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

AWS Linee guida prescrittive

AWS Linee guida prescrittive: 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 un piano AWS Unified Operations.

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 Direct Connect collegamento dal data center al 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 EC2 nella zona locale. 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 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}]
```

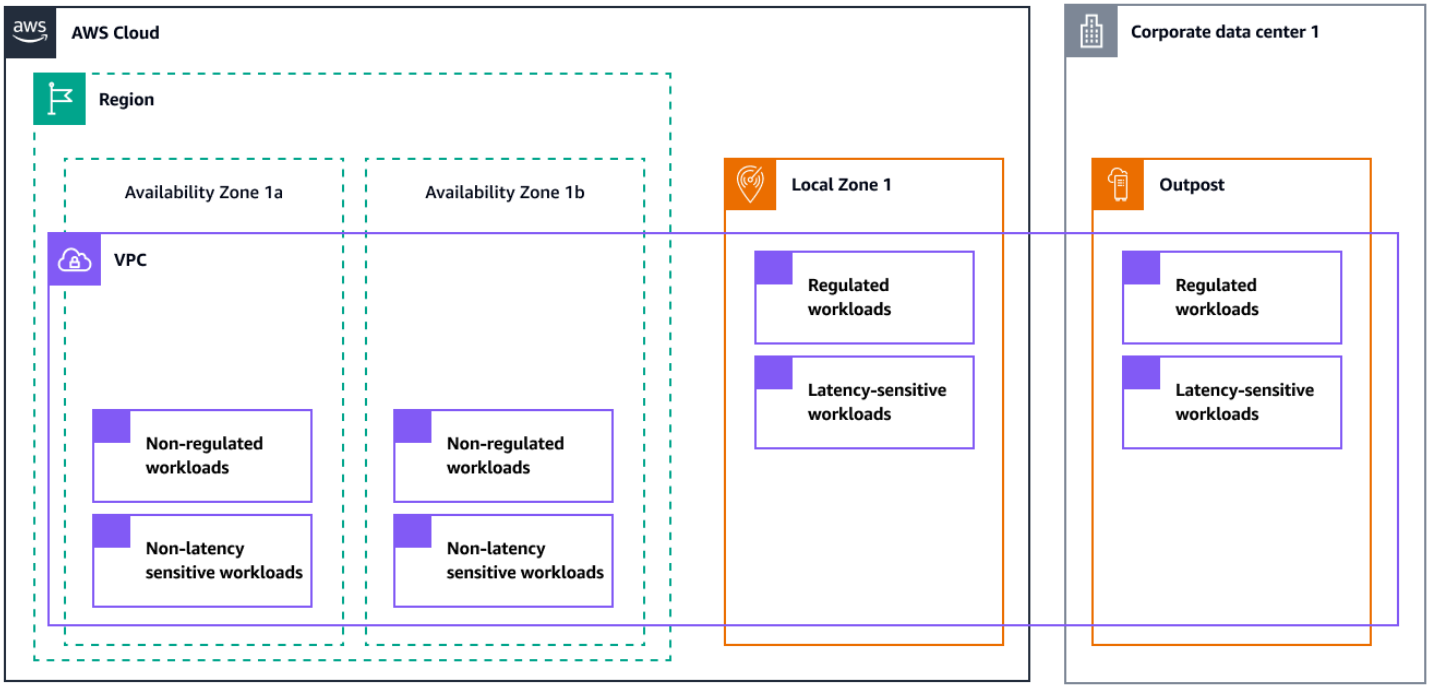
  Per ulteriori informazioni, consulta la documentazione relativa ad AWS Outposts.

- 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.

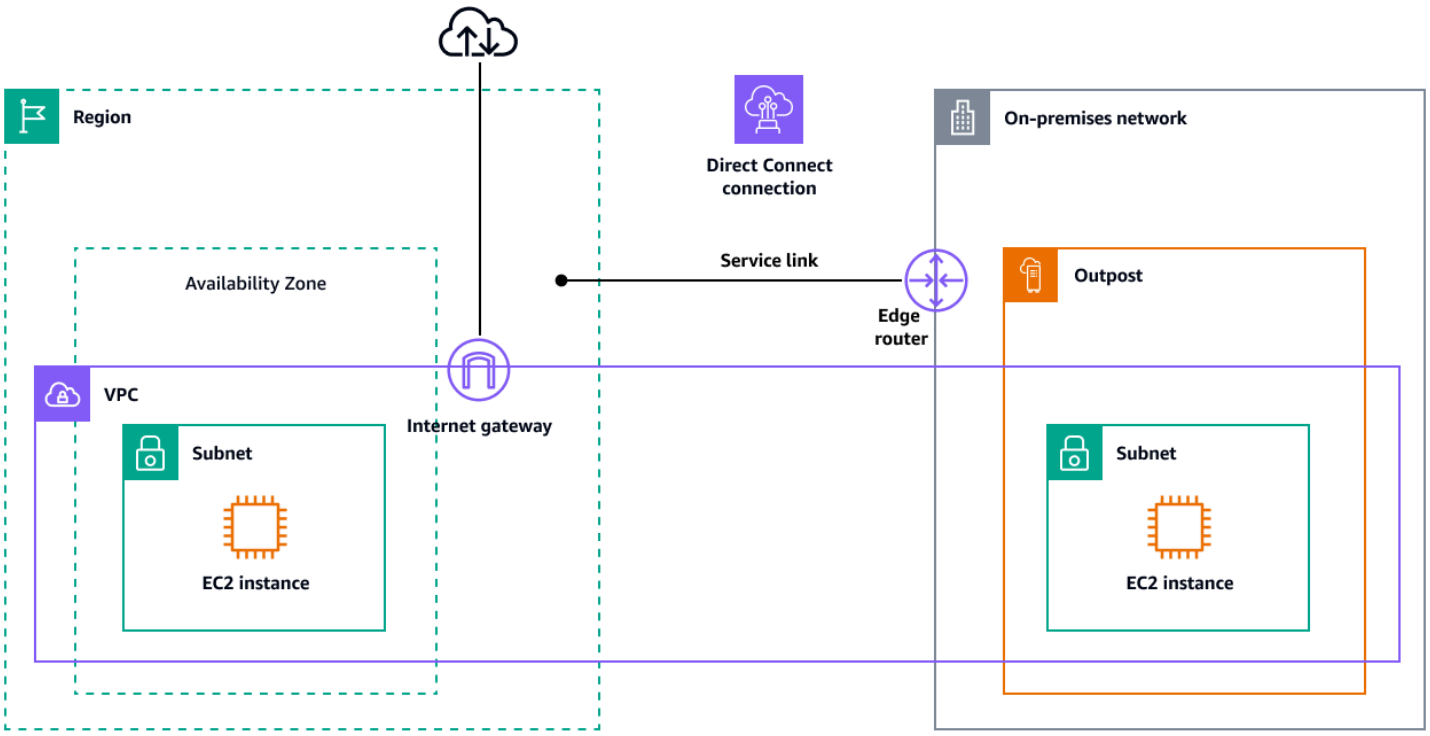


Traffico da periferia a regione

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 Direct Connect pubblica (VIF pubblica) oppure tramite un'interfaccia virtuale 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 istanze Amazon EC2, collegare volumi Amazon EBS e accedere Servizi AWS ad esempio ad Amazon EKS, Amazon EMR e parametri Amazon. CloudWatch La rete deve supportare un'unità di trasmissione massima (MTU) 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 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 collegamento di servizio 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 le istanze EC2 in AWS Outposts e le istanze EC2 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. 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 le stesse API e gli stessi set di strumenti. Regione AWS

La tabella seguente mostra le opzioni di connessione e le MTU associate.

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

Da	Per	MTU
Amazon EC2 nelle zone Local Zones	Amazon EC2 nelle zone 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.

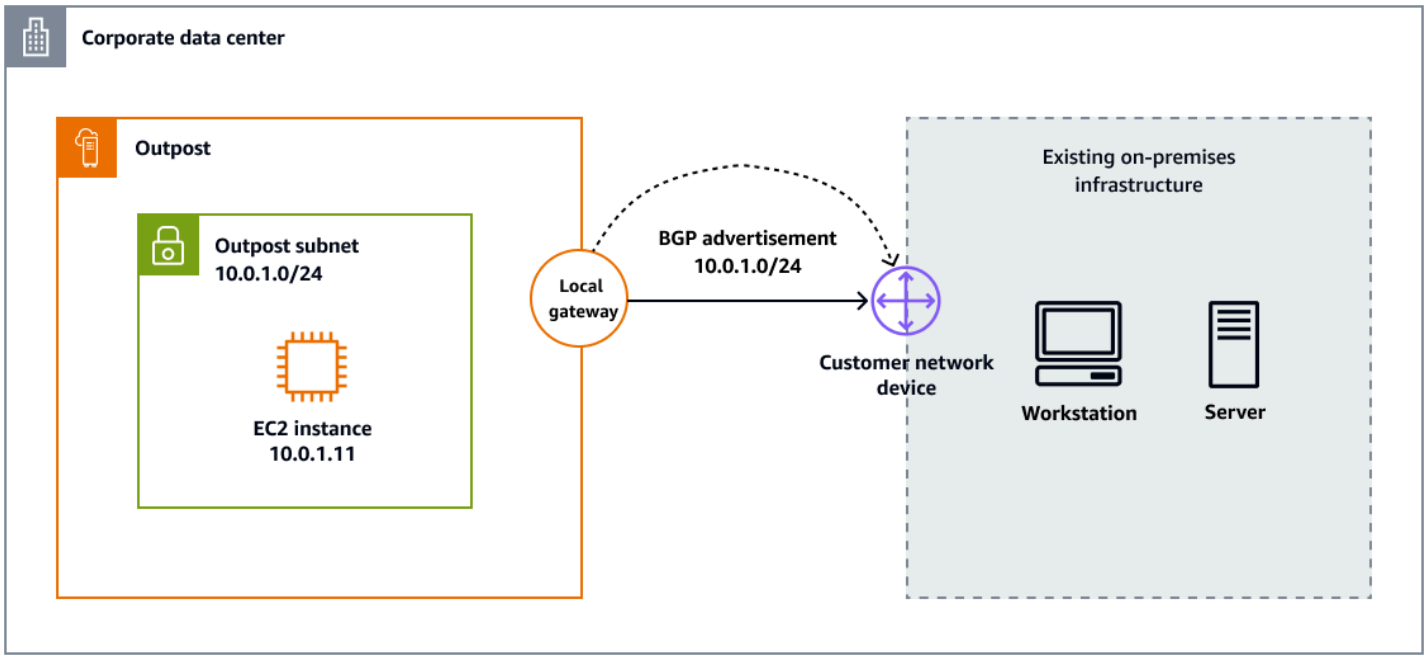
Traffico dall'edge all'ambiente locale

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.

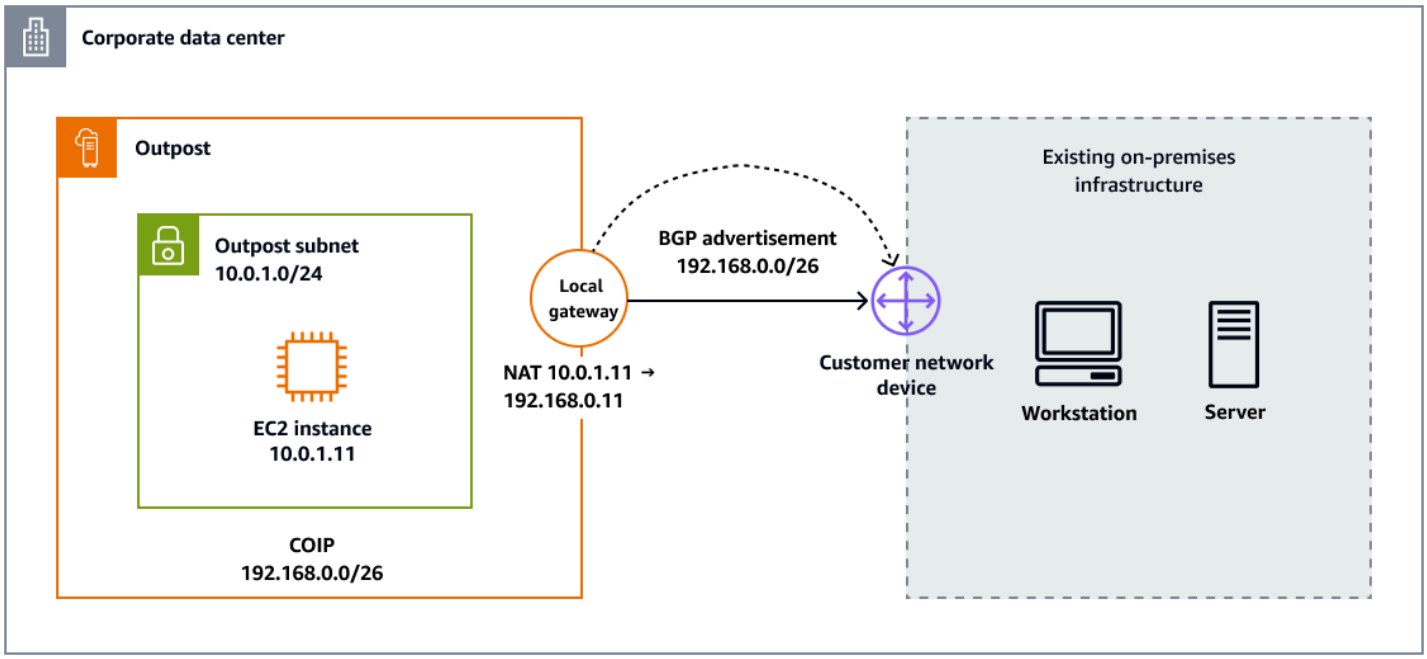
AWS Outposts gateway locale

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 istanze EC2, allocando un nuovo indirizzo IP elastico dal CoIP e quindi assegnandolo alla tua risorsa. Il diagramma seguente mostra un gateway locale che utilizza la modalità CoIP. AWS Outposts



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 un EC2-hosted carico di lavoro Amazon in una zona locale a Internet, puoi abilitare l'opzione IP Auto-assign 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'istanza EC2 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 Direct Connect

Supporta anche Local Zones 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 VPC e i carichi di lavoro della zona locale. Per ulteriori informazioni, consulta la sezione Transit gateway connection between Local Zones nella documentazione di 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 VPC estesi a Local

Zones. Quando i VPC peer si trovano nella stessa zona locale, il traffico rimane all'interno della zona locale e non attraversa la regione principale.

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. Third-party gli auditor 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 Centro identità AWS IAM. Ciò concede a ciascun utente solo le autorizzazioni necessarie per adempiere alle proprie mansioni lavorative.

Crittografia dei dati a riposo

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

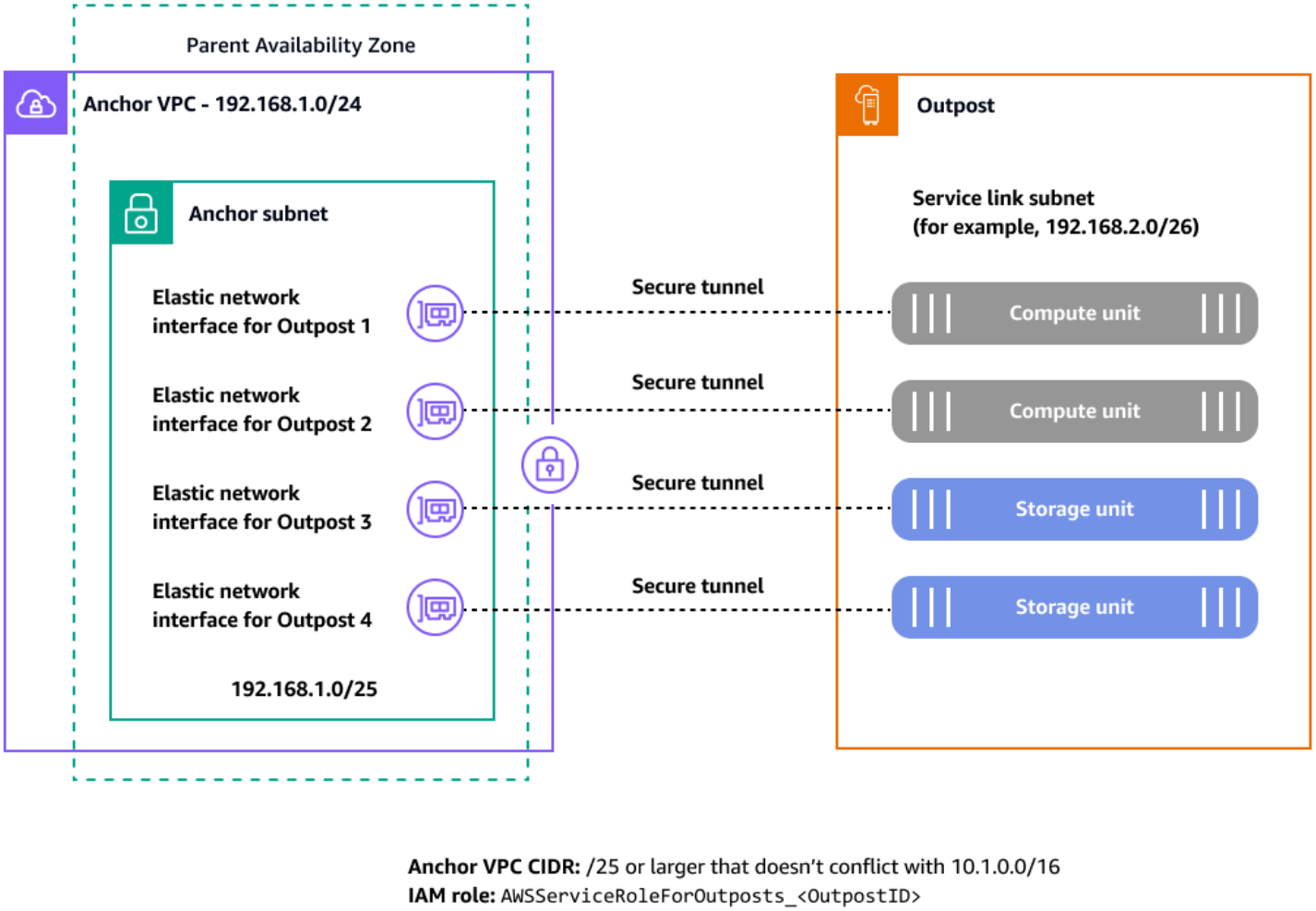
Per impostazione predefinita, tutti i dati archiviati in Amazon S3 su Outposts sono crittografati utilizzando la crittografia lato server con chiavi di crittografia gestite di Amazon S3 (). SSE-S3 Facoltativamente, puoi utilizzare la crittografia lato server con chiavi di crittografia fornite dal cliente (). SSE-C Per utilizzarla SSE-C, specifica una chiave di crittografia come parte delle richieste API degli oggetti. Server-side la crittografia crittografa solo i dati dell'oggetto, non i metadati dell'oggetto.

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

Crittografia dei dati 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 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.



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.

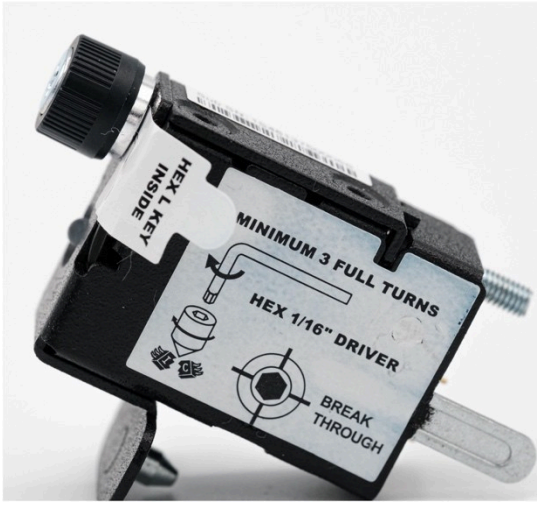
Protocollo	Porta di origine	Indirizzo di origine	Porta di destinazione	Indirizzo di destinazione
UDP	443	AWS Outposts link di servizio /26	443	AWS Outposts Percorsi pubblici della regione o

Protocollo	Porta di origine	Indirizzo di origine	Porta di destinazione	Indirizzo di destinazione
				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 sedi locali e Direct Connect PoPs per accedere a una zona locale, puoi abilitare la sicurezza MAC (MacSec) tra il router o lo switch locale e l'endpoint. Direct Connect Per ulteriori informazioni, consulta il post del AWS blog Aggiungere la sicurezza MacSec alle connessioni. Direct Connect

Eliminazione dei dati

Quando si arresta o si termina un'istanza EC2 AWS Outposts, la memoria ad essa allocata viene cancellata (impostata su zero) dall'hypervisor prima di essere allocata su 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
Identity-based politiche	Sì
Resource-based politiche	Sì*
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
Attribute-based controllo degli accessi (ABAC) (tag nelle politiche)	Sì

Funzionalità IAM	AWS Outposts supporto
Credenziali temporanee	Sì
Autorizzazioni delle entità principali	Sì
Ruoli di servizio	No
Service-linked ruoli	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 approccio di difesa approfondito per il traffico in entrata e in uscita. Ciò include l'uso di gruppi di sicurezza (firewall di ispezione stateful), ACL di rete, 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 istanze EC2, 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 istanze EC2, 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 Regioni AWS, ma sono connessi alle o Local AWS Outposts Zones tramite il percorso dati tra la regione e l'edge.

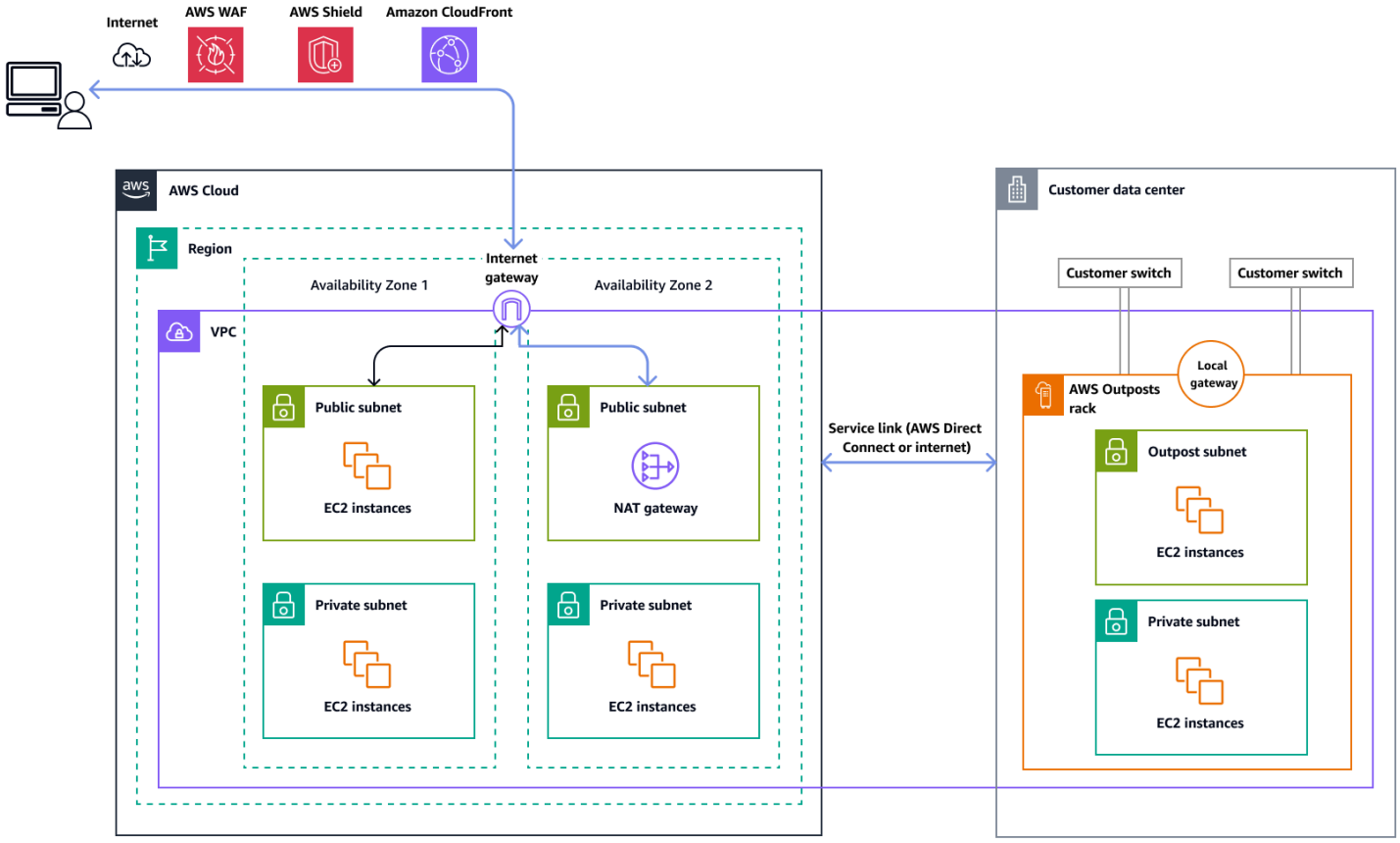
Local Zones adotta un costrutto di rete chiamato network border group, che viene utilizzato in. Regioni AWS AWS pubblicizza gli indirizzi IP pubblici di questi gruppi unici. Un gruppo di confini di rete è costituito da Availability Zones, Local Zones o Wavelength Zones. È possibile allocare in modo esplicito 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 ISV e aiutarvi a creare livelli di ispezione nella vostra 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

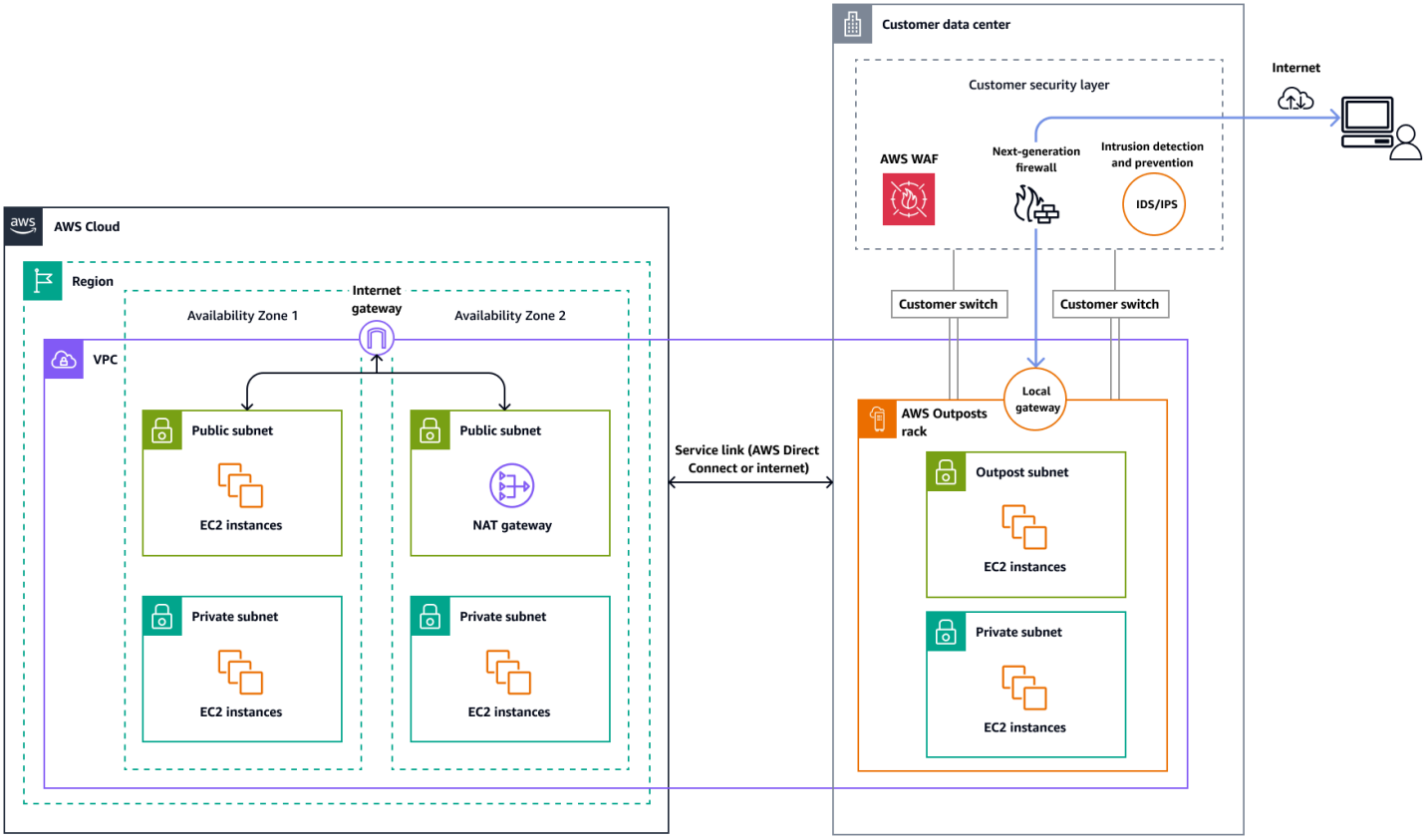
Il diagramma seguente mostra il traffico tra il carico di lavoro nell' AWS Outposts istanza e Internet che attraversa l'istanza principale. Regione AWS



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 (FSI). Per capire come implementare protezioni 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 del Framework)AWS Well-Architected

Condivisione delle risorse di Outposts

Poiché un Outpost è un'infrastruttura limitata che risiede nel 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 siti e 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, di configurare i VPC e di avviare ed eseguire istanze sull'Outpost condiviso.

Le risorse condivisibili sono: AWS Outposts

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

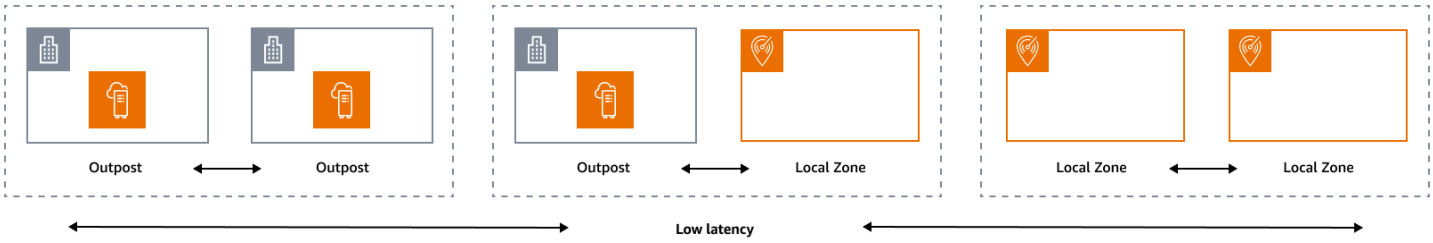
Per seguire le best practice per la condivisione delle risorse Outposts in un ambiente con più account, consulta i seguenti AWS post del blog:

- 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.

Local Zones

Le Local Zone agiscono in modo simile alle Zone di disponibilità al loro interno Regione AWS, poiché possono essere selezionate come posizione di collocamento per AWS risorse zonali come sottoreti e istanze EC2. Tuttavia, non sono situate in centri IT, industriali e industriali Regione AWS, ma in prossimità di grandi centri abitati, 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 l' AWS infrastruttura Servizi AWS, le API e gli strumenti al data center. 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 madre (nota anche come 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' Multi-AZ architettura 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
```

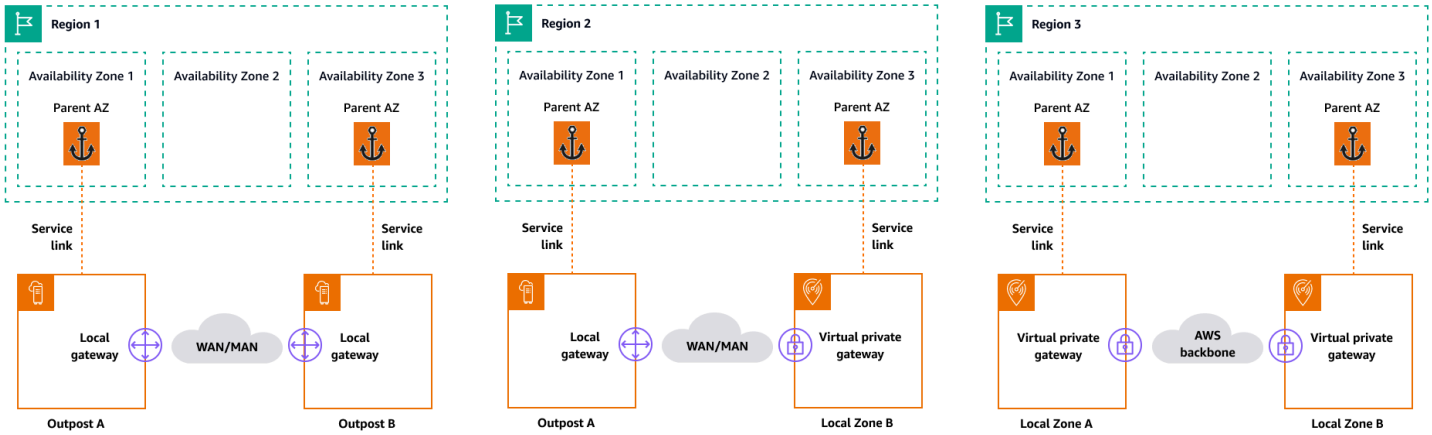
Risultato del comando precedente:

```
{     "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 per il networking all'edge, principalmente per le connessioni per accedere all'infrastruttura perimetrale. Esamina le architetture valide che forniscono una rete resiliente per il collegamento di servizio.

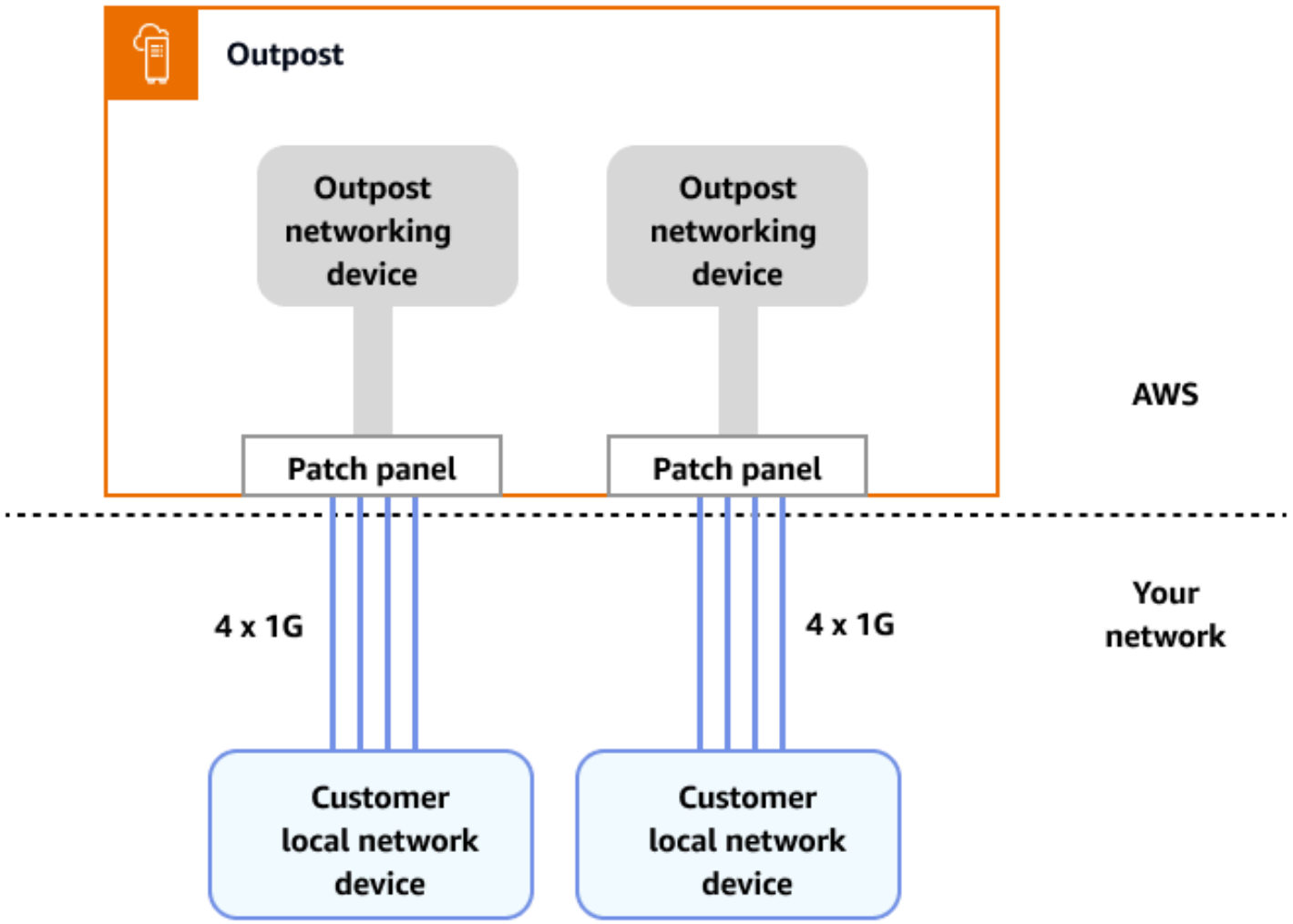
Rete resiliente per Local Zones

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. È tua responsabilità fornire la connettività dall'ambiente locale o dagli utenti alla zona locale. Indipendentemente dall'architettura di connettività scelta (ad esempio, VPN o 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 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.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 Direct Connect PoP rende impossibile la creazione delle architetture consigliate per Direct Connect la resilienza. Se hai accesso a una sola Direct Connect posizione o hai bisogno di resilienza oltre una singola connessione, puoi creare un'appliance VPN su Amazon EC2 Direct Connect e, come illustrato e discusso nel post AWS del 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 (OND). 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.

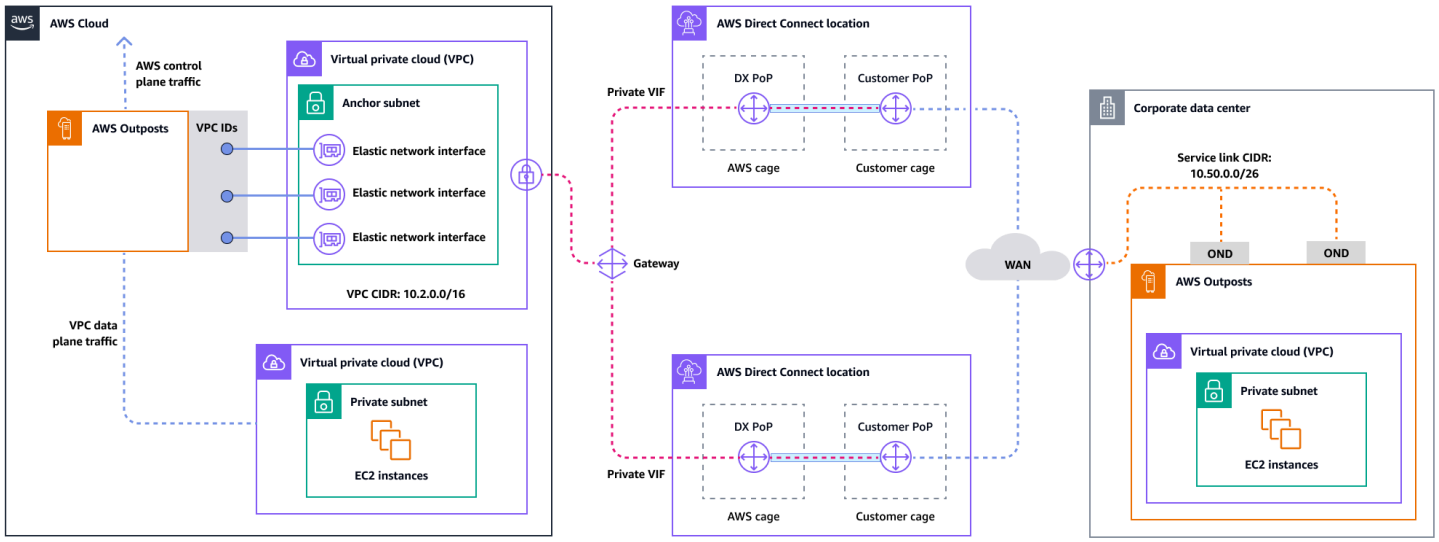
Velocità di uplink	Numero di uplink
1 Gb/s	1, 2, 4, 6 o 8
10 Gb/s	1, 2, 4, 8, 12 o 16
40 o 100 Gbps	1, 2 o 4



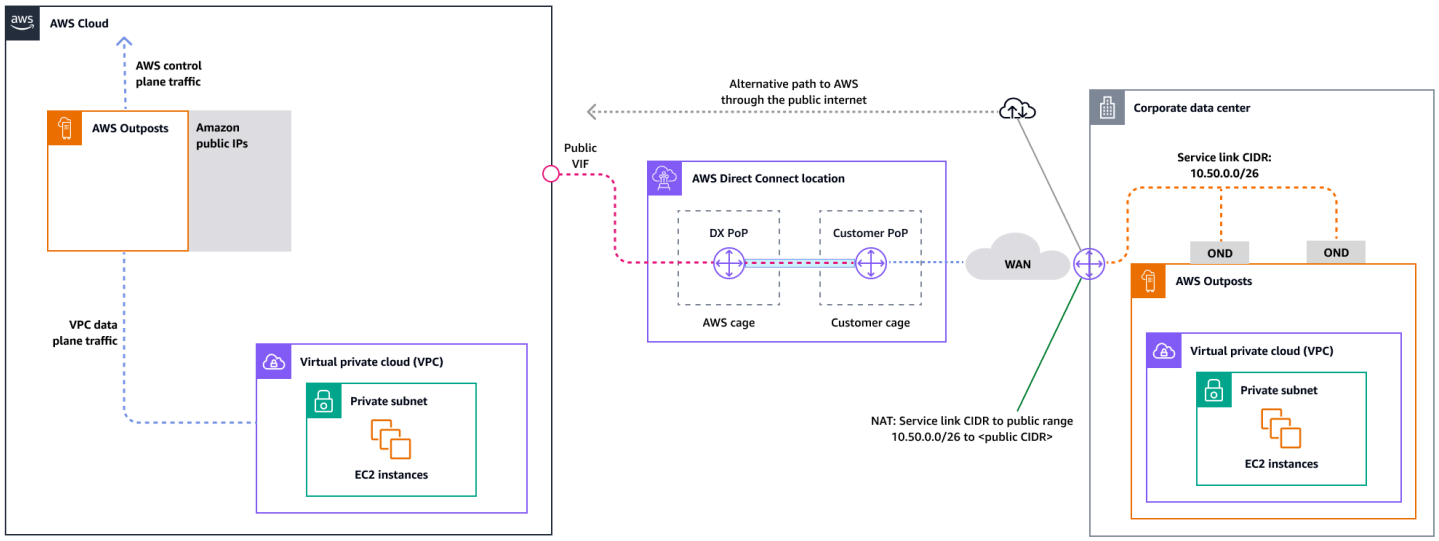
Per ulteriori informazioni su questa connettività, consulta Connettività di rete locale per Outposts Racks nella AWS Outposts documentazione.

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 Direct Connect o una connessione Internet per il collegamento al servizio. Questo minimo consente di avviare istanze EC2, collegare volumi EBS e accedere ad applicazioni come 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.



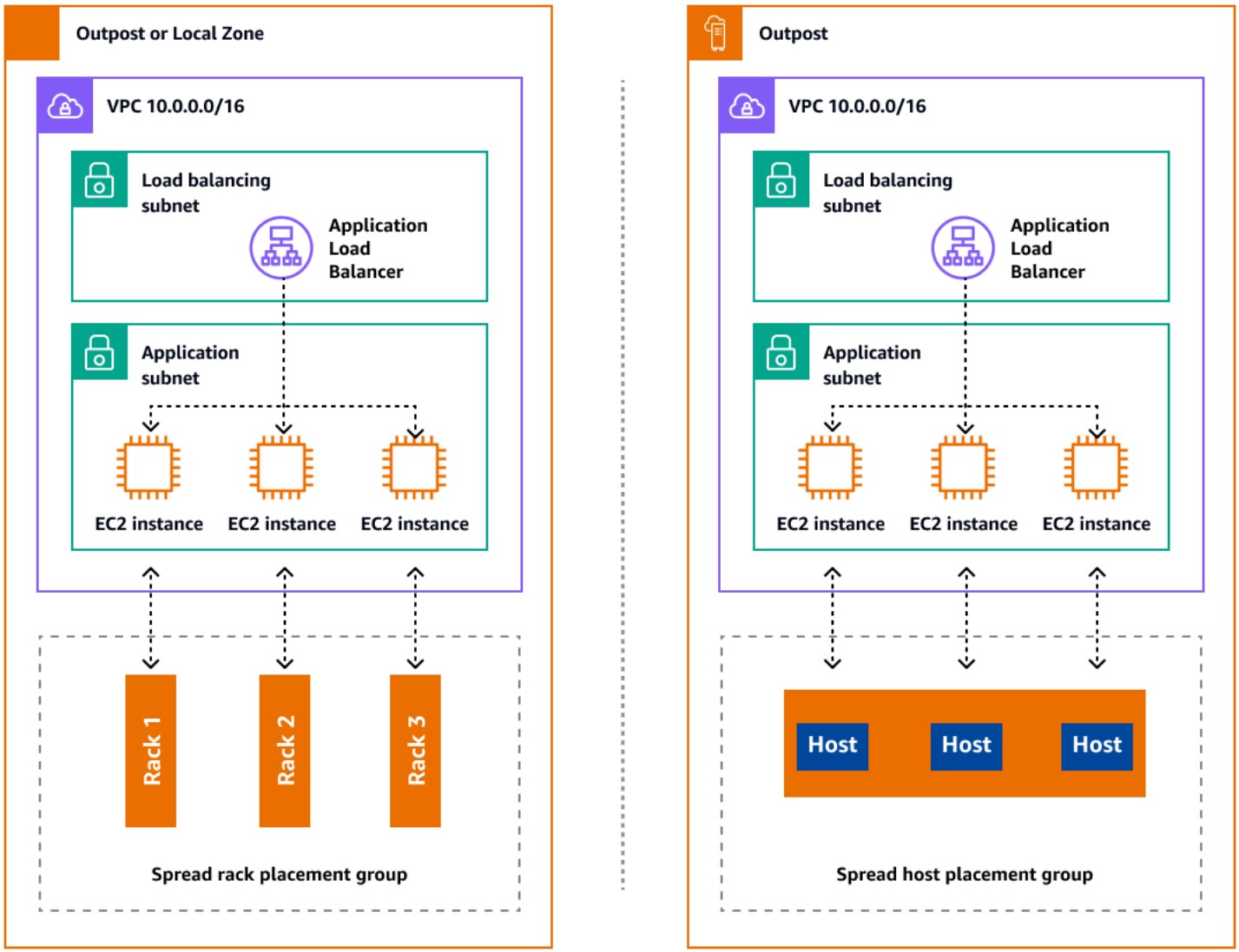
Scalabilità delle installazioni rack Outposts con i rack ACE

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 dispongono di un numero limitato 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.



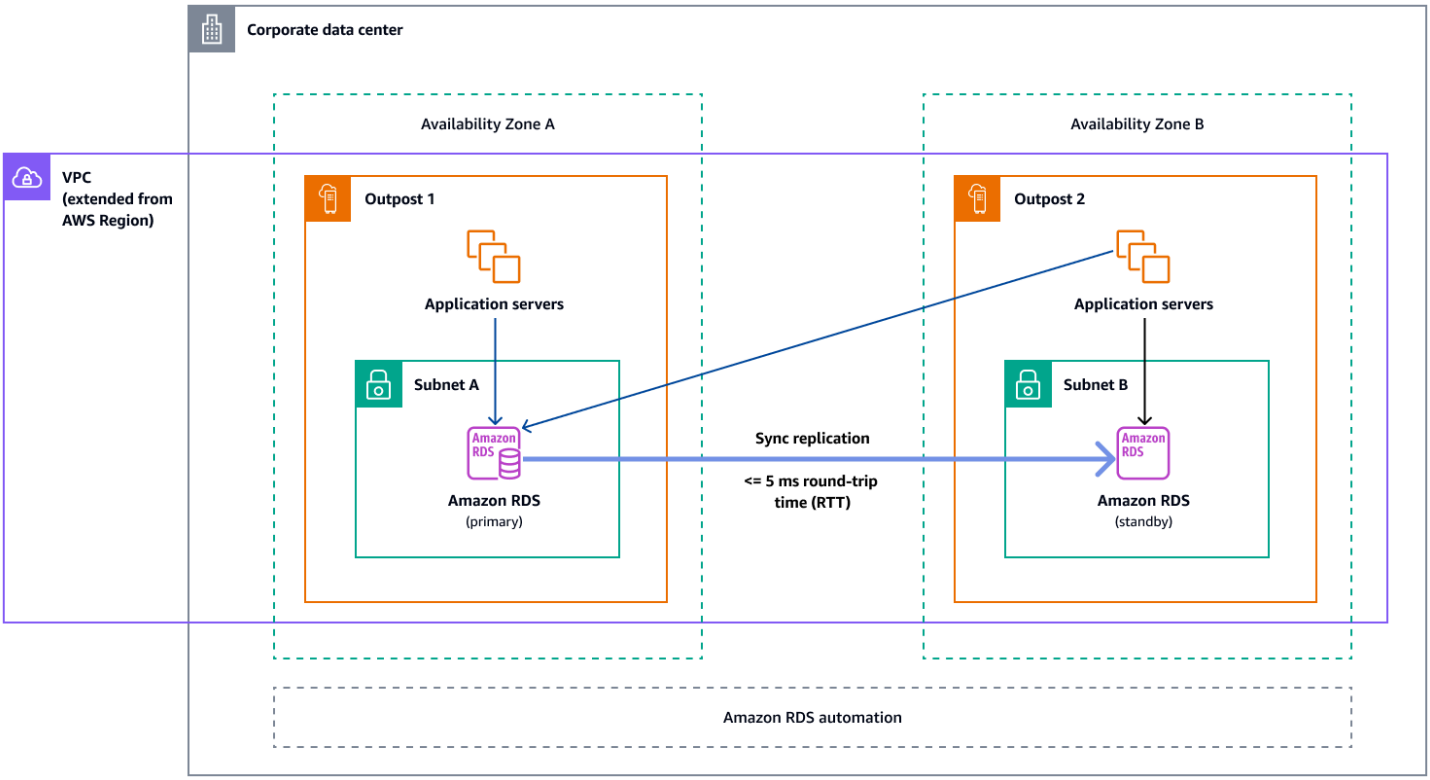
Amazon RDS in Multi-AZ AWS Outposts

Quando utilizzi le distribuzioni di Multi-AZ istanze 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 le Multi-AZ distribuzioni, Amazon RDS crea un'istanza DB principale su un Outpost e replica in modo sincrono i dati su un'istanza DB in standby su un altro Outpost. Multi-AZ le distribuzioni su Outposts funzionano come le Multi-AZ distribuzioni in Regioni AWS, con le seguenti differenze:

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

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

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



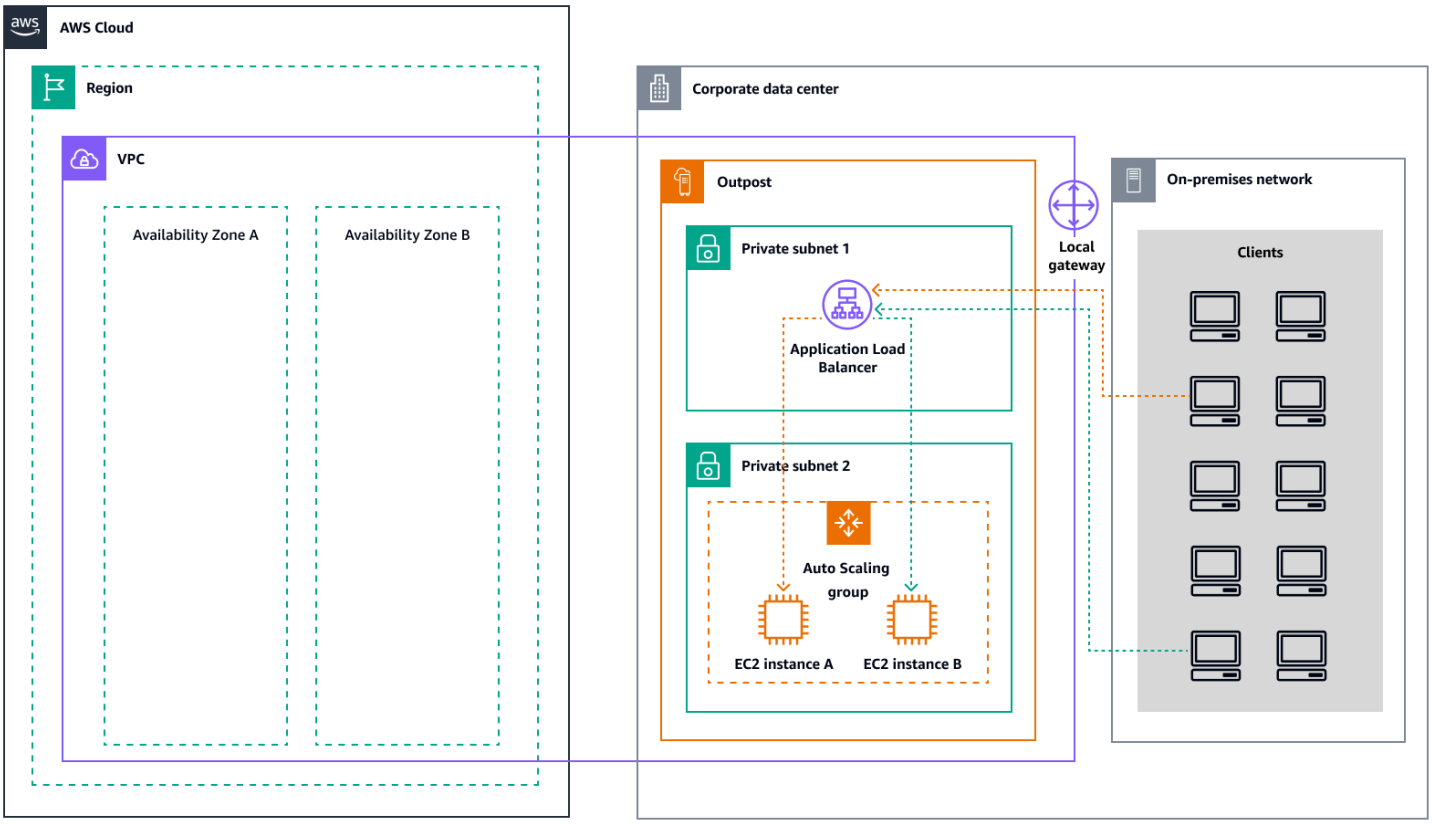
Meccanismi di failover

Bilanciamento del carico e scalabilità automatica

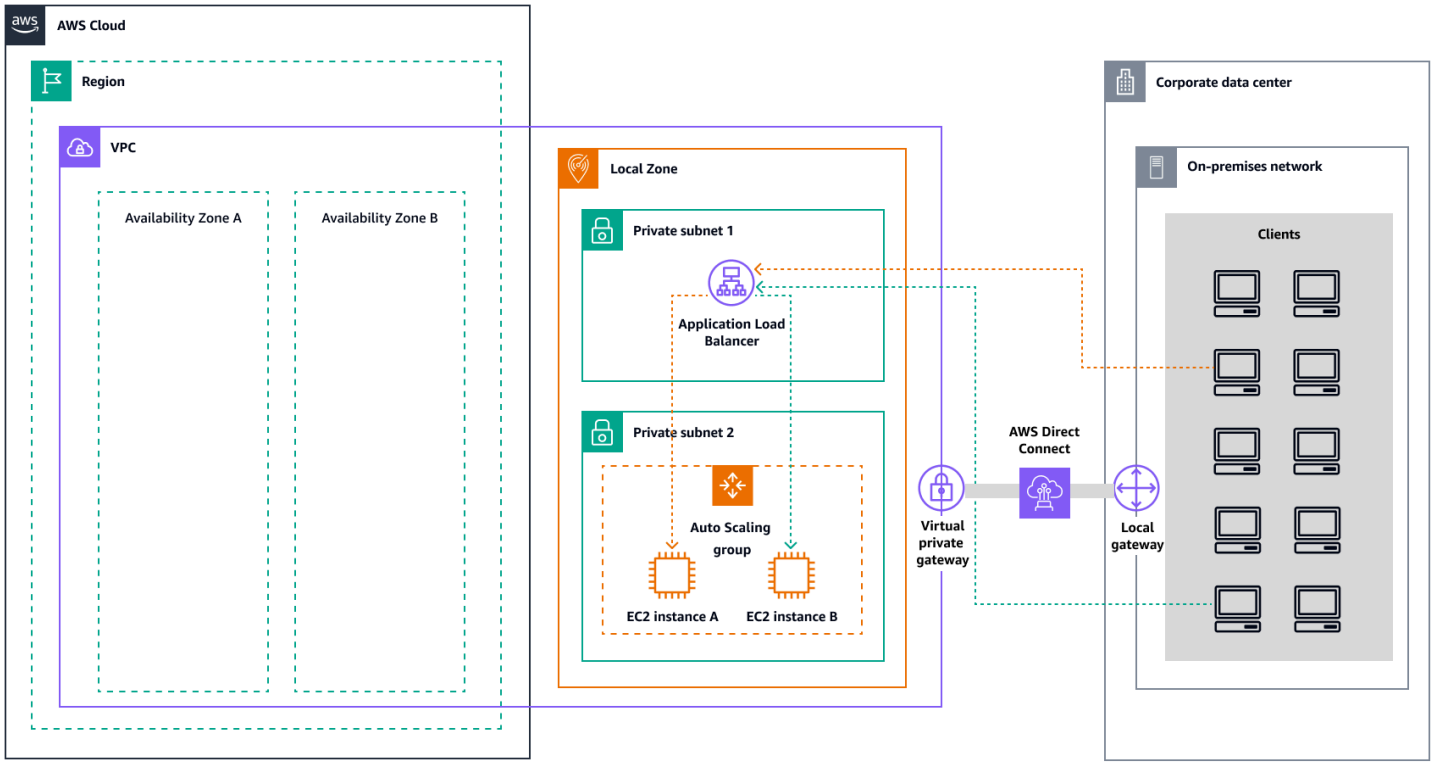
Elastic Load Balancing (ELB) distribuisce automaticamente il traffico delle applicazioni in entrata su tutte le istanze EC2 in esecuzione. ELB aiuta a gestire le richieste in entrata indirizzando il traffico in modo ottimale in modo che nessuna singola istanza venga sovraccaricata. Per utilizzare ELB

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 utilizzi ELB con il tuo gruppo Auto Scaling, non è necessario registrare singole istanze EC2 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 EC2 Auto Scaling possa identificare e sostituire 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 integri del gruppo target è inferiore a quello consentito.

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



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



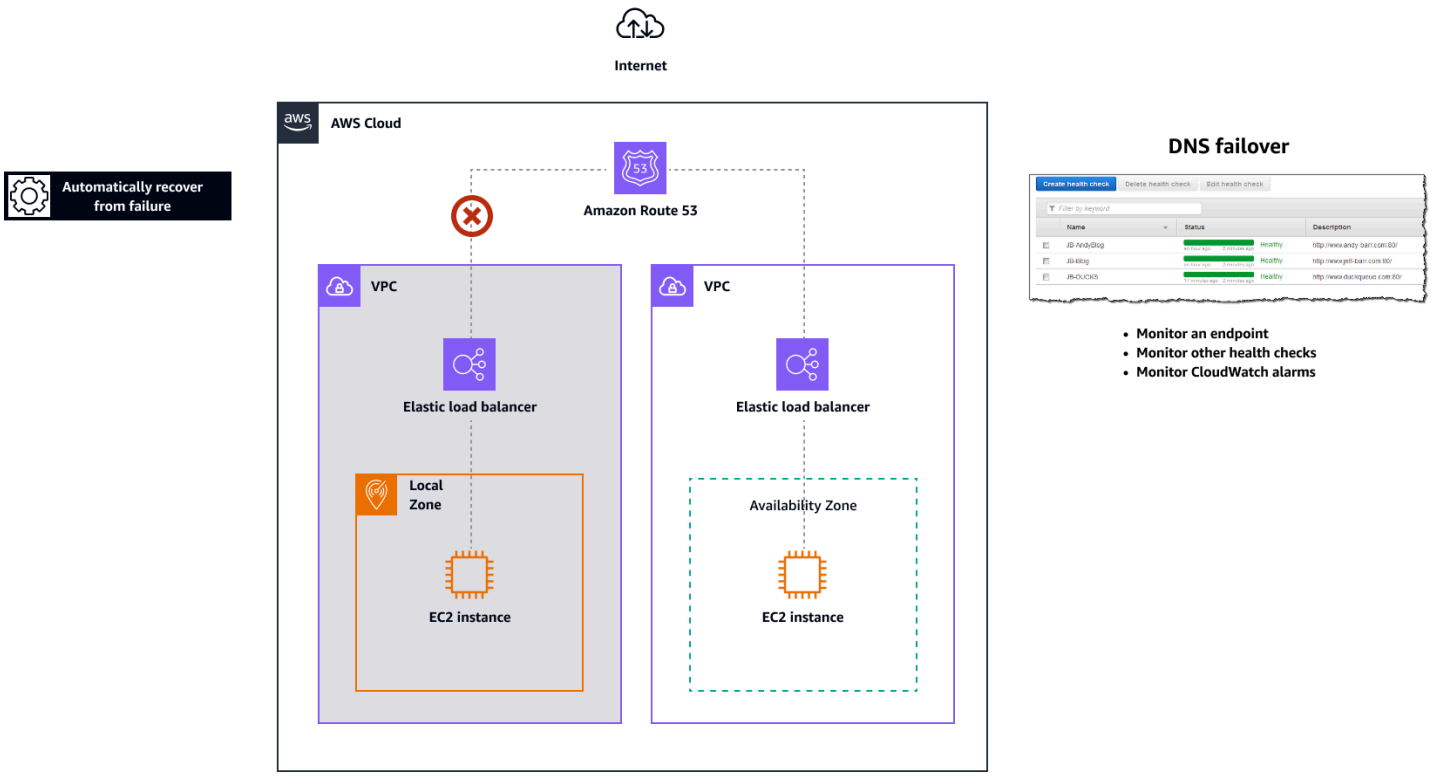
> **Note**
>
> Gli Application Load Balancer sono disponibili sia nelle Local Zones che AWS Outposts nelle Local Zones. Tuttavia, per utilizzare un Application Load Balancer in AWS Outposts, è necessario dimensionare la capacità di Amazon EC2 per fornire la scalabilità richiesta dal load balancer. Per 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) dagli IP pubblici 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. Outposts-hosted

Amazon Route 53 Resolver on 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 nei VPC Outposts 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 VPC e la rete nella documentazione di Route 53.

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 Transform MGN	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 per 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

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.