Google

Google Workspace
大型部署的网络最佳实践

管理员指南

Google Workspace

Google 公司
1600 Amphitheatre
Parkway 山景城, CA 94043

www.google.com

部件编号:NETBP_GAPPS_3.8

2020 年 12 月

目录

第 1 章:简介 4
关于本指南 4
目标受众 4
好处 4
努力程度 4
充分利用本指南 5
Google Workspace 实施的生命周期 5
第三方产品配置免责声明 5

第 2 章:网络行动清单 7
关于此清单 7
网络评估 7
网络配置 7
网络路由 8
代理服务器 8
其他服务 8
客户端配置 9
客户端访问 9
验证 9
迁移 9
网络监控 10
带宽测量 10

第 3 章:网络评估 11
概括 11
测试您的网络环境 11
网络位置清单 11
网络测试 12
DNS解析测试 12
ICMP 连通性测试 12
TCP/UDP 可靠性测试 十三
可用 WAN 带宽评估 十三
网络测试工具 十三
代理服务器评估和大小调整 十三
每个用户的基准代理负载 14
估计所需的代理资源 14
例子 15
Windows 10 上的 Chrome 15
Windows 10 上的 Firefox 15

第四章:网络配置 17
概括 17
Google Workspace 流量路由最佳实践 17
网络寻址和协议 17
Google IPv4 地址 17

Google 主机名 19
Google 全局缓存 19
Google 协议 20
Google Meet 20
网络路由 21
广域网优化 21
流量优先级 21
网络层（第 3 层)优先级对等网络路由工具代理 22
服务器代 22
理服务器配置通过代理过滤 22
Google 23
Workspace 流量代理 PAC 文件配 23
置 FindProxyForURL。 23
24
二十五
代理 PAC 文件测试 SSL 检查 阻 二十五
止访问 Google 消费者 二十五
服务 监控 URI 过滤 代理配置工具 限制访问的国家或地区 其他网络服务 二十六
二十七
二十七
二十七
二十七
DNS 解析 二十八
防火墙配置 二十九
出站防火墙规则 三十
入站防火墙规则 三十
邮件路由 三十
出站邮件连接 三十
第 5 章:客户端配置 31
概括 31
客户端访问 31
移动的 31
验证 三十二
单点登录 三十二
单点登录流程 三十二
身份验证工具 33
迁移 三十四
第六章:网络监控 三十五
概括 三十五
监控工具 三十五
网络数据包捕获 三十六

第 1 章:简介

关于本指南

本文档讨论了针对 Google Workspace 优化大型 IP 网络的最佳做法。

本指南中的建议和信息是我们与公共和私营部门的各种客户以及许多网络环境中的合作伙伴合作收集的。我们感谢我们的客户和合作伙伴分享他们的见解和经验。

目标受众

本文档适用于拥有复杂网络的 Google Workspace 客户,尤其是那些分布在广阔地理区域内的网络。拥有较小网络或位于单一位置的网络的管理员可能会发现其中一些信息很有用,并可能找到特定问题的答案,但一些主要的网络路由、容量和测试问题可能不适用。

好处

优化您的网络配置将帮助您通过以下方式改进您的 Google Workspace 实施。

- 通过减少网络延迟来提高 Google Workspace 的响应能力。
- 通过优化网络路由和网络服务来减少带宽消耗。
- 通过收集以下基准指标来预测网络性能和容量需求:
  延迟、数据包丢失和网络可用性。
- 使用 Google Workspace 减少大型文件(例如内部视频和附件)的上传和下载时间。
- 有效地将数据从现有的旧版服务器迁移到 Google Workspace。

努力程度

实施本指南中的建议所需的工作量取决于您的要求、您当前的基础设施以及您的网络团队的技能。本文档中的设计原则和实施最佳实践并非特定于行业或技术。本文档中的原则不需要行业标准网络架构和网络工程技能之外的特定技术专业知识。

充分利用本指南

本指南包括测试和规划方法、有关 Google Workspace 对 IP 网络的影响的常见问题的解答，以及有关将您的网络与 Google Workspace 集成的最佳做法的实地研究结果。

本指南旨在供以下使用：

- 作为网络最佳实践和推荐网络工具的参考指南。下一章中的清单提供了每个网络主题的参考，并提供了更多信息的链接。

- 深入讨论 Google Workspace 服务的各种网络最佳实践和相关主题。您可以完整阅读本文档，以详细了解与网络和 Google Workspace 相关的所有主题。

- 作为回答有关网络最佳特定主题问题的参考指南
  实践。

Google Workspace 的生命周期执行

本指南中提供的信息与您的多个里程碑相关
Google Workspace 部署：

1.网络评估：本部分包含有关评估您当前
在部署 Google Workspace 之前，请先检查网络。虽然这些信息在您部署 Google Workspace 后可能会有所帮助，但如果您在执行任何其他步骤之前运行这些评估和测试，您将看到最佳结果。

2.网络配置：本部分包含有关如何设置网络以最好地与 Google Workspace 配合使用的说明和信息。本部分包括网络路由信息、IP 地址、协议和端口号、代理服务器配置、DNS 配置、防火墙设置和邮件服务器设置。

3.客户端配置：本部分提供有关为用户设置环境的建议。其中包括客户端信息、移动网络期望和迁移。

4.网络监控：本节包括有关网络维护的说明，以及完成部署后出现问题时的故障排除。

第三方产品配置免责声明

本指南介绍了 Google Workspace 产品如何与常见服务器配合使用以及 Google 推荐的配置。这些说明旨在适用于最常见的情况。对配置的任何更改都应在

由您的管理员自行决定。

Google 不提供配置第三方产品的技术支持。如果出现第三方问题，您应咨询网络管理员。Google 对第三方产品不承担任何责任。您也可以联系 Google 解决方案提供商获取咨询服务。提供第三方网站链接是为了方便您使用。链接及其内容可能会更改，恕不另行通知。请查阅相应产品的网站以获取最新的配置和支持信息。

第 2 章:网络行动清单

关于此清单

本节包含本指南中所有行动项目的摘要清单。如果您没有时间从头到尾查看本指南,我们建议您先查看此网络行动清单。

本指南后面将详细描述每个主题。

网络评估

评估当前网络并规划容量需求。为了在测试期间获得最佳结果,请使用以下方法:

- 对所有网络位置进行盘点,包括位置名称、互联网接入类型（例如 T1、VPN、DSL)和可用的互联网带宽。
- 测试从所有网络位置到 Google Workspace 的 DNS 解析,以确保
  您网络中的客户端可以解析 Google Workspace 主机名 - 并且尽可能靠近用户。
- 测试从所有位置到 Google Workspace 的 TCP/UDP 可靠性,以确保您网络中的客户端能够可靠地建立并维持与 Google Workspace 的连接。
- 评估 Internet 出口位置和网络位置之间的 WAN 带宽
  使用该出口点。
- 确定限制访问 Google 服务（包括 SSL 检查)的任何要求以及如何实施这些政策。
- 如果您希望用户通过代理服务器连接到 Google Workspace,
  创建一个测试环境并测量每个用户预期的连接数,这样您就可以计算出代理服务器上预期的出站连接数。

有关评估网络的更多信息,请参阅本指南后面章节中的测试网络环境和代理服务器评估和调整大小。

网络配置

以下建议介绍了有助于为用户提供最佳 Google Workspace 体验的网络配置。这些建议可提高网络可用性和性能,并可通过简化连接 Google Workspace 所需的网络设备来降低成本。

网络路由

为了使 Google Workspace 的网络连接达到最佳性能,请执行以下操作:

通过尽快将流量传出到互联网来使用 Google 网络。将网络流量路由到尽可能靠近最终用户的互联网（无论是地理位置还是拓扑结构）。

重点解决延迟问题,而不是带宽要求。超过最低水平后,带宽考虑对 Google Workspace 来说通常不那么重要。

将防火墙打开至 Google Workspace 服务所需的端口。有关详情,请参阅Google 协议。

避免使用特定 IP 地址来允许访问 Google Workspace。请参阅Google IP 地址。

如果您使用的是中心辐射型网络拓扑 - 或者您的网络有多个位置,并且单个网络出口点横跨多个大洲 - Google 建议您确定潜在的区域出口点。

有关网络路由的更多信息,请参阅本文档后面的网络寻址和协议以及网络路由。

代理服务器

避免通过检查 HTTP 流量内容的代理基础架构路由 Google Workspace 数据。这会降低性能并且效率很低。

虽然不建议这样做,但如果您使用支持 SSL 终止的代理服务器,请设置代理服务器以在中继安全连接时检查 Google Workspace 内容。

必要时,请将代理服务器放置在靠近用户及其互联网出口点的位置（无论是地理位置还是网络拓扑）。

如果您需要通过 URI 过滤 Web 流量,请考虑在客户端桌面上使用 PAC 配置文件,因为代理看不到加密 HTTP 流量中的 URI。

有关设置代理服务器的更多信息,请参阅本指南后面的代理服务器。

其他服务

尽可能使用地理位置和网络拓扑都靠近用户的 DNS 解析器。使用位于远程网络位置的 DNS 解析器会大大降低与 Google Workspace 的连接速度。

如果无法使用用户本地的 DNS 解析器,请使用支持edns-client-subnet的 DNS 服务器扩展 例如 Google 的 DNS 服务器或 OpenDNS 允许解析器传递部分客户端 IP 地址。

遵守所有 DNS 记录类型的公布的 TTL 值。

设置防火墙规则以允许不受限制的出站 HTTPS 流量流向 Google Workspace。
您无需为入站流量设置特殊规则;Google Workspace 不会

除非特别说明,否则向用户发起入站流量。

如果可能,请避免通过网络内的网关路由入站和出站邮件。如果将入站和出站邮件路由到网络内的网关,邮件流量将消耗不必要的网络资源。

有关网络服务的更多信息,请参阅下面的其他网络服务。

客户端配置

配置网络后,请准备用户环境以使用 Google Workspace。这可能包括设置客户端、SSO 身份验证以及准备数据迁移。

客户端访问

在为连接到 Google Workspace 的客户端进行规划时,请考虑以下事项:

为了提供最佳的用户体验,Google 强烈建议使用 Google Chrome 作为 Google Workspace 服务的默认浏览器。

其他受支持的浏览器包括 Mozilla Firefox、Microsoft Internet Explorer、Microsoft Edge 和 Apple Safari。但是,这些浏览器不支持某些 Google Workspace 功能。有关浏览器支持的更多信息,请点击此处。

有关设置客户端环境的详细信息,请参阅客户端访问。

验证

如果您计划设置单点登录 (SSO) 身份验证,请考虑以下事项:

在分布式网络位置而不是中心位置设置 SSO 服务器。

与 VPN 服务器一起实施 SSO 服务器(如果需要),以避免将 VPN 连接用户的身份验证流量路由到其他位置。

设置内部 DNS 服务器以将 SSO 流量重定向到最近的 SSO 服务器,并确保备用 SSO 服务器提供冗余服务。

有关 SSO 身份验证的更多信息,请参阅身份验证。

迁移

Google Workspace 部署通常涉及迁移流量,要么来自本地客户端(例如Google Workspace Migration for Microsoft Outlook),要么来自服务器端客户端(例如Google Workspace Migration for IBM Notes和Google Workspace Migration for Microsoft Exchange)。

将旧数据迁移到 Google Workspace 通常是一项资源密集型活动。如果您计划迁移用户数据,请考虑以下事项:

在大规模迁移的情况下,强烈建议选择服务器端方法。

确保您的迁移服务器与您的旧数据服务器位于同一位置,或者服务器之间的连接具有低延迟和高带宽。

避免通过代理服务器将流量从迁移服务器路由到 Google。

在迁移之前评估您的网络容量,以确定您可以同时迁移的最大数据量。据此调整您的迁移计划。

在迁移过程中,与 Google 服务器建立的某些连接可能会保持打开状态很长时间,具体取决于迁移工具。为了避免可能的中断,并减少重新迁移数据的需要,重要的是保持这些会话打开,并且不要过早关闭任何在线网络基础设施。

有关数据迁移的更多信息,请参阅下面的迁移。

网络监控

使用监控工具来维护和管理已经与 Google Workspace 配合使用的现有 IP 网络。

有多种网络监控工具非常适合监控 Google Workspace 流量。如需查看推荐的网络监控工具列表,请参阅本指南后面的监控工具部分。

网络数据包捕获可帮助您在故障排除期间或与网络提供商/Google 支持人员合作时识别可能的性能问题。有关更多信息,请参阅网络数据包捕获。

带宽测量

客户环境和不同使用模式之间的带宽需求差异很大;没有任何一种测量方法可以适合所有使用 Google Workspace 的客户配置。

一些建议的做法包括:

设计并执行计划来监控任何 Google Workspace 部署早期阶段的带宽使用情况。

部署 Google Workspace 时,监控多个位置各种用户类型的带宽使用情况,以确保数据多样性。

第 3 章:网络评估

概括

在规划实施时,如果您首先了解当前的网络容量和 Google Workspace 的预期网络负载量,您将获得更好的结果。预测负载的最佳方法是对网络中的带宽使用情况进行基准测试,并创建测试环境来模拟普通用户需要多少容量。

本节讨论测试网络环境的方法。

如果您已经部署了 Google Workspace,但尚未运行环境测试和基准测试,那么这样做可能仍然很有价值。这可以为未来的规划和容量需求提供基准,并有助于在潜在问题影响用户体验之前发现它们。

测试您的网络环境

实施 Google Workspace 之前的网络测试主要侧重于评估容量和识别网络瓶颈、互联网代理、防火墙以及涉及路由或监控基于互联网的流量的任何其他网络组件。

以下是部署之前评估和测试网络的推荐步骤。

- 对所有网络位置进行盘点,包括位置名称、互联网接入类型（例如,T1、VPN、DSL)和可用的互联网带宽。
- 测试从所有网络位置到 Google Workspace 的 DNS 解析,以确保网络中的客户端可以解析 Google Workspace 主机名。
- 测试从所有网络位置到 Google Workspace 的 ICMP 连接,以确保您网络中的客户端可以访问 Google 服务器。
- 测试从所有位置到 Google Workspace 的 TCP/UDP 可靠性,以确保客户端在您的网络中可以可靠地建立并维持连接。
- 评估互联网出口位置和网络之间的 WAN 带宽使用该出口点的位置。

网络位置清单

在规划 Google Workspace 实施时,创建一份清单,列出用户将访问 Google Workspace 的所有位置非常重要。此清单的目的是收集有关每个网络位置的互联网连接和容量的信息。

进行清点时,请包括有关每个网络位置的以下信息:

- 位置的名称及其互联网访问描述。例如:“总部,
  “DS3。”
- 互联网带宽平均使用率和峰值使用率。例如:“平均使用率为 50%,峰值为 70%
  用法。”
- 代理服务器的数量以及当前平均和峰值使用量。
- 防火墙设备的数量以及当前平均和峰值使用情况。
- DNS 服务器的数量以及当前平均和峰值使用量。

收集到每个网络位置的信息后,请使用这些数据来评估当前容量以及是否需要升级。

网络测试

使用您在网络清点过程中收集的信息来测试每个网络路由、DNS 服务器和代理服务器。对每个位置的所有相关网络连接运行以下测试。

注意:本节描述的第三方测试软件适用于各种
操作系统,包括 Linux、Unix、Mac OS X 和 Windows。

DNS解析测试

通过测试从所有网络位置到 Google Workspace 主机名的 DNS 解析,确保您网络中的客户端可以解析 Google Workspace 主机名和 URI,如下所示:

1.打开 GitHub 上托管的示例列表文本文件。 (请注意,这只是一个示例,而不是
完整列表。

2. 将示例 .txt 文件保存在您将使用测试命令的目录中:

   a. 单击查看原始文件。

   b. 右键单击该页面,然后单击“另存为”。

3. 运行以下命令测试DNS解析:

   %挖掘+所有+跟踪-f GoogleAppsDomains.txt

ICMP 连通性测试

通过测试从所有网络位置到 Google Workspace 的 ICMP 连接,确保您网络中的客户端可以访问主机名mail.google.com 。测试您的用户是否可以访问 Google Workspace,尤其是从所有用户的 VLAN 访问。

```
% ping -s 512 -c 400 -n mail.google.com
```

如果您在 ping 请求中看到连接速度缓慢或失败,这可能表示连接丢失。调查连接的每个步骤以确定问题的根源。

TCP/UDP 可靠性测试

确保您网络中的客户端能够可靠地建立并维持与 Google Workspace 服务器的连接。使用Hping工具测试一段时间内的链接可靠性。
运行以下命令：

```
%时间 hping3 -S mail.google.com -p 443 --fast -c 1000
```

对上面提到的GoogleAppsDomains.txt文件中列出的每个域运行此测试。

注意： TCP/UDP 可靠性测试具有侵入性，可能会影响网络性能。请在非工作时间运行这些测试以收集数据，同时尽量减少对网络的影响。

可用 WAN 带宽评估

使用iperf工具评估从每个位置到其网络出口点的可用带宽量。此测试在客户端和网络出口点上运行。

此测试旨在评估您的 WAN 网络内的带宽。它不适合测试您的网络与 Google Workspace 服务器之间的带宽。

在通过 WAN 网络连接的每个远程位置上运行以下命令：

```
% iperf -c 客户端 IP 地址 -d
```

在网络出口位置，运行以下命令：

```
%iperf-s
```

注意： WAN 带宽测试具有侵入性，可能会影响网络性能。请在非工作时间运行这些测试以收集数据，同时尽量减少对网络的影响。如果您需要在工作时间运行这些测试，请注意此测试可能对您的网络性能产生的影响。

网络测试工具

您可以从以下在线资源获取上面讨论的工具：

- 从hping.org下载Hping数据包分析工具。
- 从SourceForge 下载iperf带宽性能测量工具。

代理服务器评估和大小调整

在云计算环境中，对外部主机的出站请求通常比传统环境中产生的请求更多。出站请求的增加可能会影响网络所需的代理服务器数量。

如果您打算让用户通过代理服务器连接到 Google Workspace，您可以事先运行这些测试来确定代理服务器的负载水平。使用此信息来估计您是否需要增加代理服务器的容量。

Google 服务主要利用浏览器会话中的异步调用。因此，请尽量避免为用户会话实施连接限制参数。

请按照以下步骤评估您的代理服务器需求：

1. 为您计划在用户环境中使用的每个平台和浏览器创建一个测试环境。

2. 对于每个浏览器，测量测试期间发生的连接数，
   包括最小和最大并发连接，包括空闲使用和活动使用
   使用。

3. 根据此信息和您预计的系统用户数量，计算代理服务器的预期连接数。

4. 使用这些计算来规划所需的任何代理服务器容量变化。有关这些步骤的更多信息，请参阅下文。

每个用户的基准代理负载

要对典型用户使用的代理资源量进行基准测试，请建立一个测试环境，您可以在其中测试您支持的各种平台和浏览器。您的测试环境应包括网络上可以使用您计划为用户使用的相同路由连接到 Google Workspace 的机器。测试环境准备就绪后，将流量引导至测试代理，您可以在其中测量连接数。

使用您网域中可用的 Google Workspace 服务时，为每个环境收集以下数据。例如，打开 Gmail、Google Hangouts、Google Docs 和 Google 日历。

- 平均连接数/秒
- 峰值连接数/秒
- 非峰值连接数/秒

此外，与许多在云端运行的网页应用一样，Google Workspace 会保持多个与远程服务器的连接，以轮询新数据。要评估这些开放连接造成的负载，请在测试环境中测量以下内容。

- 空闲用户与浏览器平台的最小连接数
- 空闲用户与浏览器平台的最大连接数

收集到这些数字后，您可以汇编这些信息来估算您在特定环境下可能遇到的负载。

估计所需的代理资源

要估算 Google Workspace 推出期间预期的负载量，请将每个测试环境的连接数乘以该环境预期的用户数。

使用以下计算。

预计平均负载 = 总和（每个测试机器环境的平均负载 X 预计使用该环境的用户数量）

预计峰值负载 = 总和（每个测试机器环境的峰值负载 X 预计使用该环境的用户数量）

预计空闲负载 = 总和（每个测试机器环境的空闲负载 X 预计使用该环境的用户数量）

如果预估平均负载加上代理处理的任何额外流量超出了您当前的容量，请制定计划来扩展代理服务器容量，或更改代理服务器实施，以使代理服务器不再处理用户向 Google Workspace 发出的请求。

例子

在以下示例中，一家大型企业计划部署以下内容：

- 5,000 名用户在 Windows 10 上运行 Chrome。
- 3,000 名用户在 Windows 10 上运行 Firefox。

注意：Google 建议所有用户都运行 Google Chrome，以便使用 Google Workspace 获得最佳性能。

在基准测试期间，测试显示通过代理服务器的并发连接数如下。（注意：这些仅供参考。您的环境会有所不同。）

- Windows 10 上的 Chrome

  输入 URI 时的连接数：1
  初始加载时的连接数：3
  登录时的连接数：6
  空闲几分钟后的连接数：4
  打开日历和文档时的连接数：4
  加载文档时的连接数：6

  平均负载：3.6 个连接 峰值负载：6 个连接 空闲负载：3.1 个连接

- Windows 10 上的 Firefox

  输入 URI 时的连接数：1
  初始加载时的连接数：4
  登录期间的连接数：9 几分钟空闲后的连接数：3

  打开日历和文档时的连接数：11
  加载文档时的连接数：17

  平均负载：4.1 个连接 峰值负载：17 个连接 空闲负载：3.8 个连接

基于此,预期负载为:

- 平均: (5000 x 3.6) + (3000 x 4.1)= 30,300 个连接。
- 峰值: (5000 x 6) + (3000 x 17)= 81,000 个连接。
- 空闲: (5000 x 3.1) + (3000 x 3.8)= 26,900 个连接。

根据此估计,代理环境需要能够支持至少 30,000 个连接,可能还需要更多,以避免高峰时段出现问题,或者在预计会出现增长的情况下。
如果当前代理服务器环境以 50% 的容量运行,拥有 20,000 个连接,则表明需要部署更多的代理服务器,或者路由 Google Workspace 流量以绕过代理服务器。

第四章:网络配置

概括

本部分详细介绍了如何针对 Google Workspace 优化您的网络。其中包括 Google 的 IP 地址、所用协议、路由建议、代理服务器配置选项和 DNS 配置信息。在配置网络时,请将此信息用作指南,并作为 Google Workspace 客户端将向 Google 服务器发出哪些类型的请求的参考。

Google Workspace 流量路由最佳实践

如果需要,将 Google Workspace 流量列入流量重定向和优先级许可名单的推荐且更强大的方法是将 IP 范围与通配符主机名结合使用。

不建议仅使用 IP 范围或仅使用通配符的主机名。有关更多详细信息,请参阅以下部分。

网络寻址和协议

Google IPv4 地址

Google Workspace 服务可以通过 IPv4 和 IPv6 访问 - 我们将在以下示例中使用 IPv4,但相同的方法也可以应用于 IPv6。

Google Workspace 存在于包含 Google Workspace 和消费者服务的多租户服务器环境中。因此,Google Workspace 与 Google 的消费者服务共享相同的 IP 地址空间。这也意味着不同的服务可以从同一 IP 范围运行。例如,Google Docs 服务器可以使用与 Google Photos 相同的 IP 地址空间 - 并为企业用户和消费者用户提供服务。此外,Google 主机名的特定 IP 地址（例如mail.google.com或drive.google.com)可能同时为 Google Workspace 和消费者用户提供服务。这为所有服务的所有用户提供了无与伦比的可靠性。

由于 Google Workspace 使用与其他 Google 产品（包括消费产品)相同的 IP 地址空间,因此并不总是能够使用 IP 地址区分流向不同服务的流量。

对于任何 Google 主机名（例如mail.google.com或docs.google.com）， IP 地址都不是静态的,并且仅对主机名的 DNS 查找中返回的生存时间 (TTL) 值有效。

例如,如果我们查询mail.google.com 的 A 记录,则会返回多个结果（请注意,输出不具有权威性）：

```
% 挖掘 mail.google.com +ttl

;; 答案部分：

mail.google.com。          60      在      CNAME googlemail.l.google.com。
googlemail.l.google.com。  60      在      216.58.198.229
```

结果集中的第二列是记录的 TTL（以秒为单位）。基于这些
样本结果显示，我们可以确定这些IP地址的有效期仅有一分钟。

特定主机名的 Google IP 地址不是静态的。例如，不要假设
mail.google.com 将始终为 216.58.198.229 - 或您在测试中收到的任何其他结果。如果
您需要配置您的环境以接受来自 Google 的邮件网关的邮件，
包括此帮助中心中“_spf.google.com”记录中的所有子网文章。

不建议使用 Google 的 IP 地址空间来允许访问 Google（请参阅
Google 全局缓存如下）；然而，IP 地址可用于实现流量
重定向和优先到互联网，了解谷歌全球的影响
缓存（本文档中提到的建议）。
实现这些优先级的更强大的选项可以是 Google 的主机名（请参阅
Google 主机名（下文中)与 Google 的 IP 空间结合使用。

您可以按照此帮助中心文章获取 Google IP 范围。

我们强烈建议客户监控更新并实施跟踪脚本
（请参阅下面的监控工具部分）。

Google 主机名

Google 拥有并运营着大量域名,用于服务我们的应用。要高效地服务和运营如此庞大的全球业务,需要先进的网络工程和优化。我们不建议使用 Google 的主机名作为允许访问的手段。

相反,应该使用主机名来实现互联网流量重定向或优先级排序;这是本文档中提出的建议。

但是,您可以在此帮助中心文章中找到 Google Workspace 主机名列表。

注意:帮助中心文章中包含的信息如有更改,恕不另行通知。
注意

Google 全局缓存

Google 的许多服务和应用程序都参与了Google 全局缓存 (GGC)内容交付系统。该系统的目标是通过将终端点设在尽可能靠近用户的位置,为所有用户提供最佳服务。

GGC 系统涉及网络运营商和互联网服务提供商,以分发常用的资源（主要是静态内容）。GGC 的参与者在其网络内部署了许多 Google 拥有和运营的服务器,以提供流行的 Google 内容。这导致 IP 地址被用于这些主机运营商拥有的 Google 服务和应用程序。因此,不应使用 Google 的 IP 地址来允许访问。相反,IP 地址可用于实施流量重定向或优先级排序,因为可能有一些与 Google 相关的流量会流向未列出的 IP 地址。

对于距离 Google 较远“网络距离”的用户来说,Google 使用 GGC 进行内容传递最为有效（请参阅 Google 数据中心位置）。 Google 对 GGC 的使用在它适用的服务和客户网络中都是动态的。请参阅peering.google.com上的常见问题解答了解有关 GGC 及其用途的更多信息。

Google 协议

下表列出了常见的 Google Workspace 服务以及每个服务使用的协议。如表所示,Google Workspace 服务始终基于 SSL,但 Google Meet 除外。

应用	协议	港口
邮件、日历、文档、网站	TCP	443
适用于 Microsoft 的 Google Workspace 同步办公室	TCP	443
Google 聊天	TCP	443
Google Meet	UDP UDP TCP TCP	19302 - 19309 19302 - 19309 80 443
Google Workspace 迁移 微软 交换	TCP（API）	443
适用于 Lotus 的 Google Workspace 迁移 笔记	TCP（API）	443

Google Meet

为了让用户能够以最佳方式使用 Google Meet,请参阅管理员帮助中心文章网络连接要求并针对 Google Meet 优化您的网络。

Google Meet 的一些网络注意事项包括：

- 代理流量会增加延迟,并可能导致 Meet 自动降低视频质量和音频质量,因此不建议使用代理服务器来传输 Meet 流量。

- 避免对 Meet 流量使用数据包检查或协议分析器;它们会引入延迟可能会导致 Meet 基础架构自动降低视频会议质量。

- Google 建议不要在您的网络中为 Meet 使用 QoS。Meet 会自动适应网络状况。如果您有充分的理由为 Meet 使用 QoS,请参阅Meet QoS 最佳实践指南。

- 确保网络延迟较低且一致,以便 Meet 流量以最短的客户端和 Google 之间的路径。

- 确保您的网络具有足够的带宽来处理同一地点的所有并发视频会议。请参阅帮助中心文章中介绍了建议的带宽。

- 打开出站端口,允许 UDP 和 TCP 流量进出您的网络。如果您不想允许 UDP 从您网络上的客户端出站,请至少允许 TCP 从您网络上的客户端出站到 Google（请参阅帮助中心文章优化您的Meet 网络详细信息请参见）。强制使用 TCP 连接来提供语音和视频等服务可能会给您的用户体验带来不良影响;因此,我们建议允许在您的网络中使用 UDP。

网络路由

路由到 Google Workspace 时,最简单的网络路由通常可提供最佳性能。减少从用户位置到 Google 数据中心的复杂性和不必要的网络路由。网络设计的主要目标应该是减少从您的网络到 Google 的总往返时间。如果您发现性能问题,请在增加带宽之前解决任何延迟问题,因为这通常会产生更好的效果。

为了实现与 Google Workspace 连接的最佳性能：

- 就地理位置和网络拓扑而言,将流出网络流量到互联网尽可能靠近最终用户。
- 重点解决带宽要求以外的延迟问题。
  最低带宽级别,对于 Google Workspace 来说,带宽考虑通常不太重要。
- 确保全局防火墙对 Google Workspace 服务使用的所有端口开放。
- 如果您使用的是中心辐射型网络拓扑,或者您的网络具有多个位置但只有一个网络出口点,请考虑流量优先级。

广域网优化

在规划网络云策略时,请尝试减少延迟和往返时间。如果 WAN 流量必须穿越大片地理区域才能到达互联网,远程办公室的用户将体验到性能下降。在尽可能靠近用户的地理位置上实施网络出口点,以减少比特成本高昂的链路上的流量。此优化的一部分可以通过 DNS 解析更改来实现。

有关详细信息,请参阅第 26 页的DNS 解析。

流量优先级

您可以通过流量优先级来提高 Google Workspace 的性能。这是通过赋予 Google Workspace 流量优先于其他网络流量来实现的,以减少拥塞期间的延迟。流量优先级可以在数据链路层和网络层上实现;有关详细信息,请参阅以下部分。

如果您具有以下任何环境,您可能希望考虑流量优先级以减少潜在的延迟：

- 中心辐射型网络拓扑。

- 具有单个网络出口点的多个位置。

网络层（第 3 层)优先级

如本文档前面所述,Google Workspace 使用与其他 Google 产品（包括 Gmail 和 Google Photos 等消费产品）相同的 IP 地址集。
无法区分不同产品的流量。

如果您需要网络层优先级,我们建议您执行以下一项或多项操作：

- 创建代理 PAC 文件,将 Google Workspace 流量定向到路由代理
  仅限 Google Workspace 流量。有关详细信息,请参阅第 23 页的代理 PAC 文件配置。

- 配置您的网络设备以优先考虑您的代理网络接口。
- 分发代理以避免创建中心辐射型代理拓扑。

有关 Google IP 地址和 TCP 端口使用情况的信息,请参阅第 17 页的Google IP 地址。

对等互连

对等互连是指您的网络与 Google 网络的直接互连。这可以减少延迟并提高您的网络与 Google 之间的连接的可靠性。

对于大多数 Google Workspace 客户来说,最好的方法是选择已与 Google 对等连接的 ISP 或网络提供商。Google 与全球大多数地区的许多互联网服务提供商都建立了对等连接。这是实现与 Google 对等连接的好处的最简单、最快捷的方法。请联系您的 ISP,了解他们是否已与 Google 建立对等连接。

对于较大的企业网络,可能可以直接与 Google 对等。与 Google 对等有许多要求。一般来说,如果您尚未与其他网络对等,那么让您的上游网络提供商处理对等关系更为合适。

有关适用于 ISP、网络运营商和企业网络的 Google 对等连接要求,请参阅PeeringDB 上的 Google 条目。PeeringDB 还包含 Google 能够进行对等连接的互联网交换中心和其他位置的列表。

如果您或您的互联网服务提供商根据 Google 的对等连接要求具备对等连接资格,请与您的 Google 部署或支持代表讨论对等连接关系。

网络路由工具

- 外部网站测量实验室 (Measurement Lab) 提供各种实用的工具来生成有关您的互联网连接性能的详细数据。您可以使用这些工具来衡量您的整体互联网访问性能。

代理服务器

为 Google Workspace 规划代理基础架构时,请牢记以下最佳做法:

- 避免通过检查内容的代理路由 Google Workspace 数据
  HTTPS 流量,因为这会降低性能。
- 从地理位置和网络拓扑角度来看,将代理服务器放置在靠近用户及其互联网出口点的位置。
- 如果您需要通过 URI 过滤 Web 流量,请考虑在客户端桌面上使用 PAC 配置文件,因为代理看不到加密 HTTP 流量中的 URI。
- 如果您使用支持 SSL 终止的代理服务器,则可以设置代理服务器以在中继安全连接时检查 Google Workspace 内容。

代理服务器配置

我们建议您不要通过代理服务器路由 Google Workspace 流量,除非您有充分的理由这样做。如果您决定通过代理发送 Google Workspace 流量,请查找代理服务器上可能会中断 Google Workspace 流量的设置。

查找包含以下条件的配置和设置:

- 内容过滤器可能会将与 Google 相关的流量标记为禁止
- 可以降低每个客户端每秒可能并发连接总数的设置
- SSL 超时时间过长或过短(建议使用默认设置)
- 固件版本过时
- 无需硬件加速的 SSL 检查

通过代理过滤 Google Workspace 流量

从您的用户到 Google Workspace 服务器的流量绝大部分都是 HTTPS 事务。这种类型的流量是首选,因为它安全可靠。虽然可以中断到 Google Workspace 的流量进行过滤,但这会大大降低用户的整体体验。

在支持 TLS 的服务器名称标识符 (SNI) 扩展的浏览器和协议中,您将在代理日志中看到客户端在初始 HELLO 中对主机名的请求。这些浏览器的列表可在Wikipedia 的以下页面中找到。查阅浏览器文档来了解有关 SNI 支持的信息。

在客户端/服务器之间发出初始 HELLO 请求之后以及建立 TLS 连接之后,所有流量都将被加密,包括主机名后的 URI 路径。

如果您需要过滤用户的流量,有两种推荐的方法来实现:

- 在加密之前使用代理 PAC 文件在浏览器级别过滤用户流量更容易且实施成本更低。请参阅下面的代理 PAC 文件配置。
- 加密后执行 SSL 拦截和检查更安全,但实施起来更困难且成本更高。请参阅第 24 页的SSL 检查。

代理 PAC 文件配置

代理 PAC 文件是一种经济高效的流量过滤方法,因为 URI 和 IP 评估是在加密之前在客户端计算机上执行的。

代理 PAC 文件是一组 JavaScript 命令,浏览器使用这些命令来评估从用户收到的 URI 请求。

以下示例脚本包含要测试的代码

· 如果 URI 是普通主机名 · 如果
URI 与 Google Workspace 通配符主机名之一匹配。
请注意,建议使用两个不同的规则来捕获顶级域名和潜在子域名的流量(例如https://*.google.com/* 和 https://google.com/*)· 如果 IP 是私有地址 · 如果 IP 在 Google Netblocks 中

在所有上述情况下,请求都会遵循“DIRECT”路由,否则将通过默认代理服务器进行路由。

注意:此 PAC 文件仅供参考。网络管理员应根据本文档提供的建议检查 IP 地址和 URL 列表,并应由企业更新、拥有和维护。

```
函数 FindProxyForURL(url,主机) {

        // 纯主机名。(例如 http://server)
        如果(isPlainHostName(主机)){
                返回“DIRECT”;
        }

        // 私有地址类。
        如果 (isInNet(dnsResolve(host), 10.0.0.0 , 255.0.0.0 ) ||
                isInNet(dnsResolve(主机), 172.16.0.0 , 255.240.0.0 ) ||
                isInNet(dnsResolve(主机), 192.168.0.0 , 255.255.0.0 ) ||
                isInNet(dnsResolve(主机), 127.0.0.0 , 255.255.255.0 )) {
                返回“DIRECT”;
        }

        // Google 网络块 (_netblocks.google.com)

        如果 (isInNet(dnsResolve(主机), 216.239.32.0 , 255.255.224.0 ) ||
                isInNet(dnsResolve(主机), 64.233.160.0 , 255.255.224.0 ) ||
                isInNet(dnsResolve(主机), 66.249.80.0 , 255.255.240.0 ) ||
                isInNet(dnsResolve(主机), 72.14.192.0 , 255.255.192.0 ) ||
                isInNet(dnsResolve(主机), 209.85.128.0 , 255.255.128.0 ) ||
                isInNet(dnsResolve(主机), 66.102.0.0 , 255.255.240.0 ) ||
                isInNet(dnsResolve(主机), 74.125.0.0 , 255.255.0.0 ) ||
                isInNet(dnsResolve(主机), 64.18.0.0 , 255.255.240.0 ) ||
                isInNet(dnsResolve(主机), 207.126.144.0 , 255.255.240.0 ) ||
```

```
        isInNet（dnsResolve（主机），  108.177.8.0  ，  255.255.248.0  ）||
        isInNet（dnsResolve（主机），  216.58.192.0  ，  255.255.224.0  ）||
        isInNet（dnsResolve（主机），  172.217.0.0  ，  255.255.224.0  ）||
        isInNet(dnsResolve(主机),  173.194.0.0  ，  255.255.0.0  )) {
            返回“DIRECT”；
    }

    // 捕获任何失败的通配符 Google 域名。if (shExpMatch(url,  https://*.google.com/*  ) ||

        shExpMatch (url,  https://doubleclick.net/*  ) || shExpMatch (url,  https://
        *.doubleclick.net/*  ) ||
          shExpMatch（url，“https://googleadservice.net/*”）|| shExpMatch（url，“https://
        *.googleadservice.net/*”）|| shExpMatch（url，“https://googledrive.com/*”）||

        shExpMatch（url，“https://gmail.com/*”）|| shExpMatch（url，“https://
        ssl.google-analytics.com/*”）|| shExpMatch（url，“https://*.googlegroups.com/*”）|| shExpMatch（url，
          “https://googlegroups.com/*”）||

        shExpMatch（url，  https://googleapis.com/*  ）|| shExpMatch（url，  https://
        *.googleusercontent.com/*  ）|| shExpMatch（url，  https://*.gstatic.com/*  ）|| shExpMatch
          （url，  https://*.ggpht.com/*  ）|| shExpMatch（url，  https://*.googleapis.com/
        *  ）|| shExpMatch（url，  https://s.ytimg.com/*  ）){


            返回“DIRECT”；
    }


    // 默认规则回退到代理服务器。返回“PROXY myproxyserver.corp.mycompany.com:3128; PROXY

myproxyserver2.corp.mycompany.com:3128  ;
}
```

isInNet()和shExpMatch()函数用于评估主机,检查它是否位于 Google 公开的 IP 网络地址块之一中,或者是否位于 Google 主机名的通配符列表中。

当浏览器从使函数 FindProxyForURL() 计算结果为 true 的主机请求页面时,配置文件将指示浏览器使用与该主机的直接连接。

如果函数返回 false,它将把所有内容发送到定义的代理,例如“myproxyserver.corp.mycompany.com:3128”。

在外部网站 FindProxyForURL 上可以找到更多开发代理 PAC 文件的示例。

代理 PAC 文件测试

实现功能性代理 PAC 文件需要仔细测试。使用pactester等 PAC 文件测试工具来测试不同的 JavaScript 函数。PAC 文件测试器将允许您传递主机名和 URI,并查看浏览器将在您的 PAC 文件中采用哪条路径。从GitHub pactester 项目站点下载pactester 。

SSL 检查

尽可能避免 SSL 检查。SSL 检查实际上是对您自己的用户进行 SSL“中间人攻击”,以检查 HTTPS 流量的内容。使用 SSL 终止,您的用户会连接到代理作为端点。然后,代理会终止 SSL 连接并检查流量,然后与目标服务器建立新连接

转发流量。这会导致在软件中（而不是网络设备中)执行这些操作的传统代理的负载显著增加。

有许多商业设备供应商以及许多软件代理服务器可以执行 SSL 检查。通常这需要额外的代理配置。

每个代理服务器 SSL 检查设置都不同,但典型步骤如下：

1. 使用内部主机名（例如 mail.example.com)自行签署 SSL 证书。

2.在代理服务器上安装mail.example.com证书。

3. 编写自定义代理规则。例如,将连接从https:// mail.example.com/重写为https://mail.google.com/a/example.com/。

4. 拒绝主机头包含mail.google.com 的连接。

注意 :有些代理允许你保持主机名不变,并使用内置的证书。这要求用户的浏览器信任该证书,否则用户将收到证书错误。有关如何解决这些与 SSL 检查相关的问题的信息,请咨询代理服务器供应商和文档。

阻止访问 Google 消费者服务

作为管理员,您可能希望阻止您网络上的用户使用消费者帐号（而不是您提供的 Google Workspace 帐号)登录 Google 服务。例如,您可能不希望他们使用自己的个人 Gmail 帐号。此外,您可能还希望阻止用户从其他网域登录 Google Workspace 帐号。

请注意,实现此功能需要使用 Web 代理和 SSL 拦截,本文档中明确指出不建议采用这种做法。

阻止访问网络服务的一种常见方法是使用网络代理服务器过滤指向特定 URI 或主机名的流量。这种方法在这种情况下是无效的,因为消费者和 Google Workspace 帐号之间访问的所有 URI 都是相同的。

为了仅允许用户使用您域中的特定 Google 帐户访问 Google 服务,您需要网络代理为指向*google.com 的所有流量添加 HTTP 标头。
标头标识了哪些用户可以访问 Google 服务的网域。由于大多数 Google Workspace 流量都经过加密,因此您的代理服务器还需要支持 SSL 拦截。（请参阅阻止访问消费者帐号在管理帮助中心中查看已知支持 SSL 拦截和 HTTP 标头插入的代理服务器列表。）

为了防止用户使用您明确指定以外的其他 Google 帐户登录 Google 服务,请执行以下操作：

1.通过您的网络代理服务器将所有出站流量路由到google.com 。

2. 在代理服务器上启用 SSL 拦截。

由于您将拦截 SSL 请求,因此您可能希望在使用代理的每台设备上管理客户端证书,以便用户的浏览器不会针对请求发出警告。

3. 对于每个 google.com 请求：

a. 拦截请求。b. 添加 HTTP 标头

X-GoogApps-Allowed-Domains,其值为逗号
带有允许域名的分隔列表。包括您在 Google Workspace 中注册的域名以及您可能已添加的任何辅助域名。

例如,为了允许用户使用以@altostrat.com和tenorstrat.com结尾的帐户登录,请使用您要允许的域名创建
以下标头:

X-GoogApps-Allowed-Domains = altostrat.com,tenorstrat.com

4. 可选地,创建代理策略以防止用户插入自己的标头。

监控 URI 过滤

尽可能避免使用 SSL 检查进行 URI 过滤。如果您正在使用 URI 过滤,请设置策略来监控代理日志中的 URI。查找任何
被错误阻止或允许的 URI。

所访问 URI 的这些变化可能会导致 Google Workspace 加载不完整、加载缓慢或根本无法加载。为避免 URI 过滤问题,如果您要过滤代理服务器,
请设置一项政策以持续监控代理负载,并准备好在必要时调整规则。

为了帮助发现这些新 URI 可能是什么,请在测试环境中测试新的 Google Workspace 功能或服务,然后再允许它们在生产环
境中使用。为此,您可以安装HttpWatch之类的工具或HttpFox。

代理配置工具

下载以下可能对配置代理服务器有帮助的工具:

- 使用pactester或类似工具验证不同 URI 的 PAC 文件。从Github 项目网站下载 pactester。

- 下载HttpWatch或HttpFox （Firefox 扩展)以帮助您查看正在被
浏览器在加密之前请求。

限制访问的国家或地区

谷歌限制某些国家或地区访问其部分业务服务。
某些 Google 服务可能在这些国家或地区可供个人使用,但不适用于商业或教育用途。请参阅帮助中心查看国家或地区的
列表。

其他网络服务

Google 运行着复杂的负载平衡系统,以确保为用户提供最佳体验。
Google 负载平衡系统的一个因素是 Google 响应 DNS 服务请求的方式。Google 尝试通过 DNS 解析器的 IP 地址位置部分确定用户的地理
位置。

为了确保您的用户获得最佳体验：

- 使用地理位置和网络拓扑都靠近用户的 DNS 解析器。使用位于远程网络位置的 DNS 解析器将大大降低与 Google Workspace 的连接速度。

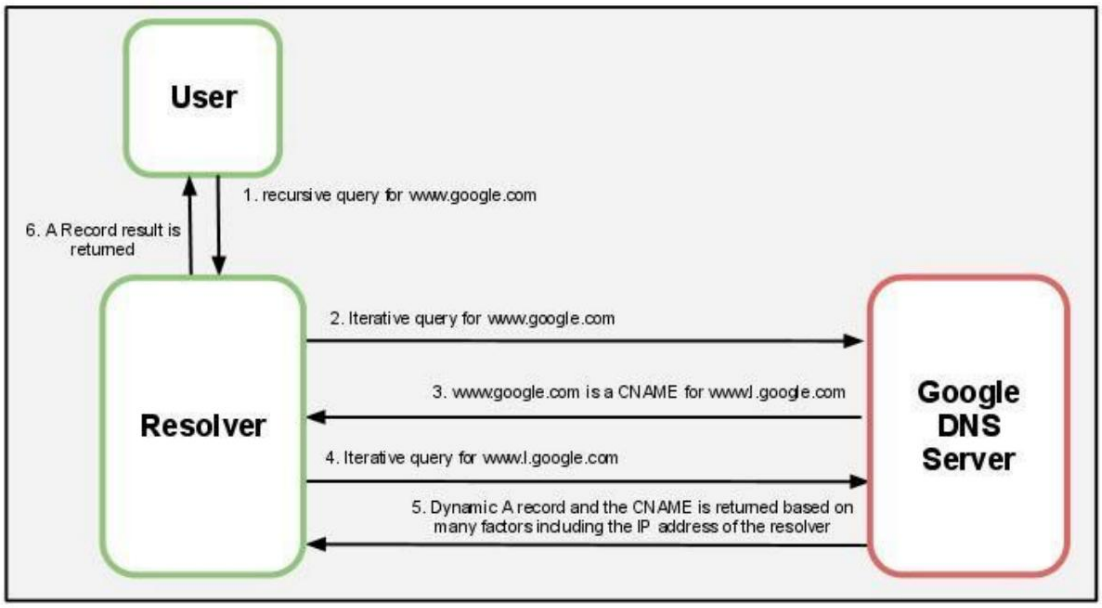
- 如果无法使用靠近用户的 DNS 解析器，请使用支持 edns-client-subnet 扩展的 DNS 服务器（草案提案2671） 例如Google 的 DNS 服务器或OpenDNS允许解析器传递部分客户端的 IP 地址。

- 遵守所有 DNS 记录类型的公布的 TTL 值。
- 设置防火墙规则以允许不受限制的出站 HTTPS 流量流向 Google Workspace。
  您不需要为入站流量设置特殊规则；Google Workspace 通常不会向用户发起入站流量。

- 避免通过网络内的网关路由入站和出站邮件。如果将入站和出站邮件路由到网络内的网关，则会消耗不必要的网络资源。

DNS 解析

下图显示了企业网络上 Google Workspace 用户的典型 DNS 解析。



Google 会动态提供 DNS A 记录查询，以确保用户在发出请求时获得最佳体验。为确保正确执行此操作，请配置 DNS 缓存解析器以遵循每个记录指定的 TTL 值。使用超过 DNS 记录上的 TTL 值的缓存结果可能会导致用户体验不佳，因为缓存的 DNS 记录可能会将用户引导至次优 IP 地址。

以下是www.l.google.com 的 TTL 值示例：

```
%dig +ttl www.l.google.com
```

对于此查询，您可能会看到以下结果：

```
; <<>> DiG 9.4.3-P3 <<>> +ttl www.l.google.com ;; 全局选
项:printcmd ;; 得到答案： ;; ->>HEADER<<-
操作码:QUERY，
状态:NOERROR,id:54488 ;; 标志:qr rd ra; 查询:1,答案:6,权威:4,附加:4 ;; 问题
部分： ;www.l.google.com。在 A ;; 答案部分： www.l.google.com。184在 A 209.85.225.104
www.l.google.com。184在
A 209.85.225.99
www.l.google.com。 184
在 209.85.225.103 www.l.google.com。184在 209.85.225.105
www.l.google.com。184在 209.85.225.147 www.l.google.com。
184在 209.85.225.106
```

在此示例中，TTL 值为 184 秒，相当于 3 分钟。请确保您的 DNS 服务器在缓存结果时遵循此值。

使用集中式 DNS 服务器架构会掩盖向 Google DNS 服务器发出请求的用户身份。如果 DNS 查询通过中央服务器路由以解析互联网主机，则用户可能无法连接到最近的 Google Workspace 服务器。在极端情况下，这种架构可能会导致一个大洲的用户连接到另一个大洲的服务器。

理想的解决方案是将本地 DNS 解析器放置在靠近用户的位置，并让远程 DNS 解析器通过用户本地的互联网连接发送所有 DNS 流量。对于仅限内部使用的地址，将请求转发到适当的内部公司 DNS

服务器。

或者，您可以使用支持 edns-client-subnet 扩展的 DNS 服务（草案提案 2671），例如Google 的 DNS 服务器或 OpenDNS。

注意：使用 edns-client-subnet 扩展的客户端和 DNS 服务器需要随请求发送更多数据，从而导致超出传统的 512 字节限制。客户端和权威 DNS 服务器之间实施或配置不当的服务通常会错误地处理请求。有关更多信息（包括有关如何测试基础架构的说明），请参阅DNS-OARC 网站。

防火墙配置

使用 Google Workspace 和其他云应用，用户可以从您的网络外部获取资源。这会导致 HTTP 连接从内部资源转移到外部资源。

由于这一变化，您网络中之前规模适当的出站防火墙可能会变得不堪重负。请注意，这可能会增加出站防火墙的占用空间。

通过对代理服务器负载进行基准测试，可以很好地估计出站防火墙上预期的连接负载。出站防火墙上唯一看不到的连接是代理服务器不允许通过的连接。有关收集和使用这些数据的更多信息，请参阅代理服务器

评估和规模在第13页。

出站防火墙规则

为了确保 Google Workspace 用户获得最佳体验,并为我们的系统提供低延迟连接,我们建议尽可能开放端口 80/443 上的出站防火墙规则以用于 TCP/IP 流量。

入站防火墙规则

Google Workspace 不会从 Google 数据中心发起到您网络的连接。所有流量均由您网络内的客户端发起到 Google。

邮件路由

更改 MX 记录以将邮件流量路由到 Google Workspace 后,您的电子邮件将不再递送到您的服务器。相反,入站电子邮件将定向到 Google Workspace 服务器。这实际上消除了网络上的入站 SMTP 邮件流量。

出站邮件连接

根据您的需要,您可能希望从自己的网络发送一些出站邮件流量,例如来自系统中应用程序的自动或批量通信。您可以使用 Google 的SMTP 中继服务安全地路由和过滤您的出站邮件。确保充分规划并估计预期的 SMTP 中继量将如何影响您的整体网络需求。

第 5 章:客户端配置

概括

了解不同客户端对 Google Workspace 性能的影响非常重要。本部分讨论了可能影响 Google Workspace 性能的用户环境元素、设置用于 Google Workspace 的身份验证的建议,以及将用户数据从现有服务器迁移到 Google Workspace 的建议。

客户端访问

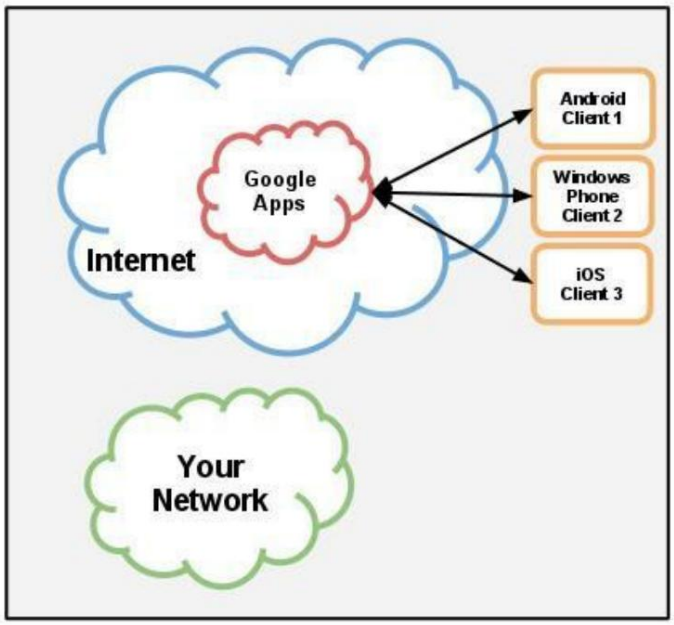
在规划用户用于访问 Google Workspace 的客户端时,请考虑以下事项:

- 为了向用户提供最佳性能 - 并体验所有 Google Workspace 功能 - Google 推荐使用 Google Chrome。
- Google 支持最新版本的 Google Chrome（每当检测到新版本时都会自动更新)以及向后一个主要修订版本。
- 其他支持的浏览器包括 Mozilla Firefox、Microsoft Internet Explorer、Microsoft Edge 和 Apple Safari 的当前版本和之前的主要版本。
  请注意,这些浏览器并不支持所有 Google Workspace 特性和功能。

移动的

Android 设备（使用 Google Sync 协议)以及 Windows Phone 和 Apple iOS 设备（使用 ActiveSync 协议)可直接与 Google 服务器通信,而无需使用您的网络资源。

请参阅下图以了解详情。



使用 Google Workspace 时,这些设备不会访问您的网络。借助 ActiveSync 或 Google Sync,Google Workspace 会将此邮件直接递送到用户的设备。

验证

用户可以通过两种方式向 Google Workspace 服务进行身份验证:

- 单点登录服务
- Google 身份验证

大型企业组织通常使用单点登录系统来授权用户。小型组织也可以选择基于云的单点登录系统。

单点登录

Google Workspace 支持对所有 Google Workspace 服务进行基于 SAML 2.0 的身份验证。客户端应用（例如 Google Workspace Sync for Microsoft Outlook)也支持单点登录。

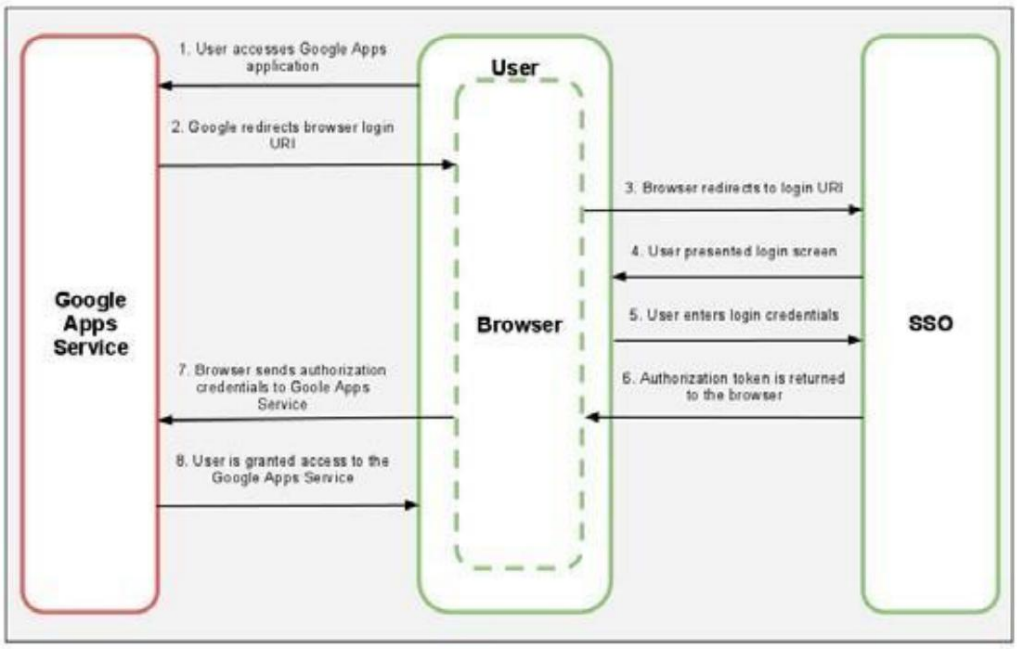
如果您计划设置单点登录身份验证,请考虑以下建议:

- 在分布式网络位置而不是中心位置设置 SSO 服务器。
- 设置内部 DNS 服务器以将 SSO 流量重定向到最近的 SSO 服务器,并确保备用 SSO 服务器到位以提供冗余服务,以防发生中断导致用户无法访问特定位置的 SSO 服务器。

单点登录流程

当未经身份验证的用户登录 Google Workspace 且配置了 SSO URI 时

对于域,身份验证需要几个步骤。请参阅下表。



这是 SSO 身份验证的过程:

1. 用户请求 Google Workspace 服务。

2. Google Workspace 身份验证系统将用户的浏览器重定向到
   为 SSO 系统配置的 URI。如果 SSO/SAML 服务器不可用,则用户无法向服务进行身份验证。

3. 浏览器重定向到登录 URI。

4. SSO 服务器显示登录屏幕。

5. 用户输入登录凭证并向 SSO 系统进行身份验证。

6. SSO 系统将授权令牌传递给用户的浏览器。

7. 用户浏览器将授权凭证发送给 Google Workspace 服务。

8. 授予用户访问 Google Workspace 服务的权限。

身份验证工具

解决身份验证过程中任何与 SAML 相关的错误的有用工具是 SAML 2.0 调试器,例如SAML 2.0 调试器。

迁移

Google Workspace 部署通常涉及迁移用户数据的流量,无论是通过本地客户端（例如Google Workspace Migration for Microsoft Outlook,或服务器端客户端,例如Google Workspace 迁移至 IBM Notes 或Google Workspace 迁移至 Microsoft Exchange。

如果您在部署 Google Workspace 的过程中迁移用户数据,则可能会产生大量数据负载,具体取决于您选择迁移的数据量。为了限制对网络的影响,我们建议您遵循以下最佳做法：

- 如果不是基于云,请确保您的迁移服务器与您的旧数据服务器位于同一位置,或者至少服务器之间的连接具有低延迟和高带宽。
- 避免通过代理服务器将流量从迁移服务器路由到 Google。
- 在迁移之前评估您的网络容量,以确定最大您可以同时迁移的最大数据量。相应地调整迁移计划。
- 在迁移期间,与 Google 服务器建立的某些连接可以保留长时间打开 - 取决于迁移工具。为了避免任何可能的迁移错误,并减少重新迁移数据的需要,重要的是保持这些会话打开,并且不要因任何代理或防火墙超时而过早关闭它们。
- 考虑将迁移安排在工作时间以外,以减少工作时间内的网络负载。这显然会延长迁移的总持续时间。

第六章:网络监控

概括

在您的网络设置为与 Google Workspace 配合使用并且您的用户已启用后,您可以
可以通过监控网络运行状况来维持用户体验的质量。
为了确保最佳用户体验,请遵循以下监控工具建议和
网络踪迹。

监控工具

有许多商业和开源工具可以监控你的
网络。SLAC 上提供了全面的网络监控工具目录
网络监控工具地点。

具体推荐的工具如下表所列。

监测类型	工具	描述
设备监控	即时消息	监控并绘制各个方面的 网络设备。
DNS 更改	网络块 监视器	监控 Google 的网络阻断和警报 你要改变。
主机监控	吸烟	监控并绘制往返时间 目的地。高度可配置。
镜子 服务器	示例列表	镜子服务器提供只读 网络运营商的路由视图 信息 包括连接、延迟、 以及其他因素 在遥远的点上 另一个网络。
网络	平图机	帮助监控网络延迟、正常运行时间以及 路线改变。
网络	复用	帮助监控网络延迟、正常运行时间以及 路线改变。
数据包捕获	Wireshark	执行数据包捕获。
RTT 延迟	盒子	尝试测量 Web 应用程序的 RTT 使用 HTTP/TCP 延迟。
痕迹	跟踪	与 traceroute 类似但使用 TCP 数据包 而不是 ICMP 数据包

网络数据包捕获

网络数据包捕获可以帮助您发现可能对 Google Workspace 用户的往返时间或总体延迟产生负面影响的问题,例如:

- 不同类型的网络泛洪问题（ARP、TCP、UDP、IP 等）
- 以太网的 MTU 不匹配
- 网络上的恶意流量

尽管 Google Workspace 通常使用 HTTPS 连接,但数据包捕获仍然很有用。数据包捕获仍会显示丢包、重新传输、窗口大小调整以及链接饱和的证据。

收集此类数据的一种方法是启用端口镜像,它允许您捕获特定端口或 VLAN 的流量并将其转移到另一个端口,服务会在该端口上监听并记录所有流量。另一种方法是使用Wireshark等技术捕获机器上的数据以供后续分析。

捕获浏览器和网站之间交互的一种简单方法是使用 HAR（HTTP ARchive)文件。它基本上是一个 JSON 对象,其中包含有关网络请求的详细信息。

HAR 文件可以由 Google Chrome、Firefox、Internet Explorer 和 Microsoft Edge 生成。
还可以使用Google Workspace Toolbox中提供的实用程序来分析 HAR 文件。

还可以使用chrome://net-export 捕获 Google Chrome 中的网络日志并将其保存到磁盘。