

Scelta AWS di un servizio di networking e distribuzione di contenuti



Scelta AWS di un servizio di networking e distribuzione di contenuti: AWS Guida decisionale

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

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Introduzione 1

Comprendi 2

Considera 4

Scegliere 8

Utilizzo 10

Esplora 21

Cronologia dei documenti 23

..... xxiv

Scelta AWS di un servizio di networking e distribuzione di contenuti

Scopo:

Aiutateci a determinare quali servizi di AWS rete e distribuzione di contenuti sono più adatti alla vostra organizzazione.

Ultimo aggiornamento:

16 gennaio 2025

Servizi coperti:

- [Gateway Amazon API](#)
- [AWS Client VPN](#)
- [Cloud AWS WAN](#)
- [Amazon CloudFront](#)
- [AWS Terminale di trasferimento dati](#)
- [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](#)
- [Accesso verificato da AWS](#)
- [Amazon VPC](#)
- [Amazon VPC IPAM](#)
- [Amazon VPC Lattice](#)

- [AWS WAF](#)

Decidere un approccio al cloud networking e alla distribuzione dei contenuti può essere complesso, soprattutto se sei abituato a gestire e configurare reti con hardware locale. Fortunatamente, la [creazione di reti nel cloud](#) condivide concetti fondamentali con la creazione locale, come l'indirizzamento IP, il bilanciamento del carico e il routing. La familiarità con questi concetti ti aiuterà a capire di cosa hai bisogno. Servizi AWS

Amazon Web Services (AWS) offre oltre 20 servizi di rete e distribuzione di contenuti appositamente progettati che puoi utilizzare per creare, gestire e proteggere le tue reti cloud in tutti i tuoi ambienti cloud e cloud distribuiti e location periferiche a livello globale. Puoi anche creare un'infrastruttura di rete che estenda il tuo ambiente locale a AWS.

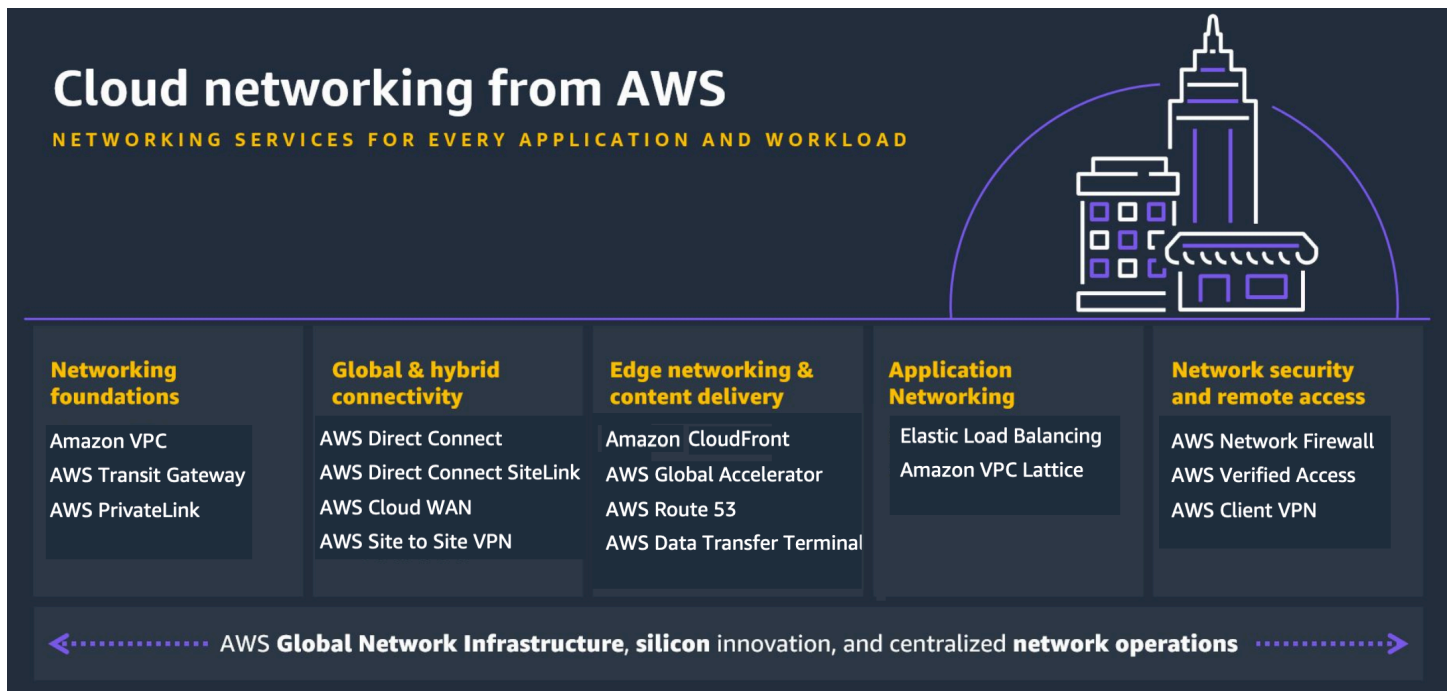
Questa guida decisionale ti aiuterà a porre le domande giuste per scegliere i servizi e gli strumenti di rete e distribuzione dei contenuti più adatti alle tue esigenze.

[Questo video fornisce un'introduzione di quattro minuti al AWS networking.](#)

Comprendi

Ciò che integri AWS dipende dalle tue esigenze aziendali. In questa guida, utilizziamo il termine carichi di lavoro per fare riferimento a qualsiasi raccolta di risorse e codice che offra valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo di backend.

I servizi di rete e distribuzione di contenuti AWS rientrano in quattro categorie: basi di rete, connettività globale e ibrida, rete perimetrale e distribuzione di contenuti e reti di applicazioni.



Fondamenti di rete

Nel AWS, i tuoi carichi di lavoro vengono eseguiti all'interno di uno o più [Amazon Virtual Private Cloud \(VPCs\)](#). Dopo l'esecuzione dei carichi di lavoro VPCs, puoi connetterli ad altri, ad VPCs esempio, [AWS Transit Gateway](#) oppure collegarli a servizi Software as a Service (SaaS), inclusi altri, ad esempio. Servizi AWS [AWS PrivateLink](#) Amazon VPC consente di effettuare il provisioning di una sezione privata e isolata Cloud AWS in cui è possibile avviare AWS risorse in una rete virtuale utilizzando intervalli di indirizzi IP definiti dal cliente. Amazon VPC offre diverse opzioni per connettere le tue reti AWS virtuali con altre reti remote.

Connettività globale e ibrida

Puoi utilizzare i servizi di questa categoria per connetterti in modo sicuro dalle reti locali ai tuoi carichi di lavoro in. Cloud AWS [Puoi creare una rete privata virtuale \(VPN\) per connettere utenti remoti utilizzando AWS Client VPN, connettere reti locali utilizzando o creare una rete WAN \(Global Wide Area Network\) con AWS Site-to-Site VPN Cloud WAN.](#) AWS Puoi anche configurare una connessione diretta e privata all' Cloud AWS utilizzo [AWS Direct Connect](#), fornendo una connessione diretta e sicura al cloud con prestazioni prevedibili. Potrebbe inoltre essere necessario connettere i data center locali, i siti remoti e il cloud. [Una rete ibrida](#) può connettere questi diversi ambienti.

Rete perimetrale e distribuzione dei contenuti

I servizi di questa categoria aiutano a garantire prestazioni più elevate attraverso la memorizzazione nella cache e il trasporto ottimizzato. Un buon esempio di ciò è [Amazon CloudFront](#). Ti consigliamo inoltre di vedere il traffico dei clienti indirizzato in modo ottimale per garantire la disponibilità utilizzando servizi come [Amazon Route 53](#). Inoltre, è importante che il traffico dei clienti venga indirizzato per sfruttare al meglio l'infrastruttura AWS globale che utilizza servizi come [AWS Global Accelerator](#) [AWS Data Transfer Terminal](#) è una posizione fisica predisposta per la rete in cui è possibile portare i dispositivi di archiviazione dati per un trasferimento rapido dei dati da e verso il Cloud AWS

Rete delle applicazioni

Man mano che aumenterai l'adozione di Cloud AWS, ti consigliamo di considerare come connettere carichi di lavoro su larga scala utilizzando [AWS App Mesh](#) [Amazon VPC](#) Lattice, integrare i carichi di lavoro nel VPCs tuo [APIs](#) ambiente utilizzando [Amazon API Gateway](#) e gestire l'utilizzo degli indirizzi IP delle risorse in esecuzione nel tuo sistema VPCs utilizzando [Amazon VPC](#) IP Address Manager (IPAM). Con l'aumento della domanda dei clienti, puoi contribuire a garantire la scalabilità e l'elevata disponibilità dei tuoi VPCs carichi di lavoro utilizzando [Elastic Load Balancing](#).

Sicurezza di rete e accesso remoto

Sebbene Amazon VPC ti aiuti ad accedere in modo sicuro ai tuoi carichi di lavoro, i servizi di questa categoria offrono una protezione avanzata contro gli autori delle minacce e gli utenti non autorizzati utilizzando [AWS Network Firewall](#), [AWS Shield](#), [Accesso verificato da AWS](#) [AWS WAF](#) Per contribuire a garantire la sicurezza della rete, prendi in considerazione l'utilizzo di Amazon Route 53 DNS Firewall, [AWS Network Firewall](#), [AWS Firewall Manager](#), [liste di controllo degli accessi alla rete](#) e gruppi di sicurezza.

Considera

È importante scegliere i servizi di rete più adatti alle esigenze aziendali. Di seguito sono riportati alcuni dei criteri da considerare nella scelta dei servizi di rete.

Business objectives

I servizi di rete scelti dipenderanno dai tuoi obiettivi aziendali. Valuta dove ti trovi ora e dove vuoi essere in termini di sicurezza, affidabilità, accessibilità e prestazioni dei tuoi carichi di lavoro in esecuzione su Cloud AWS

- Valuta in che modo i servizi di rete che utilizzi si adattano alle tue strategie di migrazione e integrazione. Un'[architettura di rete ibrida](#) può aiutarti a soddisfare questa esigenza integrando il tuo data center locale e AWS.
- Consulta i [blog sulle reti e sulla distribuzione dei contenuti in Let's architect!](#) AWS serie di blog per vedere cosa stanno costruendo gli altri nel Cloud AWS.
- Esamina le opzioni di terze parti disponibili per aiutarti ad accelerare l'adozione dei servizi di rete. [Marketplace AWS](#) Fornisce un catalogo digitale curato che puoi utilizzare per trovare, acquistare e implementare soluzioni di rete.
- Decidi se lavorare con una [AWS Partner](#) società specializzata in reti e distribuzione di contenuti sarebbe utile. I membri di AWS Partner Network sono esperti strategici e costruttori esperti che possono aiutarti a soddisfare le tue esigenze con il Cloud AWS.
- Esplora i [corsi online AWS di networking](#) su AWS Skill Builder che coprono servizi come Amazon VPC AWS , Cloud WAN e Amazon Route 53.

Workload characteristics

I servizi di rete che scegli dipenderanno dalle caratteristiche dei tuoi carichi di lavoro.

- I servizi di rete hanno ciascuno un ruolo particolare. Servizi come AWS Cloud WAN AWS Transit Gateway sono adatti per connettere carichi di lavoro in esecuzione in VPCs. Amazon API Gateway crea contenuti pubblici APIs in modo che i tuoi clienti possano connettersi ai tuoi carichi di lavoro. AWS Global Accelerator può aiutarti a migliorare l'affidabilità, la sicurezza e la latenza dei tuoi carichi di lavoro.
- Con la continua crescita di Internet, aumenta anche la necessità di indirizzi IP per i dispositivi. Il formato più comune per gli indirizzi IP è IPv4. Il formato più recente per gli indirizzi IP è IPv6. IPv6 offre più spazio di indirizzamento e risolve il problema dell'[esaurimento degli IPv4 indirizzi](#). Servizi AWS il supporto per IPv6 include il supporto per la configurazione dual stack (IPv4 o IPv6) o IPv6 solo per le configurazioni. Il numero di Servizi AWS tale supporto IPv6 è in continua crescita. Per visualizzare i servizi attualmente supportati IPv6, consulta [Servizi AWS il relativo supporto IPv6](#).

Data protection

È importante considerare la protezione dei dati in Cloud AWS.

- Le aziende devono proteggere i dati dei clienti dall'evoluzione dei rischi informatici. Sebbene Amazon VPC ti aiuti a proteggere l'accesso ai carichi di lavoro in esecuzione VPCs, prendi in considerazione misure avanzate di protezione dei dati, come AWS Network Firewall AWS Shield AWS WAF, e Amazon Route 53 Resolver DNS Firewall.
- Si consiglia di utilizzare la crittografia a livello di applicazione (TLS), indipendentemente dal trasporto, come misura di difesa approfondita per garantire la riservatezza. end-to-end
- Se i carichi di lavoro VPCs devono essere collegati ad altri Servizi AWS, puoi connetterti a tali servizi in modo programmatico utilizzando gli endpoint API sulla rete Internet pubblica. Tuttavia, se desideri inviare dati tramite una connessione privata, usa. AWS PrivateLink Molti membri AWS Partner Network offrono le proprie soluzioni SaaS tramite. AWS PrivateLink

Availability

La disponibilità è la capacità di un'applicazione di mantenere l'operatività. È importante che i clienti possano utilizzare i prodotti e i servizi integrati VPCs con tempi di inattività minimi o nulli.

- L'infrastruttura AWS globale è basata su [zone Regioni AWS di disponibilità](#). Quando si distribuiscono i carichi di lavoro nella propria VPCs, è necessario eseguire la distribuzione in più zone di disponibilità per garantire che il carico di lavoro sia ancora disponibile in caso di guasto di una singola zona di disponibilità.
- Per migliorare la disponibilità, la scalabilità, la sicurezza e le prestazioni dei carichi di lavoro in esecuzione sul tuo computer VPCs, prendi in considerazione il bilanciamento del [carico \(Elastic Load Balancing\)](#). È possibile utilizzare diversi tipi di sistemi di bilanciamento del carico a seconda delle esigenze delle applicazioni. Ogni sistema di bilanciamento del carico supporta diversi tipi di traffico su diversi protocolli e livelli di rete allineati al modello [Open Systems Interconnection](#) (OSI). [Per ulteriori informazioni sulle differenze tra i tipi di bilanciamento del carico, consulta i confronti tra i prodotti.](#)

Performance

Puoi utilizzare i servizi di rete per ottimizzare i requisiti di latenza, velocità effettiva e larghezza di banda dei carichi di lavoro in esecuzione sull'infrastruttura globale. AWS

- Se desideri ridurre al minimo la latenza per i clienti locali che utilizzano applicazioni Web in tutto il mondo, prendi in considerazione l'utilizzo di Amazon CloudFront. CloudFront è una [rete di distribuzione di contenuti](#) che fornisce contenuti ai clienti con la latenza più bassa possibile.

- Se utilizzi carichi di lavoro di gioco, Internet of Things (IoT) o Voice over IP (VoIP), prendi in considerazione l'utilizzo. AWS Global Accelerator Questo servizio ti aiuta a migliorare la disponibilità e le prestazioni dei tuoi carichi di lavoro.
- Se i carichi di lavoro VPCs devono essere collegati ad altre Regioni AWS, puoi connetterti a tali servizi in modo programmatico utilizzando endpoint API pubblici.

Operational excellence

Man mano che aumenterai Cloud AWS l'adozione, vorrai capire cosa sta succedendo ai tuoi carichi di lavoro in qualsiasi momento. Strumenti e servizi come [Reachability Analyzer](#) e [CloudWatch Amazon](#) Internet Monitor possono aiutarti a stare al passo con le mutevoli esigenze e priorità aziendali man mano che i carichi di lavoro crescono.

- La gestione degli indirizzi IP dei carichi di lavoro in esecuzione su più VPCs file può essere difficile. Valuta se devi automatizzare la gestione degli indirizzi IP tra i tuoi carichi di lavoro (Amazon VPC IPAM).
- Se utilizzi un'[architettura di microservizi](#), la gestione della connettività, della sicurezza e del monitoraggio tra i microservizi può essere una sfida. Valuta se devi automatizzare l'interazione con i microservizi (e AWS App Mesh Amazon VPC Lattice).

Connectivity

Puoi utilizzare i servizi di rete per connetterti a Cloud AWS, connettere carichi di lavoro o connettere reti.

- Considerate quanto segue per il collegamento a: Cloud AWS
 - Se desideri connettere in modo sicuro gli utenti remoti al tuo VPCs, prendi in considerazione l'utilizzo AWS Client VPN di.
 - Se desideri connettere in modo sicuro un'intera rete locale alla tua VPCs, prendi in considerazione l'utilizzo di. AWS Site-to-Site VPN
 - Se hai bisogno di prestazioni più costanti di quelle fornite da Internet, prendi in considerazione una connessione diretta dalla rete locale a AWS ().AWS Direct Connect
 - Se hai bisogno di spostare rapidamente i dati dentro o fuori da Cloud AWS, prendi in considerazione l'utilizzo di AWS Data Transfer Terminal.
- Considera quanto segue per connettere le reti:

- Se operi su più piattaforme Regioni AWS, desideri gestire le tue configurazioni di routing o preferisci utilizzare una tua automazione, prendi in considerazione l'utilizzo di AWS Transit Gateway
- Se desideri unificare il data center, la filiale e le AWS reti con una WAN, prendi in considerazione l'utilizzo AWS di Cloud WAN. Vale la pena prenderla in considerazione anche se non desideri gestire configurazioni di routing complesse o creare automazioni personalizzate per la connettività multiregionale.

Security

AWS fornisce una base sicura per la creazione e la distribuzione delle applicazioni, ma l'utente è responsabile dell'implementazione delle proprie misure di sicurezza per proteggere i dati, le applicazioni e l'infrastruttura di rete, non diversamente da quanto si farebbe in un data center in loco.

- Esamina e comprendi il [modello di responsabilitàAWS condivisa](#) e come si applica alla sicurezza in Cloud AWS
- AWS i gruppi di sicurezza e gli elenchi di controllo degli accessi alla rete (NACLs) possono essere utilizzati insieme o singolarmente per proteggere una rete, aiutandovi a creare una strategia di difesa approfondita.
- Le aziende devono proteggere le proprie applicazioni di rete dall'evoluzione dei rischi informatici. Valuta se avrai bisogno di proteggere i tuoi carichi di lavoro da attacchi dannosi o malware (con [AWS Network Firewall](#)), attacchi Distributed Denial of Service (DDoS) (con AWS Shield) o attacchi SQL injection e cross-site scripting (con). AWS WAF

Anche Amazon Route 53 [AWS Firewall Manager](#), [le liste di controllo degli accessi alla rete](#) e i gruppi di sicurezza sono importanti da considerare per garantire la sicurezza della rete.

Scegliere

Ora che conosci i criteri in base ai quali valuterai le opzioni dei tuoi servizi di rete, sei pronto a scegliere quali servizi potrebbero essere più adatti.

Categoria di servizio	Per cosa è ottimizzato?	AWS servizi di networking e distribuzione di contenuti
Fondamenti di rete	Ottimizzato per iniziare a utilizzare i servizi AWS di rete e connettersi VPCs in modo sicuro.	Amazon VPC AWS PrivateLink AWS Transit Gateway
Connettività globale e ibrida	Ottimizzato per garantire una connettività di rete privata, sicura e globale.	AWS Client VPN Cloud AWS WAN AWS Direct Connect AWS Site-to-Site VPN
Rete perimetrale e distribuzione dei contenuti	Ottimizzato per un routing del traffico affidabile e a bassa latenza da e verso i carichi di lavoro.	Amazon CloudFront AWS Global Accelerator Amazon Route 53 AWS Terminale di trasferimento dati
Rete delle applicazioni	Ottimizzato per garantire che i carichi di lavoro siano altamente disponibili, si adattino alla domanda e possano comunicare tra loro.	Gateway Amazon API Amazon VPC IPAM Amazon VPC Lattice Elastic Load Balancing
Sicurezza di rete e accesso remoto	Ottimizzato per proteggere i carichi di lavoro da malware, DDoS, SQL injection e attacchi di cross-site scripting.	AWS Firewall Manager AWS Network Firewall AWS Shield Accesso verificato da AWS

Categoria di servizio	Per cosa è ottimizzato?	AWS servizi di networking e distribuzione di contenuti
		AWS WAF

Utilizzo

Per scoprire come utilizzare e saperne di più su ciascuno dei servizi di AWS rete disponibili, abbiamo fornito un percorso per scoprire come funziona ciascuno di essi. La sezione seguente fornisce collegamenti a documentazione approfondita, tutorial pratici e risorse per iniziare.

I seguenti servizi coprono il networking globale e la connettività VPC.

Amazon CloudFront

- Che cos'è Amazon CloudFront?

Scopri come accelerare la distribuzione dei contenuti.

[Esplora la guida](#)

- Guida introduttiva ad Amazon CloudFront

Scopri i passaggi di base per distribuire contenuti con CloudFront.

[Esplora la guida](#)

- Hosting di video in streaming su richiesta con Amazon S3, Amazon e CloudFront Amazon Route 53

Scopri come ospitare video per la visualizzazione su richiesta in modo sicuro e scalabile.

[Inizia con il tutorial](#)

- Distribuisci contenuti più velocemente con Amazon CloudFront

Scopri come ridurre la latenza dell'utente finale delle tue applicazioni web.

[Inizia con il tutorial](#)

AWS Cloud WAN

- Cos'è AWS Cloud WAN?

Scopri come creare, gestire e monitorare una rete globale unificata.

[Esplora la guida](#)

- Ti presentiamo AWS Cloud WAN

Scopri i principali casi d'uso di AWS Cloud WAN e come iniziare.

[Leggi il blog](#)

- Guida introduttiva a AWS Cloud WAN

Crea la tua prima rete globale e collega un VPC.

[Inizia con il tutorial](#)

AWS Direct Connect

- Che cos'è AWS Direct Connect?

Scopri come connettere una rete locale a AWS.

[Esplora la guida](#)

- Iniziare con AWS Direct Connect

Guarda una breve introduzione AWS Direct Connect e come preparare la rete locale a cui connettersi AWS.

[Guarda il video](#)

- Connect il tuo data center a AWS

Connect il data center all' AWS utilizzo AWS Direct Connect.

[Inizia con il tutorial](#)

AWS Global Accelerator

- Che cos'è AWS Global Accelerator?

Scopri come migliorare le prestazioni dei tuoi carichi di lavoro.

[Esplora la guida](#)

- Guida introduttiva a un acceleratore standard

Crea un acceleratore per migliorare le prestazioni di rete di un carico di lavoro in esecuzione su un'istanza. EC2

[Inizia con il tutorial](#)

- Migliora la disponibilità e le prestazioni globali delle applicazioni per il tuo traffico

Guarda una breve dimostrazione sulla configurazione AWS Global Accelerator per migliorare le prestazioni della rete.

[Guarda il video](#)

AWS PrivateLink

- Che cos'è AWS PrivateLink?

Scopri come connettere privatamente il tuo VPC ai servizi.

[Esplora la guida](#)

- Inizia con AWS PrivateLink

Invia una richiesta da un' EC2 istanza in una sottorete privata ad Amazon CloudWatch utilizzando PrivateLink.

[Inizia con il tutorial](#)

- **Accelera la tua IPv6 adozione con PrivateLink servizi ed endpoint**

I clienti con un'ampia presenza su Internet sentono la pressione dell'esaurimento degli indirizzi pubblici. Scopri come aumentare l'IPv6 utilizzo nell'ambito VPCs di Using. PrivateLink

[Leggi il blog](#)

Amazon Route 53

- **What is Amazon Route 53?**

Scopri di più sulla risoluzione dei nomi di dominio ad alta disponibilità e scalabilità.

[Esplora la guida](#)

- **Tutorial sui casi d'uso di Amazon Route 53**

Come usare Route 53 per casi d'uso basati sul traffico e sulla latenza.

[Inizia con il tutorial](#)

- **Come registrare un nome di dominio con Amazon Route 53**

Questo tutorial ti aiuta a registrare un nuovo nome di dominio per un'applicazione web.

[Inizia con il tutorial](#)

- **Introduzione ad Amazon Route 53**

Guarda una breve introduzione alla risoluzione dei nomi di dominio e a Route 53.

[Guarda il video](#)

AWS Data Transfer Terminal

- **Che cos'è il terminale di trasferimento AWS dati?**

Scopri come caricare o scaricare rapidamente set di dati di grandi dimensioni Cloud AWS utilizzando i tuoi dispositivi di archiviazione.

[Esplora la guida](#)

- Presentazione del AWS Data Transfer Terminal

Scopri i principali casi d'uso e come iniziare.

[Leggi il blog](#)

AWS Site-to-Site VPN

- Che cos'è AWS Site-to-Site VPN?

Scopri come connettere utenti remoti AWS a una VPN.

[Esplora la guida](#)

- Iniziare con AWS Site-to-Site VPN

Configura una connessione Site-to-Site VPN tra un dispositivo locale e AWS.

[Inizia con il tutorial](#)

- AWS Site-to-Site VPN, scegliendo le opzioni giuste per ottimizzare le prestazioni

Scegli le opzioni migliori per configurare una connessione VPN a AWS.

[Leggi il blog](#)

AWS Transit Gateway

- What is a transit gateway?

Scopri come connetterti VPCs con i gateway di transito.

[Esplora la guida](#)

- Esempi di casi d'uso dei gateway di transito

Visualizza i casi d'uso comuni per i gateway di transito.

[Esplora la guida](#)

- AWS Transit Gateway officina

In questo workshop pratico, scopri come implementare Transit Gateway in configurazioni a regione singola e con account singolo, con più account e più aree geografiche.

[Inizia il workshop](#)

Amazon VPC

- Cos'è Amazon VPC?

Scopri i cloud privati virtuali e le funzionalità di Amazon VPC.

[Esplora la guida](#)

- Inizia a usare Amazon VPC

Una guida per iniziare rapidamente a usare Amazon VPC.

[Esplora la guida](#)

- Esempi di configurazioni VPC

Visualizza esempi di configurazioni VPC basate su diversi casi d'uso.

[Esplora la guida](#)

- Architettura VPC modulare e scalabile

Crea una base di rete virtuale basata sulle AWS migliori pratiche per la tua Cloud AWS infrastruttura.

[Inizia con il tutorial](#)

Amazon VPC IPAM

- What is IPAM?

Scopri come monitorare e gestire l'utilizzo degli indirizzi IP.

[Esplora la guida](#)

- Best practice di Amazon VPC IP Address Manager (IPAM)

Scopri come creare un piano di gestione degli indirizzi IP scalabile.

[Leggi il blog](#)

- Creazione di pool per gestire lo spazio IP

Guarda un breve video di introduzione a VPC IPAM.

[Guarda il video](#)

I seguenti servizi si riferiscono alla rete a livello di applicazione.

Amazon API Gateway

- Cos'è Amazon API Gateway?

Scopri come creare APIs per i tuoi carichi di lavoro.

[Esplora la guida](#)

- Creazione APIs con Amazon API Gateway

Scopri come iniziare APIs a creare AWS.

[Guarda il video](#)

- Configurazione di integrazioni private con Amazon API Gateway HTTP APIs

Scopri come creare un'API per controllare l'accesso privato alle risorse in un VPC.

[Leggi il blog](#)

AWS Client VPN

- Che cos'è AWS Client VPN?

Scopri come connettere le reti AWS tramite VPN.

[Esplora la guida](#)

- Iniziare con AWS Client VPN

Scarica l'AWS Client VPN applicazione e connettiti AWS tramite VPN.

[Esplora la guida](#)

- Scenari ed esempi per AWS Client VPN

Guarda gli esempi per creare e configurare l'accesso Client VPN per i tuoi clienti.

[Esplora gli esempi](#)

Elastic Load Balancing

- Cos'è l'Elastic Load Balancing?

Scopri come distribuire il traffico in entrata tra i tuoi carichi di lavoro.

[Esplora la guida](#)

- Guida introduttiva a Elastic Load Balancing

Scopri la differenza tra i diversi tipi di load balancer e crea un load balancer.

[Esplora la guida](#)

- Come scegliere il bilanciamento del carico giusto per i tuoi carichi di lavoro AWS

Scegli l'opzione giusta per bilanciare il carico di traffico rispetto ai tuoi carichi di lavoro.

[Guarda il video](#)

AWS Firewall Manager

- Guida introduttiva alle politiche AWS Firewall Manager

Scopri come utilizzare AWS Firewall Manager per abilitare diversi tipi di politiche di sicurezza.

[Esplora la guida](#)

- Come controllare e limitare continuamente i gruppi di sicurezza con AWS Firewall Manager

Questo post sul blog illustra come utilizzare AWS Firewall Manager to limit i gruppi di sicurezza per garantire che siano aperte solo le porte necessarie.

[Esplora la guida](#)

- Utilizzato AWS Firewall Manager per implementare la protezione su larga scala in AWS Organizations

Questo post fornisce step-by-step istruzioni per implementare e gestire le politiche di sicurezza in tutta l' AWS Organizations implementazione utilizzando. AWS Firewall Manager

[Esplora la guida](#)

AWS Network Firewall

- Che cos'è AWS Network Firewall?

Scopri di più sul firewall di rete e sul rilevamento delle intrusioni.

[Esplora la guida](#)

- Iniziare con AWS Network Firewall

Crea e gestisci rapidamente un firewall di rete per un VPC.

[Inizia con il tutorial](#)

- AWS Network Firewall video esplicativo animato

Guarda un breve video introduttivo a. AWS Network Firewall

[Guarda il video](#)

AWS Shield

- Cosa è AWS Shield?

Scopri di più sulla protezione DDo S.

[Esplora la guida](#)

- Esempi di architetture resilienti DDo S di base

Scopri alcune architetture S-resilienti comuni DDo.

[Esplora la guida](#)

- AWS Shield video illustrativo animato

Guarda un breve video introduttivo a. AWS Shield

[Guarda il video](#)

Accesso verificato da AWS

- Tutorial: Guida introduttiva all'accesso verificato

In questo tutorial imparerai come creare e configurare risorse di accesso verificato.

[Esplora la guida](#)

- Accesso verificato da AWS Integrazione con provider di identità di terze parti

Questo post sul blog mostra come integrare Verified Access (AVA) con il provider di identità di terze parti Okta.

[Esplora la guida](#)

- Integrazione Accesso verificato da AWS con provider affidabili per dispositivi

Questo post sul blog spiega come progettare una connettività remota basata su Zero Trust. AWS

[Esplora gli esempi](#)

Amazon VPC Lattice

- Cos'è Amazon VPC Lattice?

Scopri come connettere, proteggere e monitorare i microservizi nei tuoi carichi di lavoro.

[Esplora la guida](#)

- Configurazione di Amazon VPC Lattice

Configura e avvia VPC Lattice per la prima volta.

[Esplora la guida](#)

- Crea una connettività multi-VPC sicura per più account per le tue applicazioni con Amazon VPC Lattice

Un'introduzione a come utilizzare VPC Lattice per risolvere i problemi di connettività VPC.

[Leggi il blog](#)

- Spiegazione animata di Amazon VPC Lattice

Guarda un breve video animato su VPC Lattice.

[Guarda il video](#)

AWS WAF

- Che cos'è? AWS WAF

Scopri come controllare l'accesso ai tuoi carichi di lavoro.

[Esplora la guida](#)

- Iniziare con AWS WAF

Guarda un breve video su come AWS WAF proteggere i tuoi carichi di lavoro da exploit web e bot.

[Guarda il video](#)

- Video introduttivo a AWS WAF

Guarda un breve video introduttivo a AWS WAF.

[Guarda il video](#)

Esplora

- diagrammi di architettura

Esplora i diagrammi delle architetture di riferimento per aiutarti a sviluppare le tue architetture di rete e di distribuzione dei contenuti. AWS

[Esplora i diagrammi di architettura](#)

- Whitepaper

Esplora i white paper per aiutarti a iniziare, apprendere le migliori pratiche e comprendere le tue opzioni di rete e distribuzione dei contenuti.

[Esplora i white paper](#)

- AWS Soluzioni

Esplora soluzioni testate e linee guida architetturali per casi d'uso comuni per il networking e la distribuzione di contenuti.

[Esplora le soluzioni AWS](#)

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti a questa guida decisionale. Per ricevere notifiche sugli aggiornamenti di questa guida, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Guida aggiornata	AWS Terminale di trasferimento dati aggiunto.	16 gennaio 2025
Pubblicazione iniziale	Guida pubblicata per la prima volta.	12 dicembre 2023

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.