

AWS Leitfaden zur Entscheidungsfindung

Auswahl eines AWS Networking- und Content-Delivery-Dienstes



Auswahl eines AWS Networking- und Content-Delivery-Dienstes: AWS Leitfaden zur Entscheidungsfindung

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

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, die Kunden zu verwirren oder Amazon in einer Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht Eigentum von Amazon sind, sind Eigentum ihrer jeweiligen Inhaber, die mit Amazon verbunden oder nicht verbunden oder von Amazon gesponsert oder nicht gesponsert sein können.

Table of Contents

Einführung 1

Verstehen 2

Erwägen Sie 4

Klicken Sie auf 9

Verwenden Sie 10

Erkunden 22

Dokumentverlauf 23

..... xxiv

Auswahl eines AWS Networking- und Content-Delivery-Dienstes

Zweck:

Finden Sie heraus, welche AWS Netzwerk- und Inhaltsbereitstellungsdienste für Ihr Unternehmen am besten geeignet sind.

Letzte Aktualisierung:

16. Januar 2025

Abgedeckte Dienstleistungen:

- [Amazon API Gateway](#)
- [AWS Client VPN](#)
- [AWS Cloud WAN](#)
- [Amazon CloudFront](#)
- [AWS Datenübertragungsterminal](#)
- [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](#)
- [Amazon VPC IPAM](#)
- [Amazon VPC Lattice](#)

- [AWS WAF](#)

Die Entscheidung für einen Ansatz für Cloud-Netzwerke und Inhaltsbereitstellung kann komplex sein, insbesondere wenn Sie es gewohnt sind, Netzwerke mit lokaler Hardware zu verwalten und zu konfigurieren. Zum Glück hat der [Aufbau von Netzwerken in der Cloud](#) dieselben Kernkonzepte wie der Aufbau vor Ort, wie z. B. IP-Adressierung, Lastenausgleich und Routing. Wenn Sie mit diesen Konzepten vertraut sind, können Sie besser verstehen, was AWS-Services Sie benötigen.

Amazon Web Services (AWS) bietet mehr als 20 speziell entwickelte Netzwerk- und Inhaltsbereitstellungsdienste, mit denen Sie Ihre Cloud-Netzwerke in all Ihren Cloud-Umgebungen und verteilten Cloud- und Edge-Standorten weltweit aufbauen, betreiben und sichern können. Sie können auch eine Netzwerkinfrastruktur aufbauen, auf die Ihre lokale Umgebung ausgedehnt wird.

AWS

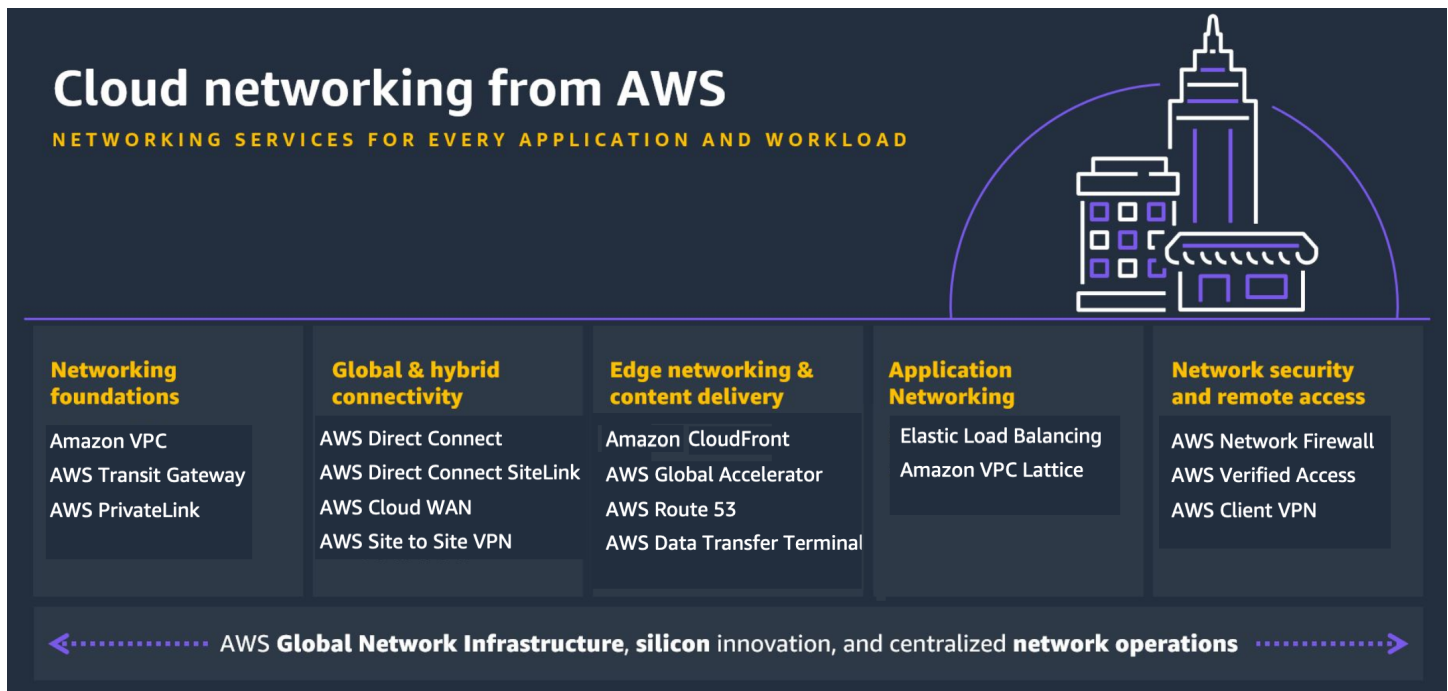
Dieser Entscheidungsleitfaden hilft Ihnen dabei, die richtigen Fragen zu stellen, um die Netzwerk- und Inhaltsbereitstellungsdienste und -tools auszuwählen, die Ihren Anforderungen entsprechen.

[Dieses Video bietet eine vierminütige Einführung in Netzwerke. AWS](#)

Verstehen

Was Sie einbauen, AWS hängt von Ihren Geschäftsanforderungen ab. In diesem Leitfaden verwenden wir den Begriff Workloads, um uns auf jede Sammlung von Ressourcen und Code zu beziehen, die einen geschäftlichen Nutzen bieten, z. B. eine kundenorientierte Anwendung oder einen Backend-Prozess.

Netzwerk- und Inhaltsbereitstellungsdienste AWS lassen sich in vier Kategorien einteilen: Netzwerkgrundlagen, globale und hybride Konnektivität, Edge-Netzwerke und Inhaltsbereitstellung sowie Anwendungsnetzwerke.



Grundlagen der Netzwerktechnik

AWS In werden Ihre Workloads in einer oder mehreren [Amazon Virtual Private Cloud \(VPCs\)](#) ausgeführt. Nachdem Ihre Workloads ausgeführt wurden VPCs, können Sie die Workloads mit anderen verbinden VPCs — z. B. mit einem [AWS Transit Gateway](#)— oder Sie können sie mit SaaS-Diensten (Software as a Service) verbinden, einschließlich anderer AWS-Services, wie z. [AWS PrivateLink](#). Mit Amazon VPC können Sie einen privaten, isolierten Bereich bereitstellen, in AWS Cloud dem Sie AWS Ressourcen in einem virtuellen Netzwerk mithilfe von kundendefinierten IP-Adressbereichen starten können. Amazon VPC bietet Ihnen mehrere Optionen, um Ihre AWS virtuellen Netzwerke mit anderen Remote-Netzwerken zu verbinden.

Globale und hybride Konnektivität

Sie können die Dienste in dieser Kategorie verwenden, um eine sichere Verbindung von lokalen Netzwerken zu Ihren Workloads in der herzustellen. AWS Cloud [Sie können ein virtuelles privates Netzwerk \(VPN\) erstellen, über das Sie Remotebenutzer verbinden AWS Client VPN, lokale Netzwerke verbinden oder ein globales Wide Area Network \(WAN\) mit AWS Cloud-WAN aufbauen. AWS Site-to-Site VPN](#) Sie können auch eine direkte, private Verbindung zum AWS Cloud Benutzer einrichten und so eine direkte, sichere Verbindung zur Cloud mit vorhersehbarer Leistung bereitstellen. [AWS Direct Connect](#) Möglicherweise müssen Sie auch Ihre lokalen Rechenzentren, Remote-Standorte und die Cloud verbinden. [Ein Hybridnetzwerk](#) kann diese verschiedenen Umgebungen verbinden.

Edge-Netzwerke und Bereitstellung von Inhalten

Dienste in dieser Kategorie tragen durch Caching und optimierten Transport zu einer höheren Leistung bei. Ein gutes Beispiel dafür ist [Amazon CloudFront](#). Sie sollten auch sicherstellen, dass der Kundenverkehr optimal weitergeleitet wird, um die Verfügbarkeit mithilfe von Diensten wie [Amazon Route 53](#) zu gewährleisten. Darüber hinaus ist es wichtig, dass der Kundenverkehr weitergeleitet wird, um das Beste aus der AWS globalen Infrastruktur herauszuholen, indem Dienste wie [AWS Global Accelerator](#) genutzt werden. Das [Datenübertragungsterminal](#) ist ein netzwerkfähiger, physischer Standort, an den Sie Ihre Datenspeichergeräte für eine schnelle Datenübertragung zum und vom bringen können. AWS Cloud

Netzwerke von Anwendungen

Mit [AWS App Mesh](#) zunehmender Akzeptanz sollten Sie darüber nachdenken AWS Cloud, wie Sie Workloads skalierbar verbinden können, indem Sie [Amazon VPC Lattice](#) verwenden, die Workloads in Ihrer Umgebung VPCs mithilfe [APIs](#) von [Amazon API Gateway](#) integrieren und die IP-Adressnutzung der in Ihrem VPCs System laufenden Ressourcen mithilfe von [Amazon VPC IP Address Manager \(IPAM\)](#) verwalten können. Wenn die Kundennachfrage steigt, können Sie mithilfe von [Elastic Load Balancing](#) sicherstellen, dass die Workloads in Ihren Workloads skaliert werden VPCs können und eine hohe Verfügbarkeit bieten.

Netzwerksicherheit und Fernzugriff

Amazon VPC hilft Ihnen zwar dabei, den Zugriff auf Ihre Workloads zu sichern, aber die Services in dieser Kategorie bieten einen verbesserten Schutz vor Bedrohungsakteuren und nicht autorisierten Benutzern, indem sie [AWS Network Firewall](#), [AWS Shield](#) [AWS Verified Access](#), und verwenden. [AWS WAF](#) Um die Netzwerksicherheit zu gewährleisten, sollten Sie die Verwendung von Amazon Route 53 DNS-Firewall, [AWS Network Firewall](#), [AWS Firewall Manager](#), [Netzwerkzugriffskontrolllisten](#) und Sicherheitsgruppen in Betracht ziehen.

Erwägen Sie

Es ist wichtig, dass Sie die Netzwerkdienste auswählen, die Ihren Geschäftsanforderungen entsprechen. Im Folgenden sind einige der Kriterien aufgeführt, die Sie bei der Auswahl von Netzwerkdiensten berücksichtigen sollten.

Business objectives

Welche Netzwerkdienste Sie wählen, hängt von Ihren Geschäftszielen ab. Beurteilen Sie, wo Sie sich gerade befinden und wo Sie sein möchten, wenn es um die Sicherheit, Zuverlässigkeit, Zugänglichkeit und Leistung Ihrer Workloads geht, die in der AWS Cloud ausgeführt werden.

- Überlegen Sie, wie die von Ihnen verwendeten Netzwerkdienste zu Ihren Migrations- und Integrationsstrategien passen. Eine [hybride Netzwerkarchitektur](#) kann Ihnen helfen, diesen Bedarf zu decken, indem Sie Ihr lokales Rechenzentrum integrieren und AWS.
- Lesen Sie die [Blogs zu Netzwerken und Inhaltsbereitstellung](#) im Let's Architect! AWS Blog-Serie, um zu sehen, was andere in der bauen AWS Cloud.
- Informieren Sie sich über die verfügbaren Optionen von Drittanbietern, mit denen Sie die Einführung von Netzwerkdiensten beschleunigen können. The [AWS Marketplace](#) bietet einen kuratierten digitalen Katalog, den Sie verwenden können, um Netzwerklösungen zu finden, zu kaufen und bereitzustellen.
- Entscheiden Sie, ob die Zusammenarbeit mit einem Unternehmen [AWS Partner](#), das sich auf Netzwerke und Inhaltsbereitstellung spezialisiert hat, von Vorteil wäre. Mitglieder von AWS Partner Network sind strategische Experten und erfahrene Bauherren, die Ihnen dabei helfen können, Ihre Anforderungen zu erfüllen AWS Cloud.
- Erfahren Sie mehr über die Teilnahme an [AWS Online-Netzwerkkursen](#) auf AWS Skill Builder, die Dienste wie Amazon VPC, AWS Cloud WAN und Amazon Route 53 abdecken.

Workload characteristics

Welche Netzwerkdienste Sie wählen, hängt von den Eigenschaften Ihrer Workloads ab.

- Netzwerkdienste haben jeweils eine bestimmte Rolle. Dienste wie AWS Cloud WAN AWS Transit Gateway eignen sich für die Verbindung von Workloads, die in VPCs ausgeführt werden. Amazon API Gateway erstellt öffentliche Inhalte, APIs sodass sich Ihre Kunden mit Ihren Workloads verbinden können. AWS Global Accelerator kann Ihnen helfen, die Zuverlässigkeit, Sicherheit und Latenz Ihrer Workloads zu verbessern.
- Mit dem weiteren Wachstum des Internets steigt auch der Bedarf an IP-Adressen für Geräte. Das gebräuchlichste Format für IP-Adressen ist IPv4. Das neueste Format für IP-Adressen ist IPv6. IPv6 bietet mehr Adressraum und löst das Problem der [IPv4 Adressüberlastung](#). AWS-Services Unterstützung für IPv6 beinhaltet Unterstützung für Dual-Stack-Konfigurationen (IPv4 oder IPv6) oder IPv6 nur Konfigurationen. Die Anzahl AWS-Services dieser IPv6

Unterstützungen wächst kontinuierlich. Welche Dienste derzeit unterstützt werden IPv6, finden Sie unter [AWS-Services diesem Support IPv6](#).

Data protection

Es ist wichtig, den Schutz Ihrer Daten in der zu berücksichtigen AWS Cloud.

- Unternehmen müssen Kundendaten vor sich entwickelnden Cyberrisiken schützen. Amazon VPC hilft Ihnen zwar dabei, den Zugriff auf die Workloads zu sichern VPCs, in denen Sie ausgeführt werden, sollten Sie jedoch erweiterte Datenschutzmaßnahmen wie, AWS Network Firewall AWS Shield AWS WAF, und Amazon Route 53 Resolver DNS-Firewall in Betracht ziehen.
- Es wird empfohlen, unabhängig vom Transport Verschlüsselung auf Anwendungsebene (TLS) als umfassende Schutzmaßnahme zur Wahrung der Vertraulichkeit zu verwenden. end-to-end
- Wenn Ihre Workloads eine Verbindung zu anderen VPCs benötigen AWS-Services, können Sie mithilfe von API-Endpunkten über das öffentliche Internet programmgesteuert eine Verbindung zu diesen Diensten herstellen. Wenn Sie jedoch Daten über eine private Verbindung senden möchten, verwenden Sie. AWS PrivateLink Viele Mitglieder von AWS Partner Network bieten ihre SaaS-Lösungen über AWS PrivateLink.

Availability

Verfügbarkeit ist die Fähigkeit einer Anwendung, die Verfügbarkeit aufrechtzuerhalten. Es ist wichtig, dass Ihre Kunden die Produkte und Services, die Sie in Ihr System integriert haben, VPCs mit minimalen oder gar keinen Ausfallzeiten nutzen können.

- Die AWS globale Infrastruktur basiert auf [AWS-Regionen Availability Zones](#). Wenn Sie Ihre Workloads in Ihren bereitstellen VPCs, sollten Sie sie in mehreren Availability Zones bereitstellen, um sicherzustellen, dass Ihr Workload auch bei einem Ausfall einer einzelnen Availability Zone verfügbar ist.
- Um die Verfügbarkeit, Skalierbarkeit, Sicherheit und Leistung der Workloads, die in Ihrem ausgeführt werden, zu verbessern VPCs, sollten Sie [Load Balancing \(Elastic Load Balancing\)](#) in Betracht ziehen. Sie können je nach den Anforderungen Ihrer Anwendungen verschiedene Arten von Load Balancern verwenden. Jeder Load Balancer unterstützt unterschiedliche Arten von Datenverkehr über verschiedene Protokolle und Netzwerkschichten, die auf das [Open Systems Interconnection \(OSI\) -Modell](#) abgestimmt sind. [Weitere Informationen zu den Unterschieden zwischen den Load Balancer-Typen finden Sie unter Produktvergleiche.](#)

Performance

Sie können Netzwerkdienste verwenden, um die Latenz-, Durchsatz- und Bandbreitenanforderungen Ihrer Workloads zu optimieren, die auf der AWS globalen Infrastruktur ausgeführt werden.

- Wenn Sie die Latenz für lokale Kunden, die Webanwendungen auf der ganzen Welt verwenden, minimieren möchten, sollten Sie Amazon in Betracht ziehen CloudFront. CloudFront ist ein [Netzwerk zur Bereitstellung von Inhalten](#), das Kunden Inhalte mit der geringstmöglichen Latenz bereitstellt.
- Wenn Sie Gaming-, Internet of Things- (IoT) - oder Voice over IP (VoIP) -Workloads ausführen, sollten Sie die Verwendung von AWS Global Accelerator. Dieser Service hilft Ihnen, die Verfügbarkeit und Leistung Ihrer Workloads zu verbessern.
- Wenn Ihre Workloads eine Verbindung zu anderen VPCs benötigen AWS-Regionen, können Sie mithilfe von öffentlichen API-Endpunkten programmgesteuert eine Verbindung zu diesen Diensten herstellen.

Operational excellence

Wenn Sie die AWS Cloud Akzeptanz erhöhen, sollten Sie jederzeit wissen, was in Ihren Workloads passiert. Tools und Services wie [Reachability Analyzer](#) und [Amazon CloudWatch Internet Monitor](#) können Ihnen helfen, mit den sich ändernden Geschäftsanforderungen und Prioritäten Schritt zu halten, wenn Ihre Workloads wachsen.

- Die Verwaltung der IP-Adressen von Workloads, die in mehreren VPCs ausgeführt werden, kann schwierig sein. Überlegen Sie, ob Sie die IP-Adressverwaltung für Ihre Workloads automatisieren müssen (Amazon VPC IPAM).
- Wenn Sie eine [Microservice-Architektur](#) verwenden, kann die Verwaltung der Konnektivität, Sicherheit und Überwachung zwischen Microservices eine Herausforderung sein. Überlegen Sie, ob Sie die Microservice-Interaktion (AWS App Mesh und Amazon VPC Lattice) automatisieren müssen.

Connectivity

Sie können Netzwerkdienste verwenden, um eine Verbindung zu den Netzwerken herzustellen AWS Cloud, Workloads zu verbinden oder zu verbinden.

- Beachten Sie Folgendes, wenn Sie eine Verbindung mit dem herstellen möchten: AWS Cloud

- Wenn Sie Remotebenutzer sicher mit Ihrem verbinden möchten VPCs, sollten Sie die Verwendung von AWS Client VPN.
- Wenn Sie ein gesamtes lokales Netzwerk sicher mit Ihrem verbinden möchten VPCs, sollten Sie die Verwendung von AWS Site-to-Site VPN.
- Wenn Sie eine konsistentere Leistung benötigen, als das Internet bieten kann, sollten Sie eine direkte Verbindung von Ihrem lokalen Netzwerk zu AWS (AWS Direct Connect in Betracht ziehen).
- Wenn Sie Daten schnell in das oder aus dem System verschieben müssen AWS Cloud, sollten Sie die Verwendung von AWS Data Transfer Terminal in Betracht ziehen.
- Beachten Sie beim Verbinden von Netzwerken Folgendes:
 - Wenn Sie mit mehreren arbeiten AWS-Regionen, Ihre eigenen Routing-Konfigurationen verwalten möchten oder lieber Ihre eigene Automatisierung verwenden möchten, sollten Sie die Verwendung von AWS Transit Gateway.
 - Wenn Sie Ihr Rechenzentrum, Ihre Niederlassung und Ihre AWS Netzwerke mit einem WAN vereinheitlichen möchten, sollten Sie AWS Cloud-WAN in Betracht ziehen. Es lohnt sich auch, darüber nachzudenken, ob Sie keine komplexen Routing-Konfigurationen verwalten oder Ihre eigenen Automatisierungen für Konnektivität in mehreren Regionen erstellen möchten.

Security

AWS bietet eine sichere Grundlage für die Erstellung und Bereitstellung Ihrer Anwendungen. Sie sind jedoch dafür verantwortlich, Ihre eigenen Sicherheitsmaßnahmen zum Schutz Ihrer Daten, Anwendungen und Netzwerkinfrastruktur zu implementieren, genauso wie Sie es in einem Rechenzentrum vor Ort tun würden.

- Machen Sie sich mit dem [Modell der AWS geteilten Verantwortung vertraut](#) und erfahren Sie, wie es sich auf die Sicherheit in der auswirkt AWS Cloud.
- AWS Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (NACLs) können zusammen oder einzeln verwendet werden, um ein Netzwerk zu schützen. So können Sie eine umfassende Sicherheitsstrategie entwickeln.
- Unternehmen müssen ihre Netzanwendungen vor neuen Cyberrisiken schützen. Überlegen Sie, ob Sie Ihre Workloads vor böswilligen Angriffen oder Malware (mit [AWS](#)

[Network Firewall](#)), Distributed-Denial-of-Service (DDoS) -Angriffen (mit AWS Shield) oder SQL-Injection und Cross-Site-Scripting-Angriffen (mit) schützen müssen. AWS WAF

Amazon Route 53 [AWS Firewall Manager](#), [Netzwerkzugriffskontrolllisten](#) und Sicherheitsgruppen sind ebenfalls wichtig, um die Netzwerksicherheit zu gewährleisten.

Klicken Sie auf

Nachdem Sie nun die Kriterien kennen, anhand derer Sie Ihre Netzwerk-Serviceoptionen bewerten werden, können Sie entscheiden, welche Dienste für Sie am besten geeignet sein könnten.

Servicekategorie	Wofür ist es optimiert?	AWS Netzwerk- und Inhaltsbereitstellungsdienste
Grundlagen von Netzwerken	Optimiert für die ersten Schritte mit AWS Netzwerkdiensten und die VPCs sichere Verbindung Ihrer Geräte.	Amazon VPC AWS PrivateLink AWS Transit Gateway
Globale und hybride Konnektivität	Optimiert, um private, sichere und globale Netzwerkonnektivität zu gewährleisten.	AWS Client VPN AWS Cloud WAN AWS Direct Connect AWS Site-to-Site VPN
Edge-Netzwerke und Inhaltsbereitstellung	Optimiert für eine zuverlässige Weiterleitung des Datenverkehrs zu und von Ihren Workloads mit niedriger Latenz.	Amazon CloudFront AWS Global Accelerator Amazon Route 53 AWS Datenübertragungsterminal
Netzwerke von Anwendungen	Optimiert, um sicherzustellen, dass Ihre Workloads hochverfügbar sind, sich an	Amazon API Gateway Amazon VPC IPAM

Servicekategorie	Wofür ist es optimiert?	AWS Netzwerk- und Inhaltsbereitstellungsdienste
	den Bedarf anpassen und miteinander kommunizieren können.	Amazon VPC Lattice Elastic Load Balancing
Netzwerksicherheit und Fernzugriff	Optimiert für den Schutz Ihrer Workloads vor Malware, DDoS, SQL-Injection und Cross-Site-Scripting-Angriffen.	AWS Firewall Manager
		AWS Network Firewall
		AWS Shield
		AWS Verified Access AWS WAF

Verwenden Sie

Um zu erfahren, wie Sie die einzelnen verfügbaren AWS Netzwerkdienste verwenden können, und um mehr über sie zu erfahren, haben wir eine Anleitung zur Funktionsweise der einzelnen Dienste bereitgestellt. Der folgende Abschnitt enthält Links zu ausführlicher Dokumentation, praktischen Tutorials und Ressourcen, die Ihnen den Einstieg erleichtern.

Die folgenden Dienste decken globale Netzwerke und VPC-Konnektivität ab.

Amazon CloudFront

- Was ist Amazon CloudFront?

Erfahren Sie, wie Sie die Verbreitung von Inhalten beschleunigen können.

[Den Leitfaden erkunden](#)

- Erste Schritte mit Amazon CloudFront

Erfahren Sie die grundlegenden Schritte zur Bereitstellung von Inhalten mit CloudFront.

[Den Leitfaden erkunden](#)

- Hosten von On-Demand-Streaming-Videos mit Amazon S3 CloudFront, Amazon und Amazon Route 53

Erfahren Sie, wie Sie Videos für die On-Demand-Anzeige auf sichere und skalierbare Weise hosten können.

[Erste Schritte mit dem Tutorial](#)

- Schnellere Bereitstellung von Inhalten mit Amazon CloudFront

Erfahren Sie, wie Sie die Latenz Ihrer Webanwendungen für Endbenutzer verringern können.

[Erste Schritte mit dem Tutorial](#)

AWS Cloud WAN

- Was ist AWS Cloud-WAN?

Erfahren Sie, wie Sie ein einheitliches globales Netzwerk aufbauen, verwalten und überwachen.

[Den Leitfaden erkunden](#)

- Wir stellen vor: AWS Cloud WAN

Erfahren Sie mehr über die wichtigsten Anwendungsfälle für AWS Cloud WAN und wie Sie damit beginnen können.

[Lesen Sie den Blog](#)

- Erste Schritte mit AWS Cloud WAN

Erstellen Sie Ihr erstes globales Netzwerk und fügen Sie eine VPC hinzu.

[Erste Schritte mit dem Tutorial](#)

AWS Direct Connect

- Was ist AWS Direct Connect?

Erfahren Sie, wie Sie ein lokales Netzwerk mit AWS verbinden.

[Den Leitfaden erkunden](#)

- Erste Schritte mit AWS Direct Connect

Sehen Sie sich eine kurze Einführung in Ihr lokales Netzwerk an AWS Direct Connect und wie Sie es vorbereiten können, um AWS eine Verbindung herzustellen.

[Video ansehen](#)

- Connect Sie Ihr Rechenzentrum mit AWS

Connect Sie Ihr Rechenzentrum AWS mit der Nutzung von AWS Direct Connect.

[Erste Schritte mit dem Tutorial](#)

AWS Global Accelerator

- Was ist AWS Global Accelerator?

Erfahren Sie, wie Sie die Leistung Ihrer Workloads verbessern können.

[Den Leitfaden erkunden](#)

- Erste Schritte mit einem Standardbeschleuniger

Erstellen Sie einen Beschleuniger, um die Netzwerkleistung eines Workloads zu verbessern, der auf einer EC2 Instance ausgeführt wird.

[Erste Schritte mit dem Tutorial](#)

- Verbessern Sie die globale Verfügbarkeit und Leistung Ihrer Anwendungen für Ihren Datenverkehr

Sehen Sie sich eine kurze Demonstration zur Einrichtung AWS Global Accelerator zur Verbesserung der Netzwerkleistung an.

[Video ansehen](#)

AWS PrivateLink

- Was ist AWS PrivateLink?

Erfahren Sie, wie Sie Ihre VPC privat mit Diensten verbinden.

[Den Leitfaden erkunden](#)

- Fangen Sie an mit AWS PrivateLink

Senden Sie eine Anfrage von einer EC2 Instance in einem privaten Subnetz an Amazon CloudWatch über PrivateLink.

[Erste Schritte mit dem Tutorial](#)

- Beschleunigen Sie Ihre IPv6 Einführung mit PrivateLink Services und Endpunkten

Kunden mit großer Internetpräsenz spüren die Belastung durch die Erschöpfung der öffentlichen Adressen. IPv4 Erfahren Sie, wie Sie die IPv6 Nutzung innerhalb VPCs der Nutzung erhöhen können. PrivateLink

[Lesen Sie den Blog](#)

Amazon Route 53

- Was ist Amazon Route 53?

Erfahren Sie mehr über die hochverfügbare und skalierbare Auflösung von Domainnamen.

[Den Leitfaden erkunden](#)

- Tutorials zu Amazon Route 53-Anwendungsfällen

So verwenden Sie Route 53 für Anwendungsfälle, die auf Traffic und Latenz basieren.

[Erste Schritte mit dem Tutorial](#)

- So registrieren Sie einen Domainnamen bei Amazon Route 53

Dieses Tutorial hilft Ihnen bei der Registrierung eines neuen Domainnamens für eine Webanwendung.

[Erste Schritte mit dem Tutorial](#)

- Einführung in Amazon Route 53

Sehen Sie sich eine kurze Einführung in die Auflösung von Domainnamen und Route 53 an.

[Video ansehen](#)

AWS Data Transfer Terminal

- Was ist ein AWS Datenübertragungsterminal?

Erfahren Sie, wie Sie AWS Cloud mit Ihren eigenen Speichergeräten schnell große Datensätze hoch- oder herunterladen können.

[Den Leitfaden erkunden](#)

- Wir stellen vor: AWS Data Transfer Terminal

Erfahren Sie mehr über die wichtigsten Anwendungsfälle und die ersten Schritte.

[Lesen Sie den Blog](#)

AWS Site-to-Site VPN

- Was ist AWS Site-to-Site VPN?

Erfahren Sie, wie Sie Remote-Benutzer AWS über VPN verbinden können.

[Den Leitfaden erkunden](#)

- Erste Schritte mit AWS Site-to-Site VPN

Richten Sie eine Site-to-Site VPN-Verbindung zwischen einem lokalen Gerät und AWS ein.

[Erste Schritte mit dem Tutorial](#)

- AWS Site-to-Site VPN, Auswahl der richtigen Optionen zur Leistungsoptimierung

Wählen Sie die besten Optionen beim Einrichten einer VPN-Verbindung zu AWS.

[Lesen Sie den Blog](#)

AWS Transit Gateway

- What is a transit gateway?

Erfahren Sie, wie Sie sich VPCs mit Transit-Gateways verbinden.

[Den Leitfaden erkunden](#)

- Beispiele für Anwendungsfälle für Transit-Gateways

Sehen Sie sich häufig vorkommende Anwendungsfälle für Transit-Gateways an.

[Den Leitfaden erkunden](#)

- AWS Transit Gateway Werkstatt

In diesem praxisnahen Workshop erfahren Sie, wie Sie Transit Gateway in Konfigurationen mit einer Region und einem Konto, mehreren Konten und mehreren Regionen einsetzen.

[Starten Sie den Workshop](#)

Amazon VPC

- Was ist Amazon VPC?

Erfahren Sie mehr über virtuelle private Clouds und die Funktionen von Amazon VPC.

[Den Leitfaden erkunden](#)

- Erste Schritte mit Amazon VPC

Ein Leitfaden für den schnellen Einstieg in Amazon VPC.

[Den Leitfaden erkunden](#)

- Beispiel für VPC-Konfigurationen

Sehen Sie sich Beispiele VPC VPC-Konfigurationen an, die auf verschiedenen Anwendungsfällen basieren.

[Den Leitfaden erkunden](#)

- Modulare und skalierbare VPC-Architektur

Bauen Sie eine virtuelle Netzwerkgrundlage auf, die auf AWS bewährten Methoden für Ihre AWS Cloud Infrastruktur basiert.

[Erste Schritte mit dem Tutorial](#)

Amazon VPC IPAM

- Was ist IPAM?

Erfahren Sie, wie Sie die Nutzung von IP-Adressen verfolgen und verwalten können.

[Den Leitfaden erkunden](#)

- Bewährte Methoden für Amazon VPC IP Address Manager (IPAM)

Erfahren Sie, wie Sie einen skalierbaren IP-Adressverwaltungsplan erstellen.

[Lesen Sie den Blog](#)

- Erstellen Sie Pools zur Verwaltung Ihres IP-Bereichs

Sehen Sie sich ein kurzes Einführungsvideo zu VPC IPAM an.

[Video ansehen](#)

Die folgenden Dienste beziehen sich auf Netzwerke auf Anwendungsebene.

Amazon API Gateway

- Was ist Amazon API Gateway?

Erfahren Sie, wie Sie Workloads APIs für Ihre Workloads erstellen.

[Den Leitfaden erkunden](#)

- Bauen APIs mit Amazon API Gateway

Erfahren Sie, wie Sie mit dem Bauen APIs beginnen können AWS.

[Video ansehen](#)

- Konfiguration privater Integrationen mit Amazon API Gateway HTTP APIs

Erfahren Sie, wie Sie eine API erstellen, um den privaten Zugriff auf Ressourcen in einer VPC zu kontrollieren.

[Lesen Sie den Blog](#)

AWS Client VPN

- Was ist AWS Client VPN?

Erfahren Sie, wie Sie Netzwerke AWS über VPN verbinden.

[Den Leitfaden erkunden](#)

- Erste Schritte mit AWS Client VPN

Laden Sie die AWS Client VPN Anwendung herunter und stellen Sie AWS über VPN eine Verbindung her.

[Den Leitfaden erkunden](#)

- Szenarien und Beispiele für AWS Client VPN

Sehen Sie sich Beispiele für die Erstellung und Konfiguration des Client-VPN-Zugangs für Ihre Kunden an.

[Erkunden Sie die Beispiele](#)

Elastic Load Balancing

- Was ist Elastic Load Balancing?

Erfahren Sie, wie Sie den eingehenden Traffic auf Ihre Workloads verteilen.

[Den Leitfaden erkunden](#)

- Erste Schritte mit Elastic Load Balancing

Lernen Sie den Unterschied zwischen den verschiedenen Arten von Load Balancern kennen und erstellen Sie einen Load Balancer.

[Den Leitfaden erkunden](#)

- So wählen Sie den richtigen Load Balancer für Ihre Workloads AWS

Wählen Sie die richtige Option für den Lastenausgleich des Datenverkehrs auf Ihre Workloads.

[Video ansehen](#)

AWS Firewall Manager

- Erste Schritte mit Richtlinien AWS Firewall Manager

Erfahren Sie, wie AWS Firewall Manager Sie verschiedene Arten von Sicherheitsrichtlinien aktivieren können.

[Den Leitfaden erkunden](#)

- Wie lassen sich Sicherheitsgruppen kontinuierlich überwachen und einschränken mit AWS Firewall Manager

In diesem Blogbeitrag wird gezeigt, wie Sie AWS Firewall Manager Sicherheitsgruppen einschränken können, um sicherzustellen, dass nur die erforderlichen Ports geöffnet sind.

[Den Leitfaden erkunden](#)

- Wird verwendet AWS Firewall Manager , um Schutz in großem Umfang bereitzustellen in AWS Organizations

Dieser Beitrag enthält step-by-step Anweisungen zur Implementierung und Verwaltung von Sicherheitsrichtlinien in Ihrer gesamten AWS Organizations Implementierung mithilfe von AWS Firewall Manager.

[Den Leitfaden erkunden](#)

AWS Network Firewall

- Was ist AWS Network Firewall?

Erfahren Sie mehr über Netzwerk-Firewall und Angriffserkennung.

[Den Leitfaden erkunden](#)

- Erste Schritte mit AWS Network Firewall

Erstellen und verwalten Sie schnell eine Netzwerk-Firewall für eine VPC.

[Erste Schritte mit dem Tutorial](#)

- AWS Network Firewall animiertes Erklärvideo

Sehen Sie sich ein kurzes Einführungsvideo zu an. AWS Network Firewall

[Video ansehen](#)

AWS Shield

- Was ist AWS Shield?

Erfahren Sie mehr über DDo S-Schutz.

[Den Leitfaden erkunden](#)

- Beispiele für grundlegende DDo S-Resilient-Architekturen

Erfahren Sie mehr über einige gängige DDo S-Resilient-Architekturen.

[Den Leitfaden erkunden](#)

- AWS Shield animiertes Erklärvideo

Sehen Sie sich ein kurzes Einführungsvideo zu an. AWS Shield

[Video ansehen](#)

AWS Verified Access

- Tutorial: Erste Schritte mit Verified Access

In diesem Tutorial erfahren Sie, wie Sie Ressourcen mit verifiziertem Zugriff erstellen und konfigurieren.

[Den Leitfaden erkunden](#)

- AWS Verified Access Integration mit Identitätsanbietern von Drittanbietern

In diesem Blogbeitrag erfahren Sie, wie Sie Verified Access (AVA) in den externen Identitätsanbieter von Okta integrieren.

[Den Leitfaden erkunden](#)

- Integration AWS Verified Access mit Vertrauensanbietern für Geräte

In diesem Blogbeitrag wird erläutert, wie auf Zero Trust basierende Fernkonnektivität aufgebaut werden kann AWS.

[Erkunden Sie die Beispiele](#)

Amazon VPC Lattice

- Was ist Amazon VPC Lattice?

Erfahren Sie, wie Sie die Microservices in Ihren Workloads verbinden, sichern und überwachen können.

[Den Leitfaden erkunden](#)

- Amazon VPC Lattice einrichten

Richten Sie VPC Lattice ein und starten Sie es zum ersten Mal.

[Den Leitfaden erkunden](#)

- Bauen Sie mit Amazon VPC Lattice sichere Multi-VPC-Konnektivität für mehrere Konten für Ihre Anwendungen auf

Eine Einführung in die Verwendung von VPC Lattice zur Lösung von VPC-Konnektivitätsproblemen.

[Lesen Sie den Blog](#)

- Animierte Erklärung zu Amazon VPC Lattice

Sehen Sie sich ein kurzes animiertes Video über VPC Lattice an.

[Video ansehen](#)

AWS WAF

- Was ist? AWS WAF

Erfahren Sie, wie Sie den Zugriff auf Ihre Workloads kontrollieren können.

[Den Leitfaden erkunden](#)

- Erste Schritte mit AWS WAF

Sehen Sie sich ein kurzes Video an, das zeigt, wie AWS WAF Sie Ihre Workloads vor Web-Exploits und Bots schützen können.

[Video ansehen](#)

- Videoeinführung zu AWS WAF

Sehen Sie sich eine kurze Videoeinführung zu an AWS WAF.

[Video ansehen](#)

Erkunden

- Architekturdiagramme

Sehen Sie sich Referenzarchitekturdiagramme an, die Sie beim Aufbau Ihrer Netzwerk- und Content-Delivery-Architekturen unterstützen. AWS

[Erkunden Sie Architekturdiagramme](#)

- Whitepapers

Schauen Sie sich Whitepapers an, die Ihnen den Einstieg erleichtern, bewährte Verfahren kennenlernen und sich mit Ihren Netzwerk- und Inhaltsbereitstellungsoptionen vertraut machen.

[Entdecken Sie Whitepapers](#)

- AWS Lösungen

Informieren Sie sich über geprüfte Lösungen und Architekturanleitungen für gängige Anwendungsfälle für Netzwerke und Inhaltsbereitstellung.

[Entdecken Sie Lösungen AWS](#)

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an diesem Entscheidungsleitfaden beschrieben. Für Benachrichtigungen über Aktualisierungen dieses Handbuchs können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Leitfaden aktualisiert	AWS Datenübertragungsterminal hinzugefügt.	16. Januar 2025
Erste Veröffentlichung	Leitfaden zuerst veröffentlicht.	12. Dezember 2023

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.