

AWS 决策指南

选择 AWS 网络和内容分发服务



选择 AWS 网络和内容分发服务: AWS 决策指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆或者贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

简介 1

明白 2

考虑一下 3

选择 6

使用 8

Explore 19

文档历史记录 20

..... xxi

选择 AWS 网络和内容分发服务

目的：	帮助确定哪些 AWS 网络和内容交付服务最适合您的组织。
最后更新时间：	2025 年 1 月 16 日
承保服务：	• Amazon API Gateway • AWS Client VPN • AWS Cloud 广域网 • Amazon CloudFront • AWS 数据传输终端 • AWS Direct Connect • Elastic Load Balancing • AWS Firewall Manager • AWS Global Accelerator • AWS Network Firewall • AWS PrivateLink • Amazon Route 53 • AWS Shield • AWS Site-to-Site VPN • AWS Transit Gateway • AWS Verified Access • Amazon VPC • 亚马逊 VPC IPAM • Amazon VPC Lattice • AWS WAF

确定云联网和内容交付的方法可能很复杂，尤其是在您习惯使用本地硬件管理和配置网络的情况下。幸运的是，在[云中构建网络](#)与在本地构建网络有着共同的核心概念，例如 IP 寻址、负载平衡和路由。熟悉这些概念将有助于 AWS 服务 你了解自己的需求。

Amazon Web Services (AWS) 提供 20 多种专门构建的网络和内容交付服务，您可以使用这些服务在全球所有云环境以及分布式云和边缘站点中构建、运营和保护您的云网络。您还可以构建将本地环境扩展到的网络基础架构 AWS。

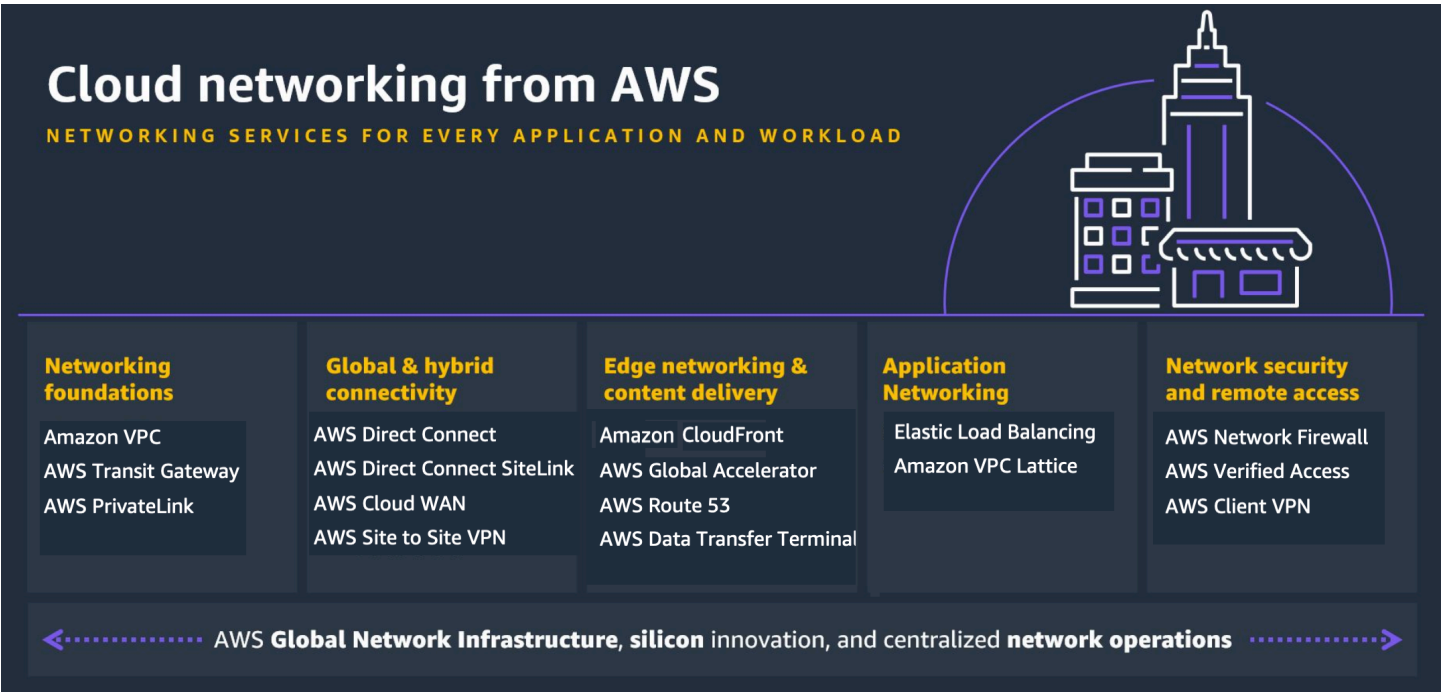
本决策指南将帮助您提出正确的问题，以选择适合您需求的网络和内容交付服务及工具。

[该视频提供了四分钟的 AWS 网络简介。](#)

明白

你内置的内容 AWS 取决于你的业务需求。在本指南中，我们使用“工作负载”一词来指可提供业务价值的任何资源和代码集合，例如面向客户的应用程序或后端流程。

网络和内容交付服务分为四类：网络基础、全球和混合连接、边缘网络和内容交付以及应用程序网络。AWS



网络基础

在中 AWS，您的工作负载在一个或多个 [Amazon Virtual Private Cloud 中运行 \(VPCs\)](#)。在您的工作负载运行后 VPCs，您可以将工作负载连接到其他 VPCs（例如），也可以将它们连接到软件 [AWS Transit Gateway](#) 即服务 (SaaS) 服务，包括其他服务 AWS 服务，例如。 [AWS PrivateLink](#) Amazon VPC 允许您预置一个私有的、隔离的部分，您可以使用客户定义的 IP 地址范围在虚拟网络中启动 AWS 资源。AWS Cloud Amazon VPC 为您提供多种选项，用于将您的 AWS 虚拟网络与其他远程网络连接起来。

全球和混合连接

您可以使用此类别中的服务从本地网络安全地连接到您的工作负载 AWS Cloud。您可以使用创建[虚拟专用网络 \(VPN\)](#) 来连接远程用户 [AWS Client VPN](#)，也可以使用云广域网连接本地网络 [AWS Site-to-Site VPN](#)，或者使用[AWS 云广域网构建全球广域网 \(WAN\)](#)。您还可以与用户建立直接、私密的 AWS Cloud 连接 [AWS Direct Connect](#)，从而以可预测的性能提供直接、安全的云连接。您可能还需要连接本地数据中心、远程站点和云。[混合网络](#)可以连接这些不同的环境。

边缘网络和内容交付

此类服务通过缓存和优化传输来帮助确保更高的性能。A [amazon](#) 就是一个很好的例子 CloudFront。您还需要使用诸如 A [amazon Route 53 之类的服务，看到客户流量以最佳方式路由](#)，以提供可用性。此外，重要的是要使用诸如[AWS Global Accelerator](#)之类的服务来路由客户流量，以充分利用 AWS 全球基础架构。[AWS Data Transfer Terminal](#) 是一个网络就绪的物理位置，您可以将数据存储设备带到和从中快速传输数据。AWS Cloud

应用程序联网

随着采用率的提高 AWS Cloud，您需要考虑如何使用[AWS App Mesh](#)和 [Amazon VPC Lattice 大规模连接工作负载，使用 Amazon API Gateway 将您的工作负载 VPCs 与 APIs](#)<https://aws.amazon.com/what-is/api/>集成，以及如何使用 [Amazon VPC IP 地址管理器 \(IPAM\)](#) 管理您 VPCs 中运行的资源的 IP 地址使用情况。随着客户需求的增长，您可以使用 [Elastic Load Balancing](#) 来帮助确保您的工作负载 [VPCs](#) 可以扩展并提供高可用性。

网络安全和远程访问

虽然 Amazon VPC 可帮助您安全访问工作负载，但此类服务通过使用[AWS Network Firewall](#)、[AWS Shield](#)[AWS Verified Access](#)、和提供了针对威胁行为者和未经授权的用户的增强保护[AWS WAF](#)。为了帮助确保网络安全，可以考虑使用 Amazon Route 53 DNS 防火墙[AWS Network Firewall](#)[AWS Firewall Manager](#)、、、[网络访问控制列表](#)和安全组。

考虑一下

选择适合您业务需求的网络服务非常重要。以下是选择网络服务时需要考虑的一些标准。

Business objectives

您选择的网络服务将取决于您的业务目标。在中运行的工作负载的安全性、可靠性、可访问性和性能方面，评估你现在的状况和你想要达到的目标 AWS Cloud。

- 考虑一下您使用的网络服务如何与您的迁移和集成策略相吻合。[混合网络架构](#)可以通过集成您的本地数据中心来帮助您满足这一需求 AWS。
- 查看 Let's architecture 中的[社交和内容交付博客](#)！AWS 博客系列，以了解其他人正在构建什么 AWS Cloud。
- 查看可帮助您加快网络服务采用速度的第三方选项。[AWS Marketplace](#)提供了精选的数字目录，可用于查找、购买和部署网络解决方案。
- 决定与专门从事网络和内容交付[AWS Partner](#)的公司合作是否有好处。其成员 AWS Partner Network 是战略专家和经验丰富的建筑商，可以帮助您满足您的需求 AWS Cloud。
- 探索在 Skill Builder 上参加[AWS 网络在线课程](#)，涵盖亚马逊 VPC、AWS Cloud WAN 和 Amazon Route 53 等服务。

Workload characteristics

您选择的网络服务将取决于您的工作负载的特征。

- 每种网络服务都有特定的作用。诸如 AWS Cloud WAN AWS Transit Gateway 之类的服务适用于连接正在运行的工作负载 VPCs。Amazon API Gateway 会创建公用，APIs 以便您的客户可以连接到您的工作负载。AWS Global Accelerator 可以帮助您提高工作负载的可靠性、安全性和延迟。
- 随着互联网的不断发展，设备对 IP 地址的需求也随之增长。IP 地址最常见的格式是 IPv4。IP 地址的最新格式是 IPv6。IPv6 提供了更多的地址空间并解决了[IPv4 地址耗尽](#)的问题。AWS 服务对的支持 IPv6 包括对双堆栈配置（IPv4 或 IPv6）或 IPv6 仅支持配置的支持。AWS 服务 这种支持的 IPv6 数量在持续增长。要查看当前支持的服务 IPv6，请参阅[AWS 服务 该支持 IPv6](#)。

Data protection

请务必考虑保护您的数据 AWS Cloud。

- 企业必须保护客户数据免受不断变化的网络风险的影响。虽然 Amazon VPC 可以帮助您安全访问中运行的工作负载 VPCs，但可以考虑采取增强的数据保护措施，例如、AWS Network Firewall AWS Shield AWS WAF、和 Amazon Route 53 Resolver DNS 防火墙。
- 无论传输方式如何，建议您使用应用程序级加密 (TLS) 作为深度防御措施，以帮助确保机密性。end-to-end
- 如果您 VPCs 需要将工作负载连接到其他工作负载 AWS 服务，则可以通过公共互联网使用 API 端点以编程方式连接到这些服务。但是，如果要通过私有连接发送数据，请使用 AWS PrivateLink。许多成员通过 AWS Partner Network 提供他们的 SaaS 解决方案 AWS PrivateLink。

Availability

可用性是指应用程序维持正常运行的能力。重要的是，您的客户可以在停机时间最少或根本没有停机时间的情况下使用您构建的产品和服务。VPCs

- AWS 全球基础设施建立在[可用区AWS 区域](#)之上。当您将工作负载部署到时 VPCs，应将工作负载部署到多个可用区，以确保在单个可用区出现故障时，您的工作负载仍然可用。
- 要提高在您的 VPCs 中运行的工作负载的可用性、可扩展性、安全性和性能，请考虑使用[负载平衡](#) (Elastic Load Balancing)。您可以根据应用程序的需求使用不同类型的负载均衡器。每个负载均衡器通过与[开放系统互联 \(OSI\)](#) 模型一致的不同协议和网络层支持不同类型的流量。有关负载均衡器类型之间差异的更多信息，请参阅[产品比较](#)。

Performance

您可以使用网络服务针对 AWS 在全球基础架构上运行的工作负载的延迟、吞吐量和带宽要求进行优化。

- 如果您想最大限度地减少全球各地使用 Web 应用程序的本地客户的延迟，请考虑使用 Amazon CloudFront。CloudFront 是一个以尽可能低的延迟向客户[交付内容的内容分发网络](#)。
- 如果您正在运行游戏、物联网 (IoT) 或 IP 语音 (VoIP) 工作负载，请考虑使用 AWS Global Accelerator。此服务可帮助您提高工作负载的可用性和性能。
- 如果您 VPCs 需要将工作负载连接到其他工作负载 AWS 区域，则可以使用公共 API 端点以编程方式连接到这些服务。

Operational excellence

随着 AWS Cloud 采用率的提高，你需要随时了解工作负载中正在发生的事情。随着工作负载的增长，[Reachability Analyzer](#) 和 [Amazon CloudWatch Internet Monitor](#) 等工具和服务可以帮助您跟上不断变化的业务需求和优先级。

- 管理多个工作负载的 IP 地址 VPCs 可能很困难。考虑一下您是否需要在工作中自动管理 IP 地址 (Amazon VPC IPAM) 。
- 如果您使用的是[微服务架构](#)，那么管理微服务之间的连接、安全性和监控可能是一项挑战。考虑一下您是否需要自动执行微服务交互 (AWS App Mesh 以及 Amazon VPC Lattice) 。

Connectivity

您可以使用网络服务连接网络 AWS Cloud、连接工作负载或连接网络。

- 连接时请考虑以下几点 AWS Cloud：
 - 如果您想将远程用户安全地连接到您的 VPCs，请考虑使用 AWS Client VPN。
 - 如果您想将整个本地网络安全地连接到您的 VPCs，请考虑使用 AWS Site-to-Site VPN。
 - 如果您需要比互联网所能提供的更稳定的性能，可以考虑从您的本地网络直接连接到 AWS (AWS Direct Connect)。
 - 如果您需要快速将数据移入或移出 AWS Cloud，请考虑使用 AWS 数据传输终端。
- 要连接网络，请考虑以下几点：
 - 如果您在多个中操作 AWS 区域，想要管理自己的路由配置，或者更喜欢使用自己的自动化，请考虑使用 AWS Transit Gateway。
 - 如果您想将数据中心、分支机构和 AWS 网络与 WAN 统一起来，可以考虑使用 AWS Cloud WAN。如果您不想管理复杂的路由配置或构建自己的多区域连接自动化系统，也值得考虑。

Security

AWS 为您构建和部署应用程序提供了安全的基础，但您有责任实施自己的安全措施来保护您的数据、应用程序和网络基础架构，这与在现场数据中心中的做法没什么不同。

- 查看并了解[AWS 共担责任模型](#)及其如何应用于安全性 AWS Cloud。
- AWS 安全组和网络访问控制列表 (NACLs) 可以一起使用，也可以单独使用来保护网络，从而帮助您制定深度防御安全策略。
- 企业必须保护其网络应用程序免受不断变化的网络风险的影响。考虑是否需要保护工作负载免受恶意攻击或恶意软件（使用 [AWS Network Firewall](#)）、分布式拒绝服务 (DDoS) 攻击（使用 AWS Shield）或 SQL 注入和跨站脚本攻击（使用 AWS WAF）的侵害。

Amazon Route 53 [AWS Firewall Manager](#)、[网络访问控制列表](#)和安全组也是确保网络安全的重要考虑因素。

选择

既然您已经知道了评估网络服务选项所依据的标准，就可以选择最合适的服务了。

服务类别	它针对什么进行了优化？	AWS 网络和内容交付服务
网络基础	针对 AWS 网络服务入门和 VPCs 安全连接进行了优化。	Amazon VPC AWS PrivateLink AWS Transit Gateway
全球和混合连接	经过优化，可确保私有、安全的全球网络连接。	AWS Client VPN AWS Cloud 广域网 AWS Direct Connect AWS Site-to-Site VPN
边缘网络和内容交付	针对低延迟、可靠的工作负载流量路由进行了优化。	Amazon CloudFront AWS Global Accelerator Amazon Route 53 AWS 数据传输终端
应用程序联网	经过优化，可确保您的工作负载具有高可用性、适应需求并且可以相互通信。	Amazon API Gateway 亚马逊 VPC IPAM Amazon VPC Lattice Elastic Load Balancing
网络安全和远程访问	经过优化，可保护您的工作负载免受恶意软件、DDoS、SQL 注入和跨站脚本攻击。 。	AWS Firewall Manager AWS Network Firewall AWS Shield AWS Verified Access AWS WAF

使用

为了探索如何使用每种可用网络服务并进一步了解每种可用 AWS 网络服务，我们提供了探索每种服务如何运作的途径。以下部分提供了指向深入文档、动手教程和资源的链接，以帮助您入门。

以下服务涵盖全球联网和 VPC 连接。

Amazon CloudFront

- 什么是亚马逊 CloudFront？

了解如何加快内容分发。

[浏览指南](#)

- 开始使用亚马逊 CloudFront

通过学习交付内容的基本步骤 CloudFront。

[浏览指南](#)

- 使用亚马逊 S3、亚马逊和亚马逊 Route CloudFront 53 托管点播流媒体视频

了解如何以安全且可扩展的方式托管视频以供按需观看。

[开始阅读本教程](#)

- 借助 Amazon 更快地交付内容 CloudFront

了解如何减少 Web 应用程序的最终用户延迟。

[开始阅读本教程](#)

AWS Cloud WAN

- 什么是 AWS 云广域网？

学习如何构建、管理和监控统一的全球网络。

[浏览指南](#)

- AWS 云广域网简介

了解 AWS Cloud WAN 的主要用例以及如何开始使用。

[阅读博客](#)

- AWS 云广域网入门

创建您的第一个全球网络并连接一个 VPC。

[开始阅读本教程](#)

AWS Direct Connect

- 什么是 AWS Direct Connect ?

了解如何将本地网络连接到 AWS.

[浏览指南](#)

- 入门 AWS Direct Connect

观看简要介绍 AWS Direct Connect 以及如何为本地网络做好连接准备 AWS。

[观看视频](#)

- 将您的数据中心连接到 AWS

将您的数据中心连接到 us AWS ing 上 AWS Direct Connect。

[开始阅读本教程](#)

AWS Global Accelerator

- 什么是 AWS Global Accelerator ?

了解如何提高工作负载的性能。

[浏览指南](#)

- 标准加速器入门

创建加速器以提高在 EC2 实例上运行的工作负载的网络性能。

[开始阅读本教程](#)

- 为您的流量提高全球应用程序可用性和性能

观看有关设置 AWS Global Accelerator 以提高网络性能的简短演示。

[观看视频](#)

AWS PrivateLink

- 什么是 AWS PrivateLink ?

了解如何以私密方式将您的 VPC 连接到服务。

[浏览指南](#)

- 开始使用 AWS PrivateLink

CloudWatch 使用从私有子网中的 EC2 实例向 Amazon 发送请求 PrivateLink。

[开始阅读本教程](#)

- IPv6 通过 PrivateLink 服务和端点加快您的采用

拥有大量互联网足迹的客户会感受到公共 IPv4 广播疲惫的压力。了解如何在使用中 VPCs 增加 IPv6 使用量 PrivateLink。

[阅读博客](#)

Amazon Route 53

- What is Amazon Route 53?

了解高可用性和可扩展性的域名解析。

[浏览指南](#)

- 亚马逊 Route 53 用例教程

如何将 Route 53 用于基于流量和延迟的用例。

[开始阅读本教程](#)

- 如何使用亚马逊 Route 53 注册域名

本教程可帮助您为 Web 应用程序注册新域名。

[开始阅读本教程](#)

- 亚马逊 53 号公路简介

观看域名解析和 Route 53 的简要介绍。

[观看视频](#)

AWS Data Transfer Terminal

- 什么是 AWS 数据传输终端？

了解如何 AWS Cloud 使用自己的存储设备将大型数据集快速上传或下载到中。

[浏览指南](#)

- 介绍 AWS 数据传输终端

了解主要用例以及如何入门。

[阅读博客](#)

AWS Site-to-Site VPN

- 什么是 AWS Site-to-Site VPN？

了解如何 AWS 通过 VPN 将远程用户连接到。

[浏览指南](#)

- 入门 AWS Site-to-Site VPN

在本地设备和之间建立 Site-to-Site VPN 连接 AWS。

[开始阅读本教程](#)

- AWS Site-to-Site VPN，选择正确的选项来优化性能

设置 VPN 连接时，请选择最佳选项 AWS。

[阅读博客](#)

AWS Transit Gateway

- What is a transit gateway?

了解如何连接公 VPCs 交网关。

[浏览指南](#)

- 网关用例示例

查看中转网关的常见用例。

[浏览指南](#)

- AWS Transit Gateway 工作坊

在本实践研讨会中，学习如何在单一区域以及单账户、多账户和多区域设置中部署 Transit Gateway。

[开始工作坊](#)

Amazon VPC

- Amazon VPC 是什么？

了解虚拟私有云和 Amazon VPC 的功能。

[浏览指南](#)

- 开始使用亚马逊 VPC

Amazon VPC 快速入门指南。

[浏览指南](#)

- VPC 配置示例

查看基于不同用例的 VPC 配置示例。

[浏览指南](#)

- 模块化和可扩展的 VPC 架构

根据基础 AWS Cloud 架构 AWS 的最佳实践建立虚拟网络基础。

[开始阅读本教程](#)

Amazon VPC IPAM

- 什么是 IPAM？

了解如何跟踪和管理 IP 地址的使用情况。

[浏览指南](#)

- 亚马逊 VPC IP 地址管理器 (IPAM) 最佳实践

了解如何创建可扩展的 IP 地址管理计划。

[阅读博客](#)

- 创建池来管理您的 IP 空间

观看 VPC IPAM 的简短视频介绍。

[观看视频](#)

以下服务与应用程序级网络有关。

Amazon API Gateway

- 什么是 Amazon API Gateway ?

了解如何为您的工作负载 APIs 进行创建。

[浏览指南](#)

- APIs 使用 Amazon API Gateway 进行构建

了解如何开始构建 APIs AWS。

[观看视频](#)

- 使用 Amazon API Gateway HTTP 配置私有集成 APIs

了解如何创建 API 来控制 VPC 中资源的私有访问权限。

[阅读博客](#)

AWS Client VPN

- 什么是 AWS Client VPN ?

了解如何 AWS 通过 VPN 将网络连接到。

[浏览指南](#)

- 入门 AWS Client VPN

下载 AWS Client VPN 应用程序并 AWS 通过 VPN 连接。

[浏览指南](#)

- 的场景和示例 AWS Client VPN

查看为客户创建和配置 Client VPN 访问权限的示例。

[探索示例](#)

Elastic Load Balancing

- 什么是 Elastic Load Balancing ?

了解如何在工作负载之间分配传入流量。

[浏览指南](#)

- Elastic Load Balancing 入门

了解不同类型的负载均衡器之间的区别并创建负载均衡器。

[浏览指南](#)

- 如何为您的 AWS 工作负载选择合适的负载均衡器

选择正确的选项，对工作负载流量进行负载均衡。

[观看视频](#)

AWS Firewall Manager

- AWS Firewall Manager 策略入门

了解如何使用 AWS Firewall Manager 来启用多种不同类型的安全策略。

[浏览指南](#)

- 如何通过以下方式持续审计和限制安全组 AWS Firewall Manager

这篇博文演示了 AWS Firewall Manager 如何使用限制安全组，以帮助确保仅打开所需的端口。

[浏览指南](#)

- AWS Firewall Manager 用于大规模部署保护 AWS Organizations

这篇文章提供了使用在整个 AWS Organizations 实施中部署和管理安全策略的 step-by-step 说明 AWS Firewall Manager。

[浏览指南](#)

AWS Network Firewall

- 什么是 AWS Network Firewall？

了解网络防火墙和入侵检测。

[浏览指南](#)

- 入门 AWS Network Firewall

快速创建和管理 VPC 的网络防火墙。

[开始阅读本教程](#)

- AWS Network Firewall 动画讲解视频

观看简短的视频介绍 AWS Network Firewall。

[观看视频](#)

AWS Shield

- 什么是 AWS Shield？

了解有关 DDoS 保护的信息。

[浏览指南](#)

- 基本 DDoS 弹性架构示例

了解一些常见的 DDoS 弹性架构。

[浏览指南](#)

- AWS Shield 动画讲解视频

观看简短的视频介绍 AWS Shield。

[观看视频](#)

AWS Verified Access

- 教程：“已验证访问权限”入门

在本教程中，您将学习如何创建和配置已验证访问资源。

[浏览指南](#)

- AWS Verified Access 与第三方身份提供商集成

这篇博文向您展示了如何将验证访问权限 (AVA) 与第三方 Okta 身份提供商集成。

[浏览指南](#)

- AWS Verified Access 与设备信任提供商集成

这篇博文讨论了如何在上构建基于 Zero Trust 的远程连接 AWS。

[探索示例](#)

Amazon VPC Lattice

- Amazon VPC Lattice 是什么？

了解如何连接、保护和监控工作负载中的微服务。

[浏览指南](#)

- 设置 Amazon VPC Lattice

首次设置并启动 VPC 莱迪思。

[浏览指南](#)

- 使用 Amazon VPC Lattice 为您的应用程序构建安全的多账户多 VPC 连接

介绍如何使用 VPC Lattice 解决 VPC 连接难题。

[阅读博客](#)

- 亚马逊 VPC Lattice 动画讲解器

观看有关 VPC 莱迪思的简短动画视频。

[观看视频](#)

AWS WAF

- 什么是 AWS WAF ?

了解如何控制对工作负载的访问权限。

[浏览指南](#)

- 入门 AWS WAF

观看一段简短的视频，了解 AWS WAF 如何使用保护工作负载免受网络漏洞和机器人的攻击。

[观看视频](#)

- 视频简介 AWS WAF

观看简短的视频介绍 AWS WAF。

[观看视频](#)

Explore

- 架构图

浏览参考架构图，帮助您构建网络和内容交付架构 AWS。

[浏览架构图](#)

- 白皮书

浏览白皮书以帮助您入门，学习最佳实践，并了解您的网络和内容交付选项。

[浏览白皮书](#)

- AWS 解决方案

浏览经过审查的解决方案和架构指南，了解网络和内容交付的常见用例。

[探索 AWS 解决方案](#)

文档历史记录

下表描述了本决策指南的重要更改。要获取有关本指南更新的通知，您可以订阅 RSS feed。

变更	说明	日期
指南已更新	AWS 添加了数据传输终端。	2025 年 1 月 16 日
初次发布	指南首次出版。	2023 年 12 月 12 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。