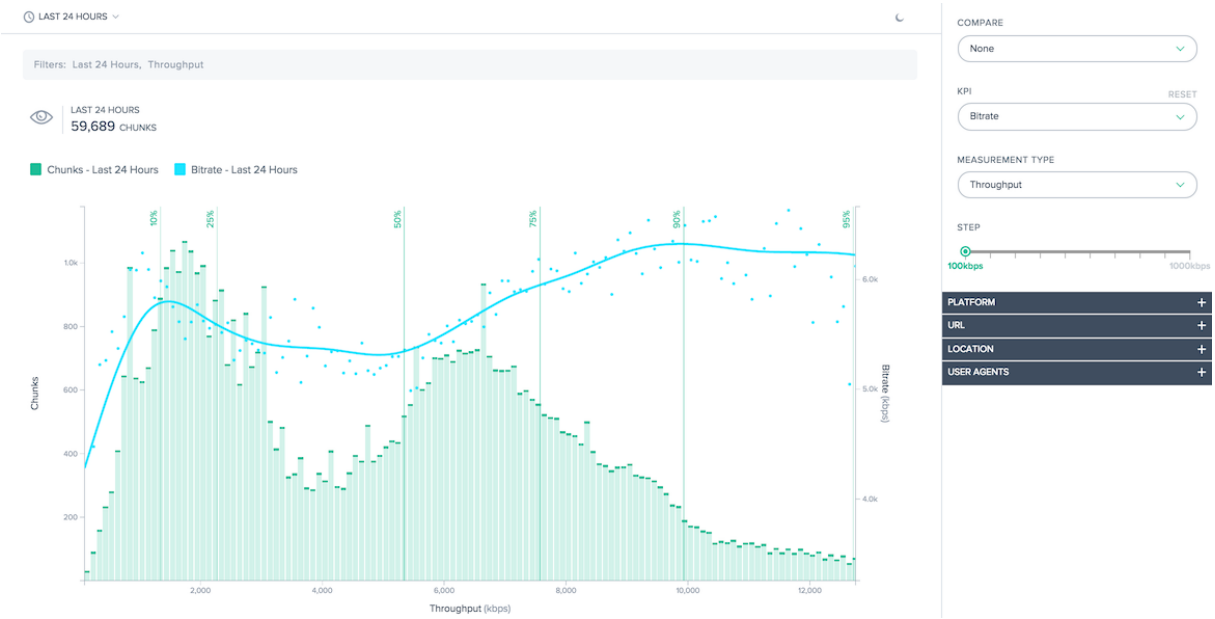
此报告显示视频观看体验随着时间的推移而变化。它允许您可视化视频传输的一致性，并更好地了解整个用户群中的观看体验。该报告计算第 10、25、50、75 和 95 个百分位数的用户性能和平均值。

与绩效报告一样，可以使用允许对多个值进行比较的维度查看数据。例如，可以按平台（服务提供商或服务器）查看数据，以比较多平台交付的一致性。

报告的时间段可以自定义，从最近的 60 分钟到最近 13 个月内的 30 天。

数据可以按用于提供内容或视频块的内容、主机名和路径、地理位置、网络或查看器用户代理的平台进行筛选。

直方图比较报告



本报告显示了视频块传输数据与体验 KPI 质量之间的关系。

本报告有两个主要特点：

- 直方图显示视频块具有指定质量级别（响应时间或吞吐量）的传送频率。
- 单个 KPI 可以叠加在直方图上。线形图表在交付具有指定质量水平的块时生成的 KPI。

例如，直方图将显示 Radar 测量的块吞吐量。KPI 可能会显示，当测量吞吐量较高时，比特率较高，回退缓冲较低。这些功能共同帮助量化传送质量与为观众提供的体验质量之间的关系。

如果默认生成报告不够，则可以自定义直方图存储桶大小，并可以选择分布的特定部分进行显示。

除了将直方图与 KPI 关联之外，还可以直接比较数据。可以选择多个 KPI 进行查看，并可以比较之前的时间段，以显示性能随着时间的推移而发生的变化。

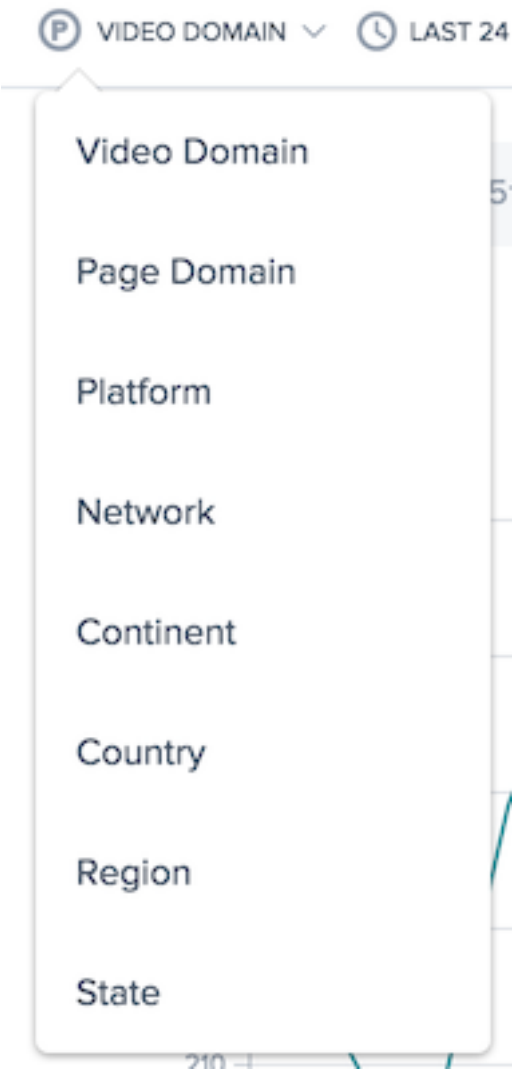
数据可以按用于提供内容或视频块的内容、主机名和路径、地理位置、网络或查看器用户代理的平台进行筛选。

使用视频播放报告

若要根据特定报表需求优化和自定义报表视图，请使用性能和统计分布视频播放报表中的以下功能。

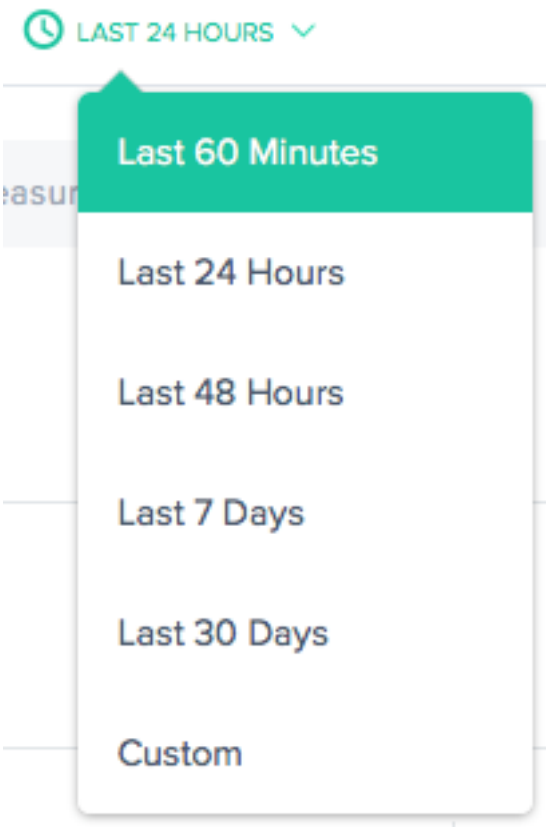
除了报表共享、后台切换、数据导出等标准功能外，还提供以下功能：

主要维度



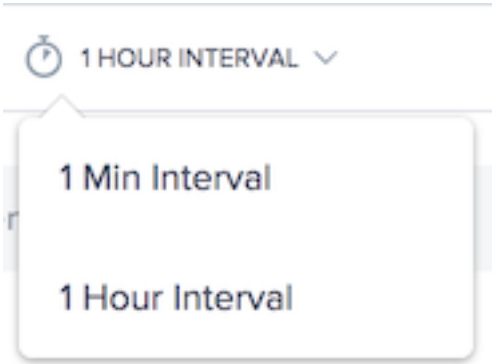
图表的主要维度通过图表上方的选择列表进行选择。使用此功能作为报表的强大枢纽，以视频域、页面域、平台、网络(ASN)、大陆、国家/地区、地区或州等方式表示数据。

筛选器：报告时间范围



可以生成报告的时间范围为最近 60 分钟、最近 24 小时、最近 48 小时、最近 7 天、最近 30 天或自定义范围。默认视图为“最近 24 小时”。

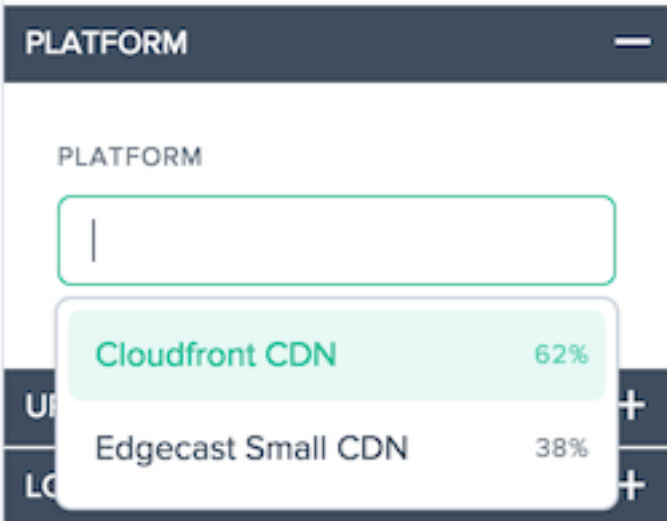
报告间隔



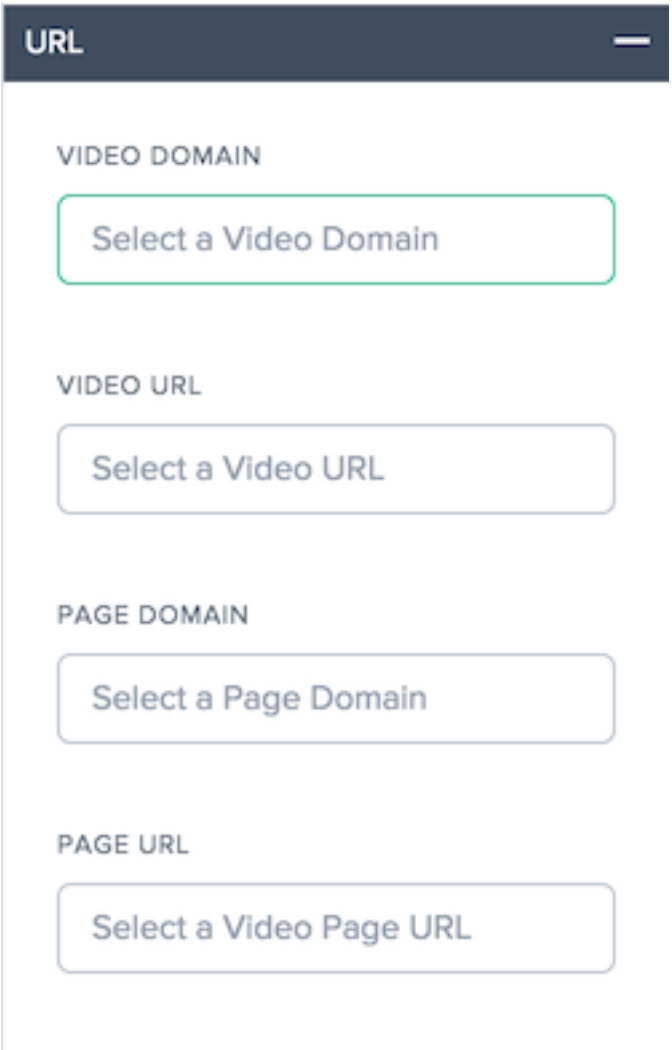
图表的主要维度通过图表上方的选择列表进行选择。这样可以对业绩数据进行细致的报告。

过滤器：强大的向下钻取功能

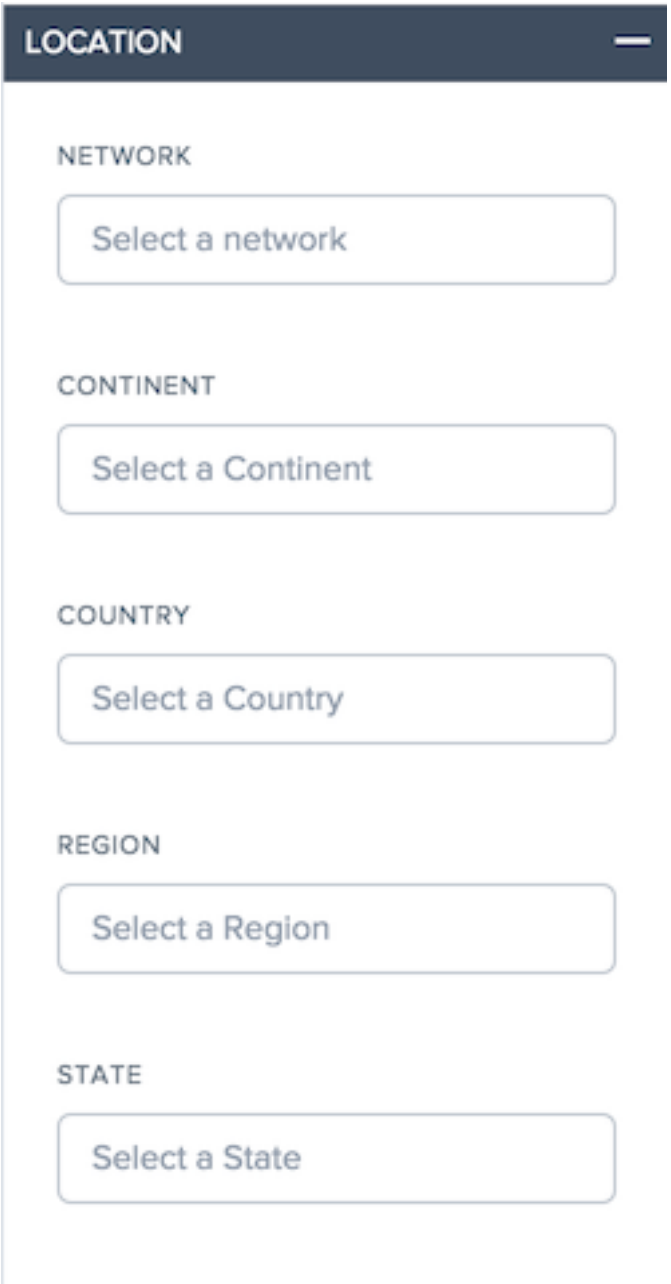
这些报告在哪些筛选器基于数据是适当的方面略有不同。视频播放报告中提供以下内容：



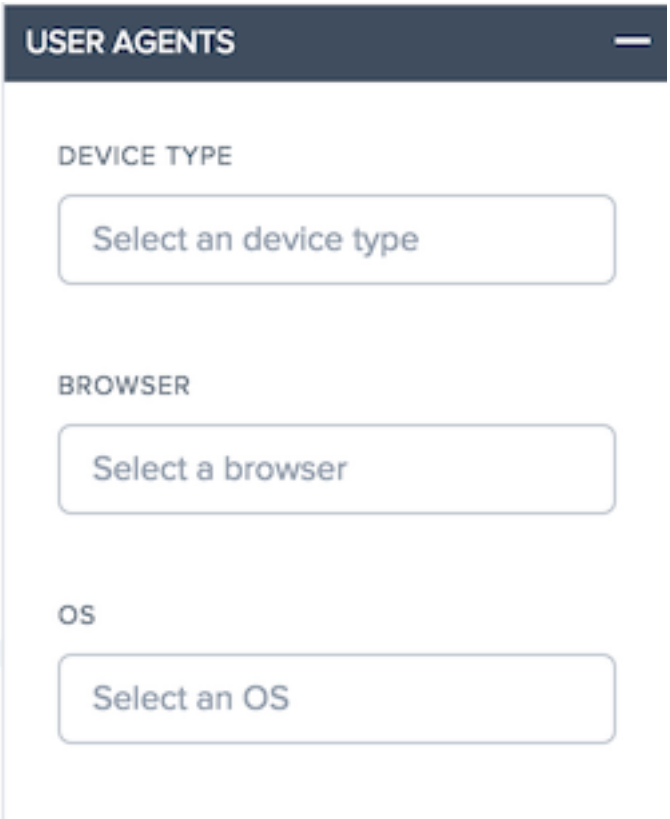
- 平台 -选择一个或平台进行筛选，默认情况下，所有平台都包含在报表中。



- **Video Domain** -选择一个或多个托管视频的主机名，默认情况下，所有主机名都包含在报表中。
- 视频 **URL** -为视频选择一个或多个路径，默认情况下，所有路径都包含在报表中。
- 页面域 -选择一个或多个托管页面的主机名，默认情况下，所有主机名都包含在报表中。
- 页面 **URL** -为页面选择一个或多个路径，默认情况下，所有路径都包含在报表中。



- 网络—选择一个或多个网络 (ASN) 以包括
- 大陆—选择要包括的一个或多个大陆
- 国家/地区—选择一个或多个国家/地区以包括
- 区域—选择一个或多个地理区域（如果适用）以包括
- 州—选择一个或多个地理州（如果适用）以包括

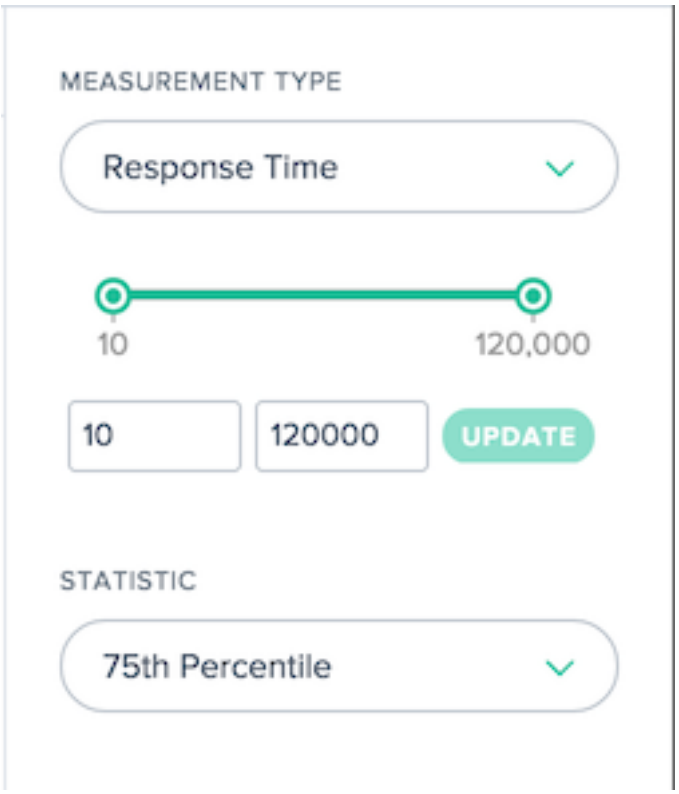


- 用户代理—选择一个或多个设备类型、浏览器和/或操作系统类型，以进一步优化报告数据。

使用视频播放性能报告

若要针对特定报告需求优化和自定义绩效报告，请使用绩效报告中的以下功能。

过滤器：强大的向下钻取功能



这些报告在哪些筛选器基于数据是适当的方面略有不同。视频播放报告中提供以下内容：

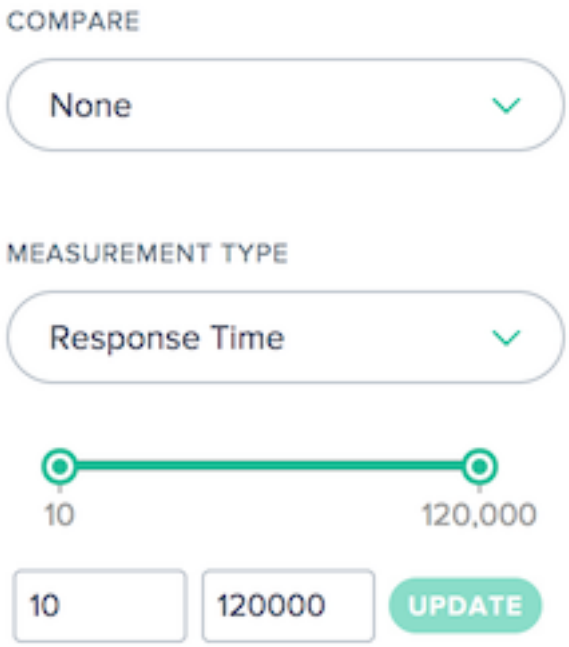
- 测量类型—选择要查看的测量类型，最初选择响应时间。
- 计数滑块 -按报表中所需的最小和最大测量计数过滤数据。
- 统计数据—选择要查看的统计度量。

除了这些特定于报表的筛选器外，标准的“视频播放”筛选器还可用于自定义结果。

使用视频播放统计分布报告

要根据特定报告需求优化和自定义报告，请在统计分布报告中应用以下功能。

过滤器：强大的向下钻取功能



这些报告在哪些筛选器基于数据是适当的方面略有不同。视频播放报告中提供以下内容：

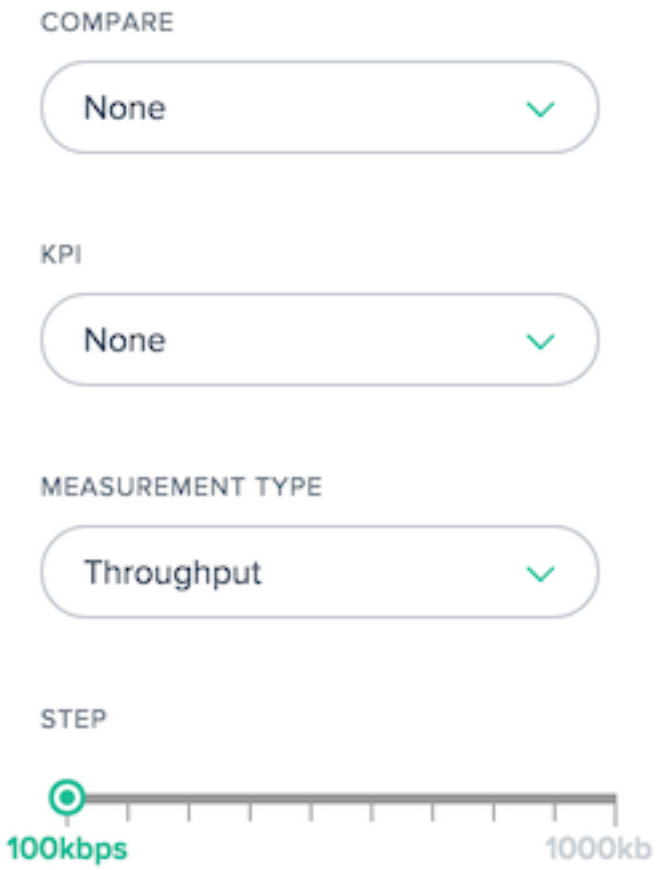
- 比较—选择用于在报表中创建比较的值。根据所做的选择，需要选择用于比较的特定值。生成的分布将并排显示，以便可以轻松比较。
- 测量类型—选择要查看的测量类型，最初选择响应时间。
- 计数滑块 -按报表中所需的最小和最大测量计数过滤数据。

除了这些特定于报表的筛选器外，标准的“视频播放”筛选器还可用于自定义结果。

使用视频播放直方图比较报告

若要根据特定报表需求优化和自定义报表，请在“直方图比较”报表中应用以下功能。

过滤器：强大的向下钻取功能



这些报告在哪些筛选器基于数据是适当的方面略有不同。“直方图比较”报告中提供以下内容：

- 比较—选择用于在报表中创建比较的值。根据所做的选择，需要选择用于比较的特定值。生成的直方图和 KPI 将相互叠加，以便可以轻松比较。
- **KPI** —选择针对直方图测量类型绘制的 KPI。
- 测量类型—选择用于填充直方图的测量类型。
- 步骤滑块 -设置用于生成直方图的桶的大小。

除了这些特定于报表的筛选器外，标准的“视频播放”筛选器还可用于自定义结果。

视频播放数据

数据收集使用的属性和事件以HTML5 视频元素提高体验数据的质量和资源计时 API来自支持 API 的浏览器的视频块数据。

视频数据显示在门户网站中，可以生成包含最终用户体验质量和网络交付性能信息的报告。

以下是所收集的每个视频指标的图表和说明：

测量	说明
每块响应时间	根据资源计时测量结果，区块开始交付所需的时间 (`responseStart - requestStart`)
每块吞吐量	基于资源定时测量值的视频块下载速度。(千位/秒)
已交付比特率	视频的每秒比特率，基于传送的块的大小。(KB)
回收率	回放期间用于回放缓冲的时间百分比。(%)
视频启动失败	初始基页的 HTTP 请求和响应时间，不包括任何消息主体。后端服务器延迟的良好指标。
视频开始时间	尝试播放后开始视频播放所花费的时间。(毫秒)

资源计时数据

June 7, 2021

概述

资源计时数据提供了一个强大的视图到您的网站个别对象级资源的性能。

资源计时可帮助客户根据我们提供的关于连接时间、下载时间和不同响应时间的数据查看页面级对象的网络性能。页面级对象的示例包括、图像、JavaScript 文件、API 调用等。它可以让客户更好地了解页面级别的性能。最终的结果是，客户可以更好地管理他们的交付，并确保整体更好的用户体验质量。

以下部分将指导您了解资源计时数据的配置、数据描述和报告。

资源计时配置

门户中的用户界面允许您直接输入资源计时配置的设置，以替代 JSON 编码。

注意：尽管通过 JSON 编码进行配置仍然可用，但强烈建议您使用 UI 进行配置。

导航

从左侧导航窗格中，选择“影响”->“资源计时数据”->“资源计时配置”。

首次配置

- 在 打开页面上选择“立即开始”以开始。
- 此时将打开“默认配置设置”对话框，以包括或排除资源并输入采样率。

默认配置设置　默认配置设置是开始使用所需的最低设置。有三个主要的默认配置设置：

- 要包括和排除的资源
- 采样率
- 默认提供程序检测

要包括或排除的资源　此功能允许您包含或排除特定资源以收集计时数据。如果留空，则默认情况下包含所有资源（即，不排除任何资源）。

您可以输入资源，如文件名、文件扩展名、文件夹名称、文件路径甚至字符串。字符串中包含的任何内容都将被拾取为资源。

每次输 入 资源名称时，按 Enter 键或 **Return** 键进行提交。如果您在“包括”字段中输入特定资源，则仅包括这些资源，并排除所有其他资源。要排除特定资源，请在“排除”字段中输入这些资源，其他所有资源都将包括在内。您甚至可以编写自定义正则表达式逻辑来自定义包含或排除过程。

采样率　采 样率 允许您输入要从中收集 IRT 数据的访客的一小部分样本。输入介于 0 和 100 之间的值（以百分比为准）。理想情况下，您必须输入采样率的最低百分比-该值足以收集所需数量的资源定时测量值。

注意：资源计时数据收集会给系统带来沉重的负载。此功能可供客户对数据进行采样，而不是为每个 Radar 会话收集数据。

注意：对于拥有大量数据的客户，从 1%的采样率开始。缓慢增加它，直到达到统计上有用的速率。高采样率可能会导致服务器过载、减慢速度，甚至崩溃。

首次采样率设置步骤

1. 从 1% 的采样率开始。等待 24-48 小时，直到您收到一些测量值。
2. 检查 **IRT** 图形，查看它是否在多个资源中看起来平滑。
3. 如果是，则将采样率保持在此值，除非客户具有高网络流量。
4. 或者，如果由于数据量较少，图形看起来不稳定，请慢慢地将其上升。
5. 重复所有检查，并继续缓慢地提高速度（理想情况下每 24-48 小时），直到您收到足够的数据（约 10%）。
6. 对于网络流量较低的客户，您可以上升 10% 以上。但是，对于每次小幅增加，请确保您执行提到的所有检查。

选择“下一步”以转到“默认提供程序检测设置”对话框。

默认提供程序检测　提供程序检测允许您识别提供资源的提供程序或平台。输入配置为检测为资源提供服务的提供程序的主机名。您可以输入多个主机名并为每个主机名单独配置提供程序检测。有关如何配置提供程序检测的信息，请参阅提供商检测部分。

选择“完 成”以完成首次配置。

站点

资 源计时数据 围绕三个主要领域进行设置：

1. 站点
2. 配置
3. 提供商检测

- 从左侧导航窗格中，转到 影响**->** 资源计时数据**->** 资源计时。
- “资源计时数据”下的“站点”页打开。

输入要从中收集资源计时数据的站点的主机名。在“站点”下，您可以找到已在系统中的主机名的列表。如果找不到所需站点（主机名），则可以通过单击“添加”按钮输入该站点。“添加站点”对话框允许您添加新站点以配置资源计时数据。

配置

从门户侧导航菜单中导航到“影响”**>**“资源计时数据”**>**“资源计时数据”**>**“资源计时配置”。“网站”页面在“资源计时数据”下打开。

从顶部导航栏中选择 配置。

您可以通过单击页面右上角的添加按钮来添加新配置。

注意：您还可能会在页面上看到包括默认配置在内的配置列表。您可以选择默认配置，或从列表中编辑现有配置，而不是添加新配置。

添加配置

要添加新配置，请单击页面右上角的“添加”按钮。

此时将打开“添加资源时间配置”对话框。这允许您输入新的配置 名称，添加 要包括或排除的资源，以及添加 采样率。

编辑配置

要编辑现有配置，请选择 配置名称旁边的编辑 配置按钮。

提供商检测

提供程序检测确定哪个平台在 Openmix 后面处理域的请求时，该域处理该请求。建议所有已启用资源计时数据的客户配置提供商检测服务。

- 要配置提供程序检测，请从左侧导航窗格导航至“影响” **>** “资源计时数据” **>** “资源计时配置”。
- “资源计时数据”下的“站点”页打开。从顶部导航栏中选择 提供程序检测。

单击页面右上角的添加按钮。

在“添加提供程序检测配置”对话框中，输入以下内容。

配置名称

输入配置的名称。名称不能包含任何空格或特殊字符，且必须是唯一的。

主机名

输入要为其配置提供程序检测的主机名。您可以输入多个主机名并单独指定每个主机名的检测方法。

检测方法

检测方法涉及为输入的每个主机名指定测试对象的类型（无论是标准还是自定义）和路径（到测试对象）。

标准测试对象　在标准测试对象的情况下，路径可以指定为 **/provider-detection/platform.html** 和 **/provider-detection/platform.png**。对于此设置，**/provider-detection/** 将是您的目录路径。

注意：输入上述路径不是强制性的。但是，对于您输入的任何路径，请确保在目录路径中找到了 **platform.html** 和 **platform.png** 文件。

自定义测试对象　对于自定义测试对象，您需要确保在输入的确切路径中找到测试对象。例如，对于主机名 `foo.com` 和路径 `static/bar.css`，URL `http://foo.com/static/bar.css` 必须有效。

标题

平台标题　如果选择 平台标题，请确保在`X-CDN-Forward: <CDN name>`测试对象上发送。如果`X-CDN-Forward: <CDN name>` 在响应标头中找不到，则客户端将继续进入下一个测试，该测试可以使用 **Custom** 进行指定。

自定义　如果选择“自定义”，请确保您输入的正则表达式与 CDN 的响应标头之一完全匹配。

如果添加多个响应标头，则每个响应标头都会按照在门户中输入的相同顺序对正则表达式进行测试。

单击 创建 以完成此过程。现在，您可以在“提供程序检测”下的列表中看到新创建的配置。如果要修改配置，请单击编辑或删除图标，或删除它。

您的配置现在已完成。要或者通过 JSON 编码配置提供商检测，请联系您的帐户代表。

资源计时测量说明

下表显示了收集的资源计时测量值。

测量	说明	资源时间计算
DNS 查找时间	资源的 DNS 解析所需的时间。称为 DNS 阶段。	`domainLookupEnd - domainLookupStart`
TCP 连接时间	浏览器与服务器建立连接所需的时间。称为 TCP 阶段。	`connectEnd - connectStart`
等待时间到第一个字节 **(TTFB)**	TTFB 是浏览器在开始接收资源之前等待的时间。	`responseStart - startTime`
往返时间 **(RTT)**	从请求开始到响应开始的时间。称为请求阶段。	`responseStart - requestStart`
等待时间	响应开始和响应结束之间的差异。称为响应阶段。响应通常来自服务器、缓存或本地资源。	`responseEnd - responseStart`
持续时间	从进程开始到完全接收资源的总时间。	`responseEnd - startTime`

了解更多信息，请访问https://www.w3.org/TR/resource-timing-1/#process

资源计时报告

“资 源计时”菜单包括以下报表：

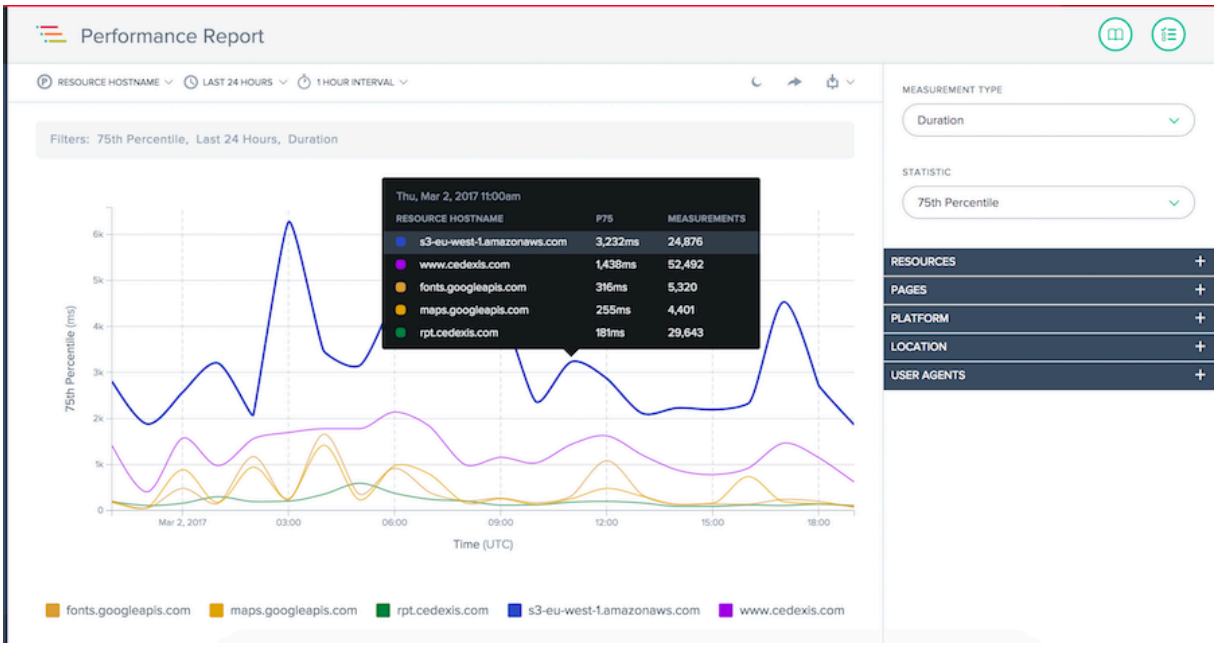
1. 绩效报告—随时间推移的资源计时测量数据。
2. 统计分布报告—通过统计分布报告视图查看资源计时数据。

绩效报告

该报告深入了解每个选定值的资源计时性能数据。

默认报告视图：

1. 维度：资源主机名
2. 测量：持续时间
3. 时间范围：过去 24 小时

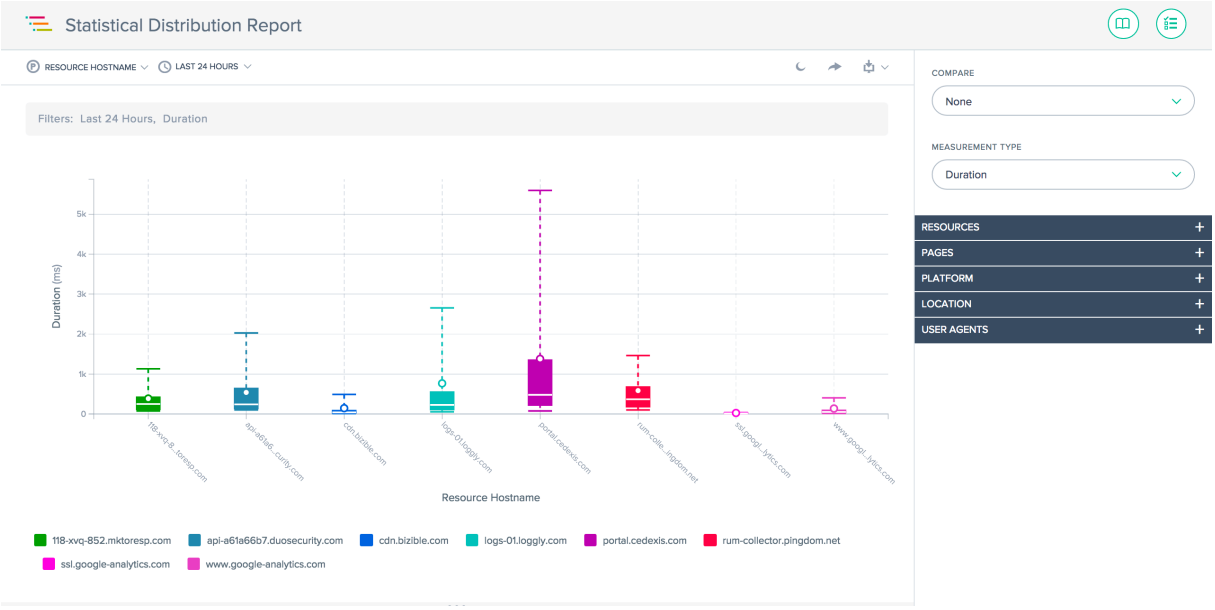


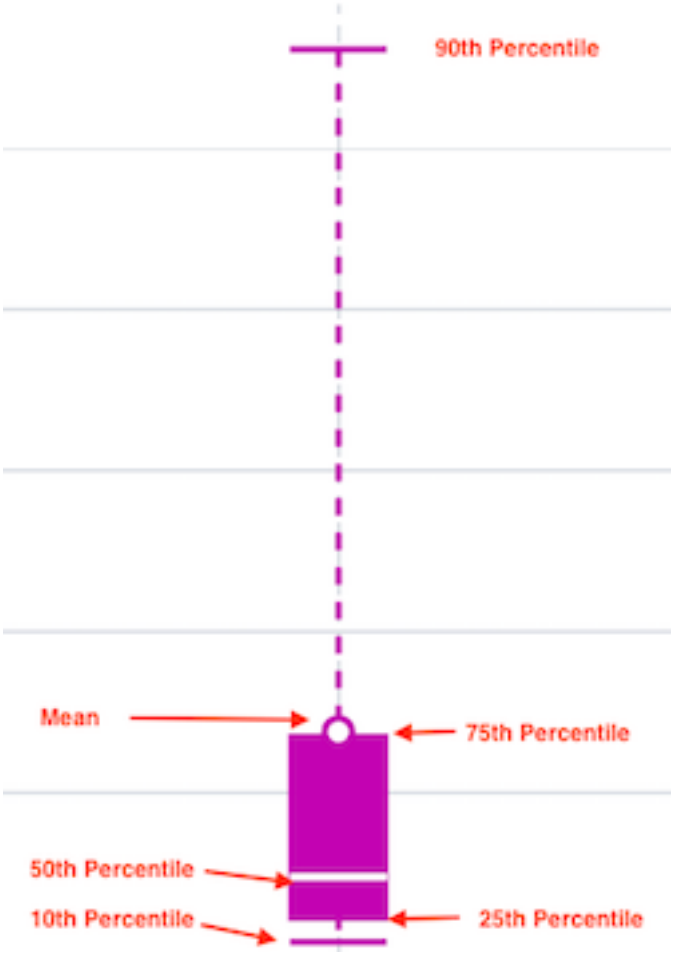
统计分布报告

本报告显示了资源时间的统计分布。该报告深入了解每个资源值收集了多少测量值。您可以根据资源、页面、平台、位置和用户代理进行筛选，在测量类型之间切换，并在特定页面、位置和用户代理详细信息之间运行比较。

默认报告视图：

1. 维度：资源主机名
2. 测量：持续时间
3. 时间范围：过去 24 小时



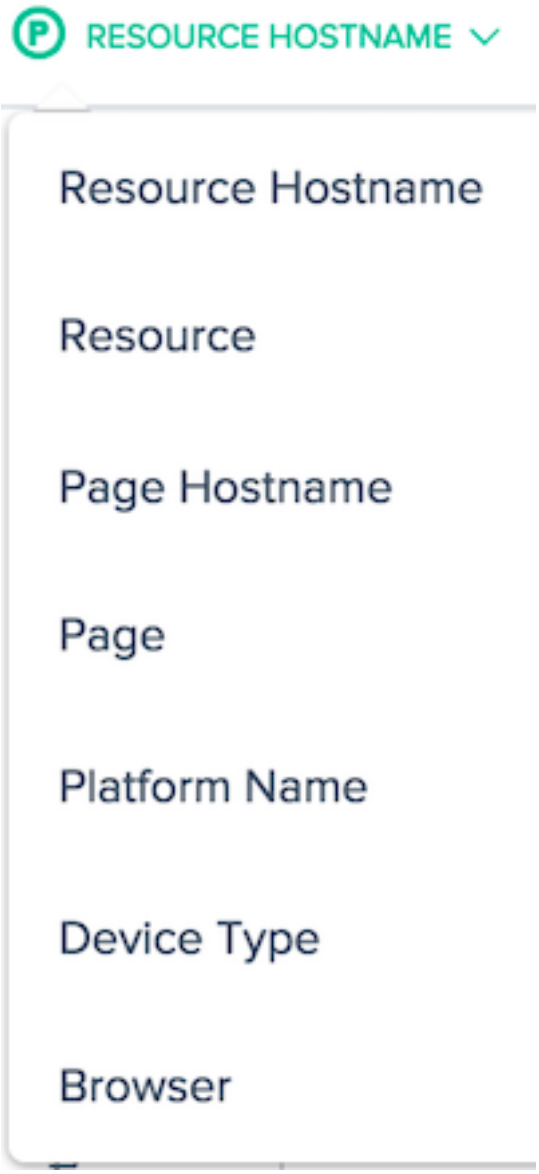


晶须图

使用报告

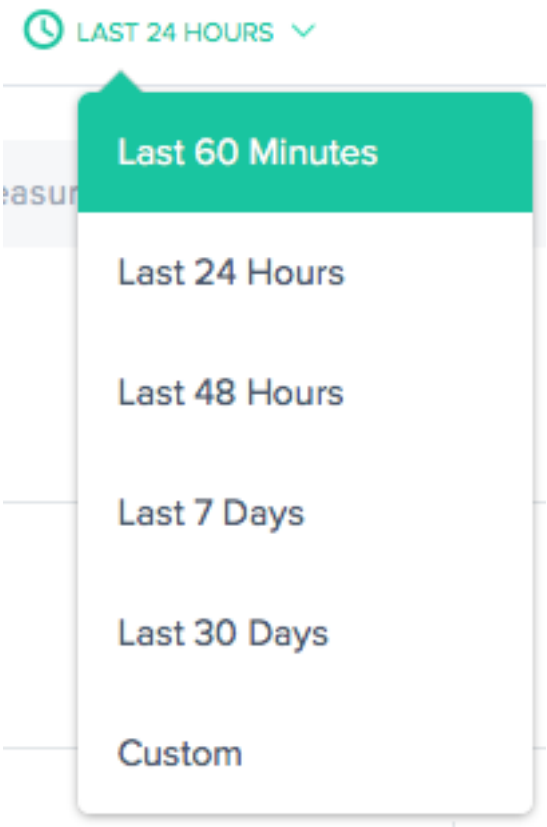
若要针对特定报表需求优化和自定义报表视图，请使用“性能”和“统计分布”报表中的以下功能。除了报表共享、后台切换、数据导出等标准功能外，还提供以下功能：

主要维度



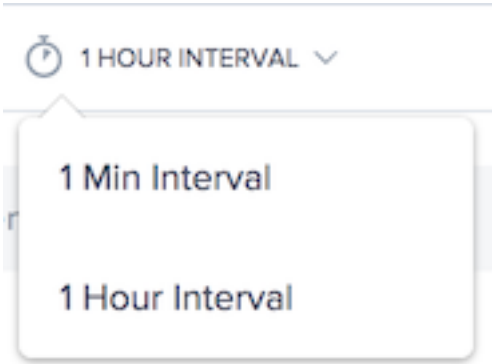
图表的主要维度通过图表上方的菜单进行选择。您可以将它用作报表上的强大数据透视表，以表达资源主机名、页面主机名、页面和平台名称的数据。

筛选器：报告时间范围



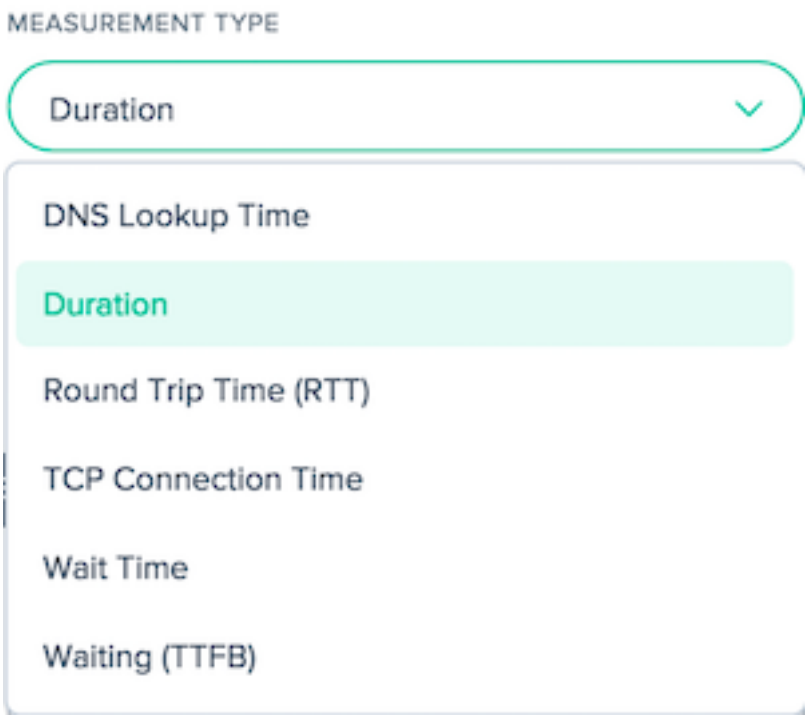
可以生成报告的时间范围为最近 60 分钟、最近 24 小时、最近 48 小时、最近 7 天、最近 30 天或自定义范围。默认视图为“最近 24 小时”。

报告间隔



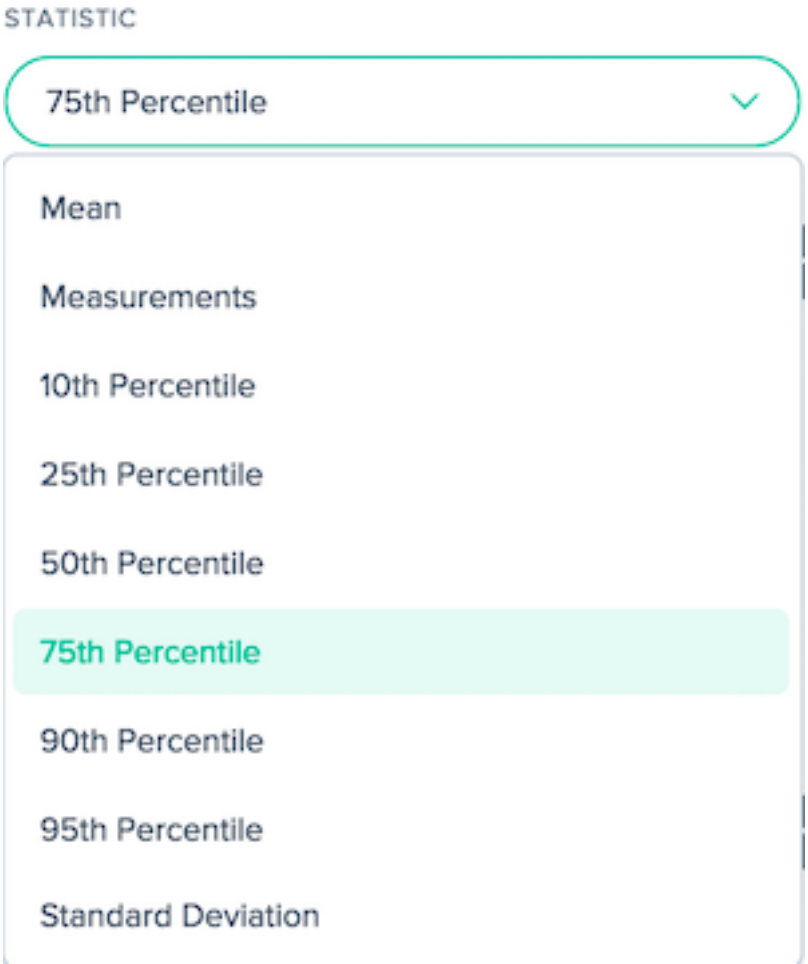
选择要在其中查看趋势图的时间间隔。根据您正在查看的日期范围，您可以在一分钟、一小时或一天的间隔内查看图表。

测量类型



选择要查看资源计时所针对的测量类型。从持续时间、DNS 查找时间、往返时间 (RTT)、TCP 连接时间、等待时间和等待 (TTFB) 中进行选择。

选择一个统计度量以查看数据。



过滤器：强大的向下钻取功能

这些报告在哪些筛选器基于数据是适当的方面略有不同。以下筛选器选项在报表中可用：

资源主机名称：

RESOURCE HOSTNAME

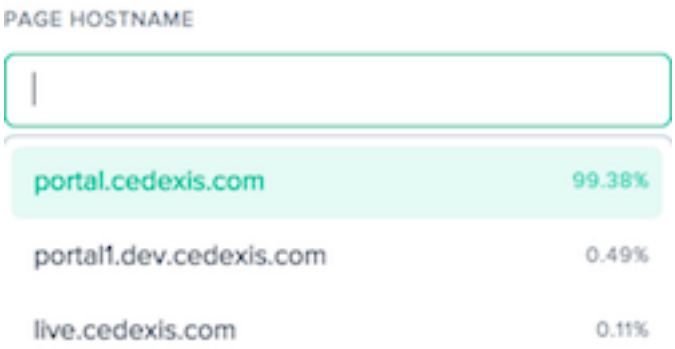
portal.cedexis.com	56.84%
www.google-analytics.com	14.7%
cdn.bizible.com	9.9%
logs-01.loggly.com	9.02%
118-xvq-852.mktoresp.com	7.46%
rum-collector.pingdom.net	2.02%
api-a61a66b7.duosecurity.com	0.05%
ssl.google-analytics.com	0.01%
api-ext.intricately.com	0.01%

资源：

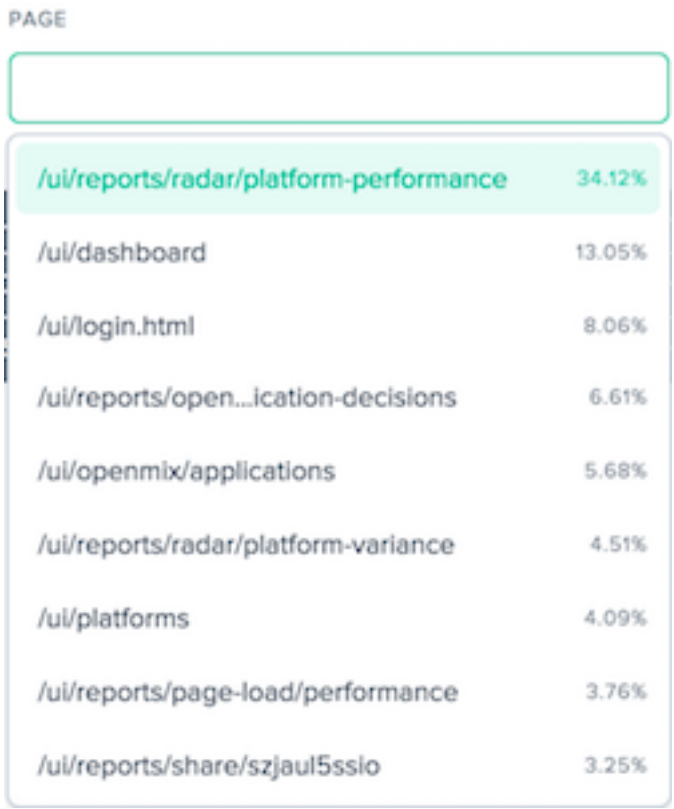
RESOURCE

/collect	11.92%
/m/ipv	9.25%
/inputs/9260e0ca...-24a42dc71056.gif	9.02%
/api/v2/reporting/radar.json	5.73%
/webevents/visitWebPage	5.67%
/api/v2/reporting/openmix.json	4.67%
/r/collect	2.77%
/provider-detection/platform.htm	2.25%
/api/v2/reporting/session.json	2.03%

页面主机名称：

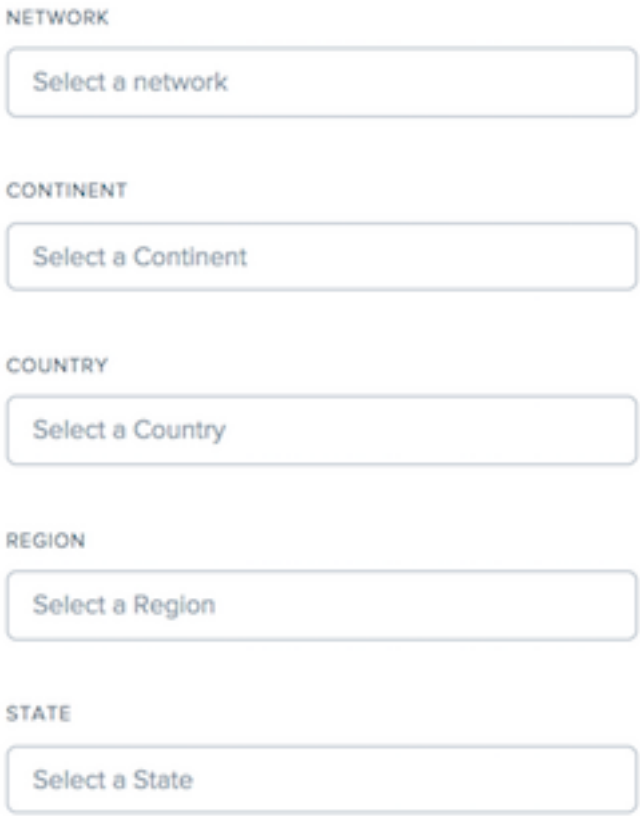


页面：

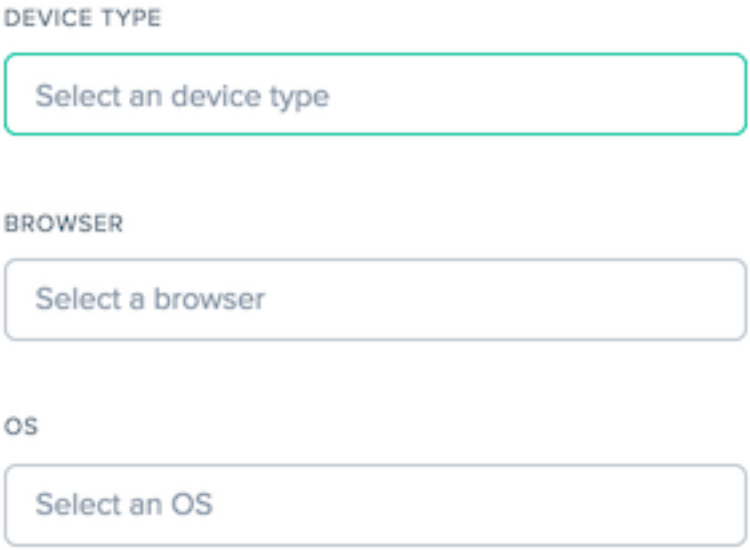


平台名称：

地点：网络、大陆、国家、地区和州：



用户代理：设备类型、浏览器和 **IOS**：

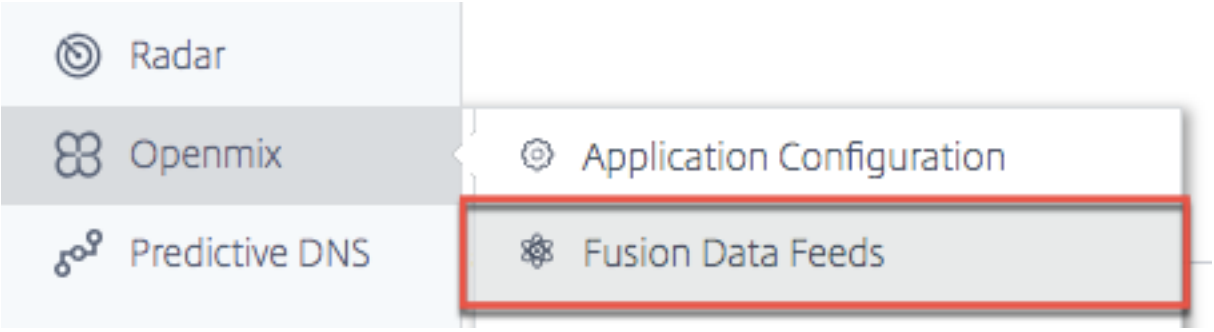


Fusion 集成

September 22, 2023

除 Radar 和 Sonar 数据外，Openmix 还可以在其决策条件中使用第三方数据。例如，您可以集成您已在使用的现有综合监控服务。或者，您可以使用 CDN 提供程序提供的最新使用数据做出基于成本的决策。

Fusion 菜单



可以从导航菜单访问“Fusion 数据馈送”，它位于 **Openmix** 下。

例如，一些与 Openmix 应用程序配合使用的常用 Fusion 数据馈送：

1. 服务器可用性—从 CatchPoint、Rigor 和 Pingdom 之类的第三方提供程序提取数据，以确定特定主机或应用程序的可访问性。
2. 服务器监控—来自 Rackspace 和 New Relic 等提供程序的指标允许 Openmix 在路由决策中考虑服务器运行时间指标，例如内存使用情况、CPU 消耗、可用磁盘空间和网络延迟。Openmix 可以使用这些指标来做出开/关路由决策，还可以使用这些指标通过切断来自某个已加载服务器的流量来逐步进行路由更改。
3. **CDN** 成本控制 - 从所有主要 CDN 中提取带宽和使用情况统计信息，并在 Openmix 应用程序中实时提供这些数据，以影响路由决策。
4. 客户定义的自定义数据馈送 - 您提供的端点上的任何数据都可以提取并在自定义 Openmix 应用程序中提供，以用于路由决策。

Fusion 集成

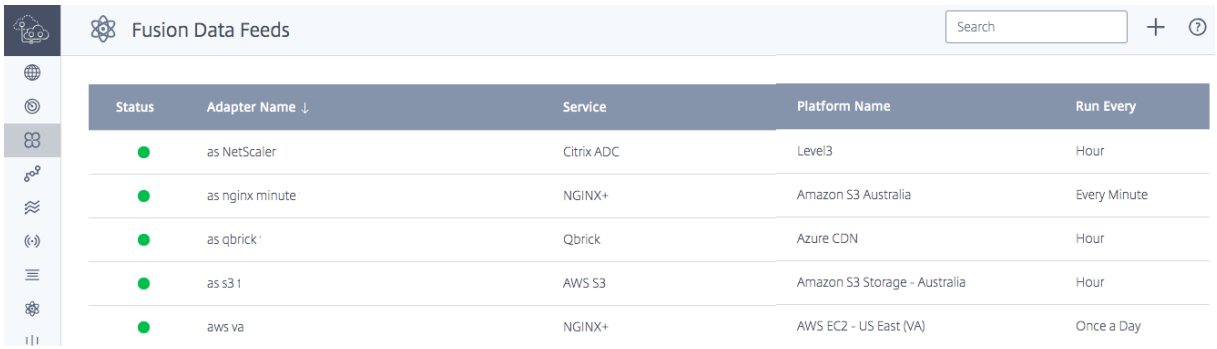
服务	类型
Akamai	CDN 带宽、CDN 使用情况
AWS CloudFront	CDN 使用情况
AWS CloudWatch	实例指标

服务	类型
AWS ELB	负载均衡器指标
AWS S3	自定义数据馈送
Azure	实例指标
Catchpoint	警报
CDNetworks	CDN 带宽、CDN 使用情况
ChinaCache	CDN 带宽
ChinaNetCenter	CDN 带宽
NetScaler	自定义数据馈送
Datadog	警报
Edgecast	CDN 带宽、CDN 使用情况
Fastly	CDN 使用情况
Fusion Direct	自定义数据馈送
Highwinds	CDN 使用情况
HTTP GET	自定义数据馈送
HTTP GET with Availability	自定义数据馈送
JSON	自定义数据馈送
Keynote	Web 监视器
Level3	CDN 带宽、CDN 使用情况
Limelight	CDN 使用情况
maxCDN	CDN 带宽、CDN 使用情况
New Relic Apdex	应用程序分数
全新 Relic 服务器监控	实例指标
NGINX	负载均衡器指标
NGINX+	负载均衡器指标
Pingdom	Web 监视器
Qbrick	CDN 使用情况
Rackspace	实例指标
Rigor	Web 监视器
SFR	CDN 带宽、CDN 使用情况

服务	类型
TCP Ping	Web 监视器
Touchstream	视频监控

Fusion 源

以下屏幕显示了所有已配置的 Fusion 数据馈送。以下列表提供了数据馈送和当前状态的概览。

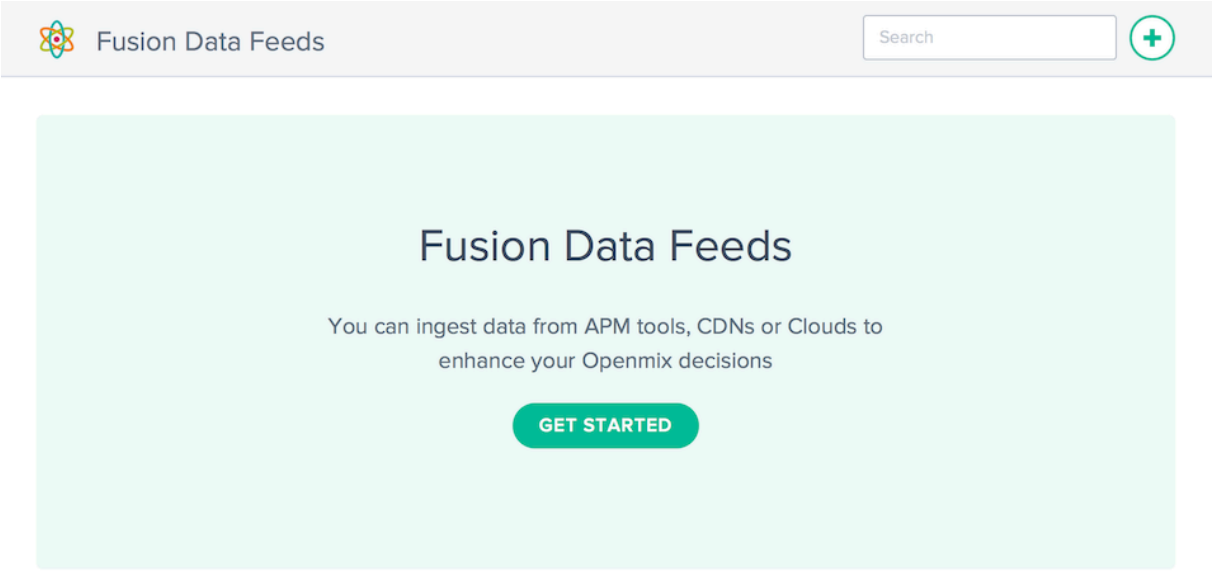


这些列提供以下信息：

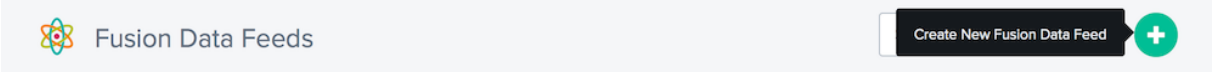
标题	说明
状态	数据馈送的当前状态。状态显示为：+ 绿色表示数据馈送正在成功从服务中检索数据；+ 黄色表示数据馈送正在等待从服务中检索数据；或 + 红色表示数据馈送无法从服务中检索数据
数据馈送名称	数据馈送中给出的名称。可选，如果未指定，则默认为“服务 - 平台名称”。
服务	数据馈送使用的服务的名称。
ID	数据馈送的 ID。这是通过 API 访问 Fusion 所必需的。
平台名称	与数据馈送关联的平台名称。
运行频率	从服务更新数据馈送的频率。

创建数据馈送

如果未配置 Fusion 数据馈送，则会出现欢迎屏幕，提示您创建数据馈送。

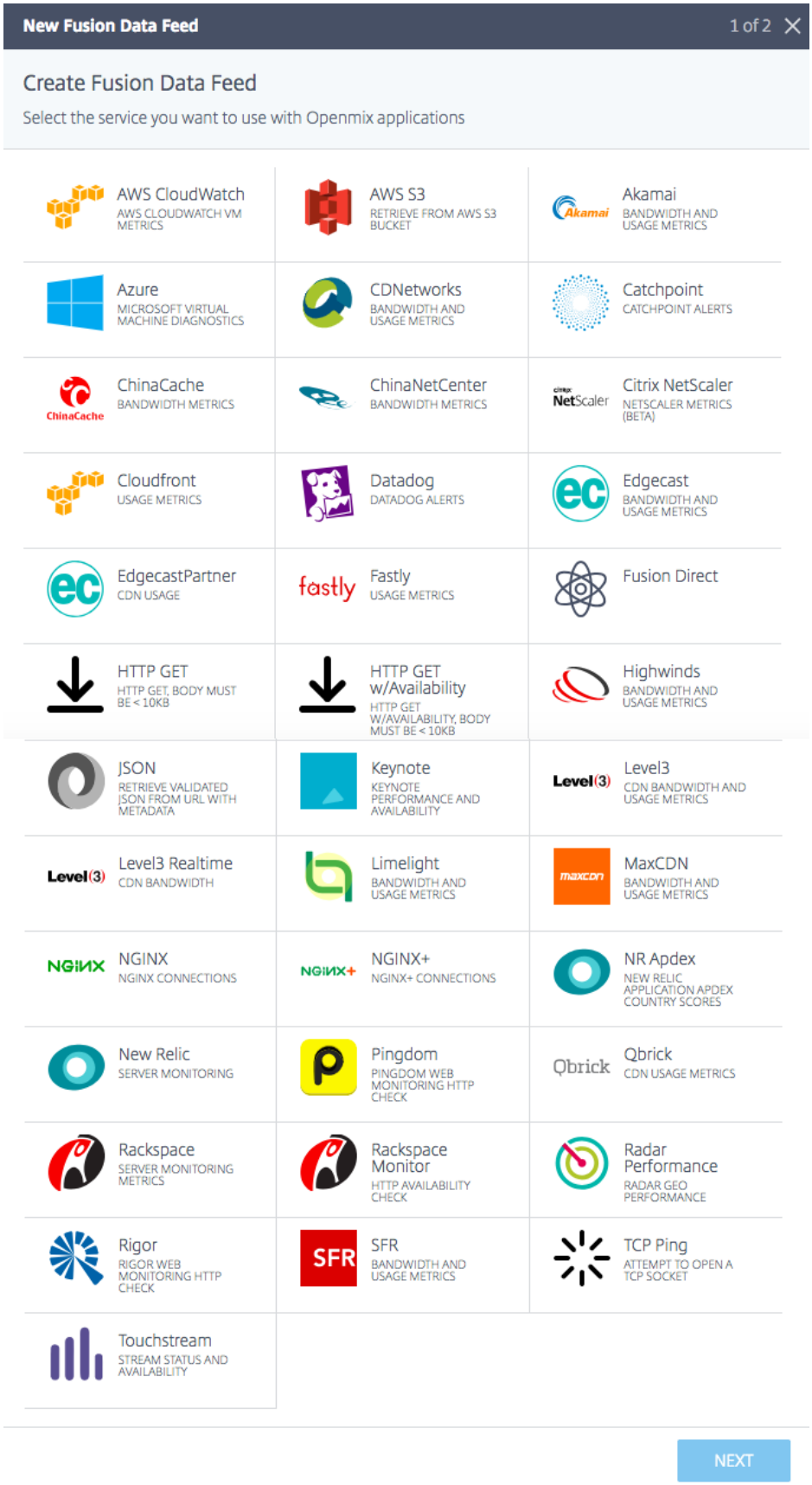


单击开始按钮或单击 **+** 来设置新的数据馈送。

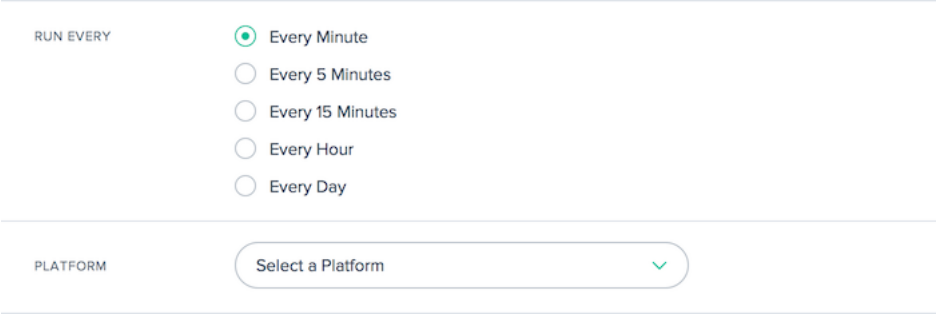


新建数据馈送

单击您要集成的服务的图标，并填写所需的配置字段。



每项服务都需要不同的配置参数。您需要用户名和密码或生成的令牌以用于身份验证，还需要任何其他特定于服务的配置。



所有 Fusion 数据馈送都与之前在 NetScaler Intelligent Traffic Management 门户中创建的平台相关联。这允许 Openmix 应用程序为每个平台查询外部 Fusion 数据，并根据路由逻辑确定是否必须将该平台视为可用于路由决策。

大多数馈送需要配置以下值：

输入项目	说明
运行频率	从外部服务更新数据馈送的频率。Fusion 按指定的时间间隔调用该服务，并根据新数据更新 Openmix 应用程序。
平台	与 Openmix 应用程序中的 Fusion 数据关联的平台。

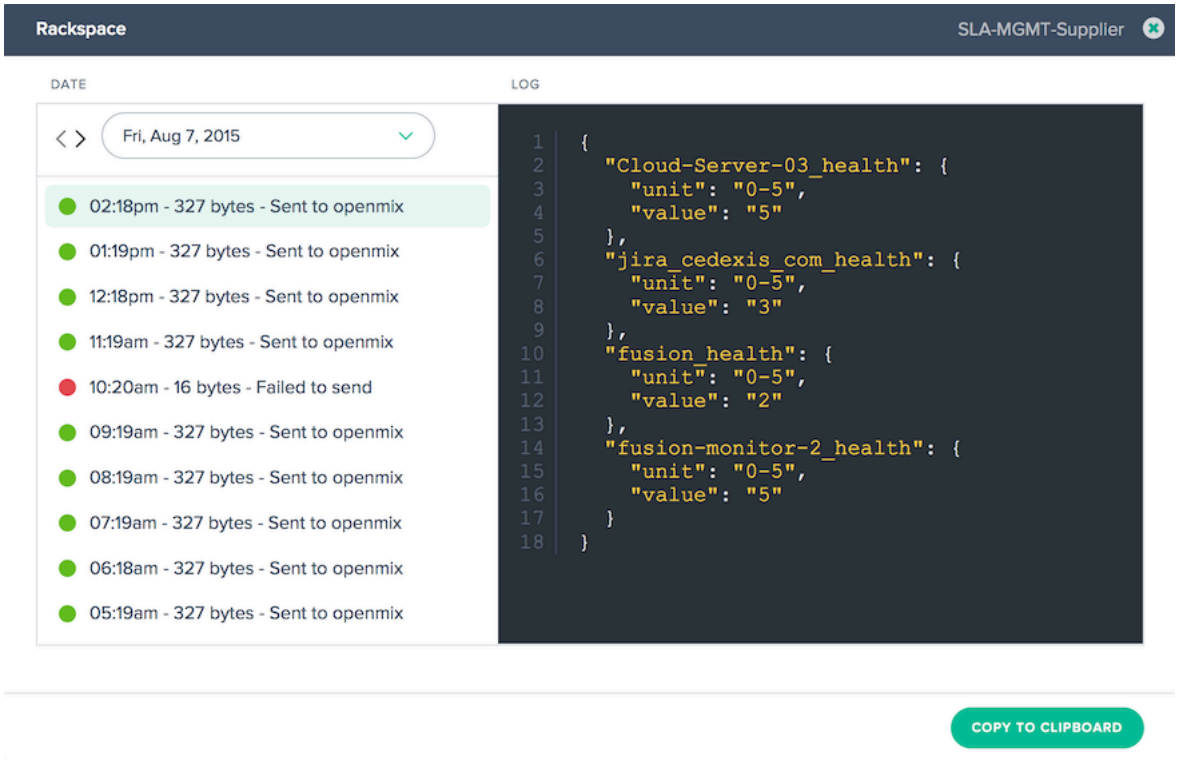
编辑数据馈送

要想编辑某个 Fusion 数据馈送，只需在表中单击该数据馈送并单击编辑按钮。

更改配置后，单击保存。这会将您带回数据馈送列表，并在数据馈送中保存并应用您的更改。

数据馈送历史记录

Fusion 会在数据馈送历史记录中收集每次运行的最后 100 个响应。您可以查看数据馈送状态、有关数据的信息以及从服务返回的负载。在列表中选择特定的数据馈送后，单击日志历史记录以显示该数据馈送的历史记录。



要更改所选日期，可以单击 **<** 或 ** 按钮从当前所选日期向后或向前移动，或者从列表中选择特定日期。选择特定实例的时间戳，将会显示从服务返回的数据。

出故障的数据馈送

对出故障的 Fusion 馈送的 Fusion 隔离

如果馈送配置为以小于 24 小时的轮询间隔运行，则会向客户出故障的 Fusion 数据馈送应用 Fusion 隔离。Fusion 将应用隔离逻辑来阻止这些出故障的馈送运行。这是为了节省资源（CPU/内存）并避免对其他有效的 Fusion 数据馈送产生任何负面影响。

隔离逻辑是通过逐步“减少”与失败的 Fusion 源的交互来实现的。这种情况一直持续到 Fusion 订阅源被隔离 24 小时。此时，Fusion 馈送将每 24 小时尝试运行一次。出故障的 Fusion 数据馈送永远不会完全关闭。它将继续运行，每 24 小时至少运行两次。

重要：

- Fusion 数据馈送将始终至少连续运行两次，并且在失败两次后才会进入隔离逻辑。例如，如果一分钟的馈送连续两次运行失败，则它将进入隔离逻辑。
- 如果 Fusion 数据馈送在任何时候运行成功，它就会从隔离逻辑中删除，并将按定期安排的时间间隔再次运行。
- 如果 Fusion 馈送在任何时候得以更新（即如果用户输入了错误的 URL 并进行了更正），则无论轮询间隔如何，Fusion 馈送都将在一分钟内尝试再次运行。如果成功，则会将其从隔离逻辑中删除。如果继续失败，则将应用隔离逻辑。

全球 CDN 清除

June 7, 2021

全局 CDN 清除是一种同时清除多个 CDN 中的数据的方法，这使得管理多个 CDN 变得更加容易。它允许您连接要清除的 CDN，指定要清除的所有附加服务的 URI，然后单击“清除”按钮。在所有连接的 CDN 中启动清除。

全局 CDN 清除功能基于三个主要组件：

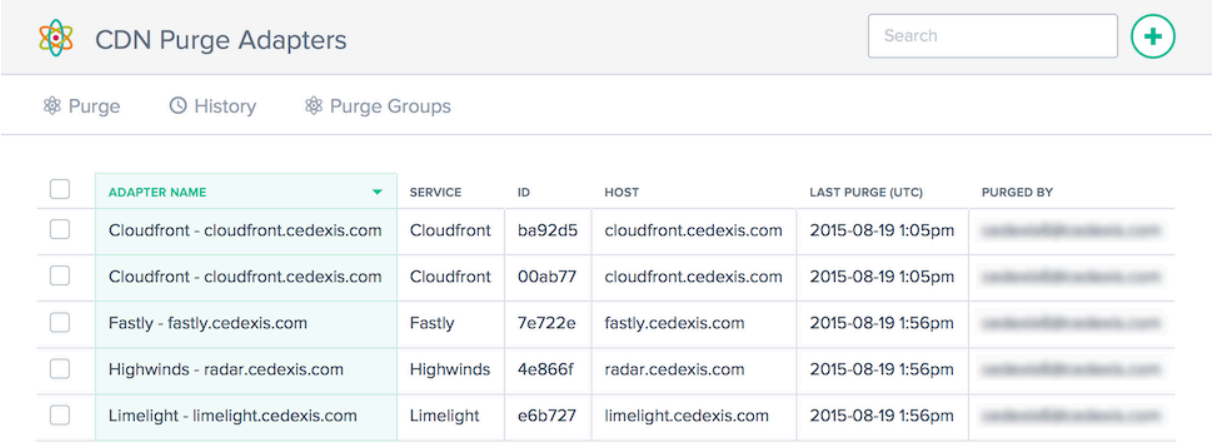
1. **CDN** 清除适配器—需要为要清除的每个 CDN /host 名组合创建 CDN 清除适配器。CDN 清除适配器收集执行清除所需的信息，例如：服务选择、身份验证信息、主机名和其他服务特定信息。对于要在 CDN 上清除的每个主机名，您需要一个 CDN 清除适配器。
2. **URI** —清除针对 CDN 上的特定位置运行。
3. 清除组 -清除组允许您创建 CDN 清除适配器和 URI 的逻辑集合，这些集合使用一个命令清除。例如，您可以清除 2 个不同 CDN 或开发、测试和生产环境中存在的目录上的‘/media’目录。

必须将 CDN 清除适配器设置为运行清除。URI 和多个 CDN 清除可以单独指定，但建议您的安装程序清除组来管理经常运行的常见清除。

全局 CDN 清除可以从导航菜单的顶层作为 CDN 清除进行访问。

CDN 清除适配器

下面的屏幕显示了所有已配置的 CDN 清除适配器。该列表提供了已配置的 CDN 适配器的概述，并允许执行清除。



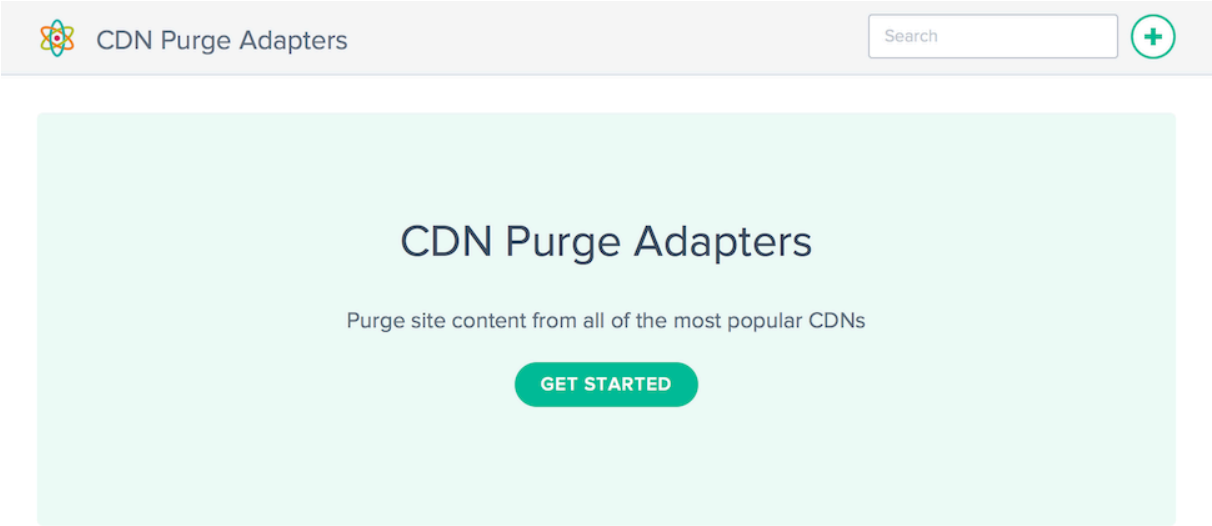
这些列提供以下信息：

标题	说明
适配器名称	给适配器的名称。可选，如果未指定，则默认为“服务-主机”。

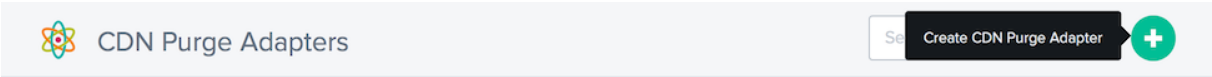
标题	说明
服务	配置清除使用的 CDN 服务的名称。
ID	CDN 适配器的 ID。这是通过 API 访问 Fusion 所需的。
主机	将清除配置为运行对象的主机。服务有时会调用此设置：主机、主机名、平台等。
上次清除 **(UTC)**	上次运行清除的时间和日期（UTC）。
清除者	上次运行清除的用户。

创建 **CDN** 清除适配器

要使用全局 CDN 清除，您需要添加 CDN 和主机名配置。当您第一次打开 **CDN** 清除时，系统会提示您创建 CDN 清除适配器。

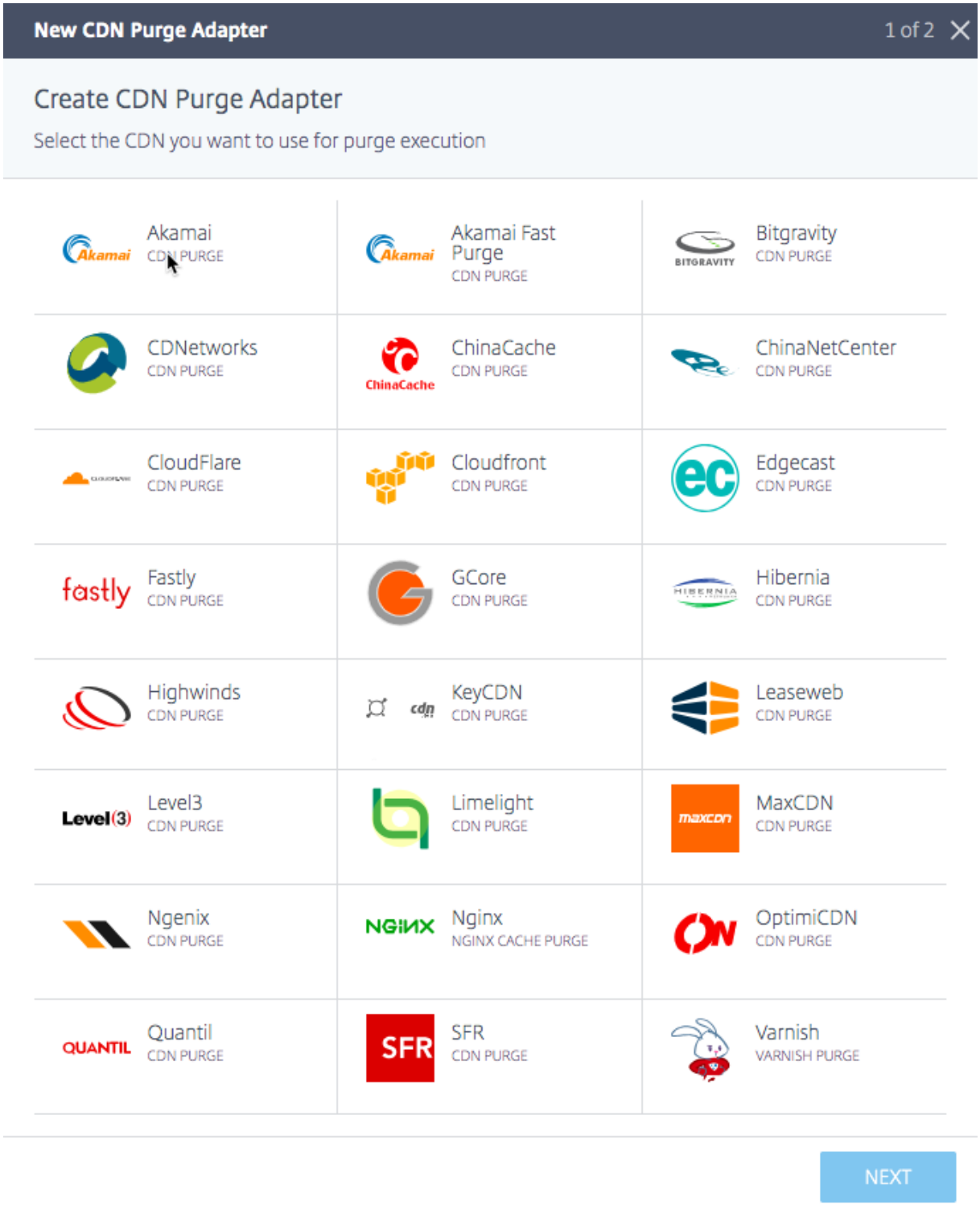


单击开始按钮或 **+** 设置可清除的 CDN。

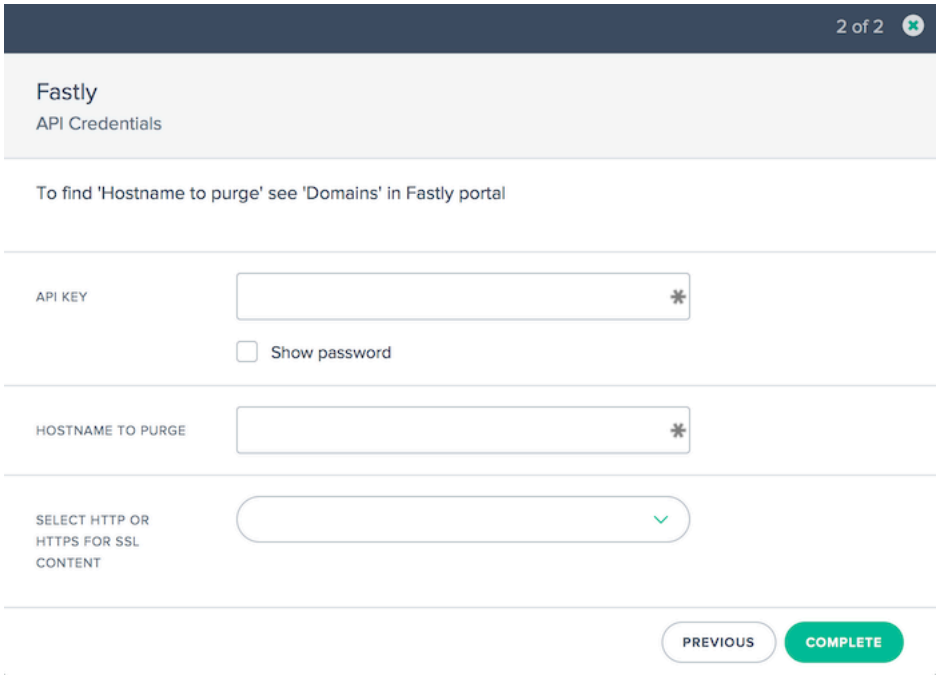


新的 **CDN** 清除适配器

单击要为其创建 CDN 清除适配器的服务图标，然后填写所需的配置字段。



每个清除适配器都需要不同的配置参数。您需要用户名和密码或生成的令牌进行身份验证和任何其他特定于服务的配置。



编辑 **CDN** 清除适配器

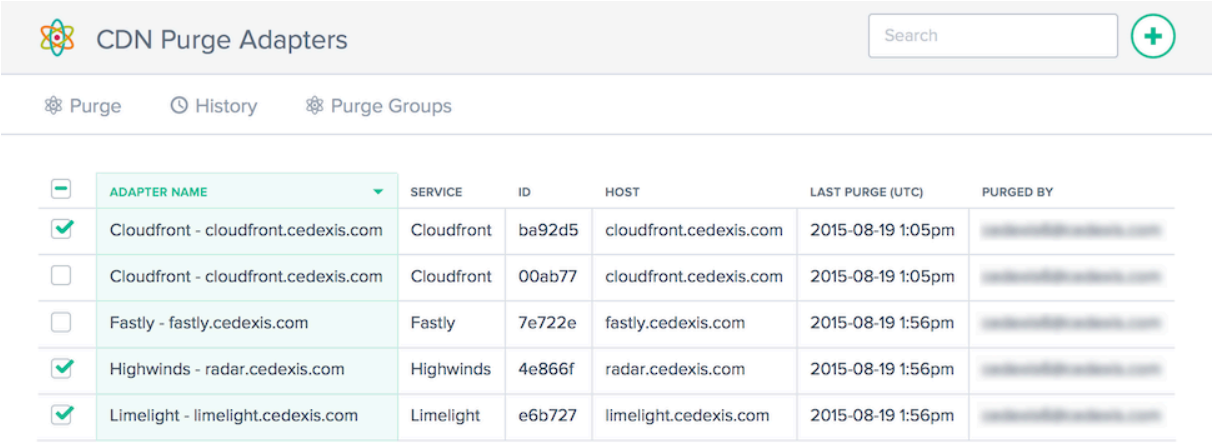
编辑 CDN 清除适配器与单击表中的 CDN 清除适配器并单击 编辑 按钮一样简单。

更改配置后，单击保存。这将使您返回到清除适配器列表，并将您的更改保存并应用于特定 CDN 清除适配器。

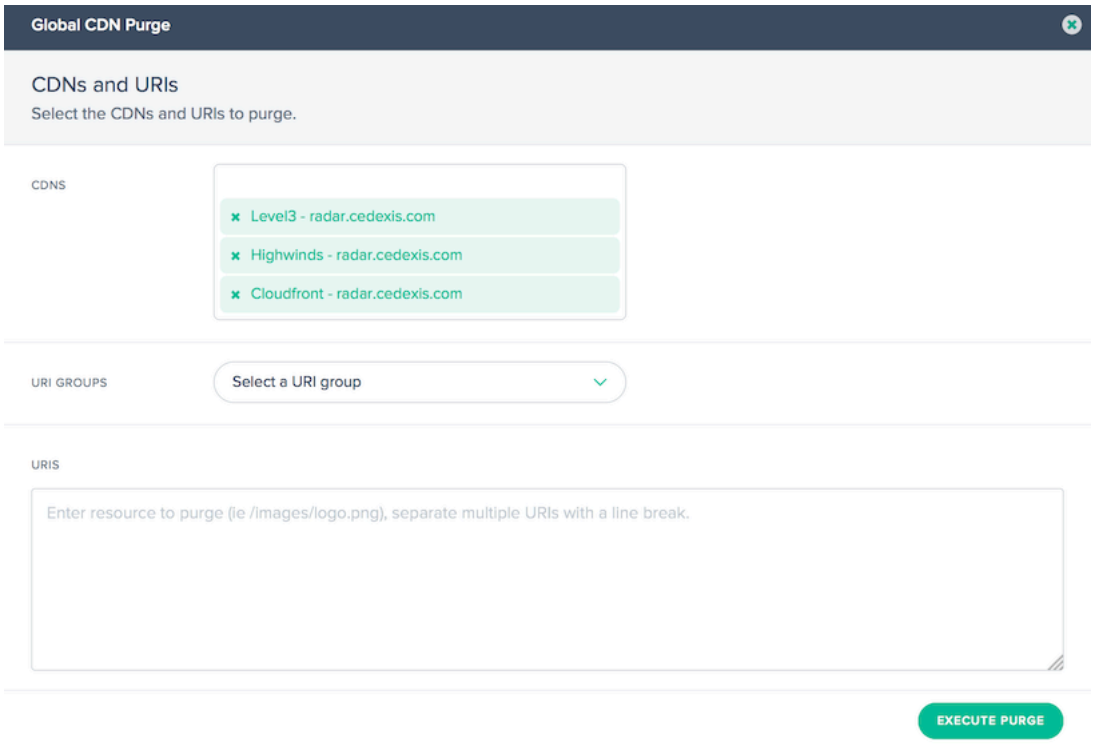
执行清除

要执行清除，请选择清除执行中必须包含的 CDN 清除适配器。

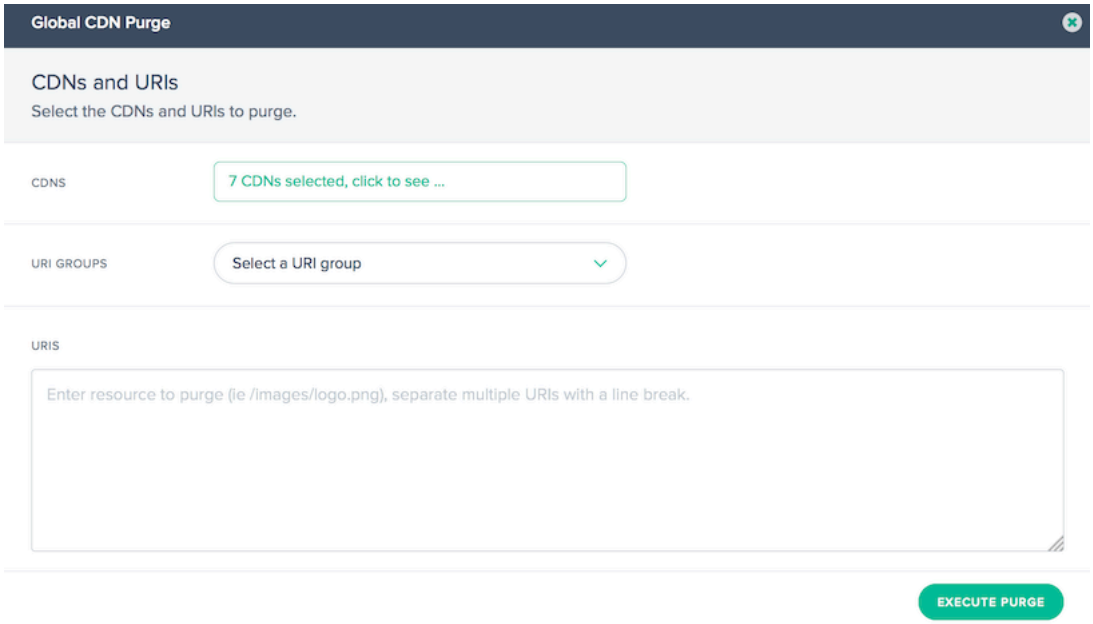
单击清除按钮开始清除过程。



此时将打开 全局 **CDN** 清除 对话框。该对话框显示了所选的 CDN 清除适配器以及在清除执行中使用的 URI。

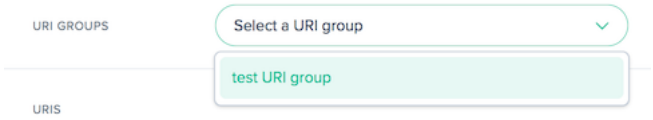


如果选择了 5 个或更少的 CDN 清除适配器，则清除对话框将显示所选 CDN 清除适配器的整个列表。如果未显示所有 CDN 清除适配器，请单击显示已选择 **X CDN**，单击以查看…的 **CDN** 文本框，以显示所有选定的清除适配器。

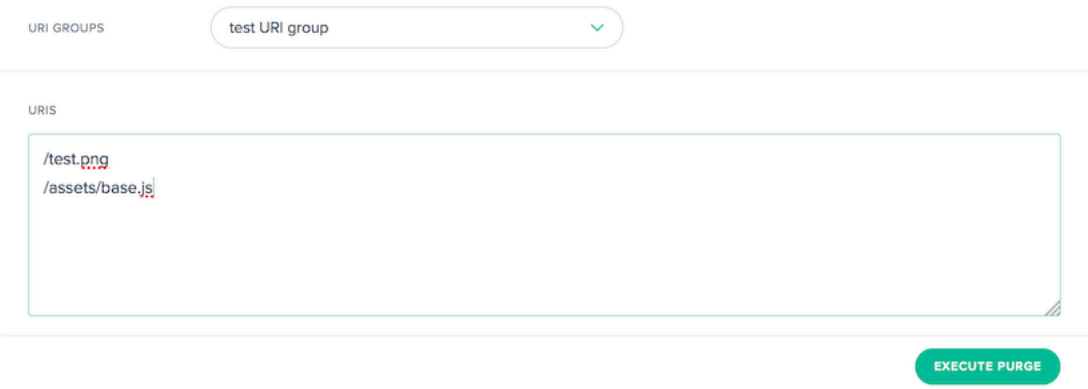


可以通过单击清除适配器列表右侧的“隐藏”按钮 来 隐藏列表。

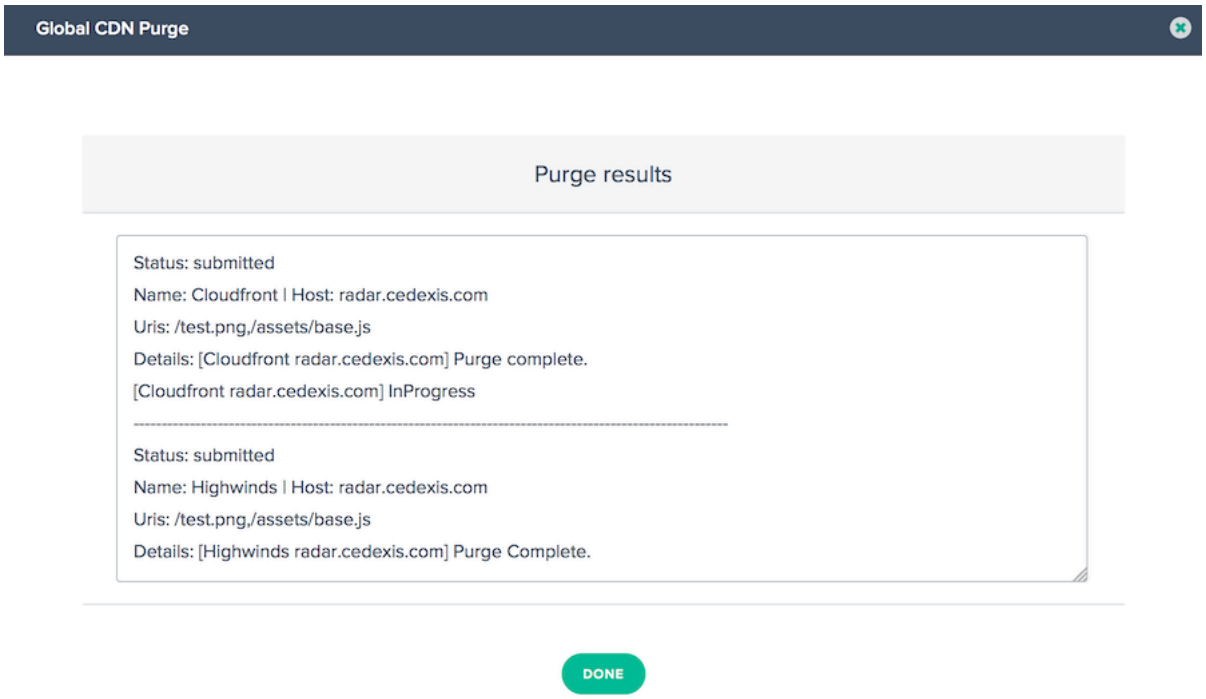
您可以通过手动输入 URI 或从可用 URI 组中进行选择来填充清除中使用的 URI。选择 URI 组会使用所选清除组中的 URI 填充 URI 输入。



输入或修改必须清除的资源的 URI。

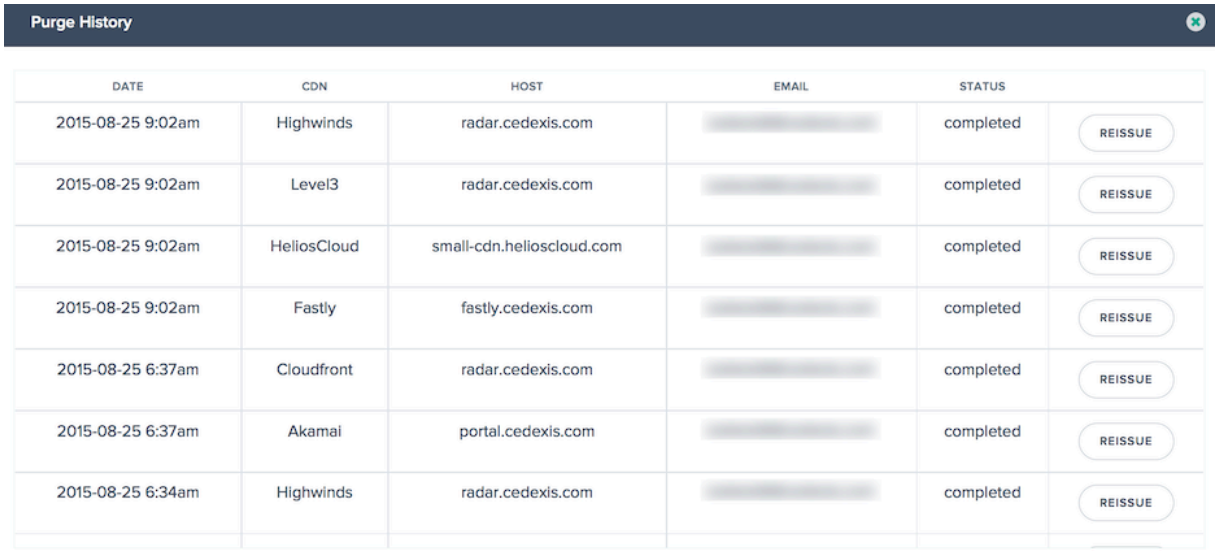


当您准备好提交清除请求时，单击“执行清除”按钮。清除将提交给所有选定的 CDN。提交和 API 响应将显示在“清除结果”对话框中。

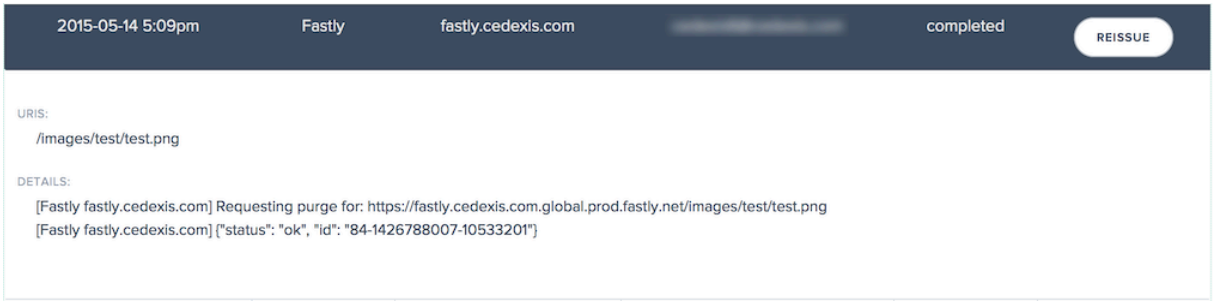


CDN 清除适配器历史记录

Fusion 每次运行时都会收集清除历史记录。您可以查看清除状态、有关清除的信息以及从服务返回的消息。要查看清除历史记录，请单击 **CDN** 清除适配器或清除组屏幕上的历史记录按钮。



该列表包括最近 100 次清除执行的时间和状态。您可以通过单击表中所需的行查看发送到 CDN 服务的清除请求的详细信息。详细信息包括为清除指定的 URI 以及清除期间从服务返回的 API 响应。



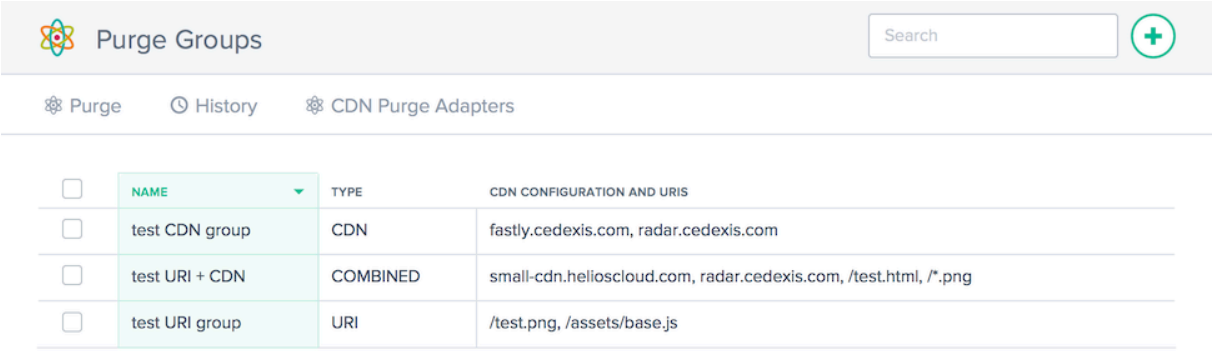
如果要重新运行包含历史记录的特定清除，请单击清除状态信息右侧的重新发布按钮。此时将显示“清除”对话框，其中显示前一次清除中的数据以供运行。

清除组

清除组允许您组织 CDN 清除适配器和 URI，以便轻松清除一组逻辑资源。例如，您可能希望对开发、测试和生产环境进行分组，并同时清除所有环境。或者一次清除多个 CDN 的所有图像资源。

清除组可以由 CDN 清除适配器、清除 URI 或两者组成。通常，只包含 CDN 清除适配器的组用于清除多个服务之间的不同资源。组合组通常用于预先指定标准、可重用的清除，例如“我的所有区域网站和 CDN 中的所有媒体”。

当您至少有一个清除组设置时，您会在打开 CDN 清除时看到此屏幕。



这些列提供以下信息：

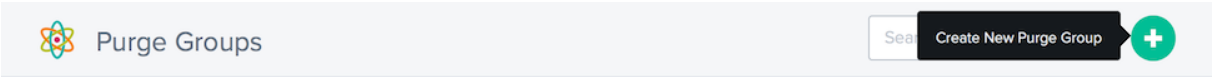
标题	说明
名称	清除组的名称。
类型	组的内容类型。+ CDN —清除组仅包含 CDN 清除适配器，用户在运行清除 + URI 时需要指定 URI-清除组仅包含 URI，用户在运行清除 + 合并时需要指定服务-清除组包含两个 CDN 清除适配器和 URI；用户无需指定更多信息即可运行清除
CDN 配置和 **URI**	CDN 清除组定义中包含的适配器和/或 URI。

创建清除组

要使用清除组，您需要指定必须包含的 CDN 清除适配器或 URI。有两种方法可以创建组：

从 CDN 清除适配器页面，您可以检查所需的清除适配器，然后单击 创建清除组。

在“清除组”页面中，单击 **+** 创建组。

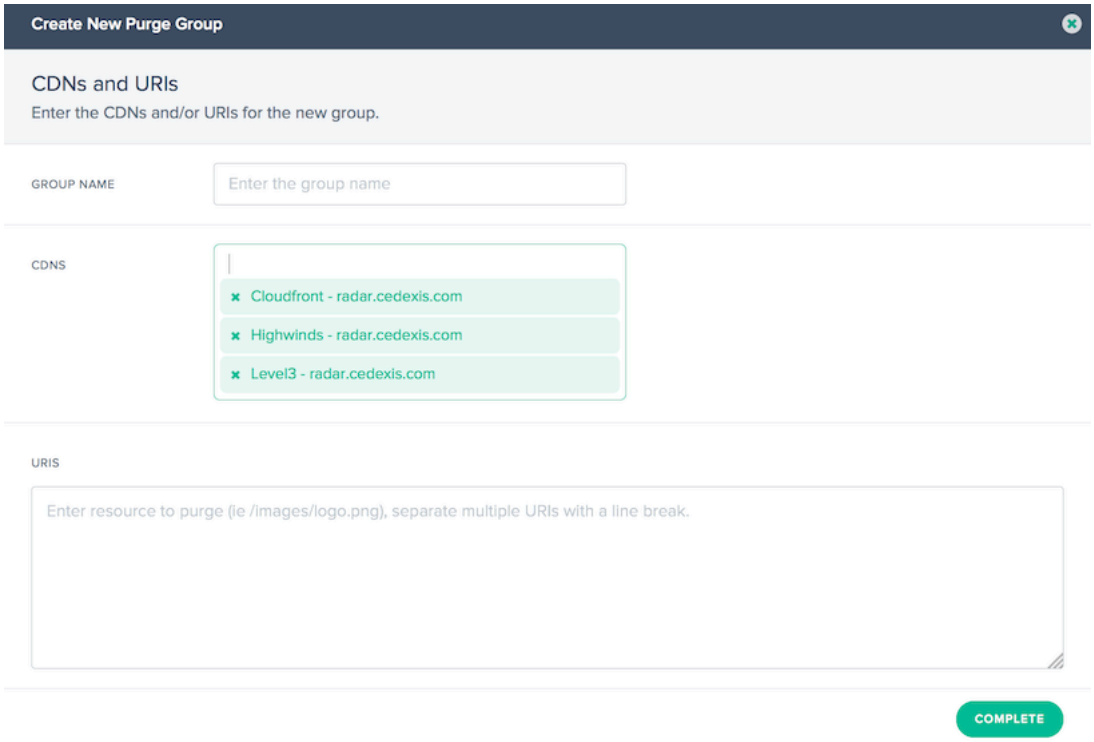


在这两种情况下，都会显示“创建新组”对话框。

输入清除组的名称。

> 注意：您可以从列表中添加或删除 CDN 清除适配器。

单击“完成”以创建组。



运行组清除

在“清除组”页面上，选择一个或多个组，然后单击“清除”按钮。**CDN** 清除 对话框将打开，其中包含清除组定义指定的参数。

单击“执行清除”按钮以开始配置的清除。

警报

September 22, 2023

警报功能可监视来自全球最终用户网络的已配置平台的性能问题或异常情况。

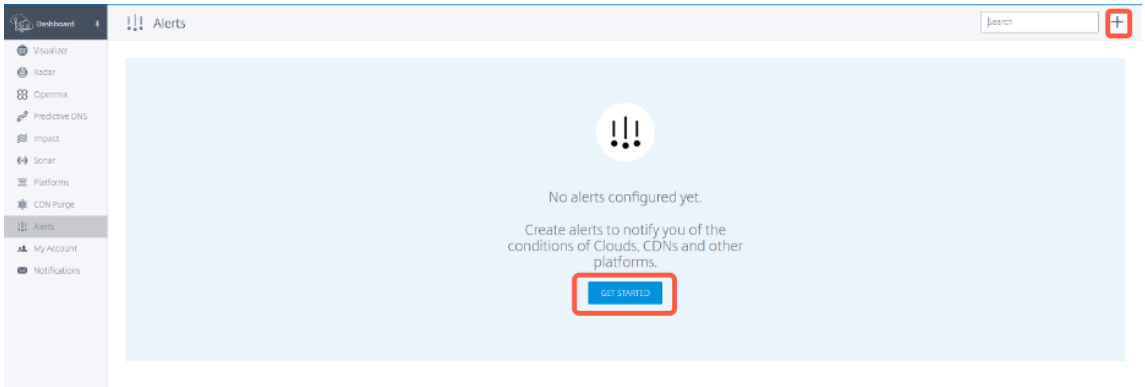
创建警报

要创建监视平台性能的警报，首先必须设置平台。在左侧边栏中，单击平台以转到平台屏幕并设置平台。

要添加新警报，请执行以下操作：

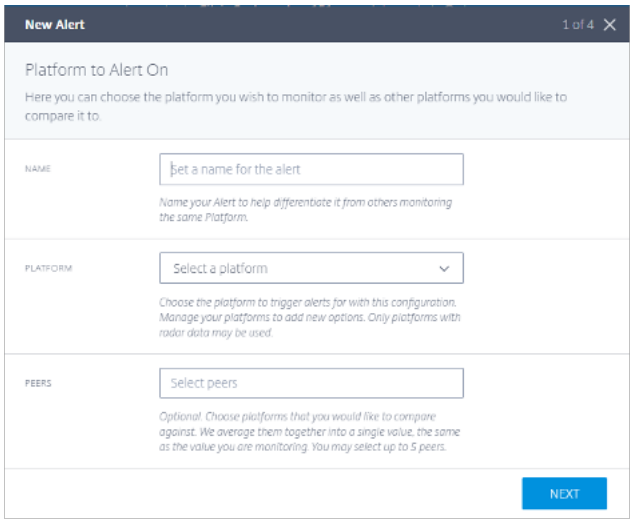
1. 在左侧边栏中，单击警报以转到警报页面并创建警报。

2. 在警报页面上，单击开始使用或右上角的 **+** 符号。

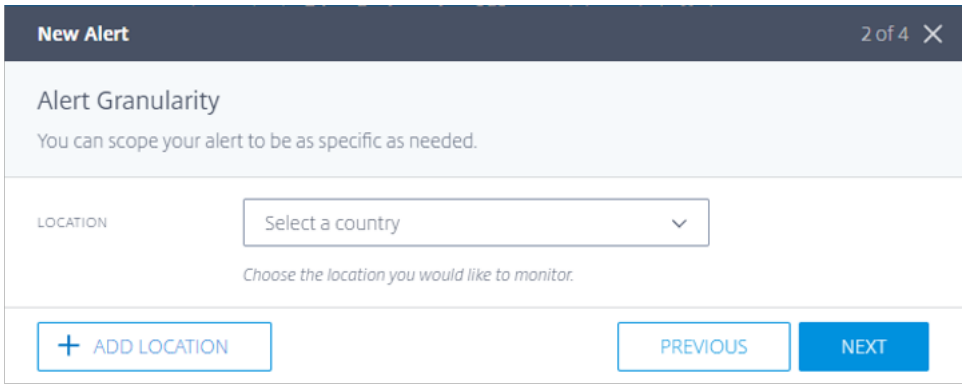


3. 在新建警报窗口中：

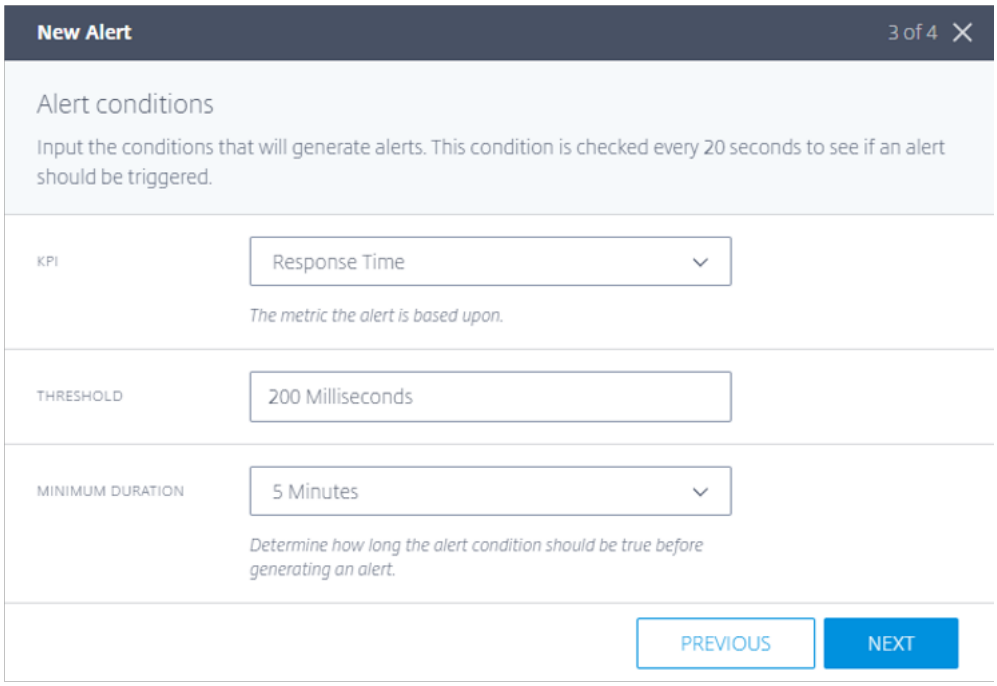
   - 输入警报名称
   - 选择要监视的相对平台
   - 选择要与之比较的对等平台（最多可以选择 5 个对等平台）。此参数为可选设置。
   - 单击 **Next**（下一步）。



4. 选择要监视警报的位置和网络，然后单击下一步。



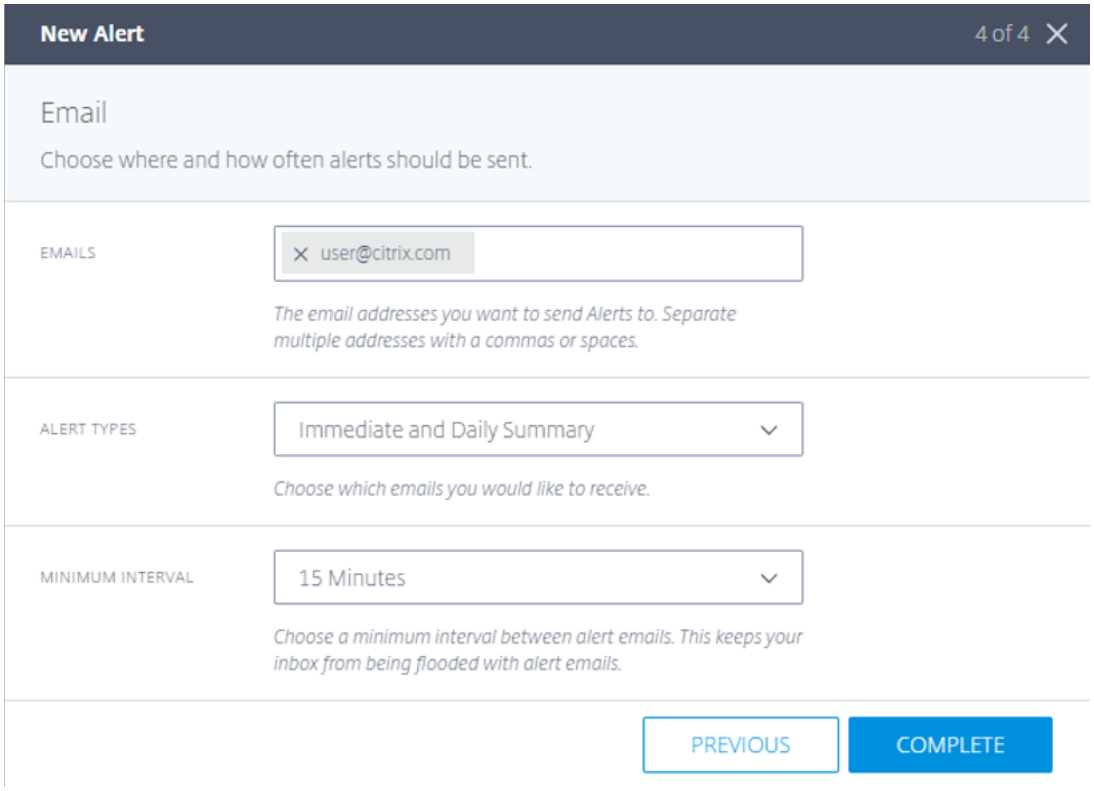
5. 选择相应的 **KPI**、阈值和触发警报的事件的最短持续时间。



NetScaler Intelligent Traffic Management 提供以下 KPI：

- 响应时间：阈值表示触发警报之前接受的最大值（以毫秒为单位）。要触发警报，测量值应至少在用户选择的 **time ≥ minimum_duration** 内高于阈值。在收到低于阈值的测量值至少时间 ≥ 最短持续时间后，同样的警报也会响起。
- 可用性：阈值表示触发预警之前接受的最小值。要触发警报，测量值应至少在用户选择的 **time ≥ minimum_duration** 内低于阈值。在收到超过阈值的测量值至少超过或等于 ≥ 最小持续时间后，同样的警报将熄灭。
- 吞吐量：阈值表示警报触发前接受的最小值（以 kbps 为单位）。要触发警报，测量值应至少在用户选择的 **time ≥ minimum_duration** 内低于阈值。在收到超过阈值的测量值至少超过或等于 ≥ 最小持续时间后，同样的警报将熄灭。

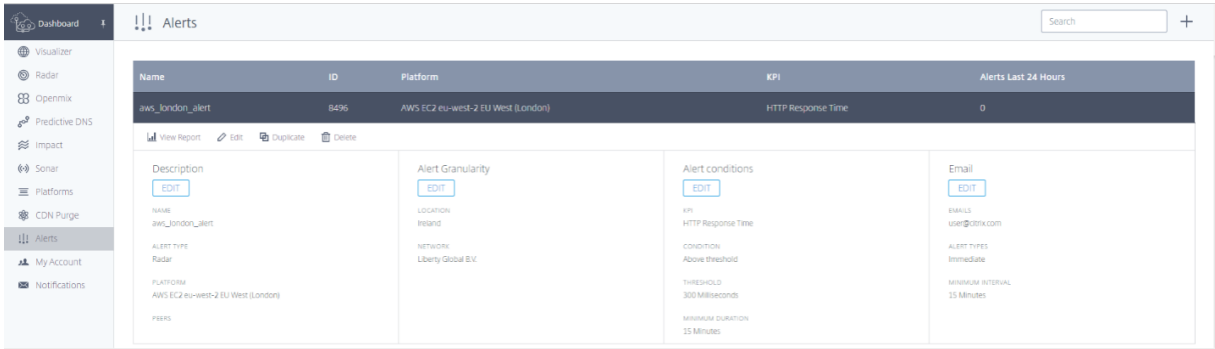
6. 输入要向其发送警报的电子邮件地址，选择警报类型，然后选择警报电子邮件之间的最小间隔。



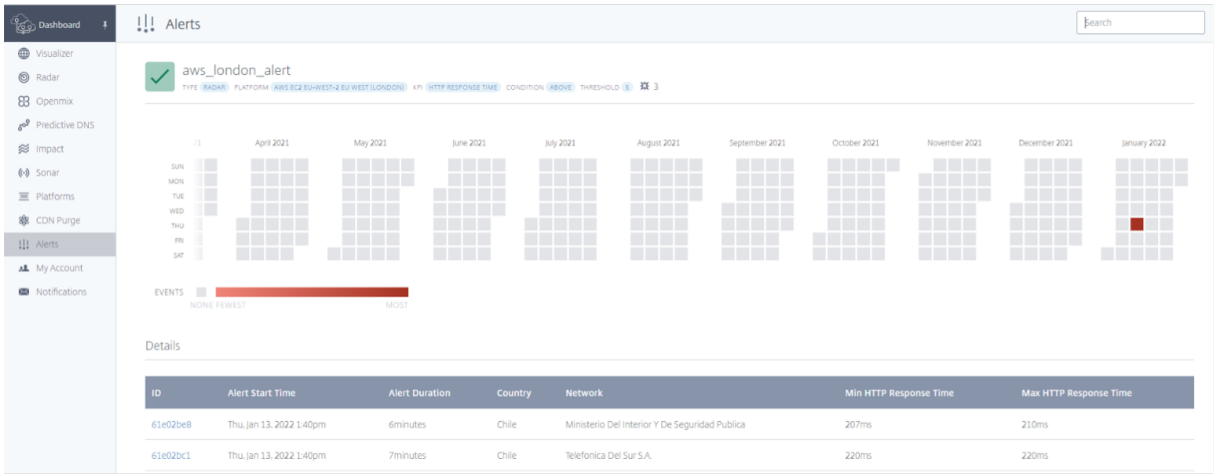
警报类型如下：

- 立即：此选项在触发警报时立即发送电子邮件。
- 每日摘要：此选项在协调世界时 (UTC) 的每个午夜仅发送一封电子邮件，包括所有触发的事件。
- 即时和每日摘要：此选项是即时发送和每日电子邮件发送的组合。

7. 配置警报后，您可以在“警报”选项卡中看到警报，在可视化工具选项卡中看到全局地图。要查看特定警报的报告，请单击警报选项卡中的查看报告。



以下报告页面显示每月每天监视的事件。例如，在下面的屏幕截图中，在 2022 年 1 月的同一天监视了 3 个事件。



您可以单击任何特定事件或事件以查看详细信息，如下图所示：

网络体验监视

September 22, 2023

概述

Citrix Network Experience Monitoring (NEM) 服务（以前称为 **Netscope**）使服务提供商、企业、ISP 和第三方服务提供商能够以汇总的可操作数据形式访问详细的 Radar 测量日志和标准报告。NEM 提供了几个标准的日志和报告，客户可以使用这些日志和报告来衡量他们的服务质量。

该解决方案包括“原始”Radar 测量交付和对 Citrix ITM 数据 API 的访问。NEM 同时提供粒度数据（作为原始测量数据或数据聚合数据）和数据阈值警报。这些服务有助于发现、隔离平台可用性以及平台对等方和底层 ISP 的性能问题。

Radar“原始”测量：Radar 测量提供每天批处理的每个事件的粒度信息。Radar 测量包括标签收集的公共社区和私有测量数据。包括可用性、响应时间、HTTP 和 HTTPS 测量的吞吐量等数据。提供了以下数据字段：

- 提供程序 ID、解析器 IP、模糊处理 (/28) 客户端 IP
- 混淆反向链接标头、用户代理、最终用户 ASN
- 解析器和客户端字段的地理数据

“原始”测量中提供的 Radar 指标包括：

- 可用性、响应时间和吞吐量（测量时）
- DNS 查找时间（可选）、TCP 连接时间（可选）和安全连接时间（可选）
- 延迟（可选）
- 下载时间（可选）

Radar 测量允许客户对收集的数据进行自己的分析。数据集包括有关一系列通信协议的提供程序性能和可用性（错误）的信息。

日志文件数据可从 AWS S3 或 Google 云存储存储桶获取 7 天。客户可以使用标准存储桶访问方法检索社区和私有数据的日志文件。

实时 **Radar**“原始”测量（可选）：原始 Radar 测量实时交付到 AWS S3 存储桶。这些日志通常在收集后的 5 分钟内可用。它们提供的粒度与上述 Radar 原始测量结果一样多。

数据 **API** —Citrix ITM Radar 数据 API 提供了 Radar 公共社区和私有测量数据的聚合。数据会持续更新，大约每 60 秒批处理一次，以供 API 检索。提供数据 API 是为了让客户将 Radar 数据集成到自己的报告和控制板中。

日志共享和交付

- Radar 日志可以实时和每天发送。
- 报告每天都会运行。
- 结果将保存到 AWS S3 (S3) 或 Google Cloud Storage (GCS)。
- 日志和报告都有 7 天的保留期，并且会在创建一周后自动删除。
- 根据报告的类型，报告通常采用 TSV（制表符分隔值）或 JSON 格式。

客户将获得访问 S3 和 GCS 存储桶的登录信息。可以使用 s3cmd、适用于 S3 的 AWS CLI 或适用于 GCS 的 gsutil 之类的命令行工具来登录。S3cmd 配置文件可识别通过门户 UI 接收的访问密钥，并帮助用户连接到 S3 存储桶。

AWS CLI 需要安装在客户的计算机上才能连接到 S3 并访问日志。对于 GCS，客户通过门户界面下载接收访问密钥文件，该用户界面可与 gsutil 工具一起使用。有关详细信息，请参阅常见问题解答。

当报告可用时，客户会收到电子邮件通知。

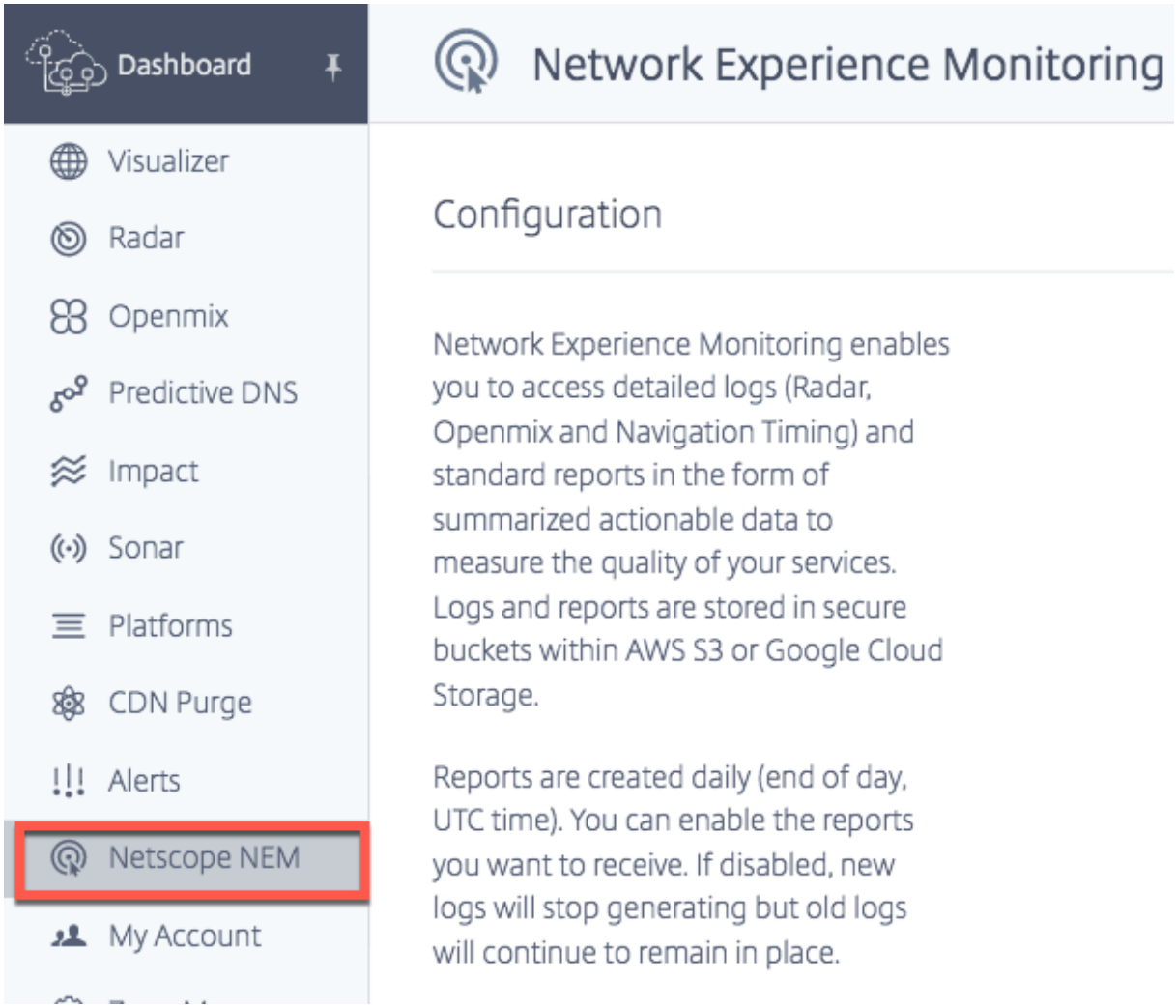
平台设置

您必须配置您的平台以支持和生成 Netscope NEM 所需的数据。在开始之前，请确保您的平台已启用以下设置：

- 对于匿名最佳报告，请启用 **Radar** 探测设置。
  - 对于匿名最佳 RTT，启用 响应时间和可用性。
  - 对于匿名最佳吞吐量，请启用 吞吐量和可用性。
- 对于缓存节点 ID 报告，请启用 **Radar** 探测设置；在高级 **Radar** 设置中，启用节点 **ID**。
- 有关资源计时详细信息，请在 高级 **Radar** 设置 中启用 包含时间戳。

导航

从主菜单中选择 **Netscope NEM**。此时将打开“网络体验监视 配置”页面。



平台和网络

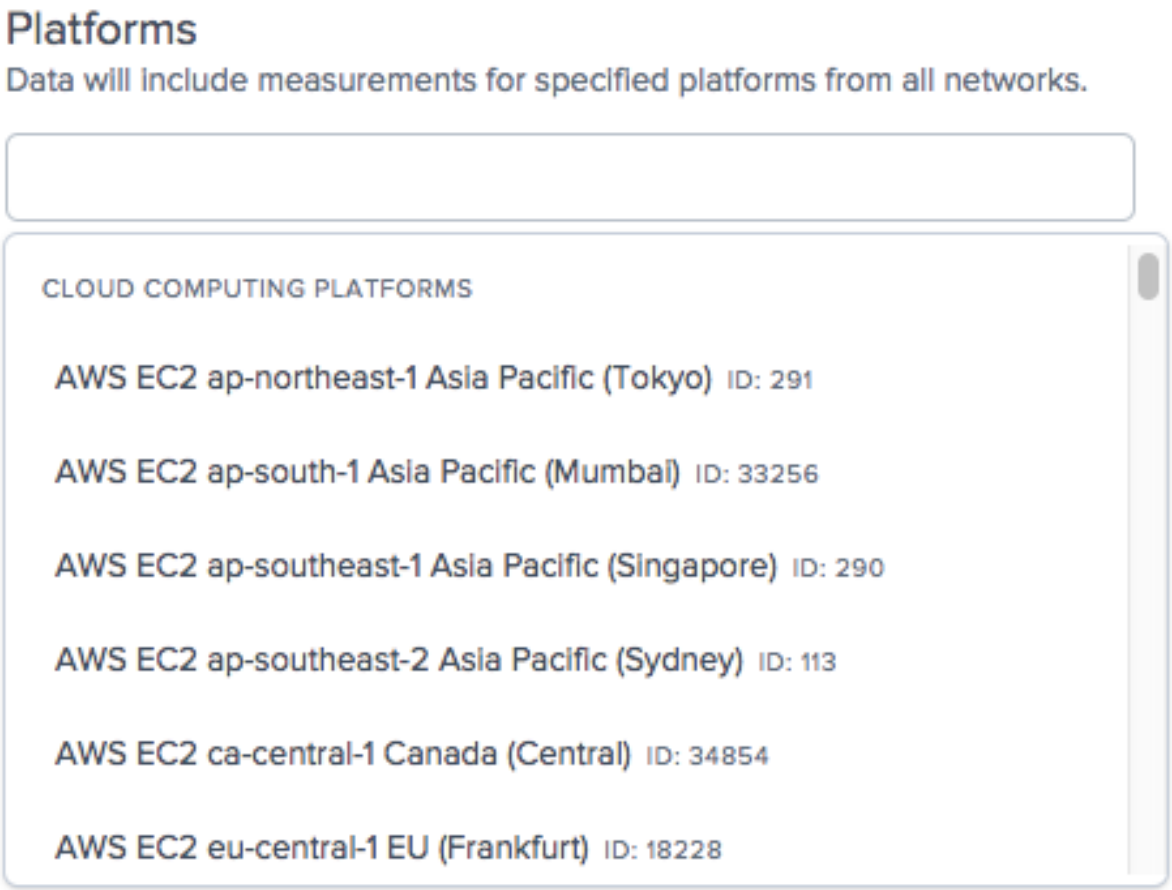
选择所需的 平台 或 网络（或两者）以启动配置过程。

> 注意：
>
> 只有在至少选择了一个平台或网络时，才能配置和生成日志和报告。

客户收到的汇总数据包括选定平台（针对所有关联网络）的 Radar 测量数据，或选定网络（针对所有关联平台测量）的 Radar 测量数据。

选择平台

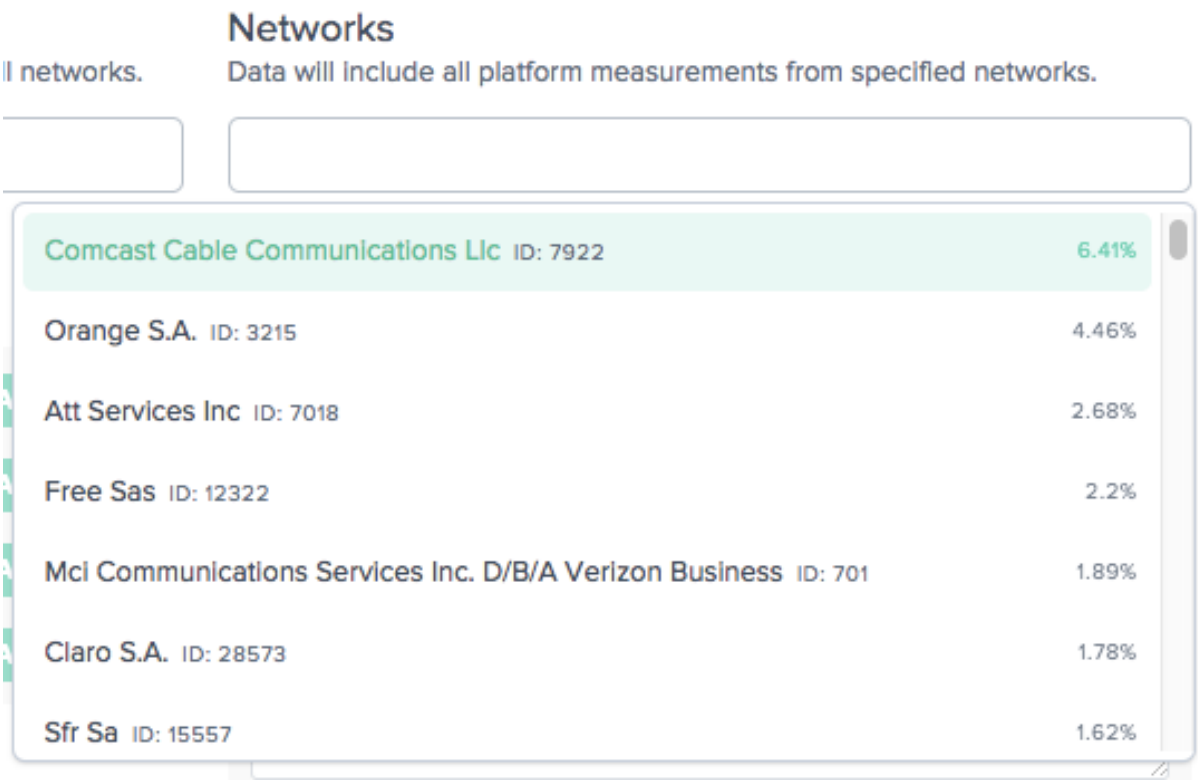
对于内容服务提供商或企业，请选择 CDN、云、数据中心或其他端点等平台。选择需要测量的平台。



选择网络

对于 ISP，从与需要测量的不同平台或终端关联的列表中选择 网 络。

> 注意：
>
> 如果在列表中找不到所需的平台，则可以在门户的平台部分对其进行配置。对于不可用的网络，请联系支持团队。



平台报告

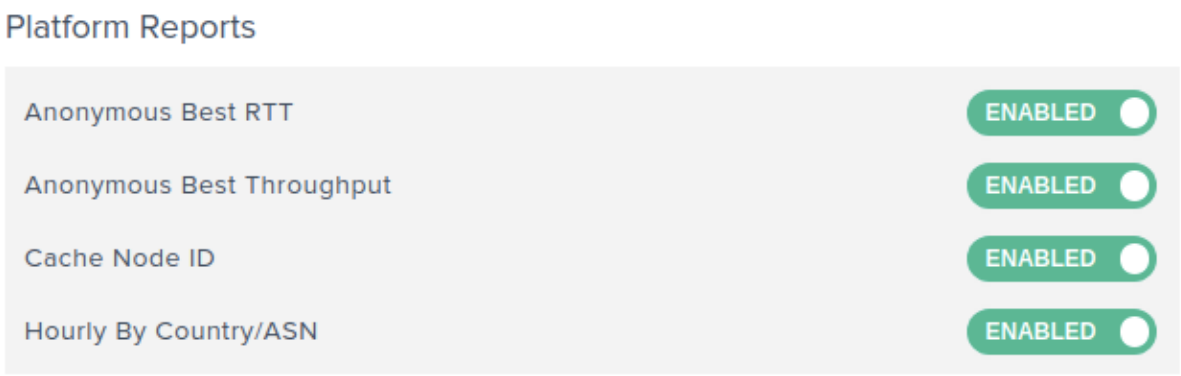
平台报告有四种类型：

1. 匿名往返时间 **(RTT)** 最佳
2. 匿名吞吐量最佳
3. 缓存节点 **ID**
4. 按国家/地区**/ASN**

有关日志说明，请参阅面向服务提供商和企业的 Radar 日志说明和报告。

启用平台报告

单击切换按钮以启用或禁用要接收的报告。如果禁用现有报告，则不会生成新日志，但旧报告会保留在当前位置。



匿名平台最佳报告

- 这些报告可帮助提供商将其绩效与其对等组内其他平台的绩效进行比较，例如在同一国家、地区或 ASN 中。
- 对等组中排名前 15 位的提供商的绩效数据是根据相同的类别汇总的。最佳值列在特定提供商的最佳价值旁边。
- SSL 平台的匿名最佳报告是可用的，因此它们的性能可以与其他 SSL 平台进行比较。
- 客户端 IP 被截断为 /28。
- “最佳”提供商的结果有助于云/CDN 将性能工作重点放在竞争力较弱的大容量或业务关键型 ASN 上。
- 该报告提供了按照 DNS 解析器 IP、客户端 IP /28 和为对象提供服务的缓存节点细分的性能的详细信息。将相同标准与“最佳”平台进行比较。

可用于 RTT 和吞吐量。

- 有关日志说明，请参阅面向服务提供商和企业的 Radar 日志说明和报告。

平台的缓存节点 **ID** 报告

- 此报告用于标识响应请求的特定服务器或数据中心，并帮助诊断服务器问题。
- 它提供响应特定请求的数据中心或计算机的 ID。
- 它有助于理解为什么通过特定节点（POP 或计算机，或节点 ID）的性能好还是坏。
- 性能包括响应时间、吞吐量、可用性（探测类型）、DNS 解析器 IP、客户端 IP /28 以及为对象提供服务的缓存节点。
- 有关日志说明，请参阅 面向服务提供商和企业的 Radar 日志说明和报告

按国家/地区/**ASN**

- 此报告有助于验证您的提供商在一天中的绩效是否有显著差异。
- 它显示测量结果被截断到小时的时间，例如 `2018-03-11T23:00:00`。
- 有关日志说明，请参阅面向服务提供商和企业的 Radar 日志说明和报告。

网络报告

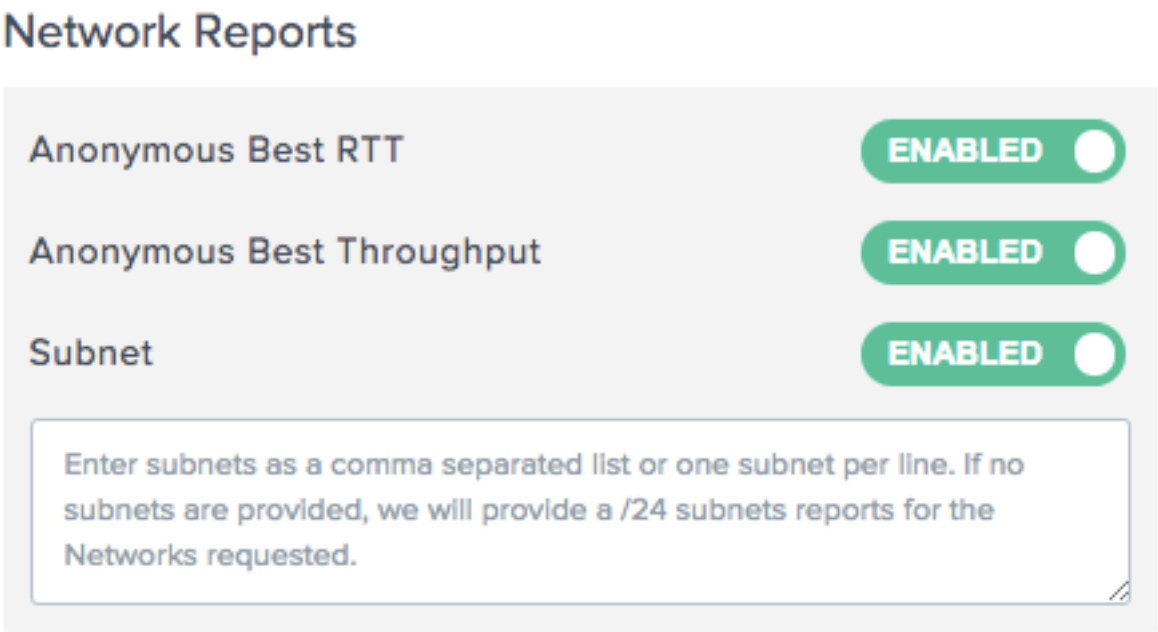
网络报告有三种类型：

1. 匿名往返时间 **(RTT)** 最佳
2. 匿名吞吐量最佳
3. 子网

有关日志说明，请参阅面向 ISP 的 Radar 日志说明和报告。

启用网络报告

单击切换按钮以启用或禁用要接收的报告。禁用后，新日志将停止生成，但旧报告就位。
要生成子网报告，请输入网络的特定子网。如果未输入任何子网，则会使用 ASN CIDR 块作为默认子网生成报告。



互联网服务提供商的匿名最佳报告

- 在 ISP 的“匿名最佳”报告中，使用同行组进行“最佳”比较。对等组基于 ISP 的位置。它通常是指定国家/地区内 10 家测量最多的互联网服务提供商，会话至少超过 1000 次。
- “最佳”ISP 的结果有助于 ISP 将性能工作重点放在高容量或业务关键型平台以及竞争力较弱的领域。
- 报告提供了按地域和平台分列的绩效细节，并将其与“最佳”ISP 进行比较，以同样的标准。
- 可用于 RTT 和吞吐量。
- 有关日志说明，请参阅面向 ISP 的 Radar 日志说明和报告。

ISP 的子网报告

- 该报告向互联网服务提供商提供了有关其网络的特定子网如何通过我们测量的平台为用户提供性能的信息。
- 它提供了有关响应特定请求的服务提供商的信息。
- 它有助于了解网络子网的性能。
- 性能包括响应时间、吞吐量、可用性（探测类型）、DNS 解析器 IP、客户端 IP /28 和用户的子网。
- 有关日志说明，请参阅面向 ISP 的 Radar 日志说明和报告。

Radar 日志

- Radar 日志可用于平台和网络。
- 它们包括原始日志中可用字段的子集，其中包括一些匿名数据：客户端 IP /28、哈希 Referer MD5。
- 无论生成测量的页面如何，都会提供公共平台的每个测量值。

> 注意：
>
> NEM 永远不会公开完整的客户端 IP。相反，它公开了 /28。例如，IP 255.255.255.255 在报告中显示为 255.255.255.240/28。

日志频率

Radar 日志可以每天（每 24 小时）生成，即一天结束时间，UTC 时间。也可以实时（每分钟）生成日志。

文件格式

选择 **TSV** 或 **JSON** 以这两种格式接收日志和报告。

测量类型

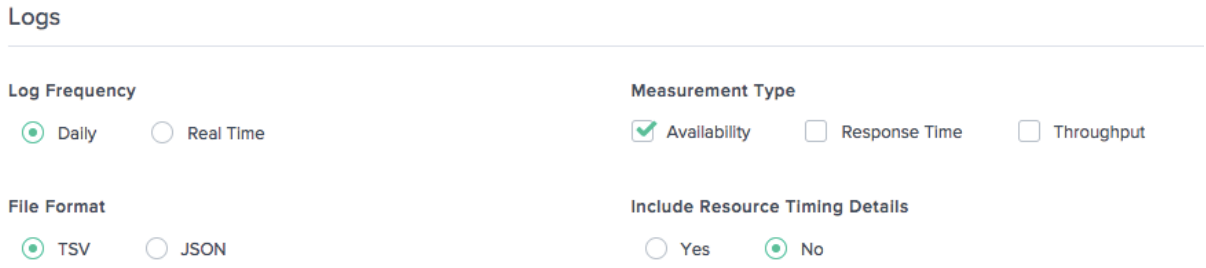
您可以为以下测量类型配置日志：可用性、响应时间和吞吐量。在报告中，1：可用性，0：HTTP 响应时间，14：HTTP 吞吐量。

资源计时详情

您可以通过单击“是”或“否”按钮选择也包括资源计时详细信息。资源计时详细信息包括：

- DNS 查找时间
- TCP 连接时间
- 安全连接时间
- 下载时间

有关日志说明，请参阅面向服务提供商和企业的 Radar 日志说明和报告。



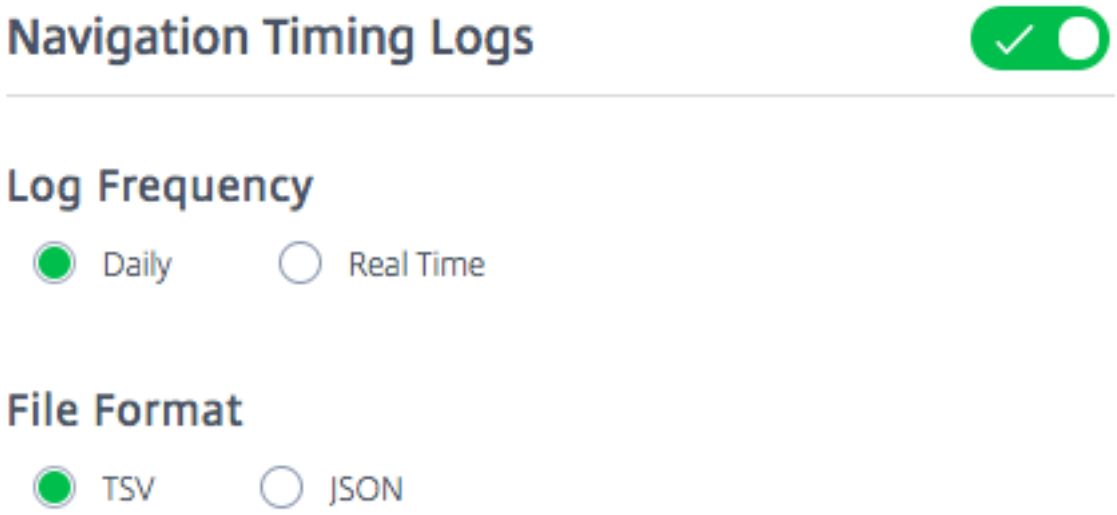
导航计时日志

日志频率

导航计时日志可以每天（每 24 小时）生成，也就是说，一天结束时，UTC 时间。也可以实时（每分钟）生成日志。

文件格式

选择 **TSV** 或 **JSON** 以接收以上任一格式的导航计时日志。有关日志说明，请参阅导航计时日志说明。



Openmix 日志

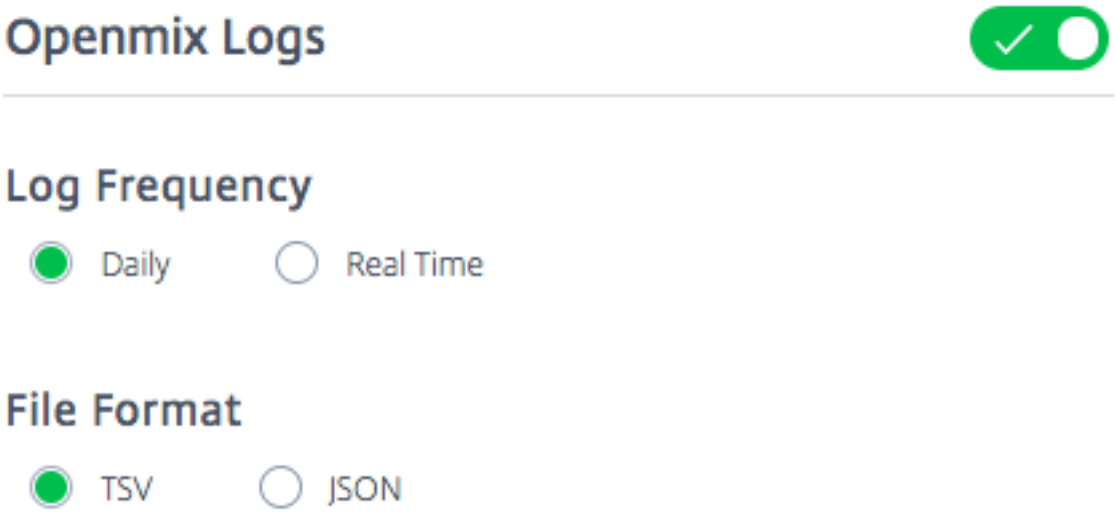
日志频率

Openmix 日志是实时生成的（即每分钟）。这些日志为 Openmix 客户提供了实时测量结果。

文件格式

选择 **TSV** 或 **JSON** 以这两种格式接收任一格式的 Openmix 和 HTTP Openmix 日志。但是，JSON 是推荐的格式。

有关日志说明，请参阅 Openmix 日志说明。



云服务交付

此选项允许您选择交货方式。您可以选择在 AWS S3 存储桶或 Google 云存储 (GCS) 存储桶中接收日志和报告。
您可以使用提供的登录信息访问 S3 和 GCS 存储桶，并使用 s3cmd 或适用于 S3 的 AWS CLI 和适用于 GCS 的 gsutil 命令行。

AWS S3

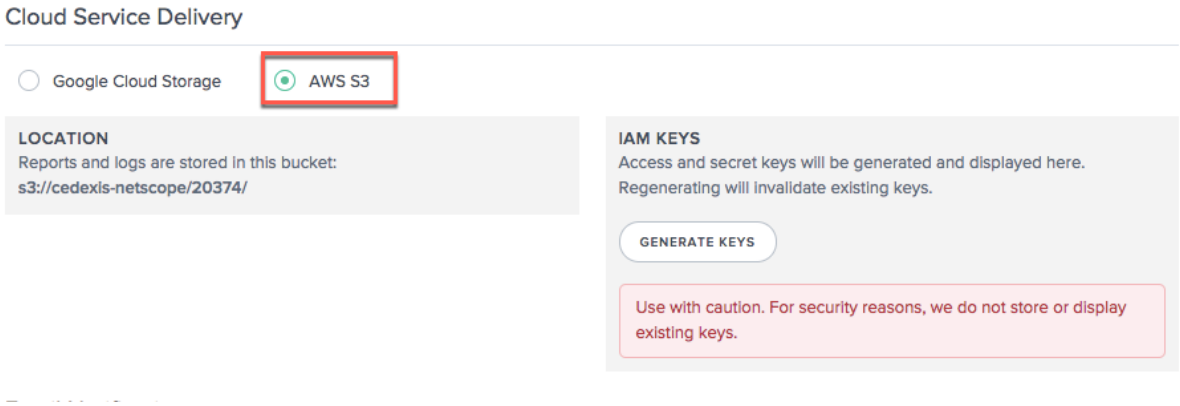
对于要传输到 AWS S3 存储桶的日志和报告，请选择 **AWS S3**。

位置　位置表示 AWS S3 中保存日志和报告的存储桶。

IAM 密钥　如果您选择 AWS S3 下的生成密钥按钮，则会生成 AWS IAM 密钥（访问密钥和私有密钥）并显示在 IAM 密钥下。请务必记录密钥，因为它们不会存储在任何地方供以后查看。

> 注意：
>
> 访问密钥和私有密钥对是私钥的唯一副本。客户必须安全地存放它们。重新生成新密钥会使现有密钥失效。S3cmd 配置文件可识别访问密钥（通过门户界面接收），并帮助客户连接到 S3 存储桶。需要在客户的计算机上安装 AWS CLI 才能连接到 S3。

有关如何使用带有 s3cmd 的访问密钥和私有密钥从 S3 存储桶下载报告的信息，请参阅常见问题解答。



Google Cloud 存储

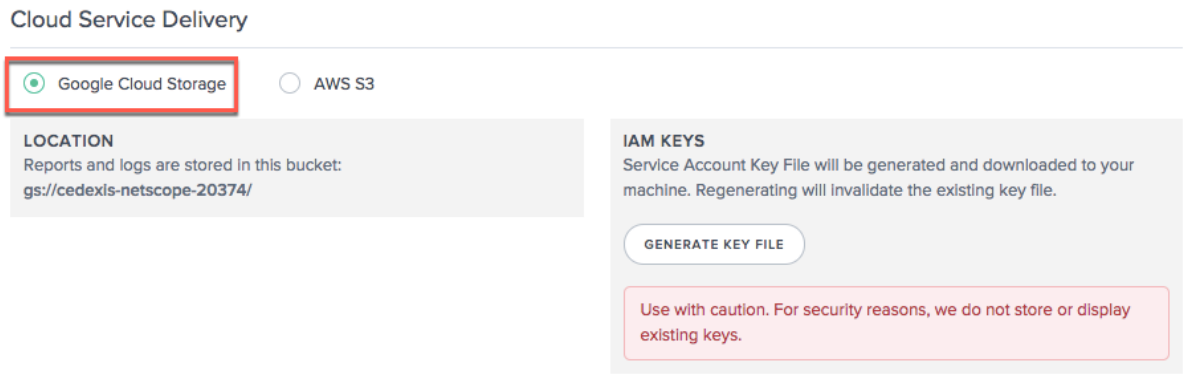
对于要发送到 GCS 的日志和报告，请选择 **Google Cloud** 存储。

位置　位置表示 Google Cloud 存储中用于保存日志和报告的存储分区。

IAM 密钥　当您选择“生成密钥文件”按钮时，Google 服务帐户密钥文件将下载到您的计算机上。

> 注意：
>
> 此密钥文件是私钥的唯一副本。记下您的服务帐户的电子邮件地址，并安全地存储服务帐户的私钥文件。重新生成新的密钥文件会使现有文件失效。

此密钥文件可与 gsutil 工具一起使用，从 GCS 存储桶下载日志和报告。有关如何使用密钥文件下载日志文件的详细信息，请参阅常见问题解答。



面向服务提供商和企业的 **Radar** 日志描述和报告

提供商的 **Radar** 日志

- 这些日志为基准测试合作伙伴提供 Radar 测量结果。
- 它们提供针对公共平台进行的所有测量，无论生成测量的页面如何。
- Radar 日志包括原始日志中可用字段的子集，其中包括一些匿名数据：客户端 IP /28、哈希 Referer MD5。
- 下面是 TSV 文件格式的平台 Radar 日志共享示例。

> 注意：
>
> - NEM 永远不会公开完整的客户端 IP。相反，它公开了 /28。例如，IP 255.255.255.255 在报告中显示为 255.255.255.240/28。
> - 客户的 GEO 信息是根据客户端的 IPv4 提取的，该信息更为详细。

日志说明　下面是 Radar 日志的列标题和说明。这些字段在输出文件中按以下顺序显示：

日志	说明
时间戳	这是请求的 UTC 时间，采用 YYYY-MM-DDTHH:MI:SSZ 格式。日志表中的实际值（向下到秒）分别四舍五入到小时/日表中最接近的小时 (2018-03-30T23:00:00Z) 或日 (2018-03-30T00:00:00Z)。在所有数据集中，时间戳始终采用 UTC 格式。
唯一节点 **ID**	也称为缓存节点 ID。它是一个任意的值。通常是 CDN 边缘服务器返回的 IP，以帮助 CDN 内部识别哪个服务器处理了特定请求。”（空字符串）：来自不支持 UNI 检测的 Radar 客户端。0：用户代理不支持 UNI 检测所需的功能。1：客户端在 UNI 检测期间遇到错误，例如 HTTP 404 或其他不成功的响应。2：尝试了 UNI 检测，但导致错误。

日志	说明
提供商 **ID**	正在测量的平台的内部 ID。
探测类型	所测量的探测类型（例如：1：HTTP 连接时间；0：HTTP 响应时间；14：HTTP 吞吐量等）。要表明该服务可用，请使用在允许的时间内成功返回的信息。
响应代码	测量结果。例如：0：成功，1：超时，4：错误。对于可用性计算，响应为 0（成功）的测量值与测量总数（总数，不管响应如何）的百分比。对于其他探测类型（RTT 和吞吐量），在计算 RTT 的统计数据时，过滤器只能考虑成功码为 0 的 RTT 数据点。吞吐量相同。
测量值	记录的测量值，其含义因探头类型而异。它以毫秒为单位表示可用性 (1) /响应时间 (0) 测量值，以 kbps 为单位表示吞吐量 (14)。
解析器市场	处理请求的 DNS 解析器的市场。通常是 DNS 解析器所在的大陆，其中 0：未知 (XX)，1：北美 (NA) 5：非洲 (AF)，3：欧洲 (EU)，4：亚洲 (AS)，2：大洋洲 (OC)，6：南美洲 (SA)。
解析器国家/地区	处理 request.IDs 的 DNS 解析器所在的国家/地区可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/countries.json.gz
解析器区域	处理 request.IDs 的 DNS 解析器所在的区域可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/regions.json.gz 注意：并非世界上所有国家/地区都定义了区域。
解析器状态	处理 request.IDs 的 DNS 解析器的状态可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/states.json.gz 注意：并非世界上所有国家/地区都定义了状态。
解析器城市	处理 request.Resolver 城市的 DNS 解析器所在的城市是通过查找解析器 IP 地址来添加的。ID 可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/cities.json.gz
解析器 **ASN**	处理请求的 DNS 解析器的自治系统编号 (ASN)。通常情况下，具有 DNS 解析器 ID 的 ASN 可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/asns.json.gz
解析器 **IP**	我们的基础结构从中接收 DNS 请求的 DNS 解析器的 IP 地址。

日志	说明
客户市场	生成此度量的最终用户市场。通常是客户端 IP 所在的大陆；其中，0：未知 (XX)，1：北美 (NA) 5：非洲 (AF)，3：欧洲 (EU)，4：亚洲 (AS)，2：大洋洲 (OC)，6：南美洲 (SA)。
客户国家/地区	生成此 measurement.IDs 的最终用户所在的国家/地区可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/countries.json.gz
客户区域	生成此测量的最终用户区域。通常情况下，客户端 IP 所在的地理区域的 ID 可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/regions.json.gz 注意：并非世界上所有国家/地区都定义了区域。
客户状态	生成此测量的最终用户的状态。通常情况下，客户端 IP 所在的州的 ID 可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/states.json.gz 注意：并非世界上所有国家/地区都定义了状态。
客户城市	生成此测量的最终用户所在的城市。通常情况下，客户端 IP 所在的城市的 ID 可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/cities.json.gz
客户端 **ASN**	生成此测量值的最终用户的自治系统编号 (ASN)。通常情况下，包含 client IP 的 ASN 的 ID 可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/asns.json.gz
客户端 **IP**	生成此测量的最终用户的 IP。
Referer 主机 **MD5**	Referer 信息（协议、主机和路径）来自 Radar HTTP 请求的 Referer 标头。Referer 主机 MD5 经过哈希处理。
用户代理	这是托管标签的浏览器页面中的用户代理字符串。例如，如果您使用 Chrome 浏览带有 Radar 标签的网页，则后台的 测 Radar 量值会记录您的 Chrome 浏览器中的用户代理。这些衡量标准包括 Chrome 浏览器、Chrome 版本、有关运行 Chrome 的操作系统的信息等。
DNS 查找时间（可选）	使用资源计时 API，计算域名查找结束和域名查找开始之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 domainLookupEnd - domainLookupStart。

日志	说明
TCP 连接时间（可选）	使用资源计时 API，计算连接端和连接启动之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 connectEnd - connectStart。
安全连接时间（可选）	使用资源计时 API，计算连接端和安全连接启动之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 connectEnd - secureConnectionStart。
延迟（可选）	使用资源计时 API，可以计算响应开始和请求启动之间的差异。它计算两个值均不为 null 且响应开始时间大于请求开始时间的情况。它的计算方式为 responseStart - requestStart
下载时间（可选）	使用资源计时 API，计算响应结束和响应开始之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 responseEnd - responseStart。
客户配置文件	此字段有助于识别数据是来自移动应用程序还是浏览器。它还允许我们区分 iOS、Android 应用程序和浏览器。数字用于标识每个客户配置文件。此字段的值为：null、0、1、2、3、4。其中，null：通常表示不支持发送 client_profile 值的较旧的 Radar 客户端。0：浏览器；1：iOS-用 Swift 编写的 iOS 版 Radar runner 应用程序；2：Android；3：移动版网站上的浏览器；4：iOS-用 Objective-C 编写的 iOS 版 Radar Runner 应用程序。
客户配置文件版本	客户端配置文件版本告诉我们在移动应用程序中使用了哪个版本的 Radar Runner 代码（适用于 iOS）或 AndroidRadar SDK（适用于 Android）。此字段仅供内部使用。
设备类别	所有设备都分为以下其中一种：智能手机、平板电脑、PC、智能电视及其他。如果解析器无法确定任何字段的值，则使用“其他”作为默认值。
设备	用户使用的设备类型，例如 Apple iPhone。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。
浏览器	用户正在使用的浏览器类型，例如移动浏览器 UI/WKWebView 0.0.0。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。
操作系统	使用的操作系统。例如，iOS 11.0.3。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。

日志	说明
举报客户端 **IP**	此 IP 是进行测量的用户的屏蔽 /48 公有 IP。它可以是 IPv4 或 IPv6 (如果支持)。

最佳匿名报告

- 匿名最佳报告可帮助提供商将其表现与其他平台的同行群体（即在同一国家、地区或 ASN 内）进行比较。
- 对等组中排名前 15 位的提供商的绩效数据是根据相同的类别汇总的。最佳值列在特定提供商的最佳价值旁边。
- SSL 平台的匿名最佳报告是可用的，因此它们的性能可以与其他 SSL 平台进行比较。
- 客户端 IP 被截断为 /28。
- “最佳”提供商的结果有助于云/CDN 将性能工作重点放在竞争力较弱的大容量或业务关键型 ASN 上。
- 该报告提供了有关性能的详细信息，包括 DNS 解析器 IP、客户端 IP /28 和为对象提供服务的缓存节点。在相同标准下，它与“最佳”平台进行了比较。
- 可用于 RTT 或吞吐量。
- 下面是 TSV 文件格式的 RTT 的平台匿名最佳报告示例。

日志说明　下面是“匿名最佳报告”的列标题和说明。这些字段在输出文件中按以下顺序显示。

日志	说明
解析器国家/地区	处理请求的 DNS 解析器所在的国家/地区。
解析器区域	处理请求的 DNS 解析器所在的区域。
解析器状态	处理请求的 DNS 解析器的状态。
解析器 **ASN ID**	处理请求的 DNS 解析器的自治系统编号。通常是具有 DNS 解析器的 ASN。
解析器 **ASN** 名称	ASN 的名称。
解析器 **IP**	我们的基础结构从中接收 DNS 请求的 DNS 解析器的 IP 地址。
客户国家/地区	生成此度量的最终用户所在的国家/地区。
客户区域	生成此测量的最终用户区域。
客户状态	生成此测量的最终用户的状态。
客户端 **ASN ID**	生成此测量值的最终用户的自治系统编号 (ASN) 编号。通常是具有客户端 IP 的 ASN。
客户端 **ASN** 名称	生成测量的最终用户的 ASN 的名称。
客户端 **IP**	生成测量的最终用户的 IP。

日志	说明
成功	成功测量的总数。提示：成功/总计 == 可用性。
超时	超时的测量次数。
错误	误差的测量次数。
总数	测量的总数。
平均值	该行所有测量值的平均值。
最佳平均值	同行组中排名前 15 位的提供商中的最佳平均值。
最佳平均值测量	产生最佳均值计数的测量总数。
中位数	当测量值按顺序列出时，第 50 个百分位数值是特定提供者的测量值的中间值。
最佳中位数	对等组中前 15 个提供商的最佳第 50 个百分位数值（低于该值的 50%的测量值）。
最佳中位数测量值	生成 best_median 的测量总数
5th	提供程序的第 5 个百分位数值。
第 **5** 次最佳	同行组中前 15 个提供商中的最佳第 5 个百分位数值。
第 **5** 次最佳测量	产生 best_5th 的测量总数
10th	提供程序的第 10 个百分位数值。
最佳第 **10** 个	同行组中前 15 个提供商中的最佳第 10 个百分位数值。
第 **10** 次最佳测量	产生 best_10 的测量总数
90th	提供程序的第 90 个百分位数值。
最佳第 **90** 个	在同行组中排名前 15 位的提供商中，最好的第 90 个百分位数值。
第 **90** 次最佳测量	产生 best_90 的测量总数
95th	提供程序的第 95 个百分位数值。
最佳第 **95** 个	在同行组中排名前 15 位的提供商中，最好的第 95 个百分位数值。
第 **95** 次最佳测量	产生 best_95 的测量总数
Stdev	提供者的标准差
最佳 **Stdev**	同行组中排名前 15 位的提供商中的最佳标准差。
最佳 **Stdev** 测量	生成最佳 std.dev 的测量总数。
可用性	提供商的可用性百分比。可用性是探测成功率，即成功率/（成功 + 失败 + 超时）

日志	说明
最佳可用性	对等组中前 15 个提供商中的最佳可用性价值。
最佳可用性测量	产生最佳可用性的测量次数
重要性	生成的合成值有助于找到可操作的数据。
唯一节点 **ID**	这些 ID 是该行度量的唯一节点 ID 的逗号分隔列表。
测量类型	记录的测量值，其含义因探头类型而异。它是 HTTP_COLD（可用性）、HTTP_RTT（往返时间）或 HTTP_KBPS（吞吐量）。
提供商 **ID**	该提供商的内部 NetScaler ITM ID 号。

缓存节点 **ID** 报告（以前的多服务提供商报告）

此报告用于标识响应请求的特定服务器或数据中心，并帮助诊断服务器问题。

- 它提供响应特定请求的数据中心或计算机的 ID。
- 它有助于理解为什么通过特定节点（POP 或计算机，或节点 ID）的性能好还是坏。
- 性能包括响应时间、吞吐量、可用性（探测类型）、DNS 解析器 IP、客户端 IP /28 以及为对象提供服务的缓存节点。
- 下面是 TSV 文件格式的平台缓存节点 ID 报告示例。

日志说明　下面是“缓存节点 ID 报告”的列标题和说明。这些字段在输出文件中按以下顺序显示：

日志	说明
提供商名称	这是正在测量的提供商的名称。
测量值	记录的测量值，其含义因探头类型而异。它是以毫秒为单位的连接 (1)/RTT (0) 测量值和吞吐量 (14) 以 kbps 为单位的测量值。
唯一节点 **ID**	它被称为缓存节点 ID。一个任意值，通常是 CDN 边缘服务器返回的 IP，以帮助 CDN 在内部识别哪个服务器处理了特定请求。”（空字符串）：来自不支持 UNI 检测的 Radar 客户端。0：用户代理不支持 UNI 检测所需的功能。1：客户端在 UNI 检测期间发现错误，例如 HTTP 404 或其他不成功的响应。2：尝试了 UNI 检测，但导致错误。
解析器国家/地区	处理请求的 DNS 解析器所在的国家/地区。
解析器区域	处理请求的 DNS 解析器所在的区域。

日志	说明
解析器状态	处理请求的 DNS 解析器的状态。
解析器 **ASN**	处理请求的 DNS 解析器的自治系统编号。通常是具有 DNS 解析器的 ASN。
解析器 **ASN** 名称	ASN 的名称。
解析器 **IP**	我们的基础结构从中接收 DNS 请求的 DNS 解析器的 IP 地址。
客户国家/地区	生成此度量的最终用户所在的国家/地区。
客户区域	生成此测量的最终用户区域。
客户状态	生成此测量的最终用户的状态。
客户端 **ASN**	生成此测量值的最终用户的自治系统编号 (ASN) 编号。通常是具有客户端 IP 的 ASN。
客户端 **ASN** 名称	生成测量的最终用户的 ASN 的名称。
客户端 **IP**	生成测量的最终用户的 IP。
成功	成功测量的总数。提示：成功/总计 == 可用性。
超时	超时的测量次数。
错误	误差的测量次数。
总数	测量的总数。
平均值	每行测量值的平均值。
中位数	当测量值按顺序列出时，第 50 个百分位数值是特定提供者的测量值的中间值。
5th	提供程序的第 5 个百分位数值。
10th	提供程序的第 10 个百分位数值。
90th	提供程序的第 90 个百分位数值。
95th	提供程序的第 95 个百分位数值。
Stdev	提供者的标准差。
可用性	提供商的可用性百分比。
重要性	生成的合成值有助于找到可操作的数据。

按国家/**ASN** 按小时列报告

- 此报告有助于验证您的提供商在一天中的绩效是否有显著差异。

- 它显示测量结果被截断到小时的时间，例如 `2018-03-11T23:00:00`。
- 下面是 TSV 文件格式的按国家/ASN 列出的平台小时报告示例。

日志说明　下面是“按国家/地区/ASN 报告列出的每小时报告”的列标题和说明。这些字段在输出文件中按以下顺序显示：

日志	说明
时间戳 **60** 分钟	进行测量时的 UTC 时间缩短为小时，例如 2018-03-11T23:00:00。
提供商名称	这是正在测量的提供商的名称。
测量类型	记录的测量值，其含义因探头类型而异。它是 HTTP_COLD（可用性）、HTTP_RTT（往返时间）或 HTTP_KBPS（吞吐量）。
客户国家/地区	生成此度量的最终用户所在的国家/地区。
客户端 **ASN**	生成此测量值的最终用户的自治系统编号 (ASN) 编号。通常是具有客户端 IP 的 ASN。
客户端 **ASN** 名称	生成测量的最终用户的 ASN 的名称。
成功	成功测量的总数。提示：成功/总计 == 可用性。
超时	超时的测量次数。
错误	误差的测量次数。
总数	测量的总数。
平均值	每行测量值的平均值。
中位数	当测量值按顺序列出时，第 50 个百分位数值是特定提供者的测量值的中间值。
5th	提供程序的第 5 个百分位数值。
10th	提供程序的第 10 个百分位数值。
90th	提供程序的第 90 个百分位数值。
95th	提供程序的第 95 个百分位数值。
Stdev	提供者的标准差。
可用性	提供商的可用性百分比。
重要性	生成的综合价值有助于找到可操作的数据。
提供商 **ID**	该提供商的内部 NetScaler ITM ID 号。

ISP 的 Radar 日志描述和报告

适用于 ISP 的 Radar 日志

利用 Radar 日志，互联网服务提供商可以详细衡量其在全球平台上的表现。互联网服务提供商可以使用这些数据来查找必须进行改进的领域或验证预期的性能。

- 提供对 Radar 测量的访问。
- 提供从公共平台上的互联网服务提供商处获取的测量数据，而不考虑生成测量结果的页面。
- Radar 日志包括原始日志中可用字段的子集，其中包括一些匿名数据：客户端 IP /28、哈希 Referer MD5。
- 日志文件采用 TSV 格式。
- 下面是 TSV 文件格式的网络 Radar 日志共享示例。

日志说明　下面是面向 ISP 的 Radar 日志的列标题和说明。这些字段在输出文件中按以下顺序显示。

日志	说明
时间戳	现在是 YYYY-MM-DDTHH:MI:SSZ 格式的请求的 UTC 时间。日志表中的实际值（向下到秒）分别四舍五入到小时/日表中最接近的小时 (2018-03-30T23:00:00Z) 或日 (2018-03-30T00:00:00Z)。在所有数据集中，时间戳始终采用 UTC 格式。
提供商 **ID**	正在测量的平台的内部 ID。
探测类型	所测量的探测类型（例如：1：HTTP 连接时间；0：HTTP 响应时间；14：HTTP 吞吐量等）。它在允许的时间内成功返回的信息将用于指示该服务可用。
响应代码	测量结果。例如：0：成功，1：超时，4：错误。对于可用性计算，响应为 0（成功）的测量值与测量总数（总计）的百分比。对于其他探测类型（RTT 和吞吐量），在计算 RTT 的统计数据时，过滤器只能考虑成功码为 0 的 RTT 数据点。吞吐量相同。
测量值	记录的测量值，其含义因探头类型而异。它的可用性 (1) /响应时间 (0) 度量单位为毫秒，吞吐量 (14) 以 kbps 为单位。
解析器市场	处理请求的 DNS 解析器的市场。通常是 DNS 解析器所在的大陆，其中 0：未知 (XX)，1：北美 (NA) 5：非洲 (AF)，3：欧洲 (EU)，4：亚洲 (AS)，2：大洋洲 (OC)，6：南美洲 (SA)。

日志	说明
解析器国家/地区	处理请求 ID 的 DNS 解析器所在的国家/地区可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/countries.json.gz
解析器区域	处理请求 ID 的 DNS 解析器所在的区域可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/regions.json.gz。并非世界上所有国家/地区都定义了区域。
解析器状态	处理请求 ID 的 DNS 解析器的状态可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/states.json.gz。并非世界上所有国家/地区都定义了州。
解析器 **ASN**	处理请求的 DNS 解析器的自治系统编号 (ASN)。通常情况下，具有 DNS 解析器 ID 的 ASN 可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/asns.json.gz。
解析器 **IP**	我们的基础结构从中接收 DNS 请求的 DNS 解析器的 IP 地址。
客户市场	生成此度量的最终用户市场。通常是客户端 IP 所在的大陆；其中，0：未知 (XX)，1：北美 (NA) 5：非洲 (AF)，3：欧洲 (EU)，4：亚洲 (AS)，2：大洋洲 (OC)，6：南美洲 (SA)。
客户国家/地区	生成此 measurement.IDs 的最终用户所在的国家/地区可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/countries.json.gz
客户区域	生成此测量的最终用户区域。通常是客户端 IP 所在的地理区域。可以将 ID 映射到以下位置下的名称：https://community-radar.citrix.com/ref/regions.json.gz。并非世界上所有国家/地区都定义了区域。
客户状态	生成此测量的最终用户的状态。通常是客户端 IP 所在的状态。可以将 ID 映射到以下位置下的名称：https://community-radar.citrix.com/ref/states.json.gz。并非世界上所有国家/地区都定义了州。

日志	说明
客户端 **ASN**	生成此测量值的最终用户的自治系统编号 (ASN)。通常是具有客户端 IP 的 ASN。可以将 ID 映射到以下位置下的名称：https://community-radar.citrix.com/ref/asns.json.gz
客户端 **IP**	生成此测量的最终用户的 IP。
Referer 主机 **MD5**	Referer 信息（协议、主机和路径）来自 Radar HTTP 请求的 Referer 标头。Referer 主机 MD5 经过哈希处理。
用户代理	这是托管标签的浏览器页面中的用户代理字符串。例如，如果您使用 Chrome 浏览带有 Radar 标签的网页，则后台的 测 Radar 量值会记录您的 Chrome 浏览器中的用户代理。这些衡量标准包括 Chrome 浏览器、Chrome 版本、有关运行 Chrome 的操作系统的信息等。
DNS 查找时间（可选）	使用资源计时 API，计算域名查找结束和域名查找开始之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 domainLookupEnd - domainLookupStart。
TCP 连接时间（可选）	使用资源计时 API，计算连接端和连接启动之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 connectEnd - connectStart。
安全连接时间（可选）	使用资源计时 API，计算连接端和安全连接启动之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 connectEnd - secureConnectionStart。
延迟（可选）	使用资源计时 API，可以计算响应开始和请求启动之间的差异。它计算两个值均不为 null 且响应开始时间大于请求开始时间的情况。它的计算方式为 responseStart - requestStart
下载时间（可选）	使用资源计时 API，计算响应结束和响应开始之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 responseEnd - responseStart。

日志	说明
客户配置文件	此字段有助于识别数据是来自移动应用程序还是浏览器。它还允许我们区分 iOS、Android 应用程序和浏览器。数字用于标识每个客户配置文件。此字段的值为：null、0、1、2、3、4。其中，null：通常表示不支持发送 client_profile 值的较旧的 Radar 客户端。0：浏览器；1：iOS-用 Swift 编写的 iOS 版 Radar runner 应用程序；2：Android；3：移动版网站上的浏览器；4：iOS-用 Objective-C 编写的 iOS 版 Radar Runner 应用程序。
客户配置文件版本	客户端配置文件版本告诉我们在移动应用程序中使用了哪个版本的 Radar Runner 代码（适用于 iOS）或 AndroidRadar SDK（适用于 Android）。此字段仅供内部使用。
设备类别	所有设备都分为以下其中一种：智能手机、平板电脑、PC、智能电视及其他。如果解析器无法确定任何字段的值，则使用“其他”作为默认值。
设备	用户使用的设备类型，例如 Apple iPhone。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。
浏览器	用户正在使用的浏览器类型，例如移动浏览器 UI/WKWebView 0.0.0。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。
操作系统	正在使用的操作系统，例如 iOS 11.0.3。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。

ISP 的子网报告

- 该报告向互联网服务提供商提供了有关其网络的特定子网如何通过测量的平台为其用户提供性能的信息。
- 它提供了有关响应特定请求的服务提供商的信息。
- 它有助于了解网络子网的性能。
- 性能包括响应时间、吞吐量、可用性（探测类型）、DNS 解析器 IP、客户端 IP /28 以及为对象提供服务的缓存节点。
- 下面是 TSV 文件格式的网络子网报告示例。

日志说明　下面是 ISP 子网报告的列标题和说明。这些字段在输出文件中按以下顺序显示：

日志	说明
ASN 名称	进行测量的自治系统的名称。
测量值	记录的测量值，其含义因探头类型而异。它是以毫秒为单位的连接 (1)/RTT (0) 测量值和吞吐量 (14) 以 kbps 为单位的测量值。
子网	发出请求的用户的子网。
解析器 **ASN**	处理请求的 DNS 解析器的自治系统编号。通常是具有 DNS 解析器的 ASN。
解析器 **IP**	我们的基础结构从中接收 DNS 请求的 DNS 解析器的 IP 地址。
客户端 **ASN**	生成此测量值的最终用户的自治系统编号 (ASN) 编号。通常是具有客户端 IP 的 ASN。
客户端 **IP**	生成测量的最终用户的 IP。
平台 **ID**	向其执行查询的服务提供商平台的 ID。
平台名称	向其执行查询的服务提供商平台的名称
成功	成功测量的总数。提示：成功/总计 == 可用性。
超时	超时的测量次数。
错误	误差的测量次数。
总数	测量的总数。
平均值	每行测量值的平均值。
中位数	当测量值按顺序列出时，第 50 个百分位数值是特定提供者的测量值的中间值。
5th	提供程序的第 5 个百分位数值。
10th	提供程序的第 10 个百分位数值。
90th	提供程序的第 90 个百分位数值。
95th	提供程序的第 95 个百分位数值。
Stdev	提供者的标准差。
可用性	提供商的可用性百分比。
重要性	生成的合成值有助于找到可操作的数据。
测量类型	记录的测量值，其含义因探头类型而异。它是 HTTP_COLD（可用性）、HTTP_RTT（往返时间）或 HTTP_KBPS（吞吐量）。

互联网服务提供商的匿名最佳报告

- 在“匿名最佳”报告中，对等组用于“最佳”比较。对等组基于 ISP 的位置。它通常是指定国家/地区内 10 家测量最多的互联网服务提供商，会话至少超过 1000 次。
- “最佳”ISP 的结果有助于 ISP 将性能工作重点放在高容量或业务关键型平台以及竞争力较弱的领域。
- 报告提供了按地域和平台分列的绩效细节，并将其与“最佳”ISP 进行比较，以同样的标准。
- 可用于 RTT 和吞吐量。
- 下面是 TSV 文件格式的 RTT 的网络匿名最佳报告示例。

日志说明　下面是“匿名最佳报告”的列标题和说明。这些字段在输出文件中按以下顺序显示。

日志	说明
测量类型	记录的测量值，其含义因探头类型而异。它是 HTTP_COLD（可用性）、HTTP_RTT（往返时间）或 HTTP_KBPS（吞吐量）。
客户国家/地区	生成此度量的最终用户所在的国家/地区。
客户区域	生成此测量的最终用户区域。
客户状态	生成此测量的最终用户的状态。
客户端 **ASN ID**	生成此测量值的最终用户的自治系统编号 (ASN) 编号。通常是具有客户端 IP 的 ASN。
客户端 **ASN** 名称	生成测量的最终用户的 ASN 的名称。
解析器国家/地区	处理请求的 DNS 解析器所在的国家/地区。
解析器区域	处理请求的 DNS 解析器所在的区域。
解析器状态	处理请求的 DNS 解析器的状态。
平台 **ID**	尝试查询的服务提供商平台的 ID。
平台名称	尝试查询的服务提供商平台的名称。
成功	成功测量的总数。提示：成功/总计 == 可用性。
超时	超时的测量次数。
错误	误差的测量次数。
总数	测量的总数。
平均值	该行所有测量值的平均值。
最佳平均值	同行组中排名前 15 位的提供商中的最佳平均值。
最佳平均值测量	产生最佳均值计数的测量总数。

日志	说明
中位数	当测量值按顺序列出时，第 50 个百分位数值是特定提供者的测量值的中间值。
最佳中位数	对等组中前 15 个提供商的最佳第 50 个百分位数值（低于该值的 50%的测量值）。
最佳中位数测量值	生成 best_median 的测量总数
5th	提供程序的第 5 个百分位数值。
第 **5** 次最佳	同行组中前 15 个提供商中的最佳第 5 个百分位数值。
第 **5** 次最佳测量	产生 best_5th 的测量总数
10th	提供程序的第 10 个百分位数值。
最佳第 **10** 个	同行组中前 15 个提供商中的最佳第 10 个百分位数值。
第 **10** 次最佳测量	产生 best_10 的测量总数
90th	提供程序的第 90 个百分位数值。
最佳第 **90** 个	在同行组中排名前 15 位的提供商中，最好的第 90 个百分位数值。
第 **90** 次最佳测量	产生 best_90 的测量总数
95th	提供程序的第 95 个百分位数值。
最佳第 **95** 个	在同行组中排名前 15 位的提供商中，最好的第 95 个百分位数值。
第 **95** 次最佳测量	产生 best_95 的测量总数
Stdev	提供者的标准差。
最佳 **Stdev**	同行组中排名前 15 位的提供商中的最佳标准差。
最佳 **Stdev** 测量	生成最佳 std.dev 的测量总数。
可用性	提供商的可用性百分比。可用性是探测成功率，即成功率/（成功 + 失败 + 超时）
最佳可用性	对等组中前 15 个提供商中的最佳可用性价值。
最佳可用性测量	产生最佳可用性的测量次数。
重要性	生成的合成值有助于找到可操作的数据。

导航计时日志说明

导航计时数据

导航计时数据提供了对网页页面加载过程各个部分的见解。

这些数据因最终用户的位置、网络问题、提供商所做的更改等原因而有所不同。客户可以使用导航计时数据来优化最终用户在加载受监视网页时的体验。

可以对每个 Radar 会话进行测量（如果启用）。每个会话都附有一个 ID 号，有助于跟踪会话中的所有测量。这些测量结果通过 NEM 作为导航定时日志与客户共享。

下面是 TSV 文件格式的导航计时数据示例。

下面是导航计时日志的列标题和说明。这些字段在输出文件中按以下顺序显示：

日志	说明
时间戳	现在是 YYYY-MM-DDTHH:MI:SSZ 格式的请求的 UTC 时间。日志表中的实际值（向下到秒）分别四舍五入到小时/日表中最接近的小时 (2018-03-30T23:00:00Z) 或日 (2018-03-30T00:00:00Z)。在所有数据集中，它始终采用 UTC 格式。
响应代码	测量结果。例如：0：成功，1：超时，4：错误。对于可用性计算，响应为 0（成功）的测量值与测量总数（总计）的百分比。对于其他探测类型（RTT 和吞吐量），在计算 RTT 的统计数据时，过滤器仅考虑成功码为 0 的 RTT 数据点。吞吐量相同。
解析器市场	处理请求的 DNS 解析器的市场。通常是 DNS 解析器所在的大陆，其中 0：未知 (XX)，1：北美 (NA) 5：非洲 (AF)，3：欧洲 (EU)，4：亚洲 (AS)，2：大洋洲 (OC)，6：南美洲 (SA)。
解析器国家/地区	处理 request.IDs 的 DNS 解析器所在的国家/地区可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/countries.json.gz
解析器区域	处理 request.IDs 的 DNS 解析器所在的区域可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/regions.json.gz。并非世界上所有国家/地区都定义了区域。
解析器状态	处理 request.IDs 的 DNS 解析器的状态可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/states.json.gz。并非世界上所有国家/地区都定义了州。

日志	说明
解析器 **ASN**	处理请求的 DNS 解析器的自治系统编号 (ASN)。通常是具有 DNS 解析器的 ASN。可以将 ID 映射到以下位置下的名称：https://community-radar.citrix.com/ref/asns.json.gz
解析器 **IP**	我们的基础结构从中接收 DNS 请求的 DNS 解析器的 IP 地址。
客户市场	生成此度量的最终用户市场。通常是客户端 IP 所在的大陆；其中，0：未知 (XX)，1：北美 (NA) 5：非洲 (AF)，3：欧洲 (EU)，4：亚洲 (AS)，2：大洋洲 (OC)，6：南美洲 (SA)。
客户国家/地区	生成此 measurement.IDs 的最终用户所在的国家/地区可以映射到以下位置下的名称：https://community-radar.citrix.com/ref/countries.json.gz
客户区域	生成此测量的最终用户区域。通常是客户端 IP 所在的地理区域。可以将 ID 映射到以下位置下的名称：https://community-radar.citrix.com/ref/regions.json.gz。并非世界上所有国家/地区都定义了区域。
客户状态	生成此测量的最终用户的状态。通常是客户端 IP 所在的状态。可以将 ID 映射到以下位置下的名称：https://community-radar.citrix.com/ref/states.json.gz。并非世界上所有国家/地区都定义了州。
客户端 **ASN**	生成此测量值的最终用户的自治系统编号 (ASN)。通常是具有客户端 IP 的 ASN。可以将 ID 映射到以下位置下的名称：https://community-radar.citrix.com/ref/asns.json.gz
客户端 **IP**	生成测量的最终用户的 IP。
Referer 主机	Referer 信息（协议、主机和路径）来自 Radar HTTP 请求的 Referer 标头。
Referer 协议	Referer 信息（协议、主机和路径）来自 Radar HTTP 请求的 Referer 标头。
Referer 路径	Referer 信息（协议、主机和路径）来自 Radar HTTP 请求的 Referer 标头。
设备类别	所有设备都分为以下其中一种：智能手机、平板电脑、PC、智能电视及其他。如果解析器无法确定任何字段的值，则使用“其他”作为默认值。

日志	说明
设备	用户使用的设备类型，例如 Apple iPhone。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。
浏览器	用户正在使用的浏览器类型，例如移动浏览器 UI/WKWebView 0.0.0。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。
操作系统	正在使用的操作系统，例如 iOS 11.0.3。用户代理字符串从托管 Radar 标签的页面上运行的浏览器中检测到它。
DNS 查找时间	使用资源计时 API，计算域名查找结束和域名查找开始之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 domainLookupEnd - domainLookupStart。
TCP 连接时间	使用资源计时 API，计算连接端和连接启动之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 connectEnd - connectStart。
安全连接时间	使用资源计时 API，计算连接端和安全连接启动之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 connectEnd - secureConnectionStart。
加载事件	这是从加载事件的开始到结束所花费的持续时间或时间。当两个值都不为空且结束时间大于开始时间时，它的计算方式为 LoadEventEnd - LoadEventStart。
重定向	这是从“导航开始”到“开始获取”所花费的持续时间或时间。当两个值都不为空且结束时间大于开始时间时，它的计算方式为 FetchStart - NavigationStart。
页面总加载量	这是从导航开始到页面加载事件结束所花费的持续时间或时间。当两个值均不为空且结束时间大于开始时间时，其计算方式为 - Load Event End - Navigation Start。
DOM	从 DOM 加载到 DOM 完成所需的持续时间或时间。当两个值都不为空且结束时间大于开始时间时，其计算方式为 DomComplete - DomLoading。
延迟	使用资源计时 API，可以计算响应开始和请求启动之间的差异。它计算两个值均不为 null 且响应开始时间大于请求开始时间的情况。它的计算方式为 responseStart - requestStart

日志	说明
下载时间	使用资源计时 API，计算响应结束和响应开始之间的差异。它计算两个值均不为 null 且结束时间大于开始时间的情况。它的计算方式为 responseEnd - responseStart。
交互式 **DOM**	从导航开始到 DOM 交互式所需的持续时间或时间。当两个值都不为空且结束时间大于开始时间时，它被计算为 DomInteractive - NavigationStart。
开始渲染	从导航开始到开始渲染所需的持续时间或时间。当两个值都不为空且结束时间大于开始时间时，它将计算为 startRender - NavigationStart。

Openmix 和 **HTTP Openmix** 日志

Openmix 和 HTTP Openmix 日志允许客户使用实时测量来监视其 Openmix 应用程序的行为。他们可以使用这些数据来查找需要改进的领域或验证其应用程序的预期性能。

- 这些日志为 Openmix 客户提供了实时测量结果。
- 这些日志的推荐文件格式为 JSON，但也有 TSV 格式。
- 下面是 TSV 文件格式的 Openmix 和 HTTP Openmix 日志共享数据的示例。

Openmix 日志说明

日志	说明
时间戳	现在是 YYYY-MM-DDTHH:MI:SSZ 格式的请求的 UTC 时间。日志表中的实际值（向下到秒）分别四舍五入到小时/日表中最接近的小时 (2018-03-30T23:00:00Z) 或日 (2018-03-30T00:00:00Z)。在所有数据集中，时间戳始终采用 UTC 格式。
应用程序所有者区域 **ID**	为请求提供服务的应用程序所有者的区域 ID。此值始终等于 1。
应用程序所有者客户 **ID**	为请求提供服务的应用程序所有者的客户 ID。对于 HTTP 请求，请在请求路径中编码此 ID，然后使用它来查找要运行的应用程序。
应用程序 **ID**	客户帐户中为请求提供服务的应用程序 ID。此 ID 也编码在 HTTP 请求路径中。应用程序 ID 从 1 开始，并且仅对客户是唯一的。您必须通过在 appOwnerCustomerId 上进行查询来完全限定特定应用程序 ID 的查询。

日志	说明
应用程序版本	为帐户提供服务的应用程序的版本。每次通过门户或 API 更新应用程序时，版本都会递增。记录请求时正在运行的版本。随着应用程序的更新，此信息可用于分隔一段时间的版本化逻辑。网络中的主机通常会在相似的时间范围内收到更新，但几乎不会在同一时刻收到更新。在更新过程中，时间上的重叠决策可能会使用不同版本的应用程序。
应用程序名称	为帐户提供服务的应用程序的名称。
市场	生成此度量的最终用户市场。
国家/地区	生成此度量的最终用户所在的国家/地区。
地理区域	生成此测量的最终用户区域。
状态	生成此测量的最终用户的状态。
ASN ID	生成此测量值的最终用户的自治系统编号 (ASN)。通常是具有客户端 IP 的自治系统编号。
ASN 名称	生成测量的最终用户的 ASN 的名称。
有效的 **IP**	有效 IP 是用于处理请求的 IP。它是查询字符串指定的 IP 覆盖请求的 IP（相对 DNS 流的解析器/ECS/EDNS ID）。这是系统在处理信息时将其视为目标的地址。此 IP 可以是请求解析器的 IP，或者是客户端的 ECS IP 地址（如果支持 EDNS ECS）。因此，传递给应用程序逻辑的所有探测性能数据、地理信息等都基于此 IP。
解析器市场	处理请求的 DNS 解析器的市场。
解析器国家/地区	处理请求的 DNS 解析器所在的国家/地区。
解析器区域	处理请求的 DNS 解析器所在的区域。
解析器状态	处理请求的 DNS 解析器的状态。
解析器 **ASN ID**	处理请求的 DNS 解析器的自治系统编号 (ASN)。通常是具有 DNS 解析器的自治系统编号。
解析器 **ASN** 名称	处理请求的解析器的 ASN 名称。
解析器 **IP**	我们的基础结构从中接收 DNS 请求的 DNS 解析器的 IP 地址。
决策提供商名称	应用程序选择的平台的别名。
原因代码	在应用程序中设置的原因代码，说明决策背后的原因。
原因日志	此日志是来自 Openmix 应用程序的客户定义输出。这是一个可选的字符串字段，使客户能够记录有关其 Openmix 应用程序决策的信息。

日志	说明
回退模式	此模式指示应用程序在处理请求时是否处于回退模式。在准备执行请求过程中出现故障时，会发生回退。
使用的 **EDNS**	如果应用程序使用 EDNS 客户端子网扩展，则为 true。
TTL	交还的 TTL（生存时间）。
回应	请求返回的 CNAME。
结果	此字段中的值始终为 1。
上下文	这是 Openmix 在处理请求时可用 Radar 数据的摘要。Openmix 会根据每个请求的有效值解析 Radar 数据，因此同时发出请求的两个客户端可以具有不同的上下文字符串。

开放式 **HTTP API** 日志说明

日志	说明
时间戳	现在是 YYYY-MM-DDTHH:MI:SSZ 格式的请求的 UTC 时间。日志表中的实际值（向下到秒）分别四舍五入到小时/日表中最接近的小时 (2018-03-30T23:00:00Z) 或日 (2018-03-30T00:00:00Z)。在所有数据集中，时间戳始终采用 UTC 格式。
应用程序所有者区域 **ID**	为请求提供服务的应用程序所有者的区域 ID。此值始终等于 1。
应用程序所有者客户 **ID**	为请求提供服务的应用程序所有者的客户 ID。对于 HTTP 请求，请在请求路径中编码此 ID，用于查找要运行的应用程序。
应用程序 **ID**	客户帐户中为请求提供服务的应用程序 ID。此 ID 也编码在 HTTP 请求路径中。应用程序 ID 从 1 开始，并且仅对客户是唯一的。您必须通过在 appOwnerCustomerId 上进行查询来完全限定特定应用程序 ID 的查询。
应用程序版本	为帐户提供服务的应用程序的版本。每次通过门户或 API 更新应用程序时，版本都会递增。记录请求时正在运行的版本。随着应用程序的更新，此信息可用于分隔一段时间的版本化逻辑。网络中的主机通常会在相似的时间范围内收到更新，但几乎不会在同一时刻收到更新。在更新过程中，时间上的重叠决策可能会使用不同版本的应用程序。

日志	说明
应用程序名称	为帐户提供服务的应用程序的名称。
市场	生成此度量的最终用户市场。
国家/地区	生成此度量的最终用户所在的国家/地区。
地理区域	生成此测量的最终用户区域。
状态	生成此测量的最终用户的状态。
ASN ID	生成此测量结果的最终用户的自治系统编号 (ASN) 的 ID，即与 ASN 名称关联的网络 ID 号
ASN 名称	生成测量的最终用户的 ASN 的名称。
有效的 **IP**	有效 IP 是用于处理请求的 IP。它是查询字符串指定的 IP 覆盖请求的 IP（相对 DNS 流的解析器/ECS/EDNS ID）。这是系统在处理信息时将其视为目标的地址。此 IP 可以是请求解析器的 IP，或者是客户端的 ECS IP 地址（如果支持 EDNS ECS）。传递给应用程序逻辑的所有探测性能数据、地理信息等都基于此 IP。
决策提供商名称	应用程序选择的平台的别名。
原因代码	在应用程序中设置的原因代码，说明决策背后的原因。
原因日志	此日志是来自 Openmix 应用程序的客户定义输出。这是一个可选的字符串字段，使客户能够记录有关其 Openmix 应用程序决策的信息。
回退模式	此模式指示应用程序在处理请求时是否处于回退模式。在准备执行请求过程中出现故障时，会发生回退。
响应代码	测量结果。例如：0：成功，1：超时，4：错误。对于可用性计算，响应为 0（成功）的测量值与测量总数（总数，不管响应如何）的百分比。对于其他探测类型（RTT 和吞吐量），在计算 RTT 的统计数据时，过滤器只能考虑成功码为 0 的 RTT 数据点。吞吐量相同。
HTTP 方法	HTTP 方法（GET/POST/OPTIONS/等）与客户服务向 HTTP Openmix 服务器发出的请求有关。这些方法共同构成了入站 URL 和出站 HTTP 响应的一部分。
URI	这是请求路径。如果客户没有得到他们想要的行为，那可能是因为请求结构不当。日志显示了我们的服务器正在接收的内容（协议、主机和路径）。Referer 信息（协议、主机和路径）来自 Radar HTTP 请求的 Referer 标头。对于 HTTP OPX，整个 Referer（协议、主机和路径）包含在一个标有 Referer 的字符串中。

日志	说明
用户代理	这是托管标签的浏览器页面中的用户代理字符串。例如，如果您使用 Chrome 浏览带有 Radar 标签的网页，则后台的 测 Radar 量值会记录您的 Chrome 浏览器中的用户代理。这些衡量标准包括 Chrome 浏览器、Chrome 版本、有关运行 Chrome 的操作系统的信息等。
上下文	这是 Openmix 在处理请求时可用 Radar 数据的摘要。Openmix 会根据每个请求的有效值解析 Radar 数据，因此同时发出请求的两个客户端可以具有不同的上下文字符串。

针对第三方组织的自定义报告

客户可以与 NetScaler 合作，根据 NetScaler 收集的 Radar 数据获取自定义报告。NetScaler 可以生成按计划运行的报告。报告以数据文件的形式提供，通常采用 TSV 格式。

常见问题解答

Radar

文件推送到 **S3** 和 **GCS** 的频率有多高　Radar 的文件存放频率为每分钟一次，报告的存档频率为每天。

报告存储在哪里　S3 旧版（位置 1）：

```
s3://public-radar/[customer name]/
```

S3（位置 2）：

```
s3://cedexis-netscope/[customer id]/
```

GCS（地点 3）：

```
gs://cedexis-netscope-[customer id]/
```

如果您还没有 **S3** 访问凭证，如何获得它们　该门户提供“访问”和“秘密”密钥。使用带有“s3cmd”、“awscli”或其他工具的密钥来访问 S3。对于 Google 存储，门户网站会下载一个带有访问凭据的文件，以便与“gsutil”工具配合使用。

如何将访问密钥和私有密钥与 **s3cmd** 一起使用来从 **S3** 存储桶下载日志和报告　首先，您需要从 https://s3tools.org/download 中下载并安装 s3cmd，有关用法、选项和命令，请参阅 https://s3tools.org/usage。然后运行以下命令：

```
s3cmd --access_key=[access key] --secret_key=[secret key] ls s3://cedexis-netscope/<customer id>/radar/
<!--NeedCopy-->
```

要下载文件，请运行以下命令：

```
s3cmd --access_key=[access_key] --secret_key=[secret_key] get s3://cedexis-netscope/<customer id>/radar/[the_filename_to_download] [the_name_of_the_local_file]
<!--NeedCopy-->
```

如何使用 **s3cmd** 配置列出 **S3** 存储桶中的文件　第一步是安装 s3cmd。可以从 http://s3tools.org/download 进行安装

要配置 s3cmd，请运行以下命令

```
s3cmd ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```

如果您已经使用了另s3cmd 一组访问密钥和私有密钥，请按照下列步骤操作：

如果您已经在使用 s3cmd，则在 ~/.s3cfg 下创建默认配置的副本。例如，制作一个副本并将其命名为 ~/.s3cfg_netscope。将 ~/.s3cfg_netscope 中的访问和私钥条目替换为我们提供的条目。
使用新配置，而不是默认配置（贵公司的）通过以下命令访问 S3 存储桶：

```
s3cmd -c ~/.s3cfg_netscope ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```

主要区别在于您必须把配置文件放在 Citrix 提供的访问和私有密钥的位置。-c

如果要在多组密钥之间切换，请将它们嵌入到文件中。请参阅带有 -c 选项的文件以指定您正在使用的密钥对。

> 注意： -c 参数指示包含访问密钥和私有密钥的配置文件的位置。

如何将密钥文件与 **gsutil** 或 **gcloud** 一起使用来下载日志文件　下载谷歌服务帐户 JSON 密钥文件后，您可以使用它来验证您的 Google 帐户凭据，查看或下载日志文件。例如，以下是使用 Google gcloud 和 gsutil 命令行实用程序来实现此目标的一种方法：

步骤 1：激活密钥文件

验证命令 gcloud auth activate- 或 gsutil config -e 是验证运行 gcloud 或 gsutil 命令的密钥文件所必需的。

对于 **gcloud**：

使用下载的密钥文件运行以下命令：

```
gcloud auth activate-service-account --key-file [downloaded config file
    ]
<!--NeedCopy-->
```

或

```
gcloud auth activate-service-account --key-file=[path and file name of
    key file]
<!--NeedCopy-->
```

对于 **gsutil**：

使用下载的配置文件运行以下命令：

```
gsutil config -e
<!--NeedCopy-->
```

步骤 2：列出 GCS（Google 云存储）存储桶中的文件

按前面步骤所述激活服务帐号密钥文件后，使用以下命令列出 GCS 存储桶中的文件：

```
gsutil ls gs://cedexis-netscope-<customer id>
<!--NeedCopy-->
```

步骤 3（如有必要）：还原原始凭据（或在帐户之间来回切换）

您可以通过执行以下操作在 NetScaler ITM 帐户与您已通过身份验证的其他 Google Cloud 凭据之间切换。

首先，运行以下命令列出所有帐户：

```
gcloud auth list
<!--NeedCopy-->
```

然后使用以下命令切换到另一个帐户：

```
gcloud config set account [email of the account to switch to as shown
    in gcloud auth list]
<!--NeedCopy-->
```

您可以使用相同的命令在帐户之间来回切换，方法是将电子邮件替换为要切换到的帐户邮箱。

文件名是什么样子　传统日报：

Radar 每日日志 ShareFile 名称具有以下结构：

`<prefix><date: YYYY-MM-DD>.<customer_id>.part<uniq_id>.kr.txt.gz`

例如`Cedexis_Daily-2017-11-07.21222.part-cc901e1dd55eal4e.kr.txt.gz`（非标准示例）

传统实时：

Radar 实时日志 ShareFile 名称具有以下结构：

`<prefix><customer_id>-YYYY-MM-DDTHH:MM<uniq_id>.txt.gz`

例如 `Cedexis_3-32291-2017-11-08T20:56-cc907e8fd71eaf4e.txt.gz`

Netscope NEM 格式：

用于每日和实时日志共享文件的 Netscope NEM 格式具有以下结构：

`<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.gz`

其中，

- `freq: "daily"| "rt"| "hr"`
- `log_type: "radar"| "opx"| "hopx"`
- `prefix: log_share.prefix`
- `id_type: "customer"| "provider"| "asn"`
- `id: log_share.match_id`
- `iso_dt: iso 8601 Date_time "YYYYMMDDTHHMMSSZ"`
- `uniq_id: hash(UUID)`
- `line_format: "tsv"| "json"`

例如 `rt-radar-TestRadar1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

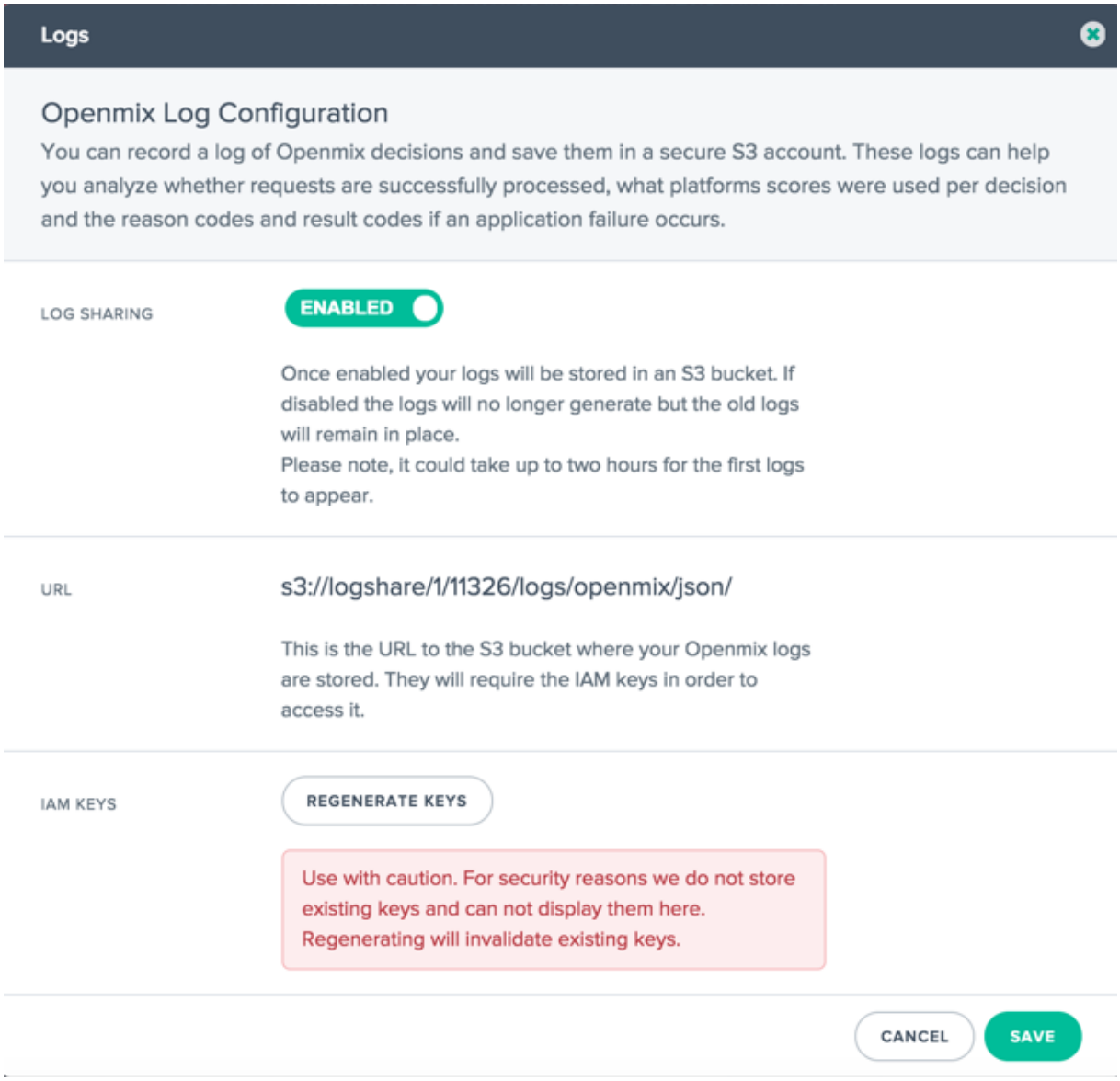
输出文件的格式是什么　对于 Radar，输出文件格式为 TSV（制表符分隔值），采用压缩格式。

开放混合和 **Openmix HTTP API**

文件推送到 **S3** 的频率有多高　文件存放的频率是 Openmix 和 HTTP Openmix 每分钟的存放次数。

如果您看不到配置 **Openmix** 和 **Openmix HTTP API** 实时日志共享的选项，该怎么办　您的客户经理可以启用所需的角色来配置和启用 Openmix 和 Openmix HTTP API 实时日志共享。

您如何开启 **Openmix** 和 **Openmix HTTP API** 实时日志共享和访问文件　在您的帐户上启用该角色后，您会看到“管理日志”图标。单击以打开“日志”对话框，您可以在其中访问 Openmix 日志配置设置。这些设置基本上就是开启 Openmix 和 HTTP Openmix 实时日志共享和访问文件所需的全部设置。



什么是后端流程　启用 Openmix 日志共享也可以启用 Openmix HTTP API 日志共享。Openmix 和 Openmix HTTP API 日志共享服务必须在 10 分钟内开始为客户输出日志。

Openmix 和 **HTTP Openmix** 报告存储在哪里　S3 旧版（位置 1）：

```
s3://logshare/[zone ID]/[customer ID]/logs/openmix/json/[YYYY]/[MM]/[DD]/[HH]/.
```

S3（位置 2）：

```
s3://cedexis-netscope/[customer id]/
```

GCS（地点 3）：


```
gs://cedexis-netscope-[customer id]/
```

文件名是什么样子　Openmix 和 HTTP Openmix 的文件名结构通常如下所示：

传统实时：

```
[zone ID, 1][customerID]-openmix-json[YYYY][MM][DD][HH][mm][ss]Z-m1-
w9-c0.gz
```

Netscope NEM 格式：

用于每日和实时日志共享文件的 Netscope NEM 格式具有以下结构：

```
<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.
gz
```

其中，

- freq: "daily"| "rt"| "hr"
- log_type: "radar"| "opx"| "hopx"
- prefix: log_share.prefix
- id_type: "customer"| "provider"| "asn"
- idv: log_share.match_id
- iso_dt: iso 8601 Date_time "YYYYMMDDTHHMMSSZ"
- uniq_id: hash(UUID)
- line_format: "tsv"| "json"

例如 `hr-opx-TestOpenmix1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

什么是输出文件格式　Openmix 和 Openmix HTTP API 的文件格式为 JSON（gzipped）。

管理

September 22, 2023

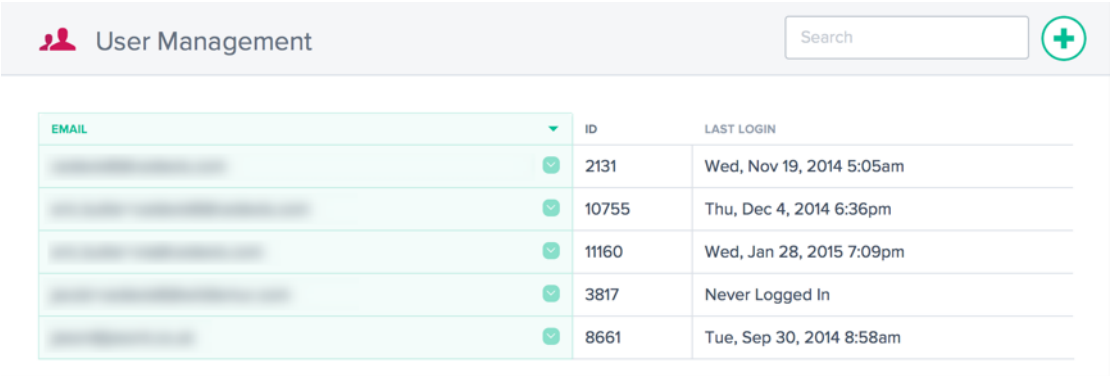
最终用户可以在我的帐户部分中管理帐户、管理可以访问该帐户的用户，以及可以访问 Fusion Purge 功能的用户。

此外，您还可以从菜单中查看到期发票并管理 OAuth API 凭据。

管理用户

在“用户”菜单中，您可以添加/删除用户，以及重置对帐户的密码访问权限。

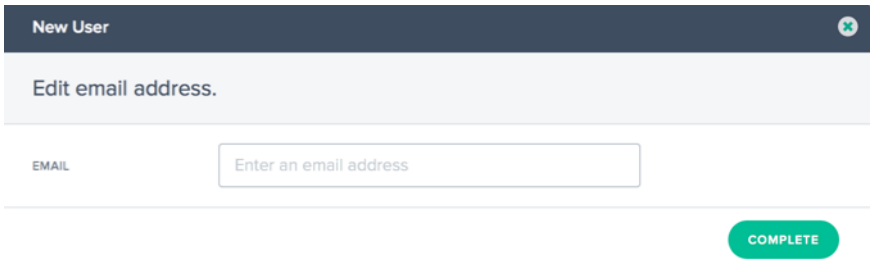
除了进行用户管理之外，您还可以输入服务通知的电子邮件地址，并查看用户的上次登录时间。



添加或删除用户以及重置密码

创建或添加用户时，请确保使用有效的电子邮件地址。密码是自动创建的，并通过电子邮件发送到作为用户名输入的电子邮件地址。

要添加新用户，请单击右上角的 **+** 。输入有效的电子邮件地址，然后单击完成。



要重置用户的密码，请单击用户电子邮件地址右侧的向下箭头，选择重置密码，然后在对话框中单击是以确认该操作。将向用户发送一封密码重置电子邮件。

单击用户电子邮件地址右侧的向下箭头并选择删除，即可将用户从系统中删除。确认该操作后，用户将被从系统中删除。

单点登录

我们支持使用第三方身份提供程序通过 SAML 2.0 以单点登录方式登录到门户。

单点登录用于对用户登录进行身份验证。我们目前不通过 SAML SSO 传递授权信息。为了能够登录，NetScaler Intelligent Traffic Management 门户中必须有一个用户具有与 SSO 身份提供程序中的用户相同的电子邮件地址。

单点登录是按帐户管理的。为帐户启用 SSO 后，所有用户都必须使用 SSO 登录来访问门户。

您可以在 **SSO** 配置菜单项中找到 SAML 配置信息。这些信息特定于您的帐户，允许您在身份提供程序中配置 SSO。如果找不到 **SSO** 配置 菜单，请联系 支持 团队。

每个身份提供程序的设置都不同，但您需要以下信息，这些信息显示在 SSO 配置页面中：

- 断言消费者服务 (ACS) URL
- 实体 ID
- 注销 URL（可选，取决于提供程序）
- 起始 URL（可选，取决于提供程序）
- 姓名格式：电子邮件
- 对响应进行签名：否

开启单点登录

添加 NetScaler Intelligent Traffic Management 门户 SSO 的一般步骤：

1. 使用 SSO 配置屏幕中的数据，设置身份提供程序
2. 从身份提供程序下载 SSO IDP 元数据文件
3. 将该文件上载到 SSO 配置页面
4. 准备好启用 SSO 后，单击启用
5. 用户现在将需要通过 SSO 登录页面进行登录。

关闭单点登录

如果配置并启用了 SSO，请单击禁用按钮。

帐户中任何想要登录的用户现在都需要在标准登录屏幕上使用 Citrix 密码。如果用户不知道自己的密码，帐户管理员可以发送密码重置电子邮件，用户也可以从登录屏幕请求密码重置电子邮件。

Google G Suite 的配置步骤

下面是将单点登录用于 Google G Suite 登录时所需的步骤：

在 Google G Suite 中：

1. 打开 G Suite 管理控制台，进入“应用程序”部分
2. 单击 **SAML** 应用程序类别
3. 单击为 **SAML** 应用程序启用 **SSO** 按钮
4. 在对话框底部，选择设置我自己的自定义应用程序

5. 在“Google IDP 信息”对话框中，在选项 2 下下载 IDP 元数据文件。
6. 在自定义应用程序的“基本信息”中，应用程序名称可以是“NetScaler Intelligent Traffic Management”
7. 在门户中填写来自 SSO 配置的以下信息：
   - ACS URL：来自 SSO 配置信息
   - 实体 ID：来自 SSO 配置信息
   - 起始 URL：来自 SSO 配置信息（可选）
   - 姓名 ID 格式：电子邮件
8. 将“属性映射”对话框留空，单击完成以创建 SAML 应用程序
9. 在应用程序列表中，单击门户项目右侧的垂直圆点，然后选择为所有人开启

在门户中：

1. 在“SSO 配置”页面上，上载 IDP 元数据文件；单击选择文件 按钮打开文件资源管理器，然后选择从 G Suite 下载的 IDP 元数据文件。
2. 如果元数据文件验证正确，则会出现一个绿色对号。
3. 单击启用为帐户中的所有用户启用 SSO。

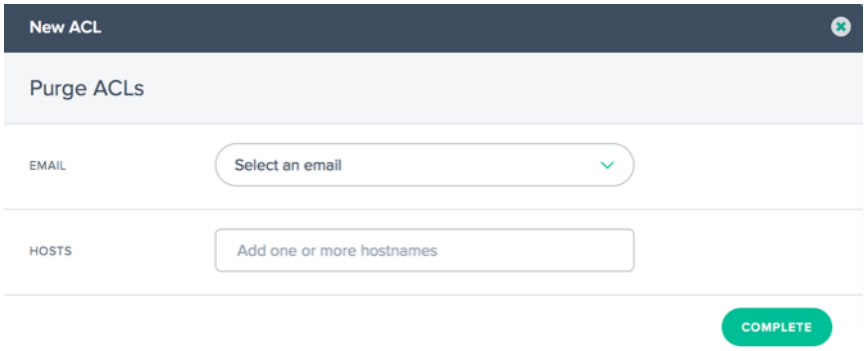
用户现在可以从 SSO 登录页面或 **G Suite** 中的应用程序菜单登录到 NetScaler Intelligent Traffic Management 门户。

有关 Google G Suite 单点登录的更多信息，请参阅 Google 帮助。

设置 **Purge ACL**

在清除 **ACL** 菜单中，用户执行 Fusion Purge 功能的能力可能会受到限制。默认情况下，用户可以在 **Fusion Purge** 设置中配置的任何主机上运行清除。Purge ACL 用来限制用户只允许在指定的主机上进行清除。

单击右上角的 **+** 按钮，为用户添加新的限制。此时将显示以下对话框：



字段	说明
电子邮件	为要配置有限清除访问权限的用户选择电子邮件。
主机	输入用户要运行清除的主机名。用户将无法清除任何未包含在用户的列表中的主机名。

发票

发票菜单选项提供您已使用的 NetScaler Intelligent Traffic Management 服务的所有发票。如果发票有任何问题，请联系您的销售代表或联系支持团队。

API

管理 **OAuth**

API 菜单选项提供有关您可能要使用的经过身份验证的 OAuth API 令牌的详细信息。如果您想使用此功能，请联系您的客户经理。

REST API 速率限制

REST API 可用于访问存储在平台中的数据和设置。但是，我们通过对请求设置速率限制来限制（访问这些数据）的次数，也就是说，我们限制了客户在给定时间段内可以进行的 API 调用次数。这样做是为了平衡系统的负载。

速率限制属性　速率限制具有以下属性：

- 时间范围（以分钟为单位）
- 允许的请求数
- 并发请求

客户可以针对其特定用例申请提高速率限制。

默认速率限制　下表列出了不同类型的 API 调用，以及应用于每种调用的默认速率限制。

API 类型	默认速率限制
报告端点	**GET**

API 类型	默认速率限制
/v2/reporting/radar.json /v2/reporting/plt.json /v2/reporting/openmix.json /v2/reporting/sonar.json	每 15 分钟 15 个请求。3 个并发请求
更新应用程序	**PUT、POST**
/v2/config/applications/dns.json	每分钟 10 个请求。3 个并发请求
Fusion Purge	**GET**
/v2/actions/fusion/purge.json	每分钟 150 个请求
Fusion Purge	**POST**
/v2/actions/fusion/purge.json	每分钟 1 个请求。3 个并发请求