



Citrix Gateway 服务

Contents

发行说明	9
September 04, 2026	9
新增功能	9
September 02, 2026	9
新增功能	9
July 06, 2026	10
新增功能	10
June 25, 2026	10
新增功能	10
March 25, 2026	11
新增功能	11
March 13, 2026	12
新增功能	12
March 11, 2026	13
新增功能	13
October 16, 2025	14
新增功能	14
October 08, 2025	14
新增功能	14
September 30, 2025	14
新增功能	14
September 24, 2025	15
新增功能	15
August 19, 2025	15
新增功能	15
August 07, 2025	15

新增功能	15
June 19, 2025	16
新增功能	16
已知问题	17
June 12, 2025	17
新增功能	17
June 05, 2025	21
新增功能	21
May 20, 2025	21
新增功能	21
May 15, 2025	22
新增功能	22
May 13, 2025	22
新增功能	22
March 27, 2025	22
新增功能	22
February 21, 2025	23
新增功能	23
January 20, 2025	23
新增功能	23
January 15, 2025	23
新增功能	23
September 18, 2024	24
新增功能	24
April 25, 2024	24
新增功能	24
April 24, 2024	24
新增功能	24

April 19, 2024	25
新增功能	25
February 27, 2024	25
新增功能	25
February 01, 2024	25
新增功能	25
November 02, 2023	26
新增功能	26
August 29, 2023	26
新增功能	26
已修复的问题	27
November 10, 2022	27
新增功能	27
已知问题	27
June 30, 2022	27
新增功能	27
April 04, 2022	28
新增功能	28
新增功能	28
October 11, 2021	28
新增功能	28
Citrix Gateway 服务入门	29
技术安全概述	30
数据流	31
数据隔离	31
审计和变更控制	31
凭据处理	31
部署注意事项	32

Citrix Cloud Connector 网络访问要求	32
Citrix Gateway 服务 HDX 连接	32
客户最佳实践	32
已弃用的密码套件	32
地理位置路由	34
如何在 Citrix Workspace 中配置地理位置路由	34
如何在 StoreFront™ 中配置地理位置路由	36
将 NetScaler Gateway 迁移到 Citrix Gateway 服务以用于 HDX 代理	37
基于云的 HDX™ 代理	37
从本地 NetScaler Gateway 迁移到基于云的 Citrix Gateway 服务	38
启用 Citrix Gateway 服务	38
回滚到 NetScaler Gateway	40
HDX 自适应传输，支持 Citrix Gateway 服务中的 EDT	42
必备条件	42
考虑事项	42
传输协议验证	43
连接回退	43
EDT MTU 发现	44
故障排除	44
Citrix Gateway 服务网络指标监控	46
支持的平台和版本	46
先决条件	46
在 DaaS Monitor 中监控 Citrix Gateway 服务网络指标	46
使用网络指标排查性能问题	46
优势	48
主要功能	48
谷歌云平台上的思杰网关服务	49
先决条件	49

Citrix Gateway 服务支持的功能	50
如何启用 Citrix Gateway 服务	50
限制	50
参考	50
支持 Citrix 虚拟应用和桌面	51
工作原理	51
适用于 StoreFront 的 Citrix Gateway 服务	52
概述	52
优势	53
必备条件	53
使用本地主机缓存 (LHC) 实现弹性	54
参考	55
已知问题和限制	55
即将推出的增强功能	55
常见问题	55
什么是适用于 StoreFront 的 Citrix Gateway 服务?	55
使用适用于 StoreFront 的 Citrix Gateway 服务有哪些优势?	55
适用于 StoreFront 的 Citrix Gateway 服务是完全托管的服务吗?	56
我需要重新架构我的访问层才能使用适用于 StoreFront 的 Citrix Gateway 服务吗?	56
采取了哪些安全措施来保护我的数据和应用程序?	56
适用于 StoreFront 的 Citrix Gateway 服务如何处理可扩展性和高流量?	56
适用于 StoreFront 的 Citrix Gateway 服务有哪些支持选项?	56
我可以将适用于 StoreFront 的 Citrix Gateway 服务与其他 Citrix 产品和服务吗?	56
适用于 StoreFront 的 Citrix Gateway 服务如何许可和定价?	56
我还需要将 CVAD 组件升级到 2407 或更高版本吗?	56
DaaS 客户与本地 CVAD 站点：解决方案的即时使用?	56
对 Citrix DaaS 环境的支持	57
对本地 Citrix Virtual Apps and Desktops 的支持	58

主要优势	58
先决条件	59
在 Citrix Cloud™ 上创建资源位置	59
在本地 Delivery Controller™ 上配置资源位置和策略	59
配置 StoreFront 以使用 Citrix Gateway 服务进行 HDX 路由	60
Citrix Gateway 服务接入点 (PoP) 列表	62
防火墙配置	62
商业区域的接入点	62
具有已定义接入点集的全局 FQDN	63
PoP FQDN	63
用于地理位置路由的区域 FQDN	68
适用于 Google Cloud Platform (GCP) 客户的接入点	70
对商业区域中接入点的支持	70
具有定义的接入点集的全局 FQDN	71
PoP FQDN	71
日本区域的接入点	74
具有已定义接入点集的全局 FQDN	74
PoP FQDN	75
美国政府区域的接入点	75
具有已定义接入点集的全局 FQDN	76
PoP FQDN	76
HDX 代理的云连接器规模和扩展性考量	77
建议	77
测试条件	77
测试方法	78
测试结果摘要	78
常见问题	79
我可以使用我的本地配置移植到 Citrix Cloud™ 吗？	79

我可以将我的门户自定义项上传到 Citrix Cloud 吗？	79
我已使用 VPX 在本地启用了多重身份验证或双因素身份验证。我可以在云端也启用此功能吗？	79
我可以使用云服务来使用 SmartControl、SmartAccess 吗？	79
如何分阶段迁移到 Citrix Gateway 服务？	79
Citrix Gateway 服务所需的最低许可证是什么？	79
拥有 Citrix Universal™ Hybrid Multi-Cloud (UHMC) 和 Citrix Platform License (CPL) 的客户的带宽配额是多少？	80
带宽配额用尽后会发生什么？	80
拥有 Citrix Universal 订阅的客户的带宽配额是多少？	80
在哪里可以查看通过 Citrix Gateway 服务建立的连接指标？	81
Citrix Gateway 服务文档历史记录	82

发行说明

Citrix Gateway 服务云发行说明描述了服务发行版中可用的新功能、现有功能的增强、已修复的问题和已知问题。发行说明包含以下一个或多个部分：

新增功能： 当前版本中可用的新功能和增强功能。

已修复的问题： 当前版本中已修复的问题。

已知问题： 当前版本中存在的问题及其适用的解决方法。

September 04, 2026

新增功能

- 已弃用的密码

Citrix Gateway 服务在 2026 年 9 月之后将不再支持以下密码。

- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1.2-AES256-GCM-SHA384
- TLS1-AES-256-CBC-SHA

September 02, 2026

新增功能

- 增强的 Citrix Gateway 服务升级

Citrix Gateway 服务现在采用分阶段方法进行服务升级，提供更受控的升级过程，从而提高服务可靠性，减少潜在中断，并降低对维护窗口的依赖。

重要提示：

- 已将 *.nssvc.net、更具体的 *.g.nssvc.net 和 *.c.nssvc.net 域，或已发布的 Citrix Gateway 服务 FQDN 列入允许列表的客户，无需执行任何操作。
- 如果您的环境通过 IP 地址限制 Citrix Gateway 服务的连接，请根据已发布的连接要求检查您当前的配置。Citrix 建议使用基于 FQDN 的规则，因为 Citrix Gateway 服务的目的地 IP 地址可能会发生变化。

有关详细信息，请参阅：[系统和连接要求](#)。[PoP 列表](#)。

July 06, 2026

新增功能

- **Citrix Gateway 服务 PoP 扩展**

为了增强业务连续性并确保为使用 Citrix Gateway 服务进行 HDX 代理的客户提供服务质量，以下新的 PoP 已于 July 01, 2026 推出。

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
AWS 亚洲 - 台湾	aws-asia-tw-rdvz.g.nssvc.net	AWS	台湾	台北

June 25, 2026

新增功能

- **Citrix Gateway 服务 PoP 扩展**

为了增强业务连续性并确保使用 Citrix Gateway 服务进行 HDX 代理的客户的**服务质量**，以下新的 PoP 已于 June 19, 2026 推出。

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
Azure 中国	az-in-c-rdvz.g.nssvc.net	阿祖尔	印度	浦那
Azure 欧洲中部	az-eu-c-rdvz.g.nssvc.net	阿祖尔	德国	法兰克福
az-us-c	az-us-c-rdvz.g.nssvc.net	阿祖尔	美国	爱荷华
AWS 欧洲南部	AWS 欧洲南部-rdvz.g.nssvc.net	AWS	意大利	米兰

有关详细信息，请参阅 [PoP FQDNs](#)。

March 25, 2026

新增功能

- 支持全球 - 备用区域的地理位置路由

Citrix Gateway 服务现在支持全球 - 备用区域的地理位置路由。

下表列出了全球 - 备用区域的 FQDN 和 PoP，用于地理位置路由：

地理位置	FQDN	包含的 POP
全球备用	- global-alt-rgn.g.nssvc.net	az-asia-se, az-aus-e, az-bz-s, az-ca-c, az-eu-n, az-eu-w, az-in-s, az-jp-e, az-nw-e, az-uae-n, az-us-e, az-us-sc, az-us-w, az-za-n, aws-aus-e, aws-bz-s, aws-ca-e, aws-eu-c, aws-in-w, aws-uk-se, aws-us-e, aws-us-nc, aws-us-

地理位置	FQDN	包含的 POP
		w, az-us-e2, aws-asia-se, aws-eu-w, aws-in-sc, aws-jp-w
	- global-alt-rgn-s.g.nssvc.net	

• 支持针对印度区域的地理位置路由

Citrix Gateway 服务现已支持针对印度区域的地理位置路由。

下表列出了用于地理位置路由的印度区域 FQDN 和 PoP：

地理位置	FQDN	包含的 POP
印度	- india-rgn.g.nssvc.net.akadns.net	aws-in-w, aws-in-sc, az-in-s
	- india-rgn-s.g.nssvc.net.akadns.net	

March 13, 2026

新增功能

• Citrix Gateway 服务 PoP 扩展

为了增强业务连续性并确保为使用 Citrix Gateway 服务进行 HDX 代理的客户提供优质服务，计划在 2026 年 5 月底前推出以下新的 PoP：

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
Azure 印度中部	az-in-c-rdvz.g.nssvc.net	Azure (阿祖尔)	印度	浦那
az-eu-c	az-eu-c-rdvz.g.nssvc.net	Azure (阿祖尔)	德国	法兰克福

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
az-us-c	az-us-c-rdvz.g.nssvc.net	Azure (阿祖尔)	美国	爱荷华
aws-eu-s	aws-eu-s-rdvz.g.nssvc.net	AWS	意大利	米兰

有关详细信息，请参阅 [PoP FQDNs](#)。

March 11, 2026

新增功能

- Citrix Gateway 服务支持 TLS 1.3

Citrix Gateway 服务将于 2026 年第三季度中期启用端到端 TLS 1.3 连接。此次升级是我们持续致力于提高安全性、性能和合规性的一部分。

客户操作

使用 Rendezvous 和 Citrix Gateway 服务的客户必须确保其 Virtual Delivery Agent (VDA) 部署满足最低支持版本，以防止潜在的会话启动问题。

- TLS 1.3 的最低 VDA 版本要求：
 - 当前版本 (CR)：2407 或更高版本
 - 长期服务版本 (LTSR)：2402 LTSR CU1 或更高版本
- Citrix Workspace 应用程序 (CWA) 要求：

明确支持 TLS 1.3 的 Citrix Workspace 应用程序版本。通过查看 Citrix Workspace 应用程序功能矩阵，验证支持 TLS 1.3 的客户端操作系统版本。有关详细信息，请参阅[Citrix Workspace 应用程序功能矩阵](#)。

注意：

特定 VDA 版本的关键升级警告：

在 2026 年第三季度中期之前，将较旧的 VDA（例如 CR 2303、CR 2308、CR 2311 或 LTSR 2402（CU1 之前））升级到最低支持版本。这可以防止潜在的会话启动失败并确保服务不中断。

TLS 1.2 回退：

不支持 TLS 1.3 的旧版受支持 VDA 版本（例如 2203 LTSR CU、2303 之前的 CR VDA）或通过网络不支持 TLS 1.3 的旧版受支持 Citrix Workspace 应用程序建立的连接，将继续运行而不会出现会话启动问题。这些连接可以安全地继续使用 TLS 1.2。

有关 VDA 版本支持的更多信息，请参阅[升级和迁移](#)。有关部署规划的更多信息，请参阅[Citrix LTSR 和当前版本生命周期文档](#)。

October 16, 2025

新增功能

- **网络指标监控 - Citrix Gateway 服务中正式发布**

网络指标监控现已在 Citrix Gateway 服务中正式发布。有关详细信息，请参阅[Citrix Gateway 服务的网络指标监控](#)。

October 08, 2025

新增功能

- **支持本地 Citrix Virtual Apps and Desktops - Citrix Gateway 服务中 StoreFront 的正式发布**

Citrix Gateway 服务中 StoreFront 的本地 Citrix Virtual Apps and Desktops 支持现已正式发布。有关详细信息，请参阅[支持本地 Citrix Virtual Apps and Desktops](#)。

September 30, 2025

新增功能

- **HDX 代理的 Cloud Connector 大小调整和扩展建议**

现在，对于不使用 Rendezvous v1 或 v2 协议的 HDX 代理部署，提供了更新的 Cloud Connector 大小调整和扩展建议。此指南可确保高可用性、稳定性和高效性能。有关详细信息，请参阅[HDX 代理的 Cloud Connector 大小调整和扩展注意事项](#)。

September 24, 2025

新增功能

- 在日本大阪新增 AWS PoP

为了增强业务连续性并确保使用 Citrix Gateway 服务进行 HDX 代理的客户的服务质量，我们正
在日本大阪新增一个 PoP。

PoP 完全限定域名：aws-jp-w-rdvz.g.nssvc.net

有关详细信息，请参阅 [PoP FQDN](#)。

August 19, 2025

新增功能

- Citrix Gateway 服务中的 DNS 服务变更

Citrix Gateway 服务正在分阶段将其 DNS 服务从当前提供商迁移到 Citrix 商业云的 Akamai
DNS。为确保顺利迁移和持续运行，您必须完成以下配置：

- 防火墙配置：**按照 [系统和连接要求](#) 中所述配置防火墙和安全 Web 网关。确保所有全局
FQDN 都属于您所需的例外情况。有关更多信息，请参阅 [具有已定义 PoP 集的全局 FQDN](#)
。
- DNS 转发器配置：**如果配置了 DNS 转发器以允许特定域的递归 DNS 解析，则必须将
`*.akadns.net` 包含在允许列表中。此配置使 Citrix Cloud Connector、Citrix Virtual Apps
and Desktops 或客户端能够连接到 Citrix Gateway 服务。

August 07, 2025

新增功能

- Citrix Gateway 服务 PoP 扩展

为增强业务连续性并确保为使用 Citrix Gateway 服务进行 HDX 代理的客户提供服务质量，计划
在即将发布的服务版本中推出以下新 PoP：

POP 代码	POP FQDN	云服务提供商	国家	位置
az-us-e2	az-us-e2-rdvz.g.nssvc.net	微软 Azure	美国	弗吉尼亚
亚马逊云服务 东南亚	aws-asia-se-rdvz.g.nssvc.net	AWS	新加坡	新加坡
aws-亚洲-台湾	aws-亚洲-台湾-rdvz.g.nssvc.net	AWS	台湾	台北

有关更多信息，请参阅 [PoP FQDNs](#)。

• 支持在 Citrix Japan Cloud 中监控 Citrix Gateway 服务带宽

Citrix Japan Cloud 的管理员现在可以通过增强的可视性和跟踪功能监控 Citrix Gateway 服务带宽使用情况。此功能可提供对跨多个授权的消耗模式的全面洞察，并支持主动监控带宽使用情况以识别潜在的超额使用。

以下是一些主要功能：

- **使用情况摘要：**“使用情况摘要”页面显示了所有授权和任何带宽超额的概览。
- ****详细使用情况界面：****多选项卡界面允许您查看月度、年度和定期授权的使用情况详细信息。
- ****基于授权的计算：****带宽根据您购买的授权分配情况精确计算。

有关更多信息，请参阅 [监控 Gateway 服务的带宽使用情况](#)。

June 19, 2025

新增功能

• Citrix Gateway 服务增强型网络指标监控 - 预览版

Citrix Gateway Service 的增强型网络指标监控现已面向所有 Citrix DaaS™ 客户提供。要使用此功能，管理员只需在 Citrix Studio 或 Web Studio 中为以下版本启用[网络遥测策略](#)即可：

组件	平台	支持的版本
Citrix Workspace 应用程序	视窗	2411 或更高版本
Citrix 虚拟应用和桌面	视窗	2411 或更高版本

[CTXENG-65466]

已知问题

- 当 Citrix Workspace 应用程序和 Citrix Virtual Apps and Desktops 的 2503 版本都启用了网络遥测策略时，会话可靠性功能可能不适用于 EDT 会话。

June 12, 2025

新增功能

- 支持本地 Citrix Virtual Apps and Desktops - 预览

Citrix Gateway 服务现在支持本地 Citrix Virtual Apps and Desktops。Citrix Gateway 服务与本地 Delivery Controller 集成，这使得 Citrix Virtual Apps and Desktops 客户的混合访问更加容易。混合访问允许您使用本地 NetScaler Gateway 和 StoreFront 进行身份验证、授权和枚举。Citrix Gateway 服务用于启动虚拟应用程序和桌面。这种方法最大限度地提高了现有远程访问基础设施的价值，并最大限度地减少了管理工作。

主要优势：

Citrix Gateway 服务与本地 Delivery Controller 的集成提供了以下优势：

- **自定义保留：** NetScaler Gateway 和 StoreFront™ 自定义项可以保留，确保一致的用户体验。
- **最小化维护：** HDX 代理性能和扩展要求现在由 Citrix Gateway 服务管理，无需客户进行管理。
- **现有 URL：** DaaS 客户可以继续使用他们熟悉的本地 NetScaler® Gateway URL。
- **利用 LHC 增强弹性：** 本地主机缓存 (LHC) 通过允许连接器在中断期间充当本地安全票证颁发机构 (STA) 来支持弹性需求。
- **更好的用户体验：** 使用地理位置更近的 PoP 可以减少延迟并提高性能。
- **高弹性：** 由于 Citrix Gateway 服务的多云和多地理架构，确保了高弹性。

先决条件：

- a. 您必须拥有一个功能正常的本地工作环境，其中 NetScaler Gateway 用于身份验证和授权，StoreFront 用于枚举。
- b. 将 StoreFront 升级到版本 2503 或更高版本。有关详细信息，请参阅 [升级 StoreFront](#)。

在 Citrix Cloud™ 上创建资源位置：

- a. 加入 Citrix Cloud。有关详细信息，请参阅 [创建 Citrix Cloud 帐户](#) 和 [连接到 Citrix Cloud](#)。
- b. 在 Citrix Cloud 上，安装 Cloud Connector 并将其与资源位置关联。有关详细信息，请参阅 [Cloud Connector 安装](#)。

注意：

要使现有应用程序和桌面可供订阅者使用，请将您的站点（Citrix Virtual Apps and Desktops 部署）添加到 Citrix Workspace。有关详细信息，请参阅 [在工作区中聚合 Virtual Apps and Desktops](#)。

在本地 Delivery Controller™ 上配置资源位置和策略：

- a. 在 Windows Active Directory (AD) 或域控制器 (DC) 服务器上运行以下命令，以检索 Windows AD 或 DC 环境中连接器计算机的安全标识符 (SID)。记下连接器计算机的 SID。

```
Get-ADComputer -Filter *|Select-Object Name, SID
```

- b. 在本地 Delivery Controller 中，创建一个区域并将其映射到在 Citrix Cloud 中创建的资源位置。
 - a. 在本地 Delivery Controller 中，在 PowerShell 中运行以下命令，并记下为所需资源位置生成的 Uid：

```
Get-ConfigZone
```

- b. 对所有 Citrix Cloud Connector 运行以下命令：

```
Set-ConfigZone -Uid <Uid from above command output> -ExternalUid  
<RL ID noted at step 1>
```

```
new-configedgeserver <User friendly name> -MachineAddress  
"<Connector FQDN"> -Sid <Connector respective SID from step 2>  
-uuid <Respective Edge server UUID from step 1> -ZoneUid <Uid  
from Get-ConfigZone output>
```

- c. 要使用 Rendezvous v1，请在 Delivery Controller 策略中启用 Rendezvous，并确保本地 Delivery Controller 已配置连接器详细信息以接受 Rendezvous 请求。有关详细信息，请参阅 [Rendezvous v1](#)。
- d. 要将 HDX 自适应传输与 EDT 结合使用，请在本地 Delivery Controller 的 Delivery Controller 策略中启用自适应传输协议。有关详细信息，请参阅 [支持 EDT 的 HDX 自适应传输，适用于 Citrix Gateway 服务](#)。

配置 Citrix Gateway 服务以使 StoreFront 与本地 Delivery Controller 集成：

执行以下步骤以将适用于 StoreFront 的 Citrix Gateway 服务与本地 Delivery Controller 集成：

- a. 配置身份验证网关
- b. 配置路由网关
- c. 配置 Delivery Controller 的远程访问设置
- d. 映射 Delivery Controller 和路由网关
- e. 配置最佳 HDX™ 网关路由

步骤 1 - 配置身份验证网关：

- a. 打开 StoreFront 管理控制台。
- b. 导航到 **Stores > Manage Citrix Gateways**，然后单击 **Add**。
- c. 在 **Display name** 中，输入身份验证网关的名称。
- d. 在 **网关类型** 中，选择 **Citrix Gateway Appliance**；并在 **用途或角色** 中，选择 **仅身份验证**。
- e. 在 **Citrix Gateway URL** 中，输入身份验证 URL。
- f. 单击 **Next**，然后单击 **Finish**。

步骤 2 - 配置路由网关：

- a. 在 StoreFront 管理控制台中，导航到 **Stores > Manage Citrix Gateways**，然后单击 **Add**。
- b. 在 **Display name** 中，输入路由网关的名称。
- c. 在 **网关类型** 中，选择 **Citrix Gateway service**。

d. 如果需要地理位置路由，请填写以下参数：

- **Citrix Gateway service URL**：输入以 `rgn.g.nssvc.net` 结尾的 FQDN，它用作地理位置路由的通用 FQDN。
- **Citrix Gateway 服务 URL（STA 连接器模式）**：输入以 `rgn-s.g.nssvc.net` 结尾的 FQDN，它支持服务连续性功能。

有关详细信息，请参阅[用于地理位置路由的区域 FQDN](#)。

e. 导航到“云连接器”选项卡，然后单击“添加”以添加云连接器 URL。

f. 启用“负载平衡多个服务器”和“启用会话可靠性”。

g. 单击“确定”。

注意：

- 如果在本地 StoreFront 上禁用“启用会话可靠性”选项，则 HDX 会话启动失败。
- 适用于 StoreFront 的 Citrix Gateway 服务不支持双 STA。因此，不得选择“从云连接器请求两个票证（如果可用）”选项。

步骤 3 - 配置 Delivery Controller 的远程访问设置：

- a. 在 StoreFront 管理控制台中，导航到您站点中的“配置远程访问设置”。
- b. 选择“启用远程访问”。
- c. 在“Citrix Gateway”中，选择之前配置的身份验证网关。
- d. 单击“确定”。

步骤 4 - 映射 Delivery Controller 和路由网关：

- a. 在 StoreFront 管理控制台中，导航到您站点中的“配置应用商店设置”>“最佳 HDX 路由”。
- b. 选择路由网关，点击**管理站点**，然后选择已配置的站点。
- c. 点击**确定**。

步骤 5 - 配置最佳 HDX 网关路由：

注意：

如果您有多个区域，请按照“步骤 2：配置路由网关”中的说明为每个区域创建路由网关。

按照以下步骤将每个区域映射到其独特的路由网关：

- a. 在 StoreFront 管理控制台中，导航到您站点中的**配置存储设置 > 最佳 HDX 路由**。
- b. 选择路由网关，然后点击**管理区域**。
- c. 在**管理区域**下点击**添加**，并创建一个与本地 Delivery Controller 上创建的区域名称相同的区域。

June 05, 2025

新增功能

- **在法国巴黎新增 AWS PoP**

为了增强业务连续性并确保使用 Citrix Gateway 服务进行 HDX 代理的客户的服务质量，在法国巴黎新增了一个 AWS PoP。

接入点完全限定域名: `aws-eu-w-rdvz.g.nssvc.net`

有关详细信息，请参阅 [PoP FQDNs](#)。

May 20, 2025

新增功能

- **安全性和合规性增强功能**

Citrix Gateway 服务现已符合以下行业标准认证，这进一步巩固了我们提供安全可靠服务的承诺：

- **系统和组织控制 (SOC) 2 类型 2**：确保符合安全性、可用性、处理完整性、保密性和隐私方面的严格要求。
- **支付卡行业数据安全标准 (PCI DSS) v4.0**：验证支付卡数据的安全处理。
- **健康保险流通与责任法案 (HIPAA)**：证明遵守受保护健康信息 (PHI) 安全法规。

有关最新认证状态，请参阅 [Citrix Trust Center](#) 中的“认证”部分。

May 15, 2025

新增功能

- 地理位置路由 - Citrix Gateway 服务中 StoreFront 的正式发布

地理位置路由现已在 Citrix Gateway 服务中正式发布，适用于 StoreFront。有关详细信息，请参阅 [添加 Citrix Gateway 服务](#)。

May 13, 2025

新增功能

- 在印度海得拉巴新增 AWS PoP

为了增强业务连续性并确保使用 Citrix Gateway 服务进行 HDX 代理的客户的服务质量，在印度中南部的海得拉巴新增了一个 AWS PoP。

PoP 完全限定域名: aws-in-sc-rdvz.g.nssvc.net

有关详细信息，请参阅 [PoP FQDNs](#)。

March 27, 2025

新增功能

- 支持对亚洲区域的 PoP 进行地理位置路由

Citrix Gateway 服务现在支持对亚洲区域的 PoP 进行地理位置路由。

下表列出了用于地理位置路由的亚洲区域 FQDN 和 PoP：

地理位置	FQDN	包含的 POP	
亚洲	• asia-rgn.g.nssvc.net • asia-rgn-s.g.nssvc.net	az-uae-n, aws-in-w, az-in-s, az-asia-se, az-jp-e	

[CTXENG-65014]

February 21, 2025

新增功能

- 为 GCP 客户增强 Citrix DaaS 体验，支持商业区域 PoP

即将推出的服务版本将为 GCP 客户提供商业区域 PoP 支持。

目前，全球 5 大洲共有 24 个商业区域 PoP。通过此即将推出的支持，除了现有的 GCP PoP 之外，您还可以在 Azure 和 AWS 中使用这些 PoP。

重要提示：

为确保您的 Citrix DaaS 部署持续运行，请在 March 15, 2025 之前完成 [适用于 Google Cloud Platform \(GCP\) 客户的 PoP](#) 中指定的说明。

January 20, 2025

新增功能

- Citrix Gateway 服务网络指标监控 - 预览版

网络指标提供 Citrix Workspace 应用程序与通过 Citrix Gateway 服务传输的虚拟投递代理 (VDA) 之间的 HDX 流量的端到端可见性。DaaS Monitor 中网络指标的可视化表示使管理员能够查看实时客户端和网络延迟指标、历史报告、端到端性能数据，并排查性能问题。有关详细信息，请参阅 [Citrix Gateway 服务中的网络指标监控 - 预览版](#)。

January 15, 2025

新增功能

- 地理位置路由 - 全面上市

地理位置路由现已在 Citrix Gateway 服务中全面上市。有关详细信息，请参阅 [地理位置路由](#)。

September 18, 2024

新增功能

- 适用于 StoreFront 的 Citrix Gateway 服务 - 全面上市

适用于 StoreFront 的 Citrix Gateway 服务现已在 Citrix DaaS 环境中全面上市。请参阅 [适用于 StoreFront 的 Citrix Gateway 服务](#)

- 通过本地主机缓存 (LHC) 实现弹性

在 StoreFront 的 Citrix Gateway 服务部署中，当 Cloud Connector 和 Citrix Cloud 之间的通信中断时，LHC 会被激活。LHC 是 Citrix DaaS 的一项功能，可在网络中断期间确保弹性。有关更多信息，请参阅[使用本地主机缓存 \(LHC\) 实现弹性](#)。

April 25, 2024

新增功能

- 适用于 StoreFront 的 Citrix Gateway 服务 - 预览版

适用于 StoreFront 的 Citrix Gateway 服务是一种基于云的 HDX 解决方案，可为从本地 StoreFront 访问的资源提供安全的远程访问。您可以利用 Citrix Cloud（用于 HDX 代理）的可扩展性和可靠性，而无需更改您的本地 StoreFront 和本地 NetScaler Gateway 环境。

此解决方案为预览版。有关详细信息，请参阅[适用于 StoreFront 的 Citrix Gateway 服务 - 预览版](#)。

April 24, 2024

新增功能

- 支持音频策略的容损模式

Citrix Gateway 服务现在支持 Citrix Virtual Apps and Desktops 中最新的音频容损模式。此模式可增强连接到高延迟和数据包丢失网络的用户的音频体验。用户必须使用 Citrix Virtual Apps and Desktops 7 2402 LTSR 或更高版本才能使用此功能。

音频容损模式基于 EDT 容损传输协议，该协议允许在传输过程中丢失数据包而无需重新发送多媒体内容，从而为用户带来更实时的体验。在有损网络条件下，它是音频的首选模式，可确保与 EDT 相比具有卓越的音频质量。

有关容损模式设置的详细信息，请参阅[音频容损模式](#)。

April 19, 2024

新增功能

- 支持多伦多（加拿大） Azure PoP

现已支持加拿大多伦多的 Azure PoP。

PoP FQDN : `az-ca-c-rdvz.g.nssvc.net`

有关详细信息，请参阅 [地理位置路由 - 预览](#)。

February 27, 2024

新增功能

- 支持 谷歌云平台

计划在即将发布的服务版本中支持 Google Cloud Platform (GCP) PoP 以及现有的 Azure 和 AWS PoP。

目前，有 5 个 GCP PoP 分布在不同的地理位置。通过即将推出的此支持，您可以利用这些 GCP PoP 以及现有的 Azure 和 AWS PoP。

重要提示：

为确保您的 Citrix DaaS 部署持续运行，请在 2024 年 3 月 15 日之前完成 [Citrix Gateway 服务 – 存在点 \(PoP\)](#) 中指定的说明。

February 01, 2024

新增功能

- 支持多伦多（加拿大） Azure PoP

计划在即将发布的服务版本中支持加拿大多伦多的 Azure PoP。

PoP FQDN : `az-ca-c-rdvz.g.nssvc.net`

November 02, 2023

新增功能

- 支持最新版本的 HDX 压缩器

Citrix Gateway 服务支持最新版本的 HDX 压缩器。HDX 压缩器是一种通用压缩器，可跨虚拟通道工作。最新的压缩器通过以下功能提高了 Citrix DaaS 的整体性能：

- 降低 HDX 会话的网络带宽利用率。
- 数据包传输时间更短，从而实现更快的响应。

以下软件版本支持最新的压缩器。

- Citrix 虚拟应用和桌面 7 2303 (Windows) 及更高版本。
- Citrix Workspace app 2303 (Windows) 及更高版本。

August 29, 2023

新增功能

- 地理位置路由 - 预览

Citrix Gateway 服务为管理员提供了一项功能，使其用户能够连接到特定区域的 PoP，或者仅通过特定的云服务提供商连接，而无论用户身在何处。有关详细信息，请参阅 [地理位置路由 - 技术预览](#)。

- HDX 性能分析

Citrix Gateway 服务支持 HDX 性能分析功能，该功能使 Citrix Analytics 管理员能够查看与连接器-网关 PoP 延迟相关的性能数据。有关详细信息，请参阅 [连接器统计信息](#)。

- 加速网络

Citrix Gateway 服务基础架构已增强，以支持加速网络，其中它使用单根 I/O 虚拟化 (SR-IOV) 为用户提供高性能网络功能。

- 已弃用的弱密码

有关 Citrix Gateway 服务已弃用密码的更新列表，请参阅 [技术安全概述](#)。

已修复的问题

- 每当 Azure 负载均衡器中的后端池被修改时，EDT 会话就会断开连接。

November 10, 2022

新增功能

- 支持 Rendezvous 协议版本 V2

Citrix Gateway 服务现在支持 Google Cloud Platform 上的 Citrix Gateway 服务的 Rendezvous 协议版本 V2。有关详细信息，请参阅 [Citrix Gateway 服务支持的功能](#)。

- Citrix Gateway 服务在 Google Cloud Platform 上在欧洲的可用性

Citrix Gateway 服务现已在以下欧洲区域的 Google Cloud Platform 上推出。

- 伦敦
- 苏黎世

有关详细信息，请参阅 [Google Cloud Platform 上的 Citrix Gateway 服务](#)。

已知问题

- 如果客户 ID 少于 6 个字符，Rendezvous v2 VDA 注册将失败。

June 30, 2022

新增功能

- Citrix Gateway 服务在 Google Cloud Platform 上的可用性

借助 Google Cloud Platform (GCP) 上的 Citrix Gateway 服务支持，在 Google Cloud 上运行工作负载的客户可以利用 Citrix Gateway 优化路由功能，使用 Google Cloud 的高性能全球网络。优化网关路由功能将客户端定向到最近的 GCP Citrix Gateway 服务 PoP。此外，Google Cloud 上的 Citrix Gateway 服务在 Citrix Workspace 客户端和虚拟化资源之间提供安全连接，以最低的延迟和最佳的用户体验交付会话。有关详细信息，请参阅 [Google Cloud Platform 上的 Citrix Gateway 服务](#)。

April 04, 2022

新增功能

- 品牌重塑更改
 - Citrix 安全工作区访问现已更名为 Citrix 安全私有访问。
 - Citrix Virtual Apps and Desktops 服务现已更名为 Citrix DaaS。

新增功能

- 将 Citrix Gateway 服务磁贴合并到 Citrix Cloud 中的单个 Citrix Secure Private Access 中

October 11, 2021

新增功能

- 将 Citrix Gateway 服务磁贴合并到 Citrix Cloud 中的单个 Citrix Secure Private Access 中

Citrix Gateway 服务磁贴和 Citrix Secure Private Access 磁贴已合并到 Citrix Secure Private Access 磁贴中，并且 Citrix Gateway 登录页面已针对 Citrix Secure Private Access 进行了修改。因此，您将看不到 **Virtual Apps and Desktops** 和 **Add a Web/SaaS app** 快捷方式。但是，Citrix Virtual Apps and Desktops 客户可以从 **Workspace configuration > Access > External Connectivity** 启用 Citrix Gateway 服务。除此之外，功能没有变化。

以下 Citrix Gateway 服务功能已移至 Citrix Secure Private Access 服务。

- 配置 SaaS 和企业 Web 应用程序
- 启用增强的安全控制
- 配置上下文策略

Citrix Secure Private Access 客户（包括 Citrix Workspace Essentials 和 Citrix Workspace Standard）现在可以使用一个 Citrix Secure Private Access 磁贴来配置 SaaS 和企业 Web 应用程序、增强的安全控制、上下文策略以及 Web 过滤策略。

Citrix Gateway 服务入门

获得 Citrix DaaS 授权的客户默认情况下会启用 Citrix Gateway 服务。客户无需申请单独的 Citrix Gateway 服务试用版。有关详细信息，请参阅 [注册服务](#)。

重要提示：

在 Citrix Cloud 主页上，您看不到 Citrix Gateway 服务磁贴。Citrix Gateway 服务磁贴和 Citrix Secure Private Access 磁贴已合并到 Citrix Secure Private Access 磁贴中，并且 Citrix Secure Private Access 的登录页面已修改。因此，您看不到 **Virtual Apps and Desktops** 快捷方式。但是，Citrix Virtual Apps and Desktops 客户可以从 **Workspace configuration > Access > External Connectivity** 启用 Citrix Gateway 服务。否则，功能没有变化。

技术安全概述

Citrix Cloud 管理 Citrix Gateway 服务的运行，从而无需客户管理 NetScaler Gateway 设备。Citrix Gateway 服务通过 Citrix Workspace 应用程序进行预配。

Citrix Gateway 服务提供以下功能：

HDX 连接：托管应用程序和桌面的虚拟投递代理 (VDA) 仍由客户在其选择的数据中心（无论是云端还是本地）中控制。这些组件使用名为 Citrix Cloud Connector 的代理连接到云服务。

DTLS 1.2 协议支持：Citrix Gateway 服务支持通过 EDT（基于 UDP 的传输协议）的 HDX 会话使用数据报传输层安全 (DTLS) 1.2。支持以下密码套件：

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS 协议支持：Citrix Gateway 服务支持以下 TLS 密码套件：

- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1-ECDHE-RSA-AES128-SHA
- TLS1.2-AES256-GCM-SHA384
- TLS1-AES-256-CBC-SHA

注意：

Citrix Gateway 服务不支持 TLS 1.0 和 TLS 1.1 版本。

Endpoint Management 集成：当与 Citrix Endpoint Management 和 Citrix Workspace 集成时，Citrix Gateway 服务可为您的内部网络和资源提供安全的远程设备访问。将 Citrix Gateway 服务与 Endpoint Management 集成快速简便。Citrix Gateway 服务全面支持 Citrix SSO，适用于 Secure Mail 和 Secure Web 等应用程序。

数据流

Citrix Gateway 服务是一种全球分布式多租户服务。最终用户使用最近的接入点 (PoP)，在该接入点提供他们所需的特定功能，而无论 Citrix Cloud 控制平面地理位置选择或所访问应用程序的位置如何。配置（例如授权元数据）会复制到所有 PoP。

Citrix® 用于诊断、监控、业务和容量规划的日志已安全存储在一个中心位置。

客户配置存储在一个中心位置，并全球分发到所有 PoP。

云与客户场所之间的数据流通过端口 443 使用安全的 TLS 连接。

用于用户身份验证和单点登录的加密密钥存储在硬件安全模块中。

数据隔离

Citrix Gateway 服务存储以下数据：

- 客户应用程序的代理和监控所需的配置数据 – 数据在持久化时由客户确定范围。
- 每个用户设备的 TOTP 种子 – TOTP 种子由客户、用户和设备确定范围。

审计和变更控制

目前，Citrix Gateway 服务不向客户提供审计和变更控制日志。日志可供 Citrix 使用，Citrix 可利用这些日志审计最终用户和管理员的活动。

凭据处理

该服务处理两种类型的凭据：

- 用户凭据：最终用户凭据（密码和身份验证令牌）可能会提供给 Citrix Gateway 服务以执行以下操作：
 - Citrix Secure Private Access - 该服务使用用户身份来确定对 SaaS 和企业 Web 应用程序以及其他资源的访问权限。
 - 单点登录 - 该服务可能拥有用户密码的访问权限，以使用 HTTP Basic、NTLM 或基于表单的身份验证完成对内部 Web 应用程序的 SSO 功能。除非您专门配置 HTTP Basic 身份验证，否则用于密码的加密协议是 TLS。
- 管理员凭据：管理员针对 Citrix Cloud 进行身份验证。这将生成一个一次性签名的 JSON Web Token (JWT)，该令牌授予管理员访问 Citrix Cloud 中管理控制台的权限。

注意事项

- 所有通过公共网络的流量都由 TLS 加密，并使用 Citrix 管理的证书。
- 用于 SaaS 应用程序 SSO 的密钥（SAML 签名密钥）由 Citrix 完全管理。
- 对于 MFA，Citrix Gateway 服务存储用于为 TOTP 算法提供种子的每设备密钥。
- 为了启用 Kerberos 单点登录功能，客户可能会使用凭据（用户名 + 密码）为受信任的服务帐户配置 Connector Appliance，以执行 Kerberos 约束委派。

部署注意事项

Citrix 建议用户查阅已发布的最佳实践文档，以部署 Citrix Gateway 服务。有关 SaaS 应用程序和企业 Web 应用程序部署以及网络连接器的更多注意事项如下。

选择正确的连接器：必须根据用例选择正确的连接器：

用例	连接器	外形规格
用户身份验证：Active Directory	Citrix 云连接器	Windows 软件
HDX 连接	Citrix 云连接器	Windows 软件

Citrix Cloud Connector 网络访问要求

有关 Citrix Cloud Connector 网络访问要求的信息，请参阅 <https://docs.citrix.com/zh-cn/citrix-cloud/overview/requirements/internet-connectivity-requirements.html>

Citrix Gateway 服务 HDX 连接

使用 Citrix Gateway 服务可避免在客户数据中心内部署 NetScaler Gateway。要使用 Citrix Gateway 服务，前提是使用从 Citrix Cloud 交付的 Citrix Workspace。

客户最佳实践

建议客户在其网络中使用 TLS，并且不要为通过 HTTP 访问的应用程序启用 SSO。

已弃用的密码套件

为增强安全性，以下密码套件已弃用：

- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES-128-SHA256
- TLS1.2-AES256-GCM-SHA384
- TLS1.2-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-128-SHA256
- TLS1.2-DHE-RSA-AES256-GCM-SHA384
- TLS1.2-DHE-RSA-AES128-GCM-SHA256
- SSL3-DES-CBC3-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-DSS-AES-256-CBC-SHA
- TLS1-DHE-DSS-AES-128-CBC-SHA
- TLS1-ECDHE-RSA-DES-CBC3-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256

地理位置路由

地理位置路由允许管理员将用户流量导向特定区域（PoP），无论用户身在何处。地理位置路由可用于以下场景：

- **数据驻留要求：**许多国家/地区都有法规要求数据在其境内存储和处理。例如，可以配置地理位置路由，以确保来自欧盟 (EU) 用户的所有数据都路由到欧盟境内的 PoP，从而符合通用数据保护条例 (GDPR) 的数据驻留要求。
- **数据主权：**数据受其收集和处理所在国家或地区的法律法规管辖。例如，跨国公司可以利用地理位置路由来确保来自 DaaS 控制区域（如美国、欧盟和亚太南部）的数据在相应的区域 PoP 中处理，从而符合数据主权法律。
- **行业特定法规：**某些行业特定法规要求以特定方式存储和处理数据。例如，医疗保健提供商可以使用地理位置路由来确保患者数据路由到美国境内符合健康保险流通与责任法案 (HIPAA) 的商业区域 PoP。
- **金融服务：**金融机构通常受法规约束，要求在特定司法管辖区内处理金融数据。例如，银行可以使用地理位置路由来确保来自亚太南部客户的交易在亚太南部境内的商业区域 PoP 中处理，从而符合当地金融法规。
- **流量优化：**地理位置路由可确保用户流量导向特定区域 PoP，通过减少延迟和改善用户体验来优化性能。
- **负载均衡：**通过将流量导向特定区域 PoP，管理员可以将负载分配到多个 PoP，从而防止任何单个区域过载。

注意：

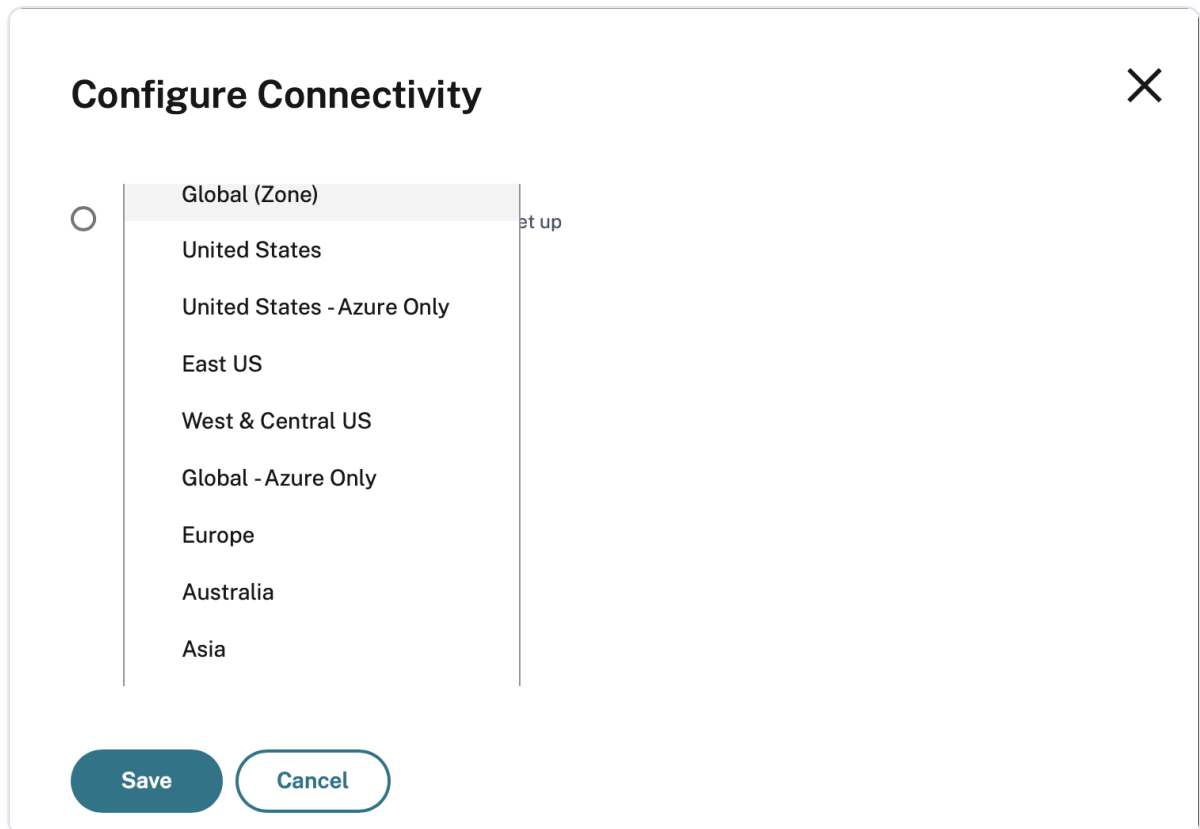
地理位置路由仅适用于商业区域的 Citrix Cloud 客户。它不适用于 Google Cloud Platform、日本和美国政府区域。

如何在 Citrix Workspace 中配置地理位置路由

您可以从 Citrix Cloud 上的“资源位置”或“Workspace 配置”页面为用户流量配置特定区域。

1. 登录到 [Citrix Cloud](#)。
2. 单击汉堡菜单并选择“资源位置”或“Workspace 配置”。

- a. 在“资源位置”页面上，选择一个位置并单击“网关”。将显示“配置连接”屏幕。
- b. 在工作区配置页面中，在“外部连接”下，选择一个位置并单击省略号。此时将显示配置连接屏幕。

A dialog box titled "Configure Connectivity" with a close button (X) in the top right corner. On the left, there is a radio button. To its right is a list of regions: "Global (Zone)", "United States", "United States - Azure Only", "East US", "West & Central US", "Global - Azure Only", "Europe", "Australia", and "Asia". The "Global (Zone)" option is currently selected and highlighted. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Configure Connectivity

☐ Global (Zone) et up

United States

United States - Azure Only

East US

West & Central US

Global - Azure Only

Europe

Australia

Asia

Save **Cancel**

有关支持基于地理位置的流量路由的 PoP 关联的 FQDN 列表，请参阅 [用于地理位置路由的区域 FQDN](#)。

3. 在**网关服务区域（可选）**中，选择要将客户流量路由到的区域。

注意：

如果您未选择任何区域，则默认选择**全球**。当区域为**全球**时，流量将分流到距离客户最近的 PoP。有关详细信息，请参阅 [最佳网关路由](#)。

在极少数情况下，如果发生中断，并且特定区域的所有 PoP 都不可用，则配置将回退到**全球**，而不是阻止流量。

4. 单击**保存**。

如何在 StoreFront™ 中配置地理位置路由

重要提示：

- 仅当您为 StoreFront 启用 Citrix Gateway 服务时，才能在 StoreFront 中配置地理位置路由。有关详细信息，请参阅 [适用于 StoreFront 的 Citrix Gateway 服务](#)。
- StoreFront 2503 及更高版本支持地理位置路由。

您可以手动指定要使用的区域的 PoP FQDN。有关如何在 StoreFront 中配置地理位置路由的详细信息，请参阅 [添加 Citrix Gateway 服务](#)。

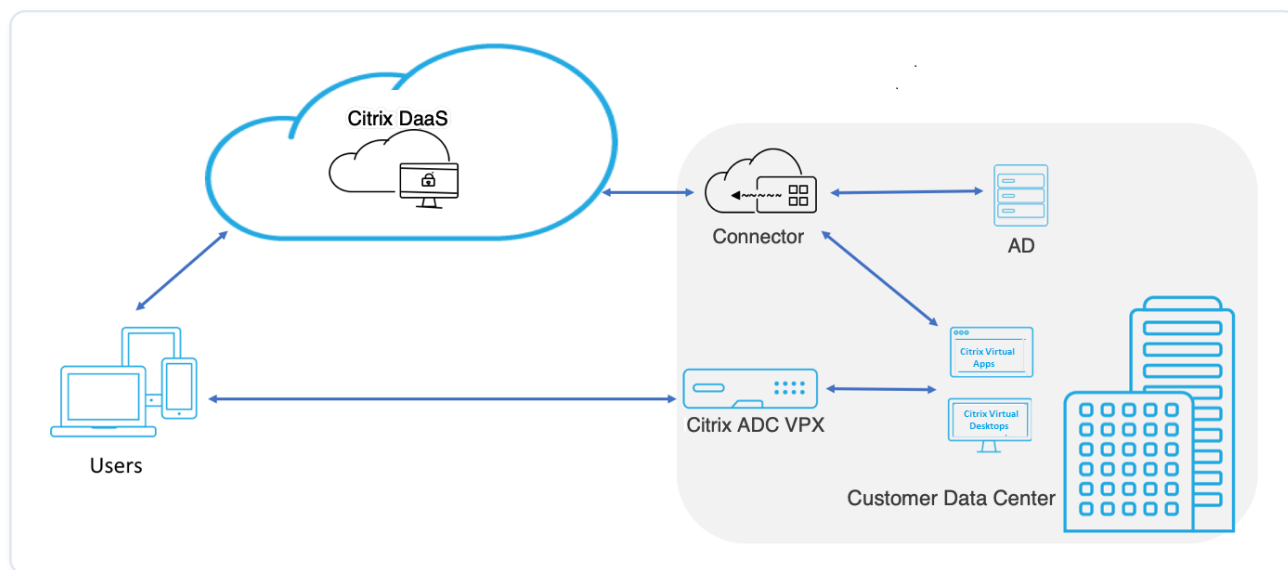
将 NetScaler Gateway 迁移到 Citrix Gateway 服务以用于 HDX 代理

您可以将 Citrix Gateway for HDX Proxy 迁移到由 Citrix Cloud 上的 Citrix Gateway 服务提供支持的完全托管的基于云的 HDX 代理。

基于云的 HDX™ 代理

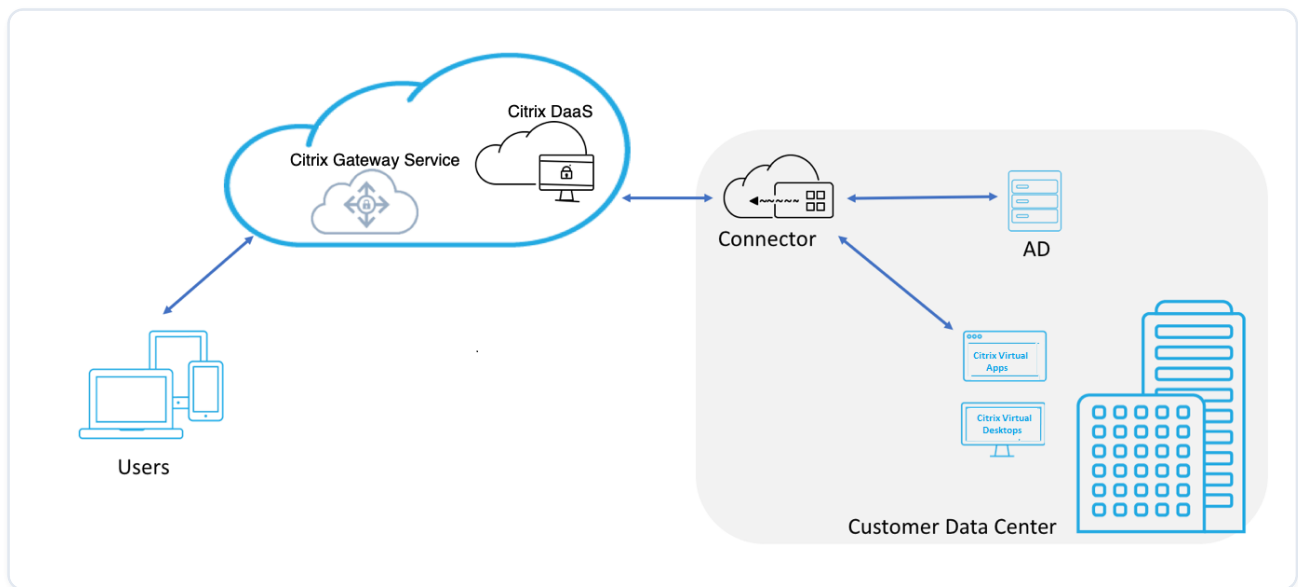
默认情况下，有权使用 Citrix DaaS 的客户将启用 Citrix Gateway 服务。客户无需申请单独的 Citrix Gateway 服务试用。

图 1. 将 NetScaler® Gateway 作为 HDX 代理的部署



Citrix Gateway 服务是一种基于云的 HDX 代理，它通过基于云的网关提供安全的远程访问，该网关作为 Citrix DaaS 环境中的虚拟应用程序和桌面环境的前端。

图 2. 将 Citrix Gateway 服务作为 HDX 代理的部署



此功能现已包含在您的 Citrix DaaS 和 Workspace 服务授权中。您可以启用此功能。

从本地 NetScaler Gateway 迁移到基于云的 Citrix Gateway 服务

NetScaler Gateway 设备由客户管理，而基于云的 Citrix Gateway 服务由 Citrix 管理。本节介绍如何将本地 NetScaler Gateway 迁移到云托管的 Citrix Gateway 服务以用于 HDX 代理。尽管 NetScaler Gateway 和 Citrix Gateway 服务都提供 HDX 代理，但底层基础架构和工作机制不同。但是，在云上启用 HDX 代理的步骤非常简单，只需点击几下即可完成。

要启用此迁移，请为 Citrix DaaS 启用 Citrix Gateway 服务。启用后，流量将开始通过 Citrix Gateway 服务传输，不再需要本地 NetScaler Gateway。

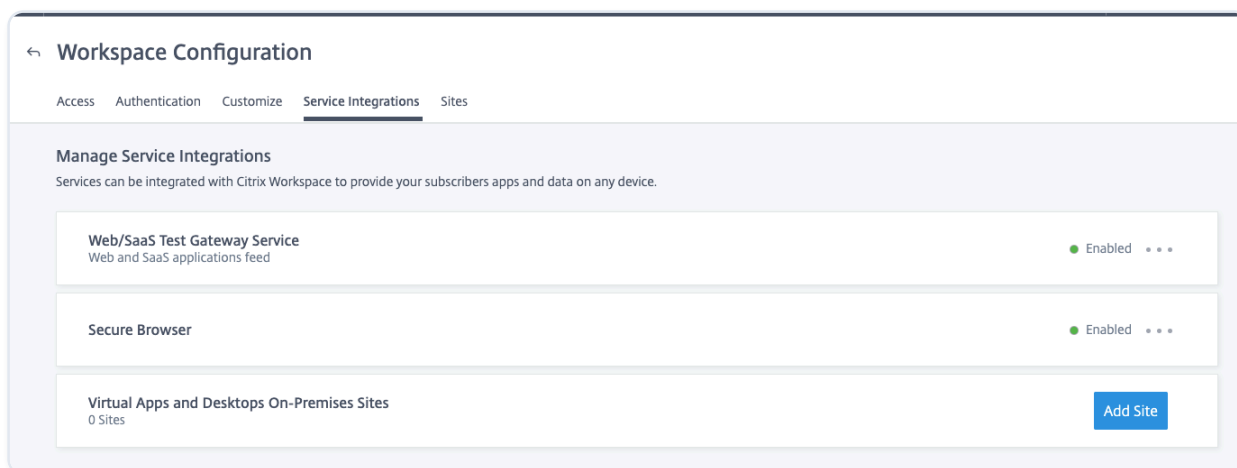
在开始从本地 NetScaler Gateway 迁移到基于云的 Citrix Gateway 服务之前，请注意以下假设。

- 客户已订阅 Citrix Cloud Service 并购买了 Citrix DaaS。
- 客户使用本地 Active Directory 在云上对用户进行身份验证。

启用 Citrix Gateway 服务

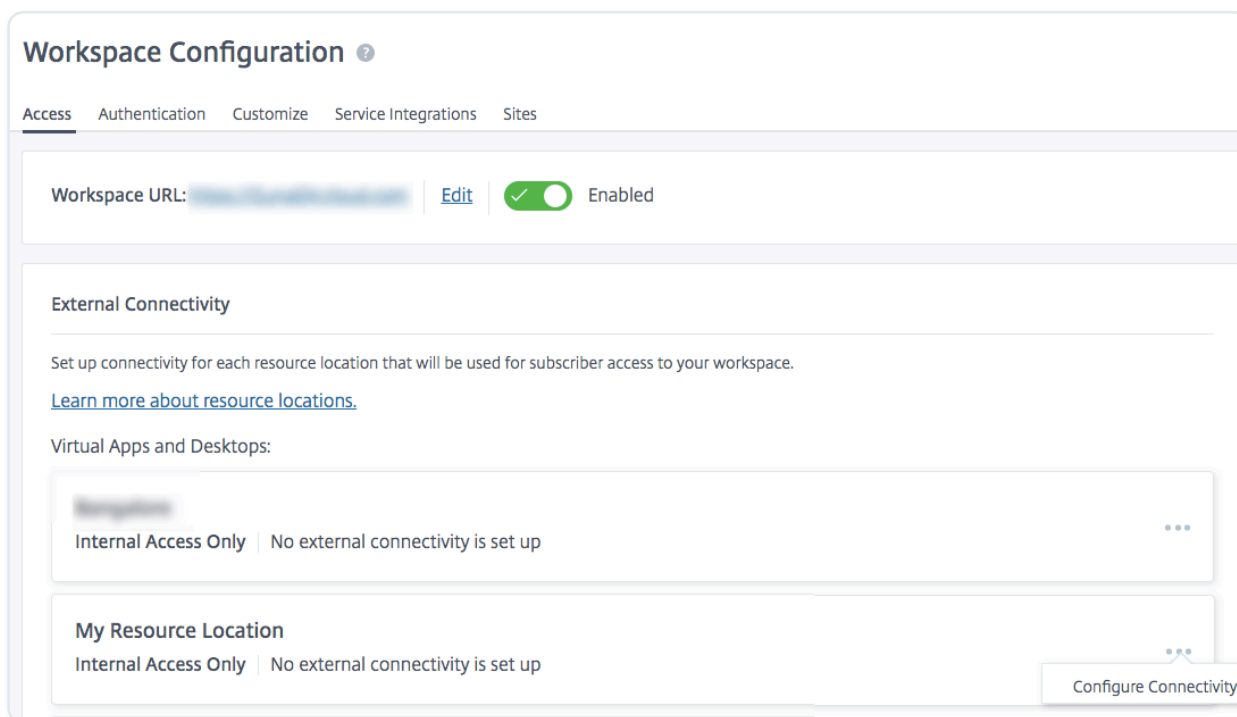
以下是为 Citrix DaaS 用户启用 Citrix Gateway 服务的步骤：

1. 以管理员用户身份登录 Citrix Cloud Services。
2. 单击汉堡图标，然后选择 **Workspace Configuration**。
3. 单击 **服务集成**。
4. 找到 **Gateway** 旁边的省略号，单击省略号，然后单击 **Enable**。



以下是为 Citrix Workspace 用户启用 Citrix Gateway 服务的步骤。

1. 以管理员用户身份登录 Citrix Cloud Services。
2. 单击汉堡图标，然后选择 **Workspace Configuration**。
3. 在 **Access** 选项卡中，在 **External Connectivity** 部分下，找到 **Citrix DaaS** 下 **My Resource Location** 旁边的省略号。
4. 单击省略号，然后单击 **Configure Connectivity**。



5. 在弹出窗口中选择 **Citrix Gateway service**，然后单击 **Save**。

Configure Connectivity

Connectivity Type

☐ Traditional Gateway

☒ Gateway Service

☐ Internal Only | No external connectivity is set up

CancelSave

回滚到 NetScaler Gateway

要将 HDX 代理回滚到本地 NetScaler Gateway，请执行以下操作。

1. 以管理员用户身份登录 Citrix Cloud Services。
2. 单击左上角的汉堡图标，然后选择 **Workspace Configuration**。
3. 在 **External Connectivity** 部分下的 **Access** 选项卡中，找到 **Citrix DaaS** 下 **My Resource Location** 旁边的省略号。

Workspace Configuration ?

Access Authentication Customize Service Integrations Sites

Workspace URL: [Edit](#) ☒ Enabled

External Connectivity

Set up connectivity for each resource location that will be used for subscriber access to your workspace.
[Learn more about resource locations.](#)

Virtual Apps and Desktops:

Internal Access Only | No external connectivity is set up

My Resource Location
Internal Access Only | No external connectivity is set up

[Configure Connectivity](#)

- 单击省略号，然后单击 **Configure Connectivity**。
- 选择 **Traditional Gateway** 并输入 FQDN。

Configure Connectivity

Connectivity Type

☒ Traditional Gateway

☐ Gateway Service

☐ Internal Only | No external connectivity is set up

- 单击 **Add**，然后单击 **Save**。

HDX 自适应传输，支持 Citrix Gateway 服务中的 EDT

Enlightened Data Transport (EDT) 是 Citrix 专有的传输协议，构建于 UDP 之上。EDT 在具有挑战性的长距离连接上提供卓越的用户体验，同时保持服务器可伸缩性。自适应传输是 Citrix Virtual Apps and Desktops 的数据传输机制。自适应传输提供了使用 EDT 作为 ICA 传输协议的能力，并在 EDT 不可用时切换到 TCP。有关自适应传输和 EDT 的更多信息，请参阅[自适应传输文档](#)。

必备条件

- 思杰 DaaS
- Virtual Delivery Agent (VDA) 2012 或更高版本
- Citrix Workspace 应用程序
 - Windows：版本 1912 或更高版本（建议使用 2105 或更高版本）
 - Linux：版本 1912 或更高版本（建议使用 2104 或更高版本）
 - Mac：版本 1912 或更高版本
 - iOS：Apple App Store 中提供的最新版本
 - Android：Google Play 中提供的最新版本
- 必须允许 UDP 端口 443 用于从 VDA 到 Citrix Gateway 服务的出站流量
- 必须启用并运行 Rendezvous 协议。有关详细信息，请参阅[Rendezvous 协议文档](#)。
- 确保已启用自适应传输。有关详细信息，请参阅[自适应传输设置文档](#)。
- 有关自适应传输和 EDT 的更多信息，请参阅[自适应传输文档](#)。

考虑事项

以下是使用 EDT 与 Citrix Gateway 服务时的一些考虑事项。

- 强烈建议启用 EDT MTU 发现。有关详细信息，请参阅[自适应传输文档](#)。
- 仅在使用 Rendezvous 时，EDT 才可与 Citrix Gateway 服务配合使用。如果 HDX 会话通过 Cloud Connector 进行代理，则只有 TCP 可用于数据传输。

- 当 EDT 会话建立失败时，会话将回退到 TCP，从而导致会话启动时间增加。
- 如果您希望继续通过 Cloud Connector 代理 HDX™ 会话，请考虑通过 Citrix Studio 策略禁用自适应传输，以避免回退序列可能导致的会话启动时间增加。
- Citrix 建议仅在运行 Windows 10 和 Windows Server 2019 的 VDA 上通过 Citrix Gateway 服务使用 EDT。Windows Server 2012 R2 和 2016 存在限制，不允许 DTLS 加密会话的 MTU 大于 1024，这可能会影响性能和用户体验。
- 使用自适应传输时，Citrix Gateway 服务不支持 UDP 音频。

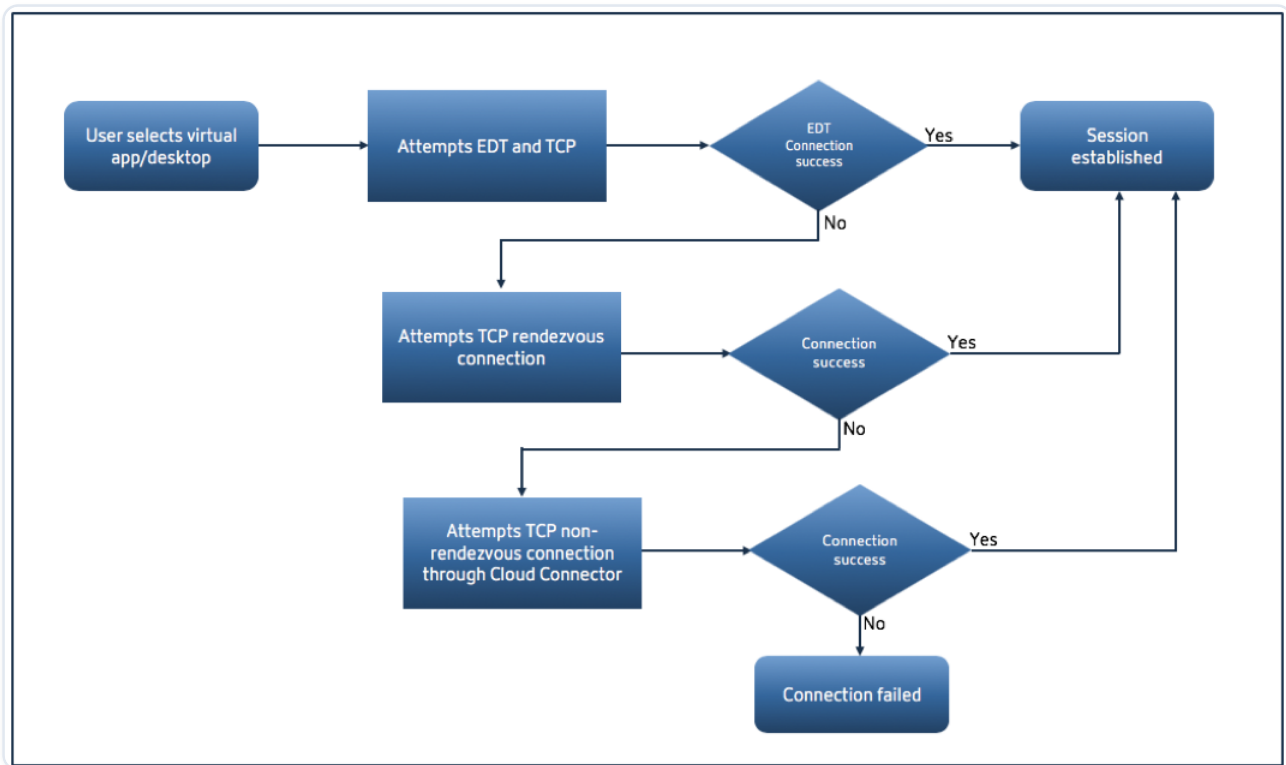
传输协议验证

要了解您的会话是否正在使用 EDT，请参阅以下内容：

- Citrix Director 中的连接协议：[<https://support.citrix.com/article/CTX220730>](https://support.citrix.com/article/CTX220730)。
- 启动应用程序或桌面后，转至 **Citrix Workspace 应用程序 > 连接中心**，选择相应的会话，单击 **属性**，然后查看“传输加密”属性。如果显示 DTLS，则会话正在使用 EDT 进行传输。如果显示 TLS，则会话正在使用 TCP 进行传输。
- 如果您启动了桌面，可以打开 PowerShell 或命令提示符并运行 `"ctxsession -v"`。“传输协议”属性显示正在使用的连接方法：
 - EDT 会合: **"UDP > DTLS > CGP > ICA®"**
 - TCP 会合: **"TCP > SSL > CGP > ICA"**
 - 通过云连接器代理: **"TCP > CGP > ICA"**

连接回退

如果 EDT 协商因任何原因失败，会话将回退到使用 Rendezvous 的 TCP。如果再次失败，则会话将回退到通过云连接器进行代理。



EDT MTU 发现

强烈建议启用 EDT MTU 发现，以确保每个会话都使用该连接的最佳 MTU。

如果 EDT MTU 发现被禁用或用户的客户端不支持此功能，EDT MTU 将自动设置为 1380，以避免与分段相关的问题。

用户可能会通过需要低于 1380 的 MTU 的网络进行连接，这主要出现在移动网络（3G、4G）或 VPN 连接中。如果您的环境中出现这种情况，并且用户使用的客户端不支持 EDT MTU 发现，Citrix 建议您禁用自适应传输，直到该功能在您的目标客户端平台上可用。

有关 EDT MTU 发现的更多详细信息，请参阅 [自适应传输文档](#)。

故障排除

以下提供了一些常规故障排除指南。

会话已连接但未使用 EDT：

1. 如果会话通过云连接器进行代理，请确保 Rendezvous 已启用并正常工作，因为这是将 EDT 与 Citrix Gateway 服务结合使用的先决条件。有关详细信息，请参阅 [Rendezvous 文档](#)。
2. 如果会话使用 TCP Rendezvous：
 - 确保您使用的是 VDA 2012 或更高版本。

- 检查 Citrix 策略中是否启用了自适应传输。
- 确保已设置适当的防火墙规则，以从 VDA 计算机到 Citrix Gateway 服务打开 UDP 443。有关更多详细信息，请参阅 [Rendezvous\]\(/zh-cn/citrix-virtual-apps-desktops-service/hdx/rendezvous-protocol.html\) 文档](#)。
- 如果 VDA 计算机中启用了本地防火墙（例如 Windows Defender 防火墙），请确保没有规则阻止 UDP 443。
- 如果使用代理，则只有 SOCKS5 代理可用于代理 EDT。有关详细信息，请参阅 [Rendezvous 文档](#)。

会话通过 EDT 连接，但一段时间后随机断开连接：

1. 确保您使用的是 VDA 2012 或更高版本。

会话连接失败：

1. 确保您使用的是 VDA 2012 或更高版本。
2. 如果使用支持 EDT MTU 发现的客户端，请确保已启用 EDT MTU 发现。这有助于缓解与分段相关的问题。有关详细信息，请参阅 [自适应传输文档](#)。
3. 如果使用 Linux 或 Android 客户端：
 - 检查 Windows 或 Mac 客户端是否正常工作。
 - 检查 CWA 版本是否已升级到 Linux 2104、Android 21.5.0 或更高版本。
 - 如果您使用的是旧版 CWA，请禁用自适应传输并确保 TCP Rendezvous 正常工作。
 - 一旦 TCP Rendezvous 正常工作，如果在重新启用自适应传输后会话连接失败，请参阅步骤 **会话已连接但未使用 EDT > 如果会话正在使用 TCP Rendezvous** 中提到的故障排除步骤。

Citrix Gateway 服务网络指标监控

Citrix Gateway 服务网络指标监控使管理员能够查看会话详细信息、延迟分解和其他关键网络指标。这有助于对 HDX 会话进行有效的故障排除和修复，包括跨跃点的延迟分解，这是以前客户无法获得的功能。网络指标为管理员提供了对 Citrix Workspace 应用程序、虚拟投递代理 (VDA) 和 Citrix Gateway 服务之间流动的 HDX 流量的完整可见性。

支持的平台和版本

下表列出了支持网络指标监控的平台和版本：

组件	平台	支持的版本
Citrix Workspace 应用程序	视窗	2411 或更高版本
思杰虚拟应用和桌面	视窗	2411 或更高版本

先决条件

- 管理员必须在 Citrix Studio 或 Web Studio 中启用 **网络遥测** 策略。有关详细信息，请参阅 [创建策略](#)。

Citrix Studio 中的网络遥测策略(/en-us/citrix-gateway-service/media/network-telemetry-policy.png)

在 DaaS Monitor 中监控 Citrix Gateway 服务网络指标

在 DaaS Monitor 中，**会话性能**选项卡提供网络指标的可视化表示，使管理员能够访问实时延迟数据、历史报告和全面的性能洞察，以便进行故障排除。实时和历史数据的可用性支持使用 Citrix Gateway 服务的客户的各种用例。有关详细信息，请参阅[诊断会话性能问题](#)。

DaaS Monitor 中的网络指标监控(/en-us/citrix-gateway-service/media/network-telemetry-monitor.png)

使用网络指标排查性能问题

下表列出了管理员可以在 DaaS Monitor 中监控以诊断性能问题的网络指标。

网络指标	描述
客户端重传	指示 PoP 与用户端点之间重传的数据包数量。此指标值较高表示带宽利用率高或链路存在问题。
ICA® RTT	高 RTT 表示网络拥塞或距离相关的延迟，并影响用户体验。
抖动	高抖动会导致应用程序性能和流畅性不稳定。
L4 指标	有关 L4 指标列表，请参阅 当前/已终止会话报告 。
第 4 层客户端-PoP 延迟	指示会话中哪个网络跃点导致了最大的延迟，从而帮助管理员更专注于该区域。
第 4 层 PoP-服务器延迟	同上
L7 客户端延迟	指示 L7 层延迟（应用程序级处理时间，OSI 模型上的第七层），通过 Citrix Workspace™ 应用程序与客户端主机之间发送的 ICA 探测和响应进行测量。
L7 服务器延迟	指示 L7 层延迟（应用程序级处理时间，OSI 模型上的第七层），通过 Citrix Workspace 应用程序与服务器端主机之间发送的 ICA 探测和响应进行测量。
网络延迟	指示网络延迟的细分，可与 ICA 延迟和 ICA RTT 进行比较，以隔离问题。

网络指标	描述
QoS	指示数据包丢失的百分比。即使少量丢失也会显著降低性能。
服务器端重传	指示 PoP 与后端服务器 (VDA) 之间重传的数据包数量。此指标值较高表示数据中心内存在网络问题。 注意： 仅在会合时，VDA 可能会出现服务器重传。
吞吐量 (bps)	指示所使用的网络带宽。高利用率表示拥塞和瓶颈。

优势

网络指标的可视化表示提供了以下优势，有助于管理员有效排查 HDX™ 会话中的问题：

- 缩短平均解决时间 (MTTR)。
- 通过最大限度地减少升级来降低支持成本。
- 统一的 HDX 会话性能故障排除体验。

主要功能

- **全面洞察：** 管理员会收到详细的网络指标，有助于分析、明智决策和主动解决问题。
- **L7 延迟监控：** 为了改进网络诊断，增强的网络指标监控允许 Citrix Gateway 服务计算以下每个跃点的 L7 延迟：
 - 从 Citrix Workspace 到 Citrix Gateway 服务的第一个跃点或前端跃点。
 - 从 Citrix Gateway 服务到 VDA 的第二个跃点或后端跃点。

L7 延迟监控使管理员能够通过监控应用程序级处理时间来识别和解决性能问题。

- **传输层独立性：** Citrix Gateway 服务的网络指标监控始终独立于所使用的传输层（TCP 和 EDT）而发生。
- **数据安全：** TLS/DTLS 加密确保网络指标通过互联网安全传输，从而维护机密性和完整性。

谷歌云平台上的思杰网关服务

借助 Google Cloud Platform (GCP) 上的 Citrix Gateway 服务支持，在 Google Cloud 上运行工作负载的客户可以利用 Google Cloud 的高性能全球网络，使用 Citrix Gateway 优化路由功能。优化网关路由功能将客户端定向到最近的 GCP Citrix Gateway 服务 POP。此外，Google Cloud 上的 Citrix Gateway 服务在 Citrix Workspace 客户端和虚拟化资源之间提供安全的连接，以最低的延迟和最佳的用户体验交付会话。

目前，适用于 GCP 的 Citrix Gateway 服务在以下区域可用。

- 美国
 - 洛杉矶
 - 俄勒冈
 - 南卡罗来纳
- 欧洲
 - 伦敦
 - 苏黎世

注意：

- GCP POP 仅适用于已从 Google Cloud Marketplace 购买订阅并在 Google Cloud 上运行其工作负载的 Citrix DaaS 客户。
- Citrix Gateway 服务帐户 - 有权使用 Citrix DaaS 的客户默认会启用 Citrix Gateway 服务。客户无需申请单独的 Citrix Gateway 服务试用版。有关详细信息，请参阅 [注册服务](#)。

先决条件

- Citrix Cloud 帐户。有关详细信息，请参阅 [注册 Citrix Cloud](#)。

Citrix Gateway 服务支持的功能

以下是 Citrix Gateway 服务为 GCP 支持的一些功能。

TCP HDX™ 代理 - 目前，仅支持 TCP HDX 代理。Virtual Apps and Desktops 启动仅通过 TCP 协议支持。

Rendezvous V1 - 使用 Citrix Gateway 服务时，Rendezvous 协议版本 V1 允许 VDA 绕过 Citrix Cloud Connectors 直接连接到网关 POP 以进行数据路径流量。有关详细信息，请参阅 [Rendezvous V1](#)。

Rendezvous V2 - Rendezvous 协议版本 V2 支持绕过 Citrix Cloud Connectors 进行控制流量和 HDX 会话流量。有关详细信息，请参阅 [Rendezvous V2](#)。

重要提示：

尚未为 GCP 启用 EDT 支持。

如何启用 Citrix Gateway 服务

默认情况下，有权使用 Citrix DaaS 的客户将启用 Citrix Gateway 服务。客户无需申请单独的 Citrix Gateway 服务试用。有关详细信息，请参阅 [注册服务](#)。

限制

目前，GCP 仅在美国和欧洲地区可用。来自其他地区的 GCP 客户可能会遇到高延迟问题。

参考

- Citrix Cloud Connector 连接要求 – 有关详细信息，请参阅 [Cloud Connector 常见服务连接要求](#)。
- Cloud Connectors 的规模和大小注意事项。有关详细信息，请参阅 [Cloud Connectors 的规模和大小注意事项](#)。

支持 Citrix 虚拟应用和桌面

Citrix Gateway 服务为用户提供对 Citrix Virtual Apps and Desktops 的安全访问，支持各种设备，包括笔记本电脑、台式机、瘦客户端、平板电脑和智能手机。

Citrix Gateway 服务支持对 Citrix Virtual Apps and Desktops 进行安全的远程访问，无需在 DMZ 中部署 NetScaler Gateway 或重新配置防火墙。使用 Citrix Gateway 的所有基础设施开销都转移到云端，并由 Citrix 托管。

您可以在 Citrix Cloud 中启用 Citrix Gateway 服务。启用该服务后，用户可以从其网络外部访问其 VDA，如下图所示。

Citrix 虚拟应用和桌面和 CGS(/en-us/citrix-gateway-service/media/xaxd_1_new.png)

工作原理

用户的端点及其本地托管的资源 VDA 通过 Citrix Cloud Connectors 连接到各自最近的 POP。随后，当用户从其 Workspace 应用程序中选择要启动的虚拟应用程序或桌面时，托管该连接的最近 POP 会识别相关的资源位置，并指示其与该 POP 建立 Citrix Cloud Connector 会话，从而形成端到端连接，然后建立虚拟会话。

- 会话通过 Citrix Gateway 服务在云合作伙伴的 WAN 之间连接。
- VDA 和 Workspace 端点在离用户最近的 Citrix Gateway 服务 POP 处汇合。
- 高质量会话。

有关更多详细信息，请参阅 [适用于 HDX 代理的 Citrix Gateway 服务](#)

适用于 StoreFront 的 Citrix Gateway 服务

重要信息：

- 适用于 StoreFront 的 Citrix Gateway 服务在 Citrix DaaS 环境和本地 Citrix Virtual Apps and Desktops 中可用。
- 本文档介绍了在您倾向于使用本地 NetScaler Gateway 进行身份验证和本地 StoreFront 进行枚举的场景中，部署适用于 StoreFront 的 Citrix Gateway 服务可执行的步骤。
- 适用于 StoreFront 的 Citrix Gateway 服务不支持在 [Citrix Cloud Japan](#) 和 [Citrix Cloud Government](#) 环境中使用。

概述

适用于 StoreFront 的 Citrix Gateway 服务是一种基于云的 HDX 解决方案，可为从本地 StoreFront 访问的资源提供安全的远程访问。您可以在不更改本地 StoreFront 和本地 NetScaler Gateway 环境的情况下，利用 Citrix Cloud（用于 HDX 代理）的可扩展性和可靠性。

假设您是 Citrix DaaS 客户，使用本地 StoreFront 作为企业应用程序商店，并使用本地 NetScaler Gateway 进行远程访问。如果您正在寻找一种利用云托管远程访问解决方案（HDX 代理）的选项，同时将本地 StoreFront 作为用户门户，并使用本地 NetScaler Gateway 进行身份验证，那么适用于 StoreFront 的 Citrix Gateway 服务就是您的理想选择。

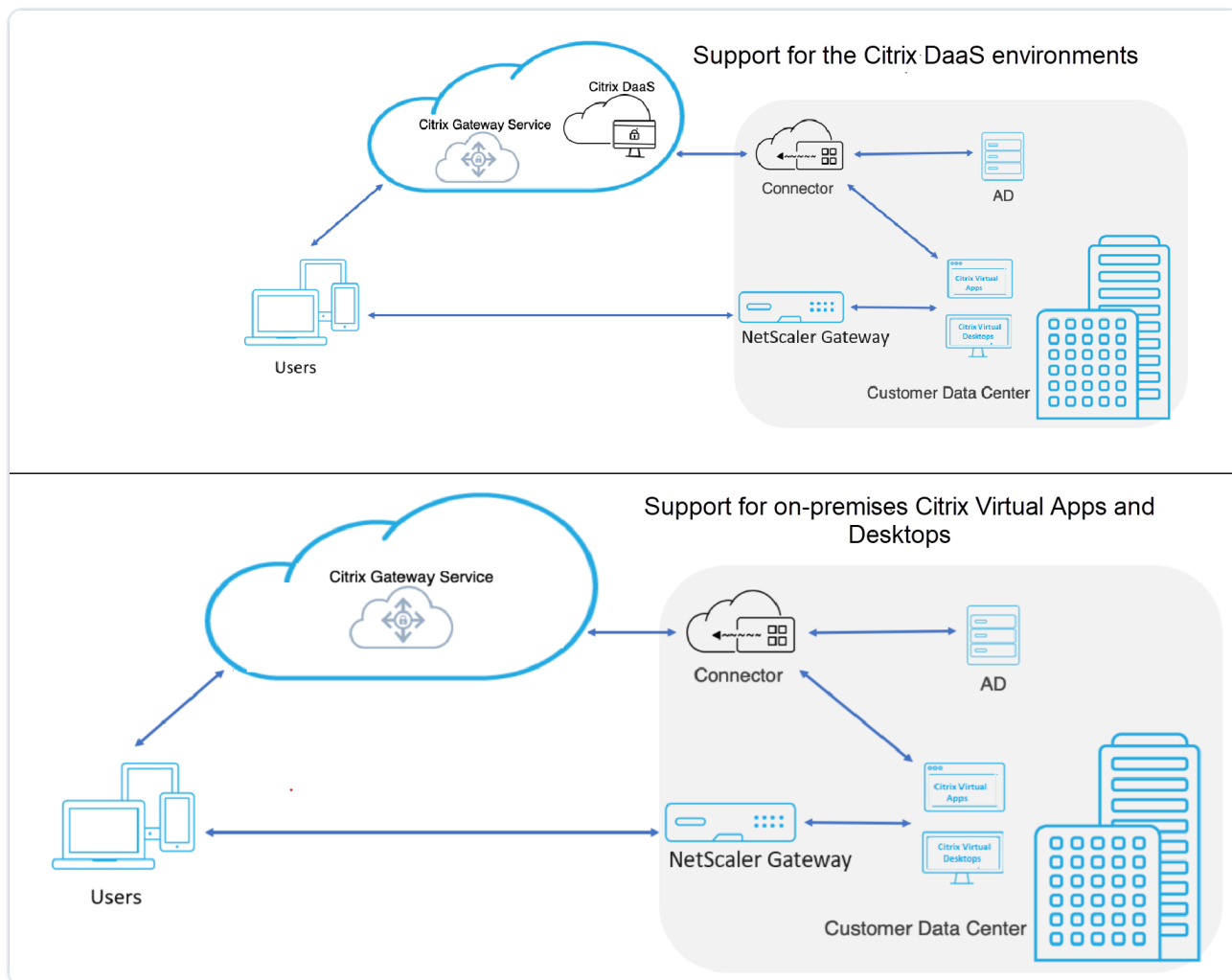
Citrix Gateway 服务使用您资源位置中基于 Windows 的 Cloud Connector 处理 HDX 代理启动。

适用于 StoreFront 的 Citrix Gateway 服务支持以下用例：

- [通过 TCP/EDT 的 HDX](#)
- [用于弹性的本地主机缓存 \(LHC\)](#)
- [Rendezvous 版本 1](#)

不支持以下用例：

- 非 HDX™ 用例，例如 RDP 代理、VPN、PC over IP (PCoIP)。



优势

- Citrix DaaS 客户可以使用其现有的本地 NetScaler Gateway URL。
- 由于 Citrix Gateway 服务的多云和多地理区域架构，可确保高弹性。
- HDX 代理性能和规模要求现在由 Citrix Gateway 服务管理。它们不再由客户管理。

必备条件

- 使用 NetScaler 13.1 或更高版本。有关详细信息，请参阅 [NetScaler 文档](#)。
- 要在 Citrix DaaS 环境中使用适用于 StoreFront 的 Citrix Gateway 服务，请使用本地 StoreFront 2407 或更高版本。对于地理位置路由，请使用 StoreFront 2503 或更高版本。有关详细信息，请参阅 [StoreFront 系统要求](#)。
- 要在本地 Citrix Virtual Apps and Desktops 中使用适用于 StoreFront 的 Citrix Gateway 服务，请使用 Citrix Virtual Apps and Desktops 2503 或更高版本。
- 加入 [Citrix Cloud](#) 并安装 [Citrix Cloud Connector](#)（用于 Citrix DaaS 中断的桌面交付控制器。用于票证的 STA）。

您可以使用现有 Cloud Connector 或部署新的 Cloud Connector。如果您的连接器升级被禁用，请联系 [支持](#) 以启用它。

有关 Citrix Cloud Connector 要求的详细信息，请参阅 [Citrix Cloud Connector 要求](#)。有关大小调整要求的详细信息，请参阅 [Cloud Connector 的大小和规模注意事项](#)。

注意：

仅支持基于 Windows 的 Cloud Connector。不支持 Connector Appliance。

使用本地主机缓存 (LHC) 实现弹性

本地主机缓存 (LHC) 是 Citrix DaaS 的一项功能，它允许用户在云连接器与 Citrix Cloud 失去连接时继续访问应用程序和桌面。

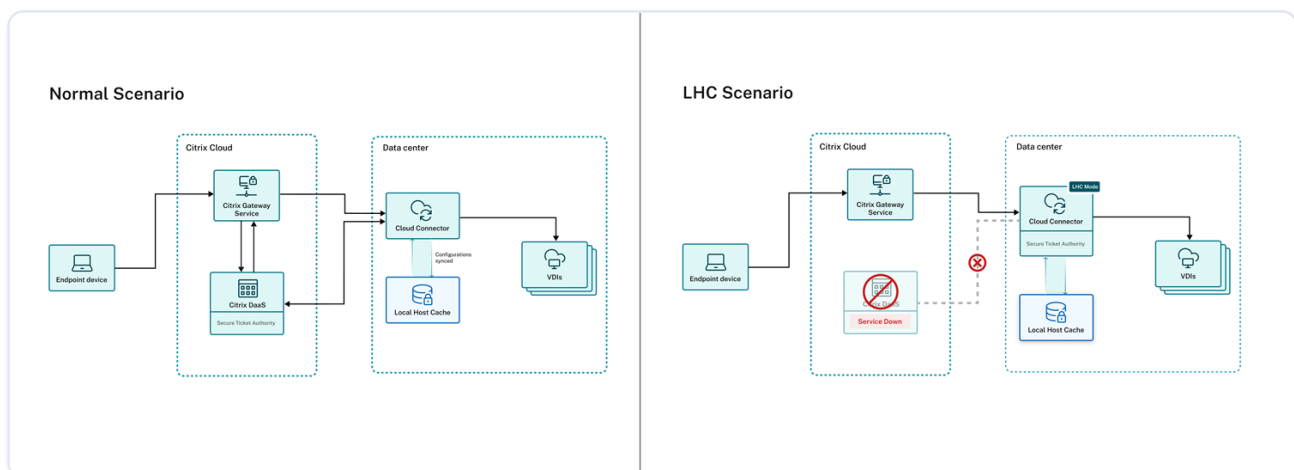
将网关服务与 StoreFront 结合使用时，STA 票证交换行为在正常工作模式和 LHC 模式下有所不同。

- 正常工作时，STA 票证从 Citrix Cloud 中托管的票证服务兑换。
- 在 LHC 模式下，STA 票证从云连接器兑换。

注意：

云连接器必须在 LHC 模式下与网关服务保持连接才能兑换 STA 票证。如果连接器无法与网关服务通信，则在 LHC 模式下启动会失败。

下图说明了在正常工作场景和 LHC 模式下，适用于 StoreFront 部署的 Citrix Gateway 服务中 STA 票证交换的工作方式。



参考

- [适用于 StoreFront 部署的 Citrix Gateway 服务 - 技术专区文章](#)
- [适用于 StoreFront 的 Citrix Gateway 服务 - GA 博客](#)
- [思杰云连接器要求](#)
- [Citrix DaaS 的本地主机缓存支持](#)
- [启动 ICA 文件日志记录](#)
- [会话启动](#)
- [支持](#)

已知问题和限制

- 如果您选择了适用于 StoreFront 2311 或 2402 的 Citrix Gateway service for StoreFront 预览版，并且您已配置了 HDX 实例的网关服务，则该配置在 StoreFront 2407 中将失效。请删除现有网关实例并创建新实例。

即将推出的增强功能

以下增强功能计划在即将发布的版本中推出：

- 会话性能 - L7 延迟细分

常见问题

什么是适用于 StoreFront 的 Citrix Gateway 服务？

适用于 StoreFront 的 Citrix Gateway 服务是一种基于云的 HDX 解决方案。它使客户能够维护其现有的访问层和身份验证基础架构（NetScaler 和 StoreFront），同时利用基于云的 HDX 代理解决方案（Citrix Gateway 服务）的优势。

使用适用于 StoreFront 的 Citrix Gateway 服务有哪些优势？

优势包括以下几点：

- 灵活性：您可以保留现有的 Citrix NetScaler 和 StoreFront 服务器。Citrix Gateway 服务与这些组件无缝集成，以实现虚拟应用程序和桌面的访问。
- 可扩展性：由于 Citrix Gateway 服务托管在云中，因此可以根据需要轻松进行扩展或缩减。

适用于 StoreFront 的 Citrix Gateway 服务是完全托管的服务吗？

否，适用于 StoreFront 的 Citrix Gateway 服务是一种解决方案，可帮助将 HDX 代理从客户管理的 NetScaler 卸载到 Citrix 管理的网关服务。

我需要重新架构我的访问层才能使用适用于 StoreFront 的 Citrix Gateway 服务吗？

不需要，适用于 StoreFront 的 Citrix Gateway 服务允许您维护现有的访问层和身份验证基础架构。

采取了哪些安全措施来保护我的数据和应用程序？

适用于 StoreFront 的 Citrix Gateway 服务采用强大的安全措施，以确保您的数据和应用程序的安全性和完整性。请参阅 [技术安全](#)。

适用于 StoreFront 的 Citrix Gateway 服务如何处理可扩展性和高流量？

适用于 StoreFront 的 Citrix Gateway 服务旨在处理高流量并扩展以满足大型企业的需求，确保不间断地访问应用程序和数据。请参阅 [CGS PoPs](#)。

适用于 StoreFront 的 Citrix Gateway 服务有哪些支持选项？

Citrix 提供全面的支持选项，包括文档、培训和技术支持，以确保适用于 StoreFront 的 Citrix Gateway 服务成功部署和运行。

我可以使用适用于 StoreFront 的 Citrix Gateway 服务与其他 Citrix 产品和服务吗？

是的，适用于 StoreFront 的 Citrix Gateway 服务旨在与其他 Citrix 产品和服务无缝集成，包括 Citrix Workspace、Citrix Virtual Apps and Desktops 和 Citrix Hypervisor。

适用于 StoreFront 的 Citrix Gateway 服务如何许可和定价？

所有 Universal HMC、CPL 和现有 DaaS 客户都有权使用适用于 StoreFront 的 Citrix Gateway 服务。

我还需要将 CVAD 组件升级到 2407 或更高版本吗？

不需要，无需将 CVAD 组件升级到 2407。只需将 StoreFront 升级到 2407 即可。

DaaS 客户与本地 CVAD 站点：解决方案的即时使用？

未来的增强功能将包括对拥有独立 Citrix Virtual Apps and Desktops 站点以及其 Citrix DaaS 部署的客户的支​​持。这将有助于卸载本地站点的 HDX 代理，并确保整个部署的一致性。

对 Citrix DaaS 环境的支持

StoreFront 的 Citrix Gateway 服务支持 Citrix DaaS 环境。假定您已拥有本地 NetScaler Gateway。您可以继续使用相同的网关进行身份验证和远程访问您的 StoreFront 商店。您还可以使用相同的网关为部分资源提供 HDX 路由，例如 Citrix Gateway 服务不支持的 Citrix DaaS 部署所托管的资源。有关配置 NetScaler Gateway 的更多详细信息，请参阅 [StoreFront 文档](#)。

要为部分或所有资源配置用于 HDX 路由的 Citrix Gateway 服务，请在 StoreFront 中创建网关，然后使用 StoreFront 的“最佳网关路由”功能配置何时使用它：

1. 在 StoreFront 中配置类型为 **Citrix Gateway Service** 的网关。通常，单个网关就足够了。但是，如果您希望对不同的站点或区域使用不同的地理位置规则，则可以配置具有不同网关服务 URL 的多个网关。有关详细信息，请参阅 [添加 Citrix Gateway 服务](#)。

Add Citrix Gateway

StoreFront

General settings
Cloud Connectors
Summary

General Settings

Complete these settings to configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

Display name:

Gateway type:

Usage or role:

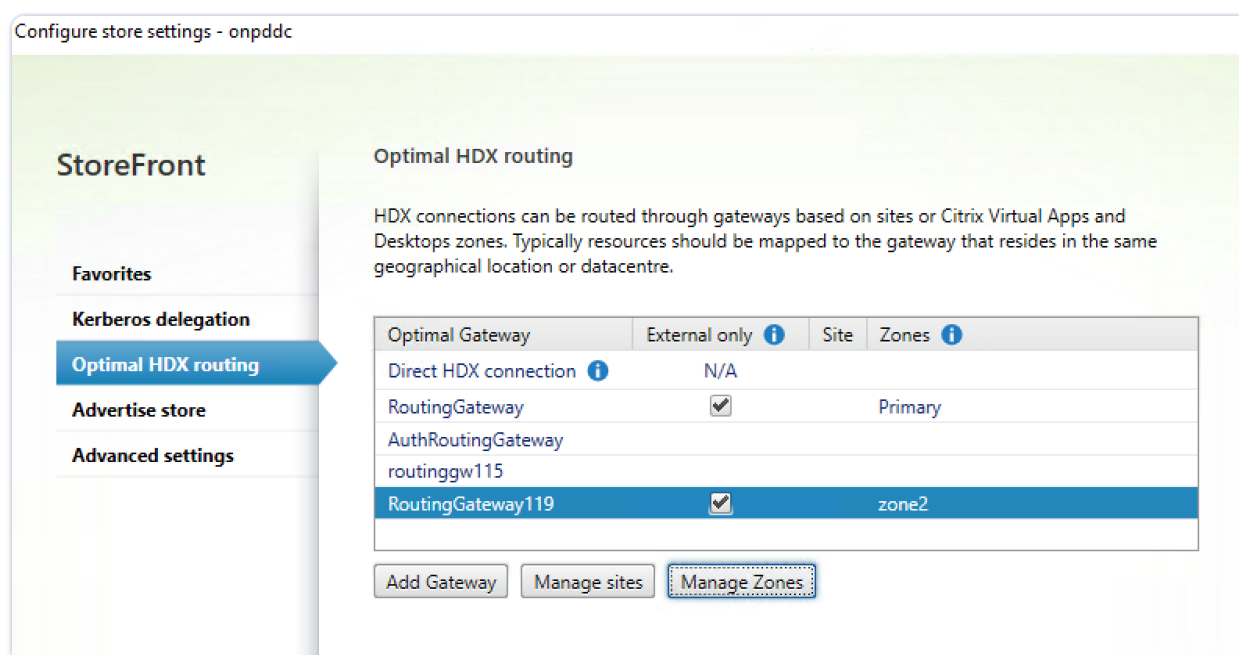
Citrix Gateway Service URL:

Citrix Gateway Service URL (STA Connector Mode):

For a list of available Citrix Gateway Service URLs, see [documentation](#)

Next **Cancel**

2. 选择希望 HDX 连接通过这些网关路由的站点或区域。有关详细信息，请参阅 [最佳 HDX 路由](#)。



对本地 Citrix Virtual Apps and Desktops 的支持

Citrix Gateway 服务可与 StoreFront 和 Citrix Virtual Apps and Desktops 的本地部署结合使用。您可以继续使用本地 NetScaler Gateway 和 StoreFront 进行身份验证、授权和枚举。Citrix Gateway 服务用于为所有或部分区域启动虚拟应用程序和桌面。这种方法最大限度地发挥了现有远程访问基础设施的价值，并最大限度地减少了管理工作。这对于为没有 StoreFront 服务器的卫星位置中的工作负载提供远程访问特别有用，从而完全消除了在该位置对 NetScaler Gateway 的需求。

主要优势

Citrix Gateway 服务与本地站点的集成提供了以下优势：

- **保留自定义设置：** 可以保留 NetScaler Gateway 和 StoreFront™ 的自定义设置，从而确保一致的用户体验。
- **最大限度地减少维护：** HDX 代理的性能和规模要求现在由 Citrix Gateway 服务管理，无需客户进行管理。
- **现有 URL：** DaaS 客户可以继续使用他们熟悉的本地 NetScaler® Gateway URL。
- **利用 LHC 增强弹性：** 本地主机缓存 (LHC) 通过允许连接器在中断期间充当本地安全票证颁发机构 (STA) 来支持弹性需求。
- **更好的用户体验：** 能够使用地理位置更近的 PoP 可减少延迟并提高性能。
- **高弹性：** 由于 Citrix Gateway 服务的多云和多地理架构，确保了高弹性。

先决条件

1. 您必须拥有一个功能正常的本地工作环境，其中 NetScaler Gateway 用于身份验证和授权，StoreFront 用于枚举。
2. 将 StoreFront 升级到版本 2503 或更高版本。有关详细信息，请参阅 [升级 StoreFront](#)。

在 Citrix Cloud™ 上创建资源位置

1. 加入 Citrix Cloud。有关详细信息，请参阅 [创建 Citrix Cloud 帐户](#) 和 [连接到 Citrix Cloud](#)。
2. 在 Citrix Cloud 上，安装 Cloud Connector 并将其与资源位置关联。有关详细信息，请参阅 [Cloud Connector 安装](#)。

注意：

要使现有应用程序和桌面可供订阅者使用，请将您的站点（Citrix Virtual Apps and Desktops 部署）添加到 Citrix Workspace。有关详细信息，请参阅 [在工作区中聚合 Virtual Apps and Desktops](#)。

在本地 Delivery Controller™ 上配置资源位置和策略

1. 在 Windows Active Directory (AD) 或域控制器 (DC) 服务器上运行以下命令，以检索 Windows AD 或 DC 环境中连接器计算机的安全标识符 (SID)。记下连接器计算机的 SID。

```
Get-ADComputer -Filter * | Select-Object Name, SID
```

2. 在本地 Delivery Controller 中，创建一个区域并将其映射到在 Citrix Cloud 中创建的资源位置。
 - a. 在本地 Delivery Controller 中，在 PowerShell 中运行以下命令，并记下为所需资源位置生成的 Uid：

```
Get-ConfigZone
```

- b. 为所有 Citrix Cloud Connector 运行以下命令：

```
Set-ConfigZone -Uid <Uid from above command output> -ExternalUid <RL ID noted at step 1>
```

```
new-configedgeserver <User friendly name> -MachineAddress
```

```
"<Connector FQDN"> -Sid <Connector respective SID from step 2> -uuid  
<Respective Edge server UUID from step 1> -ZoneUid <Uid from Get-  
ConfigZone output>
```

3. 要使用 Rendezvous v1，请在 Delivery Controller 策略中启用 Rendezvous，并确保本地 Delivery Controller 已配置连接器详细信息以接受 Rendezvous 请求。有关详细信息，请参阅 [Rendezvous v1](#)。
4. 要在 EDT 中使用 HDX 自适应传输，请在本地 Delivery Controller 的 Delivery Controller 策略中启用自适应传输协议。有关详细信息，请参阅 [支持 Citrix Gateway 服务的 HDX 自适应传输与 EDT](#)。

配置 StoreFront 以使用 Citrix Gateway 服务进行 HDX 路由

要远程访问 StoreFront，您必须继续使用现有的 NetScaler 网关。您还可以使用 NetScaler 网关远程访问某些资源，例如与 NetScaler 网关位于同一数据中心的资源。有关在 StoreFront 中配置 NetScaler 网关以进行身份验证的详细信息，请参阅 [配置 Citrix 网关](#)。

要为部分或所有资源配置用于 HDX 路由的 Citrix Gateway 服务，请在 StoreFront 中创建一个网关，然后使用 StoreFront 的最佳网关路由功能来配置何时使用它：

1. 在 StoreFront 中配置类型为 **Citrix Gateway Service** 的网关。通常，单个网关就足够了。但是，如果您希望为不同的站点或区域使用不同的地理位置规则，则可以配置具有不同网关服务 URL 的多个网关。有关详细信息，请参阅 [添加 Citrix Gateway Service](#)。

Add Citrix Gateway

StoreFront

- General settings
- Cloud Connectors
- Summary

General Settings

Complete these settings to configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

Display name:

Gateway type:

Usage or role: ⓘ

Citrix Gateway Service URL: (optional) ⓘ

Citrix Gateway Service URL (STA Connector Mode): (optional) ⓘ

For a list of available Citrix Gateway Service URLs, see [documentation](#)

2. 选择您希望 HDX 连接通过这些网关路由的站点或区域。有关详细信息，请参阅[最佳 HDX 路由](#)。

配置最佳 HDX 网关路由(/en-us/citrix-gateway-service/media/optimal-gateway-hdx-routing.png)

Citrix Gateway 服务接入点 (PoP) 列表

重要提示：

文章 [CTX270584](#) 不再维护。因此，请参阅此页面以获取最新的 PoP FQDN 列表。

Citrix 正在全球范围内增加更多 PoP，以确保 Citrix Gateway 服务客户的业务连续性和优质服务。PoP 列表分为以下几类：

- 商业区域的 PoP
- 适用于 Google Cloud Platform (GCP) 客户的 PoP
- 日本区域的 PoP
- 美国政府区域的 PoP

Citrix Workspace 和 Citrix Virtual Apps and Desktops 客户可能会看到网络流量可能路由到新的 Citrix Gateway 服务 FQDN 和目标地址。

防火墙配置

建议按照 [系统和连接要求](#) 中所述配置防火墙和安全 Web 网关。

注意：

客户可能已硬编码 FQDN 或 IP 地址以访问 Citrix Gateway 服务 PoP。他们必须更新防火墙规则，以允许防火墙和出站代理中的 Citrix Gateway 服务特定 FQDN/IP。

商业区域的接入点

对于 HDX™ 流量，我们建议以下配置：

- *.nssvc.net （包括所有子域）

如果您尚未启用所有子域，我们建议以下配置（不推荐）：

- *.c.nssvc.net

- *.g.nssvc.net

此通配符适用于所有现有和新的 PoP FQDN。使用基于通配符的允许列表的客户无需添加单个 FQDN。

注意：

- 建议配置防火墙和安全 Web 网关，如 [系统和连接要求](#) 中所述。
- 如果 DNS 转发器配置为允许特定域的递归 DNS 解析，您必须在允许列表中包含 *.akadns.net。此配置使 Citrix Cloud Connector、Citrix Virtual Apps and Desktops 或客户端能够连接到 Citrix Gateway 服务。

具有已定义接入点集的全局 FQDN

类型	FQDN	用途
全局	• global.g.nssvc.net	全球 FQDN
	主要：global-all.g.nssvc.net	
全球	• global-s.g.nssvc.net	包括服务连续性功能的全球 FQDN
全球	reg.c.nssvc.net	连接器/VDA 注册到 Citrix Cloud
仅限 Azure	azure-reg.c.nssvc.net	Azure 中的连接器注册到 Citrix Cloud

PoP FQDN

下表列出了与每个接入点 (PoP) 关联的 Citrix Gateway 服务 FQDN：

资源端 PoP FQDN (Cloud Connector 或 VDA)：用于源自资源端的 Citrix Gateway 服务连接。根据配置的连接路径，连接可能源自 Citrix Cloud Connector 或虚拟投递代理 (VDA)。

重要提示：

- 已允许 `*.nssvc.net`、更具体的 `*.g.nssvc.net` 和 `*.c.nssvc.net` 域或已发布的 Citrix Gateway 服务 FQDN 的客户，无需单独允许每个 PoP FQDN。
- 如果您的环境通过 IP 地址限制 Citrix Gateway 服务连接，请根据已发布的连接要求审查您当前的配置。Citrix 建议使用基于 FQDN 的规则，因为 Citrix Gateway 服务的目标 IP 地址可能会更改。

POP 代码	资源端 POP FQDN (CLOUD CONNECTOR 或 VDA)	云服务提供商	国家/地区	位置
az-in-c	az-in-c-rdvz.g.nssvc.net	阿祖尔	印度	浦那
az-eu-c	az-eu-c-rdvz.g.nssvc.net	阿祖尔	德国	法兰克福
az-us-c	az-us-c-rdvz.g.nssvc.net	微软 Azure	美国	爱荷华
az-亚洲-香港	az-asia-hk-rdvz.g.nssvc.net	微软 Azure	香港	香港
az-asia-se	az-asia-se-rdvz.g.nssvc.net	微软 Azure	新加坡	新加坡
Azure 澳大利亚东部	az-aus-e-rdvz.g.nssvc.net	阿祖尔	澳大利亚	新南威尔士
az-bz-s	az-bz-s-rdvz.g.nssvc.net	艾云	巴西	圣保罗

POP 代码	资源端 POP FQDN (CLOUD CONNECTOR 或 VDA)	云服务提供商	国家/地区	位置
az-ca-c	az-ca-c-rdvz.g.nssvc.net	艾云	加拿大	多伦多
az-eu-n	az-eu-n-rdvz.g.nssvc.net	艾云	爱尔兰	都柏林
az-eu-w	az-eu-w-rdvz.g.nssvc.net	艾云	荷兰	阿姆斯特丹
az-in-s	az-in-s-rdvz.g.nssvc.net	微软 Azure	印度	钦奈
Azure 日本东部	az-jp-e-rdvz.g.nssvc.net	微软 Azure	日本	东京
Azure 西北东	az-nw-e-rdvz.g.nssvc.net	微软 Azure	挪威	奥斯陆
az-uae-n	az-uae-n-rdvz.g.nssvc.net	艾萨尔	阿联酋	迪拜
az-us-e	az-us-e-rdvz.g.nssvc.net	阿祖尔	美国	弗吉尼亚
Azure-美国-东部2	az-us-e2-rdvz.g.nssvc.net	艾云	美国	弗吉尼亚

POP 代码	资源端 POP FQDN (CLOUD CONNECTOR 或 VDA)	云服务提供商	国家/地区	位置
az-us-sc	az-us-sc-rdvz.g.nssvc.net	艾哲尔	美国	德克萨斯州
艾哲尔-美国西部	az-us-w-rdvz.g.nssvc.net	艾泽	美国	加利福尼亚州
阿兹-扎-恩	阿兹-扎-恩-rdvz.g.nssvc.net	微软 Azure	南非	约翰内斯堡
aws-eu-s 区域	域名：aws-eu-s-rdvz.g.nssvc.net	AWS	意大利	米兰
区域：aws-aus-e	aws-aus-e-rdvz.g.nssvc.net	AWS	澳大利亚	悉尼
aws-asia-se	aws-asia-se-rdvz.g.nssvc.net	AWS	新加坡	新加坡
AWS 亚洲-台湾	aws-asia-tw-rdvz.g.nssvc.net	AWS	台湾	台北
aws-bz-s	aws-bz-s-rdvz.g.nssvc.net	AWS	巴西	圣保罗
aws-ca-e	aws-ca-e-rdvz.g.nssvc.net	AWS	加拿大	蒙特利尔

POP 代码	资源端 POP FQDN (CLOUD CONNECTOR 或 VDA)	云服务提供商	国家/地区	位置
aws-eu-c	aws-eu-c- rdvz.g.nssvc.net	AWS	德国	法兰克福
AWS 欧洲西部	AWS 欧洲西部- rdvz.g.nssvc.net	AWS	法国	巴黎
AWS 华南	aws-in-sc- rdvz.g.nssvc.net	AWS	印度	海得拉巴
aws-in-w	aws-in-w- rdvz.g.nssvc.net	AWS	印度	孟买
aws-jp-w	aws-jp-w- rdvz.g.nssvc.net	AWS	日本	大阪
aws-uk-se	aws-uk-se- rdvz.g.nssvc.net	AWS	英国	伦敦
aws-us-e	aws-us-e- rdvz.g.nssvc.net	AWS	美国	弗吉尼亚北部
aws-us-nc	aws-us-nc- rdvz.g.nssvc.net	AWS	美国	俄亥俄州
AWS 美国西部	aws-us-w- rdvz.g.nssvc.net	AWS	美国	北加利福尼亚

用于地理位置路由的区域 FQDN

注意：

每个地理位置都有两个 FQDN：

- 以 `rgn.g.nssvc.net` 结尾的 FQDN 是通用 FQDN。
- 以 `rgn-s.g.nssvc.net` 结尾的 FQDN 是包含服务连续性功能的 FQDN。
- 地理位置路由 FQDN 在增强升级期间不需要额外的允许列表条目，因为它们会自动解析到活动的 PoP 基础设施。

地理位置	FQDN	包含的 POP	
美国 - 东部	• <code>us-e-rgn.g.nssvc.net</code> • <code>us-e-rgn-s.g.nssvc.net</code>	<code>az-us-e</code> , <code>aws-us-e</code> , <code>aws-us-nc</code> , <code>az-us-e2</code>	
美国 - 中部和西部	• <code>us-wc-rgn.g.nssvc.net</code>	<code>az-us-w</code> , <code>aws-us-w</code> , <code>az-us-sc</code>	
	—— <code>us-wc-rgn-s.g.nssvc.net</code>		
美国	• <code>us-rgn.g.nssvc.net</code> • <code>us-rgn-s.g.nssvc.net</code>	<code>az-us-sc</code> , <code>az-us-e</code> , <code>az-us-w</code> , <code>az-us-e2</code> , <code>aws-us-e</code> , <code>aws-us-w</code> , <code>aws-us-nc</code>	
美国 - 仅限 Azure	• 美国 Azure 区域.g.nssvc.net • <code>us-azure-rgn-s.g.nssvc.net</code>	Azure 美国东部, Azure 美国西部, Azure 美国中南部, Azure 美国东部2	

地理位置	FQDN	包含的 POP	
欧洲	- eu-rgn.g.nssvc.net - eu-rgn-s.g.nssvc.net	aws-eu-c, aws-eu-w, az-eu-w, az-eu-n	
澳大利亚	- aus-rgn.g.nssvc.net - aus-rgn-s.g.nssvc.net	az-aus-e, aws-aus-e	
全球 - 仅限 Azure	- global-azure-rgn.g.nssvc.net - global-azure-rgn-s.g.nssvc.net	az-us-e, az-us-w, az-us-sc, az-bz-s, az-eu-w, az-eu-n, az-aus-e, az-asia-se, az-jp-e, az-in-s, az-uae-n, az-za-n, az-asia-hk, az-ca-c, az-us-e2, az-nw-e	
亚洲	- asia-rgn.g.nssvc.net - 亚洲-rgn-s.g.nssvc.net	az-uae-n, aws-in-w, az-in-s, az-asia-se, az-jp-e, aws-in-sc, aws-asia-tw, aws-asia-se, aws-jp-w	
印度	- 印度-rgn.g.nssvc.net - india-rgn-s.g.nssvc.net	aws-in-w, aws-in-sc, az-in-s	
全球 - 备用	global-alt-rgn.g.nssvc.net	az-asia-se, az-aus-e, az-bz-s, az-ca-c, az-eu-n, az-eu-w, az-in-s, az-jp-e, az-nw-e, az-uae-n, az-us-e,	

地理位置	FQDN	包含的 POP
	global-alt-rgn-s.g.nssvc.net	az-us-sc, az-us-w, az-za-n, aws-aus-e, aws-bz-s, aws-ca-e, aws-eu-c, aws-in-w, aws-uk-se, aws-us-e, aws-us-nc, aws-us-w, az-us-e2, aws-asia-se, aws-eu-w, aws-in-sc, aws-jp-w

适用于 Google Cloud Platform (GCP) 客户的接入点

购买了 Google Cloud Marketplace 订阅并在 Google Cloud 上运行其工作负载的 Citrix DaaS™ 客户可以使用 GCP 接入点。

注意：

建议按照 [系统和连接要求](#) 中所述配置防火墙和安全 Web 网关。

对商业区域中接入点的支持

对 GCP 客户在商业区域中接入点的支持计划在即将发布的版本中提供。借助此支持，您可以使用遍布五大洲商业区域的接入点。此支持提供以下优势：

- **改进的全球访问：**降低全球 GCP 用户的延迟并提高性能。
- **更大的灵活性：**选择最适合您需求的接入点并增强云弹性。

要使用商业区域中的接入点，请根据以下说明在 VDA、Citrix Cloud Connector™ 和 Citrix Workspace™ 应用程序（客户端）中配置防火墙规则：

- 配置防火墙以在您的资源和 Citrix Cloud 之间建立连接。有关详细信息，请参阅[系统和连接要求](#)。
- 为 Citrix Cloud Connector 配置防火墙。有关详细信息，请参阅[Citrix Cloud Connector 代理和防火墙配置](#)。
- 启用对 Azure 和 AWS 中商业区域接入点 FQDN 的访问。

具有定义的接入点集的全局 FQDN

类型	FQDN	用途
仅限 GCP	gcp.g.nssvc.net	包含 GCP 和商业区域 PoP 的全局 FQDN
全局	reg.c.nssvc.net	连接器/VDA 注册到 Citrix Cloud

PoP FQDN

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
gcp-us-sc	gcp-us-sc-rdvz.g.nssvc.net	GCP	美国	南卡罗来纳州
gcp-sz-zu	gcp-sz-zu-rdvz.g.nssvc.net	GCP	瑞士	苏黎世
gcp-us-la	gcp-us-la-rdvz.g.nssvc.net	GCP	美国	洛杉矶
GCP 英国伦敦	GCP 英国伦敦 会合 点.g.nssvc.net	GCP	英国	伦敦
gcp-us-or	gcp-us-or-rdvz.g.nssvc.net	GCP	美国	达勒斯特，俄勒冈州
az-亚洲-香港	az-亚洲-香港-rdvz.g.nssvc.net	微软 Azure	香港	香港
az-东南亚	az-asia-se-rdvz.g.nssvc.net	微软 Azure	新加坡	新加坡

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
az-aus-e	az-aus-e-rdvz.g.nssvc.net	微软 Azure	澳大利亚	新南威尔士
az-bz-s	az-bz-s-rdvz.g.nssvc.net	微软 Azure	巴西	圣保罗
az-ca-c	阿兹-加-西-尔德维兹.吉.恩斯维西.网	阿祖尔	加拿大	多伦多
阿兹-欧-恩	az-eu-n-rdvz.g.nssvc.net	微软 Azure	爱尔兰	都柏林
az-eu-w	az-eu-w-rdvz.g.nssvc.net	阿祖尔	荷兰	阿姆斯特丹
艾兹-印-南	az-in-s-rdvz.g.nssvc.net	艾云	印度	钦奈
az-jp-e	az-jp-e-rdvz.g.nssvc.net	艾云	日本	东京
az-nw-e	az-nw-e-rdvz.g.nssvc.net	艾云	挪威	奥斯陆
az-uae-n	az-uae-n-rdvz.g.nssvc.net	阿祖尔	阿联酋	迪拜
美国东部可用区	az-us-e-rdvz.g.nssvc.net	阿祖尔	美国	弗吉尼亚

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
az-us-sc	az-us-sc-rdvz.g.nssvc.net	阿祖尔	美国	德克萨斯
az-us-w	az-us-w-rdvz.g.nssvc.net	微软 Azure	美国	加州
az-za-n	az-za-n-rdvz.g.nssvc.net	微软 Azure	南非	约翰内斯堡
aws-aus-e	aws-aus-e-rdvz.g.nssvc.net	AWS	澳大利亚	悉尼
aws-bz-s	aws-bz-s-rdvz.g.nssvc.net	AWS	巴西	圣保罗
aws-ca-e	aws-ca-e-rdvz.g.nssvc.net	AWS	加拿大	蒙特利尔
aws-eu-c	aws-eu-c-rdvz.g.nssvc.net	AWS	德国	法兰克福
aws-in-w	aws-in-w-rdvz.g.nssvc.net	AWS	印度	孟买
AWS 英国东南	aws-uk-se-rdvz.g.nssvc.net	AWS	英国	伦敦
AWS 美国东部	亚马逊-美国东部-rdvz.g.nssvc.net	AWS	美国	北弗吉尼亚

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
AWS 美国中北部	亚马逊-美国中北部- rdvz.g.nssvc.net	AWS	美国	俄亥俄州
aws-us-w	aws-us-w- rdvz.g.nssvc.net	AWS	美国	北加利福尼亚

日本区域的接入点

对于日本客户，我们建议以下配置：

- *.*.nssvc.jp（包括所有子域）

如果您尚未启用所有子域，我们建议以下配置（不太推荐）：

- *.g.nssvc.jp
- *.c.nssvc.jp

注意：

- 使用推荐的地址可确保 Citrix Gateway 服务持续运行，因为 Citrix 会添加和停用地址以提高性能和可用性。
- 我们建议您根据[服务连接要求](#)配置防火墙和安全 Web 网关。
- 如果 DNS 转发器配置为允许特定域的递归 DNS 解析，则必须在允许列表中包含 *.akadns.net。此配置使 Citrix Cloud Connector、客户端或 VDA 能够连接到 Citrix Gateway 服务。请在 July 15, 2025 之前完成此配置，以确保 Citrix Gateway 服务持续运行。

具有已定义接入点集的全局 FQDN

类型	FQDN	用途
全局	• global.g.nssvc.jp	全局 FQDN

类型	FQDN	用途
	global-s.g.nssvc.jp	包括服务连续性功能的全局 FQDN
全局	reg.c.nssvc.jp	连接器/VDA 注册到 Citrix Cloud

PoP FQDN

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
azjpc-jp-w	azjpc-jp-w-rdvz.g.nssvc.jp	阿祖尔	日本	大阪
awsjpc-jp-e	awsjpc-jp-e-rdvz.g.nssvc.jp	AWS	日本	东京

美国政府区域的接入点

对于美国政府区域，我们建议以下配置：

- `*.*.nssvc.us`（包括所有子域）

如果您尚未启用所有子域，我们建议以下配置（不太推荐）：

- `*.g.nssvc.us`
- `*.c.nssvc.us`

注意：

- 使用推荐的地址可确保 Citrix Gateway 服务持续运行，因为 Citrix 会添加和停用地址以提高性能和可用性。
- 建议按照 [Citrix Cloud Government 的连接要求](#) 中所述配置防火墙和安全 Web 网关。
- 为确保 Citrix Cloud Connector、客户端或 VDA 解析必要的 DNS 查询以连接到 Citrix Gateway 服务，您必须将 `*.usgovtrafficmanager.net` 包含在 DNS 转发器上用于递归 DNS 解析的允许域列表中。此配置必须在 April 27, 2025 之前完成，以确保 Citrix Gateway 服务持续运行。

具有已定义接入点集的全局 FQDN

类型	FQDN	用途
全局	global.g.nssvc.us	用于应用程序启动的全局 FQDN
全局	reg.c.nssvc.us	Connectors/VDA 注册到 Citrix Cloud

PoP FQDN

POP 代码	POP FQDN	云服务提供商	国家/地区	位置
azusg-us-az	azusg-us-az-rdvz.g.nssvc.us	阿祖尔	美国	美国政府亚利桑那
azusg-us-tx	azusg-us-tx-rdvz.g.nssvc.us	阿祖尔	美国	美国政府德克萨斯
azusg-us-va	azusg-us-va-rdvz.g.nssvc.us	阿祖尔	美国	美国政府弗吉尼亚

HDX 代理的云连接器规模和扩展性考量

Citrix Cloud Connectors™ 的适当规模和配置对于不使用 Rendezvous v1 或 v2 协议（非 Rendezvous 模式）的 HDX™ 代理部署的高可用性、稳定性以及高效性能至关重要。云连接器在 Citrix Gateway 服务和 VDA 之间充当重要的代理，因此对其进行优化对于无缝操作至关重要。

本文提供的经过测试的最大容量和推荐机器配置提供了指导，以确保 HDX 代理部署中的最佳性能和稳定性。

注意：

这些建议适用于在非 Rendezvous 模式下充当 HDX 代理部署代理的云连接器部署。

规模不当或配置错误的云连接器可能导致性能瓶颈、服务中断和不稳定。当在 Citrix Gateway 服务和 VDA 之间处理大量 HDX 代理流量时，这些挑战会变得更加突出。适当的规模对于避免这些挑战并保持可靠的用户体验至关重要。

建议

以下是确定连接器规模的建议：

- **最少云连接器数量：**3 个云连接器以确保高可用性。
- **处理器：**Intel Ice Lake、Cascade Lake 和更新的处理器。
- **网络：**Azure 加速网络或在其他云环境或虚拟机管理程序中的等效网络设置。

请确保在您的特定环境中进行测试，以确认适当的连接器规模。

测试条件

- CPU 和内存要求仅适用于基础操作系统 (OS) 和 Citrix 服务。第三方应用程序和服务可能需要更多资源。
- 会话以持续速率启动。
- 测试在单个 Windows 连接器上执行。建议至少使用三个连接器以确保高可用性。
- 测试是在配置了 Intel Ice Lake 或 Cascade Lake 处理器的 Cloud Connector 上执行的。

- 客户端、Citrix Gateway 服务 PoP、Cloud Connector 和 VDA 托管在 Azure 的同一区域中。它们在非 Rendezvous 模式下建立端到端 HDX 会话。会话通过测试 Cloud Connector 运行，同时持续模拟数据包。
- 测试是使用 D2ds_v5、D4ds_v5、D8s_v5 和 D16s_v4 虚拟机执行的。

测试方法

执行测试以施加负载并评估连接器组件的性能。在测试期间，会收集性能数据，例如 Cloud Connector 上的 CPU 使用率和端到端延迟。Citrix 专有模拟工具用于模拟 VDA 和会话。这些工具复制传统 VDA 和会话的行为，同时比托管实际会话和 VDA 需要更少的资源。

本文中关于 Cloud Connector 大小调整的建议基于从以下测试中收集的数据：

- 执行测试以确定在不超过以下预定义条件的情况下支持的连接数和吞吐量：
 - Citrix Gateway 服务连接器进程的 CPU 使用率 < 70%
 - 端到端延迟 < 50 毫秒
- 使用最小、平均和最大数据包大小执行测试，并使用平均值作为结果。

测试结果摘要

下表列出了建议的最低 Cloud Connector CPU 和其他重要配置：

CPU	内存 (GB)	并发 HDX 连接数	HDX 吞吐量 (MBPS)
2	8	500	100
4	16	1000	200
8	32	2000	400
16	64	4000	700

注意：

上述并发 HDX 会话和吞吐量是建议值，而非硬性限制。我们建议您在特定环境中测试自己的 HDX 会话限制。

常见问题

本节提供有关将 Citrix ADC VPX 迁移到 Citrix Gateway 服务以用于 HDX 代理的常见问题解答。

我可以将我的本地配置移植到 Citrix Cloud™ 吗？

不可以，底层基础设施和机制不同。请参阅有关启用 Citrix Gateway 服务的章节。

我可以将我的门户自定义项上传到 Citrix Cloud 吗？

不支持此功能。但是，Citrix Cloud 提供了一些自定义选项。请参阅以下链接：<https://docs.citrix.com/zh-cn/xenapp-and-xendesktop/service/storefront.html>

我已使用 VPX 在本地启用了多重身份验证或双因素身份验证。我可以在云端也启用此功能吗？

Citrix DaaS 提供的 VPX 只能用于 HDX 代理（基于 EULA），而不能用于身份验证。云端身份验证通过云连接器使用本地 AD 或 Azure Active Directory 执行。

我可以将云服务用于 SmartControl、SmartAccess 吗？

Citrix Gateway 服务不支持 SmartControl 功能。SmartAccess 功能可以通过设备姿态服务 (DPS) 或网络位置服务 (NLS) 以及自适应身份验证或条件身份验证来启用。

如何分阶段迁移到 Citrix Gateway 服务？

没有配置支持混合部署（本地 Citrix ADC VPX 和 Citrix Gateway 服务）。建议通过使用试用帐户（在有限期限内有效）启用 Citrix Gateway 服务，并与一小部分用户或预览用户进行测试，从而执行分阶段迁移。

Citrix Gateway 服务所需的最低许可证是什么？

任何使用 Citrix DaaS 或 Citrix Workspace 的客户都有权使用 Citrix Gateway 服务进行 HDX 代理。

拥有 Citrix Universal™ Hybrid Multi-Cloud (UHMC) 和 Citrix Platform License (CPL) 的客户的带宽配额是多少？

UHMC 和 CPL 客户有权获得以下带宽配额：

- 用户许可：每用户每月 2.5 GB
- 并发用户许可：每用户每月 2.5 GB

UHMC 和 CPL 是新的库存单位 (SKU)。其他旧版 SKU（Citrix Universal 订阅）不再可用于续订或合同延期。

带宽配额用尽后会发生什么？

当带宽配额超出时，Citrix Gateway 服务将继续运行，不会出现任何突然中断。没有针对超额使用的自动警报，但客户可以在 Citrix Cloud 门户的 [许可使用情况洞察 -> 网关使用情况](#) 下监控其 Citrix Gateway 服务带宽使用情况。

客户无法购买额外带宽，因为 Citrix® 已停止提供仅带宽 SKU。超出配额的过度带宽使用将在合同续订期间进行审查。

拥有 Citrix Universal 订阅的客户的带宽配额是多少？

拥有 Citrix Universal 订阅的客户的带宽配额如下：

思杰网关服务 + 思杰工作区 + 思杰 DaaS 套件：

UNIVERSAL 订阅版本	用户许可	并发用户许可
DaaS 高级版和高级增强版	每用户每月 1 GB	每月每用户 2 GB
DaaS 高级版和高级增强版	每月每用户 5 GB	每月每用户 10 GB

思杰网关服务 + 思杰工作区套件：

持续时间	用户许可	并发用户许可
期限	每月每用户 1 GB	每月每用户 2 GB
	每月每用户 5 GB	每月每用户 10 GB
年度	每用户每月 1 GB	每用户每月 2 GB

持续时间	用户许可	并发用户许可
	每用户每月 5 GB	每用户每月 10 GB
每月	每用户每月 1 GB	每用户每月 2 GB
	每用户每月 5 GB	每用户每月 10 GB

Citrix Universal 订阅不再适用于续订或合同延期，客户在续订时将转为 UHMC 和 CPL 订阅。

在哪里可以查看通过 Citrix Gateway 服务建立的连接指标？

Citrix Analytics for Performance UI 的连接器统计信息仪表板提供了所选连接器在过去 24 小时内的资源消耗的全面视图，以及从连接器到虚拟应用和桌面环境中的 Citrix Gateway 服务 PoP 计算出的合成延迟视图。有关详细信息，请参阅 [连接器统计信息](#)。

Citrix Gateway 服务文档历史记录

下表介绍了对 Citrix Gateway 服务文档所做的重要变更。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	说明
05 May 2022	添加了有关 DTLS 1.2 协议支持的信息	技术安全性概述 。
05 Apr 2022	从 Secure Workspace Access 到 Secure Private Access 以及从 Citrix Virtual Apps and Desktops 服务到 Citrix DaaS 的品牌重塑变更	发行说明 。
11 Oct 2021	更新了发行说明，以包含有关 Citrix Gateway 服务和 Secure Private Access 服务磁贴合并的信息	发行说明 。
11 Oct 2021	删除了与 Web 和 SaaS 应用程序相关的主题，并将其移至 Secure Private Access 服务文档	Citrix Gateway 服务
10 May 2021	更新了面向 GA 的 HDX 与 EDT 支持主题	支持 EDT 的 HDX 自适应传输 。