Le migliori pratiche per creare un'architettura cloud ibrida con Servizi AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Le migliori pratiche per creare un'architettura cloud ibrida con Servizi AWS

Table of Contents

Le migliori pratiche per creare un'architettura cloud ibrida con Servizi AWS

Amazon Web Services (collaboratori)

Giugno 2025 (cronologia del documento)

Molte aziende e organizzazioni hanno adottato il cloud computing come aspetto chiave della loro strategia tecnologica. In genere migrano i propri carichi di lavoro verso il Cloud AWS per aumentare l'agilità, il risparmio sui costi, le prestazioni, la disponibilità, la resilienza e la scalabilità. La maggior parte delle applicazioni può essere facilmente migrata, ma alcune applicazioni devono rimanere on-premise per sfruttare la bassa latenza e l'elaborazione locale dei dati dell'ambiente locale, per evitare elevati costi di trasferimento dei dati o per garantire la conformità normativa. Inoltre, potrebbe essere necessario riprogettare o modernizzare un sottoinsieme di applicazioni prima di poter essere spostato sul cloud. Ciò porta molte organizzazioni a cercare architetture cloud ibride per integrare le proprie operazioni on-premise e cloud per supportare un ampio spettro di casi d'uso. Questo approccio ibrido può offrire i vantaggi dell'elaborazione locale e basata sul cloud e può essere particolarmente utile per gli scenari di edge computing.

Quando crei un cloud ibrido con AWS, ti consigliamo di determinare la tua strategia di cloud ibrido e la tua strategia tecnica:

- Una strategia di cloud ibrido fornisce linee guida che regolano il consumo di risorse cloud e locali per supportare i tuoi obiettivi aziendali. Questa guida descrive i casi d'uso più comuni per la creazione di un cloud ibrido, come supportare la migrazione continua verso il cloud, garantire la continuità aziendale durante i disastri, estendere l'infrastruttura cloud all'ambiente locale per supportare applicazioni a bassa latenza o espandere la presenza internazionale su. AWS La definizione di questa strategia aiuta a identificare e definire gli obiettivi aziendali per la creazione di un cloud ibrido e fornisce linee guida per il posizionamento dei carichi di lavoro sul cloud ibrido.
- Una strategia tecnica per il cloud ibrido identifica i principi guida dell'architettura cloud ibrida e definisce un framework di implementazione. Questa guida delinea i requisiti comuni per un'architettura cloud ibrida distribuita e gestita in modo coerente per aiutarti a definire i principi per un'implementazione pianificata del cloud ibrido. Questi requisiti includono interfacce standardizzate per l'approvvigionamento e la gestione delle risorse nell'infrastruttura cloud.

Questa guida descrive un framework operativo e di gestione per aiutare gli architetti e gli operatori delle soluzioni a identificare gli elementi costitutivi, le best practice e il cloud AWS ibrido e i servizi regionali con cui implementare un cloud ibrido. AWS

Molte organizzazioni hanno utilizzato le soluzioni descritte in questa guida per implementare con successo ambienti cloud ibridi che sfruttano la scalabilità, l'agilità, l'innovazione e l'impronta globale fornite da. Cloud AWS(Vedi case study). AWS i servizi cloud ibridi offrono un' AWS esperienza coerente dal cloud all'ambiente on-premise e all'edge. Servizi come AWS Outposts la Zone locali AWS collocazione di elaborazione, archiviazione, database e altro ancora sono adatti a centri industriali e Servizi AWS abitati di grandi dimensioni quando è necessaria una bassa latenza tra i dispositivi degli utenti finali o i data center e i server di carico di lavoro esistenti in locale.

In questa guida:

Panoramica

Questa guida classifica i AWS consigli per il cloud ibrido in cinque pilastri: networking, sicurezza, resilienza, pianificazione della capacità e gestione dell'infrastruttura. Fornisce linee guida per aiutarti a migliorare la tua preparazione e a sviluppare una strategia di migrazione utilizzando un servizio edge AWS ibrido come o. AWS Outposts Zone locali AWS Ti consigliamo vivamente di collaborare con il tuo Account AWS team o di AWS Partner assicurarti che uno specialista del cloud AWS ibrido sia disponibile ad assisterti mentre segui questa guida e sviluppi il tuo processo.

> **Note**
>
> Sebbene AWS Outposts Local Zones risolva problemi simili, ti consigliamo di esaminare i casi d'uso, i servizi e le funzionalità disponibili per decidere quale offerta si adatta meglio alle tue esigenze. Per ulteriori informazioni, consulta il post del AWS blog Zone locali AWS e AWS Outposts scegli la tecnologia giusta per il tuo carico di lavoro edge.

Workshop sul cloud ibrido

Con l'assistenza di un esperto in materia di cloud AWS ibrido (SME), puoi organizzare un workshop sul cloud ibrido per valutare il livello di maturità della tua azienda in relazione ai cinque pilastri discussi in questa guida.

Il workshop si concentra sulle aree interne dell'organizzazione, come il networking, la sicurezza, la conformità DevOps, la virtualizzazione e le unità aziendali. Ti aiuta a progettare un'architettura cloud ibrida che soddisfi i requisiti della tua organizzazione e definisce i dettagli di implementazione, seguendo i passaggi indicati nella sezione Processo di adozione del cloud ibrido di questa guida.

PoCs

Se hai requisiti specifici, puoi utilizzare proofs of concept (PoCs) per convalidare la funzionalità in Local Zones e AWS Outposts rispetto a tali requisiti.

AWS vengono utilizzati PoCs per aiutarti a testare i carichi di lavoro che desideri spostare in un Outpost o in una zona locale, per determinare se i carichi di lavoro funzioneranno secondo le architetture di test. Per accedere a una Local Zone per il test, segui le istruzioni nella documentazione

di Local Zones. Per testare il tuo carico di lavoro AWS Outposts, collabora con il tuo Account AWS team o accedi AWS Partner a un laboratorio di AWS Outposts test e ricevi indicazioni dagli architetti AWS delle soluzioni. In tutti gli scenari, lo sviluppo di un PoC richiede la generazione di un documento di test che contenga:

- Servizi AWS da utilizzare, ad esempio Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Virtual Private Cloud (Amazon VPC) e Amazon Elastic Kubernetes Service (Amazon EKS)
- Dimensioni e numero di istanze da utilizzare (ad esempio, o) `m5.xlarge` `c5.2xlarge`
- Diagramma dell'architettura del test
- Criteri di successo del test
- Dettagli e obiettivi di ogni test da eseguire

Pilastri

La sezione successiva tratta i prerequisiti e le limitazioni per l'utilizzo delle architetture discusse in questa guida. Le sezioni successive trattano i dettagli di ciascun pilastro in modo che il documento di raccomandazioni creato durante il workshop sul cloud ibrido possa riflettere i dettagli di progettazione necessari per l'implementazione.

- Rete alla periferia
- Sicurezza nella periferia
- Resilienza all'edge
- Pianificazione della capacità a livello perimetrale
- Gestione dell'infrastruttura perimetrale

Prerequisiti e limitazioni

Prima di seguire questa guida, collabora con il tuo Account AWS team o esamina AWS Partner i prerequisiti e le limitazioni per l'implementazione di architetture edge con e Local AWS Outposts Zones.

Prerequisiti

AWS Outposts

- Il data center esistente deve soddisfare i AWS Outposts requisiti in termini di strutture, rete e alimentazione. AWS Outposts è progettato per funzionare in un ambiente di data center con ingressi di alimentazione ridondanti da 5-15 kVA, 145,8 volte il flusso d'aria kVA di piedi cubi al minuto (CFM) e una temperatura ambiente compresa tra 41° F (5° C) e 95° F (35° C), tra gli altri requisiti.
- Verifica che il AWS Outposts FAQs servizio sia disponibile nel tuo Paese consultando il rack. AWS Outposts Vedi la domanda: In quali paesi e territori è disponibile il rack Outposts?
- Se l'organizzazione richiede quattro o più AWS Outposts rack, il data center deve soddisfare i requisiti dei rack Aggregation, Core, Edge (ACE).
- È necessario fornire e supportare una connessione Internet o un AWS Direct Connect collegamento di almeno 500 Mbps (1 Gbps è preferibile) per la connessione AWS Outposts a Regione AWS, con una connettività di backup adeguata, se il caso d'uso lo richiede. La latenza di andata e ritorno dalla regione deve essere AWS Outposts al massimo di 175 millisecondi.
- È necessario disporre di un contratto attivo per AWS Enterprise Support o AWS Enterprise On-Ramp.

Zone locali AWS

- Una zona AWS locale deve essere disponibile vicino ai data center o agli utenti. Vedi Zone locali AWS le sedi.
- Conferma di disporre della connettività di rete dall'infrastruttura locale alla zona locale:
  - Opzione 1: un AWS Direct Connect collegamento dal data center al AWS Direct Connect punto di presenza (PoP) più vicino alla zona locale. Per ulteriori informazioni, consulta Direct Connect nella documentazione di Local Zones.

- Opzione 2: un collegamento Internet in aggiunta a un'appliance di rete privata virtuale (VPN) locale e le licenze necessarie per avviare un'appliance VPN basata su software su Amazon nella zona locale. EC2 Per ulteriori informazioni, consulta Connessione VPN nella documentazione di Local Zones.

Per ulteriori opzioni di connettività, consulta la documentazione di Local Zones.

Limitazioni

AWS Outposts

- Amazon Relational Database Service (Amazon RDS) AWS Outposts su implementazioni Multi-AZ richiede pool di indirizzi IP (CoIP) di proprietà del cliente. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente per Amazon RDS on. AWS Outposts
- Multi-AZ on AWS Outposts è disponibile per tutte le versioni supportate di MySQL e PostgreSQL su Amazon RDS on. AWS Outposts Per maggiori informazioni, consultare Amazon RDS su AWS Outposts supporto per le funzionalità di Amazon RDS. Amazon RDS on AWS Outposts supporta database SQL Server, Amazon RDS for MySQL e Amazon RDS for PostgreSQL.
- AWS Outposts non è progettato per funzionare quando è disconnesso da un. Regione AWS Per ulteriori informazioni, consulta la sezione Thinking in terms of failure mode nel AWS white paper AWS Outposts High Availability Design and Architecture Considerations.
- Amazon Simple Storage Service (Amazon S3) S3) AWS Outposts on presenta alcune limitazioni. Questi sono discussi nella sezione In che modo Amazon S3 on Outposts è diverso da Amazon S3? sezione della Guida per l'utente di Amazon S3 on Outposts.
- Gli Application Load Balancer attivi AWS Outposts non supportano il TLS reciproco (MTL) o le sessioni permanenti.
- I rack ACE non sono completamente chiusi e non includono porte anteriori o posteriori.
- Lo strumento di capacità delle istanze è applicabile solo ai nuovi ordini.

Zone locali AWS

- Le Local Zones non hanno un AWS Site-to-Site VPN endpoint. Utilizza invece una VPN basata su software su Amazon. EC2

- Local Zones non supporta AWS Transit Gateway. Connettiti invece alla zona locale utilizzando un'interfaccia virtuale AWS Direct Connect privata (VIF).
- Non tutte le Local Zones supportano servizi come Amazon RDS, Amazon FSx, Amazon EMR o ElastiCache Amazon o i gateway NAT. Per ulteriori informazioni, consulta le funzionalità.Zone locali AWS
- Gli Application Load Balancer in Local Zones non supportano MTL o sessioni permanenti.

Processo di adozione del cloud ibrido

Le sezioni seguenti illustrano le architetture e i dettagli di progettazione per ogni pilastro del cloud ibrido: AWS

- Rete all'edge
- Sicurezza all'edge
- Resilienza all'edge
- Pianificazione della capacità a livello perimetrale
- Gestione dell'infrastruttura perimetrale

Rete perimetrale

Quando si progettano soluzioni che utilizzano un'infrastruttura AWS perimetrale, come AWS Outposts Local Zones, è necessario considerare attentamente la progettazione della rete. La rete costituisce la base della connettività per raggiungere i carichi di lavoro distribuiti in queste sedi periferiche ed è fondamentale per garantire una bassa latenza. Questa sezione descrive vari aspetti della connettività edge ibrida.

Architettura VPC

Un cloud privato virtuale (VPC) si estende su tutte le zone di disponibilità al suo interno. Regione AWS Puoi estendere senza problemi qualsiasi VPC nella regione a Outposts o Local Zones AWS utilizzando la console o () per aggiungere una sottorete Outpost AWS Command Line Interface o AWS CLI Local Zone. Gli esempi seguenti mostrano come creare sottoreti in AWS Outposts e Local Zones utilizzando: AWS CLI

- AWS Outposts: per aggiungere una sottorete Outpost a un VPC, specifica l'Amazon Resource Name (ARN) dell'Outpost.

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

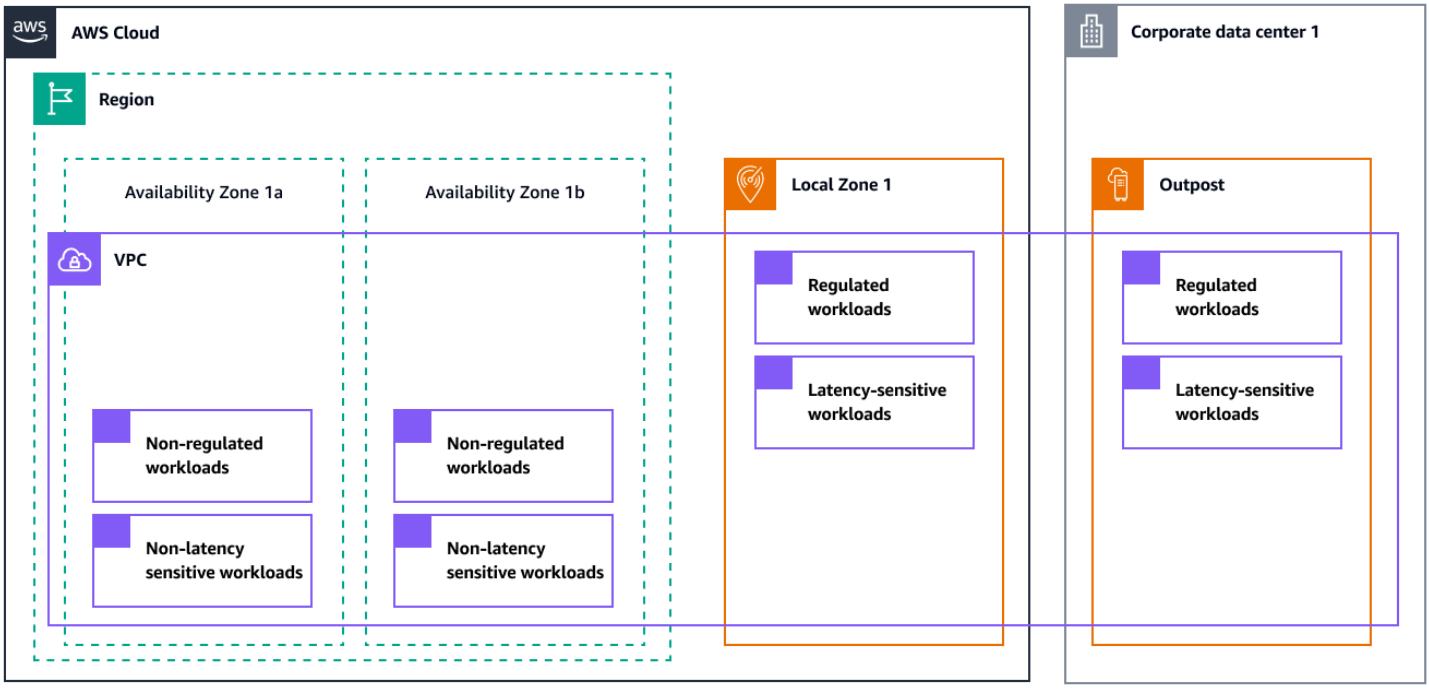
  Per ulteriori informazioni, consulta la documentazione relativa ad AWS Outposts.

- Local Zones: per aggiungere una sottorete Local Zone a un VPC, seguite la stessa procedura che utilizzate con le zone di disponibilità, ma specificate l'ID della zona locale `<local-zone-name>` (nell'esempio seguente).

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  Per ulteriori informazioni, consulta la documentazione di Local Zones.

Il diagramma seguente mostra un' AWS architettura che include le sottoreti Outpost e Local Zone.

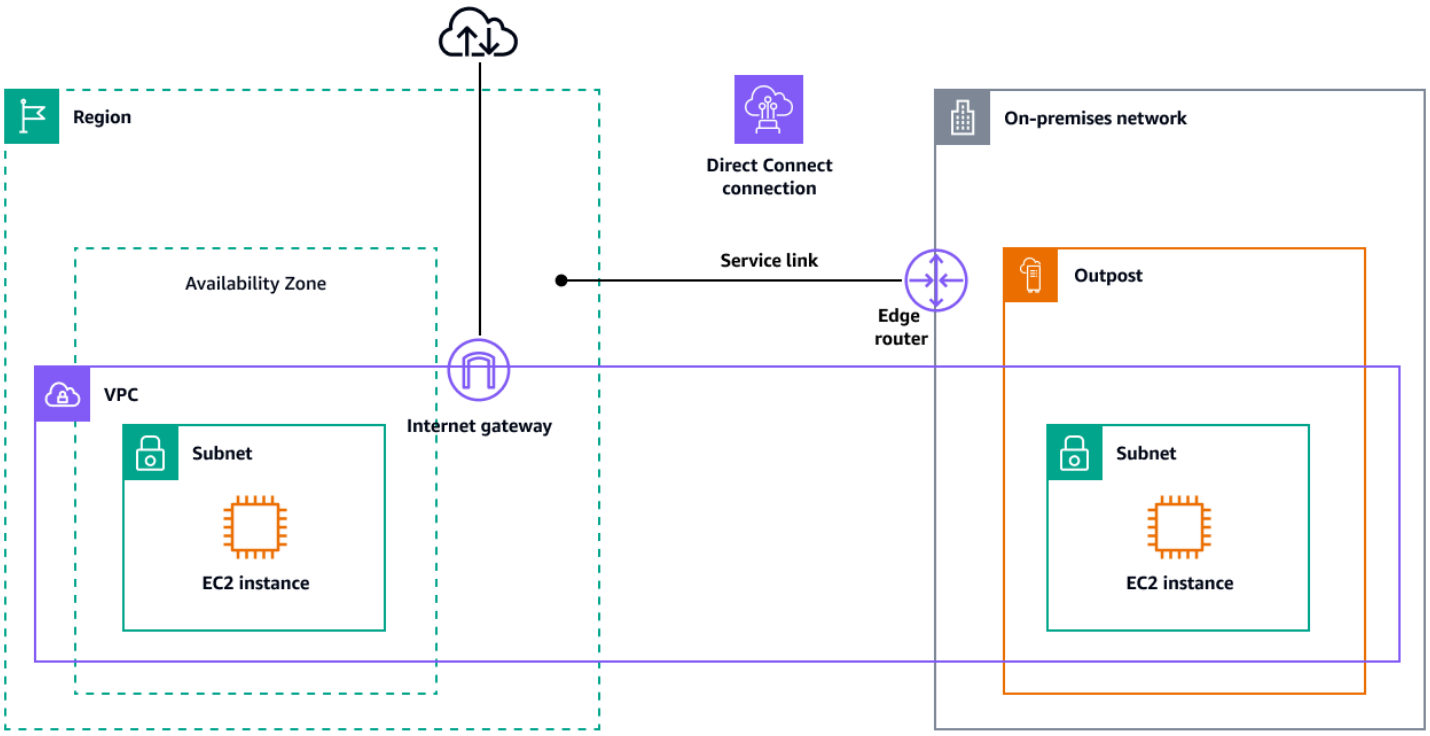


Traffico da periferia a regione

Quando progetti un'architettura ibrida utilizzando servizi come Local Zones e AWS Outposts, prendi in considerazione sia i flussi di controllo che i flussi di traffico di dati tra le infrastrutture edge e Regioni AWS. A seconda del tipo di infrastruttura perimetrale, la responsabilità dell'utente può variare: alcune infrastrutture richiedono la gestione della connessione alla regione madre, mentre altre la gestiscono tramite l'infrastruttura AWS globale. Questa sezione esplora le implicazioni della connettività del piano di controllo e del piano dati per Local Zones e AWS Outposts.

AWS Outposts piano di controllo

AWS Outposts fornisce un costrutto di rete chiamato service link. Il collegamento al servizio è una connessione richiesta tra AWS Outposts e la regione selezionata Regione AWS o principale (denominata anche regione di origine). Consente la gestione dell'Avamposto e lo scambio di traffico tra l'Avamposto e. Regione AWS Il collegamento al servizio utilizza un set crittografato di connessioni VPN per comunicare con la regione d'origine. È necessario fornire la Regione AWS connettività tra AWS Outposts e tramite un collegamento Internet o un'interfaccia virtuale AWS Direct Connect pubblica (VIF pubblica) oppure tramite un'interfaccia virtuale AWS Direct Connect privata (VIF privata). Per un'esperienza e una resilienza ottimali, si AWS consiglia di utilizzare una connettività ridondante di almeno 500 Mbps (1 Gbps è preferibile) per la connessione del service link a. Regione AWS La connessione service link di almeno 500 Mbps consente di avviare EC2 istanze Amazon, collegare volumi Amazon EBS e accedere ad Servizi AWS esempio ad Amazon EKS, Amazon EMR e parametri Amazon. CloudWatch La rete deve supportare un'unità di trasmissione (MTU) massima di 1.500 byte tra Outpost e gli endpoint del service link del dispositivo principale. Regione AWSPer ulteriori informazioni, consulta la sezione AWS Outposts relativa alla connettività Regioni AWS nella documentazione di Outposts.



Per informazioni sulla creazione di architetture resilienti per i collegamenti di servizio che utilizzano AWS Direct Connect e la rete Internet pubblica, consulta la sezione sulla connettività di Anchor nel AWS white paper AWS Outposts High Availability Design and Architecture Considerations.

AWS Outposts piano dati

Il piano dati compreso tra AWS Outposts e Regione AWS è supportato dalla stessa architettura di service link utilizzata dal piano di controllo. La larghezza di banda del collegamento di servizio del piano dati tra AWS Outposts e Regione AWS deve essere correlata alla quantità di dati che devono essere scambiati: maggiore è la dipendenza dai dati, maggiore deve essere la larghezza di banda del collegamento.

I requisiti di larghezza di banda variano in base alle seguenti caratteristiche:

- Il numero di AWS Outposts rack e le configurazioni di capacità
- Caratteristiche del carico di lavoro come le dimensioni dell'AMI, l'elasticità delle applicazioni e le esigenze di velocità di burst
- Traffico VPC verso la regione

Il traffico tra EC2 le istanze in AWS Outposts e le EC2 istanze in Regione AWS ha un MTU di 1.300 byte. Ti consigliamo di discutere questi requisiti con uno specialista del cloud AWS ibrido prima di proporre un'architettura che abbia co-dipendenze tra la regione e. AWS Outposts

Piano dati Local Zones

Il piano dati tra Local Zones e il Regione AWS è supportato dall'infrastruttura AWS globale. Il piano dati viene esteso tramite un VPC dalla zona Regione AWS a una zona locale. Le Local Zones forniscono anche una connessione sicura e ad alta larghezza di banda e consentono di connettersi senza problemi all'intera gamma di servizi regionali tramite lo stesso APIs set di strumenti. Regione AWS

La tabella seguente mostra le opzioni di connessione e quelle associate. MTUs

Da	Per	MTU
Amazon EC2 nella regione	Amazon EC2 nelle Local Zones	1.300 byte
AWS Direct Connect	Zone locali	1.468 byte
Internet Gateway	Zone locali	1.500 byte

Da	Per	MTU
Amazon EC2 nelle Local Zones	Amazon EC2 nelle Local Zones	9.001 byte

Local Zones utilizzano l'infrastruttura AWS globale con cui connettersi Regioni AWS. L'infrastruttura è completamente gestita da AWS, quindi non è necessario configurare questa connettività. Ti consigliamo di discutere i requisiti e le considerazioni relative alle Local Zones con uno specialista del cloud AWS ibrido prima di progettare qualsiasi architettura che abbia co-dipendenze tra Region e Local Zones.

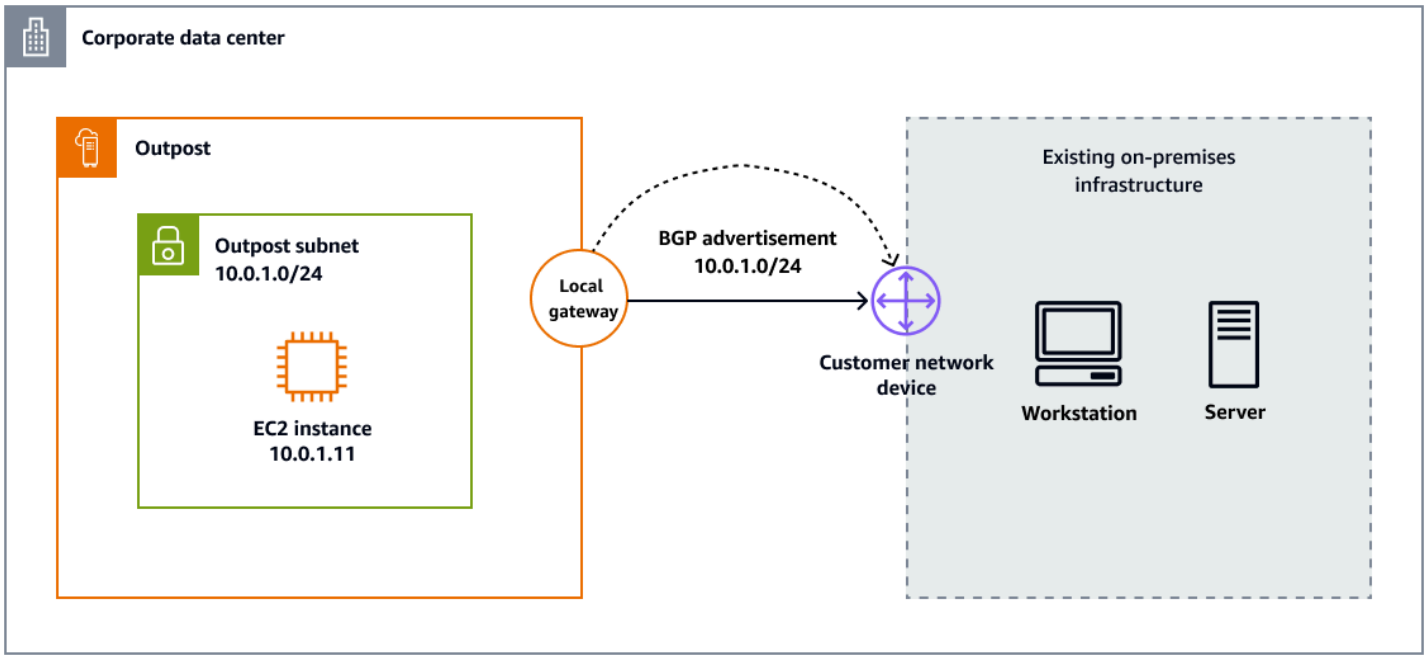
Traffico dall'edge all'ambiente locale

AWS i servizi cloud ibridi sono progettati per affrontare casi d'uso che richiedono bassa latenza, elaborazione locale dei dati o conformità alla residenza dei dati. L'architettura di rete per l'accesso a questi dati è importante e dipende dal fatto che il carico di lavoro sia in esecuzione nelle Local Zones AWS Outposts o nelle Local Zones. La connettività locale richiede anche un ambito ben definito, come illustrato nelle sezioni seguenti.

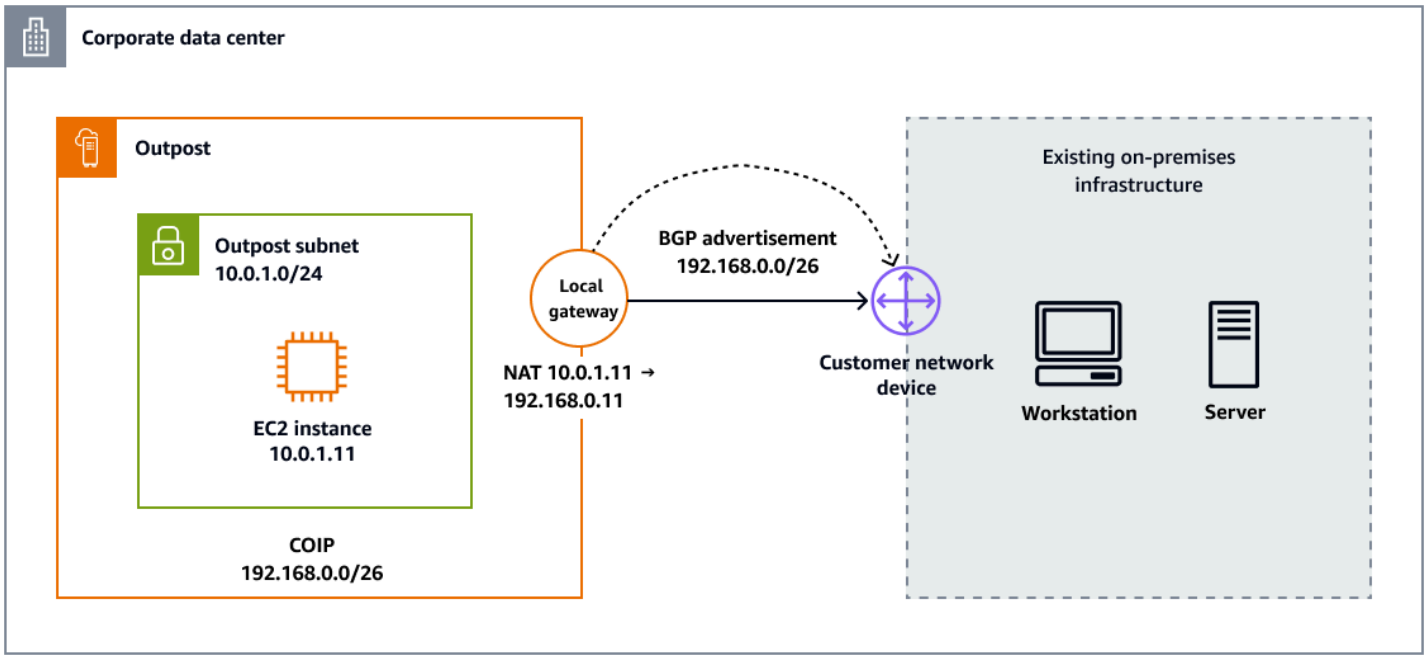
AWS Outposts gateway locale

Il gateway locale (LGW) è un componente fondamentale dell' AWS Outposts architettura. Il gateway locale stabilisce la connettività tra le sottoreti Outpost e la rete on-premise. Il ruolo principale di un LGW è fornire la connettività da un Outpost alla rete locale locale. Fornisce inoltre connettività a Internet tramite la rete locale tramite routing VPC diretto o indirizzi IP di proprietà del cliente.

- Il routing VPC diretto utilizza l'indirizzo IP privato delle istanze nel tuo VPC per facilitare la comunicazione con la tua rete locale. Questi indirizzi vengono pubblicizzati sulla rete locale tramite Border Gateway Protocol (BGP). La propagazione su BGP riguarda solo gli indirizzi IP privati che appartengono alle sottoreti del rack Outpost. Questo tipo di routing è la modalità predefinita per. AWS Outposts In questa modalità, il gateway locale non esegue NAT per le istanze e non è necessario assegnare indirizzi IP elastici alle istanze. EC2 Il diagramma seguente mostra un gateway AWS Outposts locale che utilizza il routing VPC diretto.



- Con gli indirizzi IP di proprietà del cliente, è possibile fornire un intervallo di indirizzi, noto come pool di indirizzi IP (CoIP) di proprietà del cliente, che supporta intervalli CIDR sovrapposti e altre topologie di rete. Quando si sceglie un CoIP, è necessario creare un pool di indirizzi, assegnarlo alla tabella di routing del gateway locale e ripubblicizzare questi indirizzi nella rete tramite BGP. Gli indirizzi CoIP forniscono connettività locale o esterna alle risorse della rete locale. Puoi assegnare questi indirizzi IP alle risorse di Outpost, come le EC2 istanze, allocando un nuovo indirizzo IP elastico dal CoIP e quindi assegnandolo alla tua risorsa. Il diagramma seguente mostra un AWS Outposts gateway locale che utilizza la modalità CoIP.



La connettività locale AWS Outposts da una rete locale richiede alcune configurazioni di parametri, come l'abilitazione del protocollo di routing BGP e dei prefissi pubblicitari tra i peer BGP. L'MTU che può essere supportato tra Outpost e il gateway locale è di 1.500 byte. Per ulteriori informazioni, contatta uno specialista del cloud AWS ibrido o consulta la documentazione.AWS Outposts

Local Zones e Internet

I settori che richiedono una bassa latenza o la residenza locale dei dati (ad esempio giochi, live streaming, servizi finanziari e pubblica amministrazione) possono utilizzare Local Zones per distribuire e fornire le proprie applicazioni agli utenti finali su Internet. Durante l'implementazione di una zona locale, è necessario allocare indirizzi IP pubblici da utilizzare in una zona locale. Quando si allocano indirizzi IP elastici, è possibile specificare la posizione da cui viene pubblicizzato l'indirizzo IP. Questa posizione è denominata gruppo di confine di rete. Un gruppo di confini di rete è una raccolta di Availability Zones, Local AWS Wavelength Zones o Zones da cui AWS pubblicizza un indirizzo IP pubblico. Questo aiuta a garantire una latenza o una distanza fisica minima tra la AWS rete e gli utenti che accedono alle risorse in queste zone. Per visualizzare tutti i gruppi di confine di rete per Local Zones, consulta Available Local Zones nella documentazione Local Zones.

Per esporre a Internet un carico EC2 di lavoro ospitato da Amazon in una zona locale, puoi abilitare l'opzione Assegna automaticamente un IP pubblico all'avvio dell'istanza. EC2 Se si utilizza un Application Load Balancer, è possibile definirlo come connesso a Internet in modo che gli indirizzi IP pubblici assegnati alla zona locale possano essere propagati dalla rete di confine associata alla

zona locale. Inoltre, quando utilizzi indirizzi IP elastici, puoi associare una di queste risorse a un' EC2 istanza dopo il suo avvio. Quando si invia traffico tramite un gateway Internet in Local Zones, vengono applicate le stesse specifiche di larghezza di banda dell'istanza utilizzate dalla regione. Il traffico di rete della zona locale va direttamente a Internet o ai punti di presenza (PoPs) senza attraversare la regione madre della zona locale, per consentire l'accesso all'elaborazione a bassa latenza.

Le Local Zones offrono le seguenti opzioni di connettività su Internet:

- Accesso pubblico: collega carichi di lavoro o dispositivi virtuali a Internet utilizzando indirizzi IP elastici tramite un gateway Internet.
- Accesso a Internet in uscita: consente alle risorse di raggiungere gli endpoint pubblici tramite istanze NAT (Network Address Translation) o dispositivi virtuali con indirizzi IP elastici associati, senza esposizione diretta a Internet.
- Connettività VPN: stabilisce connessioni private utilizzando Internet Protocol Security (IPsec) VPN tramite dispositivi virtuali con indirizzi IP elastici associati.

Per ulteriori informazioni, consulta Opzioni di connettività per Local Zones nella documentazione di Local Zones.

Local Zones e AWS Direct Connect

Supporta anche Local Zones AWS Direct Connect, che consente di indirizzare il traffico su una connessione di rete privata. Per ulteriori informazioni, consulta Direct Connect in Local Zones nella documentazione di Local Zones.

Local Zones e gateway di transito

AWS Transit Gateway non supporta gli allegati VPC diretti alle sottoreti della zona locale. Tuttavia, è possibile connettersi ai carichi di lavoro della zona locale creando allegati Transit Gateway nelle sottoreti della zona di disponibilità principale dello stesso VPC. Questa configurazione consente l'interconnettività tra più VPCs carichi di lavoro della zona locale e quelli della zona locale. Per ulteriori informazioni, consulta la sezione Transit gateway connection between Local Zones nella documentazione Local Zones.

Local Zones e peering VPC

È possibile estendere qualsiasi VPC da una regione principale a una zona locale creando una nuova sottorete e assegnandola alla zona locale. È possibile stabilire il peering VPC tra VPCs quelli estesi a Local Zones. Quando i peer si VPCs trovano nella stessa zona locale, il traffico rimane all'interno della zona locale e non attraversa la regione madre.

Sicurezza all'avanguardia

Nel Cloud AWS, la sicurezza è la massima priorità. Man mano che le organizzazioni adottano la scalabilità e la flessibilità del cloud, le AWS aiuta ad adottare sicurezza, identità e conformità come fattori aziendali chiave. AWS integra la sicurezza nella sua infrastruttura principale e offre servizi per aiutarti a soddisfare i tuoi requisiti di sicurezza cloud unici. Quando espandi l'ambito della tua architettura in Cloud AWS, trai vantaggio dall'integrazione di infrastrutture come Local Zones e Regioni AWS Outposts in. Questa integrazione consente di AWS estendere un gruppo selezionato di servizi di sicurezza di base all'edge.

La sicurezza è una responsabilità condivisa tra te AWS e te. Il modello di responsabilitàAWS condivisa distingue tra la sicurezza del cloud e la sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS nel Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della AWS sicurezza nell'ambito dei programmi di AWS conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal materiale Servizio AWS che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Protezione dei dati

Il modello di responsabilità AWS condivisa si applica alla protezione dei dati in AWS Outposts e Zone locali AWS. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce il Cloud AWS (sicurezza del cloud). L'utente è responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura (sicurezza nel cloud). Questo contenuto include le attività di configurazione e gestione della sicurezza per Servizi AWS ciò che utilizzi.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS Identity and Access Management (IAM) o AWS IAM Identity Center. Ciò concede a ciascun utente solo le autorizzazioni necessarie per adempiere alle proprie mansioni lavorative.

Crittografia dei dati inattivi

Crittografia nei volumi EBS

Con AWS Outposts, tutti i dati sono crittografati quando sono inattivi. Il materiale chiave è racchiuso in una chiave esterna, la Nitro Security Key (NSK), archiviata in un dispositivo rimovibile. L'NSK è necessario per decrittografare i dati sul rack Outpost. Puoi utilizzare la crittografia Amazon EBS per i tuoi volumi EBS e gli snapshot. La crittografia Amazon EBS utilizza AWS Key Management Service (AWS KMS) e chiavi KMS.

Nel caso delle Local Zones, tutti i volumi EBS sono crittografati per impostazione predefinita in tutte le Local Zones, ad eccezione dell'elenco documentato nelle Zone locali AWS FAQ (vedi la domanda: Qual è il comportamento di crittografia predefinito dei volumi EBS nelle Local Zones?), a meno che la crittografia non sia abilitata per l'account.

Crittografia in Amazon S3 su Outposts

Per default, tutti i dati memorizzati in Amazon S3 su Outposts vengono crittografati utilizzando la crittografia lato server con chiavi di crittografia gestite di Amazon S3 (SSE-S3). È possibile specificare la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C). Per utilizzare SSE-C, specifica una chiave di crittografia come parte delle richieste API sull'oggetto. La crittografia lato server viene applicata solo ai dati dell'oggetto, non dei metadati dell'oggetto.

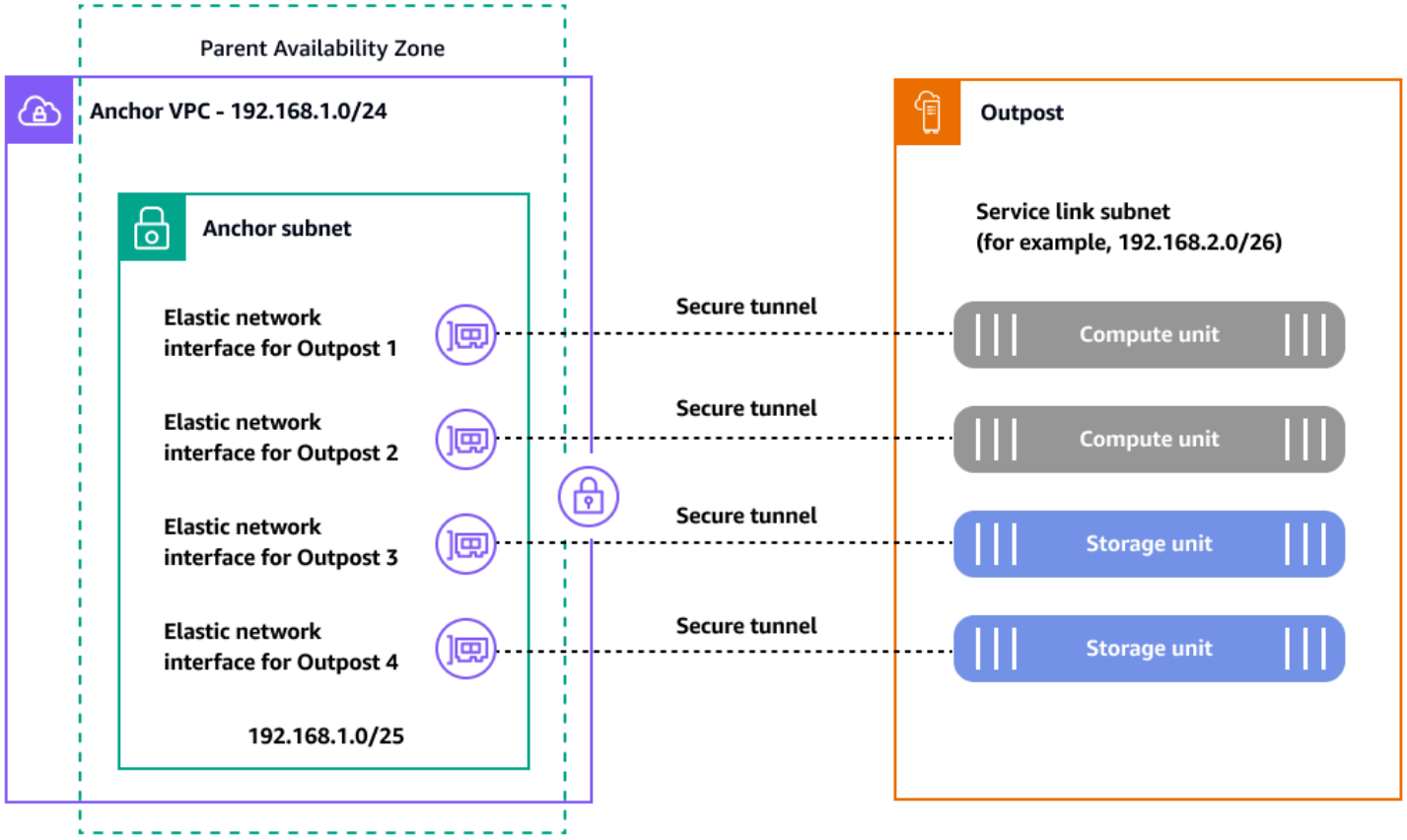
> **Note**
>
> Amazon S3 on Outposts non supporta la crittografia lato server con chiavi KMS (SSE-KMS).

Crittografia in transito

Infatti AWS Outposts, il link al servizio è una connessione necessaria tra il server Outposts e la regione prescelta Regione AWS (o la regione di residenza) e consente la gestione dell'Outpost e lo scambio di traffico da e verso il. Regione AWS Il collegamento al servizio utilizza una VPN AWS

gestita per comunicare con la regione d'origine. Ogni host interno AWS Outposts crea una serie di tunnel VPN per dividere il traffico del control plane e il traffico VPC. A seconda della connettività del service link (Internet o AWS Direct Connect) AWS Outposts, questi tunnel richiedono l'apertura di porte firewall affinché il service link crei l'overlay su di esso. Per informazioni tecniche dettagliate sulla sicurezza AWS Outposts e sul link di servizio, consulta Connettività tramite link di servizio e Sicurezza dell'infrastruttura AWS Outposts nella AWS Outposts documentazione.

Il collegamento al AWS Outposts servizio crea tunnel crittografati che stabiliscono la connettività del piano di controllo e del piano dati con il piano principale Regione AWS, come illustrato nel diagramma seguente.



Anchor VPC CIDR: /25 or larger that doesn't conflict with 10.1.0.0/16
IAM role: `AWSServiceRoleForOutposts_<OutpostID>`

Ogni AWS Outposts host (elaborazione e archiviazione) richiede questi tunnel crittografati su porte TCP e UDP note per comunicare con la regione madre. La tabella seguente mostra le porte e gli indirizzi di origine e destinazione per i protocolli UDP e TCP.

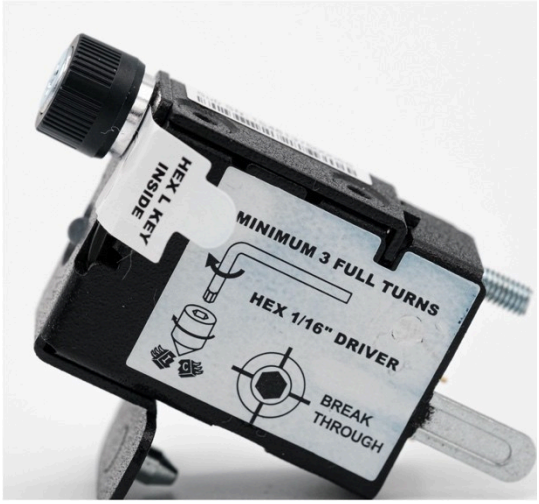
Protocollo	Porta di origine	Indirizzo di origine	Porta di destinazione	Indirizzo di destinazione
UDP	443	AWS Outposts link di servizio /26	443	AWS Outposts Percorsi pubblici della regione o ancoraggio VPC CIDR
TCP	1025-65535	AWS Outposts collegamento di servizio /26	443	AWS Outposts Percorsi pubblici della regione o ancoraggio VPC CIDR

Le Local Zones sono inoltre collegate alla regione madre tramite la dorsale privata globale ridondante e ad altissima larghezza di banda di Amazon. Questa connessione offre alle applicazioni in esecuzione in Local Zones un accesso rapido, sicuro e senza interruzioni ad altre Servizi AWS. Finché le Local Zones fanno parte dell'infrastruttura AWS globale, tutti i dati che fluiscono sulla rete AWS globale vengono automaticamente crittografati a livello fisico prima di lasciare le strutture AWS protette. Se hai requisiti specifici per crittografare i dati in transito tra le tue sedi locali e AWS Direct Connect PoPs per accedere a una zona locale, puoi abilitare MAC Security (MACsec) tra il router o lo switch locale e l'endpoint. AWS Direct Connect Per ulteriori informazioni, consulta il post del AWS blog Aggiungere MACsec sicurezza alle connessioni. AWS Direct Connect

Eliminazione dei dati

Quando si arresta o si termina un' EC2 istanza AWS Outposts, la memoria ad essa allocata viene cancellata (impostata su zero) dall'hypervisor prima di essere allocata a una nuova istanza e ogni blocco di storage viene reimpostato. L'eliminazione dei dati dall'hardware Outpost implica l'uso di hardware specializzato. L'NSK è un piccolo dispositivo, illustrato nella foto seguente, che si collega alla parte anteriore di ogni unità di elaborazione o archiviazione di un Outpost. È progettato per fornire un meccanismo per impedire che i dati vengano esposti dal data center o dal sito di colocation. I dati sul dispositivo Outpost sono protetti avvolgendo il materiale di codifica utilizzato per crittografare il dispositivo e archiviando il materiale avvolto su NSK. Quando restituisci un host

Outpost, distruggi l'NSK girando una piccola vite sul chip che schiaccia l'NSK e distrugge fisicamente il chip. Distruggendo l'NSK, i dati del tuo Outpost vengono distrutti crittograficamente.



Gestione dell'identità e degli accessi

AWS Identity and Access Management (IAM) è un dispositivo Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Outposts Se ne possiedi uno Account AWS, puoi utilizzare IAM senza costi aggiuntivi.

La tabella seguente elenca le funzionalità IAM con cui puoi utilizzare AWS Outposts.

Funzionalità IAM	AWS Outposts supporto
Policy basate su identità	Sì
Policy basate sulle risorse	Sì*
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
elenchi di controllo degli accessi (ACLs)	No

Funzionalità IAM	AWS Outposts supporto
Controllo degli accessi basato su attributi (ABAC) (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni delle entità principali	Sì
Ruoli di servizio	No
Ruoli collegati ai servizi	Sì

* Oltre alle policy basate sull'identità IAM, Amazon S3 on Outposts supporta sia le policy relative ai bucket che quelle relative ai punti di accesso. Si tratta di politiche basate sulle risorse allegate alla risorsa Amazon S3 on Outposts.

Per ulteriori informazioni su come queste funzionalità sono supportate in AWS Outposts, consulta la guida per l'utente.AWS Outposts

Sicurezza dell'infrastruttura

La protezione dell'infrastruttura è una parte cruciale di un programma di sicurezza delle informazioni. Garantisce che i sistemi e i servizi di carico di lavoro siano protetti da accessi involontari e non autorizzati e da potenziali vulnerabilità. Ad esempio, si definiscono i limiti di fiducia (ad esempio, i confini della rete e degli account), la configurazione e la manutenzione della sicurezza del sistema (ad esempio, rafforzamento, riduzione al minimo e applicazione di patch), l'autenticazione e le autorizzazioni del sistema operativo (ad esempio, utenti, chiavi e livelli di accesso) e altri punti appropriati per l'applicazione delle politiche (ad esempio, firewall per applicazioni Web o gateway API).

AWS fornisce diversi approcci alla protezione dell'infrastruttura, come illustrato nelle sezioni seguenti.

Protezione delle reti

I tuoi utenti possono far parte della tua forza lavoro o dei tuoi clienti e possono trovarsi ovunque. Per questo motivo, non puoi fidarti di tutti coloro che hanno accesso alla tua rete. Quando si segue il principio dell'applicazione della sicurezza a tutti i livelli, si utilizza un approccio zero trust. Nel modello di sicurezza Zero Trust, i componenti delle applicazioni o i microservizi sono considerati discreti e

nessun componente o microservizio considera attendibili gli altri componenti o microservizi. Per ottenere una sicurezza Zero Trust, segui questi consigli:

- Crea livelli di rete. Le reti a più livelli aiutano a raggruppare logicamente componenti di rete simili. Inoltre riducono il potenziale ambito di impatto dell'accesso non autorizzato alla rete.
- Controlla i livelli di traffico. Applica più controlli con un defense-in-depth approccio sia per il traffico in entrata che per quello in uscita. Ciò include l'uso di gruppi di sicurezza (firewall di ispezione stateful), rete ACLs, sottoreti e tabelle di routing.
- Implementa l'ispezione e la protezione. Ispeziona e filtra il traffico su ogni livello. Puoi ispezionare le configurazioni del VPC per potenziali accessi involontari utilizzando Network Access Analyzer. È possibile specificare i requisiti di accesso alla rete e identificare potenziali percorsi di rete che non li soddisfano.

Protezione delle risorse di elaborazione

Le risorse di calcolo includono EC2 istanze, contenitori, AWS Lambda funzioni, servizi di database, dispositivi IoT e altro ancora. Ogni tipo di risorsa di elaborazione richiede un approccio diverso alla sicurezza. Tuttavia, queste risorse condividono strategie comuni da prendere in considerazione: difesa approfondita, gestione delle vulnerabilità, riduzione della superficie di attacco, automazione della configurazione e del funzionamento ed esecuzione di azioni a distanza.

Ecco una guida generale per proteggere le risorse di elaborazione per i servizi chiave:

- Crea e gestisci un programma di gestione delle vulnerabilità. Scansiona e applica patch regolarmente a risorse come EC2 istanze, contenitori Amazon Elastic Container Service (Amazon ECS) e carichi di lavoro Amazon Elastic Kubernetes Service (Amazon EKS).
- Automatizza la protezione dell'elaborazione. Automatizza i meccanismi di protezione dell'elaborazione, tra cui la gestione delle vulnerabilità, la riduzione della superficie di attacco e la gestione delle risorse. Questa automazione consente di risparmiare tempo da utilizzare per proteggere altri aspetti del carico di lavoro e aiuta a ridurre il rischio di errore umano.
- Riduci la superficie di attacco. Riduci l'esposizione agli accessi involontari rafforzando i sistemi operativi e riducendo al minimo i componenti, le librerie e i servizi consumabili esternamente che utilizzi.

Inoltre, per ciascuno di essi Servizio AWS che utilizzi, consulta le raccomandazioni di sicurezza specifiche nella documentazione del servizio.

Accesso a Internet

Both AWS Outposts e Local Zones forniscono modelli architettonici che consentono ai carichi di lavoro di accedere da e verso Internet. Quando utilizzi questi modelli, considera il consumo di Internet dalla regione un'opzione praticabile solo se lo utilizzi per applicare patch, aggiornare, accedere a repository Git esterni e scenari AWS simili. Per questo modello architettonico, si applicano i concetti di ispezione centralizzata in entrata e uscita centralizzata da Internet. Questi modelli di accesso utilizzano AWS Transit Gateway gateway NAT, firewall di rete e altri componenti che risiedono in, ma sono connessi Regioni AWS, nelle Local AWS Outposts Zones tramite il percorso dati tra la regione e l'edge.

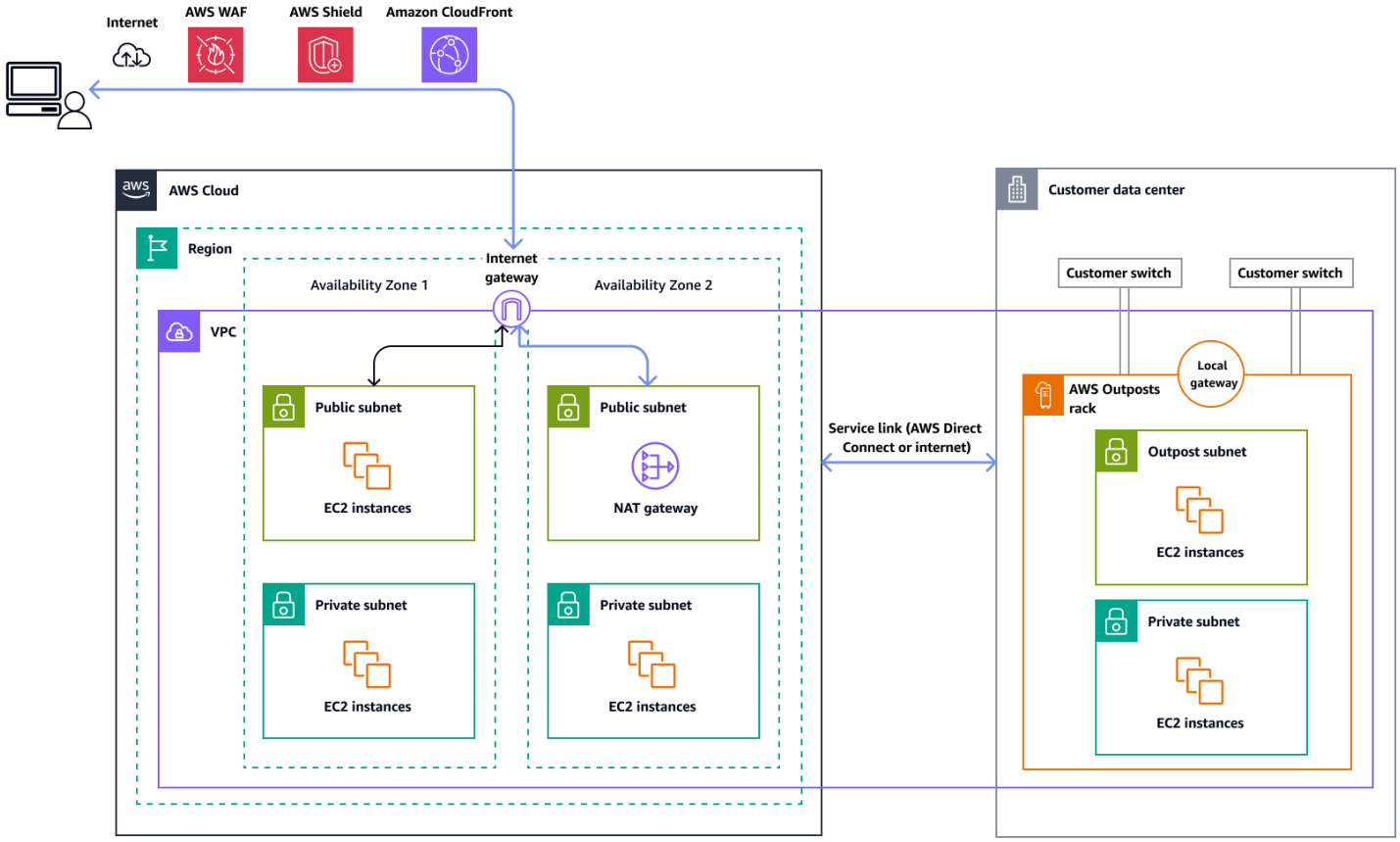
Local Zones adotta un costrutto di rete chiamato network border group, che viene utilizzato in. Regioni AWS AWS pubblicizza gli indirizzi IP pubblici di questi gruppi unici. Un gruppo di confini di rete è costituito da Availability Zones, Local Zones o Wavelength Zones. È possibile allocare in modo esplicito un pool di indirizzi IP pubblici da utilizzare in un gruppo di confini di rete. È possibile utilizzare un gruppo di confini di rete per estendere il gateway Internet alle Local Zones consentendo agli indirizzi IP elastici di essere serviti dal gruppo. Questa opzione richiede l'implementazione di altri componenti a complemento dei servizi di base disponibili in Local Zones. Questi componenti potrebbero provenire da ISVs e aiutarvi a creare livelli di ispezione nella zona locale, come descritto nel post del AWS blog Hybrid inspection architectures with. Zone locali AWS

Inoltre AWS Outposts, se desideri utilizzare il gateway locale (LGW) per raggiungere Internet dalla tua rete, devi modificare la tabella di routing personalizzata associata alla sottorete. AWS Outposts La tabella delle rotte deve avere una voce di percorso predefinita (0.0.0.0/0) che utilizza LGW come hop successivo. L'utente è responsabile dell'implementazione dei restanti controlli di sicurezza nella rete locale, comprese le difese perimetrali come firewall e sistemi di prevenzione delle intrusioni o sistemi di rilevamento delle intrusioni (IPS/IDS). Ciò è in linea con il modello di responsabilità condivisa, che divide i compiti di sicurezza tra l'utente e il provider di servizi cloud.

Accesso a Internet tramite il genitore Regione AWS

In questa opzione, i carichi di lavoro di Outpost accedono a Internet tramite il collegamento al servizio e il gateway Internet del dispositivo principale. Regione AWS Il traffico in uscita verso Internet può essere instradato attraverso il gateway NAT istanziato nel tuo VPC. Per una maggiore sicurezza del traffico in ingresso e in uscita, puoi utilizzare servizi AWS di sicurezza come AWS WAF AWS Shield, e Amazon CloudFront in the. Regione AWS

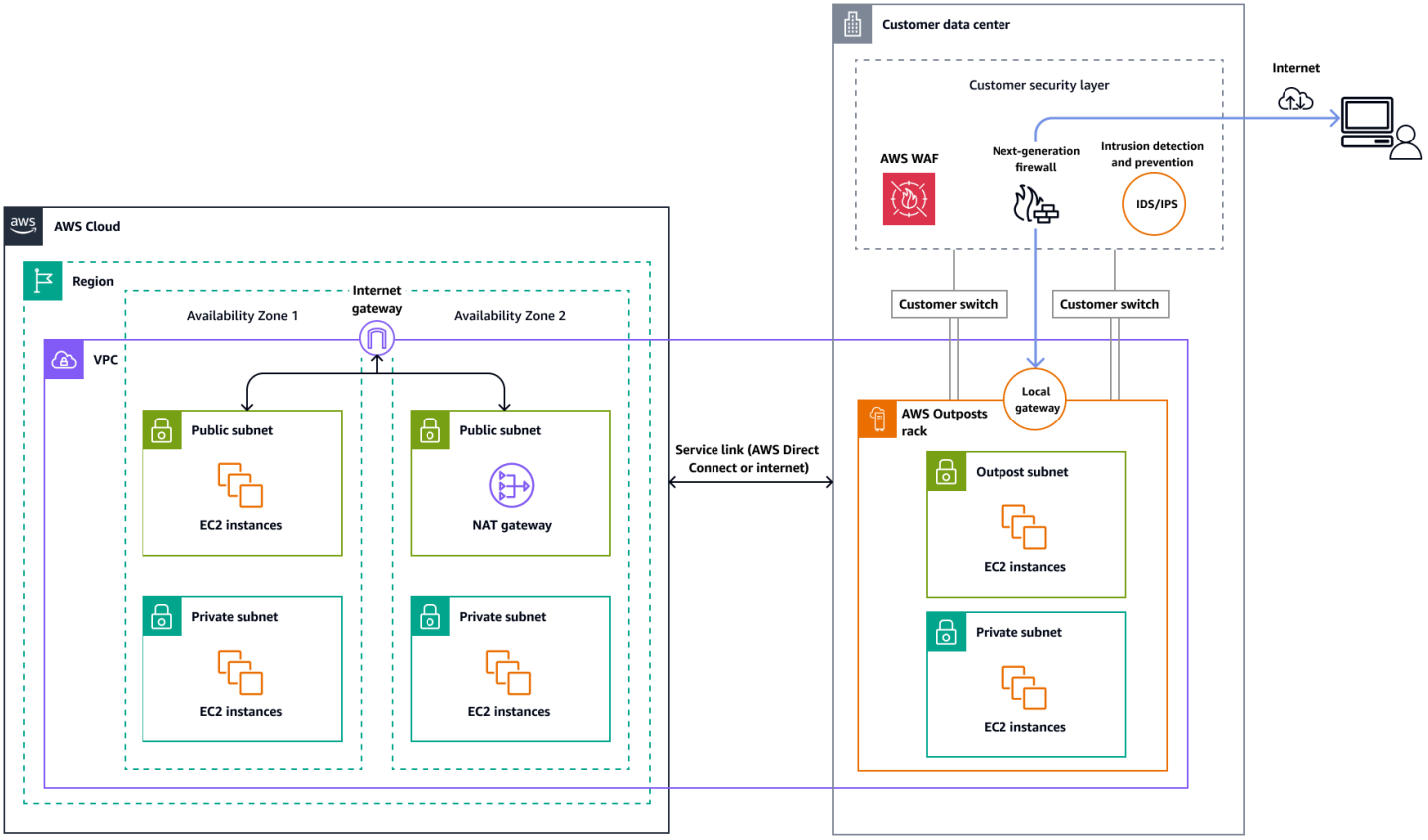
Il diagramma seguente mostra il traffico tra il carico di lavoro nell' AWS Outposts istanza e Internet che attraversa l'istanza principale. Regione AWS



Accesso a Internet tramite la rete del data center locale

In questa opzione, i carichi di lavoro di Outpost accedono a Internet tramite il data center locale. Il traffico del carico di lavoro che accede a Internet attraversa il punto di presenza Internet locale e esce localmente. In questo caso, l'infrastruttura di sicurezza di rete del data center locale è responsabile della protezione del traffico del carico di lavoro. AWS Outposts

L'immagine seguente mostra il traffico tra un carico di lavoro nella AWS Outposts sottorete e Internet che attraversa un data center.



Governance dell'infrastruttura

Indipendentemente dal fatto che i carichi di lavoro siano distribuiti in una Regione AWS zona locale o in un avamposto, puoi utilizzarli AWS Control Tower per la governance dell'infrastruttura. AWS Control Tower offre un modo semplice per configurare e gestire un ambiente AWS multi-account, seguendo le migliori pratiche prescrittive. AWS Control Tower orchestra le funzionalità di molti altri Servizi AWS AWS Organizations AWS Service Catalog, tra cui IAM Identity Center (vedi tutti i servizi integrati) per creare una landing zone in meno di un'ora. Le risorse vengono configurate e gestite per tuo conto.

AWS Control Tower fornisce una governance unificata in tutti gli AWS ambienti, inclusi Regions, Local Zones (estensioni a bassa latenza) e Outposts (infrastruttura locale). Questo aiuta a garantire sicurezza e conformità coerenti nell'intera architettura di cloud ibrido. Per ulteriori informazioni, consulta la documentazione relativa ad AWS Control Tower.

Puoi configurare funzionalità come AWS Control Tower i guardrail per soddisfare i requisiti di residenza dei dati nei governi e nei settori regolamentati come gli istituti di servizi finanziari (). FSIs Per capire come implementare barriere per la residenza dei dati nell'edge, consulta quanto segue:

- Le migliori pratiche per la gestione della residenza dei dati nell' Zone locali AWS uso dei controlli delle landing zone (post AWS sul blog)
- Progettazione per la residenza dei dati con guardrail per AWS Outposts rack e landing zone (post sul blog)AWS
- Residenza dei dati con Hybrid Cloud Services Lens (documentazione AWS Well-Architected Framework)

Condivisione delle risorse di Outposts

Poiché un Outpost è un'infrastruttura limitata che risiede nel tuo data center o in uno spazio di co-ubicazione, per una governance centralizzata è necessario controllare centralmente con quali account AWS Outposts vengono condivise le risorse. AWS Outposts

Con la condivisione di Outpost, i proprietari di Outpost possono condividere le proprie risorse Outposts e Outpost, inclusi i siti e le sottoreti Outpost, con altri Account AWS membri della stessa organizzazione in. AWS Organizations In qualità di proprietario di Outpost, puoi creare e gestire le risorse di Outpost da una posizione centrale e condividerle tra più risorse all'interno della tua organizzazione. Account AWS AWS Ciò consente ad altri utenti di utilizzare i siti Outpost, configurare VPCs, avviare ed eseguire istanze sull'Outpost condiviso.

Le risorse condivisibili in sono: AWS Outposts

- Host dedicati assegnati
- Prenotazioni della capacità
- Pool di indirizzi IP (CoIP) di proprietà del cliente
- Tabelle di routing del gateway locale
- Outposts
- Amazon S3 su Outposts
- Siti
- Sottoreti

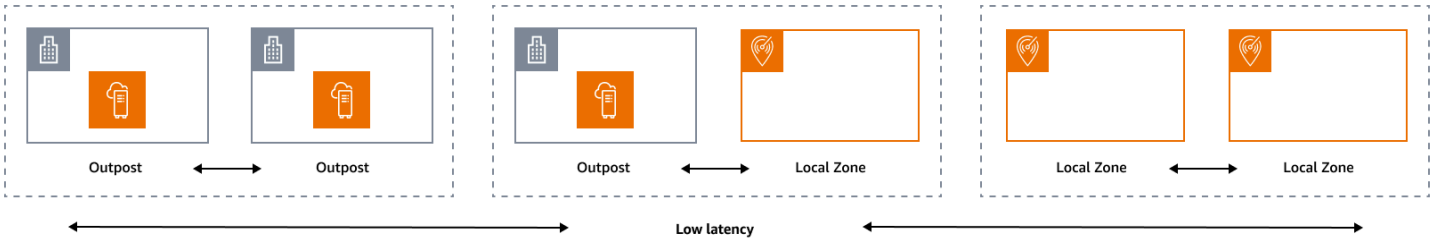
Per seguire le best practice per la condivisione delle risorse Outposts in un ambiente con più account, consulta i seguenti AWS post del blog:

- Condivisione AWS Outposts in un AWS ambiente con più account: parte 1

- Condivisione AWS Outposts in un AWS ambiente con più account: parte 2

Resilienza all'edge

Il pilastro dell'affidabilità comprende la capacità di un carico di lavoro di svolgere la funzione prevista in modo corretto e coerente quando previsto. Ciò include la capacità di utilizzare e testare il carico di lavoro durante il suo ciclo di vita. In questo senso, quando si progetta un'architettura resiliente all'edge, è necessario innanzitutto considerare quali infrastrutture verranno utilizzate per implementare tale architettura. Esistono tre possibili combinazioni da implementare utilizzando Zone locali AWS e AWS Outposts: Outpost to Outpost, Outpost to Local Zone e Local Zone to Local Zone, come illustrato nel diagramma seguente. Sebbene esistano altre possibilità per architetture resilienti, come la combinazione di servizi AWS edge con un'infrastruttura locale tradizionale, oppure Regioni AWS, questa guida si concentra su queste tre combinazioni che si applicano alla progettazione di servizi cloud ibridi



Considerazioni sull'infrastruttura

At AWS, uno dei principi fondamentali della progettazione dei servizi consiste nell'evitare singoli punti di errore nell'infrastruttura fisica sottostante. Grazie a questo principio, AWS il software e i sistemi utilizzano più zone di disponibilità e sono resilienti al guasto di una singola zona. All'edge, AWS offre infrastrutture basate su Local Zones e Outposts. Pertanto, un fattore critico per garantire la resilienza nella progettazione dell'infrastruttura è definire dove vengono distribuite le risorse di un'applicazione.

Zone locali

Le Local Zone agiscono in modo simile alle Zone di disponibilità al loro interno Regione AWS, in quanto possono essere selezionate come ubicazione di collocamento per AWS risorse zonali come sottoreti e istanze. EC2 Tuttavia, non si trovano in centri industriali e IT Regione AWS, ma in prossimità di centri abitati, industriali e IT, dove oggi non esistono. Regione AWS Nonostante ciò, mantengono ancora connessioni sicure e a elevata larghezza di banda tra i carichi di lavoro locali nella zona locale e i carichi di lavoro in esecuzione nella. Regione AWS Pertanto, è consigliabile

utilizzare Local Zones per distribuire i carichi di lavoro più vicino agli utenti per requisiti di bassa latenza.

Outposts

AWS Outposts è un servizio completamente gestito che estende AWS l'infrastruttura e gli strumenti al data center. Servizi AWS APIs La stessa infrastruttura hardware utilizzata in Cloud AWS è installata nel data center. Gli Outposts vengono quindi collegati a quelli più vicini. Regione AWS Puoi utilizzare Outposts per supportare i tuoi carichi di lavoro con bassa latenza o requisiti locali di elaborazione dei dati.

Zone di disponibilità per i genitori

Ogni zona locale o avamposto ha una regione principale (detta anche regione di origine). La regione principale è quella in cui è ancorato il piano di controllo dell'infrastruttura AWS periferica (Outpost o Local Zone). Nel caso delle Local Zones, la regione principale è un componente architettonico fondamentale di una Local Zone e non può essere modificata dai clienti. AWS Outposts si estende Cloud AWS all'ambiente locale, quindi è necessario selezionare una regione e una zona di disponibilità specifiche durante il processo di ordinazione. Questa selezione fissa il piano di controllo della distribuzione di Outposts all' AWS infrastruttura scelta.

Quando si sviluppano architetture ad alta disponibilità nell'edge, la regione principale di queste infrastrutture, come Outposts o Local Zones, deve essere la stessa, in modo che un VPC possa essere esteso tra di loro. Questo VPC esteso è la base per la creazione di queste architetture ad alta disponibilità. Quando si definisce un'architettura altamente resiliente, è per questo che è necessario convalidare la regione principale e la zona di disponibilità della regione in cui il servizio sarà (o è) ancorato. Come illustrato nel diagramma seguente, se si desidera implementare una soluzione ad alta disponibilità tra due Outposts, è necessario scegliere due diverse zone di disponibilità per ancorare gli Outposts. Ciò consente un'architettura Multi-AZ dal punto di vista del piano di controllo. Se desideri implementare una soluzione ad alta disponibilità che includa una o più Local Zones, devi prima convalidare la zona di disponibilità principale in cui è ancorata l'infrastruttura. A tale scopo, utilizzate il seguente comando: AWS CLI

```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

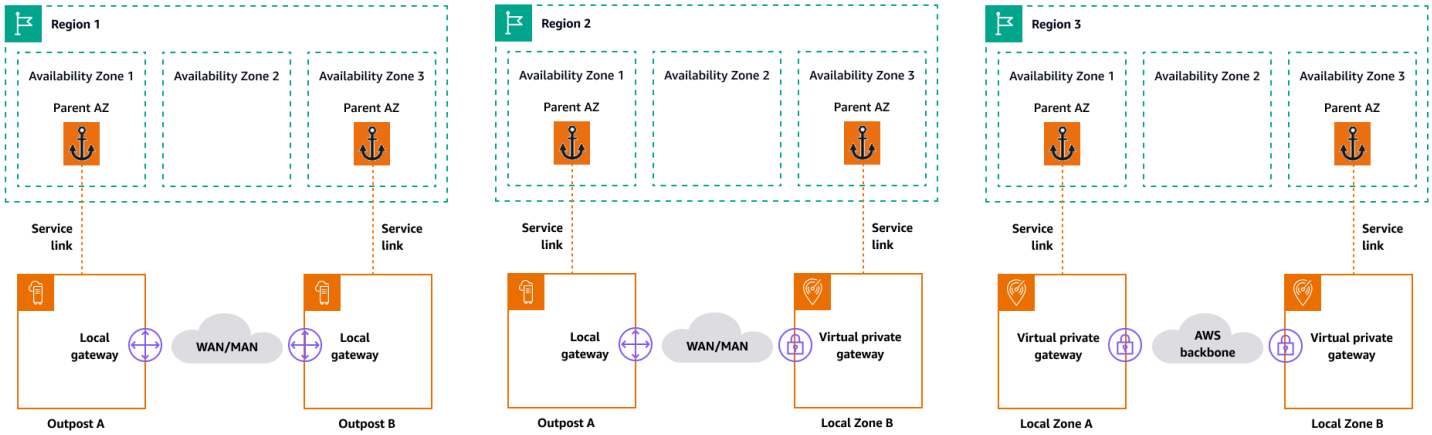
Risultato del comando precedente:

```
{     "AvailabilityZones": [
```

```
        {
            "State": "available",
            "OptInStatus": "opted-in",
            "Messages": [],
            "RegionName": "us-east-1",
            "ZoneName": "us-east-1-mia-1a",
            "ZoneId": "use1-mia1-az1",
            "GroupName": "us-east-1-mia-1",
            "NetworkBorderGroup": "us-east-1-mia-1",
            "ZoneType": "local-zone",
            "ParentZoneName": "us-east-1d",
            "ParentZoneId": "use1-az2"
        }
    ]
}
```


In questo esempio, la zona locale di Miami (`us-east-1d-mia-1a1`) è ancorata alla zona di `us-east-1d-az2` disponibilità. Pertanto, se è necessario creare un'architettura resiliente all'edge, è necessario assicurarsi che l'infrastruttura secondaria (Outposts o Local Zones) sia ancorata a una zona di disponibilità diversa da. **`us-east-1d-az2`** Ad esempio, `us-east-1d-az1` sarebbe valido.

Il diagramma seguente fornisce esempi di infrastrutture edge ad alta disponibilità.



Considerazioni sulla rete

Questa sezione illustra le considerazioni iniziali sulla rete periferica, principalmente per le connessioni per accedere all'infrastruttura perimetrale. Esamina le architetture valide che forniscono una rete resiliente per il collegamento di servizio.

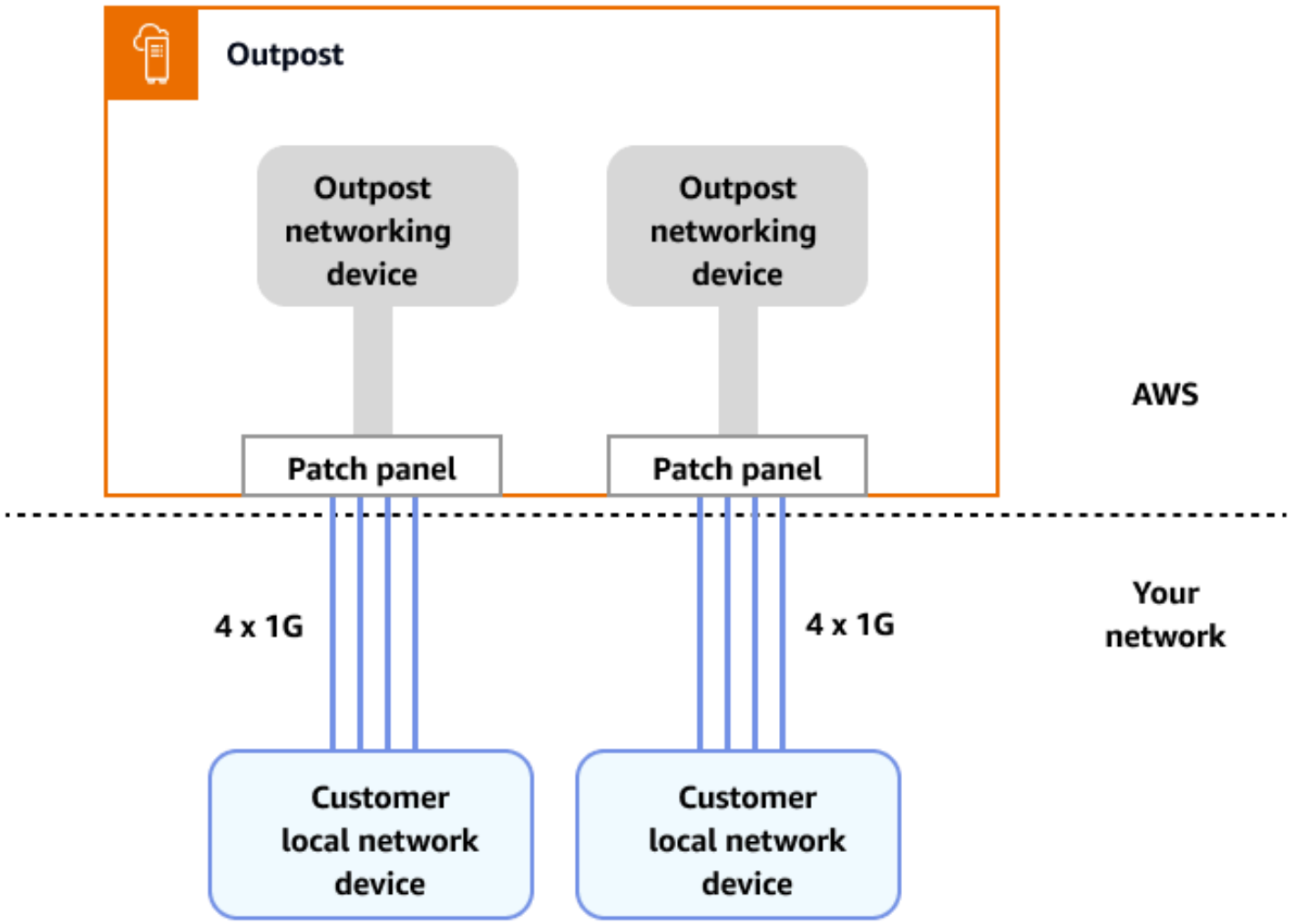
Rete resiliente per Local Zones

Le Local Zones sono collegate alla regione principale con collegamenti multipli, ridondanti, sicuri e ad alta velocità che consentono di utilizzare qualsiasi servizio regionale, come Amazon S3 e Amazon RDS, senza interruzioni. Sei responsabile della fornitura della connettività dall'ambiente locale o dagli utenti alla zona locale. Indipendentemente dall'architettura di connettività scelta (ad esempio, VPN o AWS Direct Connect), la latenza che deve essere raggiunta tramite i collegamenti di rete deve essere equivalente per evitare qualsiasi impatto sulle prestazioni delle applicazioni in caso di guasto in un collegamento principale. Se utilizzate AWS Direct Connect, le architetture di resilienza applicabili sono le stesse di quelle per l'accesso a an Regione AWS, come documentato nelle raccomandazioni sulla resilienza.AWS Direct Connect Tuttavia, esistono scenari che si applicano principalmente alle Local Zones internazionali. Nel paese in cui è abilitata la Local Zone, avere un solo AWS Direct Connect PoP rende impossibile la creazione delle architetture consigliate per AWS Direct Connect la resilienza. Se hai accesso a una sola AWS Direct Connect posizione o hai bisogno di resilienza oltre una singola connessione, puoi creare un'appliance VPN su Amazon EC2 e AWS Direct Connect, come illustrato e discusso nel post del AWS blog Enabling high availability connectivity from on-premise to. Zone locali AWS

Rete di resilienza per Outposts

A differenza delle Local Zones, gli Outposts dispongono di una connettività ridondante per accedere ai carichi di lavoro distribuiti in Outposts dalla rete locale. Questa ridondanza viene ottenuta tramite due dispositivi di rete Outposts (). ONDs Ogni OND richiede almeno due connessioni in fibra a 1 Gbps, 10 Gbps, 40 Gbps o 100 Gbps alla rete locale. Queste connessioni devono essere configurate come un gruppo di aggregazione di link (LAG) per consentire l'aggiunta scalabile di più collegamenti.

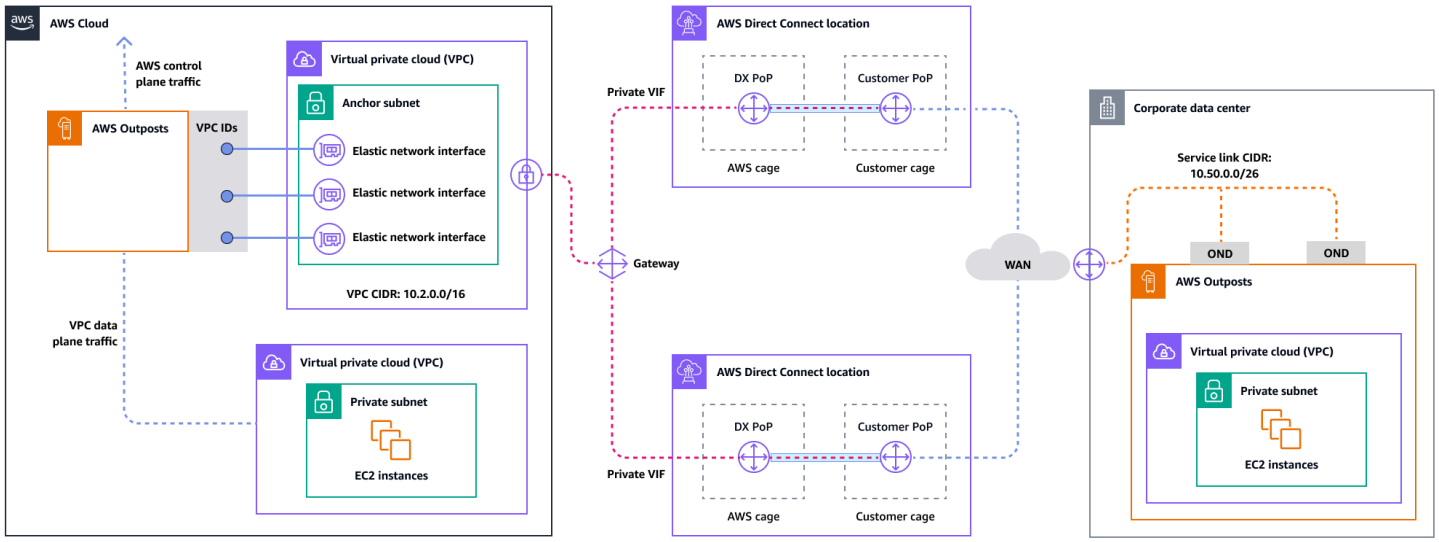
Velocità di uplink	Numero di uplink
1 Gb/s	1, 2, 4, 6 o 8
10 Gb/s	1, 2, 4, 8, 12 o 16
40 o 100 Gbps	1, 2 o 4



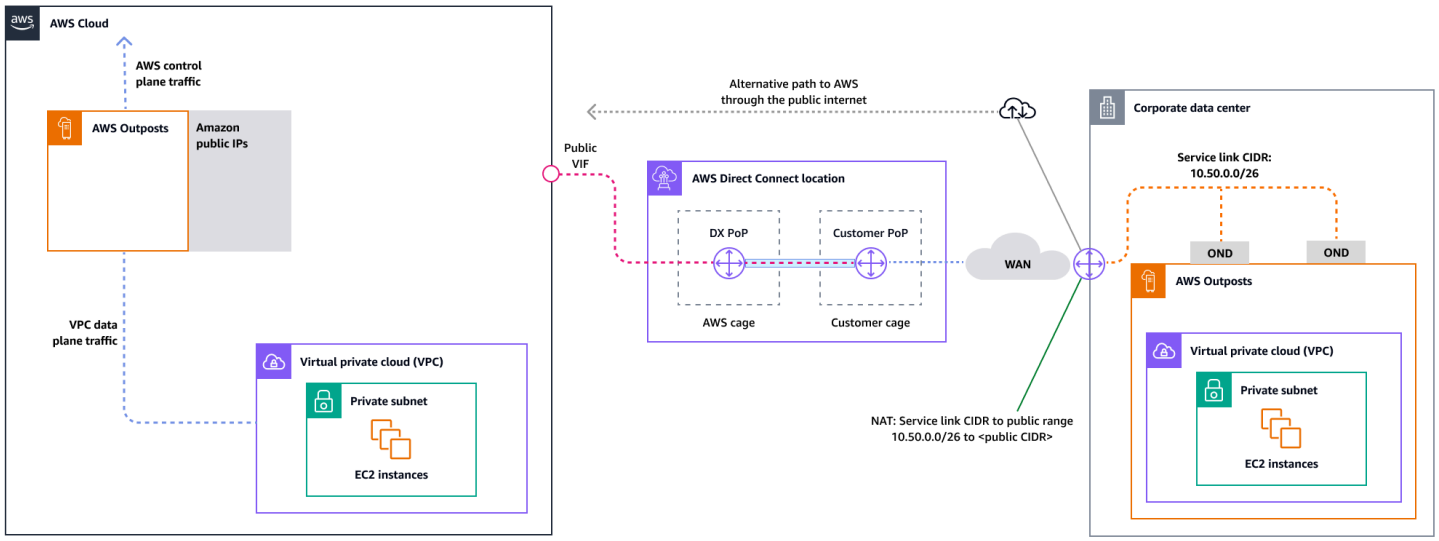
Per ulteriori informazioni su questa connettività, consulta Connettività di rete locale per Outposts Racks nella AWS Outposts documentazione.

Per un'esperienza e una resilienza ottimali, si AWS consiglia di utilizzare una connettività ridondante di almeno 500 Mbps (1 Gbps è preferibile) per la connessione Service Link a. Regione AWSÈ possibile utilizzare AWS Direct Connect o una connessione Internet per il collegamento al servizio. Questo minimo consente di avviare EC2 istanze, collegare volumi EBS e accedere, ad esempio Amazon EKS Servizi AWS, Amazon EMR e metriche. CloudWatch

Il diagramma seguente illustra questa architettura per una connessione privata ad alta disponibilità.



Il diagramma seguente illustra questa architettura per una connessione pubblica ad alta disponibilità.



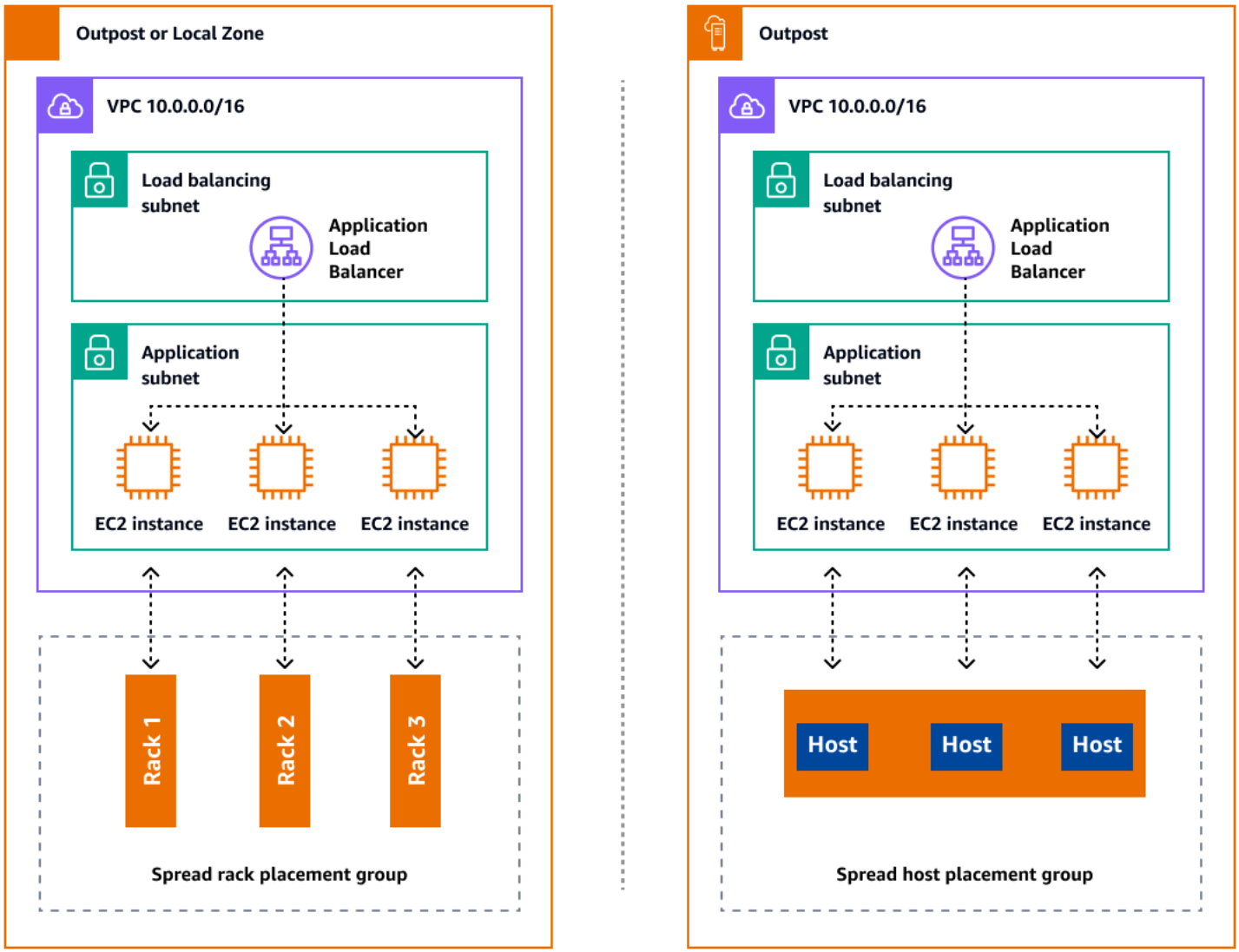
Scalabilità delle installazioni rack Outposts con i rack ACE

Il rack Aggregation, Core, Edge (ACE) funge da punto di aggregazione critico per le implementazioni AWS Outposts multi-rack ed è consigliato principalmente per installazioni che superano i tre rack o per pianificare espansioni future. Ogni rack ACE è dotato di quattro router che supportano connessioni a 10 Gbps, 40 Gbps e 100 Gbps (100 Gbps sono ottimali). Ogni rack può connettersi a un massimo di quattro dispositivi upstream del cliente per la massima ridondanza. I rack ACE consumano fino a 10 kVA di potenza e pesano fino a 705 libbre. I vantaggi principali includono la riduzione dei requisiti di rete fisica, un minor numero di uplink di cablaggio in fibra e una riduzione delle interfacce virtuali VLAN. AWS monitora questi rack tramite dati di telemetria tramite tunnel VPN e collabora a stretto contatto con i clienti durante l'installazione per garantire la corretta disponibilità

dell'alimentazione, la configurazione di rete e il posizionamento ottimale. L'architettura rack ACE offre un valore crescente man mano che le implementazioni scalano e semplifica efficacemente la connettività, riducendo al contempo la complessità e i requisiti delle porte fisiche nelle installazioni più grandi. Per ulteriori informazioni, consulta il post del AWS blog Scaling AWS Outposts rack deployments with ACE Rack.

Distribuzione delle istanze tra Outposts e Local Zones

Outposts e Local Zones hanno un numero finito di server di elaborazione. Se l'applicazione distribuisce più istanze correlate, queste istanze potrebbero essere distribuite sullo stesso server o su server nello stesso rack, a meno che non siano configurate diversamente. Oltre alle opzioni predefinite, puoi distribuire le istanze tra i server per mitigare il rischio di eseguire istanze correlate sulla stessa infrastruttura. È inoltre possibile distribuire le istanze su più rack utilizzando i gruppi di posizionamento delle partizioni. Questo è chiamato modello di distribuzione Spread Rack. Utilizza la distribuzione automatica per distribuire le istanze tra le partizioni del gruppo o distribuisci le istanze su partizioni di destinazione selezionate. Distribuendo le istanze sulle partizioni di destinazione, puoi distribuire risorse selezionate sullo stesso rack distribuendo altre risorse tra i rack. Outposts offre anche un'altra opzione chiamata spread host che consente di distribuire il carico di lavoro a livello di host. Il diagramma seguente mostra le opzioni di distribuzione spread rack e spread host.



Ingresso Amazon RDS Multi-AZ AWS Outposts

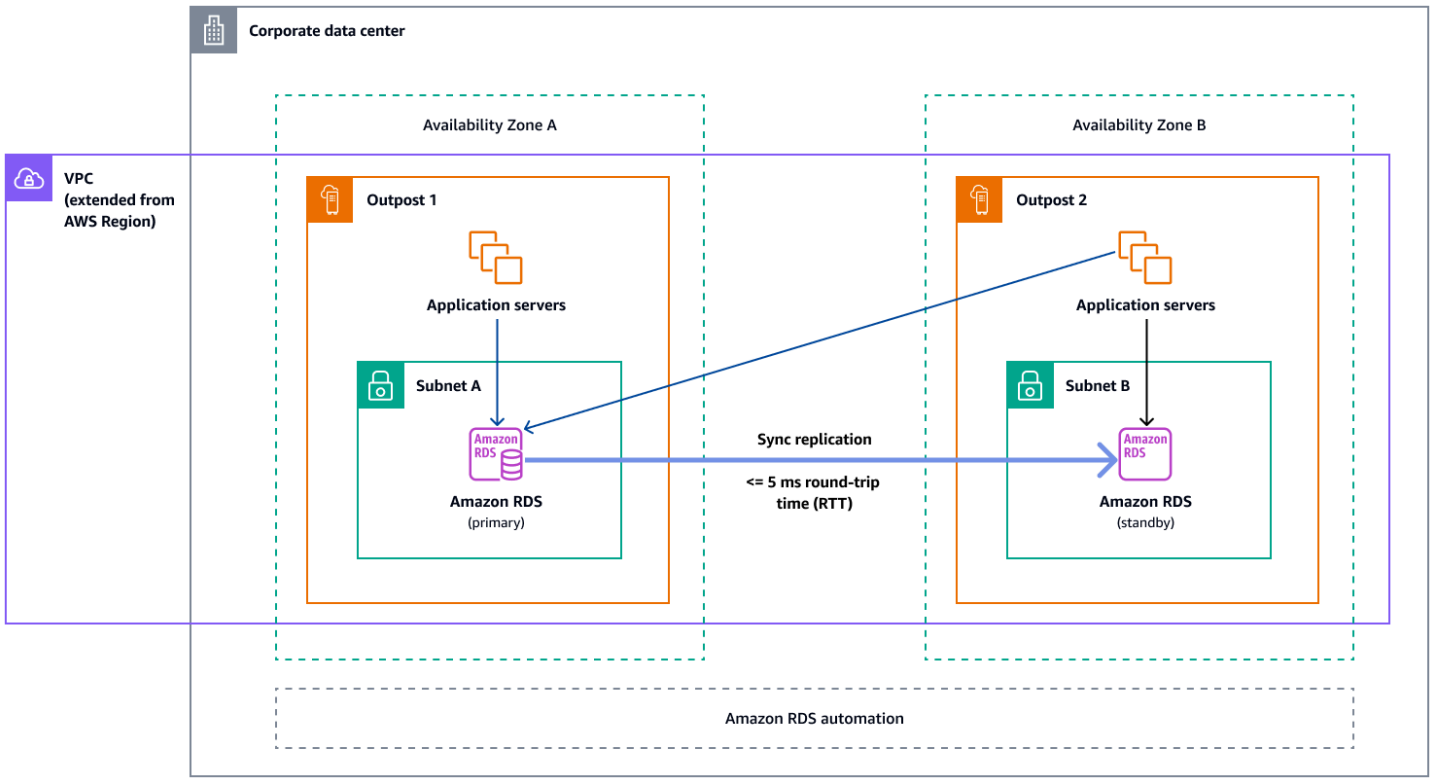
Quando utilizzi distribuzioni di istanze Multi-AZ su Outposts, Amazon RDS crea due istanze di database su due Outposts. Ogni Outpost funziona sulla propria infrastruttura fisica e si connette a diverse zone di disponibilità in una regione per un'elevata disponibilità. Quando due Outposts sono collegati tramite una connessione locale gestita dal cliente, Amazon RDS gestisce la replica sincrona tra l'istanza del database primario e quella di standby. In caso di guasto del software o dell'infrastruttura, Amazon RDS promuove automaticamente l'istanza di standby al ruolo principale e aggiorna il record DNS in modo che punti alla nuova istanza primaria. Per eseguire le implementazioni Multi-AZ, Amazon RDS crea un'istanza database primaria su un outpost e replica in modo sincrono i dati in un'istanza database in standby su un altro outpost. Le implementazioni Multi-

AZ su Outposts funzionano come le implementazioni Multi-AZ in, con le seguenti differenze: Regioni AWS

- Richiedono una connessione locale tra due o più outpost.
- Richiedono pool di indirizzi IP (CoIP) di proprietà del cliente. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente per Amazon RDS AWS Outposts nella documentazione di Amazon RDS.
- La replica viene eseguita sulla rete locale.

Le implementazioni Multi-AZ sono disponibili per tutte le versioni supportate di MySQL e PostgreSQL su Amazon RDS on Outposts. I backup locali non sono supportati per le implementazioni Multi-AZ.

Il diagramma seguente mostra l'architettura per le configurazioni Amazon RDS on Outposts Multi-AZ.



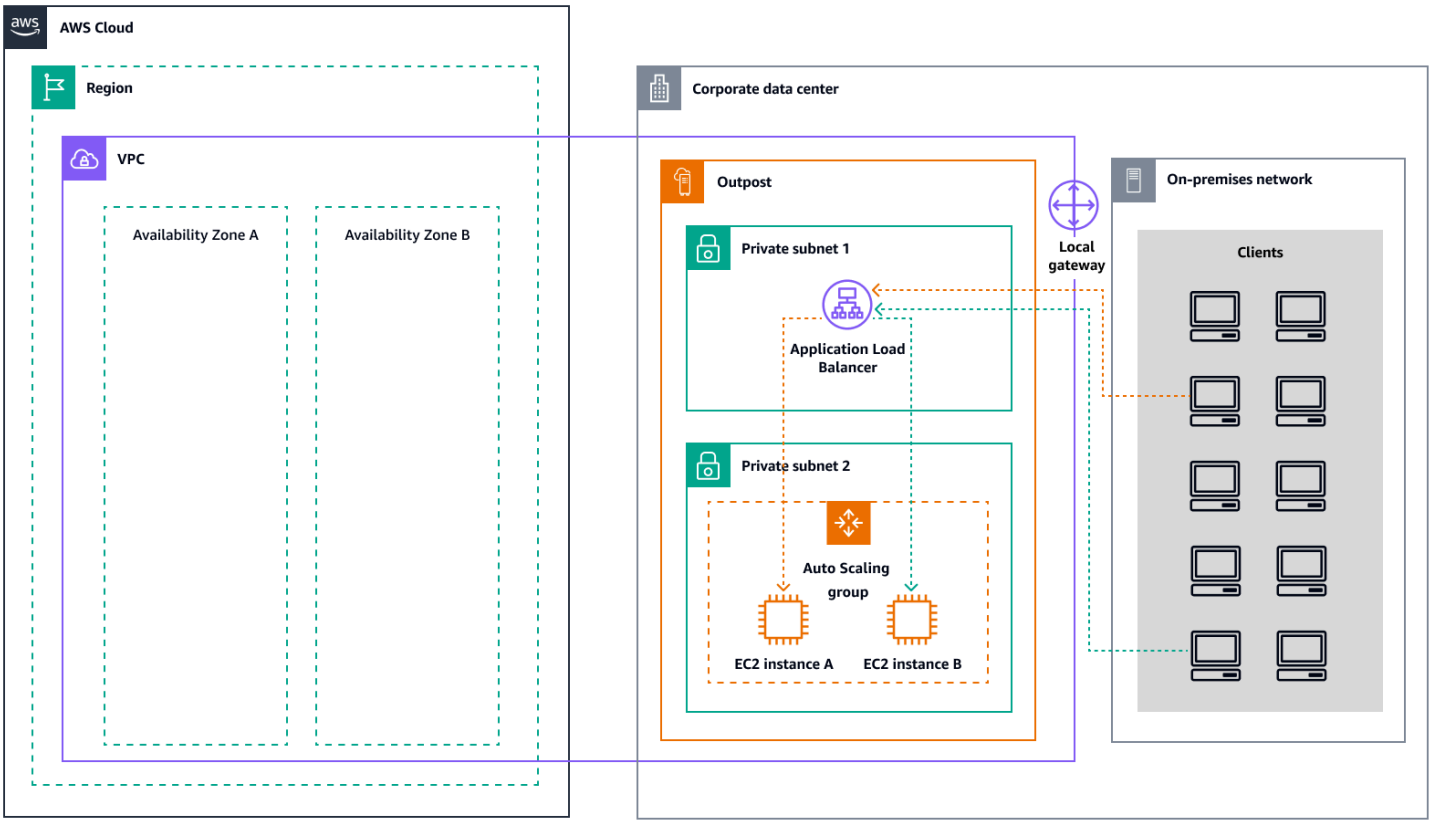
Meccanismi di failover

Bilanciamento del carico e scalabilità automatica

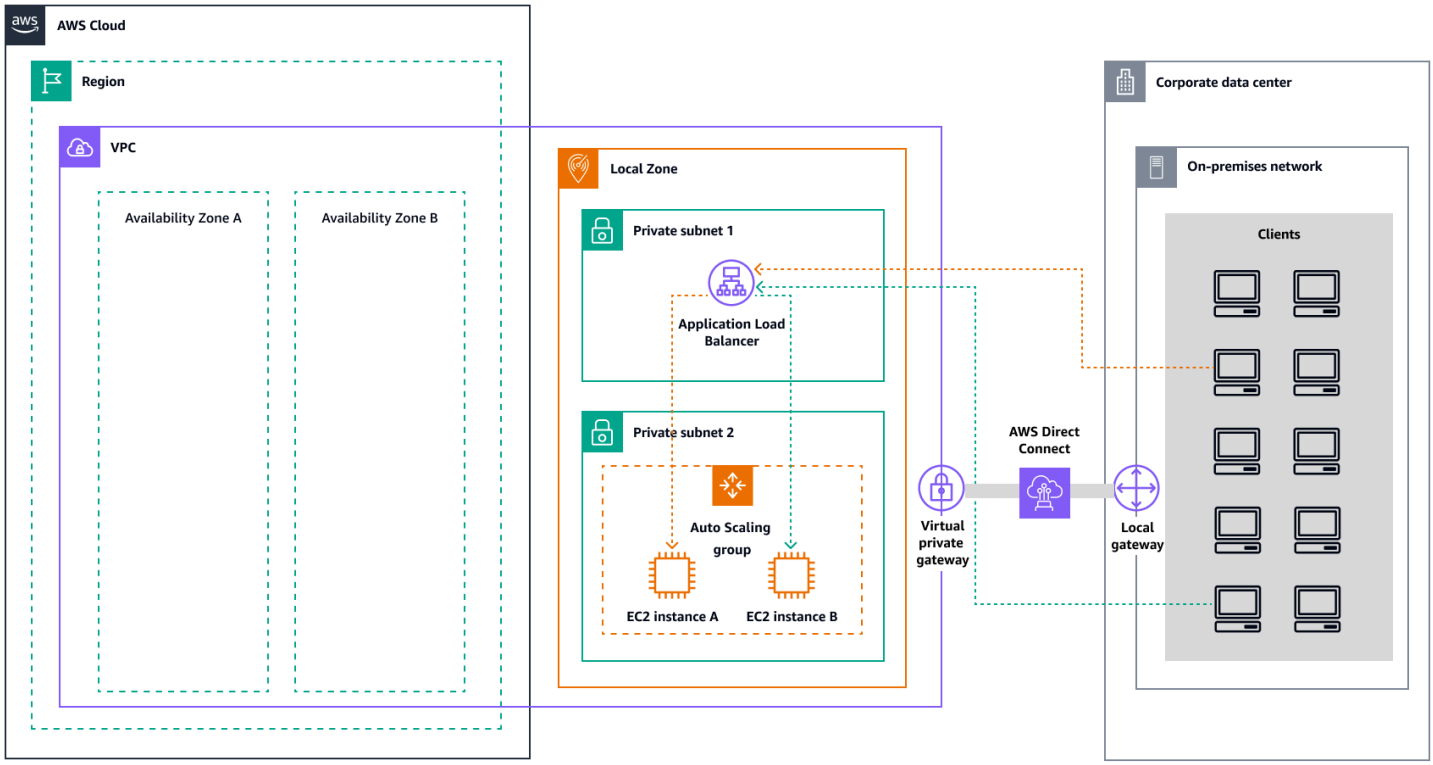
Elastic Load Balancing (ELB) distribuisce automaticamente il traffico delle applicazioni in entrata su tutte le EC2 istanze in esecuzione. ELB aiuta a gestire le richieste in entrata indirizzando il traffico

in modo ottimale in modo che nessuna singola istanza venga sovraccaricata. Per utilizzare ELB con il tuo gruppo Amazon EC2 Auto Scaling, collega il load balancer al tuo gruppo Auto Scaling. In questo modo il gruppo viene registrato con il sistema di bilanciamento del carico, che funge da unico punto di contatto per tutto il traffico web in entrata verso il gruppo. Quando si utilizza ELB con il gruppo Auto Scaling, non è necessario registrare EC2 singole istanze con il sistema di bilanciamento del carico. Le istanze avviate dal gruppo con dimensionamento automatico vengono registrate automaticamente con il sistema di bilanciamento del carico. Analogamente, le istanze terminate dal gruppo Auto Scaling vengono automaticamente cancellate dal sistema di bilanciamento del carico. Dopo aver collegato un load balancer al gruppo Auto Scaling, puoi configurare il gruppo in modo che utilizzi le metriche ELB (come il numero di richieste di Application Load Balancer per target) per scalare il numero di istanze nel gruppo in base alle fluttuazioni della domanda. Facoltativamente, puoi aggiungere controlli di integrità ELB al tuo gruppo Auto Scaling in modo che Amazon Auto Scaling possa identificare e sostituire EC2 le istanze non integre sulla base di questi controlli di integrità. Puoi anche creare un CloudWatch allarme Amazon che ti avvisi se il numero di host sani del gruppo target è inferiore a quello consentito.

Il diagramma seguente illustra come un Application Load Balancer gestisce i carichi di lavoro su Amazon in. EC2 AWS Outposts



Il diagramma seguente illustra un'architettura simile per Amazon EC2 in Local Zones.



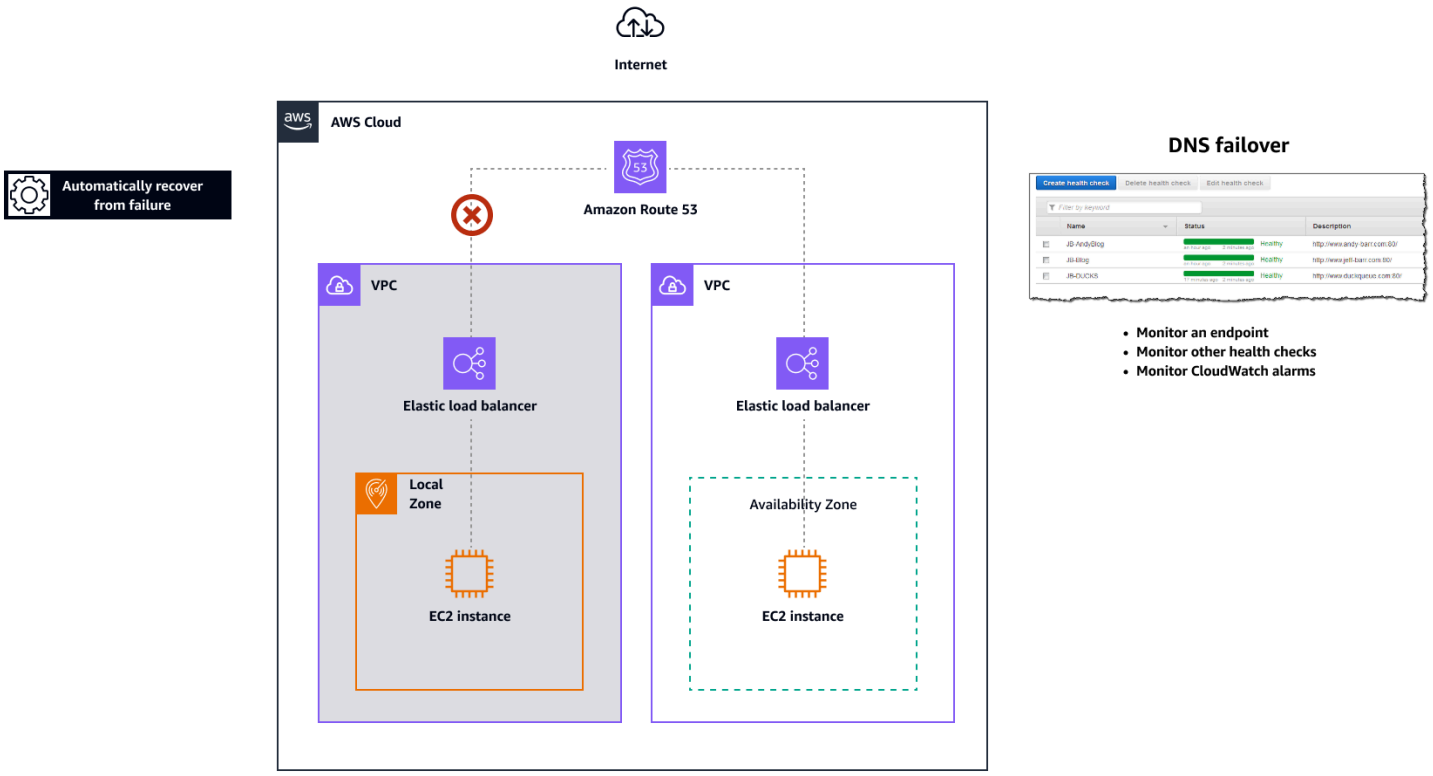
> **Note**
>
> Gli Application Load Balancer sono disponibili sia nelle Local Zones che AWS Outposts nelle Local Zones. Tuttavia, per utilizzare un Application Load Balancer in AWS Outposts, è necessario dimensionare la EC2 capacità di Amazon per fornire la scalabilità richiesta dal load balancer. Per ulteriori informazioni sul dimensionamento di un load balancer in AWS Outposts, consulta il post del AWS blog Configuring an Application Load Balancer on. AWS Outposts

Amazon Route 53 per il failover DNS

Se disponi di più risorse che svolgono la stessa funzione, ad esempio più server HTTP o di posta, puoi configurare Amazon Route 53 per verificare lo stato delle tue risorse e rispondere alle query DNS utilizzando solo le risorse integre. Ad esempio, supponiamo che il tuo sito Web sia ospitato su due server. `example.com` Un server si trova in una zona locale e l'altro server si trova in un avamposto. È possibile configurare Route 53 per verificare lo stato di tali server e rispondere alle query DNS `example.com` utilizzando solo i server attualmente integri. Se utilizzi record di alias per

indirizzare il traffico verso AWS risorse selezionate, come i sistemi di bilanciamento del carico ELB, puoi configurare Route 53 per valutare lo stato della risorsa e indirizzare il traffico solo verso risorse integre. Quando configuri un record di alias per valutare lo stato di una risorsa, non è necessario creare un controllo dello stato di quella risorsa.

Il diagramma seguente illustra i meccanismi di failover della Route 53.



> **Note**
>
> - Se stai creando record di failover in una zona ospitata privata, puoi creare una CloudWatch metrica, associare un allarme alla metrica e quindi creare un controllo dello stato basato sul flusso di dati relativo all'allarme.
> - Per rendere un'applicazione accessibile al pubblico AWS Outposts utilizzando un Application Load Balancer, configura configurazioni di rete che abilitino la traduzione degli indirizzi di rete (Destination Network Address Translation) dal pubblico IPs al nome di dominio completo (FQDN) del load balancer e crea una regola di failover Route 53 con controlli di integrità che puntano all'IP pubblico esposto. Questa combinazione garantisce un accesso pubblico affidabile all'applicazione ospitata da Outposts.

Amazon Route 53 Resolver su AWS Outposts

Amazon Route 53 Resolverè disponibile negli scaffali Outposts. Fornisce servizi e applicazioni locali con risoluzione DNS locale direttamente da Outposts. Gli endpoint Local Route 53 Resolver abilitano anche la risoluzione DNS tra Outposts e il server DNS locale. Route 53 Resolver on Outposts aiuta a migliorare la disponibilità e le prestazioni delle applicazioni locali.

Uno dei casi d'uso tipici di Outposts consiste nell'implementazione di applicazioni che richiedono un accesso a bassa latenza ai sistemi locali, come apparecchiature di fabbrica, applicazioni di trading ad alta frequenza e sistemi di diagnosi medica.

Se scegli di utilizzare i Resolver Route 53 locali su Outposts, le applicazioni e i servizi continueranno a beneficiare della risoluzione DNS locale per scoprire altri servizi, anche in caso di perdita della connettività con un genitore. Regione AWS I Resolver locali aiutano anche a ridurre la latenza per le risoluzioni DNS perché i risultati delle query vengono memorizzati nella cache e serviti localmente dagli Outposts, il che elimina inutili round trip verso il principale. Regione AWS Tutte le risoluzioni DNS per le applicazioni in Outposts VPCs che utilizzano DNS privato vengono servite localmente.

Oltre ad abilitare i Resolver locali, questo lancio abilita anche gli endpoint Resolver locali. Gli endpoint in uscita Route 53 Resolver consentono ai Resolver Route 53 di inoltrare le query DNS ai resolver DNS che gestisci, ad esempio sulla tua rete locale. Al contrario, gli endpoint in entrata di Route 53 Resolver inoltrano le query DNS che ricevono dall'esterno del VPC al Resolver in esecuzione su Outposts. Consente di inviare query DNS per i servizi distribuiti su un VPC Outposts privato dall'esterno di tale VPC. Per ulteriori informazioni sugli endpoint in entrata e in uscita, consulta Risolvere le query DNS tra e la rete nella documentazione di Route 53. VPCs

Pianificazione della capacità a livello perimetrale

La fase di pianificazione della capacità prevede la raccolta dei requisiti di vCPU, memoria e storage per implementare l'architettura. Nel pilastro dell'ottimizzazione dei costi del AWS Well-Architected Framework, il corretto dimensionamento è un processo continuo che inizia con la pianificazione. È possibile utilizzare AWS gli strumenti per definire ottimizzazioni basate sul consumo di risorse interne. AWS

La pianificazione della capacità Edge in Local Zones è la stessa di Regioni AWS. È necessario verificare che le istanze siano disponibili in ogni zona locale, poiché alcuni tipi di istanze potrebbero differire dai tipi presenti in Regioni AWS. Per Outposts, è necessario pianificare la capacità in base ai requisiti del carico di lavoro. Gli Outposts hanno un numero fisso di istanze per host e possono

essere riassegnati secondo necessità. Se i tuoi carichi di lavoro richiedono capacità di riserva, tienilo in considerazione quando pianifichi le tue esigenze di capacità.

Pianificazione della capacità su Outposts

AWS Outposts la pianificazione della capacità richiede input specifici per il corretto dimensionamento a livello regionale, oltre a fattori specifici dell'edge che influiscono sulla disponibilità, sulle prestazioni e sulla crescita delle applicazioni. Per una guida dettagliata, consulta la pianificazione della capacità nel AWS white paper AWS Outposts Considerazioni sulla progettazione e l'architettura ad alta disponibilità.

Pianificazione della capacità per Local Zones

Una zona locale è un'estensione di una Regione AWS zona geograficamente vicina agli utenti. Le risorse create in una zona locale possono servire gli utenti locali con comunicazioni a latenza molto bassa. Per abilitare una zona locale nella tua area Account AWS, consulta la sezione Guida introduttiva Zone locali AWS alla AWS documentazione. Ogni zona locale ha diversi slot disponibili per famiglie di EC2 istanze. Convalida le istanze disponibili in ogni zona locale prima di utilizzarle. Per confermare le EC2 istanze disponibili, esegui il seguente comando: AWS CLI

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

Output previsto:

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
      },
      ...
  ]
```

```
}
```

Gestione dell'infrastruttura perimetrale

AWS fornisce servizi completamente gestiti che estendono AWS l'infrastruttura APIs, i servizi e gli strumenti più vicini agli utenti finali e ai data center. I servizi disponibili in Outposts e Local Zones sono gli stessi disponibili in Regioni AWS, quindi puoi gestirli utilizzando la stessa AWS console AWS CLI, oppure. AWS APIs Per i servizi supportati, consulta la tabella di confronto delle AWS Outposts funzionalità e Zone locali AWS le funzionalità.

Implementazione di servizi all'edge

Puoi configurare i servizi disponibili in Local Zones e Outposts nello stesso modo in cui li configuri in Regioni AWS: utilizzando la AWS console, AWS CLI, o. AWS APIs La differenza principale tra le implementazioni regionali e periferiche è rappresentata dalle sottoreti in cui verranno fornite le risorse. La sezione Networking at the edge descrive come vengono distribuite le sottoreti in Outposts e Local Zones. Dopo aver identificato le sottoreti perimetrali, si utilizza l'ID della sottorete perimetrale come parametro per distribuire il servizio in Outposts o Local Zones. Le sezioni seguenti forniscono esempi di implementazione di servizi edge.

Amazon EC2 all'avanguardia

L'`run-instances`esempio seguente avvia una singola istanza di tipo `m5.2xlarge` nella sottorete edge per la regione corrente. La key pair è facoltativa se non prevedi di connetterti alla tua istanza utilizzando SSH su Linux o il protocollo RDP (Remote Desktop Protocol) su Windows.

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

Application Load Balancer a livello perimetrale

L'`create-load-balancer`esempio seguente crea un Application Load Balancer interno e abilita le Local Zones o Outposts per le sottoreti specificate.

```
aws elbv2 create-load-balancer \
```

```
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets <subnet-edge-id>
```

Per distribuire un Application Load Balancer con accesso a Internet in una sottorete di un Outpost, impostate il `internet-facing` flag nell'`--scheme`opzione e fornite un ID pool CoIP, come mostrato in questo esempio:

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

Per informazioni sulla distribuzione di altri servizi all'edge, segui questi link:

Servizio	AWS Outposts	Zone locali AWS
Amazon EKS	Implementa Amazon EKS in locale con AWS Outposts	Avvia cluster EKS a bassa latenza con Zone locali AWS
Amazon ECS	Amazon ECS su AWS Outposts	Applicazioni Amazon ECS in sottoreti condivise, Local Zones e Wavelength Zones
Amazon RDS	Amazon RDS su AWS Outposts	Seleziona la sottorete Local Zone
Amazon S3	Guida introduttiva ad Amazon S3 on Outposts	Non disponibile
Amazon ElastiCache	Usare Outposts con ElastiCache	Utilizzo di Local Zones con ElastiCache
Amazon EMR	Cluster EMR attivi AWS Outposts	Cluster EMR attivi Zone locali AWS
Amazon FSx	Non disponibile	Seleziona la sottorete Local Zone

Servizio	AWS Outposts	Zone locali AWS
AWS Elastic Disaster Recovery	Lavorare con e AWS Elastic Disaster RecoveryAWS Outposts	Non disponibile
AWS Application Migration Service	Non disponibile	Seleziona la sottorete Local Zone come sottorete di staging

CLI e SDK specifici per Outposts

AWS Outposts dispone di due gruppi di comandi, uno APIs per creare un ordine di servizio o manipolare le tabelle di routing tra il gateway locale e la rete locale.

Processo di ordinazione Outposts

Puoi usare AWS CLIo Outposts per creare un sito Outposts, APIs per creare un Outpost e per creare un ordine Outposts. Ti consigliamo di rivolgerti a uno specialista del cloud ibrido durante il processo di AWS Outposts ordinazione per garantire una corretta selezione delle risorse IDs e una configurazione ottimale per le tue esigenze di implementazione. Per un elenco completo degli ID delle risorse, consulta la pagina dei prezzi dei AWS Outposts rack.

Gestione del gateway locale

La gestione e il funzionamento del gateway locale (LGW) in Outposts richiedono AWS CLI la conoscenza dei comandi SDK disponibili per questa attività. È possibile utilizzare AWS CLI and AWS SDKs per creare e modificare percorsi LGW, tra le altre attività. Per ulteriori informazioni sulla gestione del LGW, consulta queste risorse:

- AWS CLI per Amazon EC2
- EC2.Client in AWS SDK for Python (Boto)
- Ec2Client in AWS SDK per Java

CloudWatch metriche e registri

Per Servizi AWS questo sono disponibili sia in Outposts che in Local Zones, le metriche e i log vengono gestiti allo stesso modo delle Regioni. Amazon CloudWatch fornisce metriche dedicate al monitoraggio degli Outposts nelle seguenti dimensioni:

Dimensione	Descrizione
`Account`	L'account o il servizio che utilizza la capacità
`InstanceFamily`	La famiglia di istanze
`InstanceType`	il tipo di istanza
`OutpostId`	L'ID dell'avamposto
`VolumeType`	Il tipo di volume EBS
`VirtualInterfaceId`	L'ID del gateway locale o dell'interfaccia virtuale di service link (VIF)
`VirtualInterfaceGroupId`	L'ID del gruppo VIF per il gateway locale VIF

Per ulteriori informazioni, consulta le CloudWatch metriche per i rack Outposts nella documentazione di Outposts.

Risorse

AWS riferimenti

- Cloud ibrido con AWS
- AWS Outposts Guida per l'utente dei rack Outposts
- Guida per l'utente di Zone locali AWS
- AWS Outposts Famiglia
- Zone locali AWS
- Estendere un VPC a una zona locale, Wavelength Zone o Outpost (documentazione Amazon VPC)
- Istanze Linux in Local Zones (EC2 documentazione Amazon)
- Istanze Linux in Outposts (documentazione Amazon EC2)
- Inizia a distribuire applicazioni a bassa latenza con (tutorial) Zone locali AWS

AWS post sul blog

- Esecuzione AWS dell'infrastruttura in locale con Amazon EC2
- Creazione di applicazioni moderne con Amazon EKS su Amazon EC2
- Come scegliere tra le modalità di routing CoIP e VPC diretto su Amazon rack EC2
- Selezione degli switch di rete per Amazon EC2
- Conservazione di una copia locale dei dati in Zone locali AWS
- Amazon ECS su Amazon EC2
- Gestione della rete di servizi edge-aware con Amazon EKS per Zone locali AWS
- Implementazione del routing di ingresso del gateway locale su Amazon EC2
- Automatizzazione delle distribuzioni dei carichi di lavoro in Zone locali AWS
- Condivisione di Amazon EC2 in un AWS ambiente con più account: parte 1
- Condivisione di Amazon EC2 in un AWS ambiente con più account: parte 2
- AWS Direct Connect e modelli di Zone locali AWS interoperabilità
- Implementa Amazon RDS su Amazon EC2 con disponibilità elevata Multi-AZ

Collaboratori

Le seguenti persone hanno contribuito a questa guida.

Scrittura

- Leonardo Solano, principale architetto di soluzioni di cloud ibrido, AWS
- Len Gomes, architetto di soluzioni per i partner, AWS
- Matt Price, tecnico senior del supporto aziendale, AWS
- Tom Gadomski, architetto delle soluzioni, AWS
- Obed Gutierrez, architetto delle soluzioni, AWS
- Dionysios Kakaletris, responsabile tecnico degli account, AWS
- Vamsi Krishna, specialista dei Principal Outposts, AWS

Revisione

- David Filiatrault, consulente di consegna, AWS

Scrittura tecnica

- Handan Selamoglu, responsabile della documentazione senior, AWS

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	—	10 giugno 2025

AWS Glossario delle linee guida prescrittive

I seguenti sono termini di uso comune nelle strategie, nelle guide e nei modelli forniti da AWS Prescriptive Guidance. Per suggerire voci, utilizza il link Fornisci feedback alla fine del glossario.

Numeri

7 R

Sette strategie di migrazione comuni per trasferire le applicazioni sul cloud. Queste strategie si basano sulle 5 R identificate da Gartner nel 2011 e sono le seguenti:

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione compatibile con Amazon Aurora PostgreSQL.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale ad Amazon Relational Database Service (Amazon RDS) per Oracle in. Cloud AWS
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: migra il tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com.
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: migra il database Oracle locale su Oracle su un'istanza in. EC2 Cloud AWS
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Si esegue la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione suMicrosoft Hyper-V. AWS
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati (utilizzando uno strumento di replica bidirezionale o operazioni di doppia scrittura) ed entrambi i database gestiscono le transazioni provenienti dalle applicazioni di connessione durante la migrazione. Questo metodo supporta la migrazione in piccoli batch controllati anziché richiedere una conversione una tantum. È più flessibile ma richiede più lavoro rispetto alla migrazione attiva-passiva.

migrazione attiva-passiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati, ma solo il database di origine gestisce le transazioni provenienti dalle applicazioni di connessione mentre i dati vengono replicati nel database di destinazione. Il database di destinazione non accetta alcuna transazione durante la migrazione.

funzione di aggregazione

Una funzione SQL che opera su un gruppo di righe e calcola un singolo valore restituito per il gruppo. Esempi di funzioni aggregate includono `SUM` e. `MAX`

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

Il processo di eliminazione permanente delle informazioni personali in un set di dati. L'anonimizzazione può aiutare a proteggere la privacy personale. I dati anonimi non sono più considerati dati personali.

anti-modello

Una soluzione utilizzata frequentemente per un problema ricorrente in cui la soluzione è controproducente, inefficace o meno efficace di un'alternativa.

controllo delle applicazioni

Un approccio alla sicurezza che consente l'uso solo di applicazioni approvate per proteggere un sistema dal malware.

portfolio di applicazioni

Una raccolta di informazioni dettagliate su ogni applicazione utilizzata da un'organizzazione, compresi i costi di creazione e manutenzione dell'applicazione e il relativo valore aziendale. Queste informazioni sono fondamentali per il processo di scoperta e analisi del portfolio e aiutano a identificare e ad assegnare la priorità alle applicazioni da migrare, modernizzare e ottimizzare.

intelligenza artificiale (IA)

Il campo dell'informatica dedicato all'uso delle tecnologie informatiche per svolgere funzioni cognitive tipicamente associate agli esseri umani, come l'apprendimento, la risoluzione di problemi e il riconoscimento di schemi. Per ulteriori informazioni, consulta la sezione Che cos'è l'intelligenza artificiale?

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori informazioni su come AIOps viene utilizzata nella strategia di AWS migrazione, consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

Un algoritmo di crittografia che utilizza una coppia di chiavi, una chiave pubblica per la crittografia e una chiave privata per la decrittografia. Puoi condividere la chiave pubblica perché non viene utilizzata per la decrittografia, ma l'accesso alla chiave privata deve essere altamente limitato.

atomicità, consistenza, isolamento, durabilità (ACID)

Un insieme di proprietà del software che garantiscono la validità dei dati e l'affidabilità operativa di un database, anche in caso di errori, interruzioni di corrente o altri problemi.

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta ABAC AWS nella documentazione AWS Identity and Access Management (IAM).

fonte di dati autorevole

Una posizione in cui è archiviata la versione principale dei dati, considerata la fonte di informazioni più affidabile. È possibile copiare i dati dalla fonte di dati autorevole in altre posizioni allo scopo di elaborarli o modificarli, ad esempio anonimizzandoli, oscurandoli o pseudonimizzandoli.

Zona di disponibilità

Una posizione distinta all'interno di un edificio Regione AWS che è isolata dai guasti in altre zone di disponibilità e offre una connettività di rete economica e a bassa latenza verso altre zone di disponibilità nella stessa regione.

AWS Cloud Adoption Framework (CAF)AWS

Un framework di linee guida e best practice AWS per aiutare le organizzazioni a sviluppare un piano efficiente ed efficace per passare con successo al cloud. AWS CAF organizza le linee guida in sei aree di interesse chiamate prospettive: business, persone, governance, piattaforma, sicurezza e operazioni. Le prospettive relative ad azienda, persone e governance si concentrano sulle competenze e sui processi aziendali; le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle competenze e sui processi tecnici. Ad esempio, la prospettiva relativa alle persone si rivolge alle parti interessate che gestiscono le risorse umane (HR), le funzioni del personale e la gestione del personale. In questa prospettiva, AWS CAF fornisce linee guida per lo sviluppo delle persone, la formazione e le comunicazioni per aiutare a preparare l'organizzazione all'adozione del cloud di successo. Per ulteriori informazioni, consulta il sito web di AWS CAF e il white paper AWS CAF.

AWS Workload Qualification Framework (WQF)AWS

Uno strumento che valuta i carichi di lavoro di migrazione dei database, consiglia strategie di migrazione e fornisce stime del lavoro. AWS WQF è incluso in (). AWS Schema Conversion Tool AWS SCT Analizza gli schemi di database e gli oggetti di codice, il codice dell'applicazione, le dipendenze e le caratteristiche delle prestazioni e fornisce report di valutazione.

B

bot difettoso

Un bot che ha lo scopo di interrompere o causare danni a individui o organizzazioni.

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

Una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni nel tempo. Puoi utilizzare un grafico comportamentale con Amazon Detective per esaminare tentativi di accesso non riusciti, chiamate API sospette e azioni simili. Per ulteriori informazioni, consulta Dati in un grafico comportamentale nella documentazione di Detective.

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche endianness.

Classificazione binaria

Un processo che prevede un risultato binario (una delle due classi possibili). Ad esempio, il modello di machine learning potrebbe dover prevedere problemi come "Questa e-mail è spam o non è spam?" o "Questo prodotto è un libro o un'auto?"

filtro Bloom

Una struttura di dati probabilistica ed efficiente in termini di memoria che viene utilizzata per verificare se un elemento fa parte di un set.

distribuzioni blu/verdi

Una strategia di implementazione in cui si creano due ambienti separati ma identici. La versione corrente dell'applicazione viene eseguita in un ambiente (blu) e la nuova versione dell'applicazione nell'altro ambiente (verde). Questa strategia consente di ripristinare rapidamente il sistema con un impatto minimo.

bot

Un'applicazione software che esegue attività automatizzate su Internet e simula l'attività o l'interazione umana. Alcuni bot sono utili o utili, come i web crawler che indicizzano le informazioni su Internet. Alcuni altri bot, noti come bot dannosi, hanno lo scopo di disturbare o causare danni a individui o organizzazioni.

botnet

Reti di bot infettate da malware e controllate da un'unica parte, nota come bot herder o bot operator. Le botnet sono il meccanismo più noto per scalare i bot e il loro impatto.

ramo

Un'area contenuta di un repository di codice. Il primo ramo creato in un repository è il ramo principale. È possibile creare un nuovo ramo a partire da un ramo esistente e quindi sviluppare funzionalità o correggere bug al suo interno. Un ramo creato per sviluppare una funzionalità viene comunemente detto ramo di funzionalità. Quando la funzionalità è pronta per il rilascio, il ramo di funzionalità viene ricongiunto al ramo principale. Per ulteriori informazioni, consulta Informazioni sulle filiali (documentazione). GitHub

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, vedere l'indicatore Implementate break-glass procedures nella guida Well-Architected AWS .

strategia brownfield

L'infrastruttura esistente nell'ambiente. Quando si adotta una strategia brownfield per un'architettura di sistema, si progetta l'architettura in base ai vincoli dei sistemi e dell'infrastruttura attuali. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

cache del buffer

L'area di memoria in cui sono archiviati i dati a cui si accede con maggiore frequenza.

capacità di business

Azioni intraprese da un'azienda per generare valore (ad esempio vendite, assistenza clienti o marketing). Le architetture dei microservizi e le decisioni di sviluppo possono essere guidate dalle capacità aziendali. Per ulteriori informazioni, consulta la sezione Organizzazione in base alle funzionalità aziendali del whitepaper Esecuzione di microservizi containerizzati su AWS.

pianificazione della continuità operativa (BCP)

Un piano che affronta il potenziale impatto di un evento che comporta l'interruzione dell'attività, come una migrazione su larga scala, sulle operazioni e consente a un'azienda di riprendere rapidamente le operazioni.

C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

Il rilascio lento e incrementale di una versione agli utenti finali. Quando sei sicuro, distribuisci la nuova versione e sostituisci la versione corrente nella sua interezza.

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

Il processo di tracciamento delle modifiche a un'origine dati, ad esempio una tabella di database, e di registrazione dei metadati relativi alla modifica. È possibile utilizzare CDC per vari scopi, ad esempio il controllo o la replica delle modifiche in un sistema di destinazione per mantenere la sincronizzazione.

ingegneria del caos

Introduzione intenzionale di guasti o eventi dirompenti per testare la resilienza di un sistema. Puoi usare AWS Fault Injection Service (AWS FIS) per eseguire esperimenti che stressano i tuoi AWS carichi di lavoro e valutarne la risposta.

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

Un processo di categorizzazione che aiuta a generare previsioni. I modelli di ML per problemi di classificazione prevedono un valore discreto. I valori discreti sono sempre distinti l'uno dall'altro. Ad esempio, un modello potrebbe dover valutare se in un'immagine è presente o meno un'auto.

crittografia lato client

Crittografia dei dati a livello locale, prima che il destinatario li Servizio AWS riceva.

Centro di eccellenza cloud (CCoE)

Un team multidisciplinare che guida le iniziative di adozione del cloud in tutta l'organizzazione, tra cui lo sviluppo di best practice per il cloud, la mobilitazione delle risorse, la definizione delle tempistiche di migrazione e la guida dell'organizzazione attraverso trasformazioni su larga scala. Per ulteriori informazioni, consulta gli CCoE post sull' Cloud AWS Enterprise Strategy Blog.

cloud computing

La tecnologia cloud generalmente utilizzata per l'archiviazione remota di dati e la gestione dei dispositivi IoT. Il cloud computing è generalmente collegato alla tecnologia di edge computing.

modello operativo cloud

In un'organizzazione IT, il modello operativo utilizzato per creare, maturare e ottimizzare uno o più ambienti cloud. Per ulteriori informazioni, consulta Building your Cloud Operating Model.

fasi di adozione del cloud

Le quattro fasi che le organizzazioni in genere attraversano quando migrano verso Cloud AWS:

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per scalare l'adozione del cloud (ad esempio, creazione di una landing zone, definizione di una CCo E, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni
- Reinvenzione: ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post sul blog The Journey Toward Cloud-First & the Stages of Adoption on the Enterprise Strategy. Cloud AWS Per informazioni su come si relazionano alla strategia di AWS migrazione, consulta la guida alla preparazione alla migrazione.

CMDB

Vedi database di gestione della configurazione.

repository di codice

Una posizione in cui il codice di origine e altri asset, come documentazione, esempi e script, vengono archiviati e aggiornati attraverso processi di controllo delle versioni. Gli archivi cloud più comuni includono GitHub oBitbucket Cloud. Ogni versione del codice è denominata ramo. In una

struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD può utilizzare più repository.

cache fredda

Una cache del buffer vuota, non ben popolata o contenente dati obsoleti o irrilevanti. Ciò influisce sulle prestazioni perché l'istanza di database deve leggere dalla memoria o dal disco principale, il che richiede più tempo rispetto alla lettura dalla cache del buffer.

dati freddi

Dati a cui si accede raramente e che in genere sono storici. Quando si eseguono interrogazioni di questo tipo di dati, le interrogazioni lente sono in genere accettabili. Lo spostamento di questi dati su livelli o classi di storage meno costosi e con prestazioni inferiori può ridurre i costi.

visione artificiale (CV)

Un campo dell'intelligenza artificiale che utilizza l'apprendimento automatico per analizzare ed estrarre informazioni da formati visivi come immagini e video digitali. Ad esempio, Amazon SageMaker AI fornisce algoritmi di elaborazione delle immagini per CV.

deriva della configurazione

Per un carico di lavoro, una modifica della configurazione rispetto allo stato previsto. Potrebbe causare la non conformità del carico di lavoro e in genere è graduale e involontaria.

database di gestione della configurazione (CMDB)

Un repository che archivia e gestisce le informazioni su un database e il relativo ambiente IT, inclusi i componenti hardware e software e le relative configurazioni. In genere si utilizzano i dati di un CMDB nella fase di individuazione e analisi del portafoglio della migrazione.

Pacchetto di conformità

Una raccolta di AWS Config regole e azioni correttive che puoi assemblare per personalizzare i controlli di conformità e sicurezza. È possibile distribuire un pacchetto di conformità come singola entità in una regione Account AWS and o all'interno di un'organizzazione utilizzando un modello YAML. Per ulteriori informazioni, consulta i Conformance pack nella documentazione. AWS Config

integrazione e distribuzione continua (continuous integration and continuous delivery, CI/CD)

Il processo di automazione delle fasi di origine, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD viene comunemente descritto come una pipeline. CI/CD può aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare

la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

Un processo per identificare e classificare i dati nella rete in base alla loro criticità e sensibilità. È un componente fondamentale di qualsiasi strategia di gestione dei rischi di sicurezza informatica perché consente di determinare i controlli di protezione e conservazione appropriati per i dati. La classificazione dei dati è un componente del pilastro della sicurezza nel AWS Well-Architected Framework. Per ulteriori informazioni, consulta Classificazione dei dati.

deriva dei dati

Una variazione significativa tra i dati di produzione e i dati utilizzati per addestrare un modello di machine learning o una modifica significativa dei dati di input nel tempo. La deriva dei dati può ridurre la qualità, l'accuratezza e l'equità complessive nelle previsioni dei modelli ML.

dati in transito

Dati che si spostano attivamente attraverso la rete, ad esempio tra le risorse di rete.

rete di dati

Un framework architettonico che fornisce la proprietà distribuita e decentralizzata dei dati con gestione e governance centralizzate.

riduzione al minimo dei dati

Il principio della raccolta e del trattamento dei soli dati strettamente necessari. Praticare la riduzione al minimo dei dati in the Cloud AWS può ridurre i rischi per la privacy, i costi e l'impronta di carbonio delle analisi.

perimetro dei dati

Una serie di barriere preventive nell' AWS ambiente che aiutano a garantire che solo le identità attendibili accedano alle risorse attendibili delle reti previste. Per ulteriori informazioni, consulta Building a data perimeter on. AWS

pre-elaborazione dei dati

Trasformare i dati grezzi in un formato che possa essere facilmente analizzato dal modello di ML. La pre-elaborazione dei dati può comportare la rimozione di determinate colonne o righe e l'eliminazione di valori mancanti, incoerenti o duplicati.

provenienza dei dati

Il processo di tracciamento dell'origine e della cronologia dei dati durante il loro ciclo di vita, ad esempio il modo in cui i dati sono stati generati, trasmessi e archiviati.

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

Un sistema di gestione dei dati che supporta la business intelligence, come l'analisi. I data warehouse contengono in genere grandi quantità di dati storici e vengono generalmente utilizzati per interrogazioni e analisi.

linguaggio di definizione del database (DDL)

Istruzioni o comandi per creare o modificare la struttura di tabelle e oggetti in un database.

linguaggio di manipolazione del database (DML)

Istruzioni o comandi per modificare (inserire, aggiornare ed eliminare) informazioni in un database.

DDL

Vedi linguaggio di definizione del database.

deep ensemble

Combinare più modelli di deep learning per la previsione. È possibile utilizzare i deep ensemble per ottenere una previsione più accurata o per stimare l'incertezza nelle previsioni.

deep learning

Un sottocampo del ML che utilizza più livelli di reti neurali artificiali per identificare la mappatura tra i dati di input e le variabili target di interesse.

defense-in-depth

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza, l'integrità e la disponibilità della rete e dei dati al suo interno. Quando si adotta questa strategia AWS, si aggiungono più controlli a diversi livelli della AWS Organizations struttura per proteggere le risorse. Ad esempio, un defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la crittografia.

amministratore delegato

In AWS Organizations, un servizio compatibile può registrare un account AWS membro per amministrare gli account dell'organizzazione e gestire le autorizzazioni per quel servizio. Questo account è denominato amministratore delegato per quel servizio specifico. Per ulteriori informazioni e un elenco di servizi compatibili, consulta Servizi che funzionano con AWS Organizations nella documentazione di AWS Organizations .

implementazione

Il processo di creazione di un'applicazione, di nuove funzionalità o di correzioni di codice disponibili nell'ambiente di destinazione. L'implementazione prevede l'applicazione di modifiche in una base di codice, seguita dalla creazione e dall'esecuzione di tale base di codice negli ambienti applicativi.

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

Un controllo di sicurezza progettato per rilevare, registrare e avvisare dopo che si è verificato un evento. Questi controlli rappresentano una seconda linea di difesa e avvisano l'utente in caso di eventi di sicurezza che aggirano i controlli preventivi in vigore. Per ulteriori informazioni, consulta Controlli di rilevamento in Implementazione dei controlli di sicurezza in AWS.

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di

mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

Una rappresentazione virtuale di un sistema reale, ad esempio un edificio, una fabbrica, un'attrezzatura industriale o una linea di produzione. I gemelli digitali supportano la manutenzione predittiva, il monitoraggio remoto e l'ottimizzazione della produzione.

tabella delle dimensioni

In uno schema a stella, una tabella più piccola che contiene gli attributi dei dati quantitativi in una tabella dei fatti. Gli attributi della tabella delle dimensioni sono in genere campi di testo o numeri discreti che si comportano come testo. Questi attributi vengono comunemente utilizzati per il vincolo delle query, il filtraggio e l'etichettatura dei set di risultati.

disastro

Un evento che impedisce a un carico di lavoro o a un sistema di raggiungere gli obiettivi aziendali nella sua sede principale di implementazione. Questi eventi possono essere disastri naturali, guasti tecnici o il risultato di azioni umane, come errori di configurazione involontari o attacchi di malware.

disaster recovery (DR)

La strategia e il processo utilizzati per ridurre al minimo i tempi di inattività e la perdita di dati causati da un disastro. Per ulteriori informazioni, consulta Disaster Recovery of Workloads su AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro,Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Per informazioni su come utilizzare la progettazione basata sul dominio con il modello del fico strangolatore (Strangler Fig), consulta la sezione Modernizzazione incrementale dei servizi Web Microsoft ASP.NET (ASMX) legacy utilizzando container e il Gateway Amazon API.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, è possibile AWS CloudFormation utilizzarlo per rilevare deviazioni nelle risorse di sistema oppure AWS Control Tower per rilevare cambiamenti nella landing zone che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

La tecnologia che aumenta la potenza di calcolo per i dispositivi intelligenti all'edge di una rete IoT. Rispetto al cloud computing, l'edge computing può ridurre la latenza di comunicazione e migliorare i tempi di risposta.

scambio elettronico di dati (EDI)

Lo scambio automatizzato di documenti aziendali tra organizzazioni. Per ulteriori informazioni, vedere Cos'è lo scambio elettronico di dati.

crittografia

Un processo di elaborazione che trasforma i dati in chiaro, leggibili dall'uomo, in testo cifrato.

chiave crittografica

Una stringa crittografica di bit randomizzati generata da un algoritmo di crittografia. Le chiavi possono variare di lunghezza e ogni chiave è progettata per essere imprevedibile e univoca.

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. I sistemi big-endian memorizzano per primo il byte più importante. I sistemi little-endian memorizzano per primo il byte meno importante.

endpoint

Vedi service endpoint.

servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere autorizzazioni ad altri Account AWS o a AWS Identity and Access Management (IAM) principali. Questi account o principali possono connettersi al servizio endpoint in privato creando endpoint VPC di interfaccia. Per ulteriori informazioni, consulta Creazione di un servizio endpoint nella documentazione di Amazon Virtual Private Cloud (Amazon VPC).

pianificazione delle risorse aziendali (ERP)

Un sistema che automatizza e gestisce i processi aziendali chiave (come contabilità, MES e gestione dei progetti) per un'azienda.

crittografia envelope

Il processo di crittografia di una chiave di crittografia con un'altra chiave di crittografia. Per ulteriori informazioni, vedete Envelope encryption nella documentazione AWS Key Management Service (AWS KMS).

ambiente

Un'istanza di un'applicazione in esecuzione. Di seguito sono riportati i tipi di ambiente più comuni nel cloud computing:

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.
- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.

- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una CI/CD pipeline, l'ambiente di produzione è l'ultimo ambiente di distribuzione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione. Ad esempio, le epopee della sicurezza AWS CAF includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la guida all'implementazione del programma.

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

Il processo di analisi di un set di dati per comprenderne le caratteristiche principali. Si raccolgono o si aggregano dati e quindi si eseguono indagini iniziali per trovare modelli, rilevare anomalie e verificare ipotesi. L'EDA viene eseguita calcolando statistiche di riepilogo e creando visualizzazioni di dati.

F

tabella dei fatti

Il tavolo centrale in uno schema a stella. Memorizza dati quantitativi sulle operazioni aziendali. In genere, una tabella dei fatti contiene due tipi di colonne: quelle che contengono misure e quelle che contengono una chiave esterna per una tabella di dimensioni.

fallire velocemente

Una filosofia che utilizza test frequenti e incrementali per ridurre il ciclo di vita dello sviluppo. È una parte fondamentale di un approccio agile.

limite di isolamento dei guasti

Nel Cloud AWS, un limite come una zona di disponibilità Regione AWS, un piano di controllo o un piano dati che limita l'effetto di un errore e aiuta a migliorare la resilienza dei carichi di lavoro. Per ulteriori informazioni, consulta AWS Fault Isolation Boundaries.

ramo di funzionalità

Vedi filiale.

caratteristiche

I dati di input che usi per fare una previsione. Ad esempio, in un contesto di produzione, le caratteristiche potrebbero essere immagini acquisite periodicamente dalla linea di produzione.

importanza delle caratteristiche

Quanto è importante una caratteristica per le previsioni di un modello. Di solito viene espresso come punteggio numerico che può essere calcolato con varie tecniche, come Shapley Additive Explanations (SHAP) e gradienti integrati. Per ulteriori informazioni, consulta Interpretabilità del modello di machine learning con AWS.

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

prompt con pochi scatti

Fornire a un LLM un numero limitato di esempi che dimostrino l'attività e il risultato desiderato prima di chiedergli di eseguire un'attività simile. Questa tecnica è un'applicazione dell'apprendimento contestuale, in cui i modelli imparano da esempi (immagini) incorporati nei prompt. I prompt con pochi passaggi possono essere efficaci per attività che richiedono una formattazione, un ragionamento o una conoscenza del dominio specifici. Vedi anche zero-shot prompting.

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

L'uso di più condizioni per consentire o rifiutare una richiesta di accesso.

migrazione flash-cut

Un metodo di migrazione del database che utilizza la replica continua dei dati tramite l'acquisizione dei dati delle modifiche per migrare i dati nel più breve tempo possibile, anziché utilizzare un approccio graduale. L'obiettivo è ridurre al minimo i tempi di inattività.

FM

Vedi modello di base.

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. FMs sono in grado di svolgere un'ampia varietà di attività generali, come comprendere il linguaggio, generare testo e immagini e conversare in linguaggio naturale. Per ulteriori informazioni, consulta Cosa sono i modelli Foundation.

G

AI generativa

Un sottoinsieme di modelli di intelligenza artificiale che sono stati addestrati su grandi quantità di dati e che possono utilizzare un semplice prompt di testo per creare nuovi contenuti e artefatti, come immagini, video, testo e audio. Per ulteriori informazioni, consulta Cos'è l'IA generativa.

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

In Amazon CloudFront, un'opzione per impedire agli utenti di determinati paesi di accedere alle distribuzioni di contenuti. Puoi utilizzare un elenco consentito o un elenco di blocco per specificare i paesi approvati e vietati. Per ulteriori informazioni, consulta Limitare la distribuzione geografica dei contenuti nella CloudFront documentazione.

Flusso di lavoro di GitFlow

Un approccio in cui gli ambienti inferiori e superiori utilizzano rami diversi in un repository di codice di origine. Il flusso di lavoro Gitflow è considerato obsoleto e il flusso di lavoro basato su trunk è l'approccio moderno e preferito.

immagine dorata

Un'istantanea di un sistema o di un software che viene utilizzata come modello per distribuire nuove istanze di quel sistema o software. Ad esempio, nella produzione, un'immagine dorata può essere utilizzata per fornire software su più dispositivi e contribuire a migliorare la velocità, la scalabilità e la produttività nelle operazioni di produzione dei dispositivi.

strategia greenfield

L'assenza di infrastrutture esistenti in un nuovo ambiente. Quando si adotta una strategia greenfield per un'architettura di sistema, è possibile selezionare tutte le nuove tecnologie senza il vincolo della compatibilità con l'infrastruttura esistente, nota anche come brownfield. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

guardrail

Una regola di alto livello che aiuta a governare le risorse, le politiche e la conformità tra le unità organizzative (). OUs I guardrail preventivi applicano le policy per garantire l'allineamento agli standard di conformità. Vengono implementati utilizzando le policy di controllo dei servizi e i limiti delle autorizzazioni IAM. I guardrail di rilevamento rilevano le violazioni delle policy e i problemi di conformità e generano avvisi per porvi rimedio. Sono implementati utilizzando Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector e controlli personalizzati AWS Lambda .

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in

genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

La capacità di un carico di lavoro di funzionare in modo continuo, senza intervento, in caso di sfide o disastri. I sistemi HA sono progettati per il failover automatico, fornire costantemente prestazioni di alta qualità e gestire carichi e guasti diversi con un impatto minimo sulle prestazioni.

modernizzazione storica

Un approccio utilizzato per modernizzare e aggiornare i sistemi di tecnologia operativa (OT) per soddisfare meglio le esigenze dell'industria manifatturiera. Uno storico è un tipo di database utilizzato per raccogliere e archiviare dati da varie fonti in una fabbrica.

dati di esclusione

Una parte di dati storici etichettati che viene trattenuta da un set di dati utilizzata per addestrare un modello di apprendimento automatico. È possibile utilizzare i dati di holdout per valutare le prestazioni del modello confrontando le previsioni del modello con i dati di holdout.

migrazione di database omogenea

Migrazione del database di origine in un database di destinazione che condivide lo stesso motore di database (ad esempio, da Microsoft SQL Server ad Amazon RDS per SQL Server). La migrazione omogenea fa in genere parte di un'operazione di rehosting o ridefinizione della piattaforma. Per migrare lo schema è possibile utilizzare le utilità native del database.

dati caldi

Dati a cui si accede frequentemente, come dati in tempo reale o dati di traduzione recenti. Questi dati richiedono in genere un livello o una classe di storage ad alte prestazioni per fornire risposte rapide alle query.

hotfix

Una soluzione urgente per un problema critico in un ambiente di produzione. A causa della sua urgenza, un hotfix viene in genere creato al di fuori del tipico DevOps flusso di lavoro di rilascio.

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura

da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

Una policy associata a uno o più principi IAM che definisce le relative autorizzazioni all'interno dell' Cloud AWS ambiente.

applicazione inattiva

Un'applicazione che prevede un uso di CPU e memoria medio compreso tra il 5% e il 20% in un periodo di 90 giorni. In un progetto di migrazione, è normale ritirare queste applicazioni o mantenerle on-premise.

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

Un modello che implementa una nuova infrastruttura per i carichi di lavoro di produzione anziché aggiornare, applicare patch o modificare l'infrastruttura esistente. Le infrastrutture immutabili sono intrinsecamente più coerenti, affidabili e prevedibili delle infrastrutture mutabili. Per ulteriori informazioni, consulta la best practice Deploy using immutable infrastructure in Well-Architected AWS Framework.

VPC in ingresso (ingress)

In un'architettura AWS multi-account, un VPC che accetta, ispeziona e indirizza le connessioni di rete dall'esterno di un'applicazione. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare

solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

Industria 4.0

Un termine introdotto da Klaus Schwab nel 2016 per riferirsi alla modernizzazione dei processi di produzione attraverso progressi in termini di connettività, dati in tempo reale, automazione, analisi e AI/ML.

infrastruttura

Tutte le risorse e gli asset contenuti nell'ambiente di un'applicazione.

infrastruttura come codice (IaC)

Il processo di provisioning e gestione dell'infrastruttura di un'applicazione tramite un insieme di file di configurazione. Il processo IaC è progettato per aiutarti a centralizzare la gestione dell'infrastruttura, a standardizzare le risorse e a dimensionare rapidamente, in modo che i nuovi ambienti siano ripetibili, affidabili e coerenti.

IIoInternet delle cose industriale (T)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori informazioni, vedere Creazione di una strategia di trasformazione digitale per l'Internet of Things (IIoT) industriale.

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPCs (nello stesso o in modo diverso Regioni AWS), Internet e le reti locali. La AWS Security Reference Architecture consiglia di configurare l'account di rete con informazioni in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

Internet of Things (IoT)

La rete di oggetti fisici connessi con sensori o processori incorporati che comunicano con altri dispositivi e sistemi tramite Internet o una rete di comunicazione locale. Per ulteriori informazioni, consulta Cos'è l'IoT?

interpretabilità

Una caratteristica di un modello di machine learning che descrive il grado in cui un essere umano è in grado di comprendere in che modo le previsioni del modello dipendono dai suoi input. Per ulteriori informazioni, vedere Interpretabilità del modello di machine learning con. AWS

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

Una serie di best practice per offrire servizi IT e allinearli ai requisiti aziendali. ITIL fornisce le basi per ITSM.

gestione dei servizi IT (ITSM)

Attività associate alla progettazione, implementazione, gestione e supporto dei servizi IT per un'organizzazione. Per informazioni sull'integrazione delle operazioni cloud con gli strumenti ITSM, consulta la guida all'integrazione delle operazioni.

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

Un'implementazione del controllo di accesso obbligatorio (MAC) in cui agli utenti e ai dati stessi viene assegnato esplicitamente un valore di etichetta di sicurezza. L'intersezione tra l'etichetta di sicurezza utente e l'etichetta di sicurezza dei dati determina quali righe e colonne possono essere visualizzate dall'utente.

zona di destinazione

Una landing zone è un AWS ambiente multi-account ben progettato, scalabile e sicuro. Questo è un punto di partenza dal quale le organizzazioni possono avviare e distribuire rapidamente carichi di lavoro e applicazioni con fiducia nel loro ambiente di sicurezza e infrastruttura. Per ulteriori

informazioni sulle zone di destinazione, consulta la sezione Configurazione di un ambiente AWS multi-account sicuro e scalabile.

modello linguistico di grandi dimensioni (LLM)

Un modello di intelligenza artificiale di deep learning preaddestrato su una grande quantità di dati. Un LLM può svolgere più attività, come rispondere a domande, riepilogare documenti, tradurre testo in altre lingue e completare frasi. Per ulteriori informazioni, consulta Cosa sono. LLMs

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

La best practice di sicurezza per la concessione delle autorizzazioni minime richieste per eseguire un'attività. Per ulteriori informazioni, consulta Applicazione delle autorizzazioni del privilegio minimo nella documentazione di IAM.

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche endianità.

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati

dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

malware

Software progettato per compromettere la sicurezza o la privacy del computer. Il malware potrebbe interrompere i sistemi informatici, divulgare informazioni sensibili o ottenere accessi non autorizzati. Esempi di malware includono virus, worm, ransomware, trojan horse, spyware e keylogger.

servizi gestiti

Servizi AWS per cui AWS gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e si accede agli endpoint per archiviare e recuperare i dati. Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e Amazon DynamoDB sono esempi di servizi gestiti. Questi sono noti anche come servizi astratti.

sistema di esecuzione della produzione (MES)

Un sistema software per tracciare, monitorare, documentare e controllare i processi di produzione che convertono le materie prime in prodotti finiti in officina.

MAP

Vedi Migration Acceleration Program.

meccanismo

Un processo completo in cui si crea uno strumento, si promuove l'adozione dello strumento e quindi si esaminano i risultati per apportare le modifiche. Un meccanismo è un ciclo che si rafforza e si migliora man mano che funziona. Per ulteriori informazioni, consulta Creazione di meccanismi nel AWS Well-Architected Framework.

account membro

Tutti gli account Account AWS diversi dall'account di gestione che fanno parte di un'organizzazione in. AWS Organizations Un account può essere membro di una sola organizzazione alla volta.

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

Un protocollo di comunicazione machine-to-machine (M2M) leggero, basato sul modello di pubblicazione/sottoscrizione, per dispositivi IoT con risorse limitate.

microservizio

Un servizio piccolo e indipendente che comunica tramite canali ben definiti ed è in genere di proprietà di piccoli team autonomi. APIs Ad esempio, un sistema assicurativo potrebbe includere microservizi che si riferiscono a funzionalità aziendali, come vendite o marketing, o sottodomini, come acquisti, reclami o analisi. I vantaggi dei microservizi includono agilità, dimensionamento flessibile, facilità di implementazione, codice riutilizzabile e resilienza. Per ulteriori informazioni, consulta Integrazione dei microservizi utilizzando servizi serverless. AWS

architettura di microservizi

Un approccio alla creazione di un'applicazione con componenti indipendenti che eseguono ogni processo applicativo come microservizio. Questi microservizi comunicano attraverso un'interfaccia ben definita utilizzando sistemi leggeri. APIs Ogni microservizio in questa architettura può essere aggiornato, distribuito e dimensionato per soddisfare la richiesta di funzioni specifiche di un'applicazione. Per ulteriori informazioni, vedere Implementazione dei microservizi su. AWS

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

Il processo di trasferimento della maggior parte del portfolio di applicazioni sul cloud avviene a ondate, con più applicazioni trasferite a una velocità maggiore in ogni ondata. Questa fase utilizza le migliori pratiche e le lezioni apprese nelle fasi precedenti per implementare una fabbrica di migrazione di team, strumenti e processi per semplificare la migrazione dei carichi di lavoro attraverso l'automazione e la distribuzione agile. Questa è la terza fase della strategia di migrazione AWS.

fabbrica di migrazione

Team interfunzionali che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory in genere includono addetti alle operazioni,

analisti e proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano nell'ambito degli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la discussione sulle fabbriche di migrazione e la Guida alla fabbrica di migrazione al cloud in questo set di contenuti.

metadati di migrazione

Le informazioni sull'applicazione e sul server necessarie per completare la migrazione. Ogni modello di migrazione richiede un set diverso di metadati di migrazione. Esempi di metadati di migrazione includono la sottorete, il gruppo di sicurezza e l'account di destinazione. AWS

modello di migrazione

Un'attività di migrazione ripetibile che descrive in dettaglio la strategia di migrazione, la destinazione della migrazione e l'applicazione o il servizio di migrazione utilizzati. Esempio: riorganizza la migrazione su Amazon EC2 con AWS Application Migration Service.

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione a. Cloud AWS MPA offre una valutazione dettagliata del portfolio (dimensionamento corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). Lo strumento MPA (richiede l'accesso) è disponibile gratuitamente per tutti i AWS consulenti e i consulenti dei partner APN.

valutazione della preparazione alla migrazione (MRA)

Il processo di acquisizione di informazioni sullo stato di preparazione al cloud di un'organizzazione, l'identificazione dei punti di forza e di debolezza e la creazione di un piano d'azione per colmare le lacune identificate, utilizzando il CAF. AWS Per ulteriori informazioni, consulta la guida di preparazione alla migrazione. MRA è la prima fase della strategia di migrazione AWS.

strategia di migrazione

L'approccio utilizzato per migrare un carico di lavoro verso. Cloud AWS Per ulteriori informazioni, consulta la voce 7 R in questo glossario e consulta Mobilita la tua organizzazione per accelerare le migrazioni su larga scala.

ML

Vedi machine learning.

modernizzazione

Trasformazione di un'applicazione obsoleta (legacy o monolitica) e della relativa infrastruttura in un sistema agile, elastico e altamente disponibile nel cloud per ridurre i costi, aumentare l'efficienza e sfruttare le innovazioni. Per ulteriori informazioni, vedere Strategia per la modernizzazione delle applicazioni in. Cloud AWS

valutazione della preparazione alla modernizzazione

Una valutazione che aiuta a determinare la preparazione alla modernizzazione delle applicazioni di un'organizzazione, identifica vantaggi, rischi e dipendenze e determina in che misura l'organizzazione può supportare lo stato futuro di tali applicazioni. Il risultato della valutazione è uno schema dell'architettura di destinazione, una tabella di marcia che descrive in dettaglio le fasi di sviluppo e le tappe fondamentali del processo di modernizzazione e un piano d'azione per colmare le lacune identificate. Per ulteriori informazioni, vedere Valutazione della preparazione alla modernizzazione per le applicazioni in. Cloud AWS

applicazioni monolitiche (monoliti)

Applicazioni eseguite come un unico servizio con processi strettamente collegati. Le applicazioni monolitiche presentano diversi inconvenienti. Se una funzionalità dell'applicazione registra un picco di domanda, l'intera architettura deve essere dimensionata. L'aggiunta o il miglioramento delle funzionalità di un'applicazione monolitica diventa inoltre più complessa man mano che la base di codice cresce. Per risolvere questi problemi, puoi utilizzare un'architettura di microservizi. Per ulteriori informazioni, consulta la sezione Scomposizione dei monoliti in microservizi.

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

Un processo che aiuta a generare previsioni per più classi (prevedendo uno o più di due risultati). Ad esempio, un modello di machine learning potrebbe chiedere "Questo prodotto è un libro, un'auto o un telefono?" oppure "Quale categoria di prodotti è più interessante per questo cliente?"

infrastruttura mutabile

Un modello che aggiorna e modifica l'infrastruttura esistente per i carichi di lavoro di produzione. Per migliorare la coerenza, l'affidabilità e la prevedibilità, il AWS Well-Architected Framework consiglia l'uso di un'infrastruttura immutabile come best practice.

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

Un metodo di migrazione in cui il carico di lavoro di origine viene eliminato durante il processo di migrazione. Questo metodo prevede tempi di inattività prolungati e viene in genere utilizzato per carichi di lavoro piccoli e non critici.

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

Un metodo di migrazione in cui il carico di lavoro di origine viene copiato sul sistema di destinazione senza essere messo offline. Le applicazioni connesse al carico di lavoro possono continuare a funzionare durante la migrazione. Questo metodo comporta tempi di inattività pari a zero o comunque minimi e viene in genere utilizzato per carichi di lavoro di produzione critici.

OPC-UA

Vedi Open Process Communications - Unified Architecture.

Comunicazioni a processo aperto - Architettura unificata (OPC-UA)

Un protocollo di comunicazione machine-to-machine (M2M) per l'automazione industriale. OPC-UA fornisce uno standard di interoperabilità con schemi di crittografia, autenticazione e autorizzazione dei dati.

accordo a livello operativo (OLA)

Un accordo che chiarisce quali sono gli impegni reciproci tra i gruppi IT funzionali, a supporto di un accordo sul livello di servizio (SLA).

revisione della prontezza operativa (ORR)

Un elenco di domande e best practice associate che aiutano a comprendere, valutare, prevenire o ridurre la portata degli incidenti e dei possibili guasti. Per ulteriori informazioni, vedere Operational Readiness Reviews (ORR) nel Well-Architected AWS Framework.

tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare le operazioni, le apparecchiature e le infrastrutture industriali. Nella produzione, l'integrazione di sistemi OT e di tecnologia dell'informazione (IT) è un obiettivo chiave per le trasformazioni dell'Industria 4.0.

integrazione delle operazioni (OI)

Il processo di modernizzazione delle operazioni nel cloud, che prevede la pianificazione, l'automazione e l'integrazione della disponibilità. Per ulteriori informazioni, consulta la guida all'integrazione delle operazioni.

trail organizzativo

Un percorso creato da noi AWS CloudTrail che registra tutti gli eventi di un'organizzazione per tutti Account AWS . AWS Organizations Questo percorso viene creato in ogni Account AWS che fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione nella CloudTrail documentazione.

gestione del cambiamento organizzativo (OCM)

Un framework per la gestione di trasformazioni aziendali importanti e che comportano l'interruzione delle attività dal punto di vista delle persone, della cultura e della leadership. OCM aiuta le organizzazioni a prepararsi e passare a nuovi sistemi e strategie accelerando l'adozione del cambiamento, affrontando i problemi di transizione e promuovendo cambiamenti culturali e organizzativi. Nella strategia di AWS migrazione, questo framework si chiama accelerazione delle

persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la Guida OCM.

controllo dell'accesso all'origine (OAC)

In CloudFront, un'opzione avanzata per limitare l'accesso per proteggere i contenuti di Amazon Simple Storage Service (Amazon S3). OAC supporta tutti i bucket S3 in generale Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche e dirette al bucket S3. `PUT` `DELETE`

identità di accesso origine (OAI)

Nel CloudFront, un'opzione per limitare l'accesso per proteggere i tuoi contenuti Amazon S3. Quando usi OAI, CloudFront crea un principale con cui Amazon S3 può autenticarsi. I principali autenticati possono accedere ai contenuti in un bucket S3 solo tramite una distribuzione specifica. CloudFront Vedi anche OAC, che fornisce un controllo degli accessi più granulare e avanzato.

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

In un'architettura AWS multi-account, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

P

limite delle autorizzazioni

Una policy di gestione IAM collegata ai principali IAM per impostare le autorizzazioni massime che l'utente o il ruolo possono avere. Per ulteriori informazioni, consulta Limiti delle autorizzazioni nella documentazione di IAM.

informazioni di identificazione personale (PII)

Informazioni che, se visualizzate direttamente o abbinate ad altri dati correlati, possono essere utilizzate per dedurre ragionevolmente l'identità di un individuo. Esempi di informazioni personali includono nomi, indirizzi e informazioni di contatto.

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

Una serie di passaggi predefiniti che raccolgono il lavoro associato alle migrazioni, come l'erogazione delle funzioni operative principali nel cloud. Un playbook può assumere la forma di script, runbook automatici o un riepilogo dei processi o dei passaggi necessari per gestire un ambiente modernizzato.

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

Un oggetto in grado di definire le autorizzazioni (vedi politica basata sull'identità), specificare le condizioni di accesso (vedi politicabasata sulle risorse) o definire le autorizzazioni massime per tutti gli account di un'organizzazione in (vedi politica di controllo dei servizi). AWS Organizations

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze. Per ulteriori informazioni, consulta la sezione Abilitazione della persistenza dei dati nei microservizi.

valutazione del portfolio

Un processo di scoperta, analisi e definizione delle priorità del portfolio di applicazioni per pianificare la migrazione. Per ulteriori informazioni, consulta la pagina Valutazione della preparazione alla migrazione.

predicate

Una condizione di interrogazione che restituisce o, in genere, si trova in una clausola`WHERE`. `true` `false`

predicato pushdown

Una tecnica di ottimizzazione delle query del database che filtra i dati della query prima del trasferimento. Ciò riduce la quantità di dati che devono essere recuperati ed elaborati dal database relazionale e migliora le prestazioni delle query.

controllo preventivo

Un controllo di sicurezza progettato per impedire il verificarsi di un evento. Questi controlli sono la prima linea di difesa per impedire accessi non autorizzati o modifiche indesiderate alla rete. Per ulteriori informazioni, consulta Controlli preventivi in Implementazione dei controlli di sicurezza in AWS.

principale

Un'entità in AWS grado di eseguire azioni e accedere alle risorse. Questa entità è in genere un utente root per un Account AWS ruolo IAM o un utente. Per ulteriori informazioni, consulta Principali in Termini e concetti dei ruoli nella documentazione di IAM.

privacy fin dalla progettazione

Un approccio di ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

zone ospitate private

Un contenitore che contiene informazioni su come desideri che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più. VPCs Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private nella documentazione di Route 53.

controllo proattivo

Un controllo di sicurezza progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al controllo, non viene fornita. Per ulteriori informazioni, consulta la guida di riferimento sui controlli nella AWS Control Tower documentazione e consulta Controlli proattivi in Implementazione dei controlli di sicurezza su. AWS

gestione del ciclo di vita del prodotto (PLM)

La gestione dei dati e dei processi di un prodotto durante l'intero ciclo di vita, dalla progettazione, sviluppo e lancio, attraverso la crescita e la maturità, fino al declino e alla rimozione.

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

Nella produzione, un computer altamente affidabile e adattabile che monitora le macchine e automatizza i processi di produzione.

concatenamento rapido

Utilizzo dell'output di un prompt LLM come input per il prompt successivo per generare risposte migliori. Questa tecnica viene utilizzata per suddividere un'attività complessa in sottoattività o per perfezionare o espandere iterativamente una risposta preliminare. Aiuta a migliorare l'accuratezza e la pertinenza delle risposte di un modello e consente risultati più granulari e personalizzati.

pseudonimizzazione

Il processo di sostituzione degli identificatori personali in un set di dati con valori segnaposto. La pseudonimizzazione può aiutare a proteggere la privacy personale. I dati pseudonimizzati sono ancora considerati dati personali.

publish/subscribe (pub/sub)

Un modello che consente comunicazioni asincrone tra microservizi per migliorare la scalabilità e la reattività. Ad esempio, in un MES basato su microservizi, un microservizio può pubblicare messaggi di eventi su un canale a cui altri microservizi possono abbonarsi. Il sistema può aggiungere nuovi microservizi senza modificare il servizio di pubblicazione.

Q

Piano di query

Una serie di passaggi, come le istruzioni, utilizzati per accedere ai dati in un sistema di database relazionale SQL.

regressione del piano di query

Quando un ottimizzatore del servizio di database sceglie un piano non ottimale rispetto a prima di una determinata modifica all'ambiente di database. Questo può essere causato da modifiche a statistiche, vincoli, impostazioni dell'ambiente, associazioni dei parametri di query e aggiornamenti al motore di database.

R

Matrice RACI

Vedi responsabile, responsabile, consultato, informato (RACI).

STRACCIO

Vedi Retrieval Augmented Generation.

ransomware

Un software dannoso progettato per bloccare l'accesso a un sistema informatico o ai dati fino a quando non viene effettuato un pagamento.

Matrice RASCI

Vedi responsabile, responsabile, consultato, informato (RACI).

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

Una copia di un database utilizzata per scopi di sola lettura. È possibile indirizzare le query alla replica di lettura per ridurre il carico sul database principale.

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Questo determina ciò che si considera una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

obiettivo del tempo di ripristino (RTO)

Il ritardo massimo accettabile tra l'interruzione del servizio e il ripristino del servizio.

rifattorizzare

Vedi 7 R.

Regione

Una raccolta di AWS risorse in un'area geografica. Ciascuna Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta Specificare cosa può usare Regioni AWS il tuo account.

regressione

Una tecnica di ML che prevede un valore numerico. Ad esempio, per risolvere il problema "A che prezzo verrà venduta questa casa?" un modello di ML potrebbe utilizzare un modello di regressione lineare per prevedere il prezzo di vendita di una casa sulla base di dati noti sulla casa (ad esempio, la metratura).

riospitare

Vedi 7 R.

rilascio

In un processo di implementazione, l'atto di promuovere modifiche a un ambiente di produzione.

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

La capacità di un'applicazione di resistere o ripristinare le interruzioni. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

Una policy associata a una risorsa, ad esempio un bucket Amazon S3, un endpoint o una chiave di crittografia. Questo tipo di policy specifica a quali principali è consentito l'accesso, le azioni supportate e qualsiasi altra condizione che deve essere soddisfatta.

matrice di assegnazione di responsabilità (RACI)

Una matrice che definisce i ruoli e le responsabilità di tutte le parti coinvolte nelle attività di migrazione e nelle operazioni cloud. Il nome della matrice deriva dai tipi di responsabilità definiti nella matrice: responsabile (R), responsabile (A), consultato (C) e informato (I). Il tipo di supporto (S) è facoltativo. Se includi il supporto, la matrice viene chiamata matrice RASCI e, se la escludi, viene chiamata matrice RACI.

controllo reattivo

Un controllo di sicurezza progettato per favorire la correzione di eventi avversi o deviazioni dalla baseline di sicurezza. Per ulteriori informazioni, consulta Controlli reattivi in Implementazione dei controlli di sicurezza in AWS.

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

Una tecnologia di intelligenza artificiale generativa in cui un LLM fa riferimento a una fonte di dati autorevole esterna alle sue fonti di dati di formazione prima di generare una risposta. Ad esempio, un modello RAG potrebbe eseguire una ricerca semantica nella knowledge base o nei dati personalizzati di un'organizzazione. Per ulteriori informazioni, consulta Cos'è il RAG.

rotazione

Processo di aggiornamento periodico di un segreto per rendere più difficile l'accesso alle credenziali da parte di un utente malintenzionato.

controllo dell'accesso a righe e colonne (RCAC)

L'uso di espressioni SQL di base e flessibili con regole di accesso definite. RCAC è costituito da autorizzazioni di riga e maschere di colonna.

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

Un insieme di procedure manuali o automatizzate necessarie per eseguire un'attività specifica. In genere sono progettati per semplificare operazioni o procedure ripetitive con tassi di errore elevati.

S

SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità abilita il single sign-on (SSO) federato, in modo che gli utenti possano accedere AWS Management Console o chiamare le operazioni AWS API senza che tu debba creare un utente in IAM per tutti i membri dell'organizzazione. Per ulteriori informazioni sulla federazione basata su SAML 2.0, consulta Informazioni sulla federazione basata su SAML 2.0 nella documentazione di IAM.

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

In AWS Secrets Manager, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta Cosa c'è in un segreto di Secrets Manager? nella documentazione di Secrets Manager.

sicurezza fin dalla progettazione

Un approccio di ingegneria dei sistemi che tiene conto della sicurezza durante l'intero processo di sviluppo.

controllo di sicurezza

Un guardrail tecnico o amministrativo che impedisce, rileva o riduce la capacità di un autore di minacce di sfruttare una vulnerabilità di sicurezza. Esistono quattro tipi principali di controlli di sicurezza: preventivi, investigativi, reattivi e proattivi.

rafforzamento della sicurezza

Il processo di riduzione della superficie di attacco per renderla più resistente agli attacchi. Può includere azioni come la rimozione di risorse che non sono più necessarie, l'implementazione di best practice di sicurezza che prevedono la concessione del privilegio minimo o la disattivazione di funzionalità non necessarie nei file di configurazione.

sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM)

Strumenti e servizi che combinano sistemi di gestione delle informazioni di sicurezza (SIM) e sistemi di gestione degli eventi di sicurezza (SEM). Un sistema SIEM raccoglie, monitora e analizza i dati da server, reti, dispositivi e altre fonti per rilevare minacce e violazioni della sicurezza e generare avvisi.

automazione della risposta alla sicurezza

Un'azione predefinita e programmata progettata per rispondere o porre rimedio automaticamente a un evento di sicurezza. Queste automazioni fungono da controlli di sicurezza investigativi o reattivi che aiutano a implementare le migliori pratiche di sicurezza. AWS Esempi di azioni di risposta automatizzate includono la modifica di un gruppo di sicurezza VPC, l'applicazione di patch a un'istanza EC2 Amazon o la rotazione delle credenziali.

Crittografia lato server

Crittografia dei dati a destinazione, da parte di chi li riceve. Servizio AWS

Policy di controllo dei servizi (SCP)

Una politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

L'URL del punto di ingresso per un Servizio AWS. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta Endpoint del Servizio AWS nei Riferimenti generali di AWS.

accordo sul livello di servizio (SLA)

Un accordo che chiarisce ciò che un team IT promette di offrire ai propri clienti, ad esempio l'operatività e le prestazioni del servizio.

indicatore del livello di servizio (SLI)

Misurazione di un aspetto prestazionale di un servizio, ad esempio il tasso di errore, la disponibilità o la velocità effettiva.

obiettivo a livello di servizio (SLO)

Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.

Modello di responsabilità condivisa

Un modello che descrive la responsabilità condivisa AWS per la sicurezza e la conformità del cloud. AWS è responsabile della sicurezza del cloud, mentre tu sei responsabile della sicurezza nel cloud. Per ulteriori informazioni, consulta Modello di responsabilità condivisa.

SIEM

Vedi il sistema di gestione delle informazioni e degli eventi sulla sicurezza.

punto di errore singolo (SPOF)

Un guasto in un singolo componente critico di un'applicazione che può disturbare il sistema.

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

Un modello per dimensionare e accelerare i progetti di modernizzazione. Man mano che vengono definite nuove funzionalità e versioni dei prodotti, il team principale si divide per creare nuovi team di prodotto. Questo aiuta a dimensionare le capacità e i servizi dell'organizzazione, migliora la produttività degli sviluppatori e supporta una rapida innovazione. Per ulteriori informazioni, vedere Approccio graduale alla modernizzazione delle applicazioni in. Cloud AWS

SPOF

Vedi punto di errore singolo.

schema a stella

Una struttura organizzativa di database che utilizza un'unica tabella dei fatti di grandi dimensioni per archiviare i dati transazionali o misurati e utilizza una o più tabelle dimensionali più piccole per memorizzare gli attributi dei dati. Questa struttura è progettata per l'uso in un data warehouse o per scopi di business intelligence.

modello del fico strangolatore

Un approccio alla modernizzazione dei sistemi monolitici mediante la riscrittura e la sostituzione incrementali delle funzionalità del sistema fino alla disattivazione del sistema legacy. Questo modello utilizza l'analogia di una pianta di fico che cresce fino a diventare un albero robusto e alla fine annienta e sostituisce il suo ospite. Il modello è stato introdotto da Martin Fowler come metodo per gestire il rischio durante la riscrittura di sistemi monolitici. Per un esempio di come applicare questo modello, consulta Modernizzazione incrementale dei servizi Web legacy di Microsoft ASP.NET (ASMX) mediante container e Gateway Amazon API.

sottorete

Un intervallo di indirizzi IP nel VPC. Una sottorete deve risiedere in una singola zona di disponibilità.

controllo di supervisione e acquisizione dati (SCADA)

Nella produzione, un sistema che utilizza hardware e software per monitorare gli asset fisici e le operazioni di produzione.

crittografia simmetrica

Un algoritmo di crittografia che utilizza la stessa chiave per crittografare e decrittografare i dati.

test sintetici

Test di un sistema in modo da simulare le interazioni degli utenti per rilevare potenziali problemi o monitorare le prestazioni. Puoi usare Amazon CloudWatch Synthetics per creare questi test.

prompt di sistema

Una tecnica per fornire contesto, istruzioni o linee guida a un LLM per indirizzarne il comportamento. I prompt di sistema aiutano a impostare il contesto e stabilire regole per le interazioni con gli utenti.

T

tags

Coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS I tag possono aiutarti a gestire, identificare, organizzare, cercare e filtrare le risorse. Per ulteriori informazioni, consulta l'articolo relativo all'assegnazione di tag alle risorse AWS.

variabile di destinazione

Il valore che stai cercando di prevedere nel machine learning supervisionato. Questo è indicato anche come variabile di risultato. Ad esempio, in un ambiente di produzione la variabile di destinazione potrebbe essere un difetto del prodotto.

elenco di attività

Uno strumento che viene utilizzato per tenere traccia dei progressi tramite un runbook. Un elenco di attività contiene una panoramica del runbook e un elenco di attività generali da completare. Per ogni attività generale, include la quantità stimata di tempo richiesta, il proprietario e lo stato di avanzamento.

Ambiente di test

Vedi ambiente.

training

Fornire dati da cui trarre ispirazione dal modello di machine learning. I dati di training devono contenere la risposta corretta. L'algoritmo di apprendimento trova nei dati di addestramento i pattern che mappano gli attributi dei dati di input al target (la risposta che si desidera prevedere). Produce un modello di ML che acquisisce questi modelli. Puoi quindi utilizzare il modello di ML per creare previsioni su nuovi dati di cui non si conosce il target.

Transit Gateway

Un hub di transito di rete che puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. Per ulteriori informazioni, consulta Cos'è un gateway di transito nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

Un approccio in cui gli sviluppatori creano e testano le funzionalità localmente in un ramo di funzionalità e quindi uniscono tali modifiche al ramo principale. Il ramo principale viene quindi integrato negli ambienti di sviluppo, preproduzione e produzione, in sequenza.

Accesso attendibile

Concessione delle autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione AWS Organizations e nei suoi account per conto dell'utente. Il servizio attendibile crea un ruolo collegato al servizio in ogni account, quando tale ruolo è necessario, per eseguire attività di gestione per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo AWS Organizations con altri AWS servizi nella AWS Organizations documentazione.

regolazione

Modificare alcuni aspetti del processo di training per migliorare la precisione del modello di ML. Ad esempio, puoi addestrare il modello di ML generando un set di etichette, aggiungendo etichette e quindi ripetendo questi passaggi più volte con impostazioni diverse per ottimizzare il modello.

team da due pizze

Una piccola DevOps squadra che puoi sfamare con due pizze. Un team composto da due persone garantisce la migliore opportunità possibile di collaborazione nello sviluppo del software.

U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza: l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati. Per ulteriori informazioni, consulta la guida Quantificazione dell'incertezza nei sistemi di deep learning.

compiti indifferenziati

Conosciuto anche come sollevamento di carichi pesanti, è un lavoro necessario per creare e far funzionare un'applicazione, ma che non apporta valore diretto all'utente finale né offre vantaggi competitivi. Esempi di attività indifferenziate includono l'approvvigionamento, la manutenzione e la pianificazione della capacità.

ambienti superiori

Vedi ambiente.

V

vacuum

Un'operazione di manutenzione del database che prevede la pulizia dopo aggiornamenti incrementali per recuperare lo spazio di archiviazione e migliorare le prestazioni.

controllo delle versioni

Processi e strumenti che tengono traccia delle modifiche, ad esempio le modifiche al codice di origine in un repository.

Peering di VPC

Una connessione tra due VPCs che consente di indirizzare il traffico utilizzando indirizzi IP privati. Per ulteriori informazioni, consulta Che cos'è il peering VPC? nella documentazione di Amazon VPC.

vulnerabilità

Un difetto software o hardware che compromette la sicurezza del sistema.

W

cache calda

Una cache del buffer che contiene dati correnti e pertinenti a cui si accede frequentemente. L'istanza di database può leggere dalla cache del buffer, il che richiede meno tempo rispetto alla lettura dalla memoria dal disco principale.

dati caldi

Dati a cui si accede raramente. Quando si eseguono interrogazioni di questo tipo di dati, in genere sono accettabili query moderatamente lente.

funzione finestra

Una funzione SQL che esegue un calcolo su un gruppo di righe che si riferiscono in qualche modo al record corrente. Le funzioni della finestra sono utili per l'elaborazione di attività, come il calcolo di una media mobile o l'accesso al valore delle righe in base alla posizione relativa della riga corrente.

Carico di lavoro

Una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end.

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio, il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni, della pianificazione delle ondate e della raccolta dei metadati di migrazione. Il flusso di lavoro del portfolio fornisce queste risorse al flusso di lavoro di migrazione, che quindi migra i server e le applicazioni.

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

Un modello di storage che scrive i dati una sola volta e ne impedisce l'eliminazione o la modifica. Gli utenti autorizzati possono leggere i dati tutte le volte che è necessario, ma non possono modificarli. Questa infrastruttura di archiviazione dei dati è considerata immutabile.

Z

exploit zero-day

Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.

vulnerabilità zero-day

Un difetto o una vulnerabilità assoluta in un sistema di produzione. Gli autori delle minacce possono utilizzare questo tipo di vulnerabilità per attaccare il sistema. Gli sviluppatori vengono spesso a conoscenza della vulnerabilità causata dall'attacco.

prompt zero-shot

Fornire a un LLM le istruzioni per eseguire un'attività, ma non fornire esempi (immagini) che possano aiutarla. Il LLM deve utilizzare le sue conoscenze pre-addestrate per gestire l'attività. L'efficacia del prompt zero-shot dipende dalla complessità dell'attività e dalla qualità del prompt. Vedi anche few-shot prompting.

applicazione zombie

Un'applicazione che prevede un utilizzo CPU e memoria inferiore al 5%. In un progetto di migrazione, è normale ritirare queste applicazioni.

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.