Guida per l'utente dei rack Outposts

AWS Outposts

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

AWS Outposts: Guida per l'utente dei rack Outposts

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

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

Table of Contents

Che cos'è AWS Outposts? ... 1
Concetti chiave ... 1
AWS risorse su Outposts ... 2
Prezzi ... 5
Come AWS Outposts funziona ... 6
Componenti di rete ... 7
VPCs e sottoreti ... 8
Routing ... 8
DNS ... 9
Collegamento al servizio ... 9
Gateway locali ... 10
Interfacce di rete locale ... 10
Requisiti per i rack Outposts ... 11
Struttura ... 11
Rete ... 13
Elenco di controllo di preparazione della rete ... 13
Alimentazione ... 18
Evasione dell'ordine ... 21
Requisiti per i rack ACE ... 22
Struttura ... 22
Rete ... 23
Alimentazione ... 24
Inizia a usare ... 25
Effettua un ordine ... 25
Fase 1: Creazione di un sito ... 25
Fase 2: Creazione di un Outpost ... 27
Fase 3: Effettuazione dell'ordine ... 27
Fase 4: Modificare la capacità dell'istanza ... 29
Passaggi successivi ... 21
Avvio di un'istanza ... 32
Fase 1. Creazione di un VPC ... 33
Passaggio 2: crea una sottorete e una tabella di routing personalizzata ... 33
Fase 3: Configurare la connettività del gateway locale ... 35
Fase 4: Configurare la rete locale ... 39

Passaggio 5: avvia un'istanza su Outpost ... 41
Passaggio 6: verifica la connettività ... 42
Ottimizzazione ... 46
Host dedicati su Outposts ... 46
Configurazione del ripristino dell'istanza ... 48
Gruppi di collocazione su Outposts ... 48
Collegamento al servizio ... 50
Connettività ... 50
Requisiti dell'unità di trasmissione massima (MTU) ... 50
Consigli sulla larghezza di banda ... 50
Connessioni Internet ridondanti ... 51
Configura il tuo link di servizio ... 51
Opzioni di connettività pubblica ... 52
Opzione 1. Connettività pubblica tramite Internet ... 52
Opzione 2. Connettività pubblica tramite AWS Direct Connect pubblico VIFs ... 53
Opzioni di connettività privata ... 53
Prerequisiti ... 53
Opzione 1. Connettività privata tramite rete AWS Direct Connect privata VIFs ... 55
Opzione 2. Connettività privata tramite AWS Direct Connect transito VIFs ... 55
Firewall e il collegamento al servizio ... 55
Risoluzione dei problemi di rete ... 57
Connettività con i dispositivi di rete Outpost ... 57
AWS Direct Connect connettività dell'interfaccia virtuale pubblica alla regione AWS ... 59
AWS Direct Connect interfaccia virtuale privata: connettività alla AWS regione ... 60
Connettività Internet pubblica dell'ISP alla regione AWS ... 61
Outposts è protetto da due dispositivi firewall ... 63
Gateway locali ... 65
Nozioni di base ... 65
Routing ... 67
Connettività ... 67
Tabelle di instradamento ... 68
Routing VPC diretto ... 69
Indirizzi IP di proprietà del cliente ... 73
Tabelle di routing personalizzate ... 77
Percorsi della tabella dei percorsi ... 77
Requisiti e limitazioni ... 77

Creazione delle tabelle di routing personalizzate del gateway locale 78
Cambio di modalità o eliminazione di una tabella di routing del gateway locale 79
Pool CoIP 80
Connettività di rete locale 84
Connettività fisica 84
Aggregazione dei collegamenti 86
Virtuale LANs 86
Connettività a livello di rete 88
Connettività rack ACE 90
Connettività BGP del collegamento al servizio 91
Annuncio della sottorete e intervallo IP dell'infrastruttura del collegamento al servizio 93
Connettività BGP del gateway locale 93
Pubblicità della sottorete IP di proprietà del cliente del gateway locale 96
Gestione della capacità 98
Visualizza la capacità 98
Modifica la capacità dell'istanza 29
Considerazioni 99
Risoluzione dei problemi relativi alle attività relative alla capacità 103
*oo-xxxxxx*L'ordine non è associato a Outpost ID *op-xxxxx* 103
Il piano di capacità include tipi di istanze non supportati 103
Nessun Outpost con Outpost ID *op-xxxxx* 104
CapacityTaskCappuccio attivo, *XXXX* già trovato per Outpost op *XXXX* 104
CapacityTaskCap attivo: *XXXX* già trovato per Asset *XXXX* su Outpost OP-xxxx 105
AssetId= non *XXXX* è valido per outpost=op- *XXXX* 106
Risorse condivise 108
Risorse Outpost condivisibili 109
Prerequisiti per la condivisione delle risorse Outposts 110
Servizi correlati 110
Condivisione tra le zone di disponibilità 110
Condivisione di una risorsa Outpost 111
Annullamento della condivisione di una risorsa Outpost 112
Individuazione di una risorsa Outpost condivisa 113
Autorizzazioni per le risorse Outpost condivise 114
Autorizzazioni per i proprietari 114
Autorizzazioni per gli utenti 114
Fatturazione e misurazione 114

Limitazioni ... 114
Sicurezza ... 116
Protezione dei dati ... 117
Crittografia a riposo ... 117
Crittografia in transito ... 117
Eliminazione dei dati ... 117
Gestione dell'identità e degli accessi ... 118
Come funziona AWS Outposts con IAM ... 118
Esempi di policy ... 123
Ruoli collegati ai servizi ... 126
AWS politiche gestite ... 130
Sicurezza dell'infrastruttura ... 131
Monitoraggio delle manomissioni ... 132
Resilienza ... 132
Convalida della conformità ... 133
Accesso a Internet ... 134
Accesso a Internet tramite la AWS regione madre ... 135
Accesso a Internet tramite la rete del data center locale ... 135
Monitoraggio ... 137
CloudWatch metriche ... 138
Metriche ... 138
Dimensioni metrica ... 144
... 144
Registra le chiamate API utilizzando CloudTrail ... 145
AWS Outposts eventi gestionali in CloudTrail ... 147
AWS Outposts esempi di eventi ... 147
Manutenzione ... 149
Aggiorna i dettagli di contatto ... 149
Manutenzione dell'hardware ... 149
Aggiornamenti del firmware ... 150
Manutenzione delle apparecchiature di rete ... 150
Eventi di alimentazione e di rete ... 151
Eventi di alimentazione ... 151
Eventi di connettività di rete ... 152
Risorse ... 153
End-of-term opzioni ... 155

Rinnovo dell'abbonamento 155
Chiusura dell'abbonamento 156
Conversione dell'abbonamento 160
Quote 161
AWS Outposts e le quote per altri servizi 161
Cronologia dei documenti 162
..... clxvii

Che cos'è AWS Outposts?

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura APIs, i servizi e gli strumenti alle sedi dei clienti. Fornendo l'accesso locale all'infrastruttura AWS gestita, AWS Outposts consente ai clienti di creare ed eseguire applicazioni in locale utilizzando le stesse interfacce di programmazione AWS delle regioni, utilizzando al contempo risorse di elaborazione e archiviazione locali per esigenze di elaborazione dati locali e latenza inferiori.

Un Outpost è un pool di capacità di AWS elaborazione e archiviazione distribuito presso la sede di un cliente. AWS gestisce, monitora e gestisce questa capacità come parte di una regione. AWS Puoi creare sottoreti su Outpost e specificarle quando crei AWS risorse come EC2 istanze, volumi EBS, cluster ECS e istanze RDS. Le istanze nelle sottoreti Outpost comunicano con altre istanze della AWS regione utilizzando indirizzi IP privati, tutti all'interno dello stesso VPC.

> **Note**
>
> Non puoi connettere un avamposto a un altro avamposto o zona locale all'interno dello stesso VPC.

Per ulteriori informazioni, consulta la pagina dei dettagli del prodotto AWS Outposts.

Concetti chiave

Questi sono i concetti chiave per. AWS Outposts

- Sito Outpost: gli edifici fisici gestiti dal cliente in cui AWS installerai il tuo Outpost. Un sito deve soddisfare i requisiti di infrastruttura, rete e alimentazione del tuo Outpost.
- Capacità Outpost: risorse di calcolo e storage disponibili sull'Outpost. Puoi visualizzare e gestire la capacità del tuo Outpost dalla console. AWS Outposts AWS Outposts supporta la gestione della capacità self-service che puoi definire a livello di Outposts per riconfigurare tutte le risorse in un Outposts o specificamente per ogni singola risorsa. Una risorsa Outpost può essere un singolo server all'interno di un rack Outposts o di un server Outposts.
- Apparecchiature Outpost: hardware fisico che fornisce l'accesso al servizio. AWS Outposts L'hardware include rack, server, switch e cavi di proprietà e gestiti da. AWS

- Rack Outposts: un fattore di forma Outpost che è un rack 42U standard di settore. I rack Outposts includono server montabili su rack, switch, un pannello patch di rete, un power shelf e pannelli vuoti.
- Rack Outposts ACE: il rack Aggregation, Core, Edge (ACE) funge da punto di aggregazione di rete per le implementazioni Outpost multi-rack. Il rack ACE riduce il numero di porte di rete fisiche e requisiti di interfaccia logica fornendo connettività tra più rack di elaborazione Outpost negli Outposts logici e nella rete locale.

  È necessario installare un rack ACE se si dispone di quattro o più rack di elaborazione. Se disponi di meno di quattro rack di elaborazione ma prevedi di espanderli a quattro o più rack in futuro, ti consigliamo di installare un rack ACE al più presto.

  Per ulteriori informazioni sui rack ACE, consulta Scalare le implementazioni dei AWS Outposts rack con i rack ACE.
- Server Outposts: un fattore di forma Outpost che è un server 1U o 2U standard di settore, che può essere installato in un rack a 4 staffe conforme allo standard EIA-310D 19. I server Outposts forniscono servizi di elaborazione e rete locali a siti con requisiti di spazio limitati o di capacità inferiori.
- Proprietario di Outpost: il proprietario dell'account che effettua l'ordine. AWS Outposts Dopo aver AWS interagito con il cliente, il proprietario può includere punti di contatto aggiuntivi. AWS comunicherà con i contatti per chiarire gli ordini, gli appuntamenti di installazione e la manutenzione e la sostituzione dell'hardware. Contatta il Supporto AWS Centro se le informazioni di contatto cambiano.
- Link di servizio: percorso di rete che consente la comunicazione tra Outpost e la AWS regione associata. Ogni Outpost è un'estensione di una zona di disponibilità e della relativa regione associata.
- Gateway locale (LGW): un router virtuale di interconnessione logica che consente la comunicazione tra un rack Outposts e la rete locale.
- Interfaccia di rete locale: interfaccia di rete che consente la comunicazione tra un server Outposts e la rete locale.

AWS risorse su Outposts

Puoi creare le seguenti risorse sul tuo Outpost per supportare carichi di lavoro a bassa latenza che devono essere eseguiti in prossimità di dati e applicazioni on-premise:

Calcolo

Tipo di risorsa	Rack	Server
EC2 Istanze Amazon	S	Sì
Cluster Amazon ECS	S	Sì
Nodi Amazon EKS	S	No

Database e analisi

Tipo di risorsa	Rack	Server
ElastiCacheNodi Amazon (cluster Redis, cluster Memcached)	S	No
Cluster Amazon EMR	S	No
Istanze DB Amazon RDS	S	No

Reti

Tipo di risorsa	Rack	Server
Proxy App Mesh Envoy	S	Sì
Application Load Balancer	S	No
Sottoreti Amazon VPC	S	Sì
Amazon Route 53	S	No

Storage

Tipo di risorsa	Rack	Server
Volumi Amazon EBS	S	No
Bucket Amazon S3	S	No

Altro Servizi AWS

Servizio	Rack	Server
AWS IoT Greengrass	S	Sì

Prezzi

I prezzi si basano sui dettagli dell'ordine. Quando effettui un ordine, puoi scegliere tra una varietà di configurazioni Outpost, ognuna delle quali offre una combinazione di tipi di EC2 istanze Amazon e opzioni di archiviazione. Scegliete anche una durata del contratto e un'opzione di pagamento. I prezzi includono quanto segue:

- Rack Outposts: consegna, installazione, manutenzione dei servizi di infrastruttura, patch e aggiornamenti software e rimozione dei rack.
- Server Outposts: consegna, manutenzione dei servizi di infrastruttura e patch e aggiornamenti software. L'utente è responsabile dell'installazione e dell'imballaggio del server per la restituzione.

Ti vengono addebitate le risorse condivise e l'eventuale trasferimento di dati dalla AWS Regione all'Avamposto. Ti vengono inoltre addebitati i trasferimenti di dati volti a mantenere la disponibilità e la sicurezza. AWS

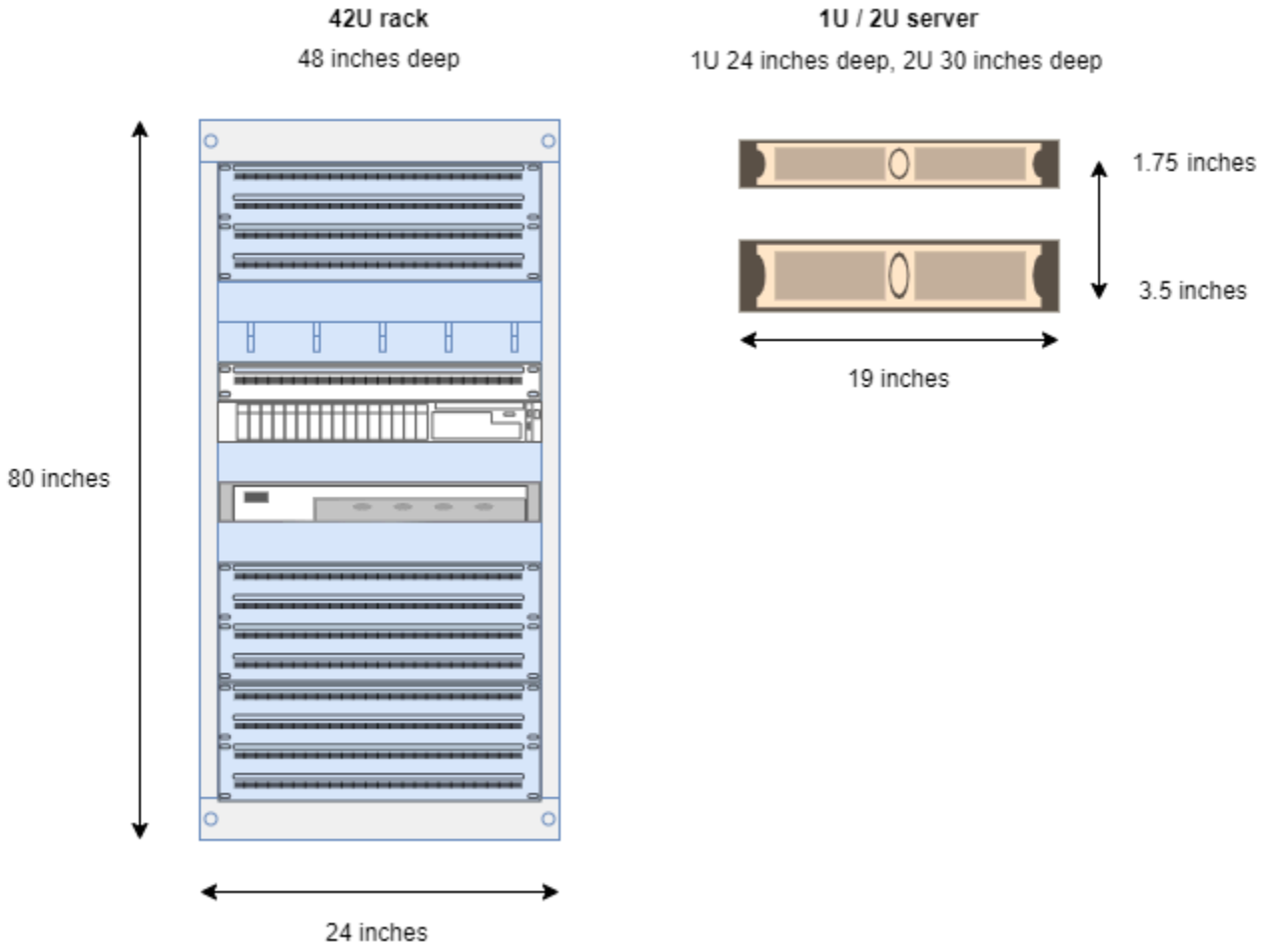
Per i prezzi in base all'ubicazione, alla configurazione e all'opzione di pagamento, consulta:

- Prezzi degli scaffali Outposts
- Prezzi dei server Outposts

Come AWS Outposts funziona

AWS Outposts è progettato per funzionare con una connessione costante e coerente tra l'Outpost e una AWS regione. Per realizzare questa connessione alla regione e ai carichi di lavoro locali nell'ambiente on-premise, è necessario connettere l'Outpost alla rete on-premise. La rete locale deve fornire l'accesso WAN (Wide Area Network) alla regione. Deve inoltre fornire l'accesso LAN o WAN alla rete locale in cui risiedono i carichi di lavoro o le applicazioni on-premise.

Il seguente diagramma illustra entrambi i fattori di forma dell'Outpost.



Indice

- Componenti di rete
- VPCs e sottoreti
- Routing
- DNS

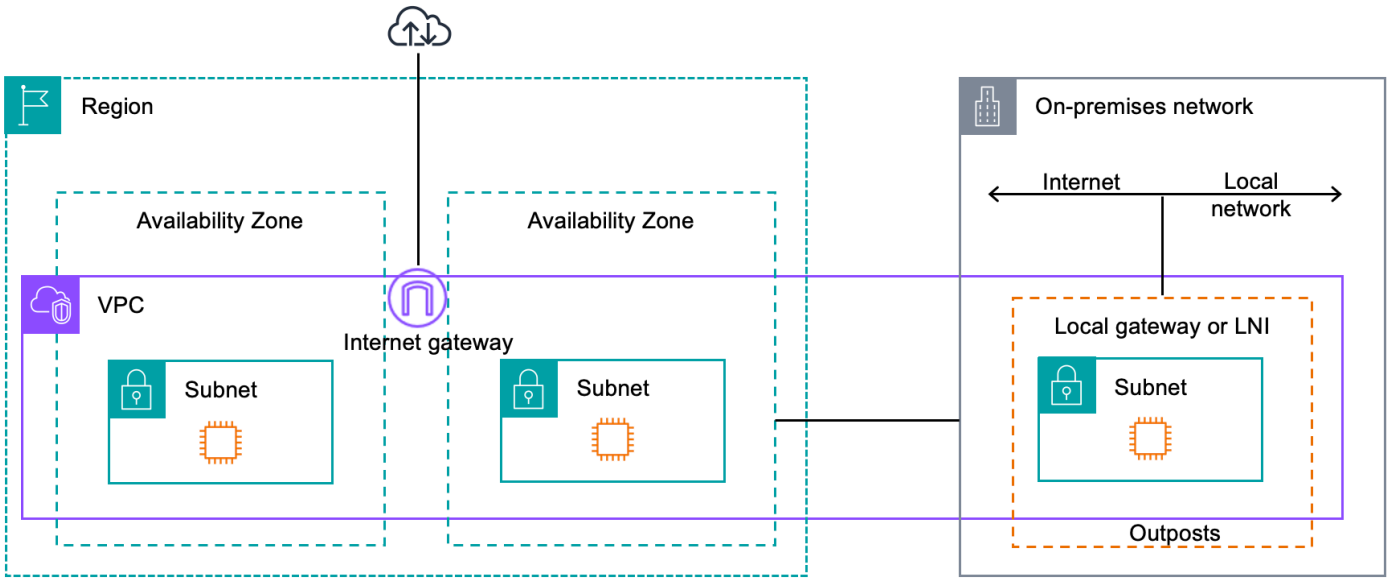
- Collegamento al servizio
- Gateway locali
- Interfacce di rete locale

Componenti di rete

AWS Outposts estende un Amazon VPC da una AWS regione a un avamposto con i componenti VPC accessibili nella regione, inclusi gateway Internet, gateway privati virtuali, gateway di transito Amazon VPC ed endpoint VPC. Un Outpost è ospitato in una zona di disponibilità nella regione ed è un'estensione della zona di disponibilità che è possibile utilizzare per la resilienza.

Il seguente diagramma mostra i componenti di rete del tuo Outpost.

- Una rete locale e una rete locale Regione AWS
- Un VPC con più sottoreti nella regione
- Un Outpost nella rete on-premise
- La connettività tra Outpost e la rete locale forniva:
  - I rack For Outposts: un gateway locale
  - Per i server Outposts: un'interfaccia di rete locale (LNI)



VPCs e sottoreti

Un cloud privato virtuale (VPC) si estende su tutte le zone di disponibilità della propria regione. AWS Puoi estendere qualsiasi VPC nella regione al tuo Outpost aggiungendo una sottorete Outpost. Per aggiungere una sottorete Outpost a un VPC, specifica il nome della risorsa Amazon (ARN) dell'outpost quando crei la sottorete.

Outposts supporta più sottoreti. Puoi specificare la sottorete dell' EC2 istanza quando avvii l' EC2 istanza in Outpost. Non è possibile specificare l'hardware sottostante su cui viene distribuita l'istanza, perché Outpost è un pool di capacità di AWS elaborazione e archiviazione.

Ogni Outpost può supportare più sottoreti Outpost VPCs che possono avere una o più sottoreti Outpost. Per informazioni sulle quote di VPC, consulta Quote di Amazon VPC nella Guida per l'utente di Amazon VPC.

Puoi creare sottoreti Outpost dall'intervallo CIDR del VPC in cui hai creato l'Outpost. Puoi utilizzare gli intervalli di indirizzi Outpost per le risorse, ad esempio le EC2 istanze che risiedono nella sottorete Outpost.

Routing

Per impostazione predefinita, ogni sottorete Outpost eredita la tabella di routing principale dal proprio VPC. Puoi creare una tabella di routing personalizzata e associarla a una sottorete Outpost.

Le tabelle di routing per le sottoreti Outpost funzionano come le sottoreti delle zone di disponibilità. È possibile specificare indirizzi IP, gateway Internet, gateway locali, gateway privati virtuali e connessioni in peering quali destinazioni. Ad esempio, ogni sottorete Outpost, tramite la tabella di routing principale ereditata o una tabella personalizzata, eredita il percorso locale VPC. Ciò significa che tutto il traffico all'interno del VPC, inclusa la sottorete Outpost con una destinazione nel CIDR del VPC, rimane instradato nel VPC.

Le tabelle di routing della sottorete Outpost possono includere le seguenti destinazioni:

- Intervallo VPC CIDR: lo AWS definisce al momento dell'installazione. Questo è il percorso locale e si applica a tutto il routing VPC, incluso il traffico tra istanze Outpost nello stesso VPC.
- AWS Destinazioni regionali: include elenchi di prefissi per Amazon Simple Storage Service (Amazon S3), endpoint gateway Amazon DynamoDB, gateway privati virtuali AWS Transit Gateway, gateway Internet e peering VPC.

Se disponi di una connessione peering con più connessioni VPCs sullo stesso Outpost, il traffico tra di esse VPCs rimane nell'Outpost e non utilizza il collegamento di servizio alla regione.

- Comunicazione all'interno dei VPC tra gli Outpost con gateway locale: puoi stabilire una comunicazione tra le sottoreti nello stesso VPC su diversi Outpost con gateway locali, utilizzando l'instradamento VPC diretto. Per ulteriori informazioni, consultare:
  - Routing VPC diretto
  - Routing a un gateway locale di AWS Outposts

DNS

Per le interfacce di rete connesse a un VPC EC2 , le istanze nelle sottoreti Outposts possono utilizzare il servizio DNS Amazon Route 53 per risolvere i nomi di dominio in indirizzi IP. Route 53 supporta le funzionalità DNS, come la registrazione del dominio, il routing DNS e i controlli dell'integrità per le istanze in esecuzione sull'Outpost. Sono supportate zone di disponibilità ospitate sia pubbliche che private per instradare il traffico verso domini specifici. I resolver Route 53 sono ospitati nella regione. AWS Pertanto, la connettività del service link dall'Outpost alla AWS regione deve essere attiva e funzionante affinché queste funzionalità DNS funzionino.

Route 53 potrebbe richiedere tempi di risoluzione DNS più lunghi, a seconda della latenza del percorso tra Outpost e la regione. AWS In questi casi, è possibile utilizzare i server DNS installati nell'ambiente on-premise. Per utilizzare i tuoi server DNS, devi creare set di opzioni DHCP per i server DNS on-premise e associarli al VPC. Devi inoltre assicurarti che vi sia connettività IP a questi server DNS. Potrebbe anche essere necessario aggiungere percorsi alla tabella di routing del gateway locale per la raggiungibilità, ma questa è solo un'opzione per i rack Outposts con gateway locale. Poiché i set di opzioni DHCP hanno un ambito VPC, le istanze nelle sottoreti Outpost e nelle sottoreti della zona di disponibilità per il VPC cercheranno di utilizzare i server DNS specificati per la risoluzione dei nomi DNS.

La registrazione delle query non è supportata per le query DNS provenienti da un Outpost.

Collegamento al servizio

Il link al servizio è un collegamento dal tuo Outpost alla AWS regione o alla regione di origine di Outposts prescelta. Il collegamento al servizio è un set crittografato di connessioni VPN che vengono utilizzate ogni volta che Outpost comunica con la regione di origine prescelta. Si utilizza una LAN virtuale (VLAN) per segmentare il traffico sul collegamento al servizio. La VLAN service link consente

la comunicazione tra l'avamposto e la AWS regione sia per la gestione dell'avamposto che per il traffico intra-VPC tra la regione e l'avamposto. AWS

Il collegamento al servizio viene creato al momento della fornitura dell'Outpost. Se disponi di un fattore di forma server, la connessione viene creata da te, Se disponi di un rack, crea il link di servizio. AWS Per ulteriori informazioni, consultare:

- AWS Outposts connettività a Regioni AWS
- Routing delle applicazioni e dei carichi di lavoro nel white paper «Considerazioni sulla progettazione e l'architettura AWS Outposts ad alta disponibilità» AWS

Gateway locali

I rack Outposts includono un gateway locale per fornire connettività alla rete locale. Se disponi di un rack Outposts, puoi includere un gateway locale come destinazione in cui la destinazione è la tua rete locale. I gateway locali sono disponibili solo per i rack Outposts e possono essere utilizzati solo nelle tabelle di routing VPC e subnet associate a un rack Outposts. Per ulteriori informazioni, consultare:

- Gateway locali per i tuoi rack Outposts
- Routing delle applicazioni e dei carichi di lavoro nel white paper Considerations dedicato alla progettazione e all'architettura AWS Outposts ad alta disponibilità AWS

Interfacce di rete locale

I server Outposts includono un'interfaccia di rete locale per fornire connettività alla rete locale. Un'interfaccia di rete locale è disponibile solo per i server Outposts in esecuzione su una sottorete Outpost. Non puoi utilizzare un'interfaccia di rete locale da un' EC2 istanza su un rack Outposts o nella AWS regione. L'interfaccia di rete locale è destinata unicamente alle sedi on-premise. Per ulteriori informazioni, consulta Interfaccia di rete locale nella Guida per l'utente dei server Outposts di AWS Outposts .

Requisiti del sito per i rack Outposts

Un sito Outpost è la posizione fisica in cui opera il tuo Outpost. I siti sono disponibili unicamente in determinati paesi e territori. Per ulteriori informazioni, consulta, AWS Outposts rack FAQs. Fai riferimento alla domanda: In quali paesi e territori è disponibile il rack Outposts?

Questa pagina descrive i requisiti per i rack Outposts. Se state installando un rack Aggregation, Core, Edge (ACE), il sito deve inoltre soddisfare i requisiti elencati in. Requisiti del sito per i rack Outpost ACE

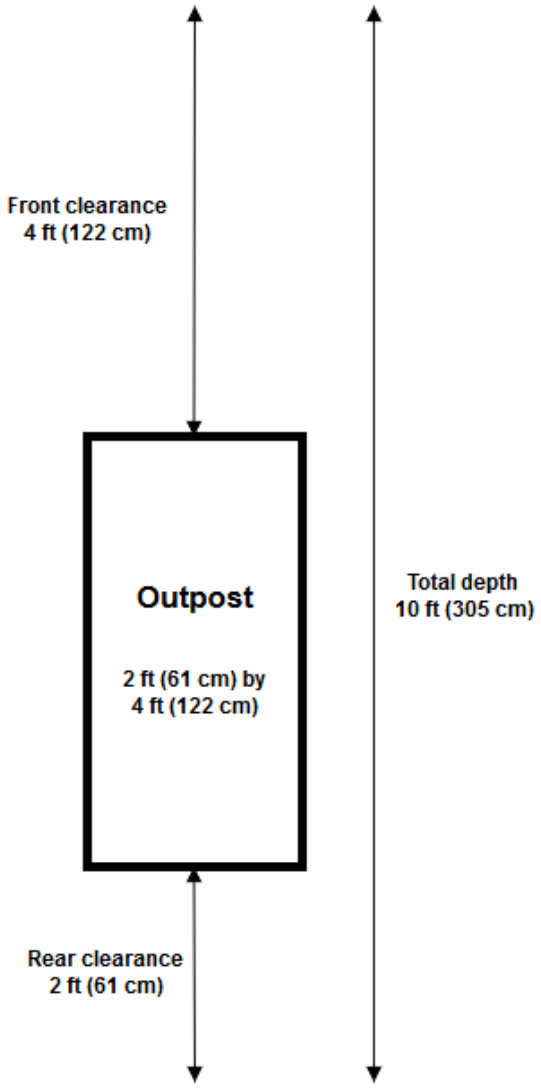
Per i requisiti relativi ai server Outposts, consulta i Requisiti del sito per i server Outposts nella AWS Outposts Guida per l'utente dei server Outposts.

Struttura

Questi sono i requisiti della struttura per i rack.

- Temperatura e umidità: la temperatura ambiente deve essere compresa tra 5 °C (41 °F) e 35 °C (95 °F). L'umidità relativa deve essere compresa tra l'8 e l'80% senza condensa.
- Circolazione dell'aria nei rack: l'aria fredda viene aspirata dal corridoio anteriore e l'aria calda viene espulsa verso il corridoio posteriore. La posizione del rack deve fornire un flusso d'aria pari ad almeno 145,8 volte il kVA di piedi cubi al minuto (CFM).
- Area di carico: l'area di carico deve contenere una cassa del rack da 239 cm (94 pollici) di altezza per 138 cm (54 pollici) di larghezza per 130 cm (51 pollici) di profondità.
- Supporto del peso: il peso varia in base alla configurazione. Il peso per la tua configurazione è specificato nel riepilogo dell'ordine in corrispondenza dei carichi a punto del rack. La posizione in cui è installato il rack e il percorso verso tale posizione devono supportare il peso specificato. Ciò include tutti gli ascensori per il trasporto merci e gli ascensori standard lungo il percorso.
- Spazio libero: il rack ha un'altezza di 203 cm (80 pollici) per 61 cm (24 pollici) di larghezza e 122 cm (48 pollici) di profondità. Tutte le porte, i corridoi, le curve, le rampe e gli ascensori devono disporre di spazio libero sufficiente. Nella posizione di riposo finale, l'area per l'Outpost deve avere le seguenti misure: 61 cm (24 pollici) di larghezza per 122 cm (48 pollici) di profondità, con ulteriori 122 cm (48 pollici) di spazio libero anteriore e 61 cm (24 pollici) di spazio libero posteriore. L'area minima totale richiesta per l'Outpost è di 61 cm (24 pollici) di larghezza per 305 cm (10 piedi) di profondità.

Il seguente diagramma mostra l'area minima totale necessaria per l'Outpost, incluso lo spazio libero.



- Rinforzo antisismico: nella misura richiesta dalla normativa o dal codice, sarà necessario installare e mantenere l'ancoraggio e il rinforzo sismici adeguati per il rack mentre si trova nella struttura. AWS fornisce staffe da pavimento che proteggono fino a 2,0 G di attività sismica con tutti i rack Outposts.
- Punto di incollaggio: si consiglia di effettuare un incollaggio nella posizione del rack wire/point in modo che l'elettricista possa fissare i rack durante l'installazione, operazione che verrà convalidata dal tecnico certificato. AWS

- Accesso alla struttura: non modificherai la struttura in modo tale da influire negativamente sulla capacità di accedere, riparare o rimuovere l' AWS Outpost.
- Altitudine: l'altitudine del locale in cui è installato il rack deve essere inferiore a 3.050 metri (10.005 piedi).

Rete

Questi sono i requisiti di rete per i rack.

- Provvedi a fornire uplink con velocità pari a 1 Gb/s, 10 Gb/s, 40 Gb/s o 100 Gb/s.

  Per consigli sulla larghezza di banda per la connessione al collegamento al servizio, consulta Raccomandazioni sulla larghezza di banda.
- Fornisci fibra monomodale (SMF) con Lucent Connector (LC), fibra multimodale (MMF) o MMF con LC. OM4
- Provvedi a fornire uno o due dispositivi upstream, che possono essere switch o router. Consigliamo due dispositivi per garantire un'elevata disponibilità.

Elenco di controllo di preparazione della rete

Utilizza questo elenco di controllo quando raccogli le informazioni per la configurazione del tuo Outpost. Ciò include la LAN, la WAN e tutti i dispositivi compresi tra Outpost e le destinazioni del traffico locale e la destinazione nella regione. AWS

Velocità di uplink, porte e fibra

Velocità e porte di uplink

Un Outpost dispone di due dispositivi di rete Outpost che si collegano alla rete locale. Il numero di uplink che può supportare ogni dispositivo dipende dalle esigenze di larghezza di banda e da ciò che il router è in grado di supportare. Per ulteriori informazioni, consulta Connettività fisica.

L'elenco seguente mostra il numero di porte uplink supportate per ogni dispositivo di rete Outpost, in base alla velocità di uplink.

1 Gb/s

1, 2, 4, 6 o 8 uplink

10 Gb/s

- 1, 2, 4, 8, 12 o 16 uplink

40 Gb/s o 100 Gb/s

- 1, 2 o 4 uplink

Fibra

Sono supportati i seguenti tipi di fibra:

- Fibra monomodale (SMF) con connettore Lucent (LC)
- Fibra multimodale (MMF) o MMF con LC OM4

A seconda della velocità di uplink e del tipo di fibra scelto, sono supportati i seguenti standard ottici.

Velocità di uplink	Tipo di fibra	Standard ottico
1 Gb/s	SMF	— 1000 Base-LX
1 Gb/s	MMF	— 1000 Base-SX
10 Gb/s	SMF	— 10 GBASE-IR — 10 GBASE-LR
10 Gb/s	MMF	— 10 GBASE-SR
40 Gb/s	SMF	— BASE DA 40 G - (L) IR4 LR4 — BASE DA 40 G- LR4
Applicazione di ripartizione 4 x 10 Gb/s	MMF	— BASE DA 40 G- ESR4 — BASE DA 40 G- SR4
100 Gb/s	SMF	— 100 G MSA PSM4 — 100 G BASE- CWDM4

Velocità di uplink	Tipo di fibra	Standard ottico
		— 100 G BASE- LR4
Applicazione di ripartizione 4 x 25 Gb/s	MMF	— 100 G BASE- SR4

Aggregazione di link Outpost e VLANs

È necessario il protocollo LACP (Link Aggregation Control Protocol) tra l'Outpost e la rete. È necessario utilizzare il LAG dinamico con LACP.

Quanto segue VLANs è necessario per ogni dispositivo di rete Outpost. Per ulteriori informazioni, consulta Virtuale LANs.

Dispositivo di rete Outpost	VLAN del collegamento al servizio	VLAN del gateway locale
N. 1	Valori validi: 1-4094	Valori validi: 1-4094
N. 2	Valori validi: 1-4094	Valori validi: 1-4094

Per ogni dispositivo di rete Outpost, puoi scegliere se utilizzare lo stesso dispositivo VLANs o uno diverso VLANs per il collegamento di servizio e il gateway locale. Tuttavia, consigliamo di avere una VLAN per ogni dispositivo di rete Outpost diversa dall'altro dispositivo di rete Outpost. Per ulteriori informazioni, consulta Link aggregation e Virtual. LANs

Consigliamo inoltre una connettività ridondante di livello 2. Il protocollo LACP viene utilizzato per l'aggregazione dei collegamenti e non per l'elevata disponibilità. Il protocollo LACP tra i dispositivi di rete Outpost non è supportato.

Connettività IP dei dispositivi di rete Outpost

Ciascuno dei due dispositivi di rete Outpost richiede un CIDR e un indirizzo IP per il collegamento di servizio e il gateway locale. VLANs Consigliamo di allocare una sottorete dedicata per ogni dispositivo di rete con un CIDR /30 o /31. Specifica una sottorete e un indirizzo IP dalla sottorete da utilizzare con Outpost. Per ulteriori informazioni, consulta Connettività a livello di rete.

Dispositivo di rete Outpost	Requisiti del collegamento al servizio	Requisiti del gateway locale
N. 1	— CIDR del collegamento al servizio (/30 o /31) — Indirizzo IP del collegamento al servizio	— CIDR del gateway locale (/30 o /31) — Indirizzo IP del gateway locale
N. 2	— CIDR del collegamento al servizio (/30 o /31) — Indirizzo IP del collegamento al servizio	— CIDR del gateway locale (/30 o /31) — Indirizzo IP del gateway locale

Unità di trasmissione massima (MTU) del collegamento al servizio

La rete deve supportare MTU da 1500 byte tra Outpost e gli endpoint di service link nella regione principale. AWS Per ulteriori informazioni sul collegamento al servizio, consulta AWS Outposts connettività verso AWS le regioni.

Border Gateway Protocol (BGP) del collegamento al servizio

L'Outpost stabilisce una sessione di peering BGP esterna (eBGP) tra ogni dispositivo di rete Outpost e il tuo dispositivo di rete locale per la connettività del collegamento al servizio sulla relativa VLAN. Per ulteriori informazioni, consulta Connettività BGP del collegamento al servizio.

Outpost	Requisiti BGP del collegamento al servizio
Il tuo Outpost	— Numero di sistema autonomo (ASN) del BGP Outpost. 2 byte (16 bit) o 4 byte (32 bit). Dal tuo intervallo ASN privato (64512-65534 o 4200000000-4294967294). — CIDR dell'infrastruttura (/26 obbligatorio, propagato come due /27 contigui).

Dispositivo di rete locale	Requisiti BGP del collegamento al servizio
N. 1	— Indirizzo IP peer BGP del collegamento al servizio. — ASN BGP del collegamento di servizio. 2 byte (16 bit) o 4 byte (32 bit).
N. 2	— Indirizzo IP peer BGP del collegamento al servizio. — ASN BGP del collegamento al servizio. 2 byte (16 bit) o 4 byte (32 bit).

Firewall del collegamento di servizio

UDP e TCP 443 devono essere elencati in modalità stateful nel firewall.

Protocollo	Porta di origine	Indirizzo di origine	Porta di destinazione	Indirizzo di destinazione
UDP	443	Collegamento al servizio Outpost /26	443	Routing pubblici della regione
TCP	1025-65535	Collegamento al servizio Outpost /26	443	Routing pubblici della regione

Puoi utilizzare una AWS Direct Connect connessione o una connessione Internet pubblica per ricollegare Outpost alla regione. AWS Per la connettività del collegamento al servizio Outpost puoi utilizzare NAT o PAT sul firewall o sul router edge. La creazione del collegamento al servizio viene sempre avviata dall'Outpost.

Per ulteriori informazioni sui requisiti del collegamento di servizio, ad esempio MTU e una latenza di 175 ms, vedi Connettività tramite collegamento al servizio.

Border Gateway Protocol (BGP) del gateway locale

L'Outpost stabilisce una sessione di peering eBGP da ogni dispositivo di rete Outpost a un dispositivo di rete locale per la connettività dalla tua rete locale al gateway locale. Per ulteriori informazioni, consulta Connettività BGP del gateway locale.

Outpost	Requisiti BGP del gateway locale
Il tuo Outpost	— Numero di sistema autonomo (ASN) del BGP Outpost. 2 byte (16 bit) o 4 byte (32 bit). Dal tuo intervallo ASN privato (64512-65534 o 4200000000-4294967294). — CIDR CoIP per la propagazione (pubblico o privato, minimo /26).

Dispositivi di rete locale	Requisiti BGP del gateway locale
N. 1	— Indirizzo IP peer BGP del gateway locale. — ASN peer BGP del gateway locale. 2 byte (16 bit) o 4 byte (32 bit).
N. 2	— Indirizzo IP peer BGP del gateway locale. — ASN peer BGP del gateway locale. 2 byte (16 bit) o 4 byte (32 bit).

Alimentazione

Il blocco alimentatore di Outposts supporta tre configurazioni di alimentazione: 5 kVA, 10 kVA o 15 kVA. La configurazione del blocco alimentatore dipende dalla potenza totale assorbita dalla capacità dell'Outpost. Ad esempio, se la risorsa Outpost ha un assorbimento energetico massimo di 9,7 kVA, è necessario fornire le configurazioni di alimentazione per 10 kVA: 4 x L6-30P o IEC3 09, 2 cadute su S1 e 2 gocce su S2 per l'alimentazione ridondante monofase. Le tre configurazioni di alimentazione sono descritte nella seconda tabella seguente.

Per visualizzare i requisiti di consumo energetico per le diverse risorse Outpost, scegli Sfoglia il catalogo nella console all'indirizzo. AWS Outposts https://console.aws.amazon.com/outposts/

Requisito	Specifiche
Tensione di rete CA	Monofase da 208 a 277 VAC; 50 o 60 Hz Trifase: • da 208 a 250 VAC (Delta); da 50 a 60 Hz • Da 346 a 480 VAC (Wye); da 50 a 60 Hz
Consumo energetico	5 kVA (4 kW), 10 kVA (9 kW) o 15 kVA (13 kW)
Protezione CA (interruttori a monte)	Sia per l'ingresso 1N (non ridondante) che per l'ingresso 2N (ridondante): 30 A, 32 A o 50 A con interruttore automatico con curva D o curva K. Solo per l'ingresso 2N (ridondante): interruttore automatico con curva C, curva D o curva K. La curva B o inferiore non è supportata.
Tipo di ingresso CA (presa)	Spine monofase 3xL6-30P, P+P+E, 30A o 3x 0309 P+N+E, 32A IEC6 IP67 Trifase, Wye 1x IEC6 0309, 3P+N+E, posizione orologio 7, spina 30A o 1x 0309, 3P+N+E, posizione orologio 6, spina 32A IP67 IEC6 IP67 Twistlock Delta CS8365 1xNEMA Twistlock C, 3P+E, messa a terra centrale, spina 50A **Note** La migliore pratica consiste nell'accoppiare una spina IP67 con una presa. IP67 Se ciò non è possibile, la IP67 spina si accoppierà con una IP44 presa. La potenza

Requisito	Specifiche
	nominale della spina e della presa combinate diventerà la valutazione inferiore (IP44).
Lunghezza cavo a frusta	3 m (10,25 piedi)
Cavo a frusta - Ingresso di cablaggio per rack	Dalla parte superiore o dalla parte inferiore del rack

Il blocco alimentatore dispone di due ingressi, S1 e S2, che possono essere configurati come segue.

	Ridondante, monofase	Ridondante, trifase	Monofase	Trifase
5 kVA	2 x L6-30P o IEC3 09; 1 goccia su S1 e 1 goccia su S2	2 x AH530P7W, AH532P6W o CS8365C; 1 goccia su S1 e 1 goccia su S2	Non offerto	1 x AH530P7W, AH532P6W o CS8365C; 1 passaggio a S1
10 kVA	4 x L6-30P o IEC3 09; 2 gocce su S1 e 2 gocce su S2		2 x L6-30P o 09; 2 gocce su S1 IEC3	
15 kVA	6 x L6-30P o IEC3 09; 3 gocce su S1 e 3 gocce su S2		3 x L6-30P o 09; 3 gocce su S1 IEC3	

Se le fruste AC AWS fornite come descritto in precedenza devono essere dotate di una presa di alimentazione alternativa, considerate quanto segue:

- Solo un elettricista qualificato incaricato dal cliente può modificare il cavo a frusta CA per il collegamento di un nuovo tipo di spina.
- L'installazione deve essere conforme a tutti i requisiti di sicurezza nazionali, statali e locali applicabili ed essere ispezionata come previsto per la sicurezza elettrica.
- Il cliente deve notificare al proprio AWS rappresentante le modifiche apportate alla presa AC Whip. Su richiesta, fornirai informazioni sulle modifiche apportate a. AWS Inoltre, dovrà includere tutte

le registrazioni delle ispezioni di sicurezza emesse dall'autorità competente. Questo è un requisito per la convalida della sicurezza dell'installazione prima che il personale di AWS esegua i lavori sull'apparecchiatura.

Evasione dell'ordine

Per evadere l'ordine, AWS fisseremo una data e un'ora con te. L'utente riceverà inoltre un elenco di controllo degli elementi da verificare o fornire prima dell'installazione.

Il team di AWS installazione arriverà sul tuo sito alla data e all'ora previste. Posizioneranno il rack nella posizione identificata. L'utente e il suo elettricista sono responsabili dell'esecuzione del collegamento elettrico e dell'installazione sul rack.

È necessario assicurarsi che gli impianti elettrici e le eventuali modifiche a tali impianti vengano eseguite da un elettricista qualificato in conformità con tutte le leggi, i codici e le best practice applicabili. È necessario ottenere l'approvazione scritta prima di apportare modifiche all'hardware di Outpost o agli impianti elettrici. AWS L'utente si impegna a fornire AWS la documentazione che verifichi la conformità e la sicurezza di eventuali modifiche. AWS non è responsabile dei rischi creati dall'impianto elettrico o dal cablaggio elettrico della struttura Outpost o da eventuali modifiche. È fatto divieto di apportare altre modifiche all'hardware Outposts.

Il team stabilirà la connettività di rete per il rack tramite l'uplink fornito dall'utente e configurerà la capacità del rack.

L'installazione è completa quando confermi che la capacità Amazon EC2 e Amazon EBS per il tuo rack Outposts è disponibile presso il tuo. Account AWS

Requisiti del sito per i rack Outpost ACE

> **Note**
>
> Si applica solo se è necessario un rack ACE.

Un rack Aggregation, Core, Edge (ACE) funge da punto di aggregazione di rete per le implementazioni Outpost multi-rack. È necessario installare un rack ACE se si dispone di quattro o più rack di elaborazione. Se disponi di meno di quattro rack di elaborazione ma prevedi di espanderli a quattro o più rack in futuro, ti consigliamo di installare un rack ACE.

Per installare un rack ACE, è necessario soddisfare i requisiti di questa sezione oltre ai requisiti elencati inRequisiti del sito per i rack Outposts.

> **Note**
>
> I rack ACE non sono completamente chiusi e non includono una porta anteriore o una porta posteriore.

Struttura

Questi sono i requisiti di struttura per un rack ACE.

- Alimentazione: tutti i rack ACE vengono forniti con connettori monofase da 10 kVA (tipi di connettori AA+BB; IEC6 0309 o L6-30P Whip).
- Supporto per i pesi: il rack ACE pesa 320 kg (705 libbre).
- Dimensioni e spazio libero: il rack ACE è alto 80 pollici (203 cm), largo 24 pollici (61 cm) e profondo 42 pollici (107 cm).

  Se il rack ACE è dotato di bracci per la gestione dei cavi, la larghezza del rack è di 36 pollici (91,5 cm).

Rete

Questi sono i requisiti di rete per un rack ACE. Per capire come il rack ACE collega i dispositivi di rete Outposts, i dispositivi di rete locali e i rack Outposts, consulta. Connettività rack ACE

- Requisiti della rete rack: assicurati di soddisfare i requisiti elencati nelle Connettività di rete locale per i rack Outposts sezioni Elenco di controllo di preparazione della rete e, ad eccezione delle seguenti modifiche:
  - Il rack ACE dispone di quattro dispositivi di rete che si collegano ai dispositivi upstream, non due come nel caso di un singolo rack Outposts.
  - I rack ACE non supportano uplink da 1 Gbps.
- Velocità di uplink: fornisci uplink con velocità di 10 Gbps, 40 Gbps o 100 Gbps. Per consigli sulla larghezza di banda per la connessione al service link,. Raccomandazioni sulla larghezza di banda dei collegamenti al servizio

> **Important**
>
> I rack ACE non supportano uplink da 1 Gbps.

- Fibra: fornisce fibra monomodale (SMF) con Lucent Connector (LC) o fibra multimodale (MMF) con Lucent Connector (LC). Per l'elenco completo dei tipi di fibre e degli standard ottici supportati, consulta. Velocità di uplink, porte e fibra
- Dispositivo upstream: fornisce due o quattro dispositivi upstream, che possono essere switch o router.
- Service VLAN e Local Gateway VLAN: per ciascuno dei quattro dispositivi di rete ACE è necessario fornire una Service VLAN e una VLAN Local Gateway diversa. È possibile scegliere di fornire solo due dispositivi di rete ACE distinti VLANs, uno per il Service VLAN e uno per il gateway locale, oppure disporre di dispositivi di rete ACE diversi VLANs per Service VLAN e LGW VLAN per un totale di 8 diversi. VLANs Per ulteriori informazioni su come vengono utilizzati i gruppi di aggregazione dei link (LAGs) e la VLAN, consulta e. Aggregazione dei collegamenti Virtuale LANs
- CIDR e indirizzo IP per il collegamento al servizio e il gateway locale VLANs: consigliamo di allocare una sottorete dedicata per ogni dispositivo di rete ACE con un CIDR /30 o /31. In alternativa, è possibile allocare una singola sottorete /29 in ogni Service e Local Gateway VLAN. In entrambi i casi, è necessario specificare gli indirizzi IP da utilizzare per i dispositivi di rete ACE. Per ulteriori informazioni, consulta Connettività a livello di rete.

- Numero di sistema autonomo (ASN) BGP del cliente e dell'Outpost per la VLAN di collegamento di servizio e una VLAN gateway locale: Outpost stabilisce una sessione di peering BGP (eBGP) esterna tra ogni dispositivo rack ACE e il dispositivo di rete locale per la connettività del collegamento di servizio tramite la VLAN del collegamento di servizio. Inoltre, stabilisce una sessione di peering eBGP da ogni dispositivo di rete ACE a un dispositivo di rete locale per la connettività dalla rete locale al gateway locale. Per ulteriori informazioni, consultare Connettività BGP del collegamento al servizio e Connettività BGP del gateway locale.

> **Important**
>
> Sottoreti dell'infrastruttura di collegamento ai servizi: è richiesta una sottorete dell'infrastruttura di collegamento ai servizi (deve essere /26) per ogni rack di elaborazione incluso nell'installazione di Outposts.

Alimentazione

Questi sono i requisiti di alimentazione per un rack ACE.

Requisito	Specifiche
Tensione di rete CA	Monofase da 200 a 240 VAC; 50 o 60 Hz
Consumo energetico	10 kVA monofase (AA+BB)
Protezione CA (interruttori a monte)	Solo per l'ingresso 2N (ridondante): interruttore automatico con curva C, curva D o curva K. La curva B o inferiore non è supportata.
Tipo di ingresso CA (presa)	IEC6Tipi di connettori a frusta 0309 o L6-30P.

Ordina un rack Outposts per iniziare. Dopo l'installazione delle apparecchiature Outpost, avvia un' EC2 istanza Amazon e configura la connettività alla rete locale.

Attività

- Crea un ordine per un rack Outposts
- Avvia un'istanza sul tuo rack Outposts
- Ottimizza Amazon EC2 per AWS Outposts

Crea un ordine per un rack Outposts

Per iniziare a utilizzarlo AWS Outposts, devi creare un Outpost e ordinare la capacità di Outpost.

Prerequisiti

- Verifica le configurazioni disponibili per i tuoi rack Outposts.
- Un sito Outpost è la posizione fisica per le tue apparecchiature Outpost. Prima di ordinare la capacità, verifica che il sito soddisfi i requisiti. Per ulteriori informazioni, consulta Requisiti del sito per i rack Outposts.
- È necessario disporre di un piano AWS Enterprise Support o di un piano AWS Enterprise On-Ramp Support.
- Determina quale Account AWS utilizzerai per creare il sito Outposts, creare Outpost ed effettuare l'ordine. Controlla l'email associata a questo account per ottenere informazioni da. AWS

Attività

- Fase 1: Creazione di un sito
- Fase 2: Creazione di un Outpost
- Fase 3: Effettuazione dell'ordine
- Fase 4: Modificare la capacità dell'istanza
- Passaggi successivi

Fase 1: Creazione di un sito

Crea un sito per specificare l'indirizzo operativo. L'indirizzo operativo è la sede fisica dei rack Outposts.

Prerequisiti

- Determina l'indirizzo operativo.

Per creare un sito

1. Accedi a AWS.
2. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
3. Per selezionare il genitore Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
4. Nel riquadro di navigazione, scegli Siti.
5. Seleziona Crea sito.
6. Per Tipo di hardware supportato, scegli Rack e server.
7. Inserisci un nome, una descrizione e un indirizzo operativo per il tuo sito.
8. Per Dettagli del sito, fornisci le informazioni richieste sul sito.
   - Peso massimo: il peso massimo del rack che questo sito può supportare, in libbre.
   - Assorbimento di potenza: la potenza assorbita disponibile nel punto di posizionamento dell'hardware del rack, in kVA.
   - Opzione alimentazione: l'opzione di alimentazione che è possibile fornire per l'hardware.
   - Connettore di alimentazione: il connettore di alimentazione che AWS deve fornire per i collegamenti all'hardware.
   - Caduta di potenza feed: indica se l'alimentazione arriva al di sopra o al di sotto del rack.
   - Velocità uplink: la velocità di uplink che il rack deve supportare per la connessione alla regione, in Gbit/s.
   - Numero di uplink: il numero di uplink per ogni dispositivo di rete Outpost che intendi utilizzare per connettere il rack alla rete.
   - Tipo di fibra: il tipo di fibra che verrà utilizzato per collegare il rack alla rete.
   - Standard ottico: il tipo di standard ottico che verrà utilizzato per collegare il rack alla rete.
9. (Facoltativo) Nelle note del sito, inserisci qualsiasi altra informazione che potrebbe essere utile per conoscere il sito. AWS
10. Leggi i requisiti della struttura, quindi seleziona Ho letto i requisiti della struttura.
11. Seleziona Crea sito.

Fase 2: Creazione di un Outpost

Crea un Outpost per i tuoi rack. Quindi, specifica questo Outpost quando effettui l'ordine.

Prerequisiti

- Determina la zona di AWS disponibilità da associare al tuo sito.

Per creare un Outpost

1. Nel riquadro di navigazione, scegli Outposts.
2. Seleziona Crea outpost.
3. Seleziona Rack.
4. Immetti un nome e una descrizione per l'Outpost.
5. Scegli una zona di disponibilità per il tuo Outpost.
6. (Facoltativo) Per configurare la connettività privata, seleziona Usa connettività privata. Scegli un VPC e una sottorete nella stessa Account AWS zona di disponibilità del tuo Outpost. Per ulteriori informazioni, consulta the section called “Prerequisiti”.

   > **Note**
   >
   > Se devi rimuovere la connettività privata per Outpost, devi contattare Center.Supporto AWS

7. Per ID sito, scegli il tuo sito.
8. Seleziona Crea outpost.

Fase 3: Effettuazione dell'ordine

Effettua un ordine per i rack Outposts di cui hai necessità.

> **Important**
>
> Non è possibile modificare un ordine dopo l'invio, pertanto consigliamo di controllare attentamente tutti i dettagli prima dell'invio. Se devi modificare un ordine, contatta il tuo AWS Account Manager.

Prerequisiti

- Decidi della modalità di pagamento dell'ordine. Puoi scegliere tra un pagamento anticipato totale, un pagamento anticipato parziale o nessun pagamento anticipato. Se scegli di non pagare tutto in anticipo, pagherai gli addebiti mensili per tutta la durata del contratto.

  I prezzi includono consegna, installazione, manutenzione del servizio dell'infrastruttura, patch e aggiornamenti software.
- Indica se l'indirizzo di consegna è diverso dall'indirizzo operativo che hai specificato per il sito.

Per effettuare un ordine

1. Nel riquadro di navigazione, scegli Ordini.
2. Scegli Effettua l'ordine.
3. Per Tipo di hardware supportato, scegli Rack.
4. Per aggiungere capacità, scegli una configurazione. Se le configurazioni disponibili non soddisfano le tue esigenze, contatta Supporto AWS Center per richiedere una configurazione di capacità personalizzata.
5. Scegli Next (Successivo).
6. Scegli Usa Outpost esistente e seleziona il tuo Outpost.
7. Scegli Next (Successivo).
8. Selezionare la durata del contratto e l'opzione di pagamento.
9. Specifica l'indirizzo di spedizione. Puoi specificare un nuovo indirizzo o selezionare l'indirizzo operativo del sito. Se selezioni l'indirizzo operativo, tieni presente che eventuali modifiche future all'indirizzo operativo del sito non si propagheranno agli ordini esistenti. Se hai bisogno di modificare il nome e l'indirizzo del luogo di spedizione di un ordine esistente, contatta il tuo AWS Account Manager.
10. Scegli Next (Successivo).
11. Nella pagina Verifica e ordina, verifica che i tuoi dati siano corretti e modificali secondo necessità. Non potrai modificare l'ordine dopo averlo inviato.
12. Scegli Effettua l'ordine.

Fase 4: Modificare la capacità dell'istanza

Un Outpost fornisce un pool di capacità di AWS elaborazione e archiviazione presso il sito come estensione privata di una zona di disponibilità in una AWS regione. Poiché la capacità di elaborazione e archiviazione disponibile in Outpost è limitata e determinata dalle dimensioni e dal numero di rack AWS installati nel tuo sito, sei tu a decidere la quantità di capacità di Amazon, Amazon EBS e Amazon S3 necessaria per eseguire i carichi di lavoro iniziali, EC2 far fronte alle crescite future e fornire AWS Outposts capacità aggiuntiva per mitigare i guasti dei server e gli eventi di manutenzione.

La capacità di ogni nuovo ordine di Outpost è configurata con una configurazione di capacità predefinita. Puoi convertire la configurazione predefinita per creare varie istanze per soddisfare le tue esigenze aziendali. A tale scopo, è necessario creare un task relativo alla capacità, specificare le dimensioni e la quantità delle istanze ed eseguire il task relativo alla capacità per implementare le modifiche.

> **Note**
>
> - Puoi modificare la quantità di dimensioni delle istanze dopo aver effettuato l'ordine per i tuoi Outposts.
> - Le dimensioni e le quantità delle istanze sono definite a livello di Outpost.
> - Le istanze vengono posizionate automaticamente in base alle migliori pratiche.

Per modificare la capacità delle istanze

1. Dal riquadro di navigazione a sinistra della AWS Outposts console, scegli Attività relative alla capacità.
2. Nella pagina Attività di capacità, scegli Crea attività di capacità.
3. Nella pagina Guida introduttiva, scegli l'ordine.
4. Per modificare la capacità, puoi utilizzare i passaggi nella console o caricare un file JSON.

Console steps

1. Scegli Modifica una configurazione di capacità di Outpost.
2. Scegli Next (Successivo).

3. Nella pagina Configura la capacità dell'istanza, ogni tipo di istanza mostra una dimensione di istanza con la quantità massima preselezionata. Per aggiungere altre dimensioni di istanza, scegli Aggiungi dimensione dell'istanza.
4. Specificate la quantità dell'istanza e annotate la capacità visualizzata per quella dimensione dell'istanza.
5. Visualizza il messaggio alla fine di ogni sezione relativa al tipo di istanza che ti informa se la capacità è eccessiva o insufficiente. Effettua modifiche a livello di dimensione o quantità dell'istanza per ottimizzare la capacità totale disponibile.
6. Puoi anche richiedere di AWS Outposts ottimizzare la quantità di istanze per una dimensione specifica dell'istanza. A tale scopo:
   a. Scegli la dimensione dell'istanza.
   b. Scegli Bilanciamento automatico alla fine della sezione relativa al tipo di istanza.
7. Per ogni tipo di istanza, assicurati che la quantità di istanza sia specificata per almeno una dimensione di istanza.
8. Scegli Next (Successivo).
9. Nella pagina Rivedi e crea, verifica gli aggiornamenti richiesti.
10. Scegli Crea. AWS Outposts crea un'attività di capacità.
11. Nella pagina dell'attività di capacità, monitora lo stato dell'attività.

> **Note**
>
> - AWS Outposts potrebbe richiedere di interrompere una o più istanze in esecuzione per consentire l'esecuzione del task di capacità. Dopo aver interrotto queste istanze, AWS Outposts eseguirà l'operazione.
> - Se hai bisogno di modificare la tua capacità dopo aver completato l'ordine, contatta Supporto AWS Center per apportare le modifiche.

Upload a JSON file

1. Scegli Carica una configurazione di capacità.
2. Scegli Next (Successivo).
3. Nella pagina del piano di configurazione della capacità di caricamento, carica il file JSON che specifica il tipo, la dimensione e la quantità dell'istanza.

Example

File JSON di esempio:

```
{
    "InstancePools": [
        {
            "InstanceType": "c5.24xlarge",
            "Count": 1
        },
        {
            "InstanceType": "m5.24xlarge",
            "Count": 2
        }
    ]
}
```

4. Esamina il contenuto del file JSON nella sezione Piano di configurazione della capacità.
5. Scegli Next (Successivo).
6. Nella pagina Rivedi e crea, verifica gli aggiornamenti che stai richiedendo.
7. Scegli Crea. AWS Outposts crea un'attività di capacità.
8. Nella pagina dell'attività di capacità, monitora lo stato dell'attività.

> **Note**
>
> - AWS Outposts potrebbe richiedere di interrompere una o più istanze in esecuzione per consentire l'esecuzione del task di capacità. Dopo aver interrotto queste istanze, AWS Outposts eseguirà l'operazione.
> - Se hai bisogno di modificare la tua capacità dopo aver completato l'ordine, contatta Supporto AWS Center per apportare le modifiche.
> - Per risolvere i problemi, consulta Risoluzione dei problemi relativi alle attività relative alla capacità.

Passaggi successivi

Puoi visualizzare lo stato del tuo ordine utilizzando la AWS Outposts console. Lo stato iniziale del tuo ordine è Ordine ricevuto. Se hai domande sul tuo ordine, contatta il Supporto AWS Centro.

Per evadere l'ordine, AWS fisseremo una data e un'ora con te.

L'utente riceverà inoltre un elenco di controllo degli elementi da verificare o fornire prima dell'installazione. Il team di AWS installazione arriverà sul tuo sito alla data e all'ora previste. Il team sposterà il rack fino alla posizione individuata e il tuo elettricista potrà collegarlo all'alimentazione. Il team stabilirà la connettività di rete per il rack tramite l'uplink fornito da te e configurerà la capacità del rack. L'installazione è completa quando confermi che la capacità Amazon EC2 e Amazon EBS per Outpost è disponibile dal tuo AWS account.

Avvia un'istanza sul tuo rack Outposts

Dopo aver installato Outpost e aver reso disponibile la capacità di calcolo e storage, puoi iniziare a creare risorse. Avvia EC2 istanze Amazon e crea volumi Amazon EBS sul tuo Outpost utilizzando una sottorete Outpost. Puoi anche creare snapshot dei volumi Amazon EBS sull'Outpost. Per ulteriori informazioni, consulta gli snapshot locali di Amazon EBS AWS Outposts nella Amazon EBS User Guide.

Prerequisito

Devi avere un Outpost installato presso il tuo sito. Per ulteriori informazioni, consulta Creare un ordine per un rack Outposts.

Attività

- Fase 1. Creazione di un VPC
- Passaggio 2: crea una sottorete e una tabella di routing personalizzata
- Fase 3: Configurare la connettività del gateway locale
- Fase 4: Configurare la rete locale
- Passaggio 5: avvia un'istanza su Outpost
- Passaggio 6: verifica la connettività

Fase 1. Creazione di un VPC

Puoi estendere qualsiasi VPC della AWS regione al tuo avamposto. Salta questo passaggio se hai già un VPC che puoi usare.

Per creare un VPC per il tuo avamposto

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Scegli la stessa regione del rack Outposts.
3. Nel riquadro di navigazione, scegli Tuo VPCs, quindi scegli Crea VPC.
4. Scegli solo VPC.
5. (Facoltativo) per il tag Nome, inserisci un nome per il VPC.
6. Per il blocco IPv4 CIDR, scegli l'immissione manuale IPv4 CIDR e inserisci l'intervallo di IPv4 indirizzi per il VPC nella casella di testo CIDR. IPv4

   > **Note**
   >
   > Se desideri utilizzare il routing VPC diretto, specifica un intervallo CIDR che non si sovrapponga all'intervallo IP utilizzato nella rete locale.

7. Per il blocco IPv6 CIDR, scegli Nessun blocco CIDR. IPv6
8. Per Tenancy, scegli Predefinito.
9. (Facoltativo) Per aggiungere un tag al tuo VPC, scegli Aggiungi tag e inserisci una chiave e un valore.
10. Seleziona Crea VPC.

Passaggio 2: crea una sottorete e una tabella di routing personalizzata

Puoi creare e aggiungere una sottorete Outpost a qualsiasi VPC nella AWS regione in cui è ospitato l'Outpost. Quando lo fai, il VPC include Outpost. Per ulteriori informazioni, consulta Componenti di rete.

> **Note**
>
> Se stai avviando un'istanza in una sottorete di Outpost che è stata condivisa con te da un altro utente Account AWS, vai al Passaggio 5: Avvia un'istanza su Outpost.

2a: Crea una sottorete Outpost

Per creare una sottorete Outpost

1. Apri la AWS Outposts console all'indirizzo. https://console.aws.amazon.com/outposts/
2. Nel riquadro di navigazione, scegli Outposts.
3. Seleziona l'Outpost, quindi scegli Operazioni, Crea sottorete. Verrai reindirizzato per creare una sottorete nella console Amazon VPC. Selezioniamo per te l'Outpost e la zona di disponibilità in cui risiede l'Outpost.
4. Selezionare un VPC.
5. Nelle impostazioni della sottorete, assegnate facoltativamente un nome alla sottorete e specificate un intervallo di indirizzi IP per la sottorete.
6. Scegliere Create subnet (Crea sottorete).
7. (Facoltativo) Per facilitare l'identificazione delle sottoreti Outpost, abilita la colonna Outpost ID nella pagina Sottoreti. Per abilitare la colonna, scegli l'icona Preferenze, seleziona Outpost ID e scegli Conferma.

2b: crea una tabella di percorsi personalizzata

Utilizza la procedura seguente per creare una tabella di routing personalizzata con un percorso verso il gateway locale. Non è possibile utilizzare la stessa tabella di routing delle sottoreti delle zone di disponibilità.

Per creare una tabella di routing personalizzata

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, seleziona Tabelle di routing.
3. Selezionare Create route table (Crea tabella di instradamento).
4. (Facoltativo) In Name (Nome), inserisci un nome per la tabella di instradamento.
5. In VPC, seleziona il VPC.
6. (Facoltativo) Per aggiungere un tag, scegli Add new tag (Aggiungi nuovo tag) e inserisci la chiave e il valore del tag.
7. Selezionare Create route table (Crea tabella di instradamento).

2c: associa la sottorete Outpost e la tabella di routing personalizzata

Per applicare le route delle tabelle di instradamento a una particolare sottorete, occorre associare la tabella di instradamento alla sottorete. Una tabella di instradamento possono essere associata a più sottoreti. Tuttavia, una sottorete può essere associata a una sola tabella di instradamento alla volta. Per impostazione predefinita, qualsiasi sottorete non esplicitamente associata a una tabella è implicitamente associata alla tabella di instradamento principale.

Per associare la sottorete Outpost e la tabella di routing personalizzata

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dal riquadro di navigazione, scegli Tabelle degli itinerari.
3. Nella scheda Associazioni sottorete scegli Modifica associazioni sottorete.
4. Seleziona la casella di controllo per la sottorete da associare alla tabella di instradamento.
5. Scegli Salva associazioni.

Fase 3: Configurare la connettività del gateway locale

Il gateway locale (LGW) consente la connettività tra le sottoreti Outpost e la rete locale.

Per ulteriori informazioni su LGW, consulta Local Gateways.

Per fornire la connettività tra un'istanza nella sottorete Outposts e la rete locale, è necessario completare le seguenti attività.

3a. Crea una tabella di routing del gateway locale personalizzata

Utilizzare la procedura seguente per creare una tabella di routing personalizzata per il gateway locale.

Per creare una tabella di routing del gateway locale personalizzata

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, seleziona Tabella di routing del gateway locale.
4. Seleziona Crea una tabella di routing del gateway locale.
5. (Facoltativo) In Name (Nome), inserisci un nome per la tabella di instradamento.

6. Per Gateway locale, scegli il tuo gateway locale.
7. Per Modalità, scegli una modalità di comunicazione con la rete on-premise.
   - Scegli il routing VPC diretto per utilizzare gli indirizzi IP privati delle tue istanze.
   - Scegli CoIP per utilizzare gli indirizzi dei pool di indirizzi IP di proprietà del cliente. Per ulteriori informazioni, consulta Creare un pool CoIP.
8. (Facoltativo) Per aggiungere un tag, scegli Aggiungi nuovo tag e immetti una chiave e un valore di tag.
9. Seleziona Crea una tabella di routing del gateway locale.

3b: Associa il VPC alla tabella delle rotte personalizzata

Utilizzare la procedura seguente per associare un VPC alla tabella di routing del gateway locale. Per impostazione predefinita questi non sono associati.

Per associare un VPC alla tabella di routing del gateway locale personalizzata

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, seleziona Tabelle di routing del gateway locale.
4. Seleziona la tabella di routing, quindi scegli Operazioni, Associa VPC.
5. In ID VPC, seleziona il VPC da associare alla tabella di routing del gateway locale.
6. (Facoltativo) Per aggiungere un tag, scegli Aggiungi nuovo tag e immetti una chiave e un valore di tag.
7. Scegli Associa VPC.

3c: Aggiungi una voce di percorso nella tabella delle rotte della sottorete di Outpost

Aggiungi una voce di percorso nella tabella di routing della sottorete di Outpost per abilitare il traffico tra le sottoreti Outpost e il gateway locale.

Le sottoreti Outpost all'interno di un VPC, associato a una tabella di routing del gateway locale, possono avere un tipo di destinazione aggiuntivo di un ID gateway locale Outpost per le relative tabelle di routing. Si consideri il caso in cui si desidera indirizzare il traffico con un indirizzo di destinazione 172.16.100.0/24 verso la rete del cliente attraverso il gateway locale. A tale scopo,

modifica la tabella delle rotte della sottorete di Outpost e aggiungete la seguente route con la rete di destinazione e una destinazione del gateway locale.

Destinazione	Target
172.16.100.0/24	`lgw-id`

Per aggiungere una voce di route con il gateway locale come destinazione nella tabella delle rotte di sottorete

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Tabelle di percorsi e seleziona la tabella delle rotte in 2b: crea una tabella di percorsi personalizzata cui hai creato.
3. Scegli Azioni, quindi Modifica percorsi.
4. Per aggiungere un routing scegli Aggiungi routing.
5. Per Destinazione, inserisci il blocco CIDR di destinazione nella rete del cliente.
6. Per Target, scegli Outpost Local Gateway ID.
7. Scegli Save changes (Salva modifiche).

3d: crea un dominio di routing del gateway locale associando la tabella di routing personalizzata ai gruppi VIF

I gruppi VIF sono raggruppamenti logici di interfacce virtuali (). VIFs Associate la tabella di routing del gateway locale al gruppo VIF per creare un dominio di routing del gateway locale.

Per associare la tabella di routing personalizzata ai gruppi VIF

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel pannello di navigazione, scegli Networking e quindi Dominio di routing LGW.
4. Scegli Crea dominio di routing LGW.
5. Immettete un nome per il dominio di routing del gateway locale.
6. Scegli il gateway locale, il gruppo VIF del gateway locale e la tabella di routing del gateway locale.

7. Scegli Crea dominio di routing LGW.

3e: aggiungi una voce di percorso nella tabella delle rotte

Modifica la tabella di routing del gateway locale per aggiungere una route statica con il gruppo VIF come destinazione e l'intervallo CIDR della sottorete locale (o 0.0.0.0/0) come destinazione.

Destinazione	Target
172.16.100.0/24	`VIF-Group-ID`

Per aggiungere una voce di percorso nella tabella delle rotte LGW

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Nel riquadro di navigazione, seleziona Tabella di routing del gateway locale.
3. Seleziona la tabella di routing del gateway locale, quindi scegli Azioni, Modifica rotte.
4. Scegli Aggiungi route.
5. In Destinazione immetti il blocco CIDR di destinazione, un singolo indirizzo IP o l'ID di un elenco di prefissi.
6. In Destinazione, seleziona l'ID del gateway locale.
7. Seleziona Salva route.

3f: (Facoltativo) Assegna un indirizzo IP di proprietà del cliente all'istanza

Se hai configurato Outposts in 3a. Crea una tabella di routing del gateway locale personalizzata per utilizzare un pool di indirizzi IP (CoIP) di proprietà del cliente, devi allocare un indirizzo IP elastico dal pool di indirizzi CoIP e associare l'indirizzo IP elastico all'istanza. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente.

Se hai configurato gli Outposts per utilizzare il routing diretto VPC (DVR), salta questo passaggio.

Pool di indirizzi IP condivisi-di proprietà del cliente

Se desideri utilizzare un pool di indirizzi IP condiviso-di proprietà del cliente, il pool deve essere condiviso prima di iniziare la configurazione. Per informazioni su come condividere un indirizzo di proprietà del cliente, consulta. IPv4 the section called “Condivisione di una risorsa Outpost”

Fase 4: Configurare la rete locale

Outpost stabilisce un peering BGP esterno da ogni Outpost Networking Device (OND) a un Customer Local Network Device (CND) per inviare e ricevere traffico dalla rete locale agli Outposts.

Per ulteriori informazioni, consulta Connettività BGP tramite gateway locale.

Per inviare e ricevere traffico dalla rete locale a Outpost, assicurati che:

- Sui dispositivi di rete dei clienti, la sessione BGP sulla VLAN del gateway locale è in uno stato ATTIVO rispetto ai dispositivi di rete.
- Per il traffico che passa dagli ambienti locali agli Outposts, assicurati di ricevere nel tuo CND gli annunci BGP di Outposts. Questi annunci BGP contengono i percorsi che la rete locale deve utilizzare per indirizzare il traffico dall'ambiente locale a Outpost. Quindi, assicurati che la tua rete abbia il giusto routing tra Outposts e le risorse locali.
- Per il traffico che va da Outposts alla rete locale, assicurati di inviare gli annunci di routing BGP delle sottoreti di rete locali a Outposts (o 0.0.0.0/0). CNDs In alternativa, puoi pubblicizzare un percorso predefinito (ad esempio 0.0.0.0/0) verso Outposts. Le sottoreti locali pubblicizzate da CNDs devono avere un intervallo CIDR uguale o incluso nell'intervallo CIDR in cui è stato configurato. 3e: aggiungi una voce di percorso nella tabella delle rotte

Esempio: pubblicità BGP in modalità Direct VPC

Si consideri lo scenario in cui si dispone di un Outpost, configurato in modalità Direct VPC, con due dispositivi di rete rack Outposts collegati tramite un gateway VLAN locale a due dispositivi di rete locale del cliente. Viene configurato quanto segue:

- VPC A con un blocco CIDR 10.0.0.0/16.
- Una sottorete Outpost nel VPC con un blocco CIDR 10.0.3.0/24.
- Una sottorete nella rete locale con un blocco CIDR 172.16.100.0/24
- Outposts utilizza l'indirizzo IP privato delle istanze sulla sottorete Outpost, ad esempio 10.0.3.0/24, per comunicare con la rete locale.

In questo scenario, il percorso pubblicizzato da:

- Il gateway locale per i dispositivi dei clienti è 10.0.3.0/24.
- I dispositivi dei clienti che accedono al gateway locale Outpost sono 172.16.100.0/24.

Di conseguenza, il gateway locale invierà il traffico in uscita con la rete di destinazione 172.16.100.0/24 ai dispositivi dei clienti. Assicurati che la tua rete abbia la configurazione di routing corretta per fornire il traffico all'host di destinazione all'interno della tua rete.

Per i comandi e la configurazione specifici necessari per verificare lo stato delle sessioni BGP e i percorsi pubblicizzati all'interno di tali sessioni, consultate la documentazione del fornitore della rete.

Per la risoluzione dei problemi, consulta la checklist per la risoluzione dei problemi relativi alla rete AWS Outposts rack.

Esempio: pubblicità BGP in modalità CoIP

Si consideri lo scenario in cui si dispone di un Outpost con due dispositivi di rete rack Outposts collegati tramite un gateway VLAN locale a due dispositivi di rete locale del cliente. Viene configurato quanto segue:

- VPC A con un blocco CIDR 10.0.0.0/16.
- Una sottorete nel VPC con un blocco CIDR 10.0.3.0/24.
- Pool di IP di proprietà del cliente (10.1.0.0/26).
- Un'associazione di indirizzi IP elastici che lega 10.0.3.112 a 10.1.0.2.
- Una sottorete nella rete locale con un blocco CIDR 172.16.100.0/24
- La comunicazione tra Outpost e la rete locale utilizzerà CoIP Elastic IPs per indirizzare le istanze in Outpost, l'intervallo VPC CIDR non viene utilizzato.

In questo scenario, il percorso pubblicizzato da:

- Il gateway locale per i dispositivi dei clienti è 10.1.0.0/26.
- I dispositivi dei clienti che accedono al gateway locale Outpost sono 172.16.100.0/24.

Di conseguenza, il gateway locale invierà il traffico in uscita con la rete di destinazione 172.16.100.0/24 ai dispositivi dei clienti. Assicurati che la tua rete abbia la giusta configurazione di routing per fornire il traffico all'host di destinazione all'interno della tua rete.

Per i comandi e la configurazione specifici necessari per verificare lo stato delle sessioni BGP e i percorsi pubblicizzati all'interno di tali sessioni, consultate la documentazione del fornitore della rete.

Per la risoluzione dei problemi, consulta la checklist per la risoluzione dei problemi relativi alla rete AWS Outposts rack.

Per la risoluzione dei problemi, consulta la checklist per la risoluzione dei problemi relativi alla rete AWS Outposts rack.

Passaggio 5: avvia un'istanza su Outpost

Puoi avviare EC2 le istanze nella sottorete Outpost che hai creato o in una sottorete Outpost che è stata condivisa con te. I gruppi di sicurezza controllano il traffico VPC in entrata e in uscita per le istanze di una sottorete Outpost, proprio come per le istanze di una sottorete zona di disponibilità. Per connetterti a un' EC2 istanza in una sottorete Outpost, puoi specificare una coppia di key pair all'avvio dell'istanza, proprio come per le istanze in una sottorete della zona di disponibilità.

Considerazioni

- Se stai collegando volumi di dati a blocchi supportati da sistemi di storage a blocchi di terze parti compatibili durante il processo di avvio dell'istanza su Outpost, consulta questo post del blog Semplificazione dell'uso dello storage a blocchi di terze parti con. AWS Outposts
- Puoi creare un gruppo di collocamento per influenzare il modo in cui Amazon EC2 dovrebbe tentare di collocare gruppi di istanze interdipendenti sull'hardware Outposts. Puoi scegliere la strategia del gruppo di collocazione che soddisfa le esigenze del tuo carico di lavoro.
- Se Outpost è stato configurato per utilizzare un pool di indirizzi IP (CoIP) di proprietà del cliente, devi assegnare un indirizzo IP di proprietà del cliente a tutte le istanze che avvii.

Per avviare istanze nella tua sottorete Outpost.

1. Apri la console all' AWS Outposts indirizzo. https://console.aws.amazon.com/outposts/
2. Nel riquadro di navigazione, scegli Outposts.
3. Seleziona l'Outpost, quindi scegli Operazioni, Visualizza i dettagli.
4. Nella pagina Riepilogo outpost, scegli Avvia istanza. Verrai reindirizzato alla procedura guidata di avvio dell'istanza nella console Amazon EC2. Selezioniamo la sottorete Outpost per te e ti mostriamo solo i tipi di istanza supportati dal tuo rack Outposts.
5. Scegli un tipo di istanza supportato dal rack Outposts. Tieni presente che le istanze che appaiono in grigio non sono disponibili.
6. (Facoltativo) Per avviare le istanze in un gruppo di collocazione, espandi Dettagli avanzati e scorri fino al Gruppo di collocazione. È possibile selezionare un gruppo di collocazione esistente o crearne uno nuovo.

7. Completa la procedura guidata per avviare l'istanza nella sottorete Outpost. Per ulteriori informazioni, consulta Launch an EC2 istance nella Amazon EC2 User Guide:

> **Note**
>
> Se aggiungi un volume Amazon EBS, devi usare il tipo di volume gp2.

Passaggio 6: verifica la connettività

È possibile testare la connettività utilizzando i casi di utilizzo opportuni.

Test della connettività dalla rete locale all'Outpost

Da un computer della rete locale, esegui il `ping` comando sull'indirizzo IP privato dell'istanza Outpost.

```
ping 10.0.3.128
```

Di seguito è riportato un output di esempio.

```
Pinging 10.0.3.128

Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Test della connettività da un'istanza Outpost alla rete locale

A seconda del sistema operativo, utilizza ssh o rdp per connetterti all'indirizzo IP privato dell'istanza Outpost. Per informazioni sulla connessione a un'istanza Linux, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.

Dopo l'esecuzione dell'istanza, esegui il comando `ping` su un indirizzo IP di un computer nella rete locale. In questo esempio, l'indirizzo IP è 172.16.0.130.

```
ping 172.16.0.130
```

Di seguito è riportato un output di esempio.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Verifica la connettività tra la AWS regione e Outpost

Avvia un'istanza nella sottorete della AWS regione. Ad esempio, utilizza il comando run-instances.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Dopo aver eseguito l'istanza, esegui le operazioni descritte di seguito:

1. Ottieni l'indirizzo IP privato dell'istanza nella AWS regione. Queste informazioni sono disponibili nella EC2 console Amazon nella pagina dei dettagli dell'istanza.
2. A seconda del sistema operativo, utilizza ssh o rdp per connetterti all'indirizzo IP privato dell'istanza Outpost.
3. Esegui il ping comando dall'istanza Outpost, specificando l'indirizzo IP dell'istanza nella AWS regione.

   ```
   ping 10.0.1.5
   ```

   Di seguito è riportato un output di esempio.

```
Pinging 10.0.1.5

Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.1.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Esempi di connettività di indirizzi IP di proprietà del cliente

Test della connettività dalla rete locale all'Outpost

Da un computer della rete locale, esegui il comando `ping` sull'indirizzo IP di proprietà del cliente dell'istanza Outpost.

```
ping 172.16.0.128
```

Di seguito è riportato un output di esempio.

```
Pinging 172.16.0.128

Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Test della connettività da un'istanza Outpost alla rete locale

A seconda del sistema operativo, utilizza ssh o rdp per connetterti all'indirizzo IP privato dell'istanza Outpost. Per informazioni, consulta Connect to your EC2 istance nella Amazon EC2 User Guide.

Dopo l'esecuzione dell'istanza Outpost, esegui il comando `ping` su un indirizzo IP di un computer nella rete locale.

```
ping 172.16.0.130
```

Di seguito è riportato un output di esempio.

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Verifica la connettività tra la AWS regione e Outpost

Avvia un'istanza nella sottorete della AWS regione. Ad esempio, utilizza il comando run-instances.

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

Dopo aver eseguito l'istanza, esegui le operazioni descritte di seguito:

1. Ottieni l'indirizzo IP privato dell'istanza AWS Region, ad esempio 10.0.0.5. Queste informazioni sono disponibili nella EC2 console Amazon nella pagina dei dettagli dell'istanza.
2. A seconda del sistema operativo, utilizza ssh o rdp per connetterti all'indirizzo IP privato dell'istanza Outpost.
3. Esegui il `ping` comando dall'istanza Outpost all'indirizzo IP dell'istanza AWS Region.

   ```
   ping 10.0.0.5
   ```

Di seguito è riportato un output di esempio.

```
Pinging 10.0.0.5

Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.0.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

Ottimizza Amazon EC2 per AWS Outposts

A differenza di Amazon Elastic Compute Cloud (Amazon EC2) Regione AWS, la capacità di un Outpost è limitata. Sei vincolato dal volume totale di capacità di calcolo che hai ordinato. Questo argomento offre best practice e strategie di ottimizzazione per aiutarti a sfruttare al massimo la tua EC2 capacità di Amazon AWS Outposts.

Indice

- Host dedicati su Outposts
- Configurazione del ripristino dell'istanza
- Gruppi di collocazione su Outposts

Host dedicati su Outposts

Un Amazon EC2 Dedicated Host è un server fisico con una capacità di EC2 istanza completamente dedicata al tuo utilizzo. Il tuo Outpost ti offre già l'hardware dedicato, ma Host dedicati consente di utilizzare le licenze software esistenti con restrizioni di licenza per socket, per core o per VM esistenti rispetto a un singolo host. Per ulteriori informazioni, consulta Dedicated Hosts AWS Outposts nella Amazon EC2 User Guide.

Oltre alle licenze, i proprietari di Outpost possono utilizzare gli host dedicati per ottimizzare i server nelle loro implementazioni Outpost in due modi:

- Modifica del layout della capacità di un server
- Controllo del posizionamento delle istanze a livello hardware

Modifica del layout della capacità di un server

Dedicated Hosts ti offre la possibilità di modificare il layout dei server nella tua distribuzione Outpost senza contattarci Supporto. Quando acquisti capacità per Outpost, specifichi un layout di EC2 capacità fornito da ciascun server. Ogni server supporta una singola famiglia di tipi di istanze. Un layout può offrire un singolo tipo di istanza o più tipi di istanze. Host dedicati ti consente di modificare ciò che hai scelto per il layout iniziale. Se viene allocato un host per supportare un singolo tipo di istanza per l'intera capacità, è possibile avviare un solo tipo di istanza da quell'host. La seguente illustrazione presenta un server m5.24xlarge con un layout omogeneo:

È possibile allocare la stessa capacità per più tipi di istanze. Quando viene allocato un host per supportare più tipi di istanze, si ottiene un layout eterogeneo che non richiede un layout di capacità esplicito. La seguente illustrazione presenta un server m5.24xlarge con un layout eterogeneo a piena capacità:

Per ulteriori informazioni, consulta Allocate a Dedicated Host nella Amazon EC2 User Guide.

Controllo del posizionamento delle istanze a livello hardware

Puoi utilizzare Host dedicati per controllare il posizionamento delle istanze a livello hardware. Utilizza l'auto-posizionamento per Host dedicati per definire se le istanze vengono avviate su un host specifico o su qualsiasi host disponibile che presenta configurazioni corrispondenti. Utilizza l'affinità degli host per stabilire una relazione tra un'istanza e un Host dedicato. Se disponi di un rack Outposts, puoi utilizzare queste funzionalità di host dedicati per ridurre al minimo l'impatto dei guasti hardware correlati. Per ulteriori informazioni sul ripristino delle istanze, consulta Posizionamento automatico degli host dedicati e affinità degli host nella Amazon EC2 User Guide.

Puoi condividere host dedicati utilizzando. AWS Resource Access Manager La condivisione di Host dedicati consente di distribuire gli host in un'implementazione Outpost su Account AWS. Per ulteriori informazioni, consulta Risorse condivise.

Configurazione del ripristino dell'istanza

Le istanze sull'Outpost che entrano in uno stato non integro a causa di un guasto hardware devono essere migrate su un host integro. Puoi configurare il ripristino automatico in modo che questa migrazione venga eseguita automaticamente in base ai controlli dello stato dell'istanza. Per ulteriori informazioni, consulta Resilienza delle istanze.

Gruppi di collocazione su Outposts

AWS Outposts supporta i gruppi di collocamento. Utilizza i gruppi di posizionamento per influenzare il modo in cui Amazon EC2 dovrebbe tentare di collocare gruppi di istanze interdipendenti che avvii sull'hardware sottostante. Puoi utilizzare diverse strategie (cluster, partizioni o di diffusione) per soddisfare le esigenze di diversi carichi di lavoro. Se disponi di un Outpost a rack singolo, puoi utilizzare la strategia di diffusione per posizionare le istanze su host anziché su rack.

Gruppi di collocazione sparsi

Utilizza un gruppo di collocazione sparso per distribuire una singola istanza su hardware separato. L'avvio delle istanze in un gruppo di collocazione sparso riduce il rischio di errori simultanei che possono verificarsi quando le istanze condividono la stessa apparecchiatura. I gruppi di collocazione possono distribuire istanze tra rack o host. Puoi utilizzare i gruppi di collocamento distribuiti a livello di host solo con. AWS Outposts

Gruppi di collocazione a livello di diffusione di rack

Il gruppo di collocazione a livello di diffusione di rack può contenere tante istanze quanti sono i rack presenti nell'implementazione Outpost. La seguente illustrazione mostra un'implementazione Outpost su tre rack che esegue tre istanze in un gruppo di collocazione a livello di diffusione di rack.

Gruppi di collocazione a livello di diffusione di host

Il gruppo di collocazione a livello di diffusione di host può contenere tante istanze quanti sono gli host presenti nell'implementazione Outpost. La seguente illustrazione mostra un'implementazione Outpost su singolo rack che esegue tre istanze in un gruppo di collocazione a livello di diffusione di host.

Gruppi di posizionamento delle partizioni

Utilizza un gruppo di posizionamento delle partizioni per distribuire più istanze su rack dotati di partizioni. Ogni partizione può contenere più istanze. Puoi utilizzare la distribuzione automatica

per suddividere le istanze tra le partizioni o distribuire le istanze sulle partizioni di destinazione. La seguente illustrazione mostra un gruppo di posizionamento delle partizioni con distribuzione automatica.

Puoi inoltre distribuire le istanze su partizioni di destinazione. La seguente illustrazione mostra un gruppo di posizionamento delle partizioni con distribuzione mirata.

Per ulteriori informazioni su come lavorare con i gruppi di collocamento, consulta la sezione Gruppi di collocamento e Gruppi di collocamento AWS Outposts nella Amazon EC2 User Guide.

Per ulteriori informazioni sull' AWS Outposts alta disponibilità, consulta Considerazioni sulla progettazione e sull'architettura AWS Outposts ad alta disponibilità.

AWS Outposts connettività verso AWS le regioni

AWS Outposts supporta la connettività WAN (Wide Area Network) tramite la connessione service link.

Indice

- Connettività tramite collegamento al servizio
- Opzioni di connettività pubblica Service Link
- Opzioni di connettività privata Service Link
- Firewall e il collegamento al servizio
- Elenco di controllo per la risoluzione dei problemi della rete rack Outposts

Connettività tramite collegamento al servizio

Il link al servizio è una connessione necessaria tra i tuoi Outposts e la AWS regione (o la regione d'origine). Consente la gestione degli Outposts e lo scambio di traffico da e verso la AWS Regione. Il collegamento al servizio sfrutta un set crittografato di connessioni VPN per comunicare con la regione di origine.

Una volta stabilita la connessione al service link, Outpost diventa operativo ed è gestito da. AWS Il link al servizio facilita il seguente traffico:

- Traffico VPC del cliente tra Outpost e qualsiasi altro dispositivo associato. VPCs
- Outposts gestisce il traffico, ad esempio la gestione delle risorse, il monitoraggio delle risorse e gli aggiornamenti firmware e software.

Requisiti dell'unità di trasmissione massima (MTU)

L'unità massima di trasmissione (MTU) di una connessione di rete è la dimensione, in byte, del pacchetto maggiore consentito trasferibile attraverso la connessione. La rete deve supportare MTU da 1500 byte tra Outpost e gli endpoint di service link nella regione principale. AWS

Il traffico che va da un'istanza in Outposts a un'istanza nella regione ha un MTU pari a 1300.

Raccomandazioni sulla larghezza di banda dei collegamenti al servizio

Per un'esperienza e una resilienza ottimali, è AWS necessario utilizzare una connettività ridondante di almeno 500 Mbps per ogni rack di elaborazione e una latenza massima di 175 ms di andata e ritorno per la connessione del service link alla regione. AWS Per il collegamento al servizio puoi utilizzare AWS Direct Connect o una connessione Internet. I requisiti minimi di 500 Mbps e di tempo massimo di andata e ritorno per la connessione service link consentono di avviare EC2 istanze Amazon, collegare volumi Amazon EBS e accedere a AWS servizi come Amazon EKS, Amazon EMR e CloudWatch metriche con prestazioni ottimali.

I requisiti di larghezza di banda del collegamento al servizio degli Outpost variano a seconda delle caratteristiche seguenti:

- Numero di rack e configurazioni di capacità AWS Outposts
- Le caratteristiche del carico di lavoro, come le dimensioni dell'AMI, l'elasticità delle applicazioni, le esigenze di velocità di burst e il traffico Amazon VPC verso la regione.

Per ricevere un consiglio personalizzato sulla larghezza di banda del service link necessaria per le tue esigenze, contatta il tuo rappresentante di AWS vendita o il partner APN.

Connessioni Internet ridondanti

Quando crei connettività dal tuo Outpost alla AWS regione, ti consigliamo di creare più connessioni per una maggiore disponibilità e resilienza. Per ulteriori informazioni, consulta Raccomandazioni per la resilienza di AWS Direct Connect.

Se necessiti di connettività alla rete Internet pubblica, puoi utilizzare connessioni Internet ridondanti e diversi provider Internet, proprio come faresti con i carichi di lavoro on-premise esistenti.

Configura il tuo link di servizio

I passaggi seguenti spiegano il processo di configurazione del collegamento di servizio.

1. Scegli un'opzione di connessione tra i tuoi Outposts e la regione d'origine AWS . Puoi scegliere una connessione pubblica o privata.
2. Dopo aver ordinato i rack Outposts, ti AWS contatta per raccogliere VLAN, IP, BGP e la sottorete dell'infrastruttura. IPs Per ulteriori informazioni, consulta Connettività di rete locale.
3. Durante l'installazione, AWS configura il collegamento al servizio su Outpost in base alle informazioni fornite.

4. L'utente configura i dispositivi di rete locali, come i router, per connettersi a ciascun dispositivo di rete Outpost tramite la connettività BGP. Per informazioni sulla connettività VLAN, IP e BGP del service link, vedere. Rete
5. È possibile configurare i dispositivi di rete, come i firewall, per consentire agli Outposts di accedere alla regione o AWS alla regione di residenza. AWS Outposts utilizza la sottorete Service Link Infrastructure IPs per configurare connessioni VPN e scambiare controllo e traffico dati con la Regione. La creazione del collegamento al servizio viene sempre avviata dall'Outpost.

> **Note**
>
> Non sarà possibile modificare la configurazione del link di servizio dopo aver completato l'ordine.

Opzioni di connettività pubblica Service Link

Puoi configurare il collegamento al servizio con una connessione pubblica per il traffico tra Outposts e la regione di origine AWS . Puoi scegliere di utilizzare la rete Internet pubblica o AWS Direct Connect pubblica VIFs.

Se prevedi di inserire nei firewall solo l'elenco AWS delle aree consentite IPs (anziché 0.0.0.0/0), devi assicurarti che le regole del firewall corrispondano up-to-date agli intervalli di indirizzi IP correnti. Per ulteriori informazioni, consulta gli intervalli di indirizzi AWS IP nella Amazon VPC User Guide.

L'immagine seguente mostra entrambe le opzioni per stabilire una connessione pubblica di service link tra i tuoi Outposts e la AWS regione:

Opzione 1. Connettività pubblica tramite Internet

Questa opzione richiede che la sottorete dell'infrastruttura di collegamento IPs al AWS Outposts servizio abbia accesso agli intervalli IP pubblici della AWS regione o della regione di residenza. È necessario consentire l'elenco AWS Region public IPs o 0.0.0.0/0 su dispositivi di rete come il firewall.

Opzione 2. Connettività pubblica tramite AWS Direct Connect pubblico VIFs

Questa opzione richiede che la sottorete dell'infrastruttura di collegamento IPs al AWS Outposts servizio abbia accesso agli intervalli IP pubblici della AWS regione o della regione di origine tramite il servizio DX. È necessario consentire l'elenco AWS Region public IPs o 0.0.0.0/0 su dispositivi di rete come il firewall.

Opzioni di connettività privata Service Link

Puoi configurare il collegamento al servizio con una connessione privata per il traffico tra Outposts e la regione di origine AWS . Puoi scegliere di usare AWS Direct Connect privato o di transito VIFs.

Seleziona l'opzione di connettività privata quando crei Outpost nella AWS Outposts console. Per istruzioni, consulta Creare un avamposto.

Quando si seleziona l'opzione di connettività privata, viene stabilita una connessione VPN service link dopo l'installazione di Outpost, utilizzando un VPC e una sottorete specificati dall'utente. Ciò consente la connettività privata tramite il VPC e riduce al minimo l'esposizione pubblica a Internet.

L'immagine seguente mostra entrambe le opzioni per stabilire una connessione privata VPN service link tra i tuoi Outposts e la AWS regione:

Prerequisiti

Prima di poter configurare la connettività privata per l'Outpost è necessario verificare i seguenti prerequisiti:

- Per consentire a un utente o un ruolo di creare o modificare un ruolo collegato ai servizi, devi configurare le autorizzazioni per un'entità IAM (utente o ruolo). L'entità IAM necessita dell'autorizzazione per accedere alle seguenti operazioni:
  - `iam:CreateServiceLinkedRole` - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `iam:PutRolePolicy` - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `ec2:DescribeVpcs`
  - `ec2:DescribeSubnets`

Per ulteriori informazioni, vedere AWS Identity and Access ManagementAWS Outposts

- Nello stesso AWS account e nella stessa zona di disponibilità del tuo Outpost, crea un VPC al solo scopo della connettività privata di Outpost con una sottorete /25 o superiore che non sia in conflitto con 10.1.0.0/16. Ad esempio, è possibile utilizzare 10.3.0.0/16.
- Configura il gruppo di sicurezza della sottorete per consentire il traffico per le direzioni UDP 443 in entrata e in uscita.
- Pubblicizza il CIDR della sottorete sulla tua rete on-premise. Puoi usare per farlo. AWS Direct Connect Per ulteriori informazioni, consulta le interfacce virtuali AWS Direct Connect e Utilizzo di gateway AWS Direct Connect nella Guida per l'utente di AWS Direct Connect .

> **Note**
>
> Per selezionare l'opzione di connettività privata quando Outpost è in sospeso, scegli Outposts dalla AWS Outposts console e seleziona Outpost. Scegli Operazioni, Aggiungi connettività privata e segui i passaggi.

Dopo aver selezionato l'opzione di connettività privata per Outpost, crea AWS Outposts automaticamente nel tuo account un ruolo collegato ai servizi che gli consente di completare le seguenti attività per tuo conto:

- Crea interfacce di rete nella sottorete e nel VPC specificati e crea un gruppo di sicurezza per le interfacce di rete.
- Concede l'autorizzazione al AWS Outposts servizio per collegare le interfacce di rete a un'istanza dell'endpoint service link nell'account.
- Collega le interfacce di rete alle istanze dell'endpoint del collegamento al servizio a partire dall'account.

> **Important**
>
> Dopo aver installato Outpost, conferma la connettività alla rete privata IPs nella sottorete da Outpost.

Opzione 1. Connettività privata tramite rete AWS Direct Connect privata VIFs

Crea una AWS Direct Connect connessione, un'interfaccia virtuale privata e un gateway privato virtuale per consentire all'Outpost locale di accedere al VPC.

Per ulteriori informazioni, consulta le seguenti sezioni della Guida per l'AWS Direct Connect utente:

- Connessioni dedicate e ospitate
- Crea un'interfaccia virtuale privata
- Associazioni di gateway privati virtuali

Se la AWS Direct Connect connessione è in un AWS account diverso dal tuo VPC, consulta Associare un gateway privato virtuale tra account nella Guida per l'AWS Direct Connect utente.

Opzione 2. Connettività privata tramite AWS Direct Connect transito VIFs

Crea una AWS Direct Connect connessione, un'interfaccia virtuale di transito e un gateway di transito per consentire al tuo Outpost locale di accedere al VPC.

Per ulteriori informazioni, consulta le seguenti sezioni della Guida per l'AWS Direct Connect utente:

- Connessioni dedicate e ospitate
- Creare un'interfaccia virtuale di transito per il gateway Direct Connect
- Associazioni di gateway di transito

Firewall e il collegamento al servizio

Questa sezione illustra le configurazioni del firewall e la connessione del collegamento al servizio.

Nel diagramma seguente, la configurazione estende Amazon VPC dalla regione AWS all'avamposto. Un'interfaccia virtuale AWS Direct Connect pubblica è la connessione di collegamento al servizio. Il seguente traffico passa attraverso il collegamento al servizio e la connessione AWS Direct Connect :

- Gestione del traffico verso Outpost attraverso il collegamento al servizio
- Traffico tra l'Outpost e tutti i siti associati VPCs

Se con la tua connessione Internet utilizzi un firewall stateful per limitare la connettività dalla rete Internet pubblica alla VLAN del collegamento al servizio, puoi bloccare tutte le connessioni in entrata che partono da Internet. Questo perché il VPN del collegamento al servizio viene avviato solo dall'Outpost alla regione, non dalla regione all'Outpost.

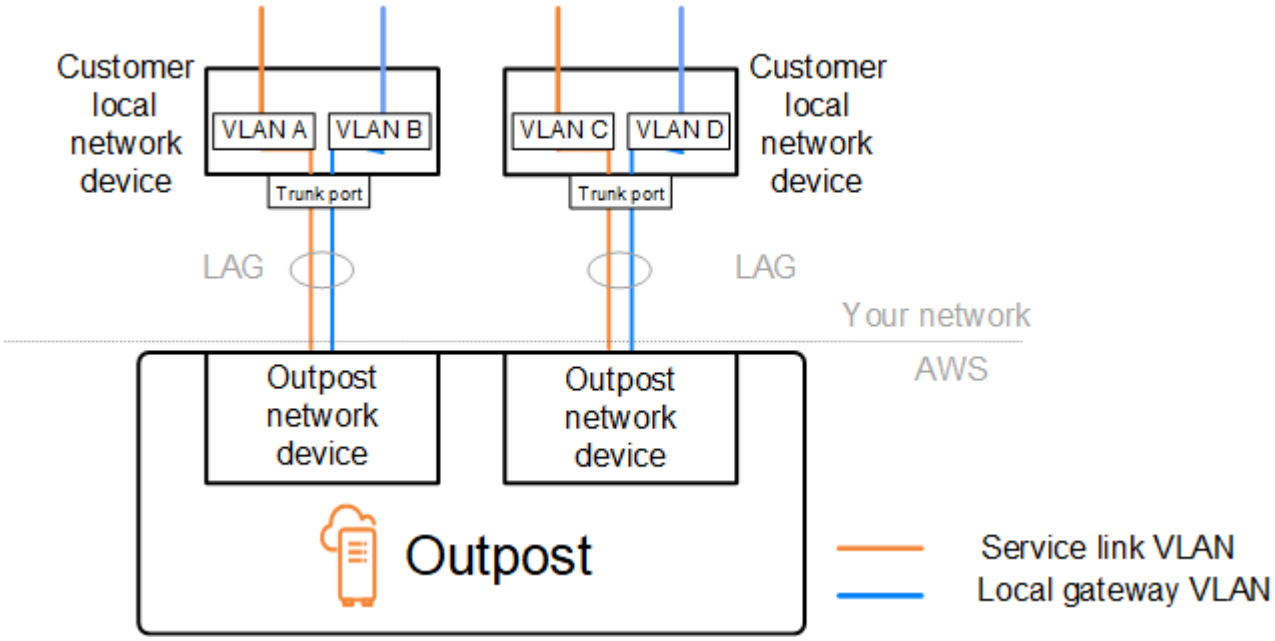
Se per limitare la connettività dalla VLAN del collegamento al servizio utilizzi un firewall, puoi bloccare tutte le connessioni in entrata. È necessario consentire le connessioni in uscita verso l'avamposto dalla AWS regione secondo la tabella seguente. Se utilizzi un firewall stateful, le connessioni in uscita dall'Outpost che sono consentite, ossia avviate dall'Outpost, devono essere consentite nuovamente in entrata.

Protocollo	Porta di origine	Indirizzo di origine	Porta di destinazione	Indirizzo di destinazione
UDP	443	AWS Outposts collegamento di servizio /26	443	AWS Outposts Il pubblico della regione IPs
TCP	1025-65535	AWS Outposts collegamento di servizio /26	443	AWS Outposts Il pubblico della regione IPs

> **Note**
>
> Le istanze in un Outpost non possono utilizzare il link di servizio per comunicare con le istanze di un altro Outpost. Sfrutta il routing attraverso il gateway locale o l'interfaccia di rete locale per comunicare tra gli Outpost.
> AWS Outposts i rack sono inoltre progettati con apparecchiature di alimentazione e rete ridondanti, inclusi componenti gateway locali. Per ulteriori informazioni, vedere Resilience in. AWS Outposts

Elenco di controllo per la risoluzione dei problemi della rete rack Outposts

Utilizza questo elenco di controllo per risolvere i problemi relativi a un collegamento al servizio con stato `DOWN`.



Connettività con i dispositivi di rete Outpost

Verifica lo stato del peering BGP sui dispositivi di rete locale del cliente collegati ai dispositivi di rete Outpost. Se lo stato di peering BGP è `DOWN`, completa la seguente procedura:

1. Esegui il ping dell'indirizzo IP peer remoto sui dispositivi di rete Outpost dai dispositivi del cliente. L'indirizzo IP peer si trova nella configurazione BGP del tuo dispositivo. Puoi anche fare riferimento all'elenco Elenco di controllo di preparazione della rete fornito al momento dell'installazione.
2. Se il ping ha esito negativo, controlla la connessione fisica e assicurati che lo stato della connettività sia `UP`.
   a. Verifica lo stato LACP dei dispositivi di rete locale del cliente.
   b. Controlla lo stato dell'interfaccia sul dispositivo. Se lo stato è `UP`, passa alla fase 3.
   c. Controlla i dispositivi della rete locale del cliente e verifica che il modulo ottico funzioni.
   d. Sostituisci le fibre difettose e assicurati che le spie (Tx/Rx) rientrino nell'intervallo accettabile.
3. Se il ping ha esito positivo, controlla i dispositivi della rete locale del cliente e assicurati che le seguenti configurazioni BGP siano corrette.

   a. Verifica che il Numero di sistema autonomo locale (ASN del cliente) sia configurato correttamente.
   b. Verifica che il Numero di sistema autonomo remoto (ASN dell'Outpost) sia configurato correttamente.
   c. Verifica che l'IP dell'interfaccia e gli indirizzi IP peer remoti siano configurati correttamente.
   d. Verifica che i routing propagati e ricevuti siano corretti.
4. Se la sessione BGP presenta un susseguirsi a ciclo continuo tra gli stati attivo e connesso, verifica che la porta TCP 179 e le altre porte temporanee pertinenti non siano bloccate sui dispositivi della rete locale del cliente.
5. Per approfondire l'analisi per la risoluzione del problema, controlla quanto segue sui dispositivi di rete locale del cliente:
   a. Log di debug BGP e TCP
   b. Log BGP
   c. Acquisizione di pacchetti
6. Se il problema persiste, esegui l'acquisizione di MTR/traceroute/pacchetti dal router connesso a Outpost agli indirizzi IP peer del dispositivo di rete Outpost. Condividi i risultati del test con AWS Support, utilizzando il tuo piano di supporto Enterprise.

Se lo stato di peering BGP è `UP` tra i dispositivi della rete locale del cliente e i dispositivi di rete Outpost, ma il collegamento al servizio è ancora `DOWN`, puoi approfondire l'analisi per la risoluzione del problema controllando i seguenti elementi sui dispositivi della rete locale del cliente. Utilizza uno dei seguenti elenchi di controllo, a seconda della modalità di provisioning della connettività del collegamento al servizio.

- Router Edge connessi a AWS Direct Connect : interfaccia virtuale pubblica in uso per la connettività Service Link. Per ulteriori informazioni, consulta AWS Direct Connect connettività dell'interfaccia virtuale pubblica alla regione AWS.
- Router edge collegati a AWS Direct Connect : interfaccia virtuale privata in uso per la connettività del service link. Per ulteriori informazioni, consulta AWS Direct Connect interfaccia virtuale privata: connettività alla AWS regione.
- Router edge connessi a Internet Service Provider (ISPs): Internet pubblico in uso per la connettività service link. Per ulteriori informazioni, consulta Connettività Internet pubblica dell'ISP alla regione AWS.

AWS Direct Connect connettività dell'interfaccia virtuale pubblica alla regione AWS

Utilizza la seguente lista di controllo per risolvere i problemi relativi ai router edge connessi AWS Direct Connect quando viene utilizzata un'interfaccia virtuale pubblica per la connettività del service link.

1. Verifica che i dispositivi che si connettono direttamente ai dispositivi di rete Outpost ricevano gli intervalli di indirizzi IP del collegamento al servizio tramite BGP.
   a. Verifica che i routing vengano ricevuti dal tuo dispositivo tramite BGP.
   b. Controlla la tabella di routing dell'istanza Virtual Routing and Forwarding (VRF) del collegamento al servizio. Dovrebbe mostrare che sta utilizzando l'intervallo di indirizzi IP.
2. Per garantire la connettività della regione, controlla la tabella di routing per la VRF del collegamento al servizio. Dovrebbe includere gli intervalli di indirizzi IP AWS pubblici o la route predefinita.
3. Se non ricevete gli intervalli di indirizzi IP AWS pubblici nel service link VRF, controllate i seguenti elementi.
   a. Controllate lo stato del AWS Direct Connect collegamento dall'edge router o dal AWS Management Console.
   b. Se il collegamento fisico è `UP`, controlla lo stato del peering BGP dal router edge.
   c. Se lo stato del peering BGP è`DOWN`, esegui il ping dell'indirizzo AWS IP del peer e controlla la configurazione BGP nel router perimetrale. Per ulteriori informazioni, consulta Risoluzione dei problemi AWS Direct Connect nella Guida per l'AWS Direct Connect utente e Lo stato BGP della mia interfaccia virtuale è inattivo nella console. AWS Cosa devo fare?
   d. Se è stato stabilito il protocollo BGP e non vedi la route predefinita o gli intervalli di indirizzi IP AWS pubblici nel VRF, contatta l'assistenza utilizzando il tuo piano di AWS supporto Enterprise.
4. Se disponi di un firewall on-premise, verifica i seguenti elementi.
   a. Verifica che le porte richieste per la connettività del collegamento al servizio siano consentite nei firewall di rete. Usa traceroute sulla porta 443 o qualsiasi altro strumento di risoluzione dei problemi di rete per confermare la connettività attraverso i firewall e i dispositivi di rete. Per la connettività del collegamento al servizio è necessario configurare le seguenti porte nelle policy del firewall.
      - Protocollo TCP – Porta di origine: TCP 1025-65535, Porta di destinazione: 443.
      - Protocollo UDP – Porta di origine: TCP 1025-65535, Porta di destinazione: 443.

b. Se il firewall è in modalità staterful, assicurati che le regole in uscita consentano l'intervallo di indirizzi IP del service link di Outpost agli intervalli di indirizzi IP pubblici. AWS Per ulteriori informazioni, consulta AWS Outposts connettività verso AWS le regioni.

c. Se il firewall non è dotato di stato, assicuratevi di consentire anche il flusso in entrata (dagli intervalli di indirizzi IP AWS pubblici all'intervallo di indirizzi IP del service link).

d. Se hai configurato un router virtuale nei firewall, assicurati che sia configurato il routing appropriato per il traffico tra Outpost e la regione AWS .

5. Se hai configurato il NAT nella rete on-premise per convertire gli intervalli di indirizzi IP del collegamento al servizio di Outpost nei tuoi indirizzi IP pubblici, verifica i seguenti elementi.

   a. Verifica che il dispositivo NAT non sia sovraccarico e disponga di porte libere da allocare per nuove sessioni.

   b. Verifica che il dispositivo NAT sia configurato correttamente per eseguire la conversione degli indirizzi.

6. Se il problema persiste, esegui l'acquisizione di pacchetti MTR /traceroute/dal router edge agli indirizzi IP del peer. AWS Direct Connect Condividi i risultati del test con AWS Support, utilizzando il tuo piano di supporto Enterprise.

AWS Direct Connect interfaccia virtuale privata: connettività alla AWS regione

Utilizza la seguente lista di controllo per risolvere i problemi relativi ai router edge connessi AWS Direct Connect quando viene utilizzata un'interfaccia virtuale privata per la connettività del service link.

1. Se la connettività tra il rack Outposts e la AWS regione utilizza la funzionalità di connettività AWS Outposts privata, controlla i seguenti elementi.

   a. Esegui il ping dell'indirizzo AWS IP di peering remoto dal router periferico e conferma lo stato del peering BGP.

   b. Assicurati che il peering BGP tramite l'interfaccia virtuale AWS Direct Connect privata tra il tuo VPC dell'endpoint service link e Outpost installato nella tua sede sia valido. UP Per ulteriori informazioni, consulta Risoluzione dei problemi AWS Direct Connect nella Guida per l'AWS Direct Connect utente, Lo stato BGP della mia interfaccia virtuale non è disponibile nella console. AWS Cosa devo fare? e In che modo posso risolvere i problemi di connessione BGP tramite Direct Connect?.

c. L'interfaccia virtuale AWS Direct Connect privata è una connessione privata al router edge nella AWS Direct Connect posizione prescelta e utilizza BGP per lo scambio di rotte. L'intervallo CIDR del tuo cloud privato virtuale (VPC) viene comunicato tramite questa sessione BGP sul tuo router edge. Analogamente, l'intervallo di indirizzi IP per il collegamento al servizio Outpost viene comunicato sulla regione tramite BGP dal router edge.

d. Verifica che la rete ACLs associata all'endpoint privato service link nel tuo VPC consenta il traffico pertinente. Per ulteriori informazioni, consulta Elenco di controllo di preparazione della rete.

e. Se disponi di un firewall on-premise, assicurati che il firewall disponga di regole in uscita che consentano gli intervalli di indirizzi IP del collegamento al servizio e gli endpoint del servizio Outpost (gli indirizzi IP dell'interfaccia di rete) situati nel VPC o nel CIDR VPC. Assicurati che le porte TCP 1025-65535 e UDP 443 non siano bloccate. Per ulteriori informazioni, consulta Introduzione alla connettività AWS Outposts privata.

f. Se il firewall non è stateful, assicurati che disponga di regole e policy per consentire il traffico in entrata verso Outpost dagli endpoint del servizio Outpost nel VPC.

2. Se hai più di 100 reti nella tua rete locale, puoi pubblicizzare un percorso predefinito tramite la sessione BGP verso la tua interfaccia virtuale AWS privata. Se non desideri propagare un routing predefinito, riepiloga i routing in modo che il numero di routing propagati sia inferiore a 100.

3. Se il problema persiste, esegui l'acquisizione di pacchetti MTR /traceroute/dal router edge agli indirizzi IP del peer. AWS Direct Connect Condividi i risultati del test con AWS Support, utilizzando il tuo piano di supporto Enterprise.

Connettività Internet pubblica dell'ISP alla regione AWS

Utilizza il seguente elenco di controllo per risolvere i problemi relativi ai router edge connessi tramite un ISP quando utilizzi un'interfaccia pubblica per la connettività del collegamento al servizio.

- Verifica che il collegamento Internet sia attivo.
- Verifica che i server pubblici siano accessibili dai tuoi dispositivi edge connessi tramite un ISP.

Se Internet o i server pubblici non sono accessibili tramite i collegamenti ISP, completa i seguenti passaggi.

1. Verifica se lo stato di peering BGP con i router ISP è stato stabilito.

   a. Verifica che il BGP non sia in fase di flapping.

   b. Verifica che il BGP riceva e propaghi i routing richiesti dall'ISP.
2. In caso di configurazione del routing statico, verifica che il routing predefinito sia configurato correttamente sul dispositivo edge.
3. Verifica se riesci a raggiungere Internet utilizzando un'altra connessione ISP.
4. Se il problema persiste, esegui l'acquisizione di MTR/traceroute/pacchetti sul tuo router edge. Condivi i risultati con il team di supporto tecnico del tuo ISP per approfondire l'analisi per la risoluzione del problema.

Se Internet e i server pubblici sono accessibili tramite i collegamenti ISP, completa i seguenti passaggi.

1. Verifica se EC2 le istanze o i sistemi di bilanciamento del carico accessibili al pubblico nella regione di residenza di Outpost sono accessibili dal tuo dispositivo periferico. Puoi utilizzare ping o telnet per confermare la connettività, quindi utilizza traceroute per confermare il percorso di rete.
2. Se lo utilizzi VRFs per separare il traffico nella tua rete, verifica che il link di servizio VRF disponga di percorsi o politiche che indirizzano il traffico da e verso l'ISP (Internet) e il VRF. Vedi i seguenti punti di controllo.
   a. Router edge che si connettono all'ISP. Controlla la tabella di routing VRF dell'ISP del router edge per confermare che l'intervallo di indirizzi IP del collegamento al servizio sia presente.
   b. Dispositivi di rete locale del cliente che si connettono a Outpost. Controllate le configurazioni del service link VRF VRFs e assicuratevi che il routing e le politiche necessarie per la connettività tra il service link VRF e l'ISP VRF siano configurati correttamente. Di norma, un routing predefinito viene inviato dalla VRF dell'ISP alla VRF del collegamento al servizio per il traffico verso Internet.
   c. Se hai configurato il routing basato sull'origine nei router collegati all'Outpost, verifica che la configurazione sia corretta.
3. Assicurati che i firewall locali siano configurati per consentire la connettività in uscita (porte TCP 1025-65535 e UDP 443) dagli intervalli di indirizzi IP di collegamento del servizio Outpost agli intervalli di indirizzi IP pubblici. AWS Se i firewall non sono stateful, assicurati che sia configurata anche la connettività in entrata all'Outpost.
4. Assicurati che il NAT sia configurato nella rete on-premise per convertire gli intervalli di indirizzi IP del collegamento al servizio di Outpost in indirizzi IP pubblici. Inoltre, verifica i seguenti elementi.
   a. Il dispositivo NAT non è sovraccarico e dispone di porte libere da allocare per nuove sessioni.
   b. Il dispositivo NAT è configurato correttamente per eseguire la conversione degli indirizzi.

Se il problema persiste, esegui l'acquisizione di MTR/traceroute/pacchetti.

- Se i risultati mostrano il rilascio o il blocco dei pacchetti nella rete on-premise, rivolgiti al team addetto alla rete o al team tecnico per ulteriori indicazioni.
- Se i risultati mostrano il rilascio o il blocco dei pacchetti nella rete dell'ISP, rivolgiti al team di supporto tecnico dell'ISP.
- Se i risultati non mostrano problemi, raccogli i risultati di tutti i test (ad esempio MTR, telnet, traceroute, acquisizioni di pacchetti e registri BGP) e contatta l'assistenza utilizzando il tuo piano di supporto Enterprise. AWS

Outposts è protetto da due dispositivi firewall

Se hai posizionato Outpost dietro una coppia di firewall sincronizzati ad alta disponibilità o due firewall autonomi, potrebbe verificarsi un routing asimmetrico del collegamento di servizio. Ciò significa che il traffico in entrata potrebbe passare attraverso il firewall-1, mentre il traffico in uscita attraversa il firewall-2. Utilizza la seguente lista di controllo per identificare il potenziale routing asimmetrico del link di servizio, specialmente se prima funzionava correttamente.

- Verificate se vi sono state modifiche recenti o interventi di manutenzione in corso nella configurazione del routing della rete aziendale che potrebbero aver portato al routing asimmetrico del link di servizio attraverso i firewall.
  - Utilizza i grafici del traffico del firewall per verificare le modifiche ai modelli di traffico corrispondenti all'inizio del problema del collegamento al servizio.
  - Verifica la presenza di un errore parziale del firewall o di uno scenario di coppia di firewall a cervello diviso che potrebbe aver impedito ai firewall di sincronizzare più le tabelle di connessione tra loro.
  - Verifica la presenza di link non funzionanti o di modifiche recenti al routing (modifiche alle OSPF/ISIS/EIGRP metriche, modifiche alla mappa di percorso BGP) nella rete aziendale che corrispondono all'inizio del problema relativo al collegamento al servizio.
- Se si utilizza la connettività Internet pubblica per il collegamento del servizio all'area di origine, la manutenzione di un provider di servizi potrebbe aver causato il routing asimmetrico del collegamento di servizio attraverso i firewall.
  - Consultate i grafici sul traffico per i collegamenti ai vostri ISP per eventuali modifiche ai modelli di traffico corrispondenti all'inizio del problema relativo al collegamento al servizio.

- Se si utilizza la AWS Direct Connect connettività per il collegamento al servizio, è possibile che una manutenzione AWS pianificata abbia attivato il routing asimmetrico del collegamento di servizio.
  - Verifica la presenza di notifiche di manutenzione pianificata sui tuoi AWS Direct Connect servizi.
  - Tieni presente che se disponi di AWS Direct Connect servizi ridondanti, puoi testare in modo proattivo il routing del collegamento al servizio Outposts su ogni probabile percorso di rete in condizioni di manutenzione. Ciò consente di verificare se un'interruzione di uno dei AWS Direct Connect servizi potrebbe portare a un routing asimmetrico del collegamento di servizio. La resilienza della AWS Direct Connect parte della connettività di end-to-end rete può essere testata dal Resiliency with Resiliency Toolkit. AWS Direct Connect Per ulteriori informazioni, vedere Testing AWS Direct Connect Resiliency with Resiliency Toolkit — Failover Testing.

Dopo aver esaminato la lista di controllo precedente e aver individuato il routing asimmetrico del collegamento al servizio come possibile causa principale, è possibile intraprendere una serie di ulteriori azioni:

- Ripristina il routing simmetrico ripristinando eventuali modifiche alla rete aziendale o aspettando il completamento della manutenzione pianificata dal provider.
- Accedi a uno o entrambi i firewall e cancella tutte le informazioni sullo stato del flusso per tutti i flussi dalla riga di comando (se supportato dal fornitore del firewall).
- Filtra temporaneamente gli annunci BGP tramite uno dei firewall o chiudi le interfacce su un firewall per forzare il routing simmetrico attraverso l'altro firewall.
- Riavviate ogni firewall a turno per eliminare eventuali danneggiamenti nel tracciamento dello stato di flusso del traffico del service link nella memoria del firewall.
- Rivolgiti al fornitore del firewall per verificare o semplificare il tracciamento dello stato di flusso UDP per le connessioni UDP provenienti dalla porta 443 e destinate alla porta 443.

Gateway locali per i tuoi rack Outposts

Il gateway locale è un componente fondamentale dell'architettura per i rack Outposts. Un gateway locale consente la connettività tra le sottoreti Outpost e la rete locale. Se l'infrastruttura locale fornisce un accesso a Internet, i carichi di lavoro in esecuzione sui rack Outposts possono anche sfruttare il gateway locale per comunicare con servizi regionali o carichi di lavoro regionali. Questa connettività può essere ottenuta utilizzando una connessione pubblica (Internet) o utilizzando. AWS Direct Connect Per ulteriori informazioni, consulta AWS Outposts connettività verso AWS le regioni.

Indice

- Nozioni di base sul gateway locale
- Routing del gateway locale
- Connettività tramite un gateway locale
- Tabelle di routing del gateway locale
- Gateway locale, tabella di routing, percorsi
- Crea un pool CoIP

Nozioni di base sul gateway locale

AWS crea un gateway locale per ogni rack Outposts come parte del processo di installazione. Un rack Outposts supporta un singolo gateway locale. Il gateway locale è di proprietà del rack Account AWS associato al rack Outposts.

> **Note**
>
> Per comprendere i limiti della larghezza di banda delle istanze per il traffico che attraversa un gateway locale, consulta la larghezza di banda della rete delle EC2 istanze Amazon nella Amazon EC2 User Guide.

Un gateway locale include i seguenti componenti:

- Tabelle di routing: solo il proprietario di un gateway locale può creare tabelle di routing del gateway locale. Per ulteriori informazioni, consulta the section called “Tabelle di instradamento”.

- Pool CoIP: (facoltativo) puoi utilizzare intervalli di indirizzi IP di tua proprietà per facilitare la comunicazione tra la rete locale e le istanze nel tuo VPC. Per ulteriori informazioni, consulta the section called “Indirizzi IP di proprietà del cliente”.
- Interfacce virtuali (VIFs) — Il gateway locale VIFs (interfaccia virtuale) è un componente dell'interfaccia logica dei rack Outposts che configura la connettività VLAN, IP e BGP tra un dispositivo di rete Outposts e un dispositivo di rete locale per la connettività del gateway locale. AWS crea un VIF per ogni LAG e li aggiunge entrambi a un gruppo VIF. VIFs La tabella delle rotte del gateway locale deve avere una route predefinita tra le due VIFs per la connettività di rete locale. Per ulteriori informazioni, consulta Connettività di rete locale.
- Gruppi VIF: AWS aggiunge i gruppi VIFs che crea a un gruppo VIF. I gruppi VIF sono raggruppamenti logici di. VIFs
- Tabella di routing del gateway locale e associazioni VPC: la tabella di routing del gateway locale e le associazioni VPC consentono di collegare le tabelle di routing del gateway locale. VPCs Con questa associazione, puoi aggiungere una route mirata al gateway locale all'interno della tabella di routing della sottorete Outposts. Ciò consente la comunicazione tra le risorse della sottorete Outposts e la rete locale tramite il gateway locale.
- Domini di routing del gateway locale: un dominio di routing del gateway locale è l'associazione di una tabella di routing del gateway locale e del gruppo VIF del gateway locale. Con questa associazione, è possibile aggiungere una route destinata a un gruppo VIF del gateway locale all'interno della tabella di routing del gateway locale. Ciò consente la comunicazione tra le risorse della sottorete Outposts e la rete locale tramite il gruppo VIF selezionato.

Durante il AWS rifornimento del rack Outposts, noi creiamo alcuni componenti e tu sei responsabile della creazione di altri.

AWS responsabilità

- Fornitura dell'hardware.
- Creazione del gateway locale.
- Crea le interfacce virtuali (VIFs) e un gruppo VIF.

Le tue responsabilità

- Creazione della tabella di routing del gateway locale.
- Associazione di un VPC alla tabella di routing del gateway locale.

- Associa un gruppo VIF alla tabella di routing del gateway locale per creare un dominio di routing del gateway locale.

Routing del gateway locale

Le istanze nella sottorete Outpost possono utilizzare una delle seguenti opzioni per la comunicazione con la rete on-premise tramite il gateway locale:

- Indirizzi IP privati: il gateway locale utilizza gli indirizzi IP privati delle istanze nella sottorete di Outpost per facilitare la comunicazione con la rete locale. Questa è l'impostazione predefinita.
- Indirizzi IP di proprietà del cliente: il gateway locale esegue la conversione degli indirizzi di rete (NAT) per gli indirizzi IP di proprietà del cliente assegnati alle istanze nella sottorete Outpost. Questa opzione supporta intervalli CIDR sovrapposti e altre topologie di rete.

Per ulteriori informazioni, consulta the section called “Tabelle di instradamento”.

Connettività tramite un gateway locale

Il ruolo principale di un gateway locale è fornire la connettività da un Outpost alla rete locale on-premise. Fornisce inoltre connettività a Internet tramite la rete on-premise. Per alcuni esempi, consulta the section called “Routing VPC diretto” e the section called “Indirizzi IP di proprietà del cliente”.

Il gateway locale può anche fornire un percorso del piano dati per tornare alla AWS regione. Il percorso del piano dati per il gateway locale passa per l'Outpost, attraverso il gateway locale, e raggiunge il segmento LAN del gateway locale privato. Seguirà quindi un percorso privato per tornare agli endpoint del servizio AWS nella regione. Ricordiamo che il percorso del piano di controllo utilizza sempre la connettività del collegamento al servizio, indipendentemente dal percorso del piano dati utilizzato.

Puoi connettere la tua infrastruttura Outposts locale Servizi AWS alla regione in modo privato. AWS Direct Connect Per ulteriori informazioni, consulta Connettività privata AWS Outposts.

L'immagine seguente mostra la connettività tramite il gateway locale:

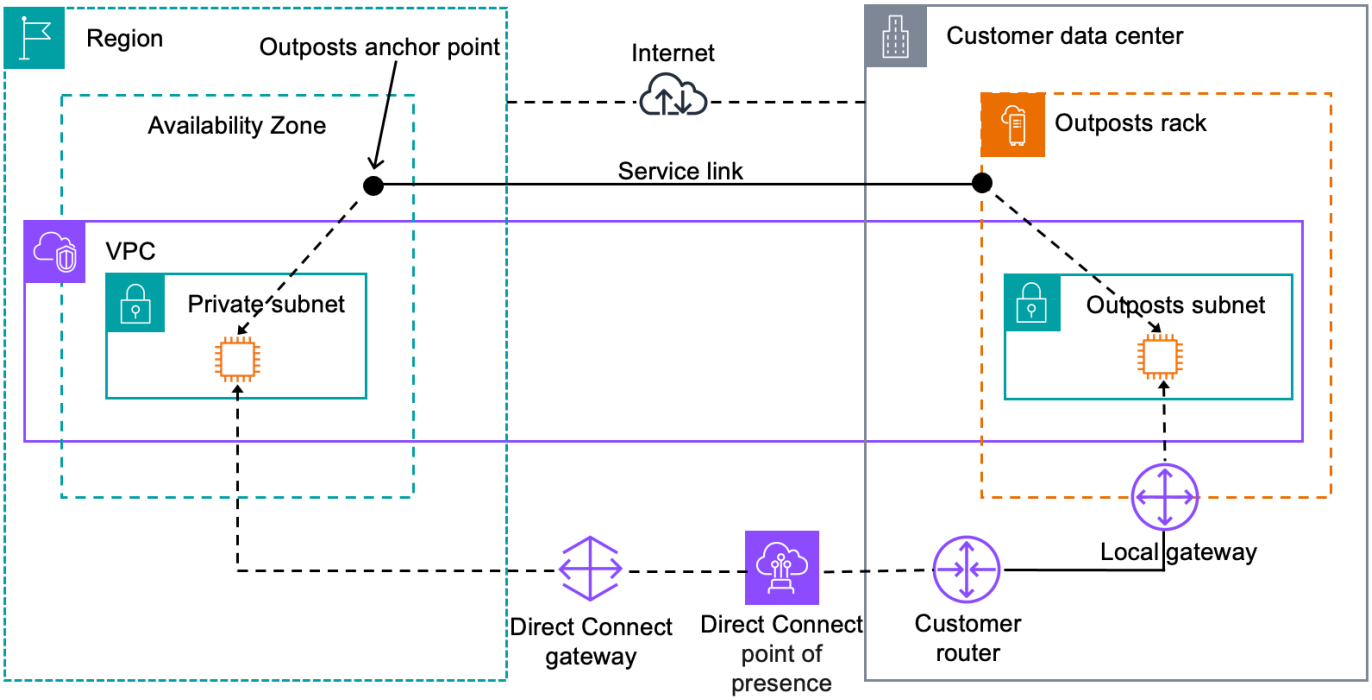


Tabelle di routing del gateway locale

Come parte dell'installazione su rack, AWS crea il gateway locale, configura VIFs e un gruppo VIF. Il gateway locale è di proprietà dell' AWS account associato a Outpost. mentre tu crei la tabella di routing del gateway locale. Una tabella di routing del gateway locale deve avere un'associazione al gruppo VIF e a un VPC. Spetta a te creare e gestire l'associazione del gruppo VIF e del VPC. Solo il proprietario del gateway locale può modificare la tabella di routing del gateway locale.

Le tabelle di routing delle sottoreti di Outpost possono includere un percorso verso i gruppi VIF del gateway locale per fornire connettività alla rete locale.

Le tabelle di routing del gateway locale dispongono di una modalità che determina il modo in cui le istanze nella sottorete Outposts comunicano con la rete locale. L'opzione predefinita è il routing VPC diretto, che utilizza gli indirizzi IP privati delle istanze. L'altra opzione consiste nell'utilizzare gli indirizzi di un pool di indirizzi IP (CoIP) di proprietà del cliente fornito dall'utente. Il routing VPC diretto e il CoIP sono opzioni che si escludono a vicenda che controllano il funzionamento del routing. Per determinare l'opzione migliore per il tuo Outpost, vedi Come scegliere tra le modalità di routing CoIP e Direct VPC sul rack Outposts. AWS

È possibile condividere la tabella di routing del gateway locale con altri AWS account o unità organizzative utilizzando. AWS Resource Access Manager Per ulteriori informazioni, vedere Lavorare con AWS Outposts risorse condivise.

Indice

- Routing VPC diretto
- Indirizzi IP di proprietà del cliente
- Tabelle di routing personalizzate

Routing VPC diretto

Il routing VPC diretto utilizza l'indirizzo IP privato delle istanze nel VPC per facilitare la comunicazione con la tua rete on-premise. Questi indirizzi vengono propagati sulla rete on-premise con BGP. La pubblicità su BGP riguarda solo gli indirizzi IP privati che appartengono alle sottoreti sul rack Outposts. Questo tipo di routing è la modalità predefinita per Outposts. In questa modalità, il gateway locale non esegue NAT per le istanze e non è necessario assegnare indirizzi IP elastici alle istanze. EC2 È possibile utilizzare il proprio spazio di indirizzi anziché la modalità di routing VPC diretta. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente.

La modalità di routing VPC diretto non supporta intervalli CIDR sovrapposti.

Il routing VPC diretto è supportato solo per le interfacce di rete delle istanze. Con le interfacce di rete AWS create per conto dell'utente (note come interfacce di rete gestite dal richiedente), i relativi indirizzi IP privati non sono raggiungibili dalla rete locale. Ad esempio, gli endpoint VPC non sono direttamente raggiungibili dalla rete on-premise.

Negli esempi seguenti viene illustrato il routing VPC diretto.

Esempi

- Esempio: connettività Internet tramite VPC
- Esempio: connettività Internet tramite la rete on-premise

Esempio: connettività Internet tramite VPC

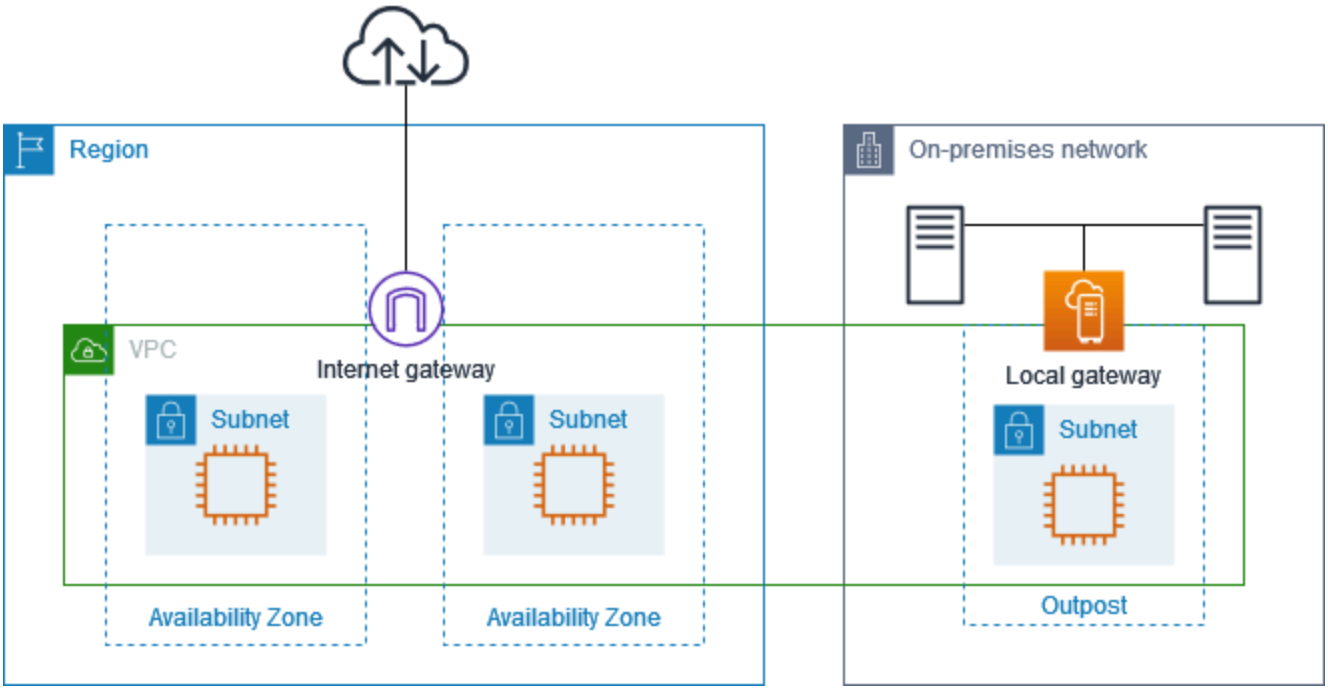
Le istanze in una sottorete Outpost possono accedere a Internet tramite il gateway Internet collegato al VPC.

Esamina la seguente configurazione:

- Il VPC principale si estende su due zone di disponibilità e presenta una sottorete in ciascuna di esse.
- L'Outpost ha una sottorete.
- Ogni sottorete ha un'istanza. EC2
- Il gateway locale utilizza l'annuncio BGP per comunicare gli indirizzi IP privati della sottorete Outpost alla rete on-premise.

> **Note**
>
> L'annuncio BGP è supportato solo per le sottoreti di un Outpost che hanno un routing con il gateway locale come destinazione. Eventuali altre sottoreti non vengono annunciate tramite BGP.

Nel seguente diagramma, il traffico proveniente dall'istanza nella sottorete Outpost può utilizzare il gateway Internet per il VPC per accedere a Internet.



Per ottenere la connettività Internet tramite la regione principale, la tabella di routing per la sottorete Outpost deve avere il seguente routing.

Destinazione	Target	Commenti
VPC CIDR	Locale	Fornisce connettività tra le sottoreti nel VPC.
0.0.0.0	*internet-gateway-id*	Invia il traffico destinato a Internet al gateway Internet.
on-premises network CIDR	*local-gateway-id*	Invia il traffico destinato alla rete on-premise al gateway locale.

Esempio: connettività Internet tramite la rete on-premise

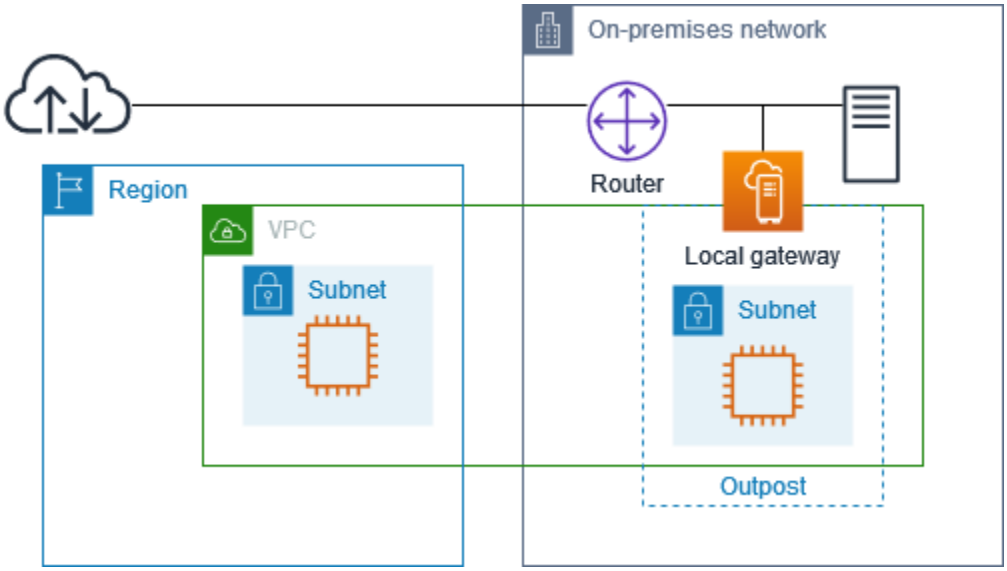
Le istanze in una sottorete Outpost possono accedere a Internet tramite la rete on-premise. Le istanze nella sottorete Outpost non richiedono un indirizzo IP pubblico o un indirizzo IP elastico.

Esamina la seguente configurazione:

- La sottorete Outpost ha un'istanza. EC2
- Il router nella rete on-premise esegue Network Address Translation (NAT).
- Il gateway locale utilizza l'annuncio BGP per comunicare gli indirizzi IP privati della sottorete Outpost alla rete on-premise.

> **Note**
>
> L'annuncio BGP è supportato solo per le sottoreti di un Outpost che hanno un routing con il gateway locale come destinazione. Eventuali altre sottoreti non vengono annunciate tramite BGP.

Nel seguente diagramma, il traffico proveniente dall'istanza nella sottorete Outpost può utilizzare il gateway locale per accedere a Internet o alla rete on-premise. Il traffico proveniente dalla rete on-premise utilizza il gateway locale per accedere all'istanza nella sottorete Outpost.



Per ottenere la connettività Internet tramite la rete on-premise, la tabella di routing per la sottorete Outpost deve avere il seguente routing.

Destinazione	Target	Commenti
VPC CIDR	Locale	Fornisce connettività tra le sottoreti nel VPC.
0.0.0.0/0	*local-gateway-id*	Invia il traffico destinato a Internet al gateway locale.

Accesso in uscita a Internet

Il traffico avviato dall'istanza nella sottorete Outpost con una destinazione Internet utilizza il routing per 0.0.0.0/0 per instradare il traffico al gateway locale. Il gateway locale invia il traffico al router. Il router utilizza NAT per convertire l'indirizzo IP privato in un indirizzo IP pubblico sul router e quindi invia il traffico alla destinazione.

Accesso in uscita alla rete on-premise

Il traffico avviato dall'istanza nella sottorete Outpost con una destinazione nella rete on-premise utilizza il routing per 0.0.0.0/0 per instradare il traffico al gateway locale. Il gateway locale invia il traffico alla destinazione nella rete on-premise.

Accesso in entrata dalla rete on-premise

Il traffico proveniente dalla rete on-premise con una destinazione dell'istanza nella sottorete Outpost utilizza l'indirizzo IP privato dell'istanza. Quando il traffico raggiunge il gateway locale, questo invia il traffico alla destinazione nel VPC.

Indirizzi IP di proprietà del cliente

Per impostazione predefinita, il gateway locale utilizza l'indirizzo IP privato delle istanze nel VPC per agevolare le comunicazioni con la rete on-premise. Tuttavia, 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.

Se scegli il CoIP, devi creare un pool di indirizzi, assegnarlo alla tabella di routing del gateway locale e comunicare nuovamente questi indirizzi alla rete dei clienti tramite BGP. Tutti gli indirizzi IP di proprietà del cliente associati alla tabella di routing del gateway locale vengono visualizzati nella tabella di routing come instradamenti propagati.

Gli indirizzi IP di proprietà del cliente forniscono connettività locale o esterna alle risorse nella rete on-premise. Puoi assegnare questi indirizzi IP alle risorse di Outpost, come le EC2 istanze, allocando un nuovo indirizzo IP elastico dal pool IP di proprietà del cliente e quindi assegnandolo alla tua risorsa. Per ulteriori informazioni, consulta Pool CoIP.

> **Note**
>
> Per un pool di indirizzi IP di proprietà del cliente, devi essere in grado di indirizzare l'indirizzo nella tua rete.

Quando esegui l'allocazione di un indirizzo IP elastico dal pool di indirizzi IP di proprietà del cliente, continui a possedere gli indirizzi IP del pool di indirizzi IP di proprietà del cliente. Sei responsabile della loro propagazione, secondo necessità, nelle tue reti interne o sulla WAN.

Facoltativamente, puoi condividere il pool di proprietà del cliente con più Account AWS membri dell'organizzazione utilizzando. AWS Resource Access Manager Dopo aver condiviso il pool, i partecipanti possono allocare un indirizzo IP elastico dal pool di indirizzi IP di proprietà del cliente e quindi assegnarlo a un' EC2 istanza su Outpost. Per ulteriori informazioni, consulta Risorse condivise.

Esempi

- Esempio: connettività Internet tramite VPC

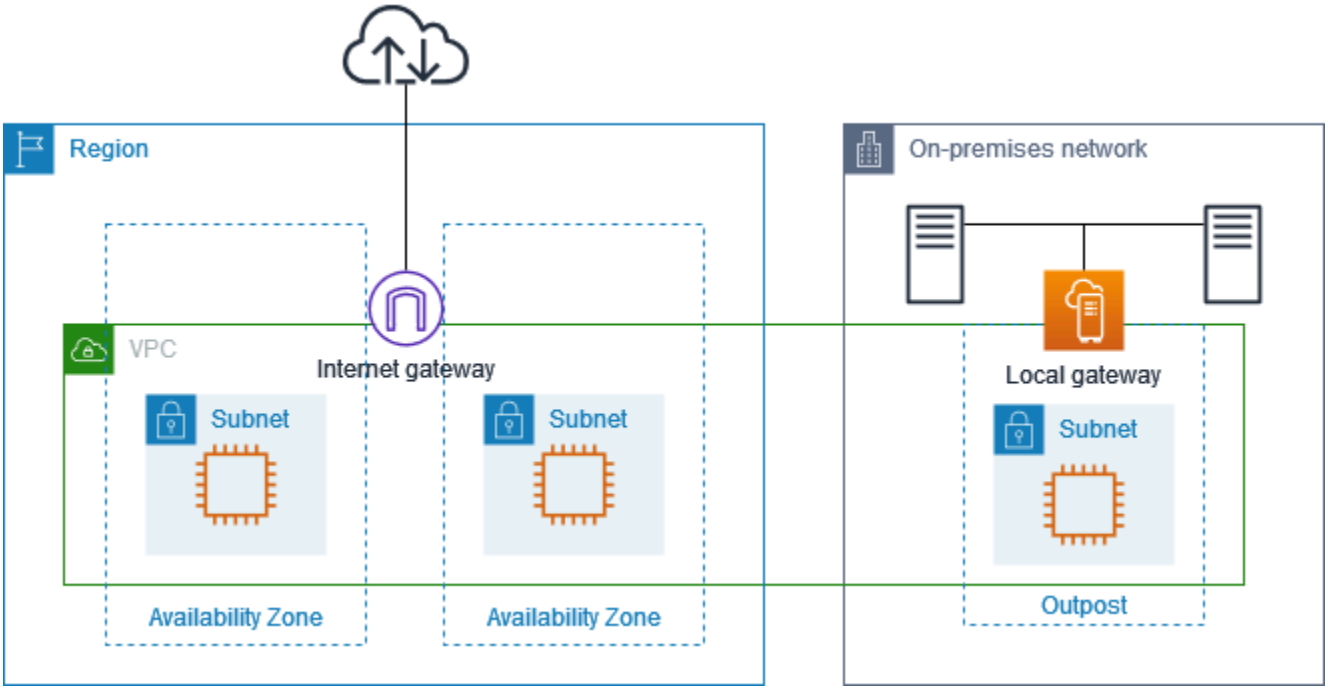
- Esempio: connettività Internet tramite la rete on-premise

Esempio: connettività Internet tramite VPC

Le istanze in una sottorete Outpost possono accedere a Internet tramite il gateway Internet collegato al VPC.

Esamina la seguente configurazione:

- Il VPC principale si estende su due zone di disponibilità e presenta una sottorete in ciascuna di esse.
- L'Outpost ha una sottorete.
- Ogni sottorete ha un'istanza. EC2
- Esiste un pool di indirizzi IP di proprietà del cliente.
- L'istanza nella sottorete Outpost ha un indirizzo IP elastico proveniente dal pool di indirizzi IP di proprietà del cliente.
- Il gateway locale utilizza l'annuncio BGP per propagare il pool di indirizzi IP di proprietà del cliente nella rete locale.



Per ottenere la connettività Internet tramite la regione, la tabella di routing per la sottorete Outpost deve avere il seguente routing.

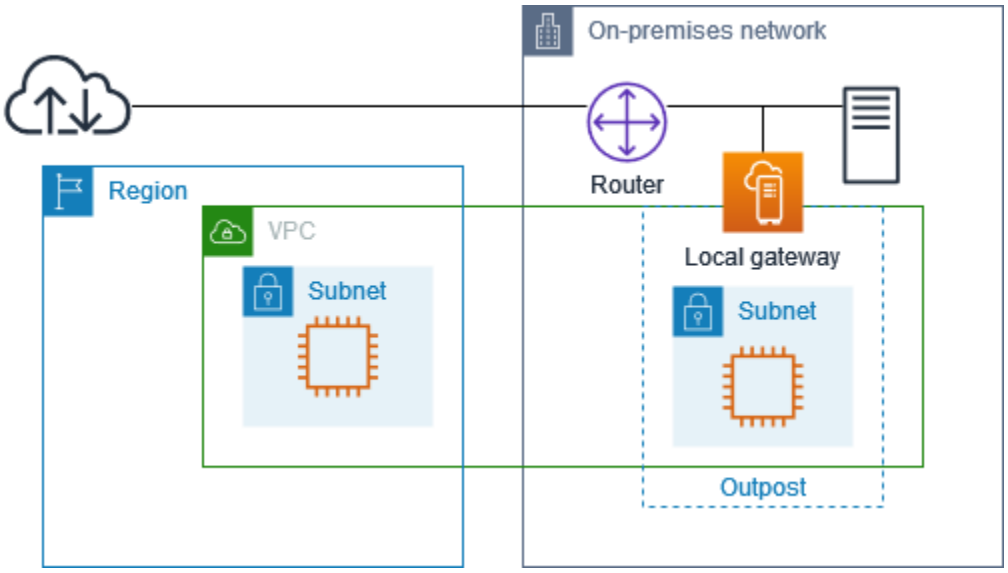
Destinazione	Target	Commenti
VPC CIDR	Locale	Fornisce connettività tra le sottoreti nel VPC.
0.0.0.0	*internet-gateway-id*	Invia il traffico destinato alla rete Internet pubblica al gateway Internet.
On-premises network CIDR	*local-gateway-id*	Invia il traffico destinato alla rete on-premise al gateway locale.

Esempio: connettività Internet tramite la rete on-premise

Le istanze in una sottorete Outpost possono accedere a Internet tramite la rete on-premise.

Esamina la seguente configurazione:

- La sottorete Outpost ha un'istanza. EC2
- Esiste un pool di indirizzi IP di proprietà del cliente.
- Il gateway locale utilizza l'annuncio BGP per propagare il pool di indirizzi IP di proprietà del cliente nella rete locale.
- Un'associazione di indirizzi IP elastici che mappa 10.0.3.112 a 10.1.0.2.
- Il router nella rete on-premise del cliente esegue NAT.



Per ottenere la connettività Internet tramite il gateway locale, la tabella di routing per la sottorete Outpost deve avere il seguente routing.

Destinazione	Target	Commenti
VPC CIDR	Locale	Fornisce connettività tra le sottoreti nel VPC.
0.0.0.0/0	*local-gateway-id*	Invia il traffico destinato a Internet al gateway locale.

Accesso in uscita a Internet

Il traffico avviato dall' EC2 istanza nella sottorete Outpost con una destinazione Internet utilizza la route 0.0.0.0/0 per indirizzare il traffico verso il gateway locale. Il gateway locale mappa l'indirizzo IP privato dell'istanza all'indirizzo IP di proprietà del cliente, quindi invia il traffico al router. Il router utilizza NAT per convertire l'indirizzo IP di proprietà del cliente in un indirizzo IP pubblico sul router e quindi invia il traffico alla destinazione.

Accesso in uscita alla rete on-premise

Il traffico avviato dall' EC2 istanza nella sottorete Outpost con una destinazione della rete locale utilizza il percorso 0.0.0.0/0 per instradare il traffico verso il gateway locale. Il gateway locale traduce l'indirizzo IP dell' EC2 istanza nell'indirizzo IP di proprietà del cliente (indirizzo IP elastico), quindi invia il traffico alla destinazione.

Accesso in entrata dalla rete on-premise

Il traffico proveniente dalla rete on-premise con una destinazione dell'istanza nella sottorete Outpost utilizza l'indirizzo IP di proprietà del cliente (indirizzo IP elastico) dell'istanza. Quando il traffico raggiunge il gateway locale, questo mappa l'indirizzo IP di proprietà del cliente (indirizzo IP elastico) nell'indirizzo IP dell'istanza e quindi invia il traffico alla destinazione nel VPC. Inoltre, la tabella di routing del gateway locale valuta tutti i routing destinati alle interfacce di rete elastiche. Se l'indirizzo di destinazione corrisponde al CIDR di destinazione di un routing statico, il traffico viene inviato a quell'interfaccia di rete elastica. Quando il traffico segue un routing statico verso un'interfaccia di rete elastica, l'indirizzo di destinazione viene mantenuto e non viene convertito nell'indirizzo IP privato dell'interfaccia di rete.

Tabelle di routing personalizzate

È possibile creare una tabella di routing personalizzata per il gateway locale. La tabella di routing del gateway locale deve avere un'associazione a un gruppo VIF e a un VPC. Per step-by-step le indicazioni, consulta Configurare la connettività del gateway locale.

Gateway locale, tabella di routing, percorsi

Puoi creare tabelle di routing dei gateway locali e percorsi in entrata verso le interfacce di rete su Outpost. È inoltre possibile modificare una route in ingresso del gateway locale esistente per modificare l'interfaccia di rete di destinazione.

Una route è attiva solo quando la relativa interfaccia di rete di destinazione è collegata a un'istanza in esecuzione. Se l'istanza viene interrotta o l'interfaccia viene scollegata, lo stato del percorso passa da attivo a blackhole.

Indice

- Requisiti e limitazioni
- Creazione delle tabelle di routing personalizzate del gateway locale
- Cambio di modalità o eliminazione di una tabella di routing del gateway locale

Requisiti e limitazioni

Si applicano i seguenti requisiti e limitazioni:

- L'interfaccia di rete di destinazione deve appartenere a una sottorete di Outpost e deve essere collegata a un'istanza di tale Outpost. Una route gateway locale non può indirizzare un' EC2istanza Amazon su un Outpost diverso o nel server principale Regione AWS.
- La sottorete deve appartenere a un VPC associato alla tabella di routing del gateway locale.
- Non devi superare più di 100 route di interfaccia di rete nella stessa tabella di routing.
- AWS dà la priorità alla route più specifica e, se le rotte corrispondono, diamo la priorità alle route statiche rispetto alle rotte propagate.
- Gli endpoint VPC di interfaccia non sono supportati.
- L'annuncio BGP è riservato solo alle sottoreti di un Outpost che hanno un routing nella relativa tabella con il gateway locale come destinazione. Se le sottoreti non hanno un routing nella relativa tabella con il gateway locale come destinazione, tali sottoreti non vengono propagate con BGP.

- Solo le interfacce di rete collegate alle istanze Outpost possono comunicare attraverso il gateway locale di quell'Outpost. Le interfacce di rete che appartengono alla sottorete Outpost ma sono collegate a un'istanza nella regione non possono comunicare attraverso il gateway locale di quell'Outpost.
- Le interfacce gestite dai richiedenti, come quelle create per gli endpoint VPC, non possono essere raggiunte dalla rete locale tramite il gateway locale. Possono essere raggiunte solo dalle istanze che si trovano nella sottorete Outpost.

Valgono le seguenti considerazioni sul NAT:

- Il gateway locale non esegue NAT sul traffico che corrisponde a un percorso di interfaccia di rete. Viene invece preservato l'indirizzo IP di destinazione.
- Disattiva il controllo di origine/destinazione per l'interfaccia di rete di destinazione. Per ulteriori informazioni, consulta i concetti dell'interfaccia di rete nella Amazon EC2 User Guide.
- Configura il sistema operativo per consentire l'accettazione del traffico proveniente dal CIDR di destinazione sull'interfaccia di rete.

Creazione delle tabelle di routing personalizzate del gateway locale

Puoi creare una tabella di routing personalizzata per il VPC tramite la console AWS Outposts .

Per creare una tabella di routing personalizzata tramite la console

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, seleziona Tabella di routing del gateway locale.
4. Seleziona Crea una tabella di routing del gateway locale.
5. (Facoltativo) In Nome, inserisci un nome per la tabella di routing del gateway locale.
6. Per Gateway locale, scegli il tuo gateway locale.
7. (Facoltativo) Scegli Associa gruppo VIF e scegli il tuo Gruppo VIF.

   Modifica la tabella di routing del gateway locale per aggiungere una route statica con il gruppo VIF come destinazione.
8. Per Modalità, scegli una modalità di comunicazione con la rete on-premise.

- Scegli Routing VPC diretto per utilizzare l'indirizzo IP privato di un'istanza.
- Scegli CoIP per utilizzare l'indirizzo IP di proprietà del cliente.
  - (Facoltativo) Aggiunta o rimozione di pool CoIP e blocchi CIDR aggiuntivi

    [Aggiunta di un pool CoIP] Scegli Aggiungi nuovo pool e procedi come segue:

    - In Nome, immetti un nome per il tuo pool CoIP.
    - In CIDR, immetti un blocco CIDR di indirizzi IP di proprietà del cliente.
  - [Aggiunta di blocchi CIDR] Scegli Aggiungi nuovo CIDR e inserisci un intervallo di indirizzi IP di proprietà del cliente.
  - [Rimozione di un pool CoIP o di un blocco CIDR aggiuntivo] Scegli Rimuovi a destra di un blocco CIDR o sotto il pool CoIP.

    Puoi specificare fino a 10 pool CoIP e 100 blocchi CIDR.

9. (Facoltativo) Aggiunta o rimozione di un tag.

   [Aggiunta di un tag] Scegli Aggiungi nuovo tag e procedi come segue:

   - In Chiave, immetti il nome della chiave.
   - In Valore, immetti il valore della chiave.

   [Rimozione di un tag] Scegli Rimuovi a destra della Chiave e del Valore del tag.

10. Seleziona Crea una tabella di routing del gateway locale.

Cambio di modalità o eliminazione di una tabella di routing del gateway locale

Per cambiare modalità devi eliminare e ricreare la tabella di routing del gateway locale. L'eliminazione della tabella di routing del gateway locale causa l'interruzione del traffico di rete.

Per cambiare modalità o eliminare una tabella di routing del gateway locale

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Verifica di essere nella posizione corretta Regione AWS.

   Per cambiare la regione, usa il selettore della regione nell'angolo in alto a destra della pagina.

3. Nel riquadro di navigazione, seleziona Tabelle di routing del gateway locale.
4. Verifica se la tabella di routing del gateway locale è associata a un gruppo VIF. Se è associata, è necessario rimuovere l'associazione tra la tabella di routing del gateway locale e il gruppo VIF.
   a. Scegliete l'ID della tabella di routing del gateway locale.
   b. Scegli la scheda di associazione del gruppo VIF.
   c. Se uno o più gruppi VIF sono associati alla tabella di routing del gateway locale, scegliete Modifica associazione di gruppi VIF.
   d. Deseleziona la casella di controllo Associa gruppo VIF.
   e. Scegli Save changes (Salva modifiche).
5. Scegli Elimina la tabella di routing del gateway locale.
6. Nella finestra di dialogo di conferma, digita **`delete`** e quindi scegli Elimina.
7. (Facoltativo) Crea una tabella di routing del gateway locale con una nuova modalità.
   a. Nel riquadro di navigazione, seleziona Tabelle di routing del gateway locale.
   b. Seleziona Crea una tabella di routing del gateway locale.
   c. Configura la tabella di routing del gateway locale utilizzando la nuova modalità. Per ulteriori informazioni, consulta Creazione di tabelle di routing personalizzate del gateway locale.

Crea un pool CoIP

Puoi fornire gli intervalli di indirizzi IP privati per facilitare la comunicazione con la rete on-premise e le istanze nel VPC. Per ulteriori informazioni, consulta Indirizzi IP di proprietà del cliente.

In modalità CoIP sono disponibili pool IP di proprietà del cliente per le tabelle di routing dei gateway locali.

Per creare un pool CoIP utilizza la seguente procedura.

Console

Per creare un pool CoIP utilizzando la console

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.

3. Nel riquadro di navigazione, seleziona Tabelle di routing del gateway locale.
4. Scegli la tabella di routing.
5. Scegli la scheda Pool CoIP nel riquadro dei dettagli, quindi scegli Crea pool CoIP.
6. (Facoltativo) In Nome, immetti un nome per il tuo pool CoIP.
7. Scegli Aggiungi nuovo CIDR e inserisci un intervallo di indirizzi IP di proprietà del cliente.
8. (Facoltativo) Per aggiungere un blocco CIDR, scegli Aggiungi nuovo CIDR e inserisci un intervallo di indirizzi IP di proprietà del cliente.
9. Scegli Crea pool CoIP.

AWS CLI

Per creare un pool CoIP utilizzando AWS CLI

1. Utilizzare il create-coip-poolcomando per creare un pool di indirizzi CoIP per la tabella di routing del gateway locale specificata.

```
aws ec2 create-coip-pool --local-gateway-route-table-id lgw-rtb-
abcdefg1234567890
```

Di seguito è riportato un output di esempio.

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

2. Utilizzare il create-coip-cidrcomando per creare un intervallo di indirizzi CoIP nel pool CoIP specificato.

```
aws ec2 create-coip-cidr --cidr 15.0.0.0/24 --coip-pool-id ipv4pool-
coip-1234567890abcdefg
```

Di seguito è riportato un output di esempio.

```
{
    "CoipCidr": {
        "Cidr": "15.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

Dopo aver creato un pool CoIP, utilizzate la procedura seguente per assegnare un indirizzo all'istanza.

Console

Per assegnare un indirizzo CoIP a un'istanza utilizzando la console

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Elastic. IPs
3. Scegli Alloca indirizzo IP elastico.
4. Per Gruppo di confine di rete, seleziona la posizione da cui vengono propagati gli indirizzi IP.
5. Per Pool di IPv4 indirizzi pubblici, scegli Pool di IPv4 indirizzi di proprietà del cliente.
6. Per Pool di IPv4 indirizzi di proprietà del cliente, seleziona il pool che hai configurato.
7. Scegli Alloca.
8. Seleziona l'indirizzo IP elastico e scegli Operazioni, Associa indirizzo IP elastico.
9. Seleziona l'istanza da Istanza, quindi scegli Associa.

AWS CLI

Per assegnare un indirizzo CoIP a un'istanza utilizzando AWS CLI

1. Utilizzate il describe-coip-poolscomando per recuperare informazioni sui pool di indirizzi di proprietà del cliente.

   ```
   aws ec2 describe-coip-pools
   ```

   Di seguito è riportato un output di esempio.

```
{
    "CoipPools": [
        {
            "PoolId": "ipv4pool-coip-0abcdef0123456789",
            "PoolCidrs":  [
                "192.168.0.0/16"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-0abcdef0123456789"
        }
    ]
}
```

2. Utilizza il comando allocate-address per allocare un indirizzo IP elastico. Utilizza l'ID del pool restituito nella fase precedente.

```
aws ec2 allocate-address--address 192.0.2.128 --customer-owned-ipv4-
pool ipv4pool-coip-0abcdef0123456789
```

Di seguito è riportato un output di esempio.

```
{
    "CustomerOwnedIp": "192.0.2.128",
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
    "CustomerOwnedIpv4Pool": "ipv4pool-coip-0abcdef0123456789",
}
```

3. Utilizza il comando associate-address per associare l'indirizzo IP elastico all'istanza Outpost. Utilizza l'ID di allocazione restituito nella fase precedente.

```
aws ec2 associate-address --allocation-id eipalloc-02463d08ceEXAMPLE --network-
interface-id eni-1a2b3c4d
```

Di seguito è riportato un output di esempio.

```
{
    "AssociationId": "eipassoc-02463d08ceEXAMPLE",
}
```

Connettività di rete locale per i rack Outposts

Sono necessari i seguenti componenti per connettere il rack Outposts alla rete locale:

- Connettività fisica dal patch panel di Outpost ai dispositivi di rete locale del cliente.
- Protocollo LACP (Link Aggregation Control Protocol) per stabilire due connessioni di gruppi di aggregazione dei collegamenti (LAG) ai dispositivi di rete Outpost e ai dispositivi di rete locale.
- Connettività LAN virtuale (VLAN) tra l'Outpost e i dispositivi di rete locale del cliente.
- point-to-pointConnettività di livello 3 per ogni VLAN.
- Protocollo BGP (Border Gateway Protocol) per l'annuncio del routing tra Outpost e il collegamento al servizio on-premise.
- BGP per l'annuncio del routing tra l'Outpost e il dispositivo di rete locale on-premise per la connettività al gateway locale.

Indice

- Connettività fisica
- Aggregazione dei collegamenti
- Virtuale LANs
- Connettività a livello di rete
- Connettività rack ACE
- Connettività BGP del collegamento al servizio
- Annuncio della sottorete e intervallo IP dell'infrastruttura del collegamento al servizio
- Connettività BGP del gateway locale
- Pubblicità della sottorete IP di proprietà del cliente del gateway locale

Connettività fisica

Un rack Outposts ha due dispositivi di rete fisici che si collegano alla rete locale.

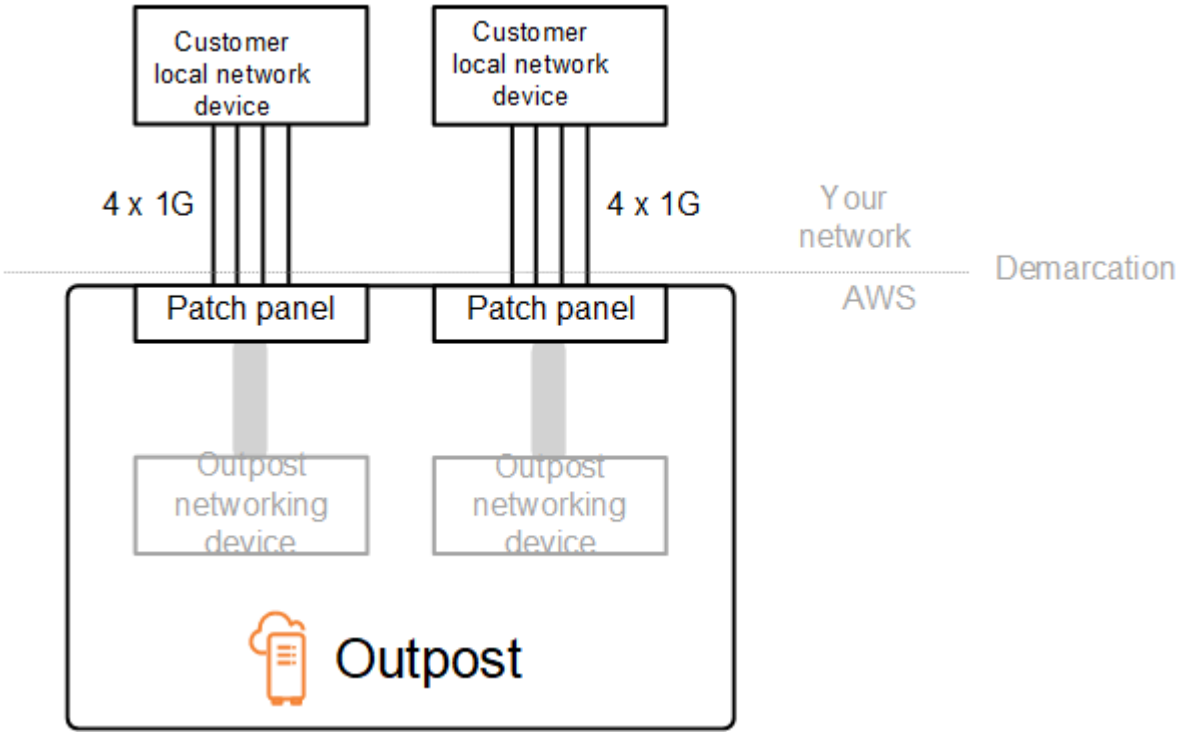
Un Outpost richiede almeno due collegamenti fisici tra questi dispositivi di rete Outpost e i dispositivi di rete locale. Un Outpost supporta le velocità e il numero di uplink indicati di seguito per ogni dispositivo di rete Outpost.

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 Gb/s o 100 Gb/s	1, 2 o 4

La velocità e il numero di uplink sono simmetrici su ogni dispositivo di rete Outpost. Se si utilizza 100 Gbps come velocità di uplink, è necessario configurare il collegamento con la correzione degli errori di inoltro (FEC). CL91

I rack Outposts possono supportare fibra monomodale (SMF) con Lucent Connector (LC), fibra multimodale (MMF) o MMF con LC. OM4 AWS fornisce le ottiche compatibili con la fibra fornita nella posizione del rack.

Nel diagramma seguente, la demarcazione fisica è rappresentata dal patch panel in fibra presente in ciascun Outpost. I cavi in fibra necessari per collegare l'Outpost al patch panel devono essere forniti da te.



Aggregazione dei collegamenti

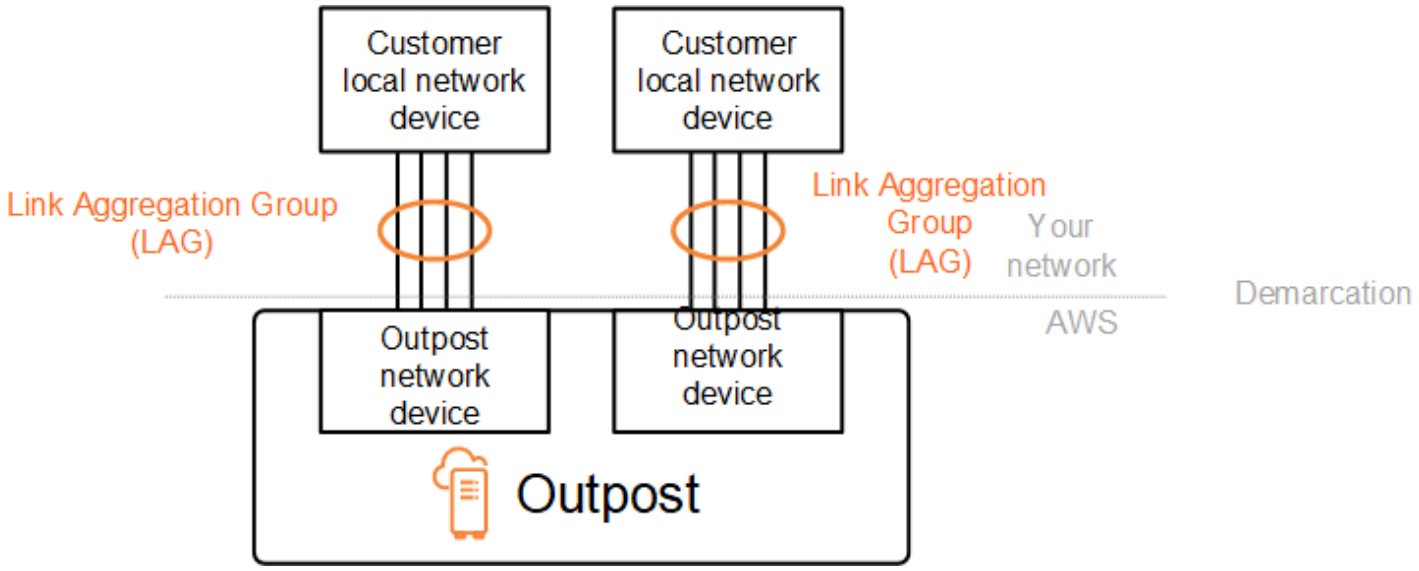
AWS Outposts utilizza il Link Aggregation Control Protocol (LACP) per stabilire connessioni LAG (Link Aggregation Group) tra i dispositivi di rete Outpost e i dispositivi di rete locale. I collegamenti da ciascun dispositivo di rete Outpost vengono aggregati in un LAG Ethernet per rappresentare una singola connessione di rete. Questi LAGs utilizzano LACP con timer veloci standard. Non è possibile configurare l'utilizzo LAGs di timer lenti.

Per abilitare un'installazione di Outpost nel tuo sito devi configurare le connessioni LAG sui dispositivi di rete dal tuo lato.

Dal punto di vista logico, ignora i patch panel di Outpost come punto di demarcazione e utilizza i dispositivi di rete Outpost.

Per le distribuzioni con più rack, un Outpost deve averne quattro LAGs tra il livello di aggregazione dei dispositivi di rete Outpost e i dispositivi di rete locali.

Il seguente diagramma mostra quattro connessioni fisiche tra ogni dispositivo di rete Outpost e il dispositivo di rete locale connesso. Utilizziamo Ethernet LAGs per aggregare i collegamenti fisici che collegano i dispositivi di rete Outpost e i dispositivi di rete locale del cliente.



Virtuale LANs

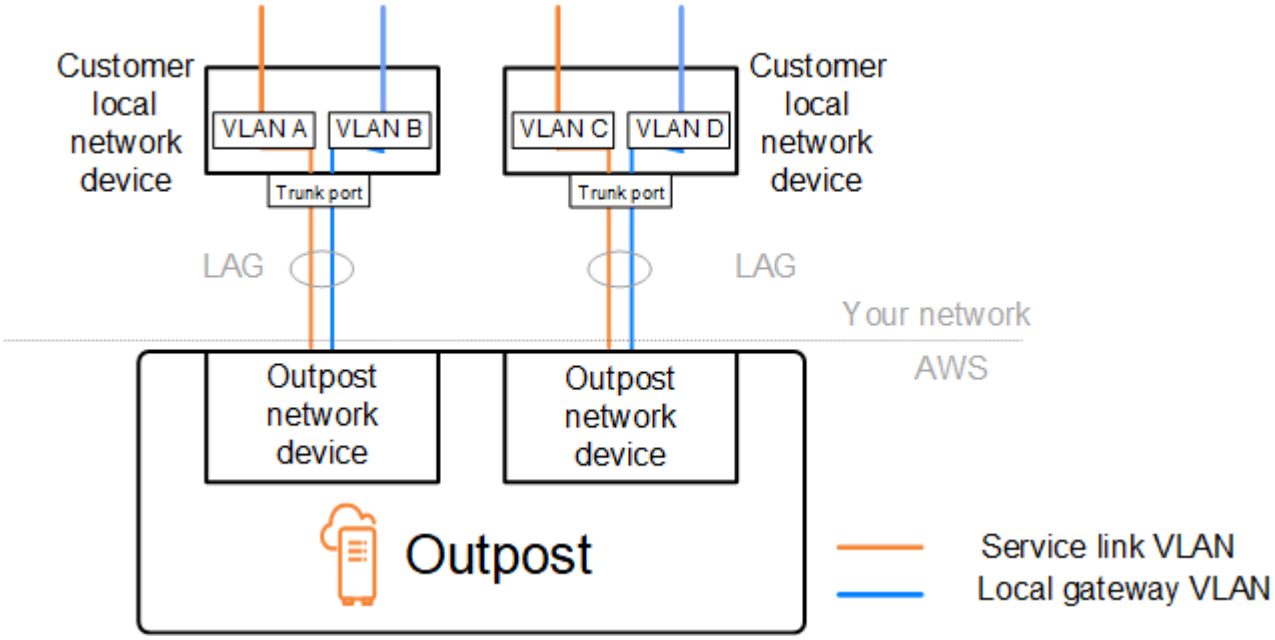
Ciascun LAG tra un dispositivo di rete Outpost e un dispositivo di rete locale deve essere configurato come trunk Ethernet IEEE 802.1q. Ciò consente l'uso di multipli VLANs per la segregazione della rete tra i percorsi di dati.

Ogni Outpost dispone di quanto segue VLANs per comunicare con i dispositivi della rete locale:

- VLAN del collegamento al servizio: consente la comunicazione tra il tuo Outpost e i dispositivi di rete locale al fine di stabilire un percorso di collegamento al servizio per la connettività di tale collegamento. Per ulteriori informazioni, consulta Connettività di AWS Outposts alle regioni AWS.
- VLAN del gateway locale: consente la comunicazione tra il tuo Outpost e i dispositivi della rete locale al fine di stabilire un percorso gateway locale per connettere le sottoreti del tuo Outpost e la tua rete locale. Il gateway locale Outpost sfrutta questa VLAN per fornire alle tue istanze la connettività alla rete on-premise, che potrebbe includere l'accesso a Internet attraverso la rete. Per ulteriori informazioni, consulta Gateway locale.

È possibile configurare la VLAN del collegamento al servizio e la VLAN del gateway locale solo tra l'Outpost e i dispositivi di rete locale del cliente.

Un Outpost è progettato per separare i percorsi dati del collegamento al servizio e del gateway locale in due reti isolate. In questo modo puoi scegliere quali delle tue reti può comunicare con i servizi in esecuzione sull'Outpost. Consente inoltre di rendere il collegamento al servizio una rete isolata dalla rete del gateway locale utilizzando una tabella di routing multipla sul dispositivo di rete locale del cliente, comunemente nota come istanze di routing e inoltro virtuali (VRF). La linea di demarcazione esiste nella porta dei dispositivi di rete Outpost. AWS gestisce qualsiasi infrastruttura sul AWS lato della connessione e tu gestisci qualsiasi infrastruttura sul lato della linea.



Per integrare Outpost con la rete locale durante l'installazione e il funzionamento continuo, è necessario allocare l'energia VLANs utilizzata tra i dispositivi di rete Outpost e i dispositivi di rete

locale del cliente. È necessario fornire queste informazioni prima dell'installazione. AWS Per ulteriori informazioni, consulta the section called “Elenco di controllo di preparazione della rete”.

Connettività a livello di rete

Per stabilire la connettività a livello di rete, ogni dispositivo di rete Outpost è configurato con interfacce virtuali (VIFs) che includono l'indirizzo IP di ogni VLAN. In questo modo VIFs, i dispositivi AWS Outposts di rete possono configurare la connettività IP e le sessioni BGP con le apparecchiature di rete locali.

Consigliamo quanto segue:

- Utilizzate una sottorete dedicata, con un CIDR /30 o /31, per rappresentare questa connettività logica. point-to-point
- Non fate da bridge VLANs tra i dispositivi della rete locale.

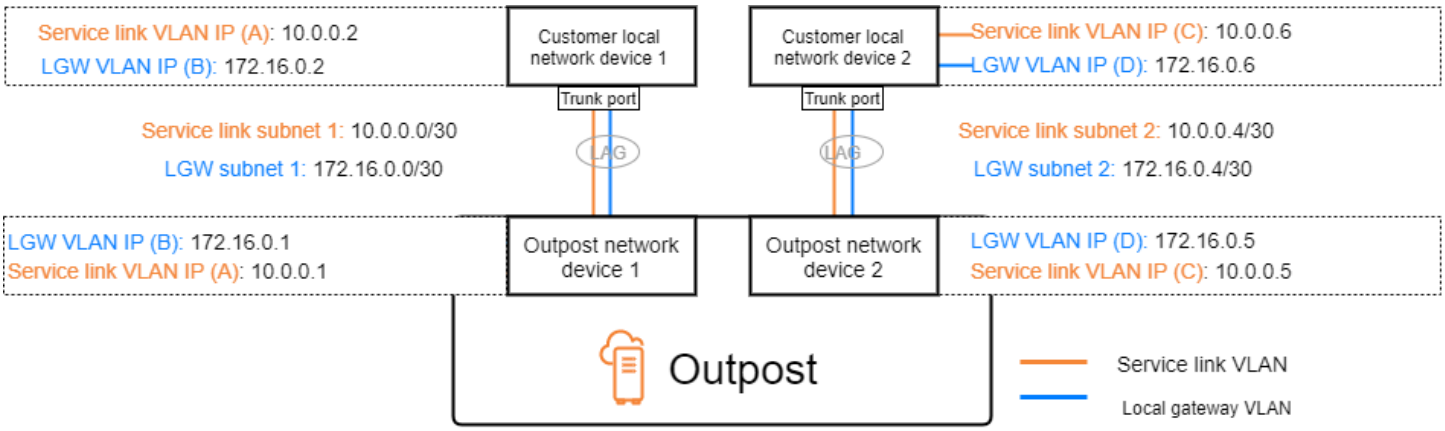
Per la connettività a livello di rete, è necessario stabilire due percorsi:

- Percorso del collegamento al servizio: per stabilire questo percorso, specifica una sottorete VLAN con un intervallo di /30 o /31 e un indirizzo IP per ogni VLAN del collegamento al servizio sul dispositivo di rete AWS Outposts . Le interfacce virtuali Service link (VIFs) vengono utilizzate per questo percorso per stabilire la connettività IP e le sessioni BGP tra Outpost e i dispositivi di rete locale per la connettività del collegamento di servizio. Per ulteriori informazioni, consulta Connettività di AWS Outposts alle regioni AWS.
- Percorso del gateway locale: per stabilire questo percorso, specifica una sottorete VLAN con un intervallo di /30 o /31 e un indirizzo IP per ogni VLAN del gateway locale sul dispositivo di rete AWS Outposts . VIFs I gateway locali vengono utilizzati su questo percorso per stabilire la connettività IP e le sessioni BGP tra Outpost e i dispositivi di rete locale per la connettività delle risorse locali.

Il seguente diagramma mostra le connessioni da ciascun dispositivo di rete Outpost al dispositivo di rete locale del cliente per il percorso del collegamento al servizio e il percorso del gateway locale. Ce ne sono quattro VLANs per questo esempio:

- La VLAN A è il percorso del collegamento al servizio che collega il dispositivo di rete Outpost 1 al dispositivo di rete locale 1 del cliente.
- La VLAN B è il percorso del gateway locale che collega il dispositivo di rete Outpost 1 al dispositivo di rete locale 1 del cliente.

- La VLAN C è il percorso del collegamento al servizio che collega il dispositivo di rete Outpost 2 al dispositivo di rete locale 2 del cliente.
- La VLAN D è il percorso del gateway locale che collega il dispositivo di rete Outpost 2 al dispositivo di rete locale 2 del cliente.



La seguente tabella mostra valori di esempio per le sottoreti che collegano il dispositivo di rete Outpost 1 al dispositivo di rete locale 1 del cliente.

VLAN	Sottorete	IP dispositivo 1 del cliente	AWS OND 1 IP
A	10.0.0.0/30	10.0.0.2	10,00,1
B	172.16.0.0/30	172,160,2	172,16,0

La seguente tabella mostra valori di esempio per le sottoreti che collegano il dispositivo di rete Outpost 2 al dispositivo di rete locale 2 del cliente.

VLAN	Sottorete	IP dispositivo 2 del cliente	AWS IP BOND 2
C	10.0.0.4/30	10.0.0.6	10.0.0.5
D	172.16.0.4/30	172.16.0.6	172.16.0.5

Connettività rack ACE

> **Note**
>
> Salta questa sezione se non hai bisogno di un rack ACE.

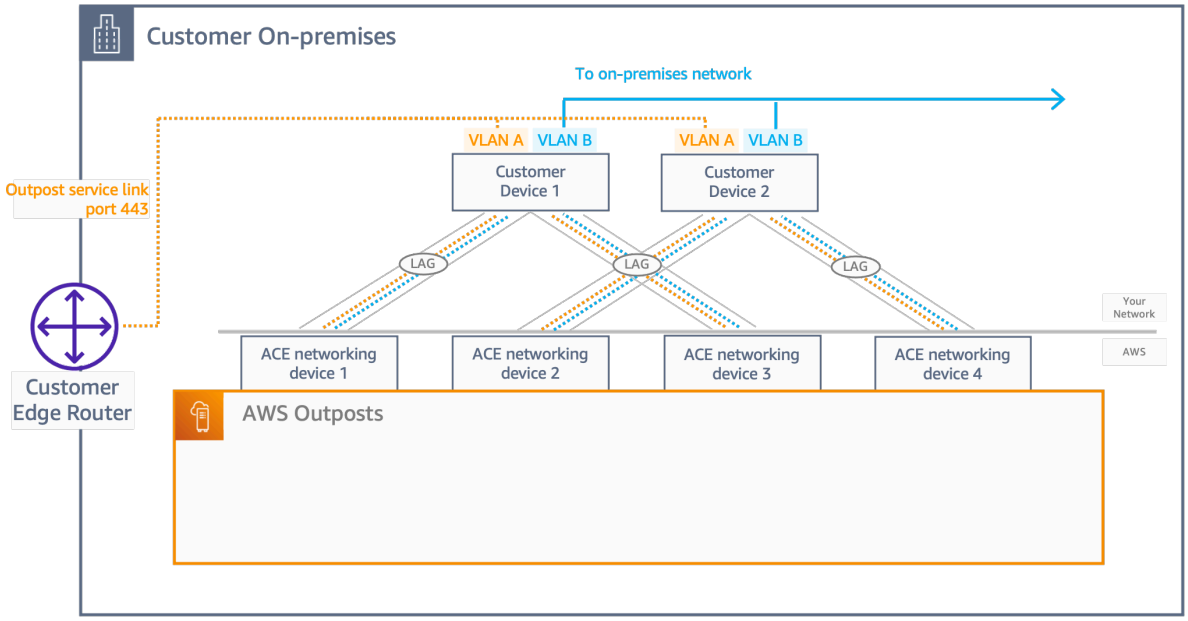
Un rack Aggregation, Core, Edge (ACE) funge da punto di aggregazione di rete per le implementazioni Outpost multi-rack. È necessario utilizzare un rack ACE se si dispone di quattro o più rack di elaborazione. Se disponi di meno di quattro rack di elaborazione ma prevedi di espanderli a quattro o più rack in futuro, ti consigliamo di installare un rack ACE al più presto.

Con un rack ACE, i dispositivi di rete Outposts non sono più collegati direttamente ai dispositivi di rete locali. Sono invece collegati al rack ACE, che fornisce la connettività ai rack Outposts. In questa topologia, AWS possiede l'allocazione e la configurazione dell'interfaccia VLAN tra i dispositivi di rete Outposts e i dispositivi di rete ACE.

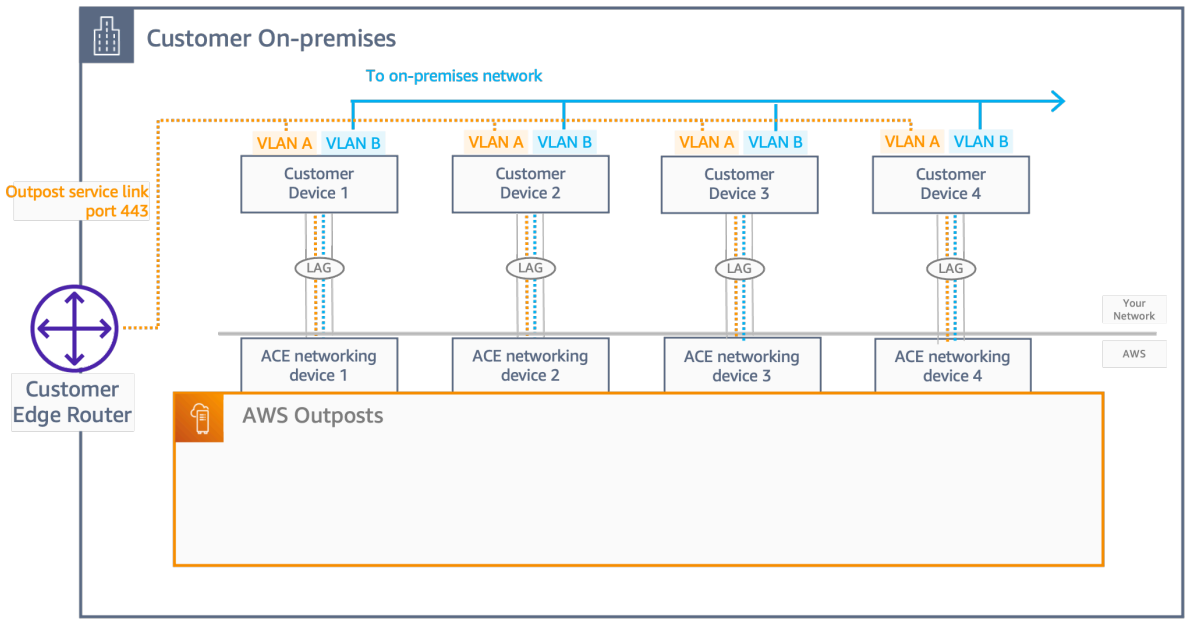
Un rack ACE include quattro dispositivi di rete che possono essere collegati a due dispositivi del cliente upstream in una rete locale del cliente o quattro dispositivi del cliente upstream per la massima resilienza.

Le immagini seguenti mostrano le due topologie di rete.

L'immagine seguente mostra i quattro dispositivi di rete ACE del rack ACE collegati a due dispositivi del cliente upstream:



L'immagine seguente mostra i quattro dispositivi di rete ACE del rack ACE collegati a quattro dispositivi upstream del cliente:



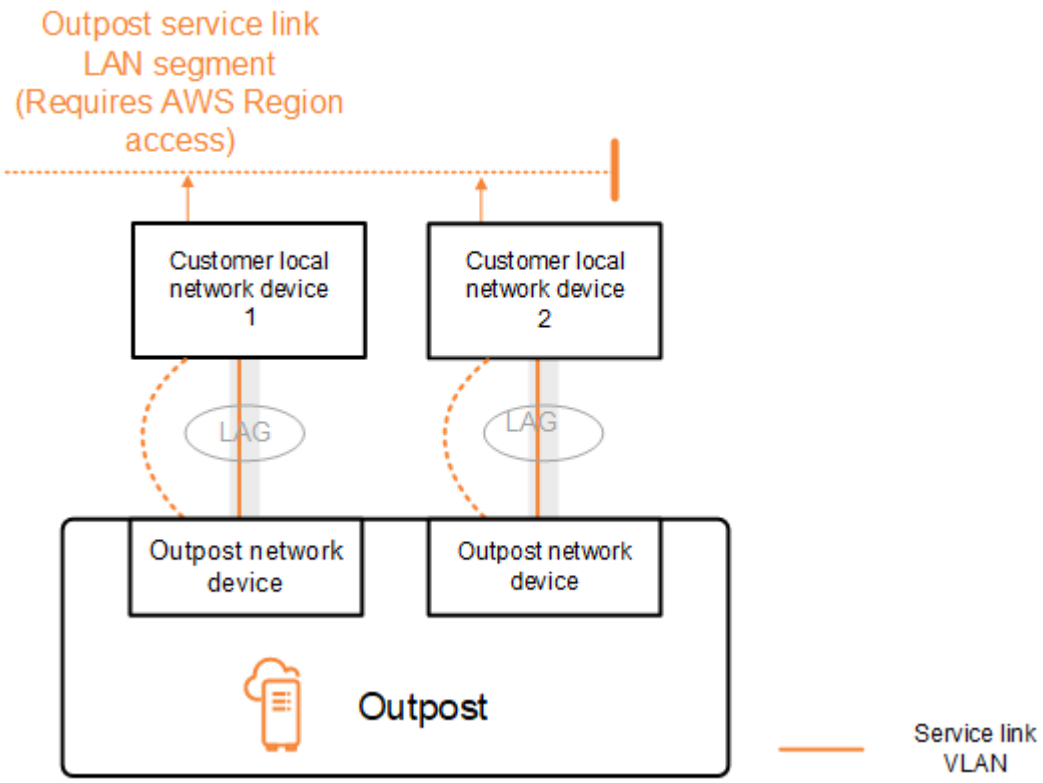
Connettività BGP del collegamento al servizio

L'Outpost stabilisce una sessione di peering BGP esterna tra ogni dispositivo di rete Outpost e il dispositivo di rete locale del cliente per la connettività del collegamento al servizio sulla relativa VLAN. La sessione di peering BGP viene stabilita tra gli indirizzi IP /30 o /31 forniti per la VLAN. point-to-point Ogni sessione di peering BGP utilizza un numero di sistema autonomo (ASN) privato sul dispositivo di rete Outpost e un ASN scelto dall'utente per i dispositivi di rete locale del cliente. Come parte del processo di installazione, AWS configura gli attributi che hai fornito.

Prendiamo in esame lo scenario in cui si dispone di un Outpost con due dispositivi di rete Outpost collegati tramite una VLAN del collegamento al servizio a due dispositivi di rete locale del cliente. Puoi configurare la seguente infrastruttura e gli attributi ASN BGP del dispositivo di rete locale del cliente per ogni collegamento al servizio:

- L'ASN BGP del collegamento di servizio. 2 byte (16 bit) o 4 byte (32 bit). I valori validi sono 64512-65535 o 4200000000-4294967294.
- L'infrastruttura CIDR. Deve essere un CIDR /26 per rack.
- Indirizzo IP peer BGP del collegamento al servizio del dispositivo di rete locale 1 del cliente.
- ASN peer BGP del collegamento al servizio del dispositivo di rete locale 1 del cliente. I valori validi sono 1-4294967294.

- Indirizzo IP peer BGP del collegamento al servizio del dispositivo di rete locale 2 del cliente.
- ASN peer BGP del collegamento al servizio del dispositivo di rete locale 2 del cliente. I valori validi sono 1-4294967294. Per ulteriori informazioni, consulta RFC4893.



L'Outpost stabilisce una sessione di peering BGP esterna sulla VLAN del collegamento al servizio applicando il seguente processo:

1. Ciascun dispositivo di rete Outpost utilizza l'ASN per stabilire una sessione di peering BGP con il dispositivo di rete locale connesso.
2. I dispositivi di rete Outpost pubblicizzano l'intervallo CIDR /26 come due intervalli CIDR /27 a supporto in caso di errori dei collegamenti e dei dispositivi. Ogni OND pubblicizza il proprio prefisso /27 con una lunghezza AS-Path di 1, più i prefissi /27 di tutti gli altri ONDs con una lunghezza AS-Path di 4 come backup.
3. La sottorete viene utilizzata per la connettività dall'Outpost alla regione. AWS

Raccomandiamo di configurare le apparecchiature di rete del cliente per ricevere annunci BGP da Outposts senza modificare gli attributi BGP. La rete del cliente dovrebbe preferire i routing provenienti da Outposts con una lunghezza AS-Path di 1 rispetto ai routing con una lunghezza AS-Path di 4.

La rete di clienti dovrebbe pubblicizzare prefissi BGP uguali con gli stessi attributi per tutti. ONDs Per impostazione predefinita, la rete Outpost bilancia il carico del traffico in uscita tra tutti gli uplink. Le policy di routing vengono utilizzate sul lato Outpost per deviare il traffico da un OND nel caso in cui sia necessario eseguire un intervento di manutenzione. Questo spostamento del traffico richiede che tutti i clienti abbiano lo stesso prefisso BGP. ONDs Nel caso in cui sia necessario eseguire un intervento di manutenzione sulla rete del cliente, raccomandiamo di utilizzare l'anteposizione di AS-Path per deviare temporaneamente la matrice del traffico da uplink specifici.

Annuncio della sottorete e intervallo IP dell'infrastruttura del collegamento al servizio

Durante il processo di preinstallazione per la sottorete dell'infrastruttura di collegamento al servizio devi fornire un intervallo CIDR /26. L'infrastruttura Outpost utilizza questo intervallo per stabilire la connettività alla regione tramite il collegamento al servizio. La sottorete del collegamento al servizio è l'origine dell'Outpost che avvia la connettività.

I dispositivi di rete Outpost pubblicizzano l'intervallo CIDR /26 come due blocchi CIDR /27 a supporto in caso di errori dei collegamenti e dei dispositivi.

È necessario fornire un ASN BGP del collegamento al servizio e una sottorete dell'infrastruttura CIDR (/26) per l'Outpost. Per ogni dispositivo di rete Outpost, fornisci l'indirizzo IP di peering BGP sulla VLAN del dispositivo di rete locale e l'ASN BGP del dispositivo di rete locale.

Se disponi di un'implementazione su più rack devi avere una sottorete /26 per rack.

Connettività BGP del gateway locale

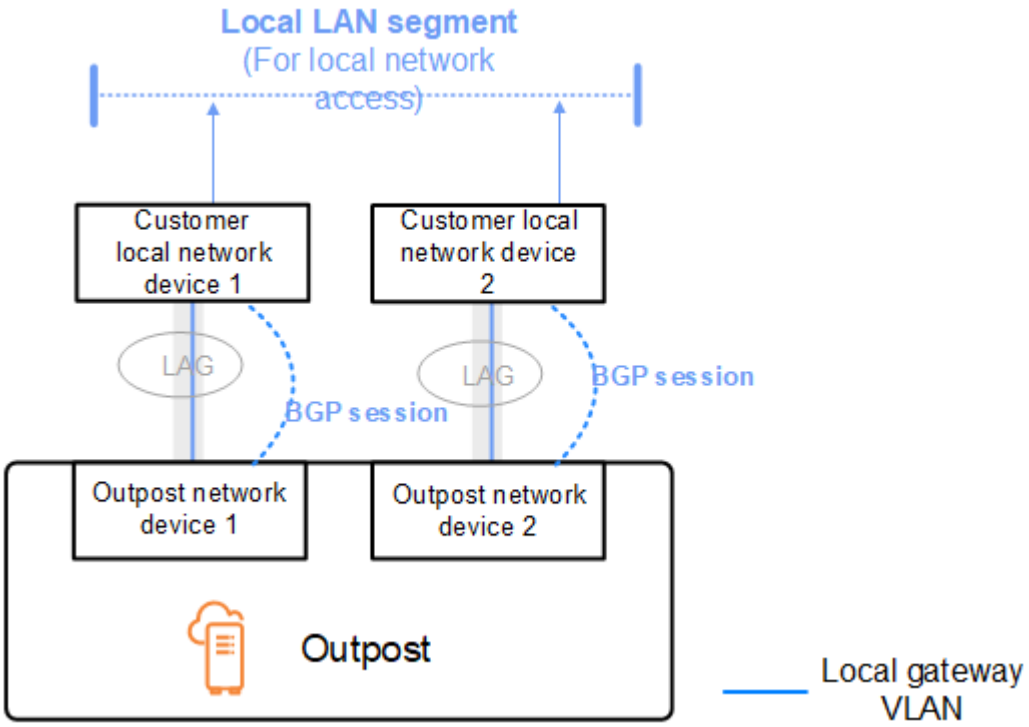
The Outpost utilizza un numero di sistema autonomo (ASN) privato assegnato dall'utente per stabilire le sessioni BGP esterne. Ogni dispositivo di rete Outpost dispone di un singolo peering BGP esterno verso un dispositivo di rete locale che utilizza la VLAN del gateway locale.

L'Outpost stabilisce una sessione di peering BGP esterna sulla VLAN del gateway locale tra ogni dispositivo di rete Outpost e il relativo dispositivo di rete locale connesso del cliente. La sessione di peering viene stabilita tra /30 o /31 IPs forniti durante la configurazione della connettività di rete e utilizza la connettività tra i dispositivi di rete Outpost e i dispositivi point-to-point di rete locale del cliente. Per ulteriori informazioni, consulta the section called “Connettività a livello di rete”.

Ogni sessione BGP utilizza l'ASN privato sul lato del dispositivo di rete Outpost e un ASN scelto dall'utente sul lato del dispositivo di rete locale del cliente. AWS configura gli attributi come parte del processo di preinstallazione.

Prendiamo in esame lo scenario in cui si dispone di un Outpost con due dispositivi di rete Outpost collegati tramite una VLAN del collegamento al servizio a due dispositivi di rete locale del cliente. Puoi configurare il seguente gateway locale e gli attributi ASN BGP del dispositivo di rete locale del cliente per ogni collegamento al servizio:

- Il cliente fornisce l'ASN BGP del gateway locale. 2 byte (16 bit) o 4 byte (32 bit). I valori validi sono 64512-65535 o 4200000000-4294967294.
- (Facoltativo) Il CIDR di proprietà del cliente che viene comunicato (pubblico o privato, minimo /26) viene fornito da te.
- L'indirizzo IP peer BGP del gateway locale del dispositivo di rete locale 1 di proprietà del cliente viene fornito da te.
- L'ASN peer BGP del gateway locale del dispositivo di rete locale 1 di proprietà del cliente viene fornito da te. I valori validi sono 1-4294967294. Per ulteriori informazioni, consulta RFC4893.
- L'indirizzo IP peer BGP del gateway locale del dispositivo di rete locale 2 di proprietà del cliente viene fornito da te.
- L'ASN peer BGP del gateway locale del dispositivo di rete locale 2 di proprietà del cliente viene fornito da te. I valori validi sono 1-4294967294. Per ulteriori informazioni, consulta RFC4893.



Raccomandiamo di configurare le apparecchiature di rete del cliente per ricevere annunci BGP da Outposts senza modificare gli attributi BGP e di abilitare il sistema di bilanciamento del carico/multipath BGP per ottenere flussi di traffico in entrata ottimali. La prependenza AS-Path viene utilizzata per i prefissi del gateway locale da cui allontanare il traffico in caso di necessità di manutenzione. ONDs La rete del cliente dovrebbe preferire i routing provenienti da Outposts con una lunghezza AS-Path di 1 rispetto ai routing con una lunghezza AS-Path di 4.

La rete di clienti dovrebbe pubblicizzare prefissi BGP uguali con gli stessi attributi per tutti. ONDs Per impostazione predefinita, la rete Outpost bilancia il carico del traffico in uscita tra tutti gli uplink. Le policy di routing vengono utilizzate sul lato Outpost per deviare il traffico da un OND nel caso in cui sia necessario eseguire un intervento di manutenzione. Questo spostamento del traffico richiede che tutti i clienti abbiano lo stesso prefisso BGP. ONDs Nel caso in cui sia necessario eseguire un intervento di manutenzione sulla rete del cliente, raccomandiamo di utilizzare l'anteposizione di AS-Path per deviare temporaneamente la matrice del traffico da uplink specifici.

Pubblicità della sottorete IP di proprietà del cliente del gateway locale

Per impostazione predefinita, il gateway locale utilizza gli indirizzi IP privati delle istanze nel tuo VPC (vedi Routing VPC diretto) per facilitare la comunicazione con la tua rete locale. Tuttavia, puoi fornire pool di indirizzi IP (CoIP) di proprietà del cliente.

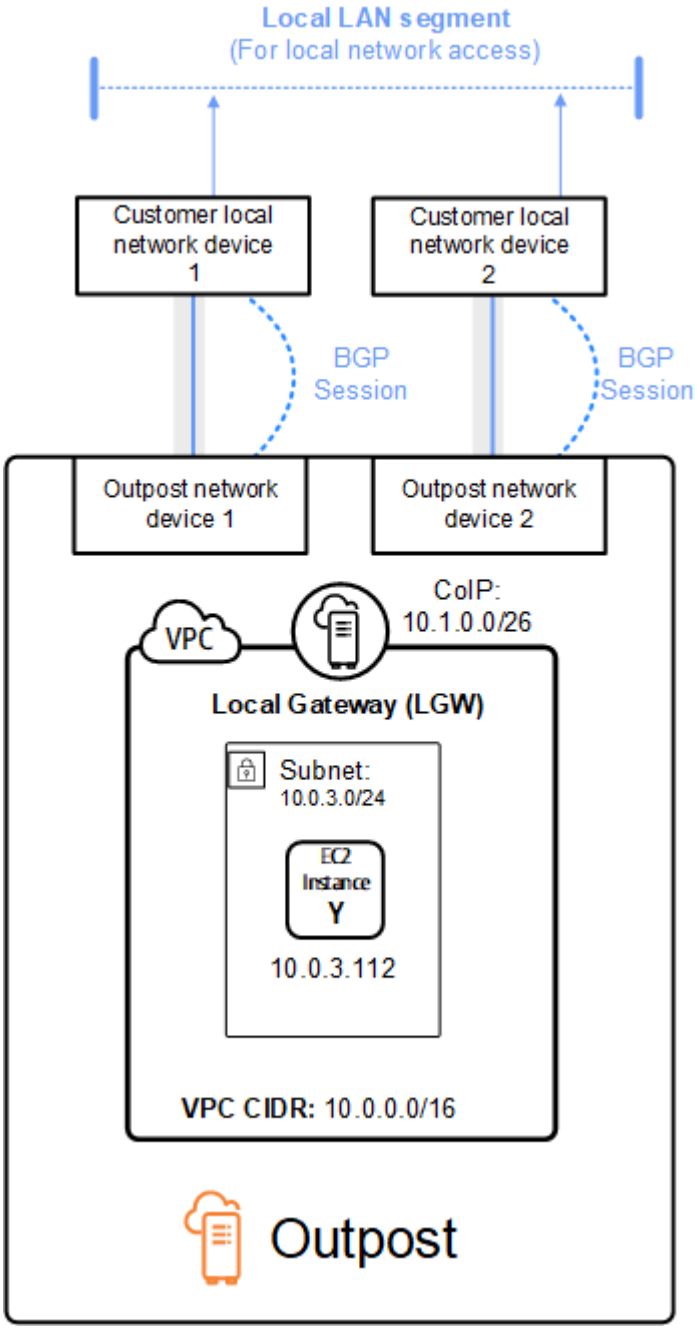
È possibile creare indirizzi IP elastici da questo pool e quindi assegnare gli indirizzi alle risorse di Outpost, ad esempio le istanze. EC2

Il gateway locale converte l'indirizzo IP elastico in un indirizzo nel pool di proprietà del cliente. Il gateway locale comunica l'indirizzo convertito sulla rete locale e su qualsiasi altra rete che comunica con l'Outpost. Gli indirizzi vengono propagati sia nelle sessioni BGP del gateway locale che nei dispositivi di rete locale.

> **Tip**
>
> Se utilizzi CoIP, BGP comunica gli indirizzi IP privati di tutte le sottoreti di Outpost che hanno un routing nella tabella di routing destinata al gateway locale.

Prendiamo in esame lo scenario in cui si dispone di un Outpost con due dispositivi di rete Outpost collegati tramite una VLAN del collegamento al servizio a due dispositivi di rete locale del cliente. Viene configurato quanto segue:

- VPC A con un blocco CIDR 10.0.0.0/16.
- Una sottorete nel VPC con un blocco CIDR 10.0.3.0/24.
- Un' EC2 istanza nella sottorete con un indirizzo IP privato 10.0.3.112.
- Pool di IP di proprietà del cliente (10.1.0.0/26).
- Un'associazione di indirizzi IP elastici che lega 10.0.3.112 a 10.1.0.2.
- Un gateway locale che utilizza BGP per propagare 10.1.0.0/26 sulla rete on-premise tramite i dispositivi locali.
- La comunicazione tra Outpost e la rete locale utilizzerà CoIP Elastic IPs per indirizzare le istanze in Outpost, l'intervallo VPC CIDR non viene utilizzato.


Local LAN segment
(For local network access)
Customer local network device 1
Customer local network device 2
BGP Session
BGP Session
Outpost network device 1
Outpost network device 2
CoIP: 10.1.0.0/26
VPC
Local Gateway (LGW)
Subnet: 10.0.3.0/24
EC2 Instance Y
10.0.3.112
VPC CIDR: 10.0.0.0/16
Outpost

Gestione della capacità per AWS Outposts

Un Outpost fornisce un pool di capacità di AWS elaborazione e archiviazione presso il sito come estensione privata di una zona di disponibilità in una AWS regione. Poiché la capacità di elaborazione e storage disponibile in Outpost è limitata e determinata dalle dimensioni e dal numero di asset da AWS installare nel tuo sito, sei tu a decidere la capacità di Amazon, Amazon EBS e Amazon S3 necessaria per eseguire i carichi di lavoro iniziali, EC2 far fronte alle crescite future e fornire AWS Outposts capacità aggiuntiva per mitigare i guasti dei server e gli eventi di manutenzione.

Argomenti

- Visualizza la capacità AWS Outposts
- Modifica la capacità delle istanze AWS Outposts
- Risoluzione dei problemi relativi alle attività relative alla capacità

Visualizza la capacità AWS Outposts

Puoi visualizzare la configurazione della capacità a livello di istanza o di Outpost.

Per visualizzare la configurazione della capacità di Outpost utilizzando la console

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Dal riquadro di navigazione a sinistra, scegli Outposts.
3. Scegli l'avamposto.
4. Nella pagina dei dettagli di Outpost, seleziona Instance view o Rack view.
   - Visualizzazione istanze: fornisce informazioni sulle istanze configurate negli Outposts e sulla distribuzione delle istanze per dimensione e famiglia.
   - Visualizzazione Rack: fornisce la visualizzazione delle istanze su ogni risorsa all'interno di ogni Outpost e consente di selezionare Modifica la capacità delle istanze per apportare modifiche alla capacità delle istanze.

Modifica la capacità delle istanze AWS Outposts

La capacità di ogni nuovo ordine Outpost è configurata con una configurazione di capacità predefinita. Puoi convertire la configurazione predefinita per creare varie istanze per soddisfare le tue

esigenze aziendali. A tale scopo, è necessario creare un task di capacità, scegliere un Outposts o un singolo asset, specificare le dimensioni e la quantità dell'istanza ed eseguire il task di capacità per implementare le modifiche.

Considerazioni

Considerate quanto segue prima di modificare la capacità dell'istanza:

- Le attività relative alla capacità possono essere eseguite solo dall' AWS account che possiede le risorse Outpost (proprietario). I consumatori non possono eseguire attività di capacità. Per ulteriori informazioni su proprietari e consumatori, consulta Condividi AWS Outposts le tue risorse.
- Le dimensioni e le quantità delle istanze possono essere definite a livello di Outpost o a livello di singolo asset.
- La capacità viene configurata automaticamente su una risorsa o su tutte le risorse di un Outpost in base a possibili configurazioni e best practice.
- Durante l'esecuzione di un'attività di capacità, le risorse associate all'avamposto selezionato possono essere isolate. Per questo motivo, ti consigliamo di creare un'attività di capacità solo quando non prevedi di lanciare nuove istanze sui tuoi Outposts.
- Puoi scegliere di eseguire l'attività relativa alla capacità all'istante o di continuare a eseguirla periodicamente nelle prossime 48 ore. La scelta dell'esecuzione immediata richiede meno tempo di isolamento delle risorse, ma l'operazione potrebbe fallire se è necessario interrompere le istanze per eseguirla. La scelta dell'esecuzione periodica consente di avere più tempo per arrestare le istanze prima che l'operazione abbia esito negativo, ma le risorse possono rimanere isolate più a lungo.
- È possibile che configurazioni di capacità valide non utilizzino tutte le vCPU disponibili su un asset. In tal caso, un messaggio alla fine della sezione Tipo di istanza ti informerà che la capacità è insufficiente, ma consentirà di applicare la configurazione come richiesto.
- Quando modifichi un Outpost nella console, non tutte le istanze supportate vengono visualizzate perché la combinazione di istanze con backup su disco con non-disk-backed istanze non è completamente supportata nella console. Per accedere a tutte le istanze possibili, utilizza l'API. StartCapacityTask
- Quando si definisce la capacità di un Outpost, tutte le famiglie e i tipi di istanze verranno inclusi nella riconfigurazione, a meno che non vengano elencati come istanze da evitare.
- Puoi modificare la configurazione della capacità di Outposts esistente solo per utilizzare EC2 istanze Amazon di dimensioni valide provenienti da famiglie di istanze supportate nel tuo rispettivo modello di asset.

- Se hai istanze in esecuzione su Outpost che non vuoi interrompere per eseguire un'attività di capacità, seleziona il rispettivo ID di istanza nella sezione Istanze da mantenere così com'è (facoltativo) e assicurati di conservare la quantità necessaria di questa dimensione dell'istanza nella configurazione di capacità aggiornata. In questo modo verranno mantenute le istanze utilizzate per supportare i carichi di lavoro di produzione durante l'esecuzione di un'attività di capacità.
- Quando configuri un asset con istanze di dimensioni diverse all'interno di una famiglia di istanze, utilizza Auto-balance per assicurarti di non tentare di sovra-fornire o sottodimensionare il droplet. L'over-provisioning non è supportato e causerà un errore nell'attività relativa alla capacità.
- Se desideri riconfigurare completamente una famiglia di istanze su Outpost senza mantenere nessuna delle dimensioni delle istanze della configurazione di capacità originale, devi interrompere tutte le istanze in esecuzione di quella famiglia su Outpost prima di eseguire l'attività di capacità. Se l'istanza è di proprietà di un altro account o viene utilizzata da un servizio a più livelli in esecuzione su Outpost, è necessario utilizzare l'account del proprietario dell'istanza per interrompere l'istanza o l'istanza del servizio.
- Diverse attività di capacità possono essere eseguite in parallelo purché si applichino a set di Asset di Asset che si escludono a vicenda. IDs Ad esempio, è possibile creare più attività di capacità a livello di asset per diversi Asset IDs contemporaneamente. Tuttavia, se è in esecuzione un'attività a livello di Outpost, non è possibile creare contemporaneamente un'altra attività a livello di Outpost o di risorsa. Analogamente, se è in esecuzione un'attività a livello di risorsa, non è possibile creare contemporaneamente un'attività a livello di Outpost o un'attività a livello di risorsa sullo stesso AssetID.

Per modificare la configurazione della capacità di Outpost utilizzando la console

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Dal riquadro di navigazione a sinistra, scegli Attività relative alla capacità.
3. Nella pagina Attività di capacità, scegli Crea attività di capacità.
4. Nella pagina Guida introduttiva, scegli l'ordine, Outpost o la risorsa da configurare.
5. Per modificare la capacità, specifica un'opzione per Metodo di modifica: e passaggi nella console o carica un file JSON.
   - Modifica il piano di configurazione della capacità per utilizzare i passaggi della console
   - Carica un piano di configurazione della capacità per caricare un file JSON

> **Note**
>
> - Per evitare che la gestione della capacità consigli l'interruzione di istanze specifiche, specifica le istanze che non devono essere interrotte. Queste istanze verranno escluse dall'elenco delle istanze da interrompere.

Console steps

1. Scegliete Instance view o Rack view.
2. Scegli Modifica una configurazione della capacità di Outpost o Modifica su un singolo asset.
3. Scegli un Outpost o una risorsa se diversa dalla selezione corrente.
4. Scegli di eseguire questa attività di capacità immediatamente o periodicamente per 48 ore.
5. Scegli Next (Successivo).
6. Nella pagina Configura la capacità dell'istanza, ogni tipo di istanza mostra una dimensione di istanza con la quantità massima preselezionata. Per aggiungere altre dimensioni di istanza, scegli Aggiungi dimensione dell'istanza.
7. Specificate la quantità dell'istanza e annotate la capacità visualizzata per quella dimensione dell'istanza.
8. Visualizza il messaggio alla fine di ogni sezione relativa al tipo di istanza che ti informa se la capacità è eccessiva o insufficiente. Effettua modifiche a livello di dimensione o quantità dell'istanza per ottimizzare la capacità totale disponibile.
9. Puoi anche richiedere di AWS Outposts ottimizzare la quantità di istanze per una dimensione specifica dell'istanza. A tale scopo:
   a. Scegli la dimensione dell'istanza.
   b. Scegli Bilanciamento automatico alla fine della sezione relativa al tipo di istanza.
10. Per ogni tipo di istanza, assicurati che la quantità di istanza sia specificata per almeno una dimensione di istanza.
11. Facoltativamente, scegli le istanze da mantenere così come sono.
12. Scegli Next (Successivo).
13. Nella pagina Rivedi e crea, verifica gli aggiornamenti richiesti.
14. Scegli Crea. AWS Outposts crea un'attività di capacità.
15. Nella pagina dell'attività di capacità, monitora lo stato dell'attività.

Upload a JSON file

1. Scegli Carica una configurazione di capacità.
2. Scegli Next (Successivo).
3. Nella pagina del piano di configurazione della capacità di caricamento, carica il file JSON che specifica il tipo, la dimensione e la quantità dell'istanza. Facoltativamente, puoi specificare i InstancesToExcludeTaskActionOnBlockingInstancesparametri e nel file JSON.

   Example

   File JSON di esempio:

```
{
  "InstancePools": [
    {
      "InstanceType": "c5.24xlarge",
      "Count": 1
    },
    {
      "InstanceType": "m5.24xlarge",
      "Count": 2
    }
  ],
  "InstancesToExclude": {
    "AccountIds": [
      "111122223333"
    ],
    "Instances": [
      "i-1234567890abcdef0"
    ],
    "Services": [
      "ALB"
    ]
  },
  "TaskActionOnBlockingInstances": "WAIT_FOR_EVACUATION"
}
```

4. Esamina il contenuto del file JSON nella sezione Piano di configurazione della capacità.
5. Scegli Next (Successivo).
6. Nella pagina Rivedi e crea, verifica gli aggiornamenti che stai richiedendo.
7. Scegli Crea. AWS Outposts crea un'attività di capacità.

8. Nella pagina dell'attività di capacità, monitora lo stato dell'attività.

Risoluzione dei problemi relativi alle attività relative alla capacità

Esamina i seguenti problemi noti per risolvere un problema relativo alla gestione della capacità in un nuovo ordine. Se non vedi il tuo problema nell'elenco, contatta Supporto.

*oo-xxxxxx*L'ordine non è associato a Outpost ID *op-xxxxx*

Questo problema si verifica quando utilizzi l'API AWS CLI or per eseguire l'Outpost ID `StartCapacityTask`e l'ID Outpost nella richiesta non corrisponde all'ID Outpost nell'ordine.

Per risolvere il problema:

1. Accedi a. AWS
2. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
3. Dal pannello di navigazione, scegli Ordini.
4. Seleziona l'ordine e verifica che lo stato dell'ordine sia uno dei seguenti: `PREPARINGIN_PROGRESS`, o`ACTIVE`.
5. Annota l'ID Outpost nell'ordine.
6. Inserisci l'ID Outpost corretto nella richiesta `StartCapacityTask` API.

Il piano di capacità include tipi di istanze non supportati

Questo problema si verifica quando si utilizza l'API AWS CLI o per creare o modificare l'attività di capacità e la richiesta contiene tipi di istanze non supportati.

Per risolvere questo problema, usa la console o la CLI.

Utilizzo della console

1. Accedi a. AWS
2. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
3. Dal riquadro di navigazione, scegli l'attività Capacity.
4. Utilizza l'opzione di configurazione Carica una capacità per caricare un JSON con lo stesso elenco di tipi di istanze.
5. La console visualizza un messaggio di errore con l'elenco dei tipi di istanze supportati.

6. Correggi la richiesta per rimuovere i tipi di istanza non supportati.
7. Crea o modifica l'attività di capacità sulla console utilizzando il JSON corretto o utilizza la CLI o l'API con questo elenco corretto di tipi di istanze.

Utilizzo della CLI

1. Usa il GetOutpostSupportedInstanceTypescomando per visualizzare l'elenco dei tipi di istanze supportati.
2. Crea o modifica l'attività di capacità con l'elenco corretto di tipi di istanze.

Nessun Outpost con Outpost ID *op-xxxxx*

Questo problema si verifica quando utilizzi l'API AWS CLI or per eseguire `StartCapacityTask`e la richiesta contiene un ID Outpost che non è valido per uno dei seguenti motivi:

- L'Outpost si trova in una regione diversa AWS .
- Non hai i permessi per questo avamposto.
- L'ID Outpost non è corretto.

Per risolvere il problema:

1. Annota la AWS regione che hai usato nella richiesta `StartCapacityTask` API.
2. Usa l'azione `ListOutposts`API per ottenere un elenco di Outposts di tua proprietà nella AWS regione.
3. Controlla se l'ID Outpost è presente nell'elenco.
4. Inserisci l'ID Outpost corretto nella `StartCapacityTask` richiesta.
5. Se non trovi l'Outpost ID, utilizza nuovamente l'azione `ListOutposts` API per verificare se l'Outpost esiste in un'altra regione. AWS

CapacityTaskCappuccio attivo, *XXXX* già trovato per Outpost op *XXXX*

Questo problema si verifica quando si utilizza la AWS Outposts console o l'API per l'esecuzione StartCapacityTasksu Outpost ed è già presente un'attività di capacità in esecuzione per Outpost. Un'attività di capacità è considerata in esecuzione se presenta uno dei seguenti stati:`REQUESTED`,`IN_PROGRESS`, `WAITING_FOR_EVACUATION` o. `CANCELLATION_IN_PROGRESS`

Per risolvere questo problema, usa la AWS Outposts console o la CLI.

Utilizzo della console

1. Accedi a. AWS
2. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
3. Dal pannello di navigazione, scegli Attività relative alla capacità.
4. Assicurati che non vi siano attività di capacità in esecuzione per OutpostId.
5. Se sono presenti attività relative alla capacità in esecuzione di OutpostId, attendi che terminino o annullale se lo desideri.
6. Se non sono presenti attività di capacità in esecuzione per quanto richiesto OutpostId, riprova la richiesta per creare l'attività di capacità.

Utilizzo della CLI

1. Usa il ListCapacityTaskscomando per trovare le attività relative alla capacità di esecuzione per Outpost.
2. Attendi che tutte le attività relative alla capacità di esecuzione terminino o, se lo desideri, annullale.
3. Se non sono presenti attività di capacità in esecuzione per quella richiesta OutpostId, riprova a eseguire la richiesta per creare l'attività di capacità.

CapacityTaskCap attivo: *XXXX* già trovato per Asset *XXXX* su Outpost OP-xxxx

Questo problema si verifica quando si utilizza la AWS Outposts console o l'API per l'esecuzione StartCapacityTasksu una risorsa ed è già presente un'attività relativa alla capacità in esecuzione per la risorsa. Un'attività di capacità è considerata in esecuzione se presenta uno dei seguenti stati:`REQUESTED`, `IN_PROGRESSWAITING_FOR_EVACUATION`, o`CANCELLATION_IN_PROGRESS`.

Per risolvere questo problema, usa la AWS Outposts console o la CLI.

Utilizzo della console

1. Accedi a. AWS
2. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.

3. Dal pannello di navigazione, scegli Attività relative alla capacità.
4. Assicurati che non vi siano attività di capacità in esecuzione per OutpostId e che non vi siano attività di capacità a livello di asset in esecuzione per. AssetId
5. Se sono presenti attività con capacità in esecuzione, attendi che terminino o annullale se lo desideri.
6. Se non sono presenti attività di capacità in esecuzione, riprova a eseguire la richiesta per creare l'attività di capacità.

Utilizzo della CLI

1. Utilizzate il ListCapacityTaskscomando per trovare le attività relative alla capacità in esecuzione per OutpostID e AssetID.
2. Assicurati che non siano in esecuzione attività di capacità a livello di Outpost per e che non siano in esecuzione attività di capacità a livello di asset per. OutpostId AssetId
3. Se sono presenti attività con capacità in esecuzione, attendi che terminino o annullale se lo desideri.
4. Riprova la richiesta per creare il task di capacità.

AssetId= non *XXXX* è valido per outpost=op- *XXXX*

Questo problema si verifica quando si utilizza la AWS Outposts console o l'API per l'esecuzione StartCapacityTasksu una risorsa e l'AssetID non è valido per uno dei seguenti motivi:

- La risorsa non è associata all'Outpost.
- La risorsa è isolata.

Per risolvere questo problema, usa la AWS Outposts console o la CLI.

Utilizzo della console

1. Accedi a. AWS
2. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
3. Scegli Rack view for the Outpost.
4. Verifica che la richiesta AssetId sia associata all'Outpost e che non sia contrassegnata come Host isolato.

   a. Se l'Asset è isolato, è possibile che su di esso sia in esecuzione un'attività di capacità. Puoi accedere al pannello delle attività relative alla capacità e verificare se sono in esecuzione attività di Outpost o a livello di risorsa per e. OutpostId AssetId Se ce ne sono, attendi che l'attività termini e che la risorsa torni a essere disponibile.
   b. Se non sono presenti attività di capacità in esecuzione per una risorsa isolata, la risorsa potrebbe subire un deterioramento.
5. Dopo aver verificato che la risorsa esista e si trovi in uno stato valido, riprova la richiesta per creare l'attività di capacità.

Utilizzo della CLI

1. Utilizzate il ListAssetscomando per trovare le risorse associate a OutpostID.
2. Verifica che la richiesta AssetId sia associata all'Outpost e che il relativo Stato lo sia. `ACTIVE`
   a. Se lo stato dell'asset non è ATTIVO, è possibile che su di esso sia in esecuzione un'attività di capacità. Usa il ListCapacityTaskscomando per determinare se sono in esecuzione attività Outpost o a livello di asset per e. OutpostId AssetId Se ce ne sono, attendi che l'attività termini e che la risorsa torni ad essere ATTIVA.
   b. Se non sono presenti attività di capacità in esecuzione per un asset isolato, l'asset potrebbe subire un deterioramento.
3. Dopo aver verificato che la risorsa esista e si trovi in uno stato valido, riprova la richiesta per creare l'attività di capacità.

Condividi le tue AWS Outposts risorse

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 della stessa organizzazione. AWS AWS In qualità di proprietario di Outpost, puoi creare e gestire le risorse di Outpost centralmente e condividerle tra più account all'interno della tua organizzazione. AWS AWS Ciò consente ad altri utenti di utilizzare i siti Outpost, configurare VPCs, avviare ed eseguire istanze sull'Outpost condiviso.

In questo modello, l' AWS account proprietario delle risorse Outpost (proprietario) condivide le risorse con altri AWS account (consumatori) della stessa organizzazione. Gli utenti possono creare risorse su Outpost condivisi con loro così come creerebbero risorse negli Outpost che creano nel proprio account. Il proprietario è responsabile della gestione dell'Outpost e delle risorse create nello stesso. I proprietari possono modificare o revocare l'accesso condiviso in qualsiasi momento. Ad eccezione delle istanze che utilizzano Prenotazioni della capacità, i proprietari possono anche visualizzare, modificare ed eliminare le risorse create dagli utenti negli Outpost condivisi. I proprietari non possono modificare le istanze che i consumatori avviano in Capacity Reservations e che hanno condiviso.

Gli utenti sono responsabili della gestione delle risorse create negli Outpost condivisi con loro, incluse le risorse che utilizzano Prenotazioni della capacità. Gli utenti non possono visualizzare o modificare le risorse di proprietà di altri utenti o del proprietario dell'Outpost. Inoltre, non possono modificare gli Outpost condivisi con loro.

Un proprietario di Outpost può condividere le risorse Outpost con:

- AWS Account specifici all'interno della sua organizzazione in AWS Organizations.
- Un'unità organizzativa all'interno dell'organizzazione in AWS Organizations.
- L'intera organizzazione in AWS Organizations.

Indice

- Risorse Outpost condivisibili
- Prerequisiti per la condivisione delle risorse Outposts
- Servizi correlati
- Condivisione tra le zone di disponibilità
- Condivisione di una risorsa Outpost
- Annullamento della condivisione di una risorsa Outpost

- Individuazione di una risorsa Outpost condivisa
- Autorizzazioni per le risorse Outpost condivise
- Fatturazione e misurazione
- Limitazioni

Risorse Outpost condivisibili

Un proprietario di Outpost può condividere le risorse Outpost elencate in questa sezione con gli utenti.

- Host dedicati allocati: gli utenti con accesso a questa risorsa possono:
  - Avvia ed esegui EC2 le istanze su un host dedicato.
- Prenotazioni della capacità: gli utenti con accesso a questa risorsa possono:
  - Individuare le Prenotazioni della capacità condivise con loro.
  - Avviare e gestire le istanze che utilizzano le Prenotazioni della capacità.
- Pool di indirizzi IP di proprietà del cliente (CoIP): gli utenti con accesso a questa risorsa possono:
  - Allocare e associare gli indirizzi IP di proprietà del cliente alle istanze.
- Tabelle di routing del gateway locale: gli utenti con accesso a questa risorsa possono:
  - Creare e gestire associazioni VPC a un gateway locale.
  - Visualizzare le configurazioni delle tabelle di routing e delle interfacce virtuali del gateway locale.
- Outposts: gli utenti che hanno accesso a questa risorsa possono:
  - Creare e gestire le sottoreti nell'Outpost.
  - Creare e gestire i volumi EBS nell'Outpost.
  - Utilizza l' AWS Outposts API per visualizzare le informazioni sull'Outpost.
- S3 su Outposts: gli utenti che hanno accesso a questa risorsa possono:
  - Creare e gestire bucket S3, punti di accesso ed endpoint sull'Outpost.
- Siti: gli utenti che hanno accesso a questa risorsa possono:
  - Creare, gestire e controllare un Outpost sul sito.
- Sottoreti: gli utenti che hanno accesso a questa risorsa possono:
  - Visualizzare le informazioni sulle sottoreti.
  - Avvia ed esegui EC2 istanze nelle sottoreti.

Utilizzare la console Amazon VPC per condividere una sottorete Outpost. Per ulteriori informazioni, consulta Condivisione di una sottorete nella Guida per l'utente di Amazon VPC.

Prerequisiti per la condivisione delle risorse Outposts

- Per condividere una risorsa Outpost con la tua organizzazione o con un'unità organizzativa in AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .
- Per condividere una risorsa Outpost, devi possederla nel tuo account. AWS Non puoi condividere una risorsa Outpost che è stata condivisa con te.
- Per condividere una risorsa Outpost, devi condividerla con un account interno alla tua organizzazione.

Servizi correlati

La condivisione delle risorse Outpost si integra con AWS Resource Access Manager ().AWS RAM AWS RAM è un servizio che ti consente di condividere AWS le tue risorse con qualsiasi AWS account o tramite. AWS Organizations Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione in AWS Organizations.

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Condivisione tra le zone di disponibilità

Per garantire che le risorse vengano distribuite tra le zone di disponibilità di una regione, mappiamo in modo indipendente le zone di disponibilità ai nomi per ciascun account. Questo potrebbe comportare una diversa denominazione delle zone di disponibilità tra i diversi account. Ad esempio, la zona `us-east-1a` di disponibilità del tuo AWS account potrebbe non avere la stessa posizione `us-east-1a` di un altro AWS account.

Per individuare la posizione della risorsa Outpost relativa ai tuoi account, devi utilizzare l'ID zona di disponibilità (ID AZ). L'ID AZ è un identificatore univoco e coerente per una zona di disponibilità per tutti gli AWS account. Ad esempio, `use1-az1` è un ID AZ per la `us-east-1` regione ed è la stessa posizione in ogni AWS account.

Per visualizzare le IDs zone di disponibilità nel tuo account

1. Accedi alla AWS RAM console all'interno della AWS RAM console.
2. Le AZ IDs per la regione corrente vengono visualizzate nel pannello Your AZ ID sul lato destro dello schermo.

> **Note**
>
> Le tabelle di routing del gateway locale si trovano nella stessa AZ di Outpost, pertanto non è necessario specificare un ID AZ per le tabelle di routing.

Condivisione di una risorsa Outpost

Quando un proprietario condivide un Outpost con un utente, l'utente può creare risorse sull'Outpost così come creerebbe risorse negli Outpost che crea nel proprio account. Gli utenti con accesso alle tabelle di routing del gateway locale condivise possono creare e gestire associazioni VPC. Per ulteriori informazioni, consulta Risorse Outpost condivisibili.

Per condividere una risorsa Outpost, devi aggiungerla a una condivisione di risorse. Una condivisione di risorse è una AWS RAM risorsa che ti consente di condividere le tue risorse tra AWS account. Una condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise. Quando condividi una risorsa Outpost utilizzando la AWS Outposts console, la aggiungi a una condivisione di risorse esistente. Per aggiungere la risorsa Outpost a una nuova condivisione di risorse, devi prima creare la condivisione di risorse la console AWS RAM.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, puoi concedere ai consumatori dell'organizzazione l'accesso dalla AWS RAM console alla risorsa Outpost condivisa. In caso contrario, gli utenti ricevono un invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'accesso alla risorsa Outpost condivisa.

Puoi condividere una risorsa Outpost di tua proprietà utilizzando la AWS Outposts console, la AWS RAM console o il. AWS CLI

Per condividere una Outpost di tua proprietà usando la console AWS Outposts

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Nel riquadro di navigazione, scegli Outposts.

3. Seleziona l'Outpost, quindi scegli Operazioni, Visualizza i dettagli.
4. Nella pagina Riepilogo outpost, scegli Condivisioni di risorse.
5. Seleziona Crea condivisione risorse.

Verrai reindirizzato alla AWS RAM console per completare la condivisione di Outpost utilizzando la seguente procedura. Per condividere una tabella di routing del gateway locale di tua proprietà, utilizza anche la seguente procedura.

Per condividere un Outpost o una tabella di routing del gateway locale di cui sei proprietario mediante la console AWS RAM

Consulta Creazione di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per condividere una tabella di routing di Outpost o di un gateway locale di tua proprietà, utilizza la AWS CLI

Utilizza il comando create-resource-share.

Annullamento della condivisione di una risorsa Outpost

Quando annulli la condivisione di Outpost con un consumatore, quest'ultimo non può più fare quanto segue:

- Visualizza Outpost nella console. AWS Outposts
- Crea nuove sottoreti sull'Outpost.
- Crea nuovi volumi Amazon EBS su Outpost.
- Visualizza i dettagli e i tipi di istanza di Outpost utilizzando la AWS Outposts console o il. AWS CLI

Le sottoreti, i volumi o le istanze che il consumatore ha creato durante il periodo di condivisione non vengono eliminati e il consumatore può continuare a fare quanto segue:

- Accedi e modifica queste risorse.
- Avvia nuove istanze su una sottorete esistente creata dal consumatore.

Per impedire al consumatore di accedere alle proprie risorse e avviare nuove istanze su Outpost, richiedi che il consumatore elimini le proprie risorse.

Quando una tabella di routing gateway locale condivisa non è condivisa, il consumatore non può più creare nuove associazioni VPC ad essa. Tutte le associazioni VPC esistenti create dal consumatore rimangono associate alla tabella di routing. Le risorse in esse VPCs contenute possono continuare a indirizzare il traffico verso il gateway locale. Per evitare che ciò accada, richiedi al consumatore di eliminare le associazioni VPC.

Per annullare la condivisione di una risorsa Outpost, è sufficiente rimuoverla dalla relativa condivisione di risorse. Puoi farlo usando la AWS RAM console o il AWS CLI.

Per annullare la condivisione di una risorsa Outpost condivisa di tua proprietà utilizzando la console AWS RAM

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per annullare la condivisione di una risorsa Outpost condivisa di tua proprietà utilizzando il AWS CLI

Utilizza il comando disassociate-resource-share.

Individuazione di una risorsa Outpost condivisa

I proprietari e i consumatori possono identificare gli Outposts condivisi utilizzando la AWS Outposts console e. AWS CLI Possono individuare le tabelle di routing del gateway locale condiviso tramite AWS CLI.

Per identificare un Outpost condiviso utilizzando la console AWS Outposts

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Nel riquadro di navigazione, scegli Outposts.
3. Seleziona l'Outpost, quindi scegli Operazioni, Visualizza i dettagli.
4. Nella pagina di riepilogo di Outpost, visualizza l'ID proprietario per identificare l'ID dell' AWS account del proprietario di Outpost.

Per identificare una risorsa Outpost condivisa utilizzando il AWS CLI

Usa i comandi list-outposts e -tables. describe-local-gateway-route Questi comandi restituiscono le risorse Outpost che possiedi e le risorse Outpost condivise con te. `OwnerId`mostra l'ID dell' AWS account del proprietario della risorsa Outpost.

Autorizzazioni per le risorse Outpost condivise

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione dell'Outpost e delle risorse create nello stesso. I proprietari possono modificare o revocare l'accesso condiviso in qualsiasi momento. Possono essere utilizzate AWS Organizations per visualizzare, modificare ed eliminare le risorse create dai consumatori su Outposts condivisi.

Autorizzazioni per gli utenti

Gli utenti possono creare risorse su Outpost condivisi con loro così come creerebbero risorse negli Outpost che creano nel proprio account. Gli utenti sono responsabili della gestione delle risorse che avviano negli Outpost condivisi con loro. Gli utenti non possono visualizzare o modificare le risorse appartenenti ad altri utenti o al proprietario dell'Outpost e non possono modificarle gli Outpost condivisi con loro.

Fatturazione e misurazione

Ai proprietari vengono fatturati gli Outpost e le risorse Outpost che condividono. Vengono inoltre addebitati gli eventuali costi di trasferimento dati associati al traffico VPN di collegamento del servizio Outpost proveniente dalla regione. AWS

Non sono previsti costi aggiuntivi per la condivisione delle tabelle di routing del gateway locale. Per le sottoreti condivise, al proprietario del VPC vengono fatturate le risorse a livello di VPC come connessioni VPN, gateway NAT AWS Direct Connect e connessioni Private Link.

Agli utenti vengono fatturate le risorse applicative che creano su Outpost condivisi, come sistemi di bilanciamento del carico e database Amazon RDS. Ai consumatori vengono inoltre fatturati i trasferimenti di dati a pagamento dalla Regione. AWS

Limitazioni

Le seguenti limitazioni si applicano all'utilizzo della AWS Outposts condivisione:

- Le limitazioni per le sottoreti condivise si applicano all'utilizzo della condivisione. AWS Outposts Per ulteriori informazioni sulle limitazioni di condivisione di VPC, consulta Limitazioni nella Guida per l'utente di Amazon Virtual Private Cloud.

- Le quote di servizio si applicano per singolo account.

Sicurezza in AWS Outposts

La sicurezza AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS Outposts, consulta AWS Servizi nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Per ulteriori informazioni sulla sicurezza e la conformità per AWS Outposts, consulta le domande rack.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Outposts. Illustra come soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse.

Indice

- Protezione dei dati in AWS Outposts
- Identity and access management (IAM) per AWS Outposts
- Sicurezza dell'infrastruttura in AWS Outposts
- Resilienza in AWS Outposts
- Convalida della conformità per AWS Outposts
- Accesso a Internet per AWS Outposts carichi di lavoro

Protezione dei dati in AWS Outposts

Il modello di responsabilità AWS condivisa di si applica alla protezione dei dati in AWS Outposts. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Questo contenuto include le attività di configurazione e gestione della sicurezza relative a Servizi AWS ciò che utilizzi.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e configurare singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti.

Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Crittografia a riposo

Con AWS Outposts, tutti i dati sono crittografati quando sono inattivi. Sul materiale della chiave viene eseguito il wrapping in una chiave esterna archiviata in un dispositivo rimovibile, la chiave di sicurezza Nitro (NSK).

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. Per ulteriori informazioni, consulta Amazon EBS Encryption nella Amazon EBS User Guide.

Crittografia in transito

AWS crittografa i dati in transito tra Outpost e la sua regione. AWS Per ulteriori informazioni, consulta Connettività tramite collegamento al servizio.

Puoi utilizzare un protocollo di crittografia quale Transport Layer Security (TLS) per eseguire la crittografia dei dati sensibili in transito attraverso il gateway locale verso la tua rete locale.

Eliminazione dei dati

Quando si arresta o si termina un' EC2 istanza, 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.

La distruzione della chiave di sicurezza Nitro elimina crittograficamente i dati presenti nel tuo Outpost.

Identity and access management (IAM) per AWS Outposts

AWS Identity and Access Management (IAM) è un AWS servizio 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 Puoi utilizzare IAM senza alcun costo aggiuntivo.

Indice

- Come funziona AWS Outposts con IAM
- AWS Esempi di policy di Outposts
- Ruoli collegati ai servizi per AWS Outposts
- AWS politiche gestite per AWS Outposts

Come funziona AWS Outposts con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Outposts, scopri quali funzionalità IAM sono disponibili per l'uso con AWS Outposts.

Funzionalità IAM	AWS Supporto Outposts
Policy basate su identità	Sì
Policy basate sulle risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì

Funzionalità IAM	AWS Supporto Outposts
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Politiche basate sull'identità per Outposts AWS

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Outposts AWS

Per visualizzare esempi di politiche basate sull'identità di AWS Outposts, consulta. AWS Esempi di policy di Outposts

Azioni politiche per AWS Outposts

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che

non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni AWS Outposts, vedere Azioni definite da AWS Outposts nel Service Authorization Reference.

Le azioni politiche in AWS Outposts utilizzano il seguente prefisso prima dell'azione:

```
outposts
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
    "outposts:action1",
    "outposts:action2"
]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `List`, includi la seguente azione:

```
"Action": "outposts:List*"
```

Risorse politiche per AWS Outposts

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Alcune azioni dell'API AWS Outposts supportano più risorse. Per specificare più risorse in un'unica istruzione, separale ARNs con virgole.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Per visualizzare un elenco dei tipi di risorse AWS Outposts e relativi ARNs, vedere Tipi di risorse definiti da AWS Outposts nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Outposts.

Chiavi relative alle condizioni delle policy per AWS Outposts

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`nè facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione di AWS Outposts, consulta Condition keys for AWS Outposts nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi usare una chiave di condizione, vedi Azioni definite da AWS Outposts.

Per visualizzare esempi di politiche basate sull'identità di AWS Outposts, consulta. AWS Esempi di policy di Outposts

ABAC con Outposts AWS

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Outposts AWS

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single

Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per Outposts AWS

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli collegati ai servizi per Outposts AWS

Supporta ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati in Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione dei ruoli collegati ai servizi AWS Outposts, consulta. Ruoli collegati ai servizi per AWS Outposts

AWS Esempi di policy di Outposts

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le AWS risorse Outposts. Inoltre, non possono eseguire attività utilizzando AWS

Management Console, AWS Command Line Interface (AWS CLI) o l' AWS API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per i dettagli sulle azioni e sui tipi di risorse definiti da AWS Outposts, incluso il formato di ARNs per ogni tipo di risorsa, vedere Azioni, risorse e chiavi di condizione AWS Outposts nel Service Authorization Reference.

Indice

- Best practice per le policy
- Esempio: Utilizzo delle autorizzazioni a livello di risorsa

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse AWS Outposts nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio

se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Esempio: Utilizzo delle autorizzazioni a livello di risorsa

L'esempio seguente utilizza le autorizzazioni a livello di risorsa per concedere l'autorizzazione al fine di ottenere informazioni sull'Outpost specificato.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

L'esempio seguente utilizza le autorizzazioni a livello di risorsa per concedere l'autorizzazione al fine di ottenere informazioni sul sito specificato.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
}
```

Ruoli collegati ai servizi per AWS Outposts

AWS Outposts utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato al servizio è un tipo di ruolo di servizio a cui è collegato direttamente. AWS Outposts AWS Outposts definisce i ruoli collegati ai servizi e include tutte le autorizzazioni necessarie per chiamare altri AWS servizi per conto dell'utente.

Un ruolo collegato ai servizi rende la configurazione AWS Outposts più efficiente perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Outposts definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Outposts Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo avere eliminato le risorse correlate. In questo modo proteggi AWS Outposts le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Autorizzazioni di ruolo collegate al servizio per AWS Outposts

AWS Outposts utilizza il ruolo collegato al servizio denominato _. AWSService RoleForOutposts ***OutpostID*** Questo ruolo concede a Outposts le autorizzazioni per gestire le risorse di rete per abilitare la connettività privata per tuo conto. Questo ruolo consente inoltre a Outposts di creare e configurare interfacce di rete, gestire gruppi di sicurezza e collegare interfacce alle istanze degli endpoint service link. Queste autorizzazioni sono necessarie per stabilire e mantenere la connessione privata e sicura tra Outpost locale e i AWS servizi, garantendo un funzionamento affidabile della distribuzione di Outpost.

Il ruolo AWSService RoleForOutposts _ *OutpostID* service-linked prevede che i seguenti servizi assumano il ruolo:

- `outposts.amazonaws.com`

Politiche relative ai ruoli collegati ai servizi

Il ruolo AWSService RoleForOutposts _ *OutpostID* service-linked include le seguenti politiche:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

AWSOutpostsServiceRolePolicy

La `AWSOutpostsServiceRolePolicy` policy consente l'accesso alle AWS risorse gestite da. AWS Outposts

Questa politica consente di AWS Outposts completare le seguenti azioni sulle risorse specificate:

- Azione: `ec2:DescribeNetworkInterfaces` su tutte le AWS risorse
- Azione: `ec2:DescribeSecurityGroups` su tutte le AWS risorse
- Azione: `ec2:DescribeSubnets` su tutte le AWS risorse
- Azione: `ec2:DescribeVpcEndpoints` su tutte le AWS risorse
- Azione: `ec2:CreateNetworkInterface` sulle seguenti AWS risorse:

```
"arn:*:ec2:*:*:vpc/*",
"arn:*:ec2:*:*:subnet/*",
"arn:*:ec2:*:*:security-group/*"
```

- Azione: `ec2:CreateNetworkInterface` sulla AWS risorsa `"arn:*:ec2:*:*:network-interface/*"` che soddisfa la seguente condizione:

```
"ForAnyValue:StringEquals" : { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

- Azione: `ec2:CreateSecurityGroup` sulle seguenti AWS risorse:

```
"arn:*:ec2:*:*:vpc/*"
```

- Azione: `ec2:CreateSecurityGroup` sulla AWS risorsa `"arn:*:ec2:*:*:security-group/*"` che soddisfa la seguente condizione:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

AWSOutpostsPrivateConnectivityPolicy_OutpostID

La `AWSOutpostsPrivateConnectivityPolicy_`*`OutpostID`* politica consente di AWS Outposts completare le seguenti azioni sulle risorse specificate:

- Azione: `ec2:AuthorizeSecurityGroupIngress` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Azione: `ec2:AuthorizeSecurityGroupEgress` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Azione: `ec2:CreateNetworkInterfacePermission` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Azione: `ec2:CreateTags` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}},
"StringEquals": {"ec2:CreateAction" : ["CreateSecurityGroup",
 "CreateNetworkInterface"]}
```

- Azione: `ec2:RevokeSecurityGroupIngress` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Azione: `ec2:RevokeSecurityGroupEgress` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Azione: `ec2:DeleteNetworkInterface` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- Azione: `ec2:DeleteSecurityGroup` su tutte AWS le risorse che soddisfano la seguente condizione:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Crea un ruolo collegato al servizio per AWS Outposts

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando configuri la connettività privata per Outpost in AWS Management Console, AWS Outposts crea automaticamente il ruolo collegato al servizio.

Per ulteriori informazioni, consulta Opzioni di connettività privata Service Link.

Modifica un ruolo collegato al servizio per AWS Outposts

AWS Outposts non consente di modificare il ruolo collegato al *OutpostID* servizio AWSService RoleForOutposts _. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Aggiornare un ruolo collegato al servizio nella Guida per l'utente IAM.

Elimina un ruolo collegato al servizio per AWS Outposts

Se non occorre più utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare tale ruolo. In questo modo si evita di avere un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Se il AWS Outposts servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Devi eliminare Outpost prima di poter eliminare il ruolo AWSService RoleForOutposts _ *`OutpostID`* service-linked.

Prima di iniziare, assicurati che il tuo Outpost non venga condiviso utilizzando (). AWS Resource Access Manager AWS RAM Per ulteriori informazioni, vedi Annullamento della condivisione di una risorsa Outpost condivisa.

Per eliminare AWS Outposts le risorse utilizzate da _ AWSService RoleForOutposts ***`OutpostID`***

Contatta AWS Enterprise Support per eliminare il tuo Outpost.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Per ulteriori informazioni, consulta Eliminare un ruolo collegato al servizio nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi AWS Outposts

AWS Outposts supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta i FAQs rack per Outposts.

AWS politiche gestite per AWS Outposts

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSOutposts ServiceRolePolicy

Questa politica è associata a un ruolo collegato al servizio che consente a AWS Outposts di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Ruoli collegati ai servizi.

AWS Outposts: aggiornamenti alle AWS politiche gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per AWS Outposts da quando questo servizio ha iniziato a tenere traccia di queste modifiche.

Modifica	Descrizione	Data
Aggiornamenti al ruolo collegato al servizio _ AWS Identity and Access Management AWSService RoleForOutposts *OutpostID*	Le autorizzazioni dei ruoli AWSServiceRoleForOutposts_ ***OutpostID*** service-linked vengono aggiornate per perfezionare la AWS Outposts gestione delle risorse di rete per la connettività privata, con controlli più precisi sull'interfaccia di rete e sulle operazioni dei gruppi di sicurezza necessari per le istanze degli endpoint service link.	18 aprile 2025
AWS Outposts ha iniziato a tracciare le modifiche	AWS Outposts ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	03 dicembre 2019

Sicurezza dell'infrastruttura in AWS Outposts

In quanto servizio gestito, AWS Outposts è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS

Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a AWS Outposts attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Per ulteriori informazioni sulla sicurezza dell'infrastruttura fornita per EC2 le istanze e i volumi EBS in esecuzione su Outpost, consulta Infrastructure Security in Amazon. EC2

I log di flusso VPC funzionano allo stesso modo in cui funzionano in una regione. AWS Ciò significa che possono essere pubblicati su CloudWatch Logs, Amazon S3 o GuardDuty Amazon per l'analisi. I dati devono essere rispediti alla regione per essere pubblicati su questi servizi, quindi non sono visibili da CloudWatch o da altri servizi quando Outpost si trova in uno stato disconnesso.

Monitoraggio delle manomissioni sulle apparecchiature AWS Outposts

Assicuratevi che nessuno modifichi, alteri, decodifichi o manometta l'apparecchiatura. AWS Outposts AWS Outposts le apparecchiature possono essere dotate di un sistema di monitoraggio delle manomissioni per garantire la conformità ai Termini di servizio.AWS

Resilienza in AWS Outposts

AWS Outposts è progettato per essere altamente disponibile. I rack Outposts sono progettati con apparecchiature di alimentazione e rete ridondanti. Per una maggiore resilienza, consigliamo di dotare l'Outpost di una doppia sorgente di alimentazione e di una connettività di rete ridondante.

Per un'elevata disponibilità, puoi fornire capacità aggiuntiva integrata e sempre attiva sui rack Outposts. Le configurazioni di capacità degli Outpost sono progettate per funzionare in ambienti di produzione e supportano N+1 istanze per ogni famiglia di istanze se si fornisce la capacità

necessaria. AWS consiglia di allocare una capacità aggiuntiva sufficiente per le applicazioni mission-critical per consentire il ripristino e il failover in caso di problemi con l'host sottostante. Puoi utilizzare i parametri di disponibilità della CloudWatch capacità di Amazon e impostare allarmi per monitorare lo stato delle tue applicazioni, creare CloudWatch azioni per configurare le opzioni di ripristino automatico e monitorare l'utilizzo della capacità dei tuoi Outposts nel tempo.

Quando crei un Outpost, selezioni una zona di disponibilità da una regione. AWS Questa zona di disponibilità supporta operazioni sul piano di controllo come la risposta alle chiamate API, il monitoraggio dell'Outpost e l'aggiornamento dell'Outpost. Per sfruttare la resilienza fornita dalle zone di disponibilità, puoi distribuire le applicazioni su più Outpost, ciascuno dei quali sarebbe collegato a una zona di disponibilità diversa. Ciò consente di creare una resilienza aggiuntiva delle applicazioni e di evitare la dipendenza da una singola zona di disponibilità. Per ulteriori informazioni sulle regioni e sulle zone di disponibilità, consulta Infrastruttura globale di AWS.

Puoi utilizzare un gruppo di posizionamento con una strategia di distribuzione per garantire che le istanze vengano posizionate su rack Outposts distinti. Così facendo si contribuisce a ridurre gli errori correlati. Per ulteriori informazioni, consulta Gruppi di collocazione su Outposts.

Puoi avviare istanze in Outposts utilizzando Amazon Auto EC2 Scaling e creare un Application Load Balancer per distribuire il traffico tra le istanze. Per ulteriori informazioni, consulta Configurazione di un Application Load Balancer in AWS Outposts.

Convalida della conformità per AWS Outposts

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.

- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Accesso a Internet per AWS Outposts carichi di lavoro

Questa sezione spiega in che modo AWS Outposts i carichi di lavoro possono accedere a Internet nei seguenti modi:

- Tramite la regione madre AWS
- Tramite la rete del data center locale

Accesso a Internet tramite la AWS regione madre

In questa opzione, i carichi di lavoro negli Outposts accedono a Internet tramite il collegamento al servizio e quindi tramite il gateway Internet (IGW) nella regione madre. AWS Il traffico in uscita verso Internet può avvenire 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 nella AWS regione.

Per l'impostazione della tabella di routing nella sottorete Outposts, vedere Tabelle di routing del gateway locale.

Considerazioni

- Utilizzate questa opzione quando:
  - È necessaria flessibilità per proteggere il traffico Internet con più AWS servizi nella AWS regione.
  - Non disponete di un punto di presenza Internet nel data center o nella struttura di co-ubicazione.
- In questa opzione, il traffico deve attraversare la AWS regione principale, il che introduce la latenza.
- Analogamente ai costi di trasferimento dei dati nelle AWS regioni, il trasferimento dei dati dalla zona di disponibilità principale all'Outpost comporta dei costi. Per ulteriori informazioni sul trasferimento dei dati, consulta la pagina dei prezzi di Amazon EC2 On-Demand.
- L'utilizzo della larghezza di banda del servizio di collegamento aumenterà.

L'immagine seguente mostra il traffico tra il carico di lavoro nell'istanza Outposts e Internet che attraversa la AWS regione principale.

Accesso a Internet tramite la rete del data center locale

In questa opzione, i carichi di lavoro che risiedono negli Outposts 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. Il livello di sicurezza della rete del data center locale è responsabile della protezione del traffico del carico di lavoro Outposts.

Per l'impostazione della tabella di routing nella sottorete Outposts, vedere Tabelle di routing del gateway locale.

Considerazioni

- Utilizzate questa opzione quando:
  - I tuoi carichi di lavoro richiedono un accesso a bassa latenza ai servizi Internet.
  - Preferisci evitare di incorrere in costi DTO (Data Transfer Out).
  - Desiderate preservare la larghezza di banda del collegamento di servizio per il controllo del traffico aereo.
- Il tuo livello di sicurezza è responsabile della protezione del traffico del carico di lavoro Outposts.
- Se opti per Direct VPC Routing (DVR), devi assicurarti che gli Outposts CIDRs non siano in conflitto con quelli locali. CIDRs
- Se la route predefinita (0/0) viene propagata tramite il gateway locale (LGW), le istanze potrebbero non essere in grado di raggiungere gli endpoint del servizio. In alternativa, puoi scegliere gli endpoint VPC per raggiungere il servizio desiderato.

L'immagine seguente mostra il traffico tra il carico di lavoro nell'istanza Outposts e Internet che attraversa il data center locale.

AWS Outposts si integra con i seguenti servizi che offrono funzionalità di monitoraggio e registrazione:

CloudWatch metriche

Usa Amazon CloudWatch per recuperare le statistiche sui punti dati per il tuo server Outposts sotto forma di set ordinato di dati di serie temporali, noti come metriche. È possibile utilizzare questi parametri per verificare che le prestazioni del sistema siano quelle previste. Per ulteriori informazioni, consulta CloudWatch .

CloudTrail registri

AWS CloudTrail Utilizzato per acquisire informazioni dettagliate sulle chiamate effettuate a AWS APIs. È possibile archiviare queste chiamate come file di log in Amazon S3. È possibile utilizzare questi CloudTrail registri per determinare informazioni come la chiamata effettuata, l'indirizzo IP di origine da cui proviene la chiamata, chi ha effettuato la chiamata e quando è stata effettuata la chiamata.

I CloudTrail log contengono informazioni sulle chiamate alle azioni API per. AWS Outposts Contengono anche informazioni per le chiamate alle azioni API da servizi su Outpost, come Amazon EC2 e Amazon EBS. Per ulteriori informazioni, consulta Registra le chiamate API utilizzando CloudTrail.

Log di flusso VPC

Utilizza i log di flusso VPC per acquisire informazioni dettagliate sul traffico in entrata e in uscita dal tuo Outpost e all'interno dello stesso. Per ulteriori informazioni, consulta Log di flusso VPC nella Guida per l'utente di Amazon VPC.

Mirroring del traffico

Usa Traffic Mirroring per copiare e inoltrare il traffico di rete dal server Outposts out-of-band ai dispositivi di sicurezza e monitoraggio. Puoi utilizzare il traffico in mirroring per l'ispezione dei contenuti, il monitoraggio delle minacce o la risoluzione dei problemi. Per ulteriori informazioni, consulta la Amazon VPC Traffic Mirroring Guide.

AWS Health Dashboard

AWS Health Dashboard Visualizza informazioni e notifiche avviate da cambiamenti nello stato delle risorse. AWS Le informazioni vengono presentate in due modi: su un pannello di controllo che mostra eventi recenti e prossimi organizzati per categoria e in un log completo che mostra tutti gli eventi degli ultimi 90 giorni. Ad esempio, un problema di connettività sul collegamento al

servizio avvierebbe un evento che verrebbe visualizzato nel pannello di controllo e nel log degli eventi e rimarrebbe nel log degli eventi per 90 giorni. Parte del AWS Health servizio, non AWS Health Dashboard richiede alcuna configurazione e può essere visualizzata da qualsiasi utente autenticato nel tuo account. Per ulteriori informazioni, consulta Nozioni di base di AWS Health Dashboard.

CloudWatch

AWS Outposts pubblica punti dati su Amazon CloudWatch per i tuoi Outposts. CloudWatch ti consente di recuperare le statistiche su tali punti dati sotto forma di un insieme ordinato di dati di serie temporali, noti come metriche. Pensa a un parametro come a una variabile da monitorare e ai dati di utilizzo come ai valori di questa variabile nel tempo. Ad esempio, puoi monitorare la capacità delle istanze disponibili per il tuo Outpost per un periodo di tempo specificato. A ogni dato sono associati una marcatura temporale e un'unità di misura facoltativa.

Puoi utilizzare le metriche per verificare che le prestazioni del sistema siano quelle previste. Ad esempio, puoi creare un CloudWatch allarme per monitorare la `ConnectedStatus` metrica. Se la metrica media è inferiore `a1`, CloudWatch può avviare un'azione, come l'invio di una notifica a un indirizzo email. Puoi quindi esaminare i potenziali problemi di rete on-premise o di uplink che potrebbero influire sulle operazioni dell'Outpost. Tra i problemi più comuni figurano le recenti modifiche alla configurazione della rete on-premise relativamente alle regole del firewall e del NAT o i problemi di connessione a Internet. In caso di `ConnectedStatus` problemi, consigliamo di verificare la connettività alla AWS regione dall'interno della rete locale e di contattare l' AWS assistenza se il problema persiste.

Per ulteriori informazioni sulla creazione di un CloudWatch allarme, consulta Using Amazon CloudWatch Alarms nella Amazon CloudWatch User Guide. Per ulteriori informazioni CloudWatch, consulta la Amazon CloudWatch User Guide.

Indice

- Metriche
- Dimensioni metrica
-

Metriche

Lo spazio dei nomi `AWS/Outposts` include i parametri descritti di seguito.

`ConnectedStatus`

Lo stato della connessione del collegamento al servizio di un Outpost. Se la statistica media è inferiore a `1`, la connessione è compromessa.

Unità: numero

Risoluzione massima: 1 minuto

Statistiche: la statistica più utile è `Average`.

Dimensioni: `OutpostId`

`CapacityExceptions`

Il numero di errori di capacità insufficiente per gli avvii delle istanze.

Unità: numero

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Maximum` e `Minimum`.

Dimensioni `InstanceType` e `OutpostId`

`IfTrafficIn`

Il bitrate dei dati che le Outposts Virtual Interfaces VIFs () ricevono dai dispositivi di rete locale connessi.

Unità: bit al secondo

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Max` e `Min`.

Dimensioni per il gateway locale VIFs (lgw-vif):,, e `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensioni per il collegamento al servizio VIFs (sl-vif): e `OutpostsId` `VirtualInterfaceId`

`IfTrafficOut`

Il bitrate dei dati che le Outposts Virtual Interfaces VIFs () trasferiscono ai dispositivi di rete locale collegati.

Unità: bit al secondo

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Max` e `Min`.

Dimensioni per il gateway locale VIFs (lgw-vif):,, e `OutpostsId` `VirtualInterfaceGroupId` `VirtualInterfaceId`

Dimensioni per il collegamento al servizio VIFs (sl-vif): e `OutpostsId` `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

La percentuale di capacità delle istanze disponibile. Questo parametro non include la capacità degli host dedicati configurati sull'Outpost.

Unità: percentuale

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni `InstanceFamily` e `OutpostId`

`InstanceFamilyCapacityUtilization`

La percentuale di capacità delle istanze in uso. Questo parametro non include la capacità degli host dedicati configurati sull'Outpost.

Unità: percentuale

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni: `Account`, `InstanceFamily` e `OutpostId`

`InstanceTypeCapacityAvailability`

La percentuale di capacità delle istanze disponibile. Questo parametro non include la capacità degli host dedicati configurati sull'Outpost.

Unità: percentuale

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni `InstanceType` e `OutpostId`

`InstanceTypeCapacityUtilization`

La percentuale di capacità delle istanze in uso. Questo parametro non include la capacità degli host dedicati configurati sull'Outpost.

Unità: percentuale

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni: `Account`, `InstanceType` e `OutpostId`

`UsedInstanceType_Count`

Il numero di tipi di istanze attualmente in uso, inclusi i tipi di istanza utilizzati da servizi gestiti come Amazon Relational Database Service (Amazon RDS) o Application Load Balancer. Questo parametro non include la capacità degli host dedicati configurati sull'Outpost.

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni: `Account`, `InstanceType` e `OutpostId`

`AvailableInstanceType_Count`

Il numero di tipi di istanze disponibili. Questa metrica include il conteggio. `AvailableReservedInstances`

Per determinare il numero di istanze che puoi prenotare, sottrai il `AvailableReservedInstances` conteggio dal conteggio. `AvailableInstanceType_Count`

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Questo parametro non include la capacità degli host dedicati configurati sull'Outpost.

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni `InstanceType` e `OutpostId`

`AvailableReservedInstances`

Il numero di istanze disponibili per l'avvio nella capacità di elaborazione riservata utilizzando Capacity Reservations.

Questa metrica non include le istanze EC2 riservate di Amazon.

Questa metrica non include il numero di istanze che puoi prenotare. Per determinare quante istanze puoi prenotare, sottrai il `AvailableReservedInstances` conteggio dal conteggio. `AvailableInstanceType_Count`

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni `InstanceType` e `OutpostId`

`UsedReservedInstances`

Il numero di istanze in esecuzione nella capacità di elaborazione riservata tramite Capacity Reservations. Questa metrica non include le istanze EC2 riservate di Amazon.

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni `InstanceType` e `OutpostId`

`TotalReservedInstances`

Il numero totale di istanze, in esecuzione e disponibili per il lancio, fornito dalla capacità di elaborazione riservata tramite Capacity Reservations. Questa metrica non include le istanze EC2 riservate di Amazon.

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni `InstanceType` e `OutpostId`

`EBSVolumeTypeCapacityUtilization`

La percentuale di capacità del tipo di volume EBS in uso.

Unità: percentuale

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni `VolumeType` e `OutpostId`

`EBSVolumeTypeCapacityAvailability`

La percentuale di capacità del tipo di volume EBS disponibile.

Unità: percentuale

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni `VolumeType` e `OutpostId`

`EBSVolumeTypeCapacityUtilizationGB`

Il numero di gigabyte in uso per il tipo di volume EBS.

Unità: gigabyte

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni `VolumeType` e `OutpostId`

`EBSVolumeTypeCapacityAvailabilityGB`

Il numero di gigabyte di capacità disponibile per il tipo di volume EBS.

Unità: gigabyte

Risoluzione massima: 5 minuti

Statistiche: le statistiche più utili sono `Average` e `pNN.NN` (percentuali).

Dimensioni `VolumeType` e `OutpostId`

Dimensioni metrica

Per filtrare i parametri relativi al tuo Outpost, utilizza le 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'Outpost.
`VolumeType`	Il tipo di volume EBS.
`VirtualInterfaceId`	L'ID dell'interfaccia virtuale (VIF) del gateway locale o del collegamento al servizio.
`VirtualInterfaceGroupId`	L'ID del gruppo di interfacce virtuali per l'interfaccia virtuale (VIF) del gateway locale.

Puoi visualizzare le CloudWatch metriche per il tuo server Outposts utilizzando CloudWatch la console.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare lo spazio dei nomi Outposts.

4. (Opzionale) Per visualizzare tutte le dimensioni di un parametro, inseriscine il nome nel campo di ricerca.

Per visualizzare le metriche utilizzando il AWS CLI

Utilizza il seguente comando list-metrics per elencare i parametri disponibili:

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

Per ottenere le statistiche relative a una metrica, utilizzare il AWS CLI

Utilizzate il get-metric-statisticscomando seguente per ottenere le statistiche per la metrica e la dimensione specificate. CloudWatch considera ogni combinazione unica di dimensioni come una metrica separata. Non si possono recuperare le statistiche utilizzando combinazioni di dimensioni che non siano state specificamente pubblicate. Occorre specificare le stesse dimensioni utilizzate al momento della creazione dei parametri.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/Outposts --metric-name InstanceTypeCapacityUtilization \
--statistics Average --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef
 Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

Registra le chiamate AWS Outposts API utilizzando AWS CloudTrail

AWS Outposts è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio. CloudTrail acquisisce le chiamate API AWS Outposts come eventi. Le chiamate acquisite includono chiamate dalla AWS Outposts console e chiamate di codice alle operazioni AWS Outposts API. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare a quale richiesta è stata effettuata AWS Outposts, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.

- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo AWS account al momento della creazione dell'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni degli eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrail Lake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta Creating a trail for your Account AWS e Creating a trail for an organization nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Lake Event Data Store

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per

ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta Prezzi.AWS CloudTrail

AWS Outposts eventi gestionali in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse di Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS Outposts registra tutte le operazioni del piano di controllo AWS Outposts come eventi di gestione. Per un elenco delle operazioni del piano di controllo AWS Outposts a cui Outposts accede, CloudTrail consulta AWS Outposts API Reference.AWS

AWS Outposts esempi di eventi

L'esempio seguente mostra un CloudTrail evento che dimostra l'`SetSiteAddress`operazione.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Secondo il modello di responsabilità condivisa di , AWS è responsabile dell'hardware e del software che eseguono AWS i servizi. Questo vale per AWS Outposts, proprio come per una AWS regione. Ad esempio, AWS gestisce le patch di sicurezza, aggiorna il firmware e mantiene le apparecchiature Outpost. AWS monitora anche le prestazioni, lo stato e le metriche del rack Outposts e determina se è necessaria una manutenzione.

> **Warning**
>
> Eventuali guasti dell'unità disco sottostante o l'arresto, l'ibernazione o l'interruzione dell'istanza comportano il rischio di perdita dei dati presenti sui volumi dell'archivio dell'istanza. Per prevenire la perdita di dati, ti consigliamo di eseguire il backup dei dati a lungo termine presenti sui volumi di archivio dell'istanza in un sistema di archiviazione persistente, come un bucket Amazon S3, un volume Amazon EBS o un dispositivo di archiviazione di rete nella tua rete on-premise.

Indice

- Aggiorna i dettagli di contatto
- Manutenzione dell'hardware
- Aggiornamenti del firmware
- Manutenzione delle apparecchiature di rete
- Best practice per gli eventi di alimentazione e di rete

Aggiorna i dettagli di contatto

Se il proprietario di Outpost cambia, contatta Supporto AWS Center con il nome e le informazioni di contatto del nuovo proprietario.

Manutenzione dell'hardware

Se AWS rileva un problema irreparabile con l'hardware durante il processo di provisioning del server o durante l'hosting di EC2 istanze Amazon in esecuzione sul tuo server Outposts, notificheremo al proprietario di Outpost e al proprietario delle istanze che è previsto il ritiro delle istanze interessate. Per ulteriori informazioni, consulta la sezione Ritiro delle istanze nella Amazon EC2 User Guide.

Il proprietario di Outpost e il proprietario dell'istanza possono collaborare per risolvere il problema. Il proprietario dell'istanza può arrestare e avviare un'istanza interessata per eseguirne la migrazione alla capacità disponibile. I proprietari delle istanze possono arrestare e avviare le istanze interessate in qualsiasi momento, in base alle proprie esigenze. Altrimenti, AWS interrompe e avvia le istanze interessate alla data di ritiro dell'istanza. Se l'Outpost non dispone di capacità aggiuntiva, l'istanza rimane in stato di arresto. Il proprietario dell'Outpost può provare a liberare la capacità usata o richiedere capacità aggiuntiva per l'Outpost al fine di poter completare la migrazione.

Se è necessaria la manutenzione dell'hardware, AWS contatterà il proprietario di Outpost per confermare la data e l'ora della visita del team di AWS installazione. Le visite possono essere programmate non appena due giorni lavorativi dal momento in cui il proprietario di Outpost parla con il AWS team.

Quando il team di AWS installazione arriverà sul posto, sostituirà gli host, gli switch o gli elementi del rack non funzionanti e metterà online la nuova capacità. Il team non eseguirà alcuna diagnostica o riparazione dell'hardware in loco. In caso di sostituzione di un host, il team rimuoverà ed eliminerà in modo permanente la chiave di sicurezza fisica conforme al NIST, eliminando adeguatamente tutti i dati che potrebbero rimanere sull'hardware. Questo garantisce che nessuno dei dati lasci il sito del cliente. Nel caso in cui il team sostituisca un dispositivo di rete Outpost, i dati sulla configurazione di rete potrebbero essere presenti sul dispositivo quando viene rimosso dal sito. Queste informazioni possono includere indirizzi IP e ASNs vengono utilizzate per stabilire interfacce virtuali per configurare il percorso verso la rete locale o il ritorno alla regione.

Aggiornamenti del firmware

L'aggiornamento del firmware di Outpost in genere non influisce sulle istanze dell'Outpost. Nella remota eventualità che sia necessario riavviare l'apparecchiatura Outpost per installare un aggiornamento, riceverai un avviso di ritiro dell'istanza per tutte le istanze in esecuzione su tale capacità.

Manutenzione delle apparecchiature di rete

La manutenzione dei dispositivi di rete Outpost (OND) viene eseguita senza compromettere le normali operazioni e il traffico di Outpost. Nel caso in cui sia necessario eseguire un intervento di manutenzione, il traffico viene deviato dall'OND. Potresti notare variazioni temporanee negli annunci BGP, come l'anteposizione di AS-Path, e le corrispondenti modifiche nei modelli di traffico sugli uplink di Outpost. Con gli aggiornamenti del firmware OND, potresti notare problemi di flapping BGP.

Raccomandiamo di configurare le apparecchiature di rete del cliente per ricevere annunci BGP da Outposts senza modificare gli attributi BGP e di abilitare il sistema di bilanciamento del carico/multipath BGP per ottenere flussi di traffico in entrata ottimali. La prependenza AS-Path viene utilizzata per i prefissi del gateway locale da cui allontanare il traffico in caso di necessità di manutenzione. ONDs La rete del cliente dovrebbe preferire i routing provenienti da Outposts con una lunghezza AS-Path di 1 rispetto ai routing con una lunghezza AS-Path di 4.

La rete di clienti dovrebbe pubblicizzare prefissi BGP uguali con gli stessi attributi per tutti. ONDs Per impostazione predefinita, la rete Outpost bilancia il carico del traffico in uscita tra tutti gli uplink. Le policy di routing vengono utilizzate sul lato Outpost per deviare il traffico da un OND nel caso in cui sia necessario eseguire un intervento di manutenzione. Questo spostamento del traffico richiede che tutti i clienti abbiano lo stesso prefisso BGP. ONDs Nel caso in cui sia necessario eseguire un intervento di manutenzione sulla rete del cliente, raccomandiamo di utilizzare l'anteposizione di AS-Path per deviare temporaneamente la matrice del traffico da uplink specifici.

Best practice per gli eventi di alimentazione e di rete

Come indicato nei Termini di AWS servizio per AWS Outposts i clienti, la struttura in cui si trovano le apparecchiature Outposts deve soddisfare i requisiti minimi di alimentazione e rete per supportare l'installazione, la manutenzione e l'uso delle apparecchiature Outposts. Un rack Outposts può funzionare correttamente solo quando l'alimentazione e la connettività di rete sono ininterrotte.

Eventi di alimentazione

In caso di interruzioni complete dell'alimentazione, esiste il rischio intrinseco che una AWS Outposts risorsa non possa tornare automaticamente in servizio. Oltre a implementare soluzioni di alimentazione ridondante e di alimentazione di backup, raccomandiamo di provvedere anticipatamente alle seguenti operazioni per mitigare l'impatto di alcuni degli scenari peggiori:

- Sposta i tuoi servizi e le tue applicazioni dalle apparecchiature Outposts in modo controllato, ricorrendo a variazioni del sistema di bilanciamento del carico basate su DNS o off-rack.
- Arresta container, istanze e database in modo incrementale ordinato e utilizza l'ordine inverso per il ripristino.
- Effettua i test dei piani per lo spostamento o l'arresto controllati dei servizi.
- Esegui il backup di dati e configurazioni critici e archiviali all'esterno degli Outposts.
- Riduci al minimo i tempi di inattività a causa dell'interruzione dell'alimentazione.
- Evitare la commutazione ripetuta degli alimentatori (off-on-off-on) durante la manutenzione.

- Programma un margine di tempo aggiuntivo nella finestra di manutenzione per far fronte a eventuali imprevisti.
- Gestisci le aspettative dei tuoi utenti e clienti indicando un intervallo di tempo per la finestra di manutenzione più ampio rispetto a quello normalmente necessario.
- Dopo il ripristino dell'alimentazione, create una segnalazione presso il Supporto AWS Centro per richiedere la verifica dell'operatività dei servizi AWS Outposts e dei servizi correlati.

Eventi di connettività di rete

La connessione service link tra Outpost e la AWS regione o la regione di origine di Outposts viene in genere ripristinata automaticamente dalle interruzioni di rete o dai problemi che possono verificarsi nei dispositivi di rete aziendali a monte o nella rete di qualsiasi provider di connettività di terze parti una volta completata la manutenzione della rete. Nel lasso di tempo in cui la connessione del collegamento al servizio è inattiva, le operazioni di Outposts sono limitate alle attività della rete locale.

EC2 Le istanze Amazon, il gateway locale e i volumi Amazon EBS sugli Outposts continueranno a funzionare normalmente e sarà possibile accedervi localmente tramite la rete locale. Allo stesso modo, le risorse di AWS servizio come i nodi di lavoro di Amazon ECS continuano a funzionare localmente. Tuttavia, la disponibilità delle API verrà ridotta. Ad esempio, l'esecuzione, l'avvio, l'arresto e la terminazione APIs potrebbero non funzionare. Le metriche e i log delle istanze continueranno a essere memorizzati nella cache locale per un massimo di 7 giorni e verranno trasferiti nella regione quando verrà ripristinata la AWS connettività. La disconnessione oltre i 7 giorni potrebbe comportare la perdita di metriche e registri.

Per ulteriori informazioni, consulta la domanda Cosa succede quando la connessione di rete della mia struttura si interrompe? nella FAQs pagina del AWS Outposts rack.

Se il collegamento al servizio non funziona a causa di un problema di alimentazione in loco o della perdita di connettività di rete, AWS Health Dashboard invia una notifica all'account proprietario degli Outposts. Né l'utente né l'utente AWS possono sopprimere la notifica di un'interruzione del collegamento di servizio, anche se l'interruzione è prevista. Per ulteriori informazioni, consulta Nozioni di base su AWS Health Dashboard nella Guida per l'utente di AWS Health .

Nel caso di un intervento di manutenzione pianificato del servizio che influisca sulla connettività di rete, adotta le seguenti misure proattive per limitare l'impatto di potenziali scenari problematici:

- Se il rack Outposts si connette alla AWS regione principale tramite Internet o Direct Connect pubblico, prima di una manutenzione pianificata, acquisisci un tracciato. Avere un percorso di

rete funzionante (pre-network-maintenance) e un percorso di rete problematico (post-network-maintenance) per identificare le differenze aiuterebbe nella risoluzione dei problemi. Se segnalate un problema post-manutenzione al AWS vostro ISP, potete includere queste informazioni.

Acquisisci un trace-route tra:

- Gli indirizzi IP pubblici presso la sede Outposts e l'indirizzo IP restituito da `outposts.region.amazonaws.com`. Sostituire *`region`* con il nome della regione principale. AWS
- Qualsiasi istanza nella regione principale con connettività della rete Internet pubblica e indirizzi IP pubblici presso la sede Outposts.

- Se hai il controllo della manutenzione della rete, limita la durata dei tempi di inattività del collegamento al servizio. Includi nel processo di manutenzione una fase che verifichi il ripristino della rete.
- Se non hai il controllo della manutenzione della rete, monitora i tempi di inattività del collegamento al servizio rispetto alla finestra di manutenzione annunciata e rivolgiti tempestivamente alla parte responsabile della manutenzione pianificata della rete se il collegamento al servizio non viene ripristinato al termine della finestra di manutenzione annunciata.

Risorse

Ecco alcune risorse relative al monitoraggio che possono dare conferma del normale funzionamento degli Outpost dopo un evento di alimentazione o di rete pianificato o non pianificato:

- Il AWS blog Monitoring best practices for AWS Outposts tratta le migliori pratiche di osservabilità e gestione degli eventi specifiche di Outposts.
- Il AWS blog Debugging tool per la connettività di rete di Amazon VPC spiega lo strumento. AWSSupport-SetupIPMonitoringFromVPC Questo strumento è un AWS Systems Manager documento (documento SSM) che crea un'istanza Amazon EC2 Monitor in una sottorete specificata da te e monitora gli indirizzi IP di destinazione. Il documento esegue test diagnostici ping, MTR, TCP trace-route e trace-path e archivia i risultati in Amazon CloudWatch Logs che possono essere visualizzati in una CloudWatch dashboard (ad esempio latenza, perdita di pacchetti). Per il monitoraggio di Outpost, l'istanza di monitoraggio deve trovarsi in una sottorete della AWS regione principale e configurata per monitorare una o più istanze Outpost utilizzando i relativi IP privati: ciò fornirà grafici sulla perdita di pacchetti e sulla latenza tra e la regione principale. AWS Outposts AWS

- Il AWS blog Deploying an automated Amazon CloudWatch dashboard for AWS Outposts use AWS CDK descrive i passaggi necessari per la distribuzione di un dashboard automatizzato.
- Se hai domande o hai necessità di ulteriori informazioni, consulta Creazione di un caso di supporto nella Guida per l'utente di AWS .

Opzioni del rack Outposts end-of-term

Alla fine del AWS Outposts mandato, devi scegliere tra le seguenti opzioni:

- Rinnova l'abbonamento e mantieni gli scaffali Outposts esistenti.
- Termina l'abbonamento e prepara gli scaffali Outposts per la restituzione.
- Trasformalo in un month-to-month abbonamento e mantieni gli scaffali Outposts esistenti.

Rinnovo dell'abbonamento

Devi completare i seguenti passaggi almeno 30 giorni prima della scadenza dell'abbonamento corrente per i tuoi rack Outposts.

Per rinnovare l'abbonamento e mantenere gli scaffali Outposts esistenti

1. Accedi alla console Centro Supporto AWS.
2. Scegli Crea caso.
3. Scegli Account e fatturazione.
4. Per Servizio, scegli Fatturazione.
5. Per Categoria, scegli Altre domande sulla fatturazione.
6. Per Gravità, scegli Domanda importante.
7. Scegli Fase successiva: informazioni aggiuntive.
8. Nella pagina Informazioni aggiuntive, per Oggetto, inserisci la tua richiesta di rinnovo, ad esempio**`Renew my Outpost subscription`**.
9. Per Descrizione, inserisci una delle seguenti opzioni di pagamento:

   - Nessun pagamento anticipato
   - Pagamento anticipato parziale
   - Pagamento anticipato totale

   Per i prezzi, consulta Prezzi dei rack AWS Outposts. Puoi anche richiedere un preventivo.
10. Scegli Passaggio successivo: risolvi ora o contattaci.
11. Nella pagina Contattaci, scegli la lingua preferita.

12. Scegli il tuo metodo di contatto preferito.
13. Rivedi i dettagli del caso e scegli Invia. Vengono visualizzati il numero di ID caso e il riepilogo.

AWS L'assistenza clienti avvierà il processo di rinnovo dell'abbonamento. Il nuovo abbonamento avrà inizio il giorno successivo alla scadenza dell'abbonamento attuale.

Se non indichi di voler rinnovare l'abbonamento o restituire il rack Outposts, verrai convertito automaticamente in month-to-month un abbonamento. Il tuo rack Outposts verrà rinnovato su base mensile alla tariffa dell'opzione di pagamento No Upfront corrispondente alla tua configurazione. AWS Outposts Il nuovo abbonamento mensile avrà inizio il giorno successivo alla scadenza dell'abbonamento attuale.

Chiusura dell'abbonamento e preparazione dei rack per il reso

È necessario completare i seguenti passaggi almeno 30 giorni prima della scadenza dell'abbonamento corrente per il rack Outposts. AWS non puoi avviare la procedura di reso finché non lo fai.

> **Important**
>
> AWS non è possibile interrompere la procedura di reso dopo aver aperto una richiesta di assistenza per terminare l'abbonamento.

Per terminare l'abbonamento

1. Accedi alla console Centro Supporto AWS.
2. Scegli Crea caso.
3. Scegli Account e fatturazione.
4. Per Servizio, scegli Fatturazione.
5. Per Categoria, scegli Altre domande sulla fatturazione.
6. Per Gravità, scegli Domanda importante.
7. Scegli Fase successiva: informazioni aggiuntive.
8. Nella pagina Informazioni aggiuntive, per Oggetto, inserisci una richiesta chiara, ad esempio **`End my Outpost subscription`**.
9. Per Descrizione, inserisci la data in cui preferisci che venga recuperato l'Outpost.

10. Scegli Passaggio successivo: risolvi ora o contattaci.
11. Nella pagina Contattaci, scegli la lingua preferita.
12. Scegli il tuo metodo di contatto preferito.
13. Rivedi i dettagli del caso e scegli Invia. Vengono visualizzati il numero di ID caso e il riepilogo.

AWS L'assistenza clienti ti contatterà per coordinare il recupero.

Per preparare gli AWS Outposts scaffali per la restituzione:

> **Important**
>
> Non spegnere il rack Outposts finché non AWS è sul posto per il recupero programmato.

1. Se le risorse dell'Outpost sono condivise, devi annullare la condivisione di tali risorse.

   Puoi annullare la condivisione di una risorsa Outpost condivisa in uno dei seguenti modi:

   - Usa la console. AWS RAM Per ulteriori informazioni, consulta Aggiornamento di una condivisione di risorse nella Guida per l'utente di AWS RAM .
   - Usa il AWS CLI per eseguire il disassociate-resource-sharecomando.

   Per l'elenco delle risorse di Outpost che possono essere condivise, consulta Risorse di Outpost condivisibili.
2. Interrompi le istanze attive associate alle sottoreti sul tuo Outpost. Per terminare le istanze, segui le istruzioni in Termina la tua istanza nella Amazon EC2 User Guide.

   > **Note**
   >
   > Alcuni servizi AWS gestiti in esecuzione su Outpost, come Application Load Balancers o Amazon Relational Database Service (RDS), consumano capacità. EC2 Tuttavia, le istanze associate non sono visibili nella EC2 dashboard di Amazon. È necessario interrompere le risorse legate a questi servizi per liberare capacità. Per ulteriori informazioni, vedi Perché manca la capacità di alcune EC2 istanze nel mio Outpost? .
3. Verifica le instance-capacity-availability tue EC2 istanze Amazon nel tuo AWS account.

a. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.

b. Scegli Outposts.

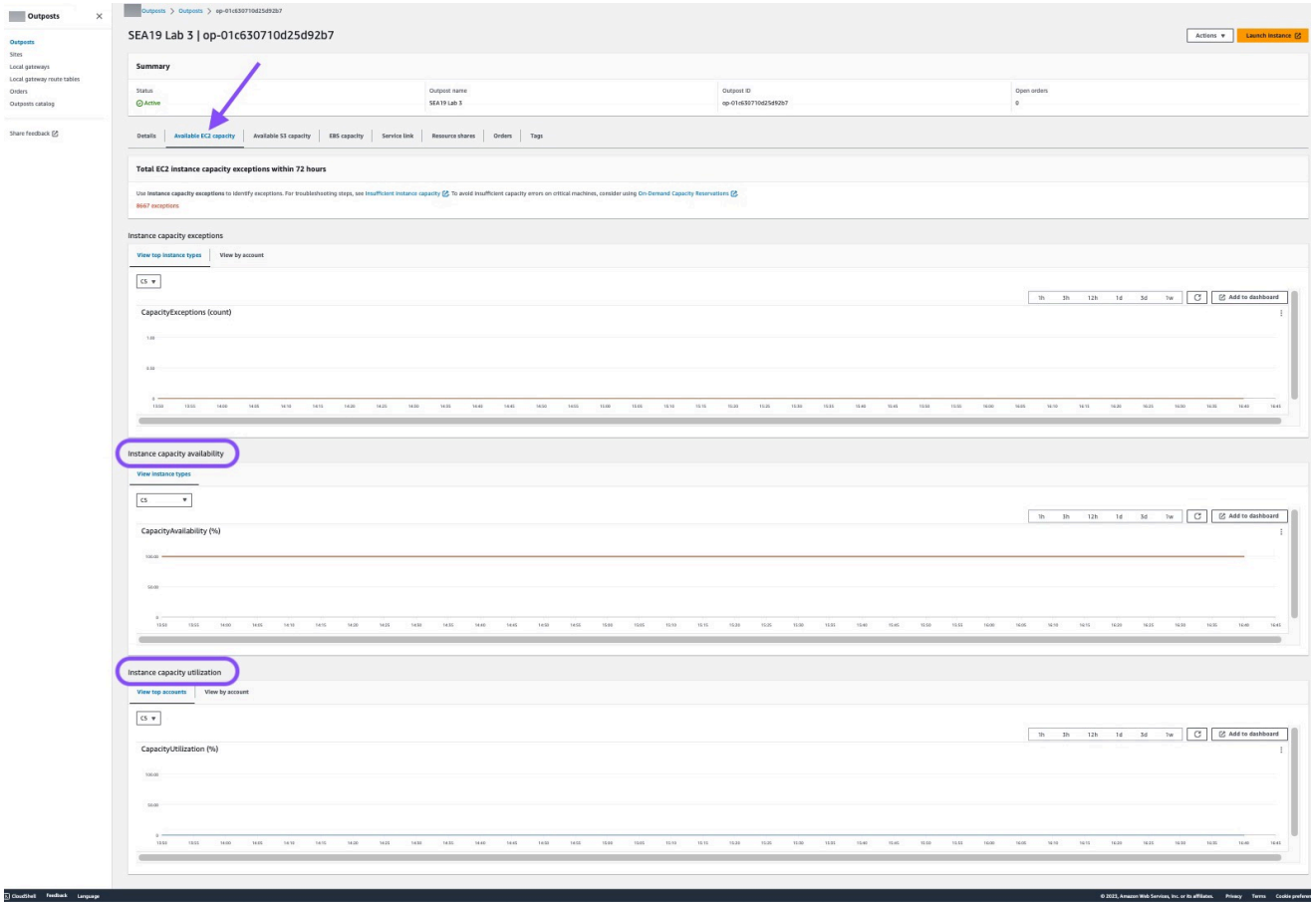
c. Scegli l'Outpost specifico che intendi restituire.

d. Nella pagina dell'Outpost, scegli la scheda EC2 Capacità disponibile.

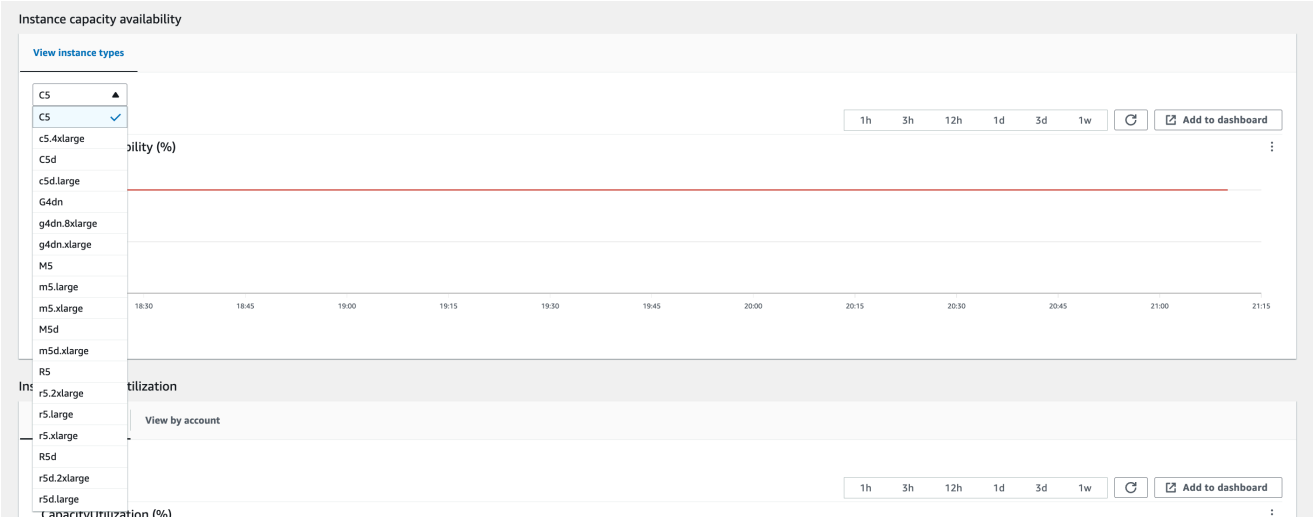
e. Assicurati che la Disponibilità della capacità delle istanze sia al 100% per ogni famiglia di istanze.

f. Assicurati che l'Utilizzo della capacità delle istanze sia allo 0% per ogni famiglia di istanze.

L'immagine seguente mostra i grafici della disponibilità della capacità dell'istanza e dell'utilizzo della capacità dell'istanza nella scheda Capacità disponibile EC2.



La seguente immagine mostra l'elenco dei tipi di istanza.



4. Crea backup delle tue EC2 istanze Amazon e dei volumi di server. Per creare i backup, segui le istruzioni in Backup e ripristino per Amazon EC2 con volumi EBS nella guida AWS Prescriptive Guidance.
5. Elimina i volumi Amazon EBS associati al tuo Outpost.
   a. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Nel riquadro di navigazione, scegli Volumi.
   c. Scegli Operazioni ed Elimina volume.
   d. Nella finestra di dialogo di conferma, seleziona Elimina.
6. Se disponi di Amazon S3 su Outposts, elimina tutti gli snapshot locali sugli Outposts.
   a. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
   b. Dal riquadro di navigazione, scegli Snapshot.
   c. Seleziona gli snapshot con un ARN dell'outpost.
   d. Scegli Operazioni, Elimina snapshot.
   e. Nella finestra di dialogo di conferma, seleziona Elimina.
7. Elimina tutti i bucket Amazon S3 associati al rack Outposts. Per eliminare i bucket, segui le istruzioni in Eliminazione del bucket Amazon S3 on Outposts nella Guida per l'utente di Amazon S3 on Outposts.
8. Elimina tutte le associazioni VPC e il pool di indirizzi IP (CoIP) CIDRs di proprietà del cliente associati al tuo Outpost.

Un team di AWS recupero spegnerà il rack. Dopo averlo spento, puoi distruggere la chiave di sicurezza AWS Nitro oppure il team di AWS recupero può farlo per tuo conto.

Converti in abbonamento month-to-month

Per passare a un month-to-month abbonamento e mantenere i rack Outposts esistenti, non è necessaria alcuna azione. In caso di domande, apri una richiesta di assistenza per la fatturazione.

I tuoi rack Outposts verranno rinnovati su base mensile alla tariffa dell'opzione di pagamento No Upfront che corrisponde alla tua configurazione Outposts. Il nuovo abbonamento mensile inizia il giorno successivo alla scadenza dell'abbonamento attuale.

Quote per AWS Outposts

Your Account AWS ha delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. È possibile richiedere un aumento per alcune quote, ma non per tutte le quote.

Per visualizzare le quote per AWS Outposts, apri la console Service Quotas. Nel riquadro di navigazione, scegli Servizi AWS, quindi seleziona AWS Outposts.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas.

Hai Account AWS le seguenti quote relative a. AWS Outposts

Risorsa	Predefinita	Adattabile	Commenti
Siti Outpost	100	Sì	Un sito Outpost è la struttura fisica gestita dal cliente in cui si alimentano e si collegano le apparecchiature Outpost alla rete. Puoi avere 100 siti Outposts in ogni regione del tuo AWS account.
Outpost per sito	10	Sì	AWS Outposts include risorse hardware e virtuali, note come Outposts. Questa quota limita le risorse virtuali dell'Outpost. È possibile avere 10 Outpost in ogni sito Outpost.

AWS Outposts e le quote per altri servizi

AWS Outposts si basa sulle risorse di altri servizi e tali servizi possono avere quote predefinite proprie. Ad esempio, la tua quota per le interfacce di rete locale proviene dalla quota Amazon VPC per le interfacce di rete.

Modifica	Descrizione	Data
Aggiornamenti alla stabilità statica	In caso di interruzione della rete, le metriche e i log delle istanze verranno memorizzati nella cache locale per un massimo di 7 giorni. In precedenza, Outposts poteva memorizzare nella cache i log solo per poche ore.	1 maggio 2025
Aggiornamenti al ruolo collegato al AWS Identity and Access Management servizio _ AWSService RoleForOutposts *OutpostID*	Le autorizzazioni dei ruoli AWSServiceRoleForOutposts_ ***OutpostID*** service-linked vengono aggiornate per perfezionare la AWS Outposts gestione delle risorse di rete per la connettività privata, con controlli più precisi sull'interfaccia di rete e sulle operazioni dei gruppi di sicurezza necessari per le istanze degli endpoint service link.	17 aprile 2025
Gestione della capacità a livello di asset	È possibile modificare la configurazione della capacità a livello di asset.	31 marzo 2025
Connettività privata tramite AWS Direct Connect Transit VIF	Ora puoi configurare il collegamento al servizio per utilizzare un VIF di AWS Direct Connect transito per abilitare la connettività privata tra gli	11 dicembre 2024

	Outposts e la AWS regione d'origine.	
Volumi a blocchi esterni supportati da storage di terze parti	Ora puoi collegare volumi di dati a blocchi supportati da sistemi di storage a blocchi compatibili di terze parti durante il processo di avvio dell'istanza su Outpost.	1 dicembre 2024
Gestione della capacità	È possibile modificare la configurazione della capacità per un'istanza.	11 novembre 2024
Gestione della capacità	Puoi modificare la configura zione di capacità predefini ta per il tuo nuovo ordine Outposts.	16 aprile 2024
AWS Outposts rack supporta le metriche di throughput dell'interfaccia service link	Ora puoi monitorare l'utilizzo del throughput tra le interfacc e virtuali Outposts rack service link VIFs () e i dispositivi della rete locale, sfruttando `IfTrafficIn` parametri e parametri. `IfTrafficOut` Amazon CloudWatch	17 novembre 2023
Comunicazione intra-VPC tramite gateway locale AWS Outposts	Puoi stabilire una comunicaz ione tra le sottoreti nello stesso VPC su diversi Outpost utilizzando i gateway locali.	30 agosto 2023
End-of-term opzioni per i rack AWS Outposts	Al AWS Outposts termine del periodo, puoi rinnovare , terminare o convertire l'abbonamento.	1° agosto 2023

Amazon Route 53 on Outposts è disponibile su AWS Outposts rack.	Amazon Route 53 on Outposts Include un Resolver che memorizza nella cache tutte le query DNS provenien ti da AWS Outposts. Puoi impostare anche una connettiv ità ibrida tra un Outpost e un resolver DNS on-premise quando metti in produzione endpoint in entrata e in uscita.	20 luglio 2023
Percorso in entrata del gateway locale	Puoi creare e modificare i percorsi in entrata del gateway locale verso le interfacce di rete elastiche sul tuo Outpost.	15 settembre 2022
Presentazione del routing VPC diretto per AWS Outposts	Utilizza l'indirizzo IP privato delle istanze nel VPC per facilitare la comunicazione con la rete on-premise.	14 settembre 2022
Guida AWS Outposts utente creata per gli scaffali Outposts	AWS Outposts La Guida per l'utente è suddivisa in guide separate per rack e server.	14 settembre 2022
Creazione e gestione delle tabelle di routing del gateway locale	Crea e modifica le tabelle di routing del gateway locale e i pool CoIP. Gestisci le associazioni di gruppi VIF.	14 settembre 2022
Gruppi di collocamento su AWS Outposts	I gruppi di collocazione che utilizzano una strategia di diffusione possono distribuire le istanze tra gli host.	30 giugno 2022
Host dedicati su AWS Outposts	Ora puoi utilizzare gli host dedicati su Outposts.	31 maggio 2022

Siti Outpost condivisi	Crea e gestisci siti Outpost e condividili con altri AWS account della tua organizza zione.	18 ottobre 2021
Nuova dimensione CloudWatc h	Una nuova CloudWatch dimensione per le metriche nel AWS Outposts namespace.	13 ottobre 2021
Condivisione dei bucket S3	Condividi e gestisci i bucket S3 sul tuo Outpost.	5 agosto 2021
Supporto per alcuni gruppi di collocazione	Puoi utilizzare strategie di collocazione in cluster, partizioni o a livello di diffusion e proprio come faresti in una regione.	28 luglio 2021
Metriche aggiuntive CloudWatch	Sono disponibili CloudWatc h metriche aggiuntive per le istanze riservate.	24 maggio 2021
Elenco di controllo per la risoluzione di problemi di rete	È disponibile un elenco di controllo per la risoluzione di problemi di rete.	22 febbraio 2021
Metriche aggiuntive CloudWatch	Sono disponibili CloudWatc h metriche aggiuntive per i volumi EBS.	2 febbraio 2021
Aggiornamenti sugli ordini da console	La procedura d'ordine della console è stata aggiornata.	14 gennaio 2021
Connettività privata	Puoi configurare l'opzione di connettività privata per il tuo Outpost quando lo crei nella console AWS Outposts .	21 dicembre 2020

Elenco di controllo di preparazione della rete	Utilizza l'elenco di controllo di preparazione della rete quando raccogli le informazioni per la configurazione del tuo Outpost.	28 ottobre 2020
Risorse condivise AWS Outposts	Con Outpost sharing, i proprietari di Outpost possono condividere le proprie risorse Outposts e Outpost, incluse le tabelle di routing dei gateway locali, con altri AWS account della stessa organizzazione. AWS	15 ottobre 2020
Metriche aggiuntive CloudWatch	Sono disponibili CloudWatch metriche aggiuntive, ad esempio il conteggio dei tipi.	21 settembre 2020
Metrica aggiuntiva CloudWatch	È disponibile una CloudWatch metrica aggiuntiva per lo stato di connessione al service link.	11 settembre 2020
Support per la condivisione di indirizzi di proprietà dei clienti IPv4	Utilizzato AWS Resource Access Manager per condividere gli indirizzi di proprietà del cliente IPv4 .	20 aprile 2020
Metriche aggiuntive CloudWatch	Sono disponibili CloudWatch metriche aggiuntive per i volumi EBS.	4 aprile 2020
Versione iniziale	Questa è la versione iniziale di. AWS Outposts	3 dicembre 2019

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.