Guida per l'utente per i server

AWS Outposts

AWS Outposts: Guida per l'utente per i server

Table of Contents

Che cos'è AWS Outposts?

AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura, i servizi, le API 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 istanze e sottoreti EC2. Le istanze nelle sottoreti Outpost comunicano con altre istanze nella regione AWS utilizzando indirizzi IP privati, tutti all'interno dello stesso VPC.

> **Note**
>
> Non è possibile connettere un Outpost a un altro Outpost 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 di Outpost dalla console AWS 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 Outpost includono server montabili su rack, switch, un patch panel di rete, un blocco alimentatore a rack e pannelli ciechi.

- È necessario installare un rack ACE se si dispone di cinque o più rack di elaborazione. Se disponi di meno di cinque rack di elaborazione ma prevedi di espanderli a cinque 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 Outpost forniscono servizi di calcolo e di rete locali a siti che dispongono di spazio limitato o con requisiti di capacità più ridotti.
- Link di servizio: percorso di rete che consente la comunicazione tra Outpost e la regione associata. AWS 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 Outpost e la rete locale.
- Interfaccia di rete locale: un'interfaccia di rete che consente la comunicazione tra un server Outpost e la rete on-premise.

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
Istanze Amazon EC2	S	Sì
Cluster Amazon ECS	S	Sì
Nodi Amazon EKS	S	No

Database e analisi

Tipo di risorsa	Rack	Server
ElastiCache Nodi 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
Amazon SageMaker Edge Manager	 S	 Sì

Prezzi

Puoi scegliere tra diverse configurazioni Outpost, ognuna delle quali offre una combinazione di tipi di istanze EC2 e opzioni di storage. Il prezzo delle configurazioni rack include l'installazione, la rimozione e la manutenzione. Per i server, è necessario installare e gestire la manutenzione dell'apparecchiatura.

È possibile acquistate una configurazione per un periodo di 3 anni e scegliere fra tre opzioni di pagamento: Pagamento anticipato totale, Pagamento anticipato parziale e Nessun pagamento anticipato. Se scegli l'opzione Parziale o l'opzione Nessun pagamento anticipato, verranno applicati canoni mensili. Eventuali canoni anticipati vengono applicati 24 ore dopo l'installazione dell'Outpost e che la capacità di calcolo e storage è disponibile per l'uso. Per ulteriori informazioni, consultare:

- AWS Outposts tieni traccia dei prezzi
- AWS Outposts prezzi dei server

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 on-premise deve fornire l'accesso di rete WAN (wide-area network) alla regione e a Internet. 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.

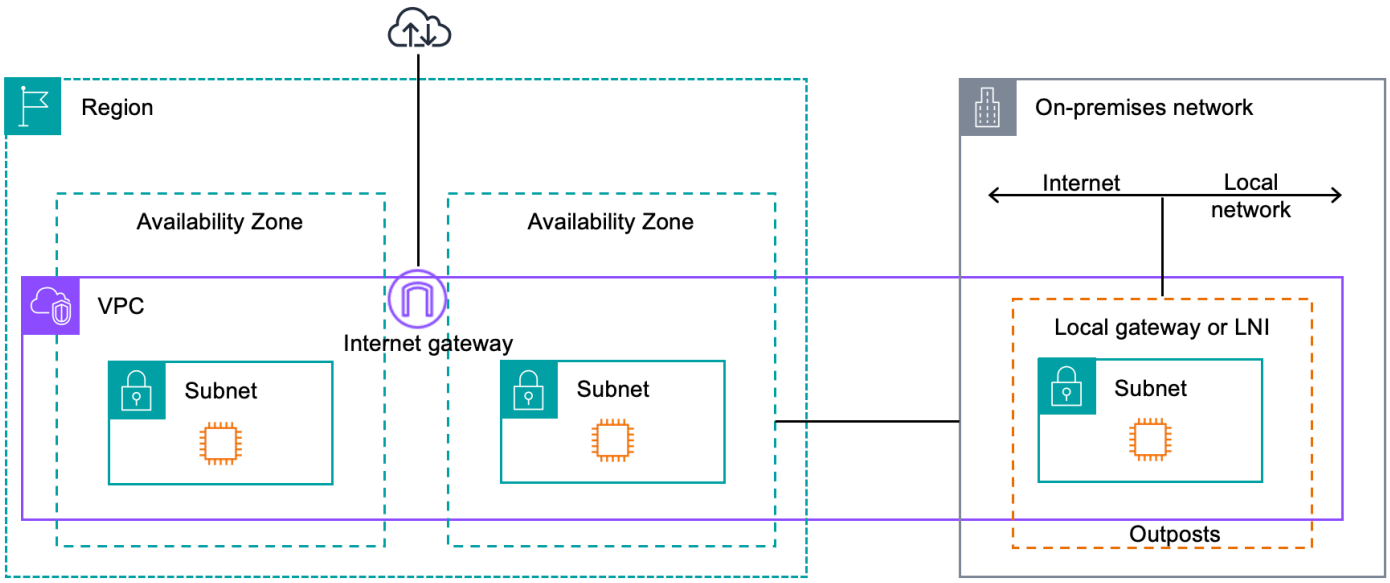
Indice

Componenti di rete

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
- Connettività tra Outpost e rete locale fornita da un gateway locale (rack) o da un'interfaccia di rete locale (server)



VPC 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'istanza EC2 quando avvii l'istanza EC2 nell'Outpost. Non è possibile specificare l'hardware sottostante su cui viene distribuita l'istanza, poiché Outpost è un pool di capacità di AWS elaborazione e archiviazione.

Ogni Outpost può supportare più VPC 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, come le istanze EC2 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 VPC sullo stesso Outpost, il traffico tra i VPC rimane nell'Outpost e non utilizza il collegamento al servizio per tornare alla regione.

DNS

Per le interfacce di rete connesse a un VPC, le istanze EC2 nelle sottoreti di Outposts possono utilizzare il servizio DNS Amazon Route 53 per risolvere i nomi dominio negli 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 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 garantire la raggiungibilità, ma questa opzione è disponibile solo per i rack Outpost 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:

- Connettività Outpost a Regioni AWS
- Routing delle applicazioni e dei carichi di lavoro nel white paper Considerations dedicato alla progettazione e all'AWS Outposts architettura ad alta disponibilità AWS

Interfacce di rete locale

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

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 Domande frequenti sui server AWS Outposts. Fai riferimento alla domanda: In quali paesi e territori sono disponibili i server Outposts?

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

Struttura

Questi sono i requisiti della struttura per i server.

> **Note**
>
> Le specifiche si riferiscono ai server in condizioni operative normali. Ad esempio, il rumore può risultare maggiore durante l'installazione iniziale e quindi tornare alla potenza acustica nominale dopo il completamento dell'installazione.

- Temperatura: la temperatura ambiente deve essere compresa tra 5-35 °C (41-95 °F).

  Il server si spegne quando la temperatura è al di fuori di questo intervallo e si riavvia quando la temperatura rientra nell'intervallo.
- Umidità: l'umidità relativa deve essere compresa tra l'8 e l'80% senza condensa.
- Qualità dell'aria: l'aria deve essere filtrata utilizzando un filtro MERV8 (o superiore).
- Circolazione dell'aria: la posizione del server deve garantire uno spazio libero minimo pari a 15 cm (6 pollici) tra il server e le pareti davanti e dietro il server per consentire una sufficiente circolazione dell'aria.
- Peso: il server 1U pesa 26 libbre e il server 2U pesa 36 libbre. Verifica che la posizione in cui intendi collocare il server sia in grado di supportare il peso del server.

  Per visualizzare i requisiti di peso per le diverse risorse Outposts, scegli Sfoglia catalogo nella AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
- Compatibilità con il kit delle guide: il kit delle guide incluso nella confezione di spedizione è compatibile con una staffa di montaggio standard a L di un rack da 19 pollici conforme allo standard EIA-310-D.

> **Important**
>
> Il kit delle guide non è compatibile con una staffa di montaggio a U, come mostrato nell'immagine seguente.

- Posizionamento su rack: consigliamo l'uso di rack EIA-310D standard da 19 pollici, con una profondità di almeno 36 pollici (914 mm).
  - I server Outposts 2U richiedono spazio con le seguenti dimensioni: altezza 3,5 pollici (88,9 mm), larghezza 17,5 pollici (447 mm), profondità 30 pollici (762 mm)
  - I server Outposts 1U richiedono spazio con le seguenti dimensioni: 1,75 pollici di altezza (44,45 mm), 17,5 pollici di larghezza (447 mm), 24 pollici di profondità (610 mm)

    > **Note**
    >
    > - Il montaggio verticale dei server non è supportato. AWS Outposts
    > - I server Outposts 1U hanno la stessa larghezza dei server Outposts 2U, ma metà dell'altezza e meno profondità

  AWS fornisce un kit ferroviario per il montaggio su rack del server. Per ulteriori informazioni, consulta Fase 3: Montaggio su rack.

  Se non si posiziona il server in un rack, è comunque necessario soddisfare gli altri requisiti elencati in questa sezione.
- Facilità di manutenzione: la manutenzione dei server Outposts può essere eseguita dal lato anteriore.
- Acustica: la potenza acustica nominale è inferiore a 78 dBA a temperature di 27 °C (80 °F) ed è conforme allo standard GR-63 CORE NEBS.
- Rinforzo antisismico: nella misura richiesta dalla normativa o dai codici, devi provvedere a installare e gestire l'ancoraggio e il rinforzo antisismici opportuni per il server mentre si trova nella tua struttura.
- Altitudine: l'altitudine del locale in cui è installato il rack deve essere inferiore a 3.050 metri (10.005 piedi).
- Pulizia: le superfici devono essere pulite con salviette umide contenenti detergenti chimici antistatici approvati.

Rete

Ogni server Outposts include non ridondanti. Le porte hanno i propri requisiti di velocità e connettori, come indicati di seguito.

Etichetta della porta	Velocità	Connettore sul dispositivo di rete upstream	Traffico
Porta 3	10 Gbe	SFP+	Sia traffico del collegamento al servizio o LNI – Il cavo di ripartizione QSFP+ (3 m/10 piedi) segmenta il traffico. Per ulteriori informazioni, consulta Configurazione della rete QSFP.

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	1024-65535	IP del collegamento al servizio	53	Server DNS fornito da DHCP
UDP	443, 1024-65535	IP del collegamento al servizio	443	Endpoint Outposts Service Link
TCP	1024-65535	IP del collegamento al servizio	443	Endpoint di registrazione Outposts

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

Unità di trasmissione massima (MTU) del collegamento al servizio

La rete deve supportare un 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.

Raccomandazioni sulla larghezza di banda dei collegamenti al servizio

Per un'esperienza e una resilienza ottimali, AWS consiglia di utilizzare una connettività ridondante di almeno 500 Mbps per la connessione del service link alla regione. AWS L'utilizzo massimo per ogni server Outpost è di 500 Mbps. Per aumentare la velocità di connessione, utilizza più server Outpost. Ad esempio, se hai tre server AWS Outposts , la velocità massima di connessione aumenta a 1,5 Gbit/s (1.500 Mbps). Per ulteriori informazioni, consulta Traffico del collegamento al servizio per i server.

I requisiti di larghezza di banda del collegamento di AWS Outposts servizio variano in base alle 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. Tieni presente che i AWS Outposts server non memorizzano nella cache le AMI. Le AMI vengono scaricate dalla regione ad ogni avvio dell'istanza.

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.

La risposta DHCP richiede il collegamento al servizio

Il collegamento al servizio richiede una risposta DHCP IPv4 per configurare le impostazioni di rete.

Latenza massima del collegamento al servizio

I collegamenti al servizio possono supportare una latenza di rete massima di 250 ms dal server e dalla relativa zona di disponibilità.

Alimentazione

Questi sono i requisiti di alimentazione per i server Outposts.

Requisiti

- Supporto di potenza
- Assorbimento di potenza
- Cavo di alimentazione
- Ridondanza dell'alimentazione

Supporto di potenza

I server hanno una potenza nominale massima di 1.600 W, 90-264 VCA, 47/63 Hz.

Assorbimento di potenza

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

Cavo di alimentazione

Il server viene fornito con un cavo di alimentazione IEC C14-C13.

Cablaggio elettrico dal server al rack

Utilizzare il cavo di alimentazione IEC C14-C13 fornito per collegare il server al rack.

Cablaggio elettrico dal server alla presa a muro

Per collegare il server a una presa a muro standard è necessario utilizzare un adattatore per l'ingresso C14 o un cavo di alimentazione specifico per il paese.

Assicurati di disporre dell'adattatore o del cavo di alimentazione corretto per la tua regione per risparmiare tempo durante l'installazione del server.

- Negli Stati Uniti è necessario un cavo di alimentazione da IEC C13 a NEMA 5-15P.
- In alcune parti dell'Europa potrebbe essere necessario un cavo di alimentazione da IEC C13 a CEE 7/7.

- In India è necessario un cavo di alimentazione da IEC C13 a IS1293.

Ridondanza dell'alimentazione

I server includono più collegamenti elettrici e vengono forniti con cavi per consentire il funzionamento ridondante dall'alimentazione. Si consiglia di impostare la ridondanza dell'alimentazione, ma la ridondanza non è richiesta.

I server non includono gruppi di continuità (UPS, Uninterruptible Power Supply).

Evasione dell'ordine

Per evadere l'ordine, AWS spediremo le apparecchiature server Outposts, compresi i supporti ferroviari e i cavi di alimentazione e di rete necessari, all'indirizzo che hai fornito. La confezione in cui viene spedito il server ha le seguenti dimensioni:

- Scatola con un server 2U:
  - Lunghezza: 44 pollici/111,8 cm
  - Altezza: 67,3 cm/26,5 pollici
  - Larghezza: 43,2 cm/17 pollici
- Scatola con un server 1U:
  - Lunghezza: 87,6 cm/34,5 pollici
  - Altezza: 61 cm/24 pollici
  - Larghezza: 22,9 cm/9 pollici

L'apparecchiatura deve essere installata dal tuo team o da un fornitore terzo. Per ulteriori informazioni, consulta Installazione del server Outpost.

L'installazione è completa quando confermi che la capacità Amazon EC2 per il tuo server Outposts è disponibile dal tuo account. AWS

Inizia con AWS Outposts

Ordina un Outpost per iniziare. Dopo l'installazione delle apparecchiature Outpost, avvia le istanze Amazon EC2 e accedi alla tua reteon-premise.

Attività

- Creazione di un Outpost e ordine della capacità dell'Outpost
- Installazione del server Outpost
- Avvia un'istanza sul tuo server Outpost

Creazione di un Outpost e ordine della capacità dell'Outpost

Per iniziare a utilizzarlo AWS Outposts, accedi con l' AWS account proprietario dell'Outpost. Crea un sito e un Outpost. Successivamente, effettua un ordine per i server Outposts di cui hai bisogno.

Prerequisiti

- Verifica le configurazioni disponibili per i tuoi server 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 .
- È necessario disporre di un piano AWS Enterprise Support o di un piano AWS Enterprise On-Ramp Support.
- Determina chi Account AWS sarà il proprietario dell'Outpost. Usa questo account per creare il sito Outposts, creare l'Outpost ed effettuare l'ordine. Controlla l'email associata a questo account alla ricerca di informazioni provenienti 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 in cui installerai e gestirai i server Outposts. Dopo aver creato il sito, AWS Outposts assegna un ID al sito. È necessario specificare questo sito quando si crea un Outpost.

Prerequisiti

- Determina l'indirizzo operativo.

Per creare un sito

1. Accedi AWS utilizzando l' Account AWS Outpost che sarà proprietario.
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 Solo server.
7. Inserisci il nome, la descrizione e l'indirizzo operativo per il tuo sito.
8. (Facoltativo) Per le note sul sito, inserite qualsiasi altra informazione che potrebbe essere utile per AWS conoscere il sito.
9. Seleziona Crea sito.

Fase 2: Creazione di un Outpost

Crea un Outpost per ogni server. Un Outpost può essere associato solamente a un singolo server. Specificherai questo Outpost al momento dell'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 Server.
4. Immetti il nome e una descrizione per l'Outpost.
5. Scegli una zona di disponibilità per il tuo Outpost.
6. Per ID sito, scegli il tuo sito.
7. Seleziona Crea outpost.

Fase 3: Effettuazione dell'ordine

Effettua un ordine per i server Outposts di cui hai bisogno. Dopo aver inviato l'ordine, sarai contattato da un rappresentante di AWS Outposts .

> **Important**
>
> Non è possibile modificare un ordine dopo l'invio, pertanto consigliamo di controllare attentamente tutti i dettagli prima dell'invio. Se hai bisogno di 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 l'opzione di pagamento anticipato parziale o nessun pagamento anticipato, pagherai i canoni mensili per un periodo di tre anni.

  I prezzi includono consegna, manutenzione del servizio dell'infrastruttura, patch e aggiornamenti software.
- Indica se l'indirizzo di spedizione 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 Server.

4. Per aggiungere capacità, scegli una configurazione.
5. Seleziona Successivo.
6. Scegli Usa Outpost esistente e seleziona il tuo Outpost.
7. Seleziona 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 l'indirizzo di spedizione di un ordine esistente, contatta il tuo AWS Account Manager.
10. Seleziona 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

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 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 AWS Outposts 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 nuova configurazione di capacità di Outpost.
2. Seleziona 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. Seleziona 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.

Upload JSON file

1. Scegli Carica una configurazione di capacità.
2. Seleziona 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:

   ```
   {
       "RequestedInstancePools": [
           {
               "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. Seleziona 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.

Passaggi successivi

Puoi visualizzare lo stato del tuo ordine utilizzando la AWS Outposts console. Lo stato iniziale del tuo ordine è Ordine ricevuto. Un AWS rappresentante ti contatterà entro tre giorni lavorativi. Riceverai un'e-mail di conferma quando lo stato del tuo ordine diventerà Ordine in elaborazione. Un AWS rappresentante può contattarti per ottenere tutte le informazioni aggiuntive AWS necessarie.

In caso di domande sull'ordine, contatta l' AWS assistenza.

Per evadere l'ordine, AWS fisseremo una data di consegna.

Sarai responsabile di tutte le attività di installazione, inclusa l'installazione fisica e la configurazione di rete. Puoi affidare a terzi l'esecuzione di queste attività per tuo conto. A prescindere dal fatto che si affidi l'installazione al proprio personale o a terzi, l'installazione richiede le credenziali IAM nell' Account AWS che contiene l'Outpost ai fini della verifica dell'identità del nuovo dispositivo. Sarai responsabile della fornitura e della gestione di tale accesso. Per ulteriori informazioni, consulta the section called “Installazione del server Outpost”.

L'installazione risulterà completata non appena la capacità Amazon EC2 per l'Outpost sarà disponibile dal tuo Account AWS. Non appena la capacità sarà disponibile potrai avviare le istanze Amazon EC2 sul tuo server Outpost. Per ulteriori informazioni, consulta the section called “Avvio di un'istanza ”.

Installazione del server Outpost

Quando ordini un server Outpost, sei responsabile della relativa installazione, indipendentemente dal fatto che ti affidi al tuo personale o a terzi. Gli addetti che effettuano l'installazione necessitano di autorizzazioni specifiche per verificare l'identità del nuovo dispositivo. Per ulteriori informazioni, consulta Concessione delle autorizzazioni.

Prerequisito

Devi disporre di un fattore di forma del server Outpost presso il tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordine della capacità dell'Outpost.

> **Note**
>
> Si consiglia di guardare il video di formazione sull'installazione AWS Outposts dei server prima e durante il processo di installazione. Per accedere al materiale di formazione, devi effettuare l'accesso all'account o crearne uno in AWS Skill Builder.

Attività

- Fase 1: Concessione delle autorizzazioni
- Fase 2: Ispezione
- Fase 3: Montaggio su rack
- Fase 4: Accensione
- Fase 5: Connessione alla rete
- Fase 6: Autorizzazione del server
- Riferimento ai comandi dello strumento di configurazione di Outpost

Fase 1: Concessione delle autorizzazioni

Per verificare l'identità del nuovo dispositivo, è necessario disporre delle credenziali IAM nell' Account AWS che contiene l'Outpost. La policy AWSOutpostsAuthorizeServerPolicy concede le autorizzazioni necessarie per installare un server Outpost. Per ulteriori informazioni, consulta the section called “Gestione dell'identità e degli accessi”.

Considerazioni

- Se utilizzi una terza parte che non ha accesso ai tuoi Account AWS, devi fornire un accesso temporaneo.
- AWS Outposts supporta l'utilizzo di credenziali temporanee. Puoi configurare credenziali temporanee che hanno una durata massima di 36 ore. Assicurati di concedere all'installatore il tempo sufficiente per eseguire tutti i passaggi per l'installazione del server. Per ulteriori informazioni, consulta the section called “Credenziali temporanee”.

Fase 2: Ispezione

Per completare un'ispezione delle apparecchiature Outposts, è necessario verificare che la scatola di spedizione non risulti danneggiata, disimballare la scatola di spedizione e individuare la chiave di sicurezza Nitro (NSK). Tenere presente quanto segue per l'ispezione del server:

- La scatola di spedizione è dotata di sensori d'urto posizionati sui due lati più grandi della scatola.
- L'aletta interna della scatola di spedizione riporta le istruzioni su come disimballare il server e individuare la NSK.
- La NSK è un modulo di crittografia. Per completare l'ispezione, è necessario individuare la NSK. La NSK viene collegata al server in una fase successiva.

Controllo della scatola di spedizione

Per ispezionare la scatola di spedizione

- Prima di aprire la scatola di spedizione, controlla entrambi i sensori d'urto e verifica se sono stati attivati. Se i sensori d'urto sono stati attivati, è possibile che l'unità sia stata danneggiata. Procedi con l'installazione prestando attenzione a rilevare eventuali ulteriori danni al server o agli accessori. Se una parte del sistema è palesemente danneggiata o l'installazione non riesce a procedere come previsto, contatta il AWS Supporto per ricevere assistenza sulla sostituzione del server Outposts.

Se la barra al centro del sensore è rossa, il sensore è stato attivato.

Disimballaggio della scatola di spedizione

Per disimballare la scatola di spedizione

- Apri la scatola e assicurati che contenga i seguenti elementi:
  - Server
  - Chiave di sicurezza Nitro (modulo di crittografia): confezione contrassegnata con "NSK" in rosso. Per ulteriori informazioni, consulta la seguente procedura per individuare la NSK nella scatola di spedizione.
  - Kit di installazione su rack (2 guide interne, 2 guide esterne e viteria)
  - Opuscolo di installazione
  - Kit accessori
    - Coppia di cavi di alimentazione C13/14 - 10 piedi (3 m)
    - Cavo di ripartizione QSFP - 10 piedi (3 m)

- Cavo USB, da micro-USB a USB-C - 10 piedi (3 m)
- Maschera di protezione

Individuazione della NSK

La NSK si trova all'interno della confezione denominata A che include gli accessori per il server.

> **Important**
>
> Non utilizzare la NSK per eliminare i dati sul server durante l'installazione.

La NSK è necessaria per attivare il server. La NSK viene utilizzata anche per eliminare i dati sul server quando ne viene eseguito il reso. In questa fase di installazione, occorre ignorare le istruzioni sul corpo della NSK poiché fanno riferimento all'eliminazione dei dati.

Fase 3: Montaggio su rack

Per completare questo passaggio, è necessario collegare le guide interne al server, le guide esterne al rack, quindi montare il server sul rack. Per completare questi passaggi, è necessario un cacciavite a croce.

Alternative al montaggio su rack

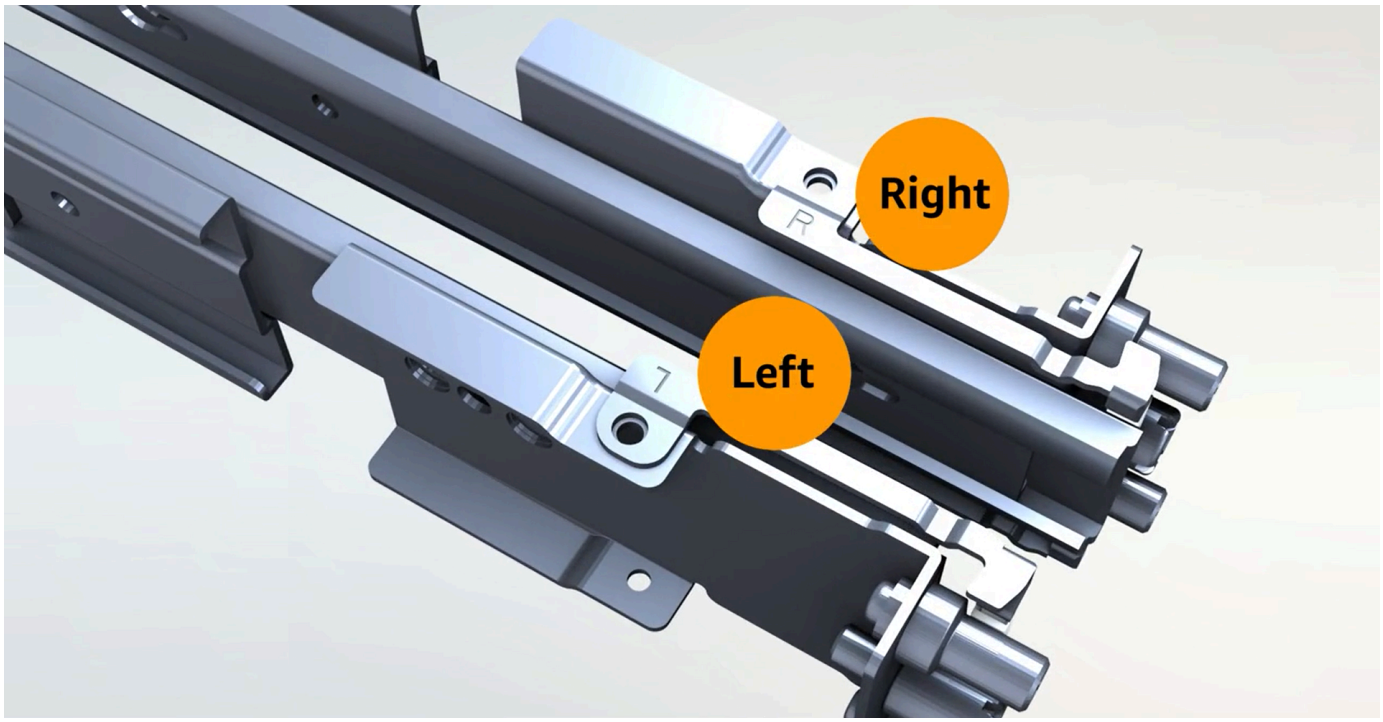
Non è necessario montare il server su un rack. Se decidi di non montare il server su un rack, prendi in considerazione quanto segue:

- Assicurati di lasciare uno spazio libero minimo pari a 15 cm (6 pollici) tra il server e le pareti davanti e dietro il server per consentire la circolazione dell'aria calda.
- Posiziona il server su una superficie stabile e non esposta a rischi meccanici quali umidità o caduta di oggetti.
- Per utilizzare i cavi di rete inclusi con il server, posiziona il server a una distanza di 3 m (10 piedi) dal dispositivo di rete upstream.
- Segui le linee guida locali per i rinforzo e il fissaggio conformi alle disposizioni antisismiche.

Identificazione dei lati e delle estremità

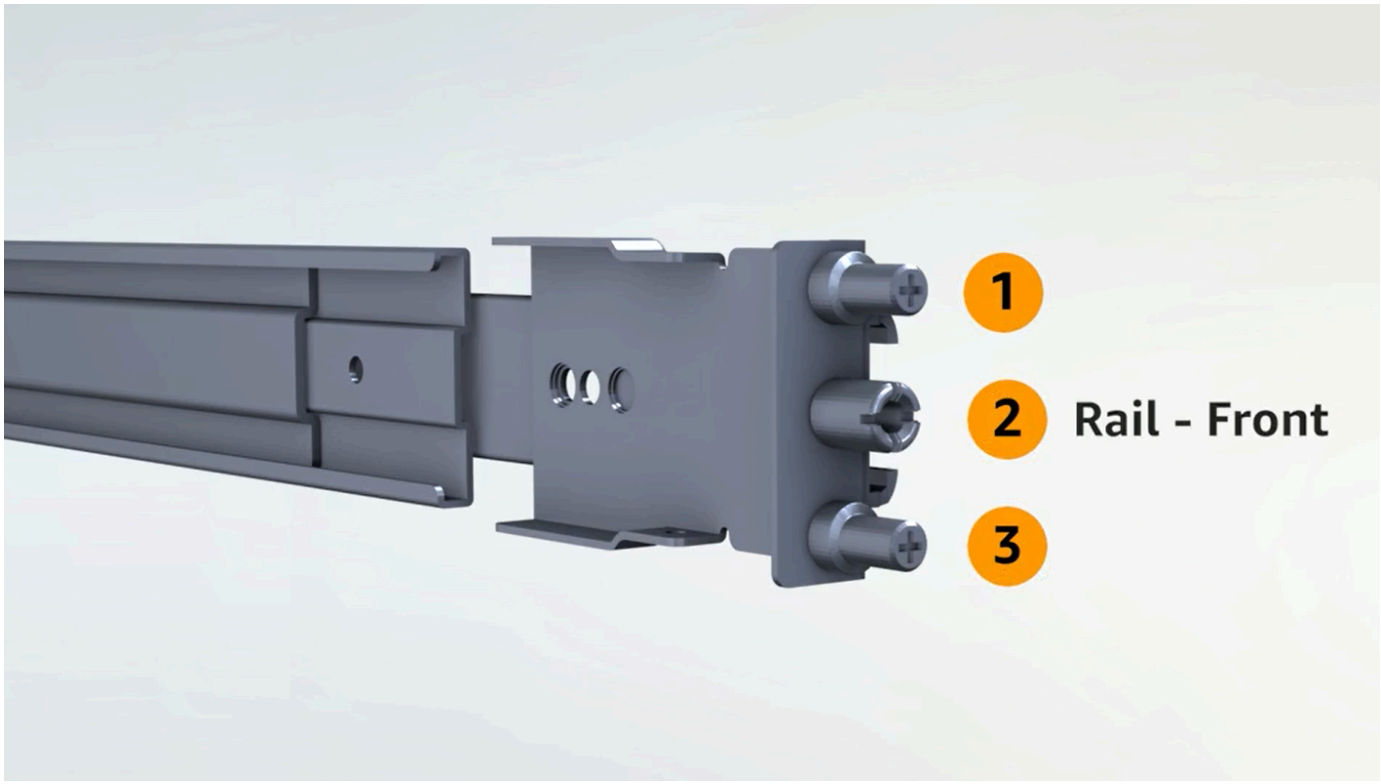
Per identificare la parte sinistra rispetto a quella destra, la parte anteriore rispetto a quella posteriore

1. Individua e apri la confezione delle guide del rack fornita con il server.
2. Osserva i contrassegni sulle guide per individuare la guida di destra e di sinistra. Questi contrassegni determinano su quale lato del server viene fissata ciascuna guida.

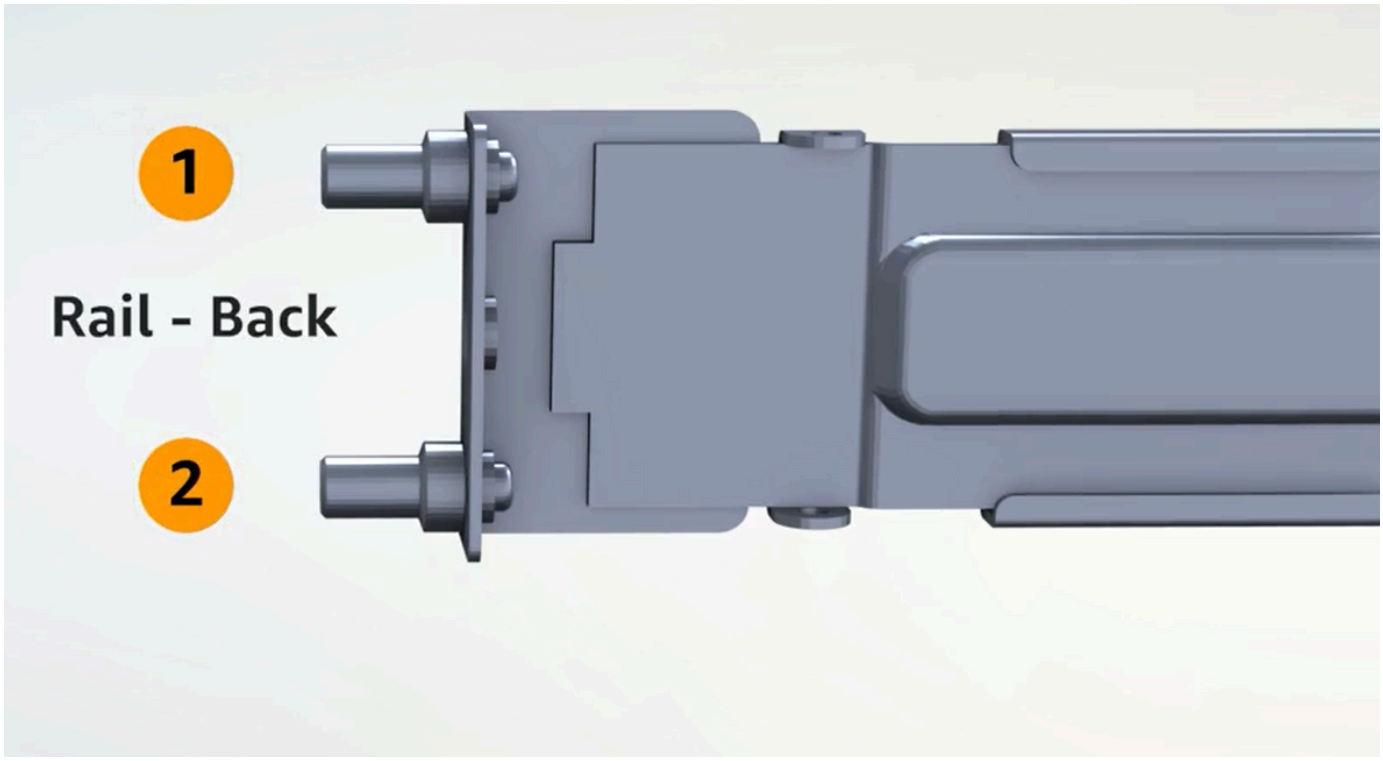


3. Osserva i montanti su ciascuna estremità delle guide per determinare il lato anteriore e posteriore.

   L'estremità anteriore ha tre montanti.



L'estremità posteriore ha due montanti.



Fissaggio delle guide interne

Per fissare le guide interne al server

1. Stacca la guida interna da quella esterna per entrambe le guide. A questo punto dovresti avere quattro guide.
2. Collega la guida interna destra al lato destro del server e fissa la guida con una vite. Assicurati di orientare correttamente la barra rispetto al server. Rivolgi la parte anteriore della guida verso la parte anteriore del server.
3. Collega la guida interna sinistra al lato sinistro del server e fissa la guida con una vite.

Fissaggio delle guide esterne

Per fissare le guide esterne al rack

1. Posizionati di fronte al rack e utilizza la guida contrassegnata con la lettera R (destra) sul lato destro del rack. Fissa prima la parte posteriore della guida al rack, quindi estendi la guida per collegarla alla parte anteriore del rack.

   > **Tip**
   >
   > Presta particolare attenzione all'orientamento delle guide. Se necessario, utilizza gli adattatori a spina inclusi.

2. Ripeti la procedura con la guida sinistra sul lato sinistro.

Montaggio del server

Per montare il server sul rack

- Inserisci il server nelle guide esterne installate sul rack nel passaggio precedente e fissa il server in corrispondenza della parte anteriore con le due viti in dotazione.

  > **Tip**
  >
  > L'operazione di inserimento del server sul rack deve essere eseguita da due persone.

Fase 4: Accensione

Per completare l'accensione, inserisci la NSK, collega il server a una fonte di alimentazione e verifica che il server sia acceso. Tieni presente quanto segue riguardo all'accensione del server:

- Il server funziona con una sola fonte di alimentazione, ma si AWS consiglia di utilizzare due fonti di alimentazione per la ridondanza.
- Collega i cavi di alimentazione prima di collegare i cavi di rete.
- Utilizza la coppia di cavi di alimentazione con connettore di uscita C13/di ingresso C14 per collegare il server a un alimentatore sul rack. Se non si utilizza il cavo di alimentazione con connettore di ingresso C14 per collegare il server a un alimentatore sul rack, è necessario fornire adattatori per i connettori di ingresso C14 che si collegano a una fonte di alimentazione.

Fissaggio della NSK

È necessario fissare la NSK al server affinché possa decrittografare i dati sul server durante il funzionamento.

Important

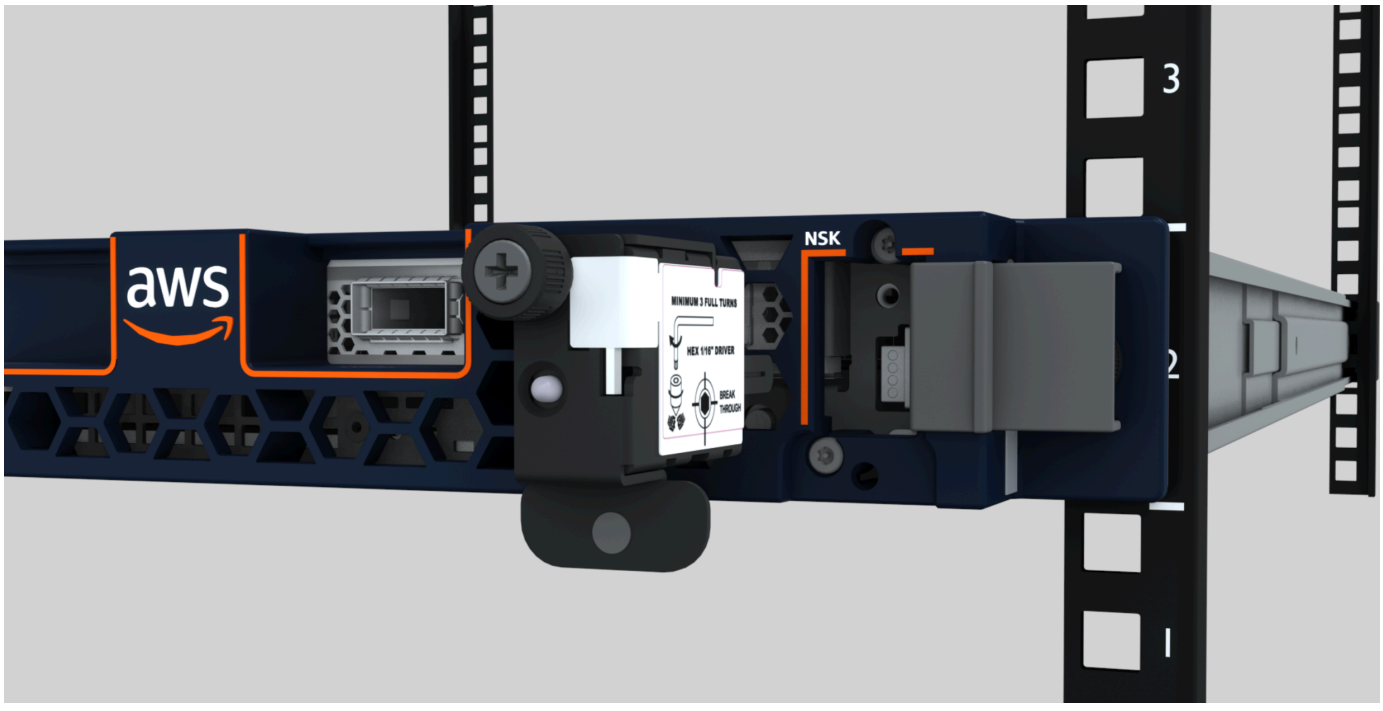
- A lato della NSK sono riportate le istruzioni necessarie per eliminare la chiave. Non seguire tali istruzioni in questa fase. Segui queste istruzioni solo quando effettui il reso del server a AWS, per eliminare crittograficamente i dati sul server.
- Se installi più server contemporaneamente, assicurati di non scambiare le NSK. È necessario fissare al server la NSK con cui è stata spedita. Se utilizzi una NSK diversa, il server non si avvia.

Per fissare la NSK

1. Sul lato anteriore destro del server, apri il vano NSK.

   L'immagine seguente mostra la NSK fissata un server 2U.

L'immagine seguente mostra la NSK fissata a un server 1U.

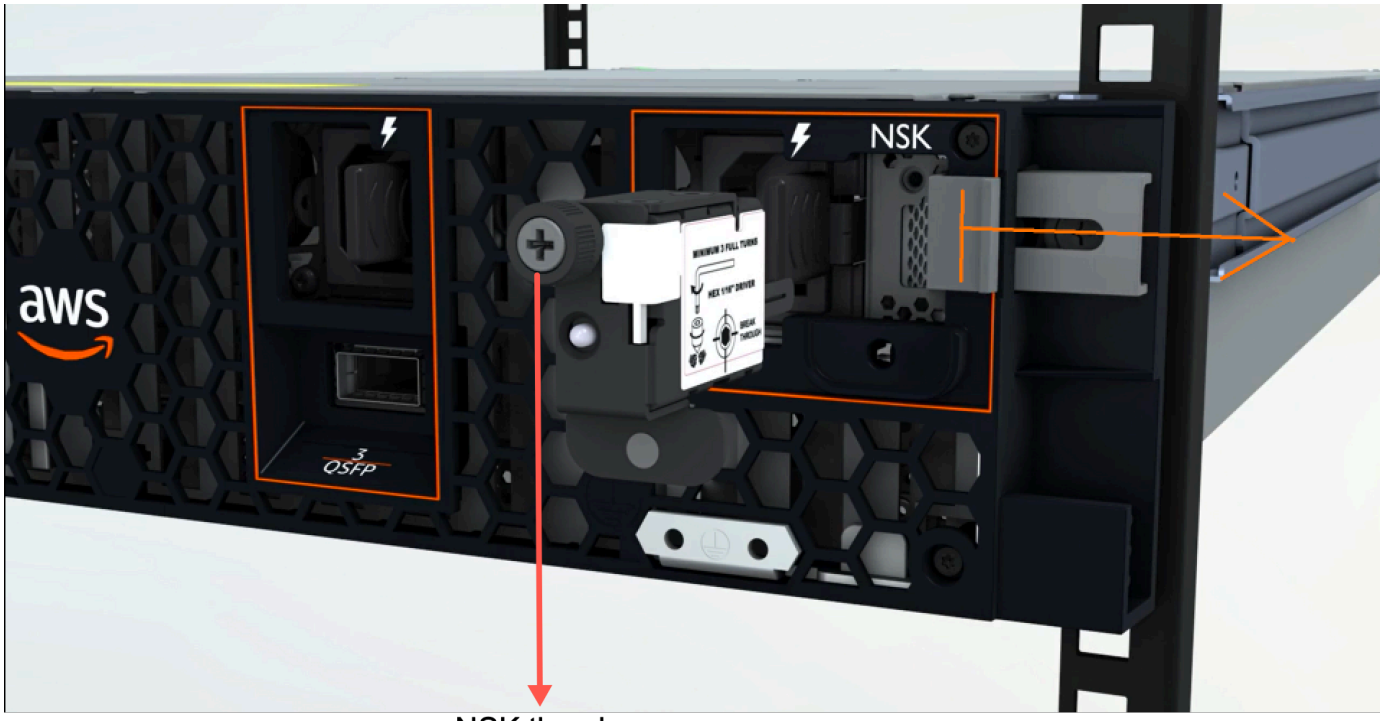


2. Assicurati che il numero di serie (SN) sulla NSK corrisponda a quello riportato sulla linguetta estraibile della mascherina del vano NSK sul server.

   L'immagine seguente mostra il codice SN sulla NSK e sulla linguetta estraibile della mascherina:

3. Inserisci la NSK nello slot.
4. Serra a mano utilizzando la vite a testa zigrinata o con un cacciavite (0,7 Nm/0,52 lb-ft) finché risulta ben stretta. Non utilizzare utensili elettrici in quanto potrebbero stringere eccessivamente e danneggiare la NSK.

   L'immagine seguente mostra la posizione della vite a testa zigrinata.



NSK thumbscrew

L'immagine seguente mostra il tipo di cacciavite che è possibile utilizzare per fissare la NSK al server.

Accensione

Per collegare il server all'alimentazione

1. Individua la coppia di cavi di alimentazione C13/C14 in dotazione con il server.
2. Collega l'estremità C14 di entrambi i cavi alla fonte di alimentazione.
3. Collega l'estremità C13 di entrambi i cavi alle porte sul lato anteriore del server.

Verificare l'alimentazione del server

Per verificare che il server sia alimentato

1. Verifica che si senta il rumore del server in funzione.

   > **Tip**
   >
   > Il livello di rumore diminuisce dopo che il server esegue automaticamente il provisioning.

2. Verifica che le spie di alimentazione a LED sopra le porte di alimentazione siano accese.

   L'immagine seguente mostra le spie di alimentazione a LED su un server 2U

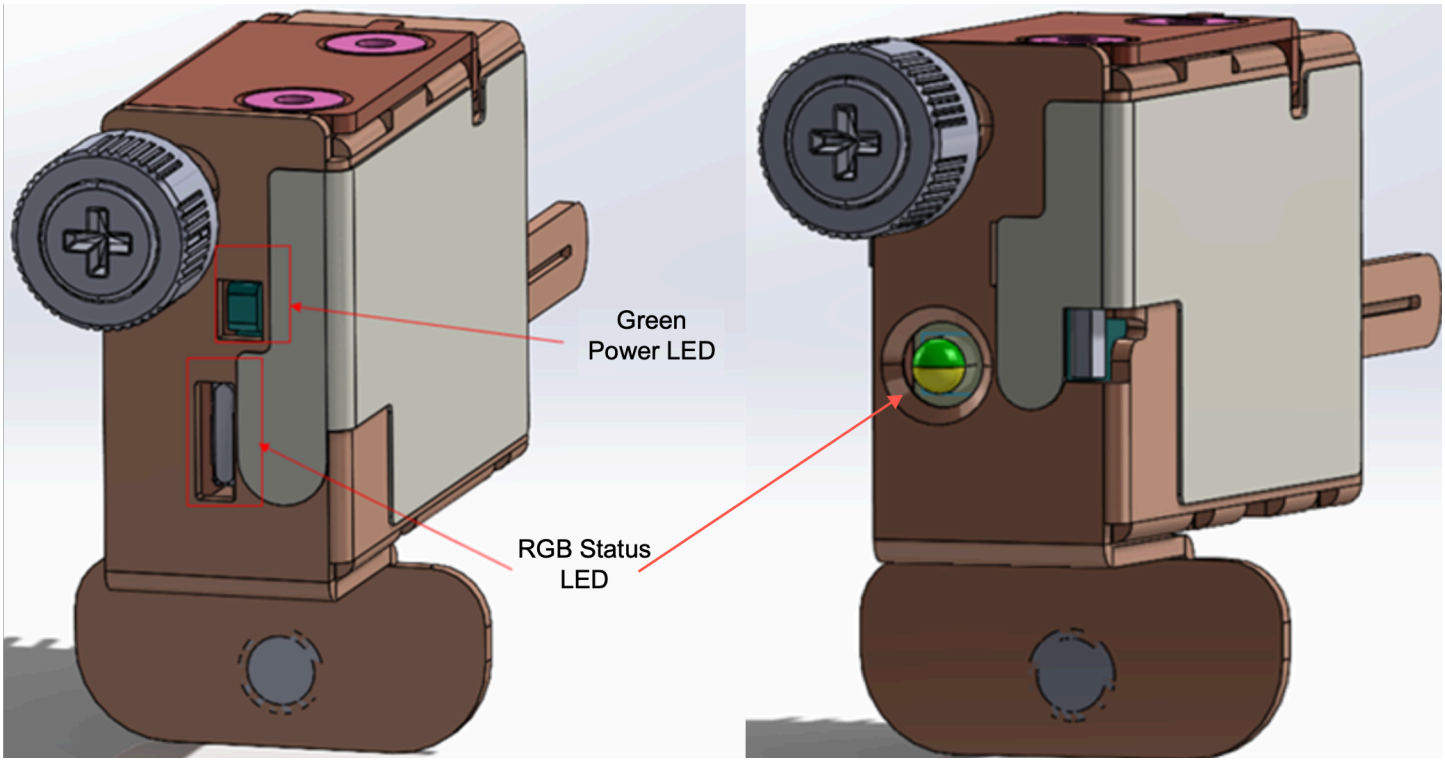
   

   L'immagine seguente mostra le spie di alimentazione a LED su un server 1U

Controllate il LED di alimentazione sull'Atlas 3.0. NSK

AWS Outposts supporta due versioni di NSK: Atlas 2.0 e Atlas 3.0. Entrambe le versioni di NSK hanno un LED di stato RGB. Inoltre, l'Atlas 3.0 è dotato di un Power LED verde. Questo passaggio è solo per Atlas 3.0 NSK.

L'immagine seguente mostra la posizione dei LED sugli NSK Atlas 2.0 e Atlas 3.0:



Atlas 3.0 Atlas 2.0

Se avete Atlas 2.0 NSK, passate al passaggio successivo, Fase 5: Connessione alla rete perché questa versione di NSK ha solo il LED di stato RGB, che dovete controllare dopo il provisioning e l'attivazione del server Outpost.

Se hai Atlas 3.0 NSK, controlla il LED di alimentazione verde:

- Se la luce verde è accesa, l'NSK è collegato correttamente all'host ed è alimentato. È possibile procedere al passaggio successivo.
- Se la luce verde è spenta, l'NSK non è collegato correttamente all'host e/o non è alimentato. Contatto. AWS Support

Fase 5: Connessione alla rete

Per completare la configurazione della rete, collega il server al dispositivo di rete upstream mediante un cavo di rete.

Tieni presente quanto segue circa la connessione alla rete:

- Il server richiede connessioni per due tipi di traffico: traffico del collegamento al servizio e traffico del collegamento con l'interfaccia di rete locale (LNI). Le istruzioni riportate nella sezione seguente

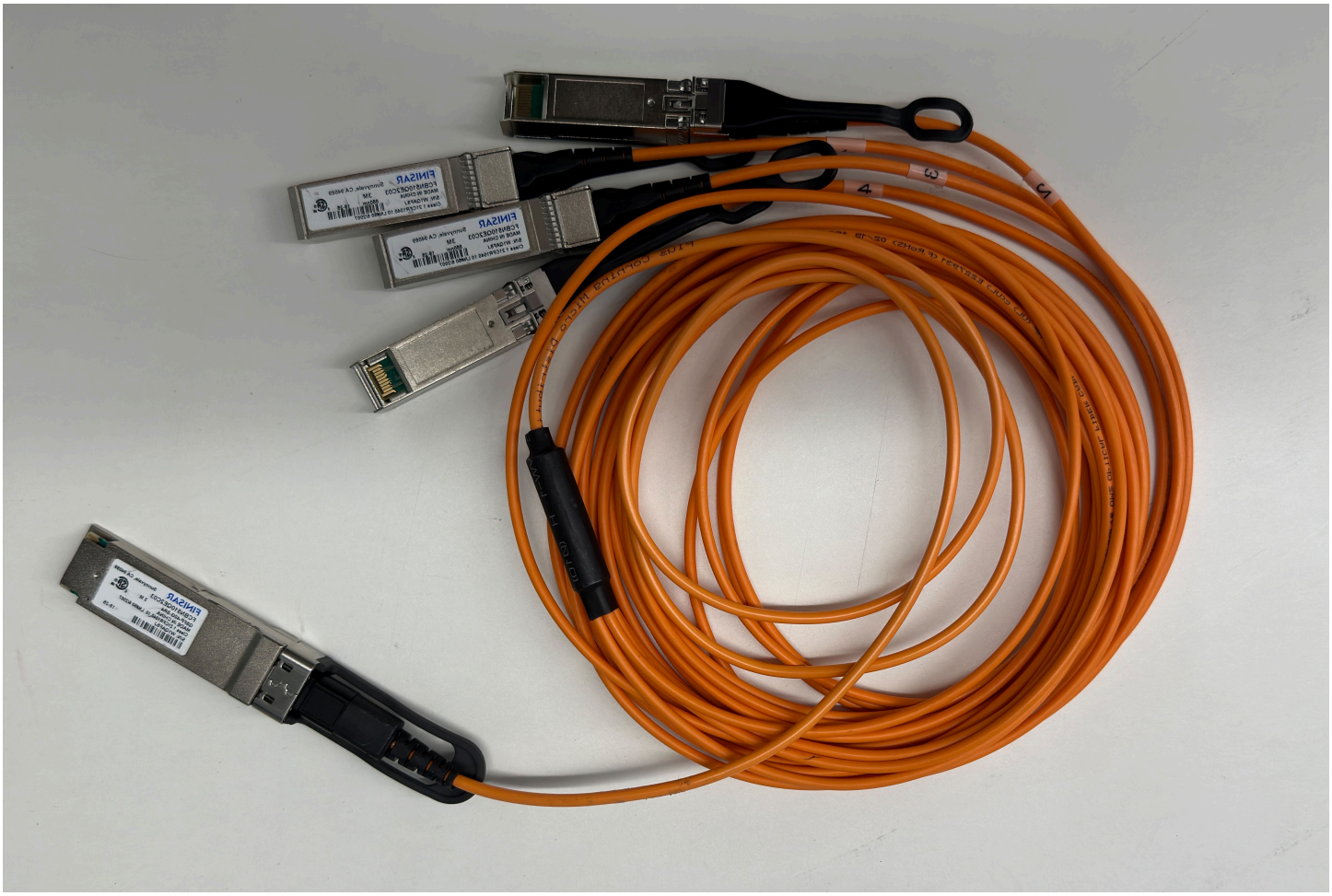
descrivono le porte da utilizzare sul server per suddividere il traffico. Rivolgiti al tuo personale IT per stabilire quale porta del dispositivo di rete upstream deve trasferire ciascun tipo di traffico.

- Assicurati che il server sia connesso al dispositivo di rete upstream e che gli sia stato assegnato un indirizzo IP. Per ulteriori informazioni, consulta Assegnazione dell'indirizzo IP del server.
- La connessione ottica su un AWS Outposts server supporta solo 10 Gbit e non supporta la negoziazione automatica della velocità delle porte. Se la porta host tenta di negoziare la velocità della porta, ad esempio tra 10 e 25 Gbit/s, potrebbero verificarsi dei problemi. In questi casi, ti consigliamo di procedere come segue:
  - Sulla porta dello switch, imposta la velocità della porta su 10 Gbit/s.
  - Rivolgiti al fornitore dello switch per richiedere il supporto per una configurazione statica.

Configurazione della rete QSFP

Servendosi del cavo di ripartizione QSFP, le ripartizioni vengono utilizzate per suddividere il traffico.

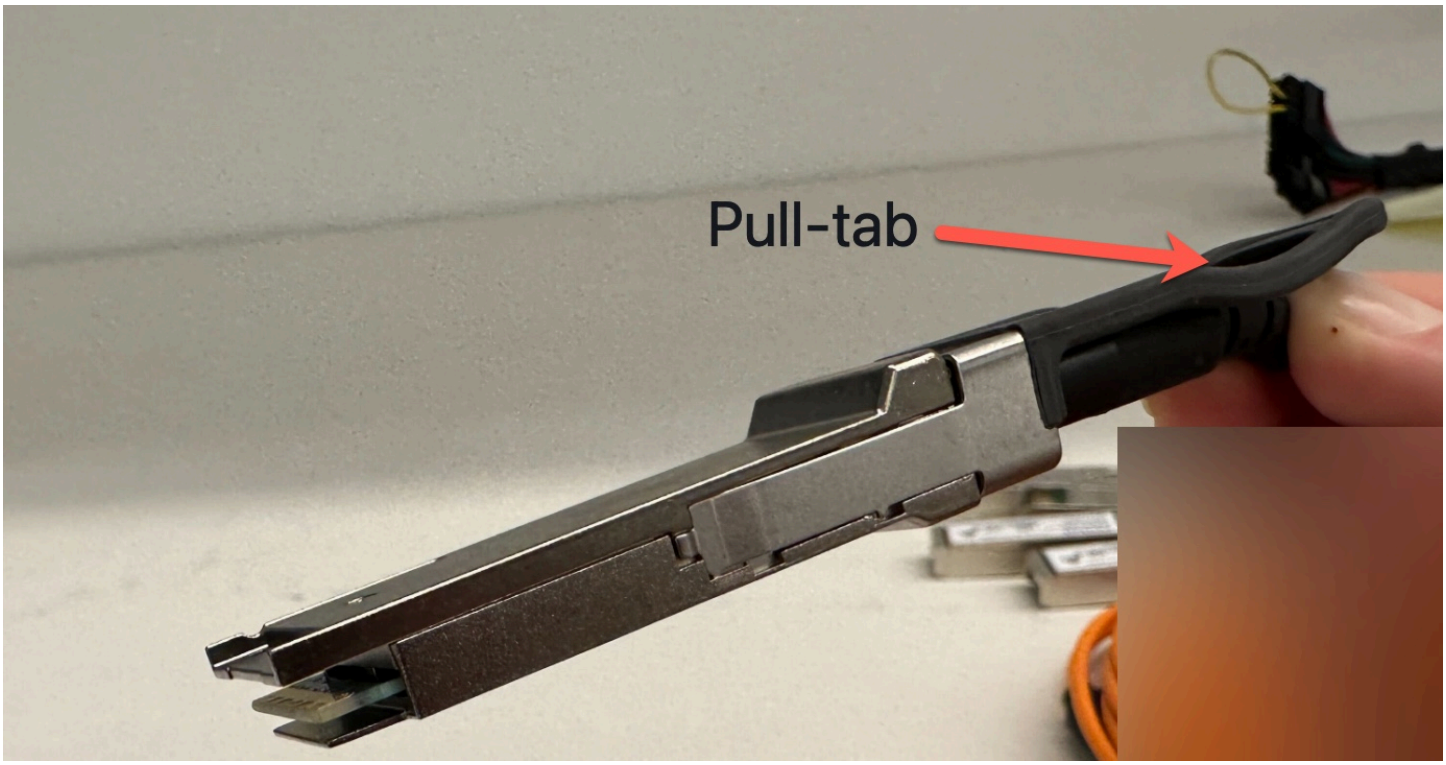
L'immagine seguente mostra il cavo di ripartizione QSFP:



> **Note**
>
> AWS Outposts i server dispongono di una porta RJ45 fisica accanto alla porta QSFP. Tuttavia, questa porta RJ45 non è abilitata per l'uso da parte dei clienti. Se è necessaria la connettività RJ45 1GbE, utilizza il cavo QSFP incluso per collegare un SFP+ 10GBASE-X a un convertitore multimediale RJ45 da 1 GbE.

Un'estremità del cavo QSFP ha un singolo connettore. Collega questa estremità al server.

L'immagine seguente mostra l'estremità del cavo con il singolo connettore:



L'altra estremità del cavo QSFP ha 4 cavi di ripartizione contrassegnati da 1 a 4. Utilizza il cavo contrassegnato con il numero 1 per il traffico del collegamento LNI e il cavo contrassegnato con il numero 2 per il traffico del collegamento al servizio.

L'immagine seguente mostra l'estremità del cavo con i 4 cavi di ripartizione:

Per collegare il server alla rete con i cavi di ripartizione QSFP

1. Individua il cavo di ripartizione QSFP fornito con il server.
2. Collega l'estremità con il singolo connettore del cavo di ripartizione QSFP alla porta QSFP sul server.

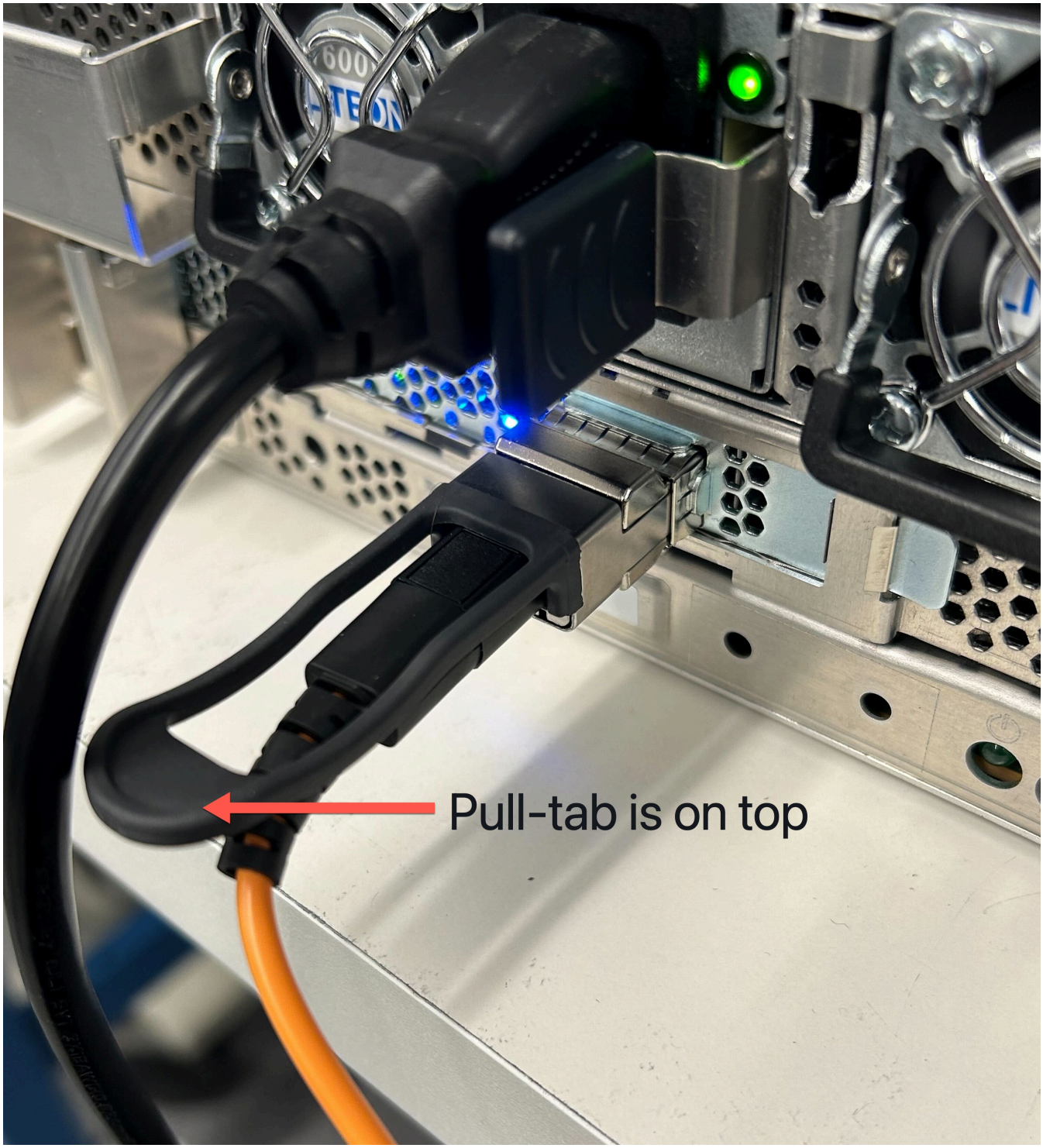
    1. Individua la porta QSFP.

L'immagine seguente mostra la posizione della porta QSFP sul server 2U.

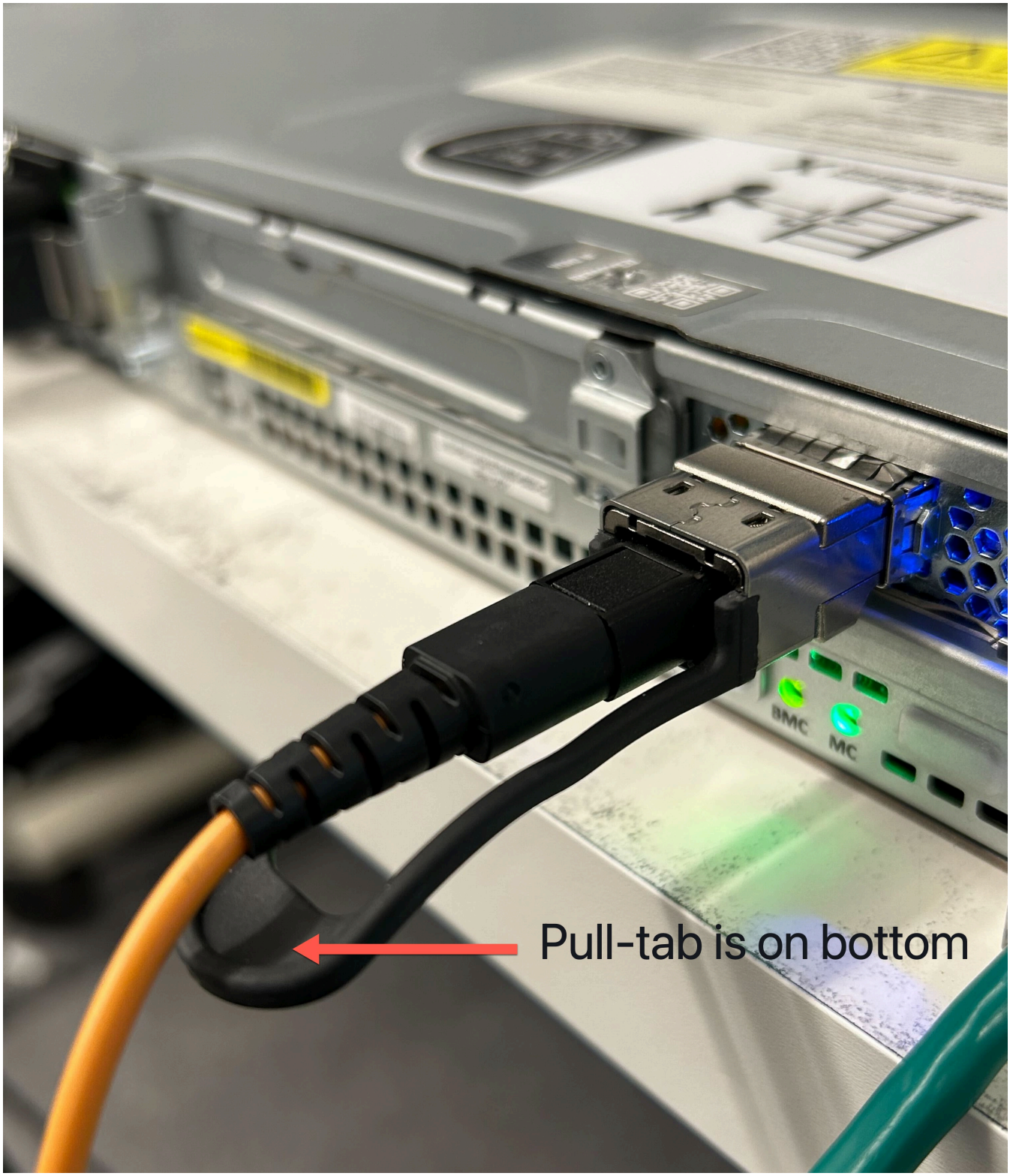
L'immagine seguente mostra la posizione della porta QSFP sul server 1U.

2. Collega il cavo QSFP con la linguetta presentata nell'orientamento corretto.

   Per il server 2U, collega il cavo QSFP con la linguetta in alto, come mostra l'immagine seguente.



Per il server 1U, collega il cavo QSFP con la linguetta in basso, come mostra l'immagine seguente.



3. Assicurati di avvertire o sentire uno scatto quando inserisci i cavi. Ciò indica che i cavi sono stati inseriti correttamente.

3. Collega i cavi di ripartizione 1 e 2 del cavo QSFP al dispositivo di rete upstream.

> **Important**
>
> Entrambi i seguenti cavi sono necessari per il funzionamento di un server Outpost.
>
> - Utilizza il cavo contrassegnato con il numero 1 per il traffico del collegamento LNI.
> - Utilizza il cavo contrassegnato con il numero 2 per il traffico del collegamento al servizio.

Fase 6: Autorizzazione del server

Per autorizzare il server, è necessario collegare il laptop al server con un cavo USB, quindi utilizzare un protocollo seriale basato su comandi per testare la connessione e autorizzare il server. Oltre alle credenziali IAM, per completare questi passaggi sono necessari un cavo USB, un laptop e un software per terminale seriale, come PuTTY o screen.

In alternativa, se disponi di un telefono o tablet Android con connettore USB-C o micro-USB con supporto USB On The Go (OTG), puoi utilizzare l'app Outposts Server Activator per assistenza durante il processo di autorizzazione del server. Puoi scaricare l'app da Google Play

Tieni presente quanto segue riguardo all'autorizzazione del server:

- Per autorizzare il server, tu o la parte che installa il server avete bisogno delle credenziali IAM presenti nel file Account AWS che contiene Outpost. Per ulteriori informazioni, consulta the section called “Fase 1: Concessione delle autorizzazioni”.
- Non è necessario eseguire l'autenticazione con le credenziali IAM per testare la connessione.
- Valuta la possibilità di testare la connessione prima di utilizzare il comando export per impostare le credenziali IAM come variabili di ambiente.
- Per proteggere il tuo account, lo strumento di configurazione di Outpost non salva mai le tue credenziali IAM.
- Per eseguire il collegamento tra il laptop e il server, collega sempre il cavo USB prima al laptop e poi al server.

Attività

- Connessione del laptop al server
- Creazione di una connessione seriale al server

- Test della connessione
- Autorizzazione del server
- Verifica i LED NSK

Connessione del laptop al server

Collega il cavo USB prima al laptop e poi al server. Il server include un chip USB che crea una porta seriale virtuale disponibile sul laptop. È possibile utilizzare questa porta seriale virtuale per collegarsi al server con un software di emulazione del terminale seriale. Puoi utilizzare questa porta seriale virtuale solo per eseguire i comandi dello strumento di configurazione di Outpost.

Per collegare il laptop al server

Collega il cavo USB prima al laptop e poi al server.

> **Note**
>
> Il chip USB richiede i driver per la creazione della porta seriale virtuale. Il sistema operativo dovrebbe installare automaticamente i driver richiesti se non sono già presenti. Per scaricare e installare i driver, consulta le Guide all'installazione di FTDI.

Creazione di una connessione seriale al server

Questa sezione riporta le istruzioni per l'uso dei programmi di terminali seriali più diffusi, ma non è necessario utilizzare questi programmi. Utilizza il programma di terminale seriale che preferisci con una velocità di connessione di `115200` baud.

Esempi

- Connessione seriale Windows
- Connessione seriale Mac

Connessione seriale Windows

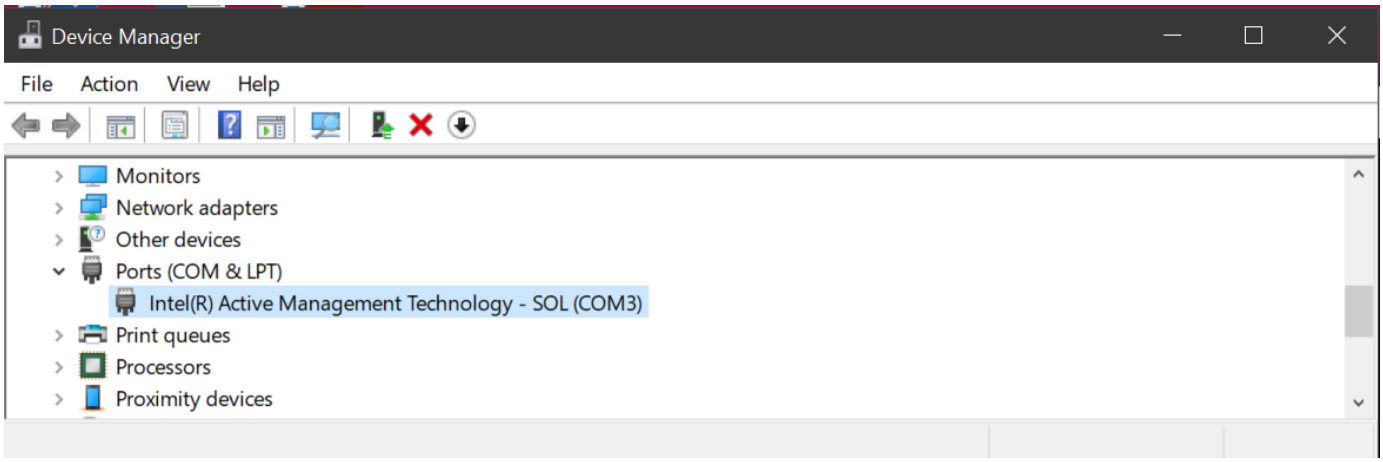
Le seguenti istruzioni si applicano a PuTTY su Windows. PuTTY è gratuito, ma potrebbe essere necessario scaricarlo.

Download di PuTTY

Scarica e installa PuTTY dalla pagina di download di PuTTY.

Per creare un terminale seriale su Windows utilizzando PuTTY

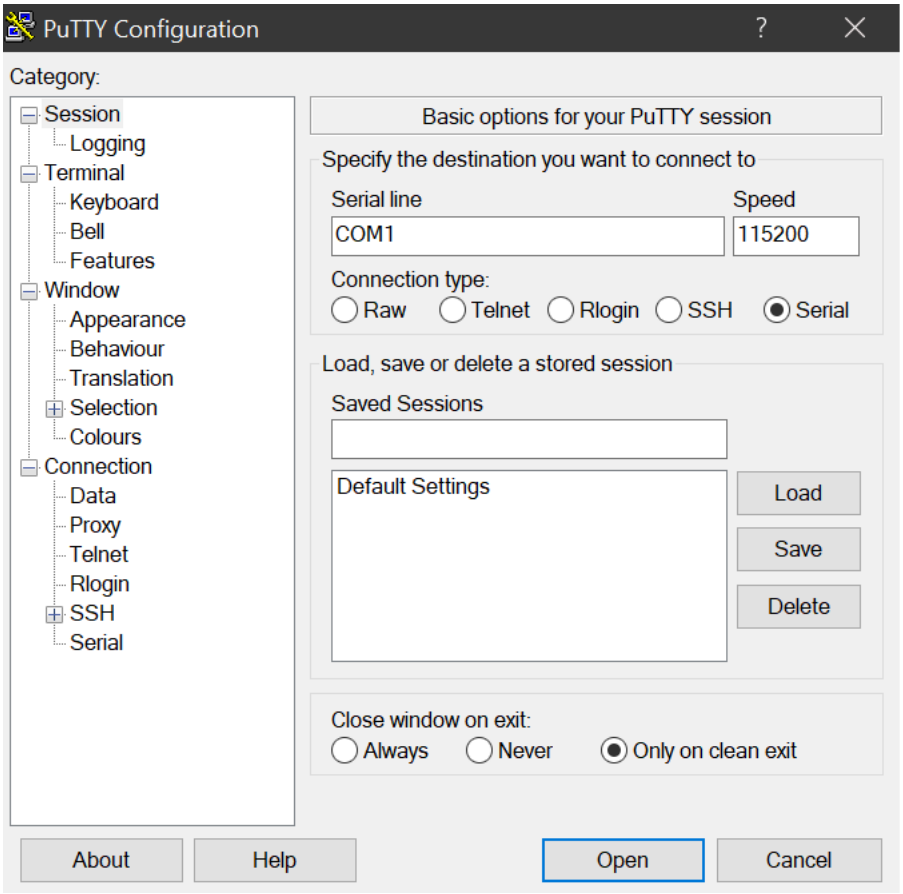
1. Collega il cavo USB prima al laptop Windows e poi al server.
2. Dal Desktop, fai clic con il pulsante destro del mouse su Start e scegli Gestione dispositivi.
3. In Gestione dispositivi, espandi Porte (COM e LPT) per individuare la porta COM per la connessione seriale USB. Verrà visualizzato un nodo denominato USB Serial Port (COM ***#).*** Il valore della porta COM dipende dall'hardware in uso.



4. In PuTTY, da Sessione, scegli Seriale per il Tipo di connessione, quindi inserisci le seguenti informazioni:

   - In Linea seriale, inserisci la porta COM # da Gestione dispositivi.
   - In Velocità, inserisci: `115200`

   L'immagine seguente mostra un esempio nella pagina di Configurazione PuTTY:



5. Seleziona Apri.

   Viene visualizzata una finestra della console vuota. Possono essere necessari da 1 a 2 minuti prima che venga visualizzata una delle seguenti opzioni:

   - `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
   - Il prompt `Outpost>`.

Connessione seriale Mac

Le seguenti istruzioni si riferiscono a screen su macOS. Puoi trovare screen incluso nel sistema operativo.

Per creare un terminale seriale su macOS utilizzando screen

1. Collega il cavo USB prima al laptop Mac e poi al server.

2. In Terminale, genera elenco `/dev` con un filtro `*usb*` di output per trovare la porta seriale virtuale.

```
ls -ltr /dev/*usb*
```

Il dispositivo seriale appare come `tty`. Esaminiamo il seguente output di esempio restituito dal precedente comando per la generazione dell'elenco:

```
ls -ltr /dev/*usb*
crw-rw-rw-  1 root  wheel   21,   3 Feb  8 15:48 /dev/cu.usbserial-EXAMPLE1
crw-rw-rw-  1 root  wheel   21,   2 Feb  9 08:56 /dev/tty.usbserial-EXAMPLE1
```

3. In Terminale, utilizza screen con il dispositivo seriale e una velocità di trasmissione della connessione seriale per configurare la connessione seriale. Nel seguente comando, sostituisci *EXAMPLE1* con il valore restituito dal laptop.

```
screen /dev/tty.usbserial-EXAMPLE1 115200
```

Viene visualizzata una finestra della console vuota. Possono essere necessari da 1 a 2 minuti prima che venga visualizzata una delle seguenti opzioni:

- `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
- Il prompt `Outpost>`.

Test della connessione

Questa sezione spiega come utilizzare lo strumento di configurazione di Outpost per testare la connessione. Non sono necessarie le credenziali IAM per testare la connessione. La tua connessione deve essere in grado di risolvere il DNS per accedere ad Regione AWS.

1. Test dei collegamenti e raccolta delle informazioni sulla connessione
2. Test per il resolver DNS
3. Test di accesso al Regione AWS

Per testare i collegamenti

1. Collega il cavo USB prima al laptop e poi al server.
2. Usa un programma terminale seriale, come PuTTY o screen per connetterti al server. Per ulteriori informazioni, consulta the section called “Creazione di una connessione seriale al server”.
3. Premi Enter per accedere al prompt dei comandi dello strumento di configurazione di Outpost.

```
Outpost>
```

> **Note**
>
> Se dopo l'accensione si attiva una luce persistente rossa all'interno dello chassis del server, sul lato sinistro, e non è possibile connettersi allo strumento di configurazione di Outpost, potrebbe essere necessario spegnere e scaricare il server per procedere. Per scaricare il server, scollega tutti i cavi di rete e di alimentazione, attendi cinque minuti, quindi accendi e riconnetti la rete.

4. Utilizza describe-links per restituire informazioni sui collegamenti di rete sul server. I server Outpost devono avere un collegamento al servizio e un collegamento all'interfaccia di rete locale (LNI).

```
Outpost>describe-links
---
service_link_connected: True
local_link_connected: False
links:
-
  name: local_link
  connected: False
  mac: 00:00:00:00:00:00
-
  name: service_link
  connected: True
  mac: 0A:DC:FE:D7:8E:1F
checksum: 0x46FDC542
```

Se viene restituito `connected: False` per uno dei due collegamenti, risolvi i problemi relativi alla connessione di rete sull'hardware.

5. Utilizza describe-ip per restituire lo stato di assegnazione IP e la configurazione del collegamento al servizio.

```
Outpost>describe-ip
---
links:
-
  name: service_link
  configured: True
  ip: 192.168.0.0
  netmask: 255.255.0.0
  gateway: 192.168.1.1
  dns: [ "192.168.1.1" ]
  ntp: [ ]
checksum: 0x8411B47C
```

Il valore NTP potrebbe mancare poiché NTP è facoltativo in un set di opzioni DHCP. Non dovrebbero mancare altri valori.

Per testare il DNS

1. Collega il cavo USB prima al laptop e poi al server.
2. Usa un programma terminale seriale, come PuTTY o screen per connetterti al server. Per ulteriori informazioni, consulta the section called “Creazione di una connessione seriale al server”.
3. Premi Enter per accedere al prompt dei comandi dello strumento di configurazione di Outpost.

```
Outpost>
```

> **Note**
>
> Se dopo l'accensione si attiva una luce persistente rossa all'interno dello chassis del server, sul lato sinistro, e non è possibile connettersi allo strumento di configurazione di Outpost, potrebbe essere necessario spegnere e scaricare il server per procedere. Per scaricare il server, scollega tutti i cavi di rete e di alimentazione, attendi cinque minuti, quindi accendi e riconnetti la rete.

4. Utilizza export per inserire la regione principale del server Outpost come valore per AWS_DEFAULT_REGION.

   AWS_DEFAULT_REGION=*Region*

   ```
   Outpost>export AWS_DEFAULT_REGION=us-west-2

   result: OK
   checksum: 0xB2A945RE
   ```

   - Non inserire spazi prima o dopo il segno di uguale (=).
   - Non viene salvato alcun valore di ambiente. È necessario esportare Regione AWS ogni volta che si esegue Outpost Configuration Tool.
   - Se per l'installazione del server ti affidi a terzi, devi fornire la regione principale.

5. Utilizza describe-resolve per determinare se il server Outpost è in grado di raggiungere un resolver DNS e di risolvere l'indirizzo IP dell'endpoint di configurazione Outpost nella regione. Richiede almeno un collegamento con una configurazione IP.

   ```
   Outpost>describe-resolve
   ---
   dns_responding: True
   dns_resolving: True
   dns: [ "198.xx.xxx.xx", "198.xx.xxx.xx" ]
   query: outposts.us-west-2.amazonaws.com
   records: [ "18.xxx.xx.xxx", "44.xxx.xxx.xxx", "44.xxx.xxx.xxx" ]
   checksum: 0xB6A961CE
   ```

Per testare l'accesso a Regioni AWS

1. Collega il cavo USB prima al laptop e poi al server.
2. Usa un programma terminale seriale, come PuTTY o screen per connetterti al server. Per ulteriori informazioni, consulta the section called “Creazione di una connessione seriale al server”.
3. Premi Enter per accedere al prompt dei comandi dello strumento di configurazione di Outpost.

   ```
   Outpost>
   ```

> **Note**
>
> Se dopo l'accensione si attiva una luce persistente rossa all'interno dello chassis del server, sul lato sinistro, e non è possibile connettersi allo strumento di configurazione di Outpost, potrebbe essere necessario spegnere e scaricare il server per procedere. Per scaricare il server, scollega tutti i cavi di rete e di alimentazione, attendi cinque minuti, quindi accendi e riconnetti la rete.

4. Utilizza export per inserire la regione principale del server Outpost come valore per `AWS_DEFAULT_REGION`.

   `AWS_DEFAULT_REGION=`*`Region`*

   ```
   Outpost>export AWS_DEFAULT_REGION=us-west-2

   result: OK
   checksum: 0xB2A945RE
   ```

   - Non inserire spazi prima o dopo il segno di uguale (=).
   - Non viene salvato alcun valore di ambiente. È necessario esportare Regione AWS ogni volta che si esegue Outpost Configuration Tool.
   - Se per l'installazione del server ti affidi a terzi, devi fornire la regione principale.

5. Utilizza describe-reachability per determinare se il server Outpost è in grado di raggiungere l'endpoint di configurazione Outpost nella regione. Richiede una configurazione DNS funzionante, che è possibile determinare utilizzando describe-resolve.

   ```
   Outpost>describe-reachability
   ---
   is_reachable: True
   src_ip: 10.0.0.0
   dst_ip: 54.xx.x.xx
   dst_port: xxx
   checksum: 0xCB506615
   ```

   - `is_reachable` indica l'esito del test
   - `src_ip` è l'indirizzo IP del server
   - `dst_ip` è l'indirizzo IP dell'endpoint di configurazione Outpost nella regione

- `dst_port` è la porta utilizzata dal server per la connessione a `dst_ip`

Autorizzazione del server

Questa sezione descrive come utilizzare lo strumento di configurazione di Outpost e le credenziali IAM dell'account AWS che contiene Outpost per autorizzare il server.

Per autorizzare il server

1. Collega il cavo USB prima al laptop e poi al server.
2. Usa un programma terminale seriale, come PuTTY o screen per connetterti al server. Per ulteriori informazioni, consulta the section called “Creazione di una connessione seriale al server”.
3. Premi Enter per accedere al prompt dei comandi dello strumento di configurazione di Outpost.

   ```
   Outpost>
   ```

   > **Note**
   >
   > Se dopo l'accensione si attiva una luce persistente rossa all'interno dello chassis del server, sul lato sinistro, e non è possibile connettersi allo strumento di configurazione di Outpost, potrebbe essere necessario spegnere e scaricare il server per procedere. Per scaricare il server, scollega tutti i cavi di rete e di alimentazione, attendi cinque minuti, quindi accendi e riconnetti la rete.

4. Utilizza export per inserire le tue credenziali IAM nello strumento di configurazione di Outpost. Se per l'installazione del server ti affidi a terzi, devi fornire le credenziali IAM.

   Per eseguire l'autenticazione devi esportare le seguenti quattro variabili. Esporta una variabile alla volta. Non inserire spazi prima o dopo il segno di uguale (=).

   - `AWS_ACCESS_KEY_ID=`*`access-key-id`*
   - `AWS_SECRET_ACCESS_KEY=`*`secret-access-key`*
   - `AWS_SESSION_TOKEN=`*`session-token`*
     - Usa il AWS CLI `GetSessionToken` comando per ottenere il`AWS_SESSION_TOKEN`. Per ulteriori informazioni, consulta get-session-token nella Guida di riferimento dei comandi di AWS CLI .

> **Note**
>
> Devi avere il ruolo AWSOutpostsAuthorizeServerPolicyassociato al tuo ruolo IAM per ottenere ilAWS_SESSION_TOKEN.

- Per installare AWS CLI, consulta Installazione o aggiornamento della versione più recente della CLI AWS nella Guida per l'AWS CLI utente per la versione 2.

- `AWS_DEFAULT_REGION=`*`Region`*

  Utilizza la regione principale del server Outpost come valore per `AWS_DEFAULT_REGION`. Se per l'installazione del server ti affidi a terzi, devi fornire la regione principale.

L'output dei seguenti esempi mostra le esportazioni riuscite.

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
```

```
result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

5. Utilizza start-connection per creare una connessione sicura alla regione.

   L'output dell'esempio seguente mostra una connessione avviata con successo.

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connection-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

6. Attendi circa 5 minuti.
7. Utilizza get-connection per verificare se la connessione alla regione è stata stabilita.

   L'output dell'esempio seguente mostra una connessione riuscita.

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
```

```
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Dopo che `keys_exchanged` e `connection_established` cambiano in `True`, sul server Outpost viene automaticamente eseguito il provisioning e l'aggiornamento al software e alla configurazione più recenti.

> **Note**
>
> Ricordiamo quanto segue in relazione al processo di provisioning:
>
> - Una volta completata l'attivazione, possono essere necessarie fino a 10 ore prima che il server Outpost sia utilizzabile.
> - È necessario mantenere l'alimentazione e la rete del server Outpost connesse e stabili durante questo processo.
> - È normale che il collegamento al servizio mostri delle fluttuazioni durante questo processo.
> - Se `exchange_active` è `True`, la connessione è ancora in corso di attivazione. Riprova tra 5 minuti.
> - Se `keys_exchanged` o `connection_established` è `False` e se `exchange_active` è `True`, la connessione è ancora in corso di attivazione. Riprova tra 5 minuti.
> - Se `keys_exchanged` o `connection_established` è `False` anche dopo 1 ora, contatta il Centro AWS Support.
> - Se `primary_status: No such asset id found.` viene visualizzato il messaggio, conferma quanto segue:
>   - Hai specificato la regione corretta.
>   - Stai utilizzando lo stesso account usato per ordinare il server Outpost.
>
>   Se la regione è corretta e stai utilizzando lo stesso account utilizzato per ordinare il server Outpost, contatta AWS Support il Centro.

- L'attributo `LifeCycleStatus` dell'Outpost passerà da `Provisioning` a `Active`. Riceverai quindi un'e-mail con la quale si informa della riuscita del provisioning e dell'attivazione del tuo server Outpost.
- Non è necessario autorizzare nuovamente il server Outposts dopo l'attivazione dello stesso.

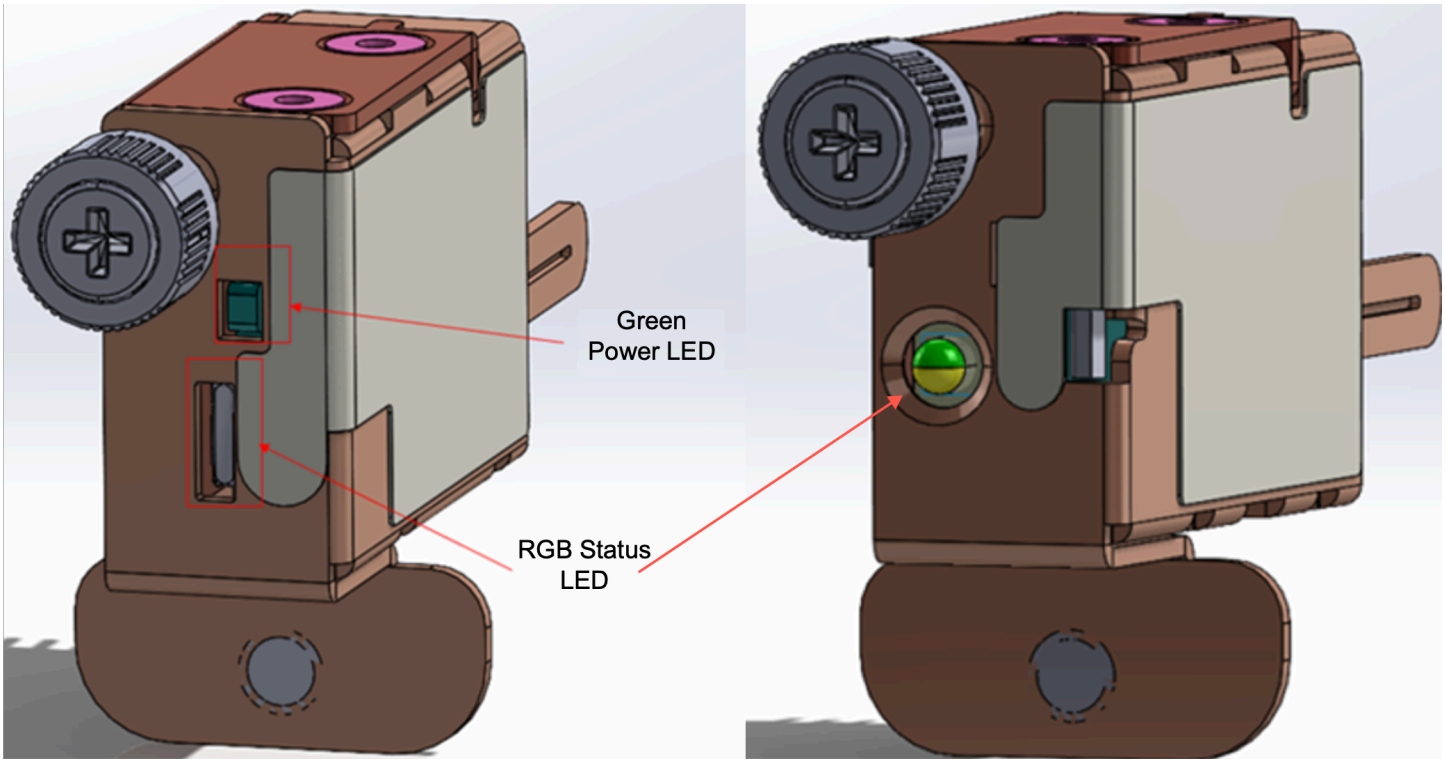
8. Dopo aver completato correttamente la connessione, puoi disconnettere il laptop dal server.

Verifica i LED NSK

Una volta completato il processo di fornitura, controllate i LED NSK.

AWS Outposts supporta due versioni di NSK: Atlas 2.0 e Atlas 3.0. Entrambe le versioni di NSK hanno un LED di stato RGB. Inoltre, l'Atlas 3.0 è dotato di un Power LED verde.

L'immagine seguente mostra la posizione dei LED su Atlas 2.0 e Atlas 3.0:



Atlas 3.0 Atlas 2.0

Per verificare i LED di stato e di alimentazione sull'NSK

1. Controllate il colore del LED di stato RGB. Se il colore è verde, l'NSK è integro. Se il colore non è verde, contatta AWS Support.
2. Se hai un Atlas 3.0 NSK, controlla il LED di alimentazione verde. Se la luce verde è accesa, l'NSK è collegato correttamente all'host ed è alimentato. Se la luce verde non è accesa, contattateci AWS Support.

Riferimento ai comandi dello strumento di configurazione di Outpost

Lo strumento di configurazione di Outpost fornisce i seguenti comandi.

Comandi

- Esporta
- Eco
- Descrivi collegamenti
- Descrivi IP
- Descrivi risolvere
- Descrivi raggiungibilità
- Avvia connessione
- Ottieni connessione

Esporta

export

Utilizza export per impostare le credenziali IAM come variabili di ambiente.

Sintassi

```
Outpost>export variable=value
```

export accetta l'istruzione di assegnazione delle variabili.

Deve essere usato questo formato: *variable*=*value*

Per eseguire l'autenticazione devi esportare le seguenti quattro variabili. Esporta una variabile alla volta. Non inserire spazi prima o dopo il segno di uguale (=).

- AWS_ACCESS_KEY_ID=*access-key-id*
- AWS_SECRET_ACCESS_KEY=*secret-access-key*
- AWS_SESSION_TOKEN=*session-token*
- AWS_DEFAULT_REGION=*Region*

  Utilizza la regione principale del server Outpost come valore per AWS_DEFAULT_REGION.

Example : importazioni di credenziali riuscite

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

Eco

echo

Utilizza echo per visualizzare il valore impostato per una variabile mediante il comando export.

Sintassi

```
Outpost>echo $variable-name
```

Il *variable-name* può essere uno dei seguenti:

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example : riuscito

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

variable name: AWS_DEFAULT_REGION
variable value: us-west-2
checksum: example-checksum
```

Example : errore perché il valore della variabile non è stato impostato con il comando export

```
Outpost> echo $AWS_ACCESS_KEY_ID
```

```
error_type: execution_error
error_attributes:
  AWS_ACCESS_KEY_ID: no value set
error_message: No value set for AWS_ACCESS_KEY_ID using export.
checksum: example-checksum
```

Example : errore perché il nome della variabile non è valido

```
Oupost>echo $foo

error_type: invalid_argument
error_attributes:
  foo: invalid variable name
error_message: Variables can only be AWS credentials.
checksum: example-checksum
```

Example : errore dovuto a un problema di sintassi

```
Outpost>echo AWS_SECRET_ACCESS_KEY

error_type: invalid_argument
error_attributes:
  AWS_SECRET_ACCESS_KEY: not a variable
error_message: Expecting $ before variable name.
checksum: example-checksum
```

Descrivi collegamenti

describe-links

Utilizza describe-links per restituire informazioni sui collegamenti di rete sul server. I server Outpost devono avere un collegamento al servizio e un collegamento all'interfaccia di rete locale (LNI).

Sintassi

```
Outpost>describe-links
```

describe-links non accetta alcun argomento.

Descrivi IP

describe-ip

Utilizza describe-ip per restituire lo stato di assegnazione IP e la configurazione di ciascun collegamento connesso.

Sintassi

```
Outpost>describe-ip
```

describe-ip non accetta alcun argomento.

Descrivi risolvere

describe-resolve

Utilizza describe-resolve per determinare se il server Outpost è in grado di raggiungere un resolver DNS e di risolvere l'indirizzo IP dell'endpoint di configurazione Outpost nella regione. Richiede almeno un collegamento con una configurazione IP.

Sintassi

```
Outpost>describe-resolve
```

describe-resolve non accetta alcun argomento.

Descrivi raggiungibilità

describe-reachability

Utilizza describe-reachability per determinare se il server Outpost è in grado di raggiungere l'endpoint di configurazione Outpost nella regione. Richiede una configurazione DNS funzionante, che è possibile determinare utilizzando describe-resolve.

Sintassi

```
Outpost>describe-reachability
```

describe-reachability non accetta alcun argomento.

Avvia connessione

start-connection

Utilizza start-connection per avviare una connessione con il servizio Outpost nella regione. Questo comando recupera le credenziali Signature Version 4 (SigV4) dalle variabili di ambiente che hai caricato con export. La connessione viene eseguita in modo asincrono e viene restituita immediatamente. Utilizza get-connection per verificare lo stato della connessione.

Sintassi

```
Outpost>start-connection [0|1]
```

start-connection richiede un indice di connessione opzionale per avviare un'altra connessione. Sono validi solo i valori di `0` e `1`.

Example : connessione avviata

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connecdtion-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

Ottieni connessione

get-connection

Utilizza get-connection per restituire lo stato della connessione.

Sintassi

```
Outpost>get-connection [0|1]
```

get-connection richiede un indice di connessione opzionale per restituire lo stato di un'altra connessione. Sono validi solo i valori di `0` e `1`.

Example : connessione riuscita

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

Nota:

- Se `exchange_active` è `True`, la connessione è ancora in corso di attivazione. Riprova tra 5 minuti.
- Se `keys_exchanged` o `connection_established` è `False` e se `exchange_active` è `True`, la connessione è ancora in corso di attivazione. Riprova tra 5 minuti.

Se il problema persiste dopo 1 ora, contatta il Centro AWS Support.

Avvia un'istanza sul tuo server Outpost

Dopo aver installato Outpost e aver reso disponibile la capacità di calcolo e storage, puoi iniziare a creare risorse. Ad esempio, è possibile avviare le istanze Amazon EC2.

Prerequisito

Devi avere un Outpost installato presso il tuo sito. Per ulteriori informazioni, consulta Creazione di un Outpost e ordine della capacità dell'Outpost.

Attività

- Fase 1: Creazione di una sottorete
- Fase 2: Avvio di un'istanza nell'Outpost
- Fase 3: Configurazione della connettività
- Fase 4: Test della connettività

Fase 1: Creazione di una sottorete

Puoi aggiungere sottoreti Outpost a qualsiasi VPC nella regione dell' AWS Outpost. Quando esegui questa operazione, il VPC si estende anche all'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, passa a. Account AWSFase 2: Avvio di un'istanza nell'Outpost

Per creare una sottorete Outpost.

1. Apri la console all'indirizzo https://console.aws.amazon.com/outposts/ AWS 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. Scegli un VPC e specifica un intervallo di indirizzi IP per la sottorete.
5. Scegli Crea.
6. Dopo aver creato la sottorete, abilita la sottorete per le interfacce di rete locale.

Fase 2: Avvio di un'istanza nell'Outpost

Puoi avviare istanze EC2 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 connettersi a un'istanza EC2 in una sottorete Outpost, puoi specificare una coppia di chiavi quando avvii l'istanza, proprio come fai per le istanze in una sottorete zona di disponibilità.

Considerazioni

- Le istanze sui server Outposts includono volumi Instance store ma non volumi EBS. Scegli una dimensione dell'istanza con spazio di archiviazione sufficiente per soddisfare le esigenze della tua applicazione. Per ulteriori informazioni, consulta Volumi Instance store nella Guida per l'utente di Amazon EC2.
- Devi specificare un'AMI con un solo snapshot. Le AMI con più di uno snapshot non sono supportate.
- I dati sui volumi Instance store persistono dopo il riavvio dell'istanza ma non dopo l'arresto dell'istanza. Per mantenere i dati a lungo termine sui volumi Instance store oltre la durata dell'istanza, assicurati di eseguire il backup dei dati su un sistema di archiviazione persistente, come un bucket Amazon S3 o un dispositivo di archiviazione di rete nella tua rete on-premise.
- Per connettere un'istanza in una sottorete Outpost alla rete on-premise, devi aggiungere un'interfaccia di rete locale, come descritto nella procedura seguente.

Per avviare istanze nella tua 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, 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 dai tuoi server Outposts.
5. Scegli un tipo di istanza supportato dai tuoi server Outposts.
6. (Facoltativo) Puoi aggiungere un'interfaccia di rete locale in questa fase o dopo aver creato l'istanza. Per aggiungerla in questa fase, espandi Configurazione di rete avanzata e scegli Aggiungi interfaccia di rete. Scegli la sottorete Outpost. Questo crea un'interfaccia di rete per l'istanza utilizzando l'indice del dispositivo 1. Se hai specificato 1 come indice del dispositivo LNI per la sottorete Outpost, questa interfaccia di rete sarà l'interfaccia di rete locale per l'istanza.
7. Completa la procedura guidata per avviare l'istanza nella sottorete Outpost. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di Amazon EC2:

- Linux: avvia un'istanza utilizzando la nuova procedura guidata di avvio dell'istanza
- Windows: avvia un'istanza utilizzando la nuova procedura guidata di avvio dell'istanza

Fase 3: Configurazione della connettività

Se non hai aggiunto un'interfaccia di rete locale all'istanza durante l'avvio dell'istanza, devi farlo in questa fase. Per ulteriori informazioni, consulta Aggiunta di un LNI dopo l'avvio.

È necessario configurare l'interfaccia di rete locale per l'istanza con un indirizzo IP proveniente dalla rete locale. In genere, questa operazione viene eseguita utilizzando DHCP. Per informazioni, consulta la documentazione per il sistema operativo che esegue l'istanza. Cerca le informazioni sulla configurazione di altre interfacce di rete e di indirizzi IP secondari.

Fase 4: Test della 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 dell'interfaccia di rete locale 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 Linux istance nella Amazon EC2 User Guide. Per informazioni sulla connessione a un'istanza Windows, consulta Connect to your Windows 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 console Amazon EC2 nella pagina di dettaglio 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
```

AWS Outposts connettività verso AWS le regioni

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

> **Note**
>
> Non è possibile utilizzare la connettività privata per la connessione service link che collega il server Outpost alla AWS regione o alla regione di AWS Outposts origine.

Indice

Connettività tramite collegamenti al servizio

Durante il AWS Outposts provisioning, tu o AWS crei una connessione di service link che collega Outpost alla AWS regione o AWS Outposts alla regione d'origine 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

Outpost è in grado di riportare il VPN del collegamento al servizio alla regione AWS tramite la connettività pubblica della regione. A tal fine, Outpost necessita di connettività agli intervalli di IP pubblici della AWS Regione, tramite Internet pubblico o interfaccia virtuale pubblica. AWS Direct Connect Questa connettività può avvenire tramite routing specifici nella VLAN del collegamento al servizio o tramite un routing predefinito di 0.0.0.0/0. Per ulteriori informazioni sugli intervalli pubblici per AWS, consulta Intervalli di indirizzi IP AWS.

Dopo aver stabilito il collegamento di servizio, l'Outpost è in servizio e gestito da. AWS Il collegamento al servizio viene utilizzato per il seguente traffico:

- Gestione del traffico verso l'Outpost tramite il collegamento al servizio, incluso il traffico piano di controllo (control-plane) interno, il monitoraggio delle risorse interne e gli aggiornamenti di firmware e software.
- Traffico tra Outpost e qualsiasi VPC associato, compreso il traffico del piano dati dei clienti.

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 Per informazioni sull'MTU richiesto tra un'istanza in Outpost e un'istanza nella AWS regione tramite il collegamento al servizio, consulta l'unità di trasmissione massima di rete (MTU) per la tua istanza Amazon EC2 nella Guida per l'utente di Amazon EC2.

Raccomandazioni sulla larghezza di banda dei collegamenti al servizio

Per un'esperienza e una resilienza ottimali, AWS consiglia di utilizzare una connettività ridondante di almeno 500 Mbps per la connessione del collegamento di servizio alla regione. AWS L'utilizzo massimo per ogni server Outpost è di 500 Mbps. Per aumentare la velocità di connessione, utilizza più server Outpost. Ad esempio, se hai tre server AWS Outposts , la velocità massima di connessione aumenta a 1,5 Gbit/s (1.500 Mbps). Per ulteriori informazioni, consulta Traffico del collegamento al servizio per i server.

I requisiti di larghezza di banda del collegamento di AWS Outposts servizio variano in base alle 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. Tieni presente che i AWS Outposts server non memorizzano nella cache le AMI. Le AMI vengono scaricate dalla regione a ogni avvio dell'istanza.

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.

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 Outpost e qualsiasi VPC associato.

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	1024-65535	IP del collegamento al servizio	53	Server DNS fornito da DHCP
UDP	443, 1024-65535	IP del collegamento al servizio	443	AWS Outposts Endpoint Service Link
TCP	1024-65535	IP del collegamento al servizio	443	AWS Outposts Endpoint di registrazione

Note

Le istanze di un Outpost non possono utilizzare il collegamento al 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.

Aggiornamenti e collegamento al servizio

AWS mantiene una connessione di rete sicura tra il server Outpost e la regione madre. AWS Questa connessione di rete, denominata service link, è essenziale per la gestione dell'Outpost in quanto fornisce traffico intra-VPC tra l'Outpost e la regione. AWS AWS Le best practice di Well-Architected consigliano di distribuire applicazioni su due Outposts gestiti da diverse zone di disponibilità con un design active-active. Per ulteriori informazioni, consulta Considerazioni sulla progettazione e sull'architettura ad alta disponibilitàAWS Outposts .

Il collegamento al servizio viene aggiornato regolarmente per mantenere la qualità e le prestazioni operative. Durante la manutenzione, è possibile osservare brevi periodi di latenza e perdita di pacchetti su questa rete con conseguente impatto sui carichi di lavoro che dipendono dalla connettività VPC alle risorse ospitate nella regione. Tuttavia, il traffico che attraversa le interfacce di rete locali (LNI) non verrà influenzato. È possibile evitare l'impatto sull'applicazione seguendo le best practice di AWS Well-Architected e assicurando che le applicazioni siano resilienti ai guasti o alle attività di manutenzione che interessano un singolo server Outpost.

Connessioni Internet ridondanti

Quando crei connettività da 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.

Outposts e siti

Gestisci Outposts e siti per. AWS Outposts

Puoi aggiungere tag a siti e Outposts per individuarli o classificarli in base alle esigenze dell'organizzazione. Per ulteriori informazioni sull'etichettatura, consulta Tagging AWS Resources nella Guida.Riferimenti generali di AWS

Argomenti

- Gestione di Outposts
- Gestione dei siti Outpost

Gestione di Outposts

AWS Outposts include risorse hardware e virtuali note come Outposts. Fai riferimento a questa sezione per creare e gestire Outposts, inclusa la modifica del nome e l'aggiunta o la visualizzazione di dettagli o tag.

Per creare un Outpost

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, scegli Outposts.
4. Seleziona Crea outpost.
5. Scegli un tipo di hardware per questo Outpost.
6. Immetti un nome e una descrizione per l'Outpost.
7. Seleziona una zona di disponibilità per il tuo Outpost.
8. (Facoltativo) Scegli Opzione di connettività privata. Per VPC e Subnet, seleziona un VPC e una sottorete nello stesso AWS account e nella stessa zona di disponibilità del tuo Outpost.

> **Note**
>
> Per annullare la connettività privata per il tuo Outpost, devi contattare il Supporto alle imprese AWS .

9. Da ID sito, procedi in uno dei seguenti modi:

   - Per selezionare un sito esistente, scegli il sito.
   - Per creare un nuovo sito, scegli Crea sito, fai clic su Successivo e inserisci le informazioni sul tuo sito nella nuova finestra.

     Dopo aver creato il sito, torna a questa finestra per selezionare il sito. Potrebbe essere necessario aggiornare l'elenco dei siti per visualizzare il nuovo sito. Per aggiornare i dati, scegli l'icona di aggiornamento ().

     Per ulteriori informazioni, consulta the section called “Siti”.

10. Seleziona Crea outpost.

> **Tip**
>
> Per aggiungere capacità al tuo nuovo Outpost, devi effettuare un ordine.

Fai riferimento ai seguenti passaggi per modificare il nome e la descrizione di un Outpost.

Per modificare il nome e la descrizione dell'Outpost

1. Apri la console all'indirizzo https://console.aws.amazon.com/outposts/. AWS Outposts
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, scegli Outposts.
4. Seleziona l'Outpost, quindi scegli Operazioni, Modifica.
5. Modifica il nome e la descrizione

   Immetti il Nome nel relativo campo.

   Immetti la Descrizione nel relativo campo.
6. Seleziona Salvataggio delle modifiche.

Fai riferimento ai seguenti passaggi per visualizzare i dettagli di un Outpost.

Per visualizzare i dettagli dell'Outpost

1. Apri la console all'indirizzo https://console.aws.amazon.com/outposts/ AWS Outposts .
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, scegli Outposts.
4. Seleziona l'Outpost, quindi scegli Operazioni, Visualizza i dettagli.

Puoi anche utilizzarlo per visualizzare i dettagli di Outpost AWS CLI .

Per visualizzare i dettagli dell'Outpost con AWS CLI

- Usa il comando get-outpost AWS CLI .

Fai riferimento ai seguenti passaggi per gestire i tag in un Outpost.

Per gestire i tag Outpost

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, scegli Outposts.
4. Seleziona l'Outpost, quindi scegli Operazioni, Gestisci tag.
5. Aggiungi o rimuovi un tag.

   Per aggiungere un tag scegli Aggiungi nuovo tag e procedi come segue:

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

   Per rimuovere un tag, scegli Rimuovi a destra della chiave e del valore del tag.
6. Seleziona Salvataggio delle modifiche.

Gestione dei siti Outpost

Gli edifici fisici gestiti dal cliente in cui installerai il tuo Outpost. AWS Un sito deve soddisfare i requisiti di infrastruttura, rete e alimentazione del tuo Outpost. Per ulteriori informazioni, consulta Requisiti.

Per creare un sito Outpost

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, scegli Siti.
4. Seleziona Crea sito.
5. Scegli un tipo di hardware supportato per il sito.
6. Inserisci un nome, una descrizione e un indirizzo operativo per il tuo sito. Se sceglie di supportare i rack presso il sito, inserisci le seguenti informazioni:
   - Peso massimo: specifica il peso massimo del rack che può supportare questo sito.
   - Assorbimento di potenza: specifica la potenza assorbita in kVA disponibile nel punto di posizionamento dell'hardware del rack.
   - Opzione alimentazione: specifica l'opzione di alimentazione che è possibile fornire per l'hardware.
   - Connettore di alimentazione: specificare il connettore di alimentazione che AWS dovrebbe fornire le connessioni all'hardware.
   - Caduta di potenza feed: specifica se l'alimentazione arriva al di sopra o al di sotto del rack.
   - Velocità uplink: specifica la velocità di uplink che il rack deve supportare per la connessione alla regione.
   - Numero di uplink: specifica il numero di uplink per ogni dispositivo di rete Outpost che intendi utilizzare per connettere il rack alla rete.
   - Tipo di fibra: specifica il tipo di fibra che verrà utilizzato per collegare l'Outpost alla rete.
   - Standard ottico: specifica il tipo di standard ottico che verrà utilizzato per collegare l'Outpost alla rete.
   - Note: specifica le note relative a un sito.
7. Leggi i requisiti della struttura, quindi seleziona Ho letto i requisiti della struttura.
8. Seleziona Crea sito.

Fai riferimento ai seguenti passaggi per modificare un sito Outpost.

Per modificare un sito

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, scegli Siti.
4. Seleziona il sito, quindi scegli Operazioni, Modifica sito.
5. Puoi modificare il nome, la descrizione, l'indirizzo operativo e i dettagli del sito.

   Se cambi l'indirizzo operativo, tieni presente che eventuali modifiche non si propagheranno agli ordini esistenti.
6. Seleziona Salvataggio delle modifiche.

Fai riferimento ai seguenti passaggi per visualizzare i dettagli di un sito Outpost.

Per visualizzare i dettagli del sito

1. Apri la console all'indirizzo https://console.aws.amazon.com/outposts/ AWS Outposts .
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, scegli Siti.
4. Seleziona il sito, quindi scegli Operazioni, Visualizza i dettagli.

Fai riferimento ai seguenti passaggi per gestire i tag su un sito Outpost.

Per gestire i tag del sito

1. Apri la console all'indirizzo https://console.aws.amazon.com/outposts/ AWS Outposts .
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, scegli Siti.
4. Seleziona il sito, quindi scegli Operazioni, Gestisci tag.
5. Aggiungi o rimuovi un tag.

Per aggiungere un tag scegli Aggiungi nuovo tag e procedi come segue:

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

Per rimuovere un tag, scegli Rimuovi a destra della chiave e del valore del tag.

6. Scegli Save changes (Salva modifiche).

Restituisci un AWS Outposts server

Se AWS Outposts rileva un difetto nel server, ti informeremo, avvieremo la procedura di sostituzione per inviarti un nuovo server e ti forniremo l'etichetta di spedizione tramite la AWS Outposts console.

Se desideri restituire il server perché è stata raggiunta la scadenza del contratto o per qualsiasi altro motivo, contatta il Centro AWS Support.

Argomenti

La seguente procedura illustra come restituire un server a AWS.

1. Prepara il server per la restituzione

Per preparare il server per la restituzione, annulla la condivisione delle risorse, esegui il backup dei dati, elimina le interfacce di rete locale e interrompi le istanze attive.

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 .
   - Utilizzare il AWS CLI per eseguire il comando disassociate-resource-share.

   Per l'elenco delle risorse di Outpost che possono essere condivise, consulta Risorse di Outpost condivisibili.
2. Crea backup dei dati archiviati nello storage delle istanze Amazon EC2 in esecuzione sul server. AWS Outposts
3. Elimina le interfacce di rete locale associate alle istanze in esecuzione sul server.
4. Interrompi le istanze attive associate alle sottoreti sul tuo Outpost. Per terminare le istanze, segui le istruzioni in Termina la tua istanza nella Guida per l'utente di Amazon EC2.

2. Richiedi l'etichetta di spedizione per la restituzione

> **Important**
>
> È necessario utilizzare solo l'etichetta di spedizione fornita. AWS Non creare un'etichetta di spedizione personalizzata.

Richiedi l'etichetta di spedizione in base al motivo della restituzione.

Shipping label for a server that is being replaced

1. Apri la AWS Outposts console all'indirizzo https://console.aws.amazon.com/outposts/.
2. Nel riquadro di navigazione, scegli Ordini.
3. In Riepilogo dell'ordine di sostituzione, scegli Stampa l'etichetta di reso e scegli l'ID di configurazione del server che intendi restituire.

Shipping label for a server that is not being replaced

1. Contatta il Centro AWS Support.
2. Richiedi un'etichetta di spedizione per il server che intendi restituire.

3. Prepara il pacco per la restituzione del server

Per preparare il pacco per la restituzione del server, utilizza la scatola e il materiale di imballaggio con cui è stato originariamente spedito il server. Puoi anche utilizzare la scatola con cui arriva il server sostitutivo. In alternativa, contatta il Centro AWS Support per richiedere una scatola. Dopo aver imballato il server, apponi l'etichetta di spedizione AWS fornita.

4. Restituisci il server tramite il corriere

È necessario effettuare la restituzione del server tramite il corriere designato per il proprio paese. Puoi consegnare il server al corriere o fissare il giorno e l'ora che preferisci affinché il corriere ritiri il server. L'etichetta di spedizione AWS fornita contiene l'indirizzo corretto per restituire il server.

La tabella seguente indica i referenti ai quali rivolgersi per il paese da cui si effettua la spedizione:

Paese	Contatti
Argentina	Contatta il Centro AWS Support. Nella tua richiesta, includi le informazioni che seguono: • Il numero di tracciamento riportato sull'etic hetta AWS di spedizione fornita • La data e l'ora in cui preferisci che il corriere ritiri il server • Un nome di contatto • Un numero di telefono • Un indirizzo e-mail
Bahrein	
Brasile	
Brunei	
Canada	
Cile	
Colombia	
Hong Kong	
India	
Indonesia	
Giappone	
Malesia	
Nigeria	
Oman	
Panama	
Perù	
Filippine	
Serbia	
Singapore	
Sudafrica	

Paese	Contatti
Corea del Sud	
Taiwan	
Tailandia	
Emirati Arabi Uniti	
Vietnam	
Stati Uniti d'America	Contatta UPS. È possibile effettuare la restituzione del server nei modi seguenti: • Restituisci il server durante un normale ritiro UPS presso la tua sede. • Consegna il server presso una sede UPS. • Pianifica un ritiro per la data e l'ora che preferisci. Inserisci il numero di tracciamento riportato sull'etichetta AWS di spedizione fornita per la spedizione gratuita.

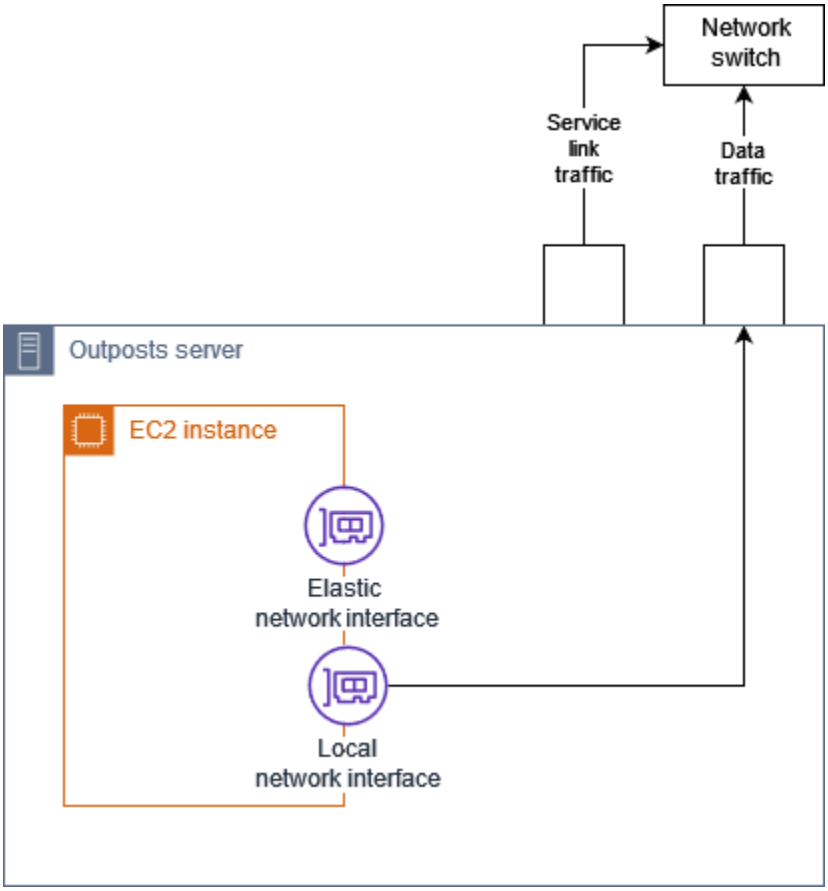
Paese	Contatti
Tutti gli altri paesi	Contatta DHL. È possibile effettuare la restituzione del server nei modi seguenti: • Consegna il server presso una sede DHL. • Pianifica un ritiro per la data e l'ora che preferisci. Inserisci il numero DHL Waybill riportato sull'etichetta di spedizione AWS fornita per la spedizione gratuita. Se ricevi il seguente errore `Courier pickup cannot be scheduled for an import shipment`, di solito significa che il paese di ritiro selezionato non corrisponde al paese di ritiro sull'etichetta di spedizione del reso. Seleziona il paese di origine della spedizione e riprova.

Interfacce di rete locale

Con AWS Outposts i server, un'interfaccia di rete locale (LNI) è un componente di rete logico che collega le istanze Amazon EC2 nella sottorete Outposts alla rete locale.

L'interfaccia di rete locale viene eseguita direttamente sulla tua rete LAN. Con questo tipo di connettività locale non sono necessari router o gateway per comunicare con le apparecchiature on-premise. Le interfacce di rete locale sono denominate in modo simile alle interfacce di rete o alle interfacce di rete elastiche. Facciamo una distinzione tra le due interfacce utilizzando sempre il termine locale quando ci riferiamo alle interfacce di rete locale.

Dopo aver abilitato le interfacce di rete locale su una sottorete Outpost, puoi configurare le istanze EC2 nella sottorete Outpost per includere un'interfaccia di rete locale oltre all'interfaccia di rete elastica. L'interfaccia di rete locale si connette alla rete on-premise mentre l'interfaccia di rete si connette al VPC. Il seguente diagramma mostra un'istanza EC2 su un server Outposts con un'interfaccia di rete elastica e un'interfaccia di rete locale.



È necessario configurare il sistema operativo per consentire all'interfaccia di rete locale di comunicare sulla LAN, proprio come si farebbe per qualsiasi altra apparecchiatura on-premise. Non è possibile utilizzare i set di opzioni DHCP in un VPC per configurare un'interfaccia di rete locale perché un'interfaccia di rete locale viene eseguita sulla LAN.

L'interfaccia di rete elastica funziona esattamente allo stesso modo delle istanze in una sottorete della zona di disponibilità. Ad esempio, puoi utilizzare la connessione di rete VPC per accedere agli endpoint regionali pubblici oppure puoi utilizzare gli endpoint VPC di interfaccia per Servizi AWS accedere utilizzando. Servizi AWS AWS PrivateLink Per ulteriori informazioni, consulta AWS Outposts connettività verso AWS le regioni.

Indice

Informazioni di base sull'interfaccia di rete locale

Le interfacce di rete locali forniscono l'accesso a una rete fisica a due livelli. Un VPC è una rete virtualizzata a tre livelli. Le interfacce di rete localei non supportano i componenti di rete VPC. Questi componenti includono gruppi di sicurezza, liste di controllo gli accessi alla rete, router virtualizzati o tabelle di routing e log di flusso. L'interfaccia di rete locale non fornisce al server Outpost la visibilità nei flussi VPC di livello tre. Il sistema operativo host dell'istanza offre una visibilità completa dei frame della rete fisica. Puoi applicare la logica firewall standard alle informazioni all'interno di questi frame. Tuttavia, questa comunicazione avviene all'interno dell'istanza ma al di fuori dell'ambito dei costrutti virtualizzati.

Considerazioni

- Le interfacce di rete locale supportano i protocolli ARP e DHCP. Non supportano i messaggi di trasmissione L2 generici.
- Le quote per le interfacce di rete locale derivano dalla quota per le interfacce di rete. Per ulteriori informazioni, consulta Interfacce di rete nella Guida per l'utente di Amazon VPC.
- Ogni istanza EC2 può avere un'interfaccia di rete locale.
- Un'interfaccia di rete locale non può utilizzare l'interfaccia di rete primaria (eth0) dell'istanza.

- I server Outposts possono ospitare più istanze EC2, ognuna con un'interfaccia di rete locale.

> **Note**
>
> Le istanze EC2 all'interno dello stesso server possono comunicare direttamente senza inviare dati all'esterno del server Outposts. Questa comunicazione include il traffico su un'interfaccia di rete locale o su interfacce di rete elastiche.

- Un'interfaccia di rete locale è disponibile solo per i server Outposts in esecuzione su una sottorete Outpost.
- Le interfacce di rete locale non supportano la modalità promiscua o lo spoofing degli indirizzi MAC.

Prestazioni

L'LNI di ogni dimensione dell'istanza fornisce una parte della larghezza di banda fisica disponibile di 10 GbE LNI. La tabella seguente elenca le prestazioni della rete LNI per ogni tipo di istanza:

Tipo di istanza	Larghezza di banda di base (Gb/s)	Larghezza di banda burst (Gb/s)
c6id.large	0,15625	2.5
c6id.large	0,15625	2.5
c6id.xlarge	0,3125	2.5
c6id.2xlarge	0,625	2.5
c6id.4xlarge	1,25	2.5
c6id.8xlarge	2.5	2.5
c6id.12xlarge	3,75	3,75
c6id.16xlarge	5	5
c6id.24xlarge	7,5	7,5
c6id.32xlarge	10	10

Tipo di istanza	Larghezza di banda di base (Gb/s)	Larghezza di banda burst (Gb/s)
c6gd.medium	0,15625	4
c6gd.large	0,3125	4
c6gd.xlarge	0,625	4
c6gd.2xlarge	1,25	4
c6gd.4xlarge	2.5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7,5	7,5
c6gd.16xlarge	10	10

Gruppi di sicurezza

Da progettazione, l'interfaccia di rete locale non utilizza gruppi di sicurezza nel tuo VPC. Un gruppo di sicurezza controlla il traffico VPC in entrata e in uscita. L'interfaccia di rete locale non è collegata al VPC. L'interfaccia di rete locale è collegata alla tua rete locale. Per controllare il traffico in entrata e in uscita sull'interfaccia di rete locale, utilizza un firewall o una strategia analoga, proprio faresti con il resto delle apparecchiature on-premise.

Monitoraggio

CloudWatch le metriche vengono prodotte per ogni interfaccia di rete locale, proprio come per le interfacce di rete elastiche. Per ulteriori informazioni sulle istanze Linux, consulta Monitora le prestazioni di rete per la tua istanza EC2 nella Amazon EC2 User Guide. Per le istanze Windows, consulta Monitora le prestazioni di rete per la tua istanza EC2 nella Amazon EC2 User Guide.

Indirizzi MAC

AWS fornisce indirizzi MAC per le interfacce di rete locali. Le interfacce di rete locale utilizzano indirizzi amministrati localmente (LAA) per i rispettivi indirizzi MAC. Un'interfaccia di rete locale utilizza lo stesso indirizzo MAC fino a quando l'interfaccia non viene eliminata. Dopo aver eliminato

un'interfaccia di rete locale, rimuovi l'indirizzo MAC dalle configurazioni locali. AWS può riutilizzare gli indirizzi MAC che non sono più in uso.

Abilitazione delle sottoreti sui server Outposts per le interfacce di rete locale

Usa il comando modify-subnet-attribute di AWS CLI per abilitare una sottorete Outpost per le interfacce di rete locali. È necessario specificare la posizione dell'interfaccia di rete nell'indice del dispositivo. Tutte le istanze avviate in una sottorete Outpost abilitata utilizzano questa posizione del dispositivo per le interfacce di rete locale. Ad esempio, un valore pari a 1 indica che l'interfaccia di rete secondaria (eth1) per un'istanza nella sottorete Outpost è l'interfaccia di rete locale.

Per abilitare una sottorete Outpost per le interfacce di rete locale

Al prompt dei comandi, utilizza il seguente comando per specificare la posizione del dispositivo per l'interfaccia di rete locale.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-1a2b3c4d \
    --enable-lni-at-device-index 1
```

Utilizzo delle interfacce di rete

Questa sezione illustra come utilizzare le interfacce di rete locale.

Attività

- Aggiunta di un'interfaccia di rete locale
- Visualizzazione dell'interfaccia di rete locale
- Configurazione del sistema operativo

Aggiunta di un'interfaccia di rete locale

Puoi aggiungere un'interfaccia di rete locale (LNI) a un'istanza Amazon EC2 su una sottorete Outposts durante o dopo l'avvio. A tale scopo aggiungi un'interfaccia di rete secondaria all'istanza, utilizzando l'indice dei dispositivi che hai specificato quando hai abilitato la sottorete Outpost per le interfacce di rete locale.

Considerazione

Quando si specifica l'interfaccia di rete secondaria mediante la console, l'interfaccia di rete viene creata utilizzando l'indice del dispositivo 1. Se questo non è l'indice del dispositivo specificato quando hai abilitato la sottorete Outpost per le interfacce di rete locali, puoi specificare l'indice del dispositivo corretto utilizzando invece o un SDK. AWS CLI AWS Ad esempio, usa i seguenti comandi da AWS CLI: create-network-interface e attach-network-interface.

Per aggiungere una LNI durante l'avvio dell'istanza

1. Nella procedura guidata di avvio dell'istanza, scegli Modifica accanto a Impostazioni di rete.
2. Expand Configurazione di rete avanzata.
3. Scegli Aggiungi interfaccia di rete. Questo crea un'interfaccia di rete mediante l'indice del dispositivo 1. Se hai specificato 1 come indice del dispositivo LNI per la sottorete Outpost, questa interfaccia di rete sarà l'interfaccia di rete locale per l'istanza.
4. Scegli la sottorete Outpost e aggiorna la configurazione dell'interfaccia di rete secondo necessità.
5. Completa la procedura guidata per avviare l'istanza.

Per aggiungere una LNI dopo l'avvio dell'istanza

1. Nel riquadro di navigazione, scegli Rete e sicurezza, quindi Interfacce di rete.
2. Crea l'interfaccia di rete
    a. Seleziona Crea un'interfaccia di rete.
    b. Seleziona la stessa sottorete Outpost dell'istanza.
    c. Verifica che l'Indirizzo IPv4 privato sia impostato su Assegnazione automatica.
    d. Seleziona un gruppo di sicurezza I gruppi di sicurezza non si applicano alle LNI, quindi il gruppo di sicurezza selezionato non è pertinente.
    e. Seleziona Crea un'interfaccia di rete.
3. Collega l'interfaccia di rete all'istanza
    a. Seleziona la casella di controllo relativa all'interfaccia di rete appena creata.
    b. Seleziona Operazioni, Collega.
    c. Seleziona l'istanza.

d. Scegli Collega. L'interfaccia di rete è collegata all'indice del dispositivo 1. Se hai specificato 1 come indice del dispositivo LNI per la sottorete Outpost, questa interfaccia di rete è l'interfaccia di rete locale per l'istanza.

Visualizzazione dell'interfaccia di rete locale

Mentre l'istanza è in esecuzione, puoi utilizzare la console Amazon EC2 per visualizzare sia l'interfaccia di rete elastica che l'interfaccia di rete locale per le istanze nella sottorete Outpost. Seleziona l'istanza e scegli la scheda Rete.

La console visualizza un indirizzo IPv4 privato per la LNI dalla sottorete CIDR. Questo indirizzo non è l'indirizzo IP della LNI e non è utilizzabile. Tuttavia, questo indirizzo viene allocato dalla sottorete CIDR, pertanto è necessario tenerne conto nel dimensionamento della sottorete. Devi impostare l'indirizzo IP per la LNI all'interno del sistema operativo guest, in modo statico o tramite il server DHCP.

Configurazione del sistema operativo

Dopo aver abilitato le interfacce di rete locale, le istanze Amazon EC2 avranno due interfacce di rete, una delle quali è un'interfaccia di rete locale. Assicurati di configurare il sistema operativo delle istanze Amazon EC2 che avvii affinché supporti una configurazione di rete multihomed.

Connettività della rete locale per i server

Questo argomento illustra i requisiti di cablaggio e topologia di rete per l'hosting di un server Outpost. Per ulteriori informazioni, consulta Interfacce di rete locale.

Indice

Topologia del server nella rete

Il server Outpost richiede due collegamenti distinti alle apparecchiature di rete. Ogni collegamento utilizza un cavo diverso e gestisce un tipo di traffico diverso. I cavi multipli servono solo per l'isolamento della classe di traffico e non per la ridondanza. Non è necessario collegare i due cavi a una rete comune.

La tabella seguente descrive i tipi di traffico e le etichette dei server Outpost.

Etichetta di traffico	Descrizione
2	Traffico di collegamento al servizio: questo traffico 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' AWS avamposto . Tale tipo di traffico include il collegamento al servizio dall'Outpost alla regione. Il collegame nto al servizio è uno o più VPN personalizzati dall'Outpost alla regione. L'Outpost si connette alla zona di disponibilità nella regione scelta al momento dell'acquisto.
1	Traffico di collegamento dell'interfaccia di rete locale (LNI): questo traffico consente la comunicazione dal VPC alla LAN locale tramite l'interfaccia di rete locale. Il traffico di collegame nto locale include le istanze in esecuzione sull'Outpost che comunicano con la rete on-premise. Il traffico di collegamento locale può includere anche le istanze che comunicano con Internet tramite la tua rete on-premise.

Connettività fisica del server

Ogni server Outpost include porte uplink fisiche non ridondanti. Le porte hanno i propri requisiti di velocità e connettori, come segue:

- 10 GbE — tipo di connettore QSFP+

Cavo QSFP+

Il cavo QSFP+ ha un connettore da collegare alla porta 3 del server Outpost. L'altra estremità del cavo QSFP+ ha quattro interfacce SFP+ da collegare allo switch. Due delle interfacce sul lato switch sono contrassegnate 1 e 2. Entrambe le interfacce sono necessarie per il funzionamento di un server Outpost. Utilizza l'interfaccia 2 per il traffico del collegamento al servizio e l'interfaccia 1 per il traffico del collegamento LNI. Le interfacce rimanenti non vengono utilizzate.

Traffico del collegamento al servizio per i server

Configura la porta del collegamento al servizio sullo switch come porta di accesso senza tag a una VLAN con un gateway e un routing verso i seguenti endpoint della regione:

- Endpoint del collegamento al servizio
- Endpoint di registrazione Outposts

La connessione service link deve disporre di un DNS pubblico per consentire a Outpost di rilevare il proprio endpoint di registrazione nella regione. AWS La connessione può avere un dispositivo NAT tra il server Outpost e l'endpoint di registrazione. Per ulteriori informazioni sugli intervalli di indirizzi pubblici per AWS, consulta gli intervalli di indirizzi AWS IP nella Amazon VPC User Guide e gli AWS Outposts endpoint e le quote nel. Riferimenti generali di AWS

Per registrare il server, apri le seguenti porte di rete:

- TCP 443
- UDP 443
- UDP 53

Velocità di uplink

Ogni server Outposts richiede una velocità minima di uplink di 20 Mbps verso la regione AWS .

Potrebbe essere necessario un uplink più veloce a seconda dell'utilizzo del collegamento LNI e del collegamento al servizio. Per ulteriori informazioni, consulta Raccomandazioni relative alla larghezza di banda per i collegamenti al servizio.

Traffico del collegamento dell'interfaccia di rete locale (LNI)

Configura la porta del collegamento LNI sul dispositivo di rete upstream come porta di accesso standard a una VLAN sulla rete locale. Se disponi di più di una VLAN, configura tutte le porte del dispositivo di rete upstream come porte trunk. Configura la porta sul dispositivo di rete upstream in modo da prevedere più indirizzi MAC. Ogni istanza avviata sul server utilizzerà un indirizzo MAC. Alcuni dispositivi di rete offrono funzionalità di sicurezza delle porte che disattivano una porta che riporta più indirizzi MAC.

> **Note**
>
> AWS Outposts i server non etichettano il traffico VLAN. Se configuri la tua LNI come trunk, devi assicurarti che il sistema operativo assegni i tag al traffico VLAN.

Nell'esempio seguente viene illustrato come configurare il tagging VLAN per la propria LNI su Amazon Linux 2023. Se utilizzi un'altra distribuzione Linux, consulta la relativa documentazione per la configurazione del tagging VLAN.

Esempio: per configurare il tagging VLAN per la tua LNI su Amazon Linux 2023 e Amazon Linux 2

1. Assicurati che il modulo 8021q sia caricato nel kernel. In caso contrario, caricalo utilizzando il comando `modprobe`.

   ```
   modinfo 8021q
   modprobe --first-time 8021q
   ```

2. Crea il dispositivo VLAN. In questo esempio:

   - Il nome dell'interfaccia della LNI è `ens6`
   - L'ID VLAN è `59`
   - Il nome assegnato al dispositivo VLAN è `ens6.59`

   ```
   ip link add link ens6 name ens6.59 type vlan id 59
   ```

3. Facoltativo. Completa questo passaggio se desideri assegnare manualmente l'IP. In questo esempio stiamo assegnando l'IP 192.168.59.205, dove la sottorete CIDR è 192.168.59.0/24.

```
ip addr add 192.168.59.205/24 brd 192.168.59.255 dev ens6.59
```

4. Attiva il collegamento.

```
ip link set dev ens6.59 up
```

Per configurare le interfacce di rete a livello di sistema operativo e rendere permanenti le modifiche ai tag VLAN, fai riferimento alle seguenti risorse:

- Se utilizzi Amazon Linux 2, consulta Configurare l'interfaccia di rete utilizzando ec2-net-utils per Amazon Linux nella Amazon EC2 User Guide.
- Se utilizzi Amazon Linux 2023, consulta Servizio di rete nella Guida per l'utente di Amazon Linux 2023.

Assegnazione dell'indirizzo IP del server

Non è necessaria l'assegnazione di indirizzi IP pubblici per i server Outpost.

Il protocollo DHCP (Dynamic Host Control Protocol) è un protocollo di gestione della rete utilizzato per automatizzare il processo di configurazione dei dispositivi sulle reti IP. Nel contesto dei server Outpost, puoi utilizzare DHCP in due modi:

- Schede di rete sul server
- Interfacce di rete locale sulle istanze

Per il collegamento al servizio, i server Outpost utilizzano DHCP per connettersi alla rete locale. DHCP deve restituire i server di nomi DNS e un gateway predefinito. I server Outpost non supportano l'assegnazione di un indirizzo IP statico del collegamento al servizio.

Per il collegamento LNI, utilizza DHCP per configurare le istanze da collegare alla rete locale. Per ulteriori informazioni, consulta the section called “Configurazione del sistema operativo”.

> **Note**
>
> Assicurati di utilizzare un indirizzo IP stabile per il server Outpost. Le modifiche all'indirizzo IP possono causare interruzioni temporanee del servizio nella sottorete Outpost.

Registrazione del server

Quando i server Outpost stabiliscono una connessione sulla rete locale, utilizzano la connessione del collegamento al servizio per connettersi agli endpoint di registrazione Outpost e registrarsi. La registrazione richiede un DNS pubblico. Quando i server si registrano, creano un tunnel sicuro verso il loro endpoint del collegamento al servizio nella regione. I server Outpost utilizzano la porta TCP 443 per facilitare le comunicazioni con la regione sulla rete Internet pubblica. Attualmente, AWS Outposts i server non supportano la connettività privata tramite VPC. Per ulteriori informazioni, consulta the section called “Fase 6: Autorizzazione del server”.

Lavorare con AWS Outposts risorse condivise

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 i VPC e avviare ed eseguire istanze sull'Outpost condiviso.

In questo modello, l'AWSaccount proprietario delle risorse Outpost (proprietario) condivide le risorse con altri AWS account (consumatori) della stessa organizzazione. I consumatori possono creare risorse su Outposts che vengono condivise con loro nello stesso modo in cui creerebbero risorse su Outposts create nel proprio account. Il proprietario è responsabile della gestione dell'Outpost e delle risorse che crea al suo interno. I proprietari possono modificare o revocare l'accesso condiviso in qualsiasi momento. Ad eccezione delle istanze che utilizzano Capacity Reservations, i proprietari possono anche visualizzare, modificare ed eliminare le risorse create dai consumatori su Outposts condivisi. I proprietari non possono modificare le istanze che i consumatori avviano in Prenotazioni di capacità che hanno condiviso.

I consumatori sono responsabili della gestione delle risorse che creano su Outposts e che vengono condivise con loro, comprese le risorse che utilizzano le prenotazioni di capacità. I consumatori non possono visualizzare o modificare le risorse di proprietà di altri consumatori o del proprietario di Outpost. Inoltre, non possono modificare gli Outposts condivisi con loro.

Un proprietario di Outpost può condividere le risorse di Outpost con:

- AWSAccount specifici all'interno della sua organizzazione in. AWS Organizations
- Un'unità organizzativa all'interno della sua organizzazione inAWS Organizations.
- La sua intera organizzazione inAWS Organizations.

Indice

- Condivisione di una risorsa Outpost
- Annullamento della condivisione di una risorsa Outpost condivisa
- Identificare una risorsa Outpost condivisa
- Autorizzazioni condivise per le risorse Outpost
- Fatturazione e misurazione
- Limitazioni

Risorse Outpost condivisibili

Un proprietario di Outpost può condividere le risorse Outpost elencate in questa sezione con i consumatori.

Per le risorse del rack, consulta Lavorare con AWS Outposts le risorse condivise nella Guida per AWS Outposts l'utente del rack Outposts.

- Host dedicati allocati: i consumatori con accesso a questa risorsa possono:
  - Avvia ed esegui istanze EC2 su un host dedicato.
- Outposts: i consumatori che hanno accesso a questa risorsa possono:
  - Crea e gestisci sottoreti su Outpost.
  - Usa l'AWS OutpostsAPI per visualizzare le informazioni sull'Outpost.
- Siti: i consumatori con accesso a questa risorsa possono:
  - Crea, gestisci e controlla un Outpost sul sito.
- Sottoreti: i consumatori con accesso a questa risorsa possono:
  - Visualizzare informazioni sulle sottoreti.
  - Avvia ed esegui istanze EC2 nelle sottoreti.

  Usa la console Amazon VPC per condividere una sottorete Outpost. Per ulteriori informazioni, consulta Condivisione di una sottorete nella Amazon VPC User Guide.

Prerequisiti per la condivisione delle risorse Outposts

- Per condividere una risorsa di Outpost con l'organizzazione o con un'unità organizzativa inAWS Organizations, è necessario 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 AWS account. 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 di Outpost si integra con AWS Resource Access Manager (). AWS RAM AWS RAMè 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 i consumatori con cui condividerle. I consumatori possono essere singoli AWS account, unità organizzative o un'intera organizzazione inAWS Organizations.

Per ulteriori informazioni su AWS RAM, consulta la Guida per l'utente di AWS RAM.

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 di disponibilità `us-east-1a` per l'account AWS potrebbe avere un'ubicazione diversa rispetto a `us-east-1a` per un altro account AWS.

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

Per visualizzare gli ID AZ per le zone di disponibilità nell'account

1. Aprire la console AWS RAM all'indirizzo https://console.aws.amazon.com/ram.
2. Gli ID AZ per la regione attuale vengono visualizzati nel pannello Il tuo ID AZ sul lato destro dello schermo.

> **Note**
>
> Le tabelle di routing del gateway locale si trovano nella stessa AZ di Outpost, quindi 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 consumatore, quest'ultimo può creare risorse sull'Outpost nello stesso modo in cui creerebbe risorse su Outposts create con il proprio account. I consumatori con accesso alle tabelle di routing dei gateway locali condivise possono creare e gestire associazioni VPC. Per ulteriori informazioni, consulta Risorse Outpost condivisibili.

Per condividere una risorsa Outpost, è necessario aggiungerla a una condivisione di risorse. Una condivisione di risorse è una risorsa AWS RAM che ti consente di condividere le risorse tra account AWS. Un 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 utilizzando la AWS RAM console.

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, i consumatori ricevono un invito a partecipare alla condivisione di risorse e ottengono l'accesso alla risorsa Outpost condivisa dopo aver accettato l'invito.

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 console AWS Outposts all'indirizzo https://console.aws.amazon.com/outposts/.
2. Nel riquadro di navigazione, scegli Outposts.
3. Seleziona l'avamposto, quindi scegli Azioni, Visualizza dettagli.
4. Nella pagina di riepilogo di Outpost, scegli Condivisioni di risorse.
5. Selezionare Create resource share (Crea condivisione di 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, usa anche la seguente procedura.

Per condividere una tabella di routing di Outpost o del gateway locale di tua proprietà utilizzando 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 utilizzando la AWS CLI

Utilizza il comando create-resource-share.

Annullamento della condivisione di una risorsa Outpost condivisa

Quando una Outpost condivisa non viene condivisa, i consumatori non possono più visualizzare Outpost nella console. AWS Outposts Non possono creare nuove sottoreti su Outpost, creare nuovi volumi EBS su Outpost o visualizzare i dettagli e i tipi di istanza di Outpost utilizzando la console o il. AWS Outposts AWS CLI Le sottoreti, i volumi o le istanze esistenti creati dai consumatori non vengono eliminati. Tutte le sottoreti esistenti create dai consumatori in Outpost possono ancora essere utilizzate per avviare nuove istanze.

Quando una tabella di routing gateway locale condivisa non è condivisa, i consumatori non possono più creare nuove associazioni VPC ad essa. Tutte le associazioni VPC esistenti create dai consumatori rimangono associate alla tabella delle rotte. Le risorse in questi VPC possono continuare a indirizzare il traffico verso il gateway locale.

Per annullare la condivisione di una risorsa Outpost condivisa di tua proprietà, devi rimuoverla dalla condivisione di risorse. È possibile effettuare tale operazione mediante la console AWS RAM o l'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.

Identificare una risorsa Outpost condivisa

I proprietari e i consumatori possono identificare gli Outposts condivisi utilizzando la AWS Outposts console e. AWS CLI Possono identificare le tabelle di routing dei gateway locali condivise utilizzando. AWS CLI

Per identificare un Outpost condiviso utilizzando la console AWS Outposts

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

Autorizzazioni condivise per le risorse Outpost

Autorizzazioni per i proprietari

I proprietari sono responsabili della gestione dell'Outpost e delle risorse che vi creano. 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 i consumatori

I consumatori possono creare risorse su Outposts che vengono condivise con loro nello stesso modo in cui creerebbero risorse su Outposts create nel proprio account. I consumatori sono responsabili della gestione delle risorse che lanciano su Outposts e che vengono condivise con loro. I consumatori non possono visualizzare o modificare le risorse di proprietà di altri consumatori o del proprietario di Outpost e non possono modificare gli Outpost condivisi con loro.

Fatturazione e misurazione

Ai proprietari vengono fatturate le risorse Outposts e 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 dei gateway locali. 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.

Ai consumatori vengono fatturate le risorse applicative che creano su Outposts 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 sui limiti di condivisione dei 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 maggiori informazioni sui programmi di conformità applicabili AWS Outposts, consulta la sezione AWS Servizi rientranti 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 .

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

Il modello di responsabilità AWS condivisa modello di 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 di mantenere il controllo sui 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). La NSK è necessaria per decrittografare i dati sui serverOutpost.

Crittografia in transito

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

Eliminazione dei dati

Quando termina un'istanza EC2, la memoria a essa allocata viene annullata (impostata su zero) dall'hypervisor prima che venga allocata a una nuova istanza e ogni blocco di archiviazione viene ripristinato.

La distruzione della chiave di sicurezza Nitro elimina crittograficamente i dati presenti nel tuo Outpost. Per ulteriori informazioni, consulta Eliminazione crittografica dei dati del server.

Gestione delle identità e degli accessi (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 AWS risorse. 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

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 che puoi usare con AWS Outposts

Funzionalità IAM	AWS Supporto Outposts
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
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 azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM 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

Politiche basate sulle risorse all'interno di Outposts AWS

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il

principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per AWS Outposts

Supporta le operazioni di policy	Sì

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

L'elemento `Action`di una policy JSON descrive le azioni 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 azioni 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. Cioè, 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). Puoi eseguire questa operazione per azioni 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 una singola istruzione, separa gli ARN con le virgole.

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

Per visualizzare un elenco dei tipi di risorse AWS Outposts e dei relativi ARN, consulta 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. Cioè, quale principale può eseguire azioni 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`è facoltativo. Puoi 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.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi 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

ACL in Outposts AWS

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

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 Che cos'è 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 Cambio di un ruolo (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 la pagina Forward access sessions.

Ruoli di servizio per AWS Outposts

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

Ruoli collegati ai servizi per Outposts AWS

Supporta i 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 nel tuo account 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. Utilizzo di 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 nella Guida per l'utente di IAM.

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

Indice

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. Puoi 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 puoi 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 IAM Access Analyzer 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 Configurazione dell'accesso alle API protetto 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"
    }
  ]
}
```

Utilizzo di ruoli collegati ai servizi per AWS Outposts

AWS Outposts utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Outposts I ruoli collegati ai servizi sono predefiniti AWS Outposts e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio 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 aver eliminato le risorse correlate. In questo modo proteggi AWS Outposts le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai

servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per AWS Outposts

AWS Outposts utilizza il ruolo collegato al servizio denominato AWSServiceRoleForOutposts_ ***OutpostID: consente a Outposts*** di accedere alle AWS risorse per la connettività privata per tuo conto. Questo ruolo collegato ai servizi consente la configurazione della connettività privata, crea interfacce di rete e le collega alle istanze degli endpoint del collegamento al servizio.

Il ruolo collegato al servizio AWSServiceRoleForOutposts _ *OutpostID prevede* che i seguenti servizi assumano il ruolo:

- `outposts.amazonaws.com`

Il ruolo collegato al AWSServiceRoleForOutpostsservizio _ ***OutpostID include*** le seguenti politiche:

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ OutpostID

La AWSOutpostsServiceRolePolicypolitica è una politica di ruolo collegata al servizio che consente l'accesso alle risorse gestite da AWS . AWS Outposts

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

- Operazione: `ec2:DescribeNetworkInterfaces` su `all AWS resources`
- Operazione: `ec2:DescribeSecurityGroups` su `all AWS resources`
- Operazione: `ec2:CreateSecurityGroup` su `all AWS resources`
- Operazione: `ec2:CreateNetworkInterface` su `all AWS resources`

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

- Operazione: `ec2:AuthorizeSecurityGroupIngress` su `all AWS resources that match the following Condition:`

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

- Operazione: `ec2:AuthorizeSecurityGroupEgress` su `all AWS resources that match the following Condition:`

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

- Operazione: `ec2:CreateNetworkInterfacePermission` su `all AWS resources that match the following Condition:`

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

- Operazione: `ec2:CreateTags` su `all AWS resources that match the following Condition:`

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}}
```

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.

Creazione di un ruolo collegato ai servizi 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.

Modifica di un ruolo collegato ai servizi per AWS Outposts

AWS Outposts non consente di modificare il ruolo collegato al servizio AWSServiceRoleForOutposts _ *OutpostID*. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi 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.

> **Note**
>
> 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.

> **Warning**
>
> È necessario eliminare Outpost prima di poter eliminare il ruolo collegato al servizio AWSServiceRoleForOutposts _ *`OutpostID`*. La seguente procedura consente di eliminare il tuo Outpost.

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

Per eliminare AWS Outposts le risorse utilizzate da AWSServiceRoleForOutposts _ OutpostID

- Contatta AWS Enterprise Support per eliminare Outpost.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al servizio AWSServiceRoleForOutposts _ *`OutpostID`*. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS Outposts

AWS Outposts supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote per AWS 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: AWSOutpostsServiceRolePolicy

Questa policy è associata a un ruolo collegato al servizio che consente di eseguire azioni AWS Outposts per conto dell'utente. Per ulteriori informazioni, consulta Uso di ruoli collegati ai servizi.

AWS politica gestita: AWSOutpostsPrivateConnectivityPolicy

Questa policy è associata a un ruolo collegato al servizio che consente di eseguire azioni AWS Outposts per conto dell'utente. Per ulteriori informazioni, consulta Uso di ruoli collegati ai servizi.

AWS politica gestita: AWSOutpostsAuthorizeServerPolicy

Utilizza questa policy per concedere le autorizzazioni necessarie per ammettere l'hardware del server Outpost nella tua rete on-premise. Per ulteriori informazioni, consulta Concessione dell'autorizzazione.

Questa policy include le seguenti autorizzazioni:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Outposts aggiornamenti alle politiche AWS gestite

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

Modifica	Descrizione	Data
AWSOutpostsAuthorizeServerPolicy: nuova policy	AWS Outposts ha aggiunto un criterio che concede le autorizzazioni per autorizzare l'hardware del server Outpost nella rete locale.	4 gennaio 2023
AWS Outposts ha iniziato a tenere traccia delle 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 le istanze EC2 e i volumi EBS in esecuzione su Outpost, consulta Sicurezza dell'infrastruttura 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.

Resilienza in AWS Outposts

Per un'elevata disponibilità, puoi ordinare server Outposts aggiuntivi. 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.

I server Outposts includono volumi di archivio dell'istanza ma non supportano i volumi Amazon EBS. I dati sui volumi di archivio dell'istanza persistono dopo il riavvio dell'istanza ma non dopo l'arresto dell'istanza. Per mantenere i dati a lungo termine sui volumi Instance store oltre la durata dell'istanza, assicurati di eseguire il backup dei dati su un sistema di archiviazione persistente, come un bucket Amazon S3 o un dispositivo di archiviazione di rete nella tua rete on-premise.

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:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti 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.

Monitoraggio dell'Outpost

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 i tuoi 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 metriche per AWS Outposts.

CloudTrail registri

Utilizza AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate alle API AWS. È possibile archiviare queste chiamate come file di log in Amazon S3. È possibile utilizzare questi CloudTrail registri per determinare informazioni quali 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 inoltre informazioni per le chiamate alle azioni API dai servizi su un Outpost, come Amazon EC2 e Amazon EBS. Per ulteriori informazioni, consulta AWS Outpostsinformazioni in 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 da Outpost ai dispositivi di out-of-band sicurezza e monitoraggio di Outpost. 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 Guida al mirroring del traffico per Amazon Virtual Private Cloud.

AWS Health Dashboard

AWS Health Dashboard visualizza le informazioni e le notifiche che vengono avviate da modifiche nell'integrità 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. In quanto parte del servizio AWS Health, AWS Health Dashboard non richiede l'installazione e può essere visualizzato da qualsiasi utente autenticato nell'account. Per ulteriori informazioni, consulta Nozioni di base di AWS Health Dashboard.

CloudWatch metriche per AWS Outposts

AWS Outpostspubblica 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 a`1`, 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 problemi di `ConnectedStatus`, consigliamo di verificare la connettività alla regione AWS dall'interno della rete on-premise e di contattare l'assistenza AWS 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

Parametri di Outpost

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`

`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. 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 sull'Outpost per Prenotazioni della capacità on demand (ODCR). Questo parametro non misura le istanze riservate Amazon EC2.

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni `InstanceType` e `OutpostId`

`UsedReservedInstances`

Il numero di istanze disponibili sull'Outpost per Prenotazioni della capacità on demand (ODCR). Questo parametro non misura le istanze riservate Amazon EC2.

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni `InstanceType` e `OutpostId`

`TotalReservedInstances`

Il numero di istanze disponibili sull'Outpost per Prenotazioni della capacità on demand (ODCR). Questo parametro non misura le istanze riservate Amazon EC2.

Unità: numero

Risoluzione massima: 5 minuti

Dimensioni `InstanceType` e `OutpostId`

Dimensioni dei parametri dell'Outpost

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.

Visualizza le CloudWatch metriche relative al tuo avamposto

Puoi visualizzare le CloudWatch metriche dei tuoi sistemi di bilanciamento del carico utilizzando la console. CloudWatch

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. (Facoltativo) Per visualizzare tutte le dimensioni di un parametro, inseriscine il nome nella casella di ricerca.

Visualizzazione dei parametri usando AWS CLI

Utilizza il seguente comando list-metrics per elencare i parametri disponibili:

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

Per ottenere le statistiche su un parametro utilizzando AWS CLI

Usa il get-metric-statisticscomando seguente per ottenere 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 chiamate API AWS Outposts con AWS CloudTrail.

AWS Outpostsè integrato conAWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio inAWS Outposts. CloudTrail acquisisce tutte le chiamate API AWS Outposts come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS Outposts e le chiamate di codice alle operazioni delle API AWS Outposts. Se crei un trail, puoi abilitare la consegna continua di CloudTrail eventi a un bucket S3, inclusi gli eventi per. AWS Outposts Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviataAWS Outposts, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

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

AWS Outpostsinformazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività inAWS Outposts, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nell'account AWS che includa gli eventi per AWS Outposts, crea un trail. Un trail consente di CloudTrail inviare i file di registro a un bucket S3 nel dispositivo principale. Regione AWS Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni nella partizione AWS e distribuisce i file di log nel bucket S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte AWS Outposts le azioni vengono registrate da CloudTrail. Sono documentate nella Documentazione di riferimento API AWS Outposts. Ad esempio, le chiamate a `CreateOutpost`, `GetOutpostInstanceTypes`, e `ListSites` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni sull'identità consentono di stabilire se la richiesta è stata effettuata:

- Con le credenziali root o utente.
- Con credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Da un altro Servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di log di AWS Outposts

Un trail è una configurazione che consente la consegna di eventi come file di registro a un bucket S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta da un'origine. Include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateOutpost`azione.

```
{
    "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"
}
```

Manutenzione dell'Outpost

Secondo il modello di responsabilità condivisa modello 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 inoltre le prestazioni, lo stato e le metriche di Outpost e determina se è necessaria una manutenzione.

> **Warning**
>
> Eventuali guasti dell'unità disco sottostante 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 o un dispositivo di archiviazione di rete nella tua rete on-premise.

Indice

Manutenzione dell'hardware

Se AWS rileva un problema irreparabile con l'hardware che ospita le istanze Amazon EC2 in esecuzione sul tuo Outpost, notificheremo al proprietario dell'Outpost e al proprietario delle istanze che è previsto il ritiro delle istanze interessate. Per ulteriori informazioni, consulta Ritiro dell'istanza nella Guida per l'utente di Amazon EC2.

AWS interrompe le istanze interessate alla data di ritiro dell'istanza. I dati sui volumi dell'archivio dell'istanza non persistono dopo l'interruzione dell'istanza. Pertanto, è importante agire prima della data di ritiro dell'istanza. Innanzitutto, trasferisci i dati a lungo termine dai volumi dell'archivio dell'istanza per ogni istanza interessata al sistema di archiviazione persistente, ad esempio un bucket Amazon S3 o un dispositivo di storage di rete nella tua rete.

Il server sostitutivo verrà inviato al sito Outpost. Successivamente, esegui queste operazioni:

- Stacca i cavi di rete e di alimentazione dal server che presenta il problema irreversibile e, se necessario, rimuovilo dal rack.
- Installa il server sostitutivo nella stessa posizione. Segui le istruzioni di installazione riportate in Installazione del server Outpost.
- Imballa il server irreparabile nella stessa confezione AWS in cui è arrivato il server sostitutivo.
- Utilizza l'etichetta prepagata per la spedizione del reso disponibile nella console e allegata ai dettagli di configurazione dell'ordine o all'ordine del server sostitutivo.
- Restituisci il server a. AWS Per ulteriori informazioni, consulta Reso di un server AWS Outposts.

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.

Procedure ottimali per gli eventi AWS Outposts 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 server 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.
- Evita la commutazione ripetuta dei sistemi di alimentazione (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.

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.

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 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:

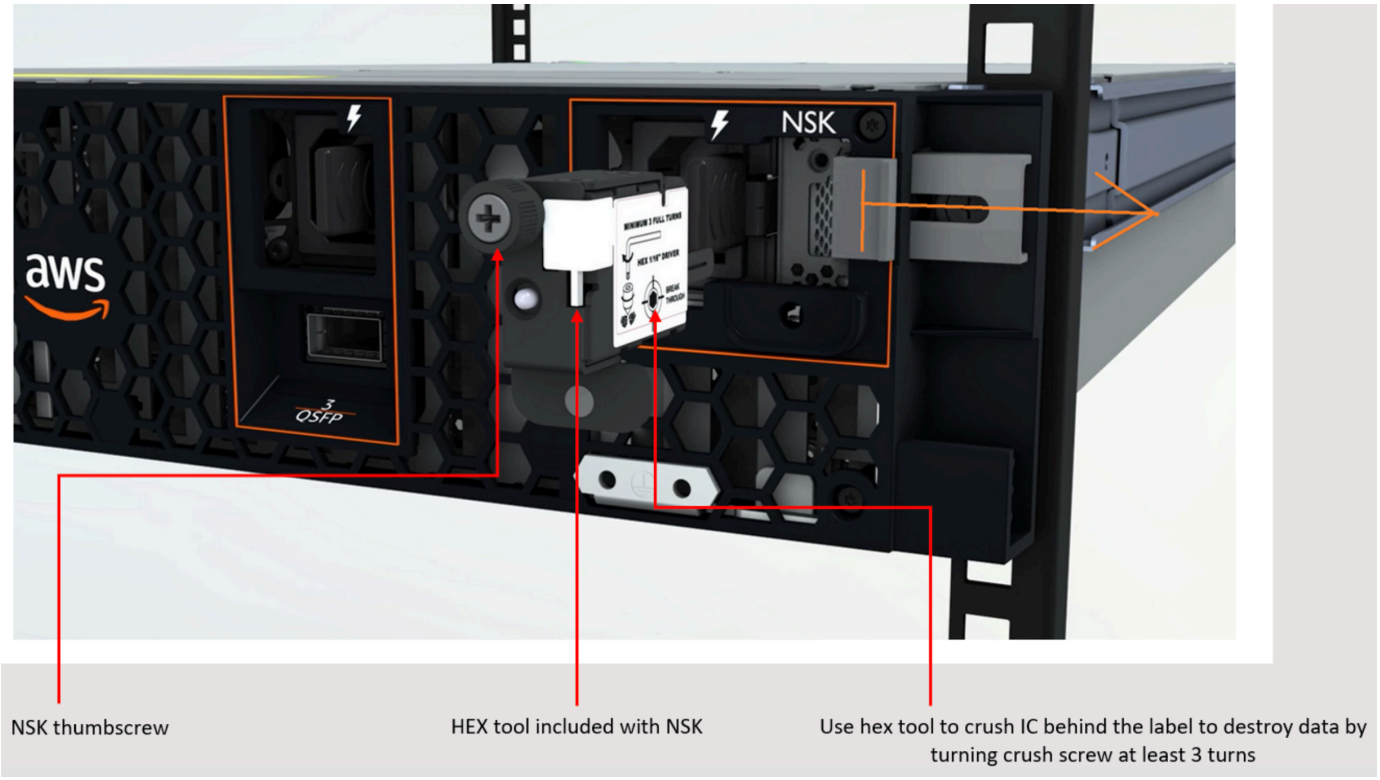
- Il AWS blog Monitoring best practices for AWS Outposts tratta le migliori pratiche di osservabilità e gestione degli eventi specifiche di Outposts.
- Il AWS blog Debugging tool per la connettività di rete di Amazon VPC spiega lo strumento VPC - SetupIP. AWSSupport MonitoringFrom Questo strumento è un documento AWS Systems Manager (documento SSM) che crea un'istanza di monitoraggio Amazon EC2 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 automatic 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 .

Eliminazione crittografica dei dati del server

La chiave di sicurezza Nitro (NSK) è necessaria per decrittografare i dati sul server. Quando restituite il server AWS, sia perché state sostituendo il server o interrompendo il servizio, potete distruggere l'NSK per distruggere crittograficamente i dati sul server.

Per eliminare crittograficamente i dati sul server

1. Rimuovere l'NSK dal server prima di rispedirlo a. AWS
2. Verifica di disporre della NSK corretta fornita con il server.
3. Rimuovi la piccola chiave esagonale/chiave a brugola che si trova sotto l'adesivo.
4. Usa la chiave esagonale per dare tre giri completi alla piccola vite posta sotto l'adesivo. Questa operazione distrugge la NSK ed elimina crittograficamente tutti i dati sul server.


NSK
aws
QSFP
NSK thumbscrew
HEX tool included with NSK
Use hex tool to crush IC behind the label to destroy data by turning crush screw at least 3 turns

AWS Outposts end-of-term opzioni

Alla fine del AWS Outposts mandato, hai tre opzioni:

- Rinnovare l'abbonamento e mantenere il tuo Outpost esistente.
- Chiudere l'abbonamento e restituire il server Outpost.
- Passa a un month-to-month abbonamento e mantieni il server Outpost esistente.

Argomenti

Rinnovo dell'abbonamento

Per rinnovare l'abbonamento e mantenere il server Outpost esistente:

Completa i seguenti passaggi almeno 30 giorni prima della scadenza del contratto per il tuo Outpost:

1. Accedi alla console Centro AWS Support.
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 server 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 server Outpost, verrai convertito automaticamente in un month-to-month abbonamento. Il tuo Outpost 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 reso del server

> **Important**
>
> AWS non è possibile iniziare la procedura di restituzione finché non avrai completato la seguente procedura. Non possiamo interrompere la procedura di reso dopo l'apertura di una richiesta di assistenza per la chiusura dell'abbonamento.

Per chiudere l'abbonamento:

Completa i seguenti passaggi almeno 30 giorni prima della scadenza del contratto per il tuo Outpost:

1. Accedi alla console Centro AWS Support.
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 desideri terminare l'abbonamento.
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. Se necessario, esegui il backup di tutte le istanze e i dati delle istanze presenti sul server.
14. Termina le istanze avviate sul tuo server.
15. Rivedi i dettagli del caso e scegli Invia. Vengono visualizzati il numero di ID caso e il riepilogo.
16. NON spegnete o disconnettete il server dalla rete fino a quando non vi viene richiesto dal supporto tecnico.

Per restituire il AWS Outposts server, segui le procedure riportate in Restituisci un AWS Outposts server.

Converti in month-to-month abbonamento

Per passare a un month-to-month abbonamento e mantenere il server Outpost esistente, non è necessaria alcuna azione. In caso di domande, apri una richiesta di assistenza per la fatturazione.

Il tuo Outpost 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.

Quote per AWS Outposts

Il tuoAccount AWS dispone delle seguenti quote di default per ciascunaServizio AWS. Salvo dove diversamente specificato, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, è possibile richiedere aumenti.

Per visualizzare le quote per AWS Outposts, apri la console Service Quotas. Nel riquadro di navigazione Servizi AWS, scegli e seleziona AWS Outposts.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas.

Di seguito sono riportate le quote dell'Account AWS in relazione a AWS Outposts:

Risorsa	Di default	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 OutpostsAWS.
Outposts per sito	10	Sì	AWS Outpostsinclude risorse hardware e Outposts. Questa quota limita le risorse virtuali dell'Outpost. Puoi avere 10 Outposts in ogni sito Outpost.

AWS Outpostse le quote per altri servizi

AWS Outpostssi basa sulle risorse di altri servizi e tali servizi possono avere le proprie quote predefinite. Ad esempio, la tua quota per le interfacce di rete locali proviene dalla quota Amazon VPC per le interfacce di rete.

Cronologia dei documenti

Nella tabella seguente sono descritte le modifiche importanti apportate alla Guida per l'utente di AWS Outposts .

Modifica	Descrizione	Data
Gestione della capacità	Puoi modificare la configura zione di capacità predefini ta per il tuo nuovo ordine Outposts.	16 aprile 2024
Opzioni nd-of-term E per server AWS Outposts	Al AWS Outposts termine del periodo, puoi rinnovare , terminare o convertire l'abbonamento.	1° agosto 2023
Guida AWS Outposts utente creata per i server Outposts	AWS Outposts La Guida per l'utente è suddivisa in guide separate per rack e server.	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
Presentazione dei server Outpost	Aggiunti i server Outposts, un nuovo fattore di AWS Outposts forma.	30 novembre 2021

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.