



Guida per l'utente

Amazon VPC Lattice



Amazon VPC Lattice: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cos'è Amazon VPC Lattice?	1
Componenti chiave	1
Ruoli e responsabilità	4
Funzionalità	5
Accesso a VPC Lattice	6
Endpoint del servizio VPC Lattice	7
Endpoint IPv4	7
Endpoint dualstack (IPv4 e IPv6)	8
Specificazione degli endpoint	8
Prezzi	8
Come funziona VPC Lattice	10
Reti di servizio	14
Crea una rete di servizi	15
Gestire le associazioni	18
Gestisci le associazioni dei servizi di rete di servizio	18
Gestisci le associazioni di risorse di rete di servizio	19
Gestisci le associazioni VPC della rete di assistenza	20
Gestisci le associazioni di endpoint VPC della rete di assistenza	22
Modifica le impostazioni di accesso	23
Modifica i dettagli del monitoraggio	24
Gestione dei tag	26
Eliminare una rete di servizi	26
Servizi	28
Fase 1: Creare un servizio VPC Lattice	29
Fase 2: Definizione del routing	31
Fase 3: Creare associazioni di rete	32
Fase 4: Revisione e creazione	32
Gestisci le associazioni	32
Modifica le impostazioni di accesso	33
Modifica i dettagli del monitoraggio	35
Gestione dei tag	36
Configura un nome di dominio personalizzato	36
Associa il tuo nome di dominio personalizzato al tuo servizio	38
BYOC	40

Proteggere la chiave privata del certificato	41
Eliminazione di un servizio	42
Gruppi di destinazione	43
Creazione di un gruppo target	44
Creazione di un gruppo target	44
Sottoreti condivise	47
Registrazione di destinazioni	47
ID istanza	48
Indirizzi IP	49
Funzioni Lambda	49
Application Load Balancer	50
Configura i controlli sanitari	50
Impostazioni del controllo dello stato	51
Controllo dello stato delle destinazioni	53
Modifica le impostazioni del controllo sanitario	54
Configurazione dell'instradamento	54
Algoritmo di instradamento	55
Target type (Tipo di destinazione)	55
Tipo di indirizzo IP	57
Obiettivi HTTP	57
x-forwarded headers	57
Intestazioni relative all'identità del chiamante	58
Funzioni Lambda come destinazioni	59
Preparazione della funzione Lambda	60
Creazione di un gruppo di destinazioni per la funzione Lambda	49
Ricevi eventi dal servizio VPC Lattice	61
Rispondi al servizio VPC Lattice	64
Multi-value intestazioni	65
Multi-value parametri della stringa di interrogazione	66
Annullamento della registrazione della funzione Lambda	66
Application Load Balancer come destinazioni	67
Prerequisiti	67
Fase 1: Creare un gruppo target di tipo ALB	68
Fase 2: Registrare l'Application Load Balancer come destinazione	68
Versione del protocollo	69
Aggiornamento dei tag	70

Eliminazione di un gruppo target	71
Listener	73
Configurazione dei listener	73
Listener HTTP	74
Prerequisiti	74
Aggiunta di un ascoltatore HTTP	74
Listener HTTPS	76
Policy di sicurezza	76
Politica ALPN	77
Aggiunta di un ascoltatore HTTPS	78
Ascoltatori TLS	79
Considerazioni	80
Aggiungi un listener TLS	81
Regole dei listener	82
Regole predefinite	82
Priorità delle regole	82
Operazione delle regole	82
Condizioni della regola	83
Aggiungere una regola	84
Aggiorna una regola	85
Eliminare una regola	85
Eliminazione di un listener	86
Risorse VPC	87
Gateway per le risorse	87
Considerazioni	88
Gruppi di sicurezza	89
Tipi di indirizzi IP	89
Indirizzi IPv4 per ENI	90
Risoluzione DNS di Resource Config	90
Creazione di un gateway per le risorse	91
Eliminare un gateway di risorse	91
Configurazioni delle risorse	92
Tipi di configurazioni delle risorse	93
Protocollo	94
Gateway per le risorse	87
Nomi di dominio personalizzati per i provider di risorse	94

Nomi di dominio personalizzati per consumatori di risorse	95
Nomi di dominio personalizzati per i proprietari di reti di servizi	97
Definizione della risorsa	97
Intervalli di porte	97
Accesso alle risorse	98
Associazione con il tipo di rete di servizi	98
Tipi di reti di servizio	99
Condivisione delle configurazioni delle risorse tramite AWS RAM	99
Monitoraggio	100
Crea e verifica un dominio	100
Crea una configurazione delle risorse	103
Gestisci le associazioni	105
Condividi entità VPC Lattice	108
Prerequisiti	108
Condividi entità	109
Interrompi la condivisione di entità	110
Responsabilità e autorizzazioni	110
Proprietari delle entità	111
Consumatori dell'entità	112
Eventi multi-account	113
Lattice VPC per Oracle Database@AWS	117
Considerazioni	117
Backup gestito dell'infrastruttura Oracle Cloud (OCI) su Amazon S3	119
Accesso ad Amazon S3	120
Considerazioni	120
Abilita l'integrazione gestita di Amazon S3 Access	120
Accesso sicuro con una politica di autenticazione	120
Zero-ETL per Amazon Redshift	121
Considerazioni	121
Accedi e condividi entità VPC Lattice	122
Accedi ai servizi e alle risorse VPC Lattice	122
Condividi la tua rete ODB tramite VPC Lattice	122
Sicurezza	124
Gestisci l'accesso ai servizi	125
Politiche di autenticazione	126
Gruppi di sicurezza	143

Liste di controllo accessi (ACL) di rete	148
Richieste autenticate	150
Protezione dei dati	169
Crittografia dei dati in transito	169
Crittografia dei dati a riposo	169
Gestione dell'identità e degli accessi	176
Come funziona Amazon VPC Lattice con IAM	176
Autorizzazioni API	182
Identity-based politiche	185
Uso di ruoli collegati ai servizi	191
AWS politiche gestite	193
Convalida della conformità	196
Accedi in modo privato alle API Lattice	197
Considerazioni sugli endpoint VPC di interfaccia	197
Creazione di un endpoint VPC di interfaccia per VPC Lattice	197
Resilienza	198
Sicurezza dell'infrastruttura	198
Monitoraggio	199
CloudWatch metriche	199
Visualizza i CloudWatch parametri di Amazon	199
Metriche del gruppo target	200
Parametri del servizio	213
Log di accesso	215
Autorizzazioni IAM necessarie per abilitare i log di accesso	216
Accedi alle destinazioni dei log	217
Abilitare log di accesso	219
Richiedi il tracciamento	220
Accedere al contenuto del registro	221
Contenuto del registro di accesso alle risorse	227
Risolvi i problemi relativi ai log di accesso	229
CloudTrail registri	230
Eventi di gestione VPC Lattice in CloudTrail	231
Esempi di eventi VPC Lattice	231
Quote	235
Cronologia dei documenti	242
.....	ccxlv

Cos'è Amazon VPC Lattice?

Amazon VPC Lattice è un servizio di rete di applicazioni completamente gestito che usi per connettere, proteggere e monitorare i servizi e le risorse per la tua applicazione. Puoi utilizzare VPC Lattice con un singolo cloud privato virtuale (VPC) o su più VPC da uno o più account.

Le applicazioni moderne possono essere costituite da più componenti piccoli e modulari, spesso chiamati microservizi, come un'API HTTP, risorse come database e risorse personalizzate costituite da endpoint DNS e indirizzi IP. Sebbene la modernizzazione abbia i suoi vantaggi, può anche introdurre complessità e sfide di rete quando si connettono questi microservizi e risorse. Ad esempio, se gli sviluppatori sono distribuiti in diversi team, potrebbero creare e distribuire microservizi e risorse su più account o VPC.

In VPC Lattice, ci riferiamo a un microservizio come a un servizio e rappresentiamo una risorsa solo come configurazione di risorse. Questi sono i termini che vedi e che utilizzerai nella guida per l'utente di VPC Lattice.

Indice

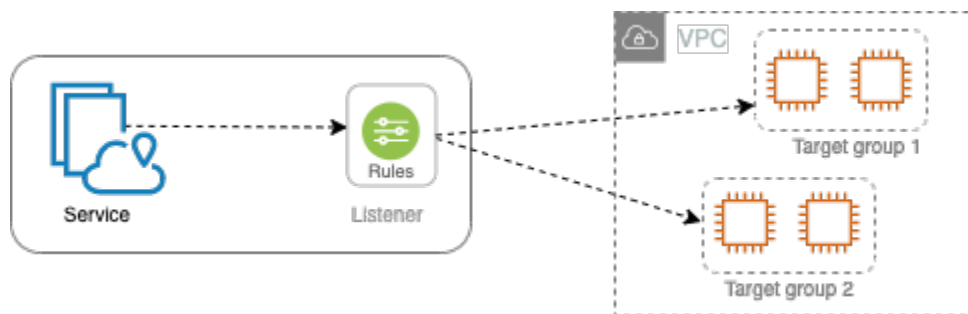
- [Componenti chiave](#)
- [Ruoli e responsabilità](#)
- [Funzionalità](#)
- [Accesso a VPC Lattice](#)
- [Endpoint del servizio VPC Lattice](#)
- [Prezzi](#)

Componenti chiave

Per utilizzare Amazon VPC Lattice, è necessario conoscere i suoi componenti chiave.

Servizio

Un'unità software distribuibile in modo indipendente che svolge un'attività o una funzione specifica. Un servizio può essere eseguito su istanze o ECS/EKS/Fargate contenitori EC2 o come funzioni Lambda, all'interno di un account o di un cloud privato virtuale (VPC). Un servizio VPC Lattice ha i seguenti componenti: gruppi target, ascoltatori e regole.



Gruppo di destinazione

Una raccolta di risorse, note anche come destinazioni, che eseguono l'applicazione o il servizio. Questi sono simili ai gruppi target forniti da Elastic Load Balancing, ma non sono intercambiabili. I tipi di destinazione supportati includono istanze EC2, indirizzi IP, funzioni Lambda, Application Load Balancer, attività Amazon ECS e Kubernetes Pods.

Ascoltatore

Un processo che verifica le richieste di connessione e le indirizza verso le destinazioni di un gruppo di destinazione. Si configura un listener con un protocollo e un numero di porta.

Regola

Un componente predefinito di un listener che inoltra le richieste alle destinazioni in un gruppo di target VPC Lattice. Ogni regola consiste in una priorità, una o più operazioni e una o più condizioni. Le regole determinano il modo in cui il listener indirizza le richieste dei client.

Risorsa

Una risorsa è un'entità come un database Amazon Relational Database Service (Amazon RDS), un'istanza Amazon EC2, un endpoint dell'applicazione, una destinazione del nome di dominio o un indirizzo IP. Puoi condividere una risorsa nel tuo VPC creando una condivisione di risorse in AWS Resource Access Manager (AWS RAM), creando un gateway di risorse e definendo una configurazione delle risorse.

Gateway per le risorse

Un gateway di risorse è un punto di ingresso nel VPC in cui risiedono le risorse.

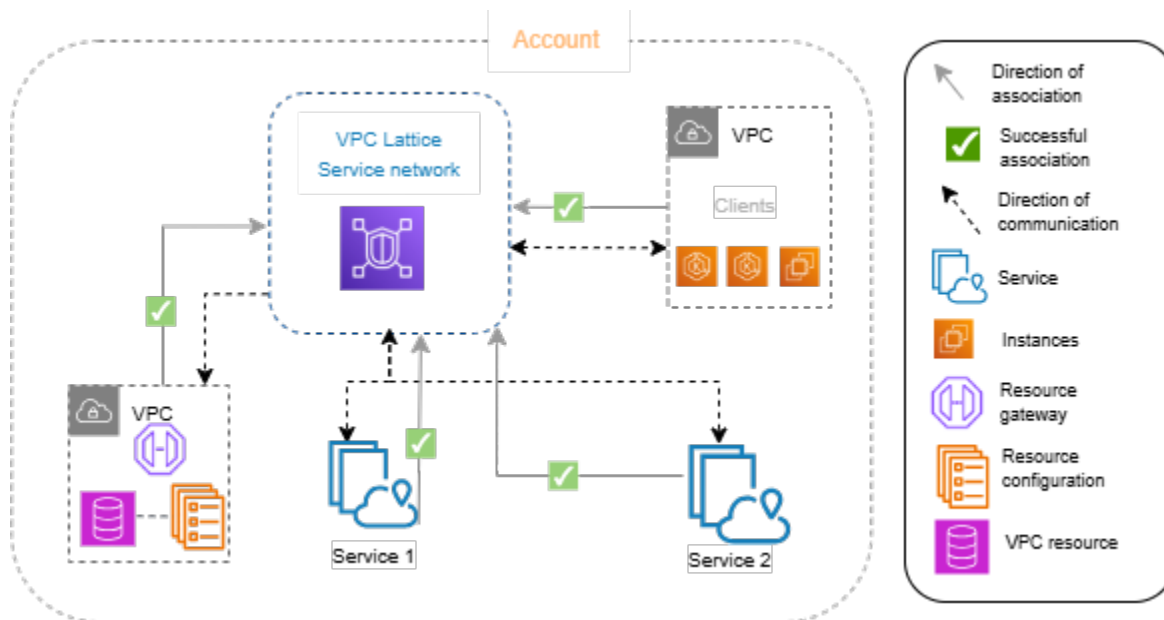
Configurazione delle risorse

Una configurazione delle risorse è un oggetto logico che rappresenta una singola risorsa o un gruppo di risorse. Una risorsa può essere un indirizzo IP, una destinazione con nome di dominio o un database Amazon RDS.

Rete di assistenza

Un limite logico per una raccolta di servizi e configurazioni di risorse. Un client può trovarsi in un VPC associato alla rete di servizi. I client e i servizi associati alla stessa rete di servizi possono comunicare tra loro se sono autorizzati a farlo.

Nella figura seguente, i client possono comunicare con entrambi i servizi, poiché il VPC e i servizi sono associati alla stessa rete di servizi.



Elenco dei servizi

Un registro centrale di tutti i servizi VPC Lattice che possiedi o tramite cui condividi il tuo account. AWS RAM

Politiche di autenticazione

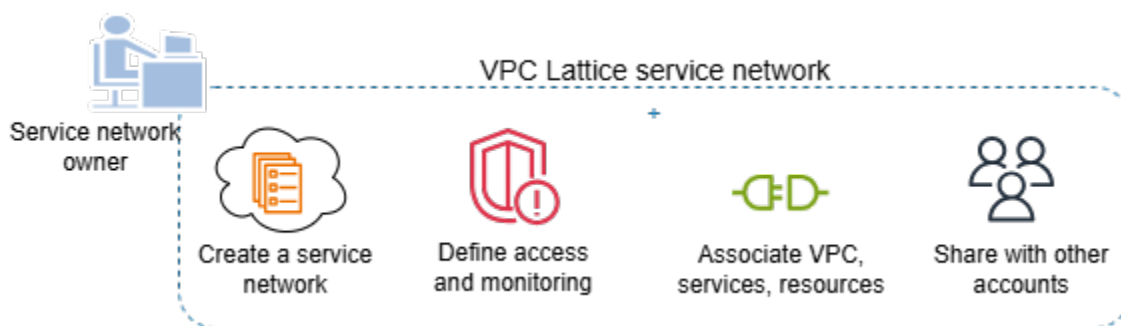
Fine-grained politiche di autorizzazione che possono essere utilizzate per definire l'accesso ai servizi. È possibile allegare politiche di autenticazione separate ai singoli servizi o alla rete di servizi. Ad esempio, puoi creare una policy che stabilisca come un servizio di pagamento in esecuzione su un gruppo di istanze EC2 con scalabilità automatica debba interagire con un servizio di fatturazione in esecuzione. AWS Lambda

Auth-policies non sono supportati nelle configurazioni delle risorse. Le politiche di autenticazione di una rete di servizi non sono applicabili alle configurazioni delle risorse nella rete di servizi.

Ruoli e responsabilità

Un ruolo determina chi è responsabile della configurazione e del flusso di informazioni all'interno di Amazon VPC Lattice. In genere esistono due ruoli, proprietario della rete di servizio e proprietario del servizio, e le loro responsabilità possono sovrapporsi.

Proprietario della rete di servizi: il proprietario della rete di servizi è in genere l'amministratore di rete o l'amministratore del cloud di un'organizzazione. I proprietari della rete di assistenza creano, condividono e forniscono la rete di servizi. Gestiscono anche chi può accedere alla rete di servizi o ai servizi all'interno di VPC Lattice. Il proprietario della rete di servizi può definire impostazioni di accesso granulari per i servizi associati alla rete di servizi. Questi controlli vengono utilizzati per gestire la comunicazione tra client e servizi utilizzando politiche di autenticazione e autorizzazione. Il proprietario della rete di servizi può anche associare una configurazione di servizi o risorse a una o più reti di servizi, se la configurazione del servizio o della risorsa è condivisa con l'account del proprietario della rete di servizio.

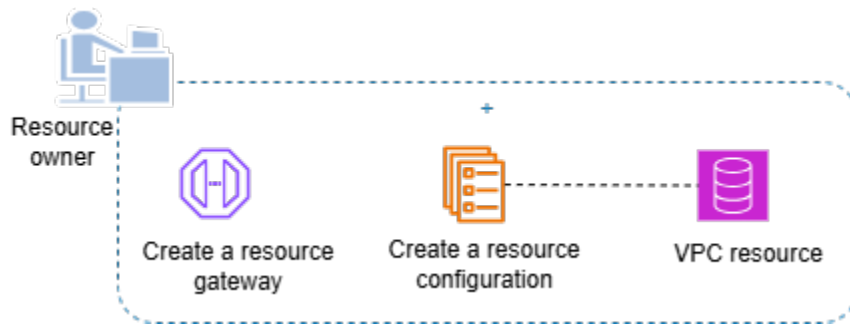


Proprietario del servizio: il proprietario del servizio è in genere uno sviluppatore di software in un'organizzazione. I proprietari dei servizi creano servizi all'interno di VPC Lattice, definiscono le regole di routing e associano i servizi alla rete di servizi. Possono anche definire impostazioni di accesso granulari, che possono limitare l'accesso solo a servizi e client autenticati e autorizzati.



Proprietario della risorsa: il proprietario della risorsa è in genere uno sviluppatore di software in un'organizzazione e funge da amministratore per una risorsa come un database. Il proprietario della

risorsa crea una configurazione delle risorse per la risorsa, definisce le impostazioni di accesso per la configurazione della risorsa e associa la configurazione delle risorse alle reti di servizi.



Funzionalità

Di seguito sono riportate le funzionalità principali fornite da VPC Lattice.

Individuazione dei servizi

Tutti i client e i servizi in VPC associati alla rete di servizi possono comunicare con altri servizi all'interno della stessa rete di servizi. Il DNS indirizza il traffico da client a servizio e da servizio a servizio attraverso l'endpoint VPC Lattice. Quando un client desidera inviare una richiesta a un servizio, utilizza il nome DNS del servizio. Il Route 53 Resolver invia il traffico a VPC Lattice, che quindi identifica il servizio di destinazione.

Connettività

Client-to-service e la connettività client-risorsa viene stabilita all'interno dell'infrastruttura di rete. AWS Quando si associa un VPC alla rete di servizi, qualsiasi client all'interno del VPC può connettersi ai servizi e alle risorse (tramite configurazioni delle risorse) nella rete di servizi, se dispone dell'accesso richiesto. VPC Lattice supporta la tecnologia CIDR sovrapposta.

Accesso in sede

È possibile abilitare la connettività a una rete di servizi da un VPC utilizzando un endpoint VPC (con tecnologia). AWS PrivateLink Un endpoint VPC di tipo service network consente di abilitare l'accesso ai servizi e alle risorse della rete di servizi da reti locali tramite Direct Connect e VPN. Traffico che attraversa il peering VPC o AWS Transit Gateway può anche accedere a risorse e servizi tramite un endpoint VPC.

Osservabilità

VPC Lattice genera metriche e log per ogni richiesta e risposta che attraversa la rete di servizi, per aiutarti a monitorare e risolvere i problemi delle applicazioni. Per impostazione predefinita,

le metriche vengono pubblicate nell'account del proprietario del servizio. I proprietari dei servizi e delle risorse hanno la possibilità di attivare la registrazione e ricevere i log relativi ai servizi e access/requests alle risorse di tutti i client. I proprietari delle reti di servizio possono anche attivare la registrazione sulla rete di servizio, per access/requests registrare tutti i servizi e le risorse dei client nei VPC connessi alla rete di servizi.

VPC Lattice funziona con i seguenti strumenti per aiutarti a monitorare e risolvere i problemi dei tuoi servizi: Amazon CloudWatch gruppi di log, flussi di distribuzione Firehose e bucket Amazon S3.

Sicurezza

VPC Lattice fornisce un framework che puoi utilizzare per implementare una strategia di difesa su più livelli della rete. Il primo livello è la combinazione di servizio, configurazione delle risorse, associazione VPC ed endpoint VPC di tipo rete di servizio. Senza un VPC e un'associazione di servizi o un endpoint VPC di tipo rete di servizi, i client non possono accedere ai servizi. Allo stesso modo, senza un VPC e una configurazione delle risorse e un'associazione di servizi o un endpoint VPC di tipo rete di servizio, i client non possono accedere alle risorse.

Il secondo livello consente agli utenti di collegare gruppi di sicurezza all'associazione tra il VPC e la rete di servizi. Il terzo e il quarto livello sono politiche di autenticazione che possono essere applicate singolarmente a livello di rete di servizio e a livello di servizio.

Affinità della zona di disponibilità

VPC Lattice supporta l'affinità Availability Zone (AZ) per il routing del traffico. Quando un client invia una richiesta a VPC Lattice, VPC Lattice risponde con l'indirizzo IP del servizio o della risorsa dalla stessa AZ del client. Se quella AZ non è disponibile, VPC Lattice risponde con gli indirizzi IP di altre AZ. Da VPC Lattice alla destinazione, il routing è verso le destinazioni, che potrebbero essere distribuite tra AZ. Inoltre, non sono previsti costi di trasferimento dati Inter-AZ in VPC Lattice.

Accesso a VPC Lattice

Puoi creare, accedere e gestire VPC Lattice utilizzando una delle seguenti interfacce:

- **AWS Management Console**— Fornisce un'interfaccia web che è possibile utilizzare per accedere a VPC Lattice.
- **AWS Command Line Interface(AWS CLI)** — Fornisce comandi per un'ampia gamma di AWS servizi, incluso VPC Lattice. AWS CLI È supportato su Windows, macOS e Linux. Per ulteriori

informazioni sulla CLI, vedere. [AWS Command Line Interface](#) Per ulteriori informazioni sulle API, consulta [Amazon VPC Lattice](#) API Reference.

- VPC Lattice Controller per Kubernetes: gestisce le risorse VPC Lattice per un cluster Kubernetes. [Per ulteriori informazioni sull'utilizzo di VPC Lattice con Kubernetes, consulta la Gateway API Controller User Guide. AWS](#)
- CloudFormation— Ti aiuta a modellare e configurare le tue risorse. AWS Per ulteriori informazioni, consulta il riferimento sul tipo di [risorsa Amazon VPC Lattice](#).

Endpoint del servizio VPC Lattice

Un endpoint è un URL che funge da punto di ingresso per un servizio Web. AWS VPC Lattice supporta i seguenti tipi di endpoint:

- [the section called “Endpoint IPv4”](#)
- [Endpoint dualstack](#) (che supportano sia IPv4 sia IPv6)

Quando si effettua una richiesta, è possibile specificare l'endpoint da utilizzare. Se non specifichi un endpoint, per impostazione predefinita viene utilizzato l'endpoint IPv4. Per utilizzare un tipo di endpoint diverso, devi specificarlo nella richiesta. Per esempi su come eseguire questa operazione, consulta [the section called “Specificazione degli endpoint”](#). Per una tabella degli endpoint disponibili, consulta gli endpoint [Amazon VPC Lattice](#).

Endpoint IPv4

Gli endpoint IPv4 supportano solo il traffico IPv4. Gli endpoint IPv4 sono disponibili per tutte le Regioni.

Se specifichi l'endpoint generico, `vpc-lattice.amazonaws.com`, utilizziamo l'endpoint per `us-east-1`. Per utilizzare una Regione diversa, specifica l'endpoint associato. Ad esempio, se specifichi `vpc-lattice.us-east-2.amazonaws.com` come endpoint, indirizzeremo la tua richiesta all'endpoint `us-east-2`.

I nomi degli endpoint IPv4 usano la seguente convenzione di denominazione:

- `vpc-lattice.region.amazonaws.com`

Ad esempio, il nome dell'endpoint IPv4 per la Regione eu-west-1 è `vpc-lattice.eu-west-1.amazonaws.com`.

Endpoint dualstack (IPv4 e IPv6)

Gli endpoint dualstack supportano sia il traffico IPv4 sia il traffico IPv6. Gli endpoint Dualstack sono disponibili per tutte le regioni. Quando si effettua una richiesta a un endpoint dualstack, l'URL dell'endpoint viene risolto in un indirizzo IPv6 o IPv4 a seconda del protocollo utilizzato dalla rete e dal client.

Dual-stack i nomi degli endpoint utilizzano la seguente convenzione di denominazione:

- `vpc-lattice.region.api.aws`

Ad esempio, il nome dell'endpoint dual-stack per la Regione eu-west-1 è `vpc-lattice.eu-west-1.api.aws`.

Specificazione degli endpoint

Gli esempi seguenti mostrano come specificare un endpoint per la us-east-2 regione utilizzando for. AWS CLI `vpc-lattice`

- IPv4

```
aws vpc-lattice get-service --service-identifier svc-0285b53b2eEXAMPLE --region us-east-2 --endpoint-url https://vpc-lattice.us-east-2.amazonaws.com
```

- Dualstack

```
aws vpc-lattice get-service --service-identifier svc-0285b53b2eEXAMPLE --region us-east-2 --endpoint-url https://vpc-lattice.us-east-2.api.aws
```

Prezzi

Con VPC Lattice paghi in base al tempo di fornitura di un servizio, alla quantità di dati trasferiti tramite ciascun servizio e al numero di richieste. In qualità di proprietario di una risorsa, paghi per i dati trasferiti da e verso ogni risorsa. In qualità di proprietario di una rete di servizi, paghi ogni ora per le configurazioni delle risorse associate alla tua rete di servizi. In qualità di consumatore che ha un VPC

associato a una rete di servizi, paghi per i dati trasferiti da e verso le risorse della rete di servizio dal tuo VPC. Per ulteriori informazioni, consulta i prezzi di [Amazon VPC Lattice](#).

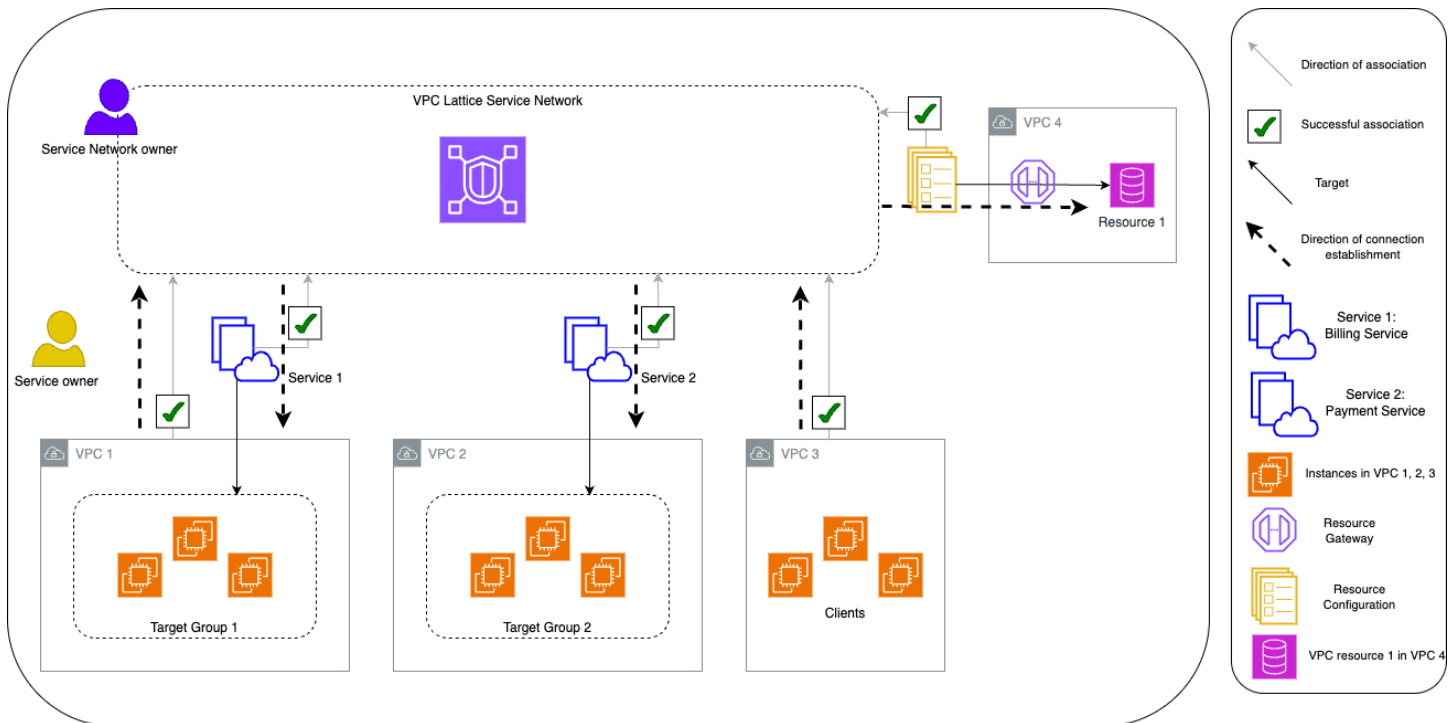
Come funziona VPC Lattice

VPC Lattice è progettato per aiutarti a scoprire, proteggere, connettere e monitorare in modo semplice ed efficace tutti i servizi e le risorse al suo interno. Ogni componente all'interno di VPC Lattice comunica in modo unidirezionale o bidirezionale all'interno della rete di servizi in base alla sua associazione con la rete di servizi e alle sue impostazioni di accesso. Le impostazioni di accesso comprendono le politiche di autenticazione e autorizzazione necessarie per questa comunicazione.

Il seguente riepilogo descrive la comunicazione tra i componenti all'interno di VPC Lattice:

- Esistono due modi in cui un VPC può essere collegato a una rete di servizi: tramite un'associazione VPC e tramite un endpoint VPC di tipo rete di servizio.
- I servizi e le risorse associati alla rete di servizi possono ricevere richieste da client i cui VPC sono anch'essi connessi alla rete di servizi.
- Un client può inviare richieste a servizi e risorse associati a una rete di servizi solo se si trova in un VPC connesso alla stessa rete di servizi. Il traffico client che attraversa una connessione peering VPC, un gateway di transito, Direct Connect o VPN può raggiungere risorse e servizi solo se il VPC è connesso alla rete di servizio tramite un endpoint VPC.
- Gli obiettivi dei servizi nei VPC associati alla rete di servizi sono anche client e possono inviare richieste ad altri servizi e risorse associati alla rete di servizi.
- Gli obiettivi dei servizi nei VPC che non sono associati alla rete di servizi non sono client e non possono inviare richieste ad altri servizi e risorse associati alla rete di servizi.
- I client in VPC che dispongono di risorse ma in cui il VPC non è associato alla rete di servizi non sono client e non possono inviare richieste ad altri servizi e risorse associati alla rete di servizi.

Il seguente diagramma di flusso utilizza uno scenario di esempio per spiegare il flusso di informazioni e la direzione della comunicazione tra i componenti all'interno di VPC Lattice. Esistono due servizi associati a una rete di servizi. Entrambi i servizi e tutti i VPC sono stati creati nello stesso account della rete di servizi. Entrambi i servizi sono configurati per consentire il traffico proveniente dalla rete di servizi.



Il servizio 1 è un'applicazione di fatturazione in esecuzione su un gruppo di istanze registrate con il gruppo target 1 in VPC 1. Service 2 è un'applicazione di pagamento in esecuzione su un gruppo di istanze registrate con il gruppo target 2 in VPC 2. VPC 3 si trova nello stesso account e dispone di client ma non di servizi. La risorsa 1 è un database che contiene i dati dei clienti in VPC 4.

L'elenco seguente descrive, in ordine, il flusso di lavoro tipico delle attività per VPC Lattice.

1. Crea una rete di servizi

Il proprietario della rete di assistenza crea la rete di servizi.

2. Creazione di un servizio

I proprietari del servizio creano i rispettivi servizi, il servizio 1 e il servizio 2. Durante la creazione, il proprietario del servizio aggiunge listener e definisce le regole per l'instradamento delle richieste al gruppo target per ciascun servizio.

3. Definisci il routing

I proprietari del servizio creano il gruppo target per ogni servizio (gruppo target 1 e gruppo target 2). A tale scopo, specificano le istanze di destinazione su cui vengono eseguiti i servizi. Specificano inoltre i VPC in cui risiedono questi obiettivi.

Nel diagramma precedente, le frecce piene rappresentano i servizi che instradano il traffico verso i gruppi target e le configurazioni delle risorse che instradano verso le risorse.

VPC Lattice supporta l'affinità Availability Zone (AZ) per il routing del traffico. Quando un client invia una richiesta a VPC Lattice, VPC Lattice risponde con l'indirizzo IP del servizio o della risorsa dalla stessa AZ del client. Se quella AZ non è disponibile, VPC Lattice risponde con gli indirizzi IP di altre AZ. Da VPC Lattice alla destinazione, il routing è verso le destinazioni, che potrebbero essere distribuite tra AZ. Inoltre, non sono previsti costi di trasferimento dati Inter-AZ in VPC Lattice.

4. Associa i servizi alla rete di assistenza

Il proprietario della rete di assistenza o il proprietario del servizio associa i servizi alla rete di assistenza. Le associazioni sono visualizzate come frecce con segni di spunta che indicano la rete di assistenza dal servizio. Quando si associa un servizio a una rete di servizi, tale servizio diventa rilevabile dagli altri servizi associati alla rete di servizi e dai client nei VPC collegati alla rete di servizi.

Le frecce tratteggiate tra la rete di servizi e i gruppi target mostrano la direzione di creazione della connessione. Il traffico di ritorno viene restituito ai client che utilizzano la rete di servizi. Le frecce che rappresentano il traffico di ritorno non sono incluse in questo diagramma.

5. Creazione di un gateway per le risorse

Il proprietario della risorsa crea un gateway di risorse in VPC 4 per consentire la connettività dai client alla risorsa 1.

6. Creare una configurazione delle risorse

Il proprietario della risorsa crea una configurazione di risorse per rappresentare la risorsa 1 e specifica il gateway di risorse per la risorsa 1.

7. Associa le configurazioni delle risorse alla rete di servizi

Il proprietario della rete di servizio o il proprietario della risorsa associa la configurazione delle risorse alla rete di servizi. L'associazione viene mostrata come una freccia con un segno di spunta che indica la rete di servizi dalla configurazione delle risorse. Quando si associa una configurazione di risorse a una rete di servizi, tale configurazione di risorse diventa rilevabile da altri servizi associati alla rete di servizi e dai client nei VPC collegati alla rete di servizi.

Le frecce tratteggiate dalla rete di servizi alla risorsa rappresentano la risorsa che riceve le richieste dai client. Il traffico di ritorno torna al client utilizzando la rete di servizi. Le frecce che rappresentano il traffico di ritorno non sono incluse in questo diagramma.

8. Connect i VPC con la rete di servizi

I VPC possono essere collegati alla rete di servizio in due modi: associando il VPC alla rete di servizio o creando un endpoint VPC. Qui, il proprietario della rete di assistenza associa VPC 1 e VPC 3 alla rete di servizio. Le associazioni vengono visualizzate mediante frecce con segni di spunta puntati verso la rete di servizi. Con queste associazioni, qualsiasi risorsa nel VPC può fungere da client e può effettuare richieste ai servizi all'interno della rete di servizi. Le frecce tratteggiate tra VPC 1 e la rete di servizi mostrano la direzione di creazione della connessione. La rete di servizi avvia solo connessioni verso le risorse destinate ai gruppi target del servizio 1. Qualsiasi risorsa in VPC 1 può fungere da client e avviare connessioni ai servizi e alle risorse della rete di servizio.

VPC 2 non ha una freccia o un segno di spunta che rappresenti un'associazione. Ciò significa che il proprietario della rete di servizi o il proprietario del servizio non ha associato VPC 2 alla rete di servizio. Questo perché il servizio 2, in questo esempio, deve solo ricevere richieste e inviare risposte utilizzando la stessa richiesta. In altre parole, gli obiettivi del servizio 2 non sono client e non è necessario effettuare richieste ad altri servizi nella rete di servizi.

Allo stesso modo, VPC 4 non ha una freccia o un segno di spunta che rappresenta un'associazione. Ciò significa che il proprietario della rete di servizi o il proprietario della risorsa non ha associato VPC 4 alla rete di servizi. Questo perché la risorsa 1 riceve richieste e invia risposte solo utilizzando la stessa richiesta. Non può effettuare richieste ad altri servizi e risorse nella rete di servizi.

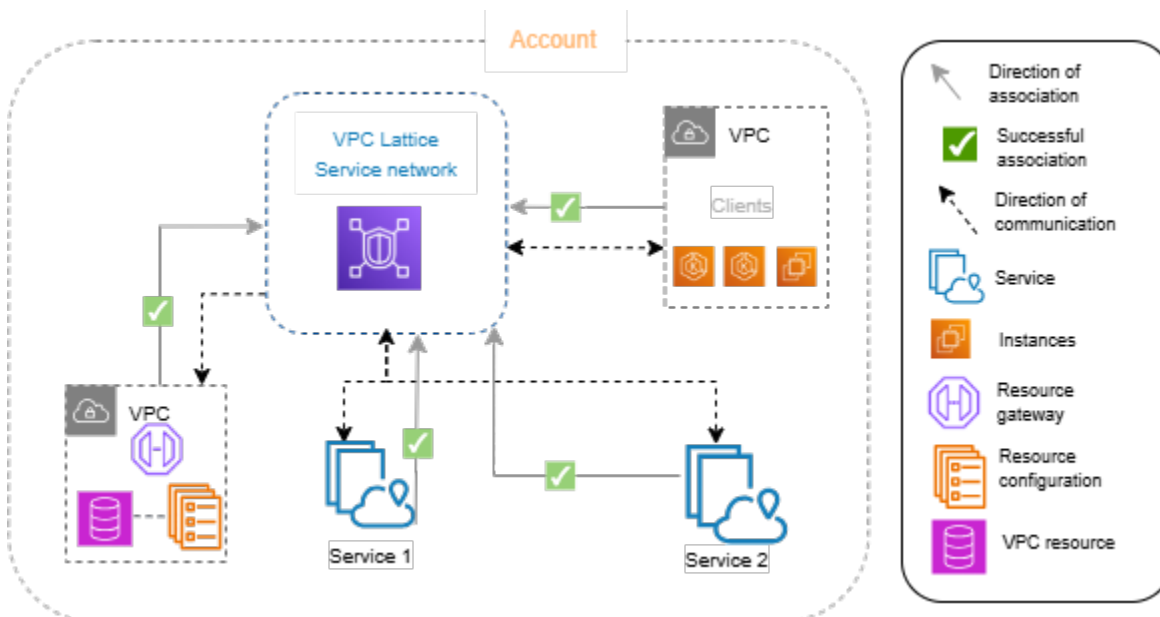
In sintesi, il diagramma precedente mostrava i seguenti scenari:

- VPC con connessioni solo in ingresso da VPC Lattice alle relative risorse. VPC 2 e VPC 4 rappresentano questi scenari.
- Un VPC con connessioni solo in uscita dalle proprie risorse a VPC Lattice. VPC 3 rappresenta questo scenario.
- Un VPC con connessioni in ingresso da VPC Lattice alle relative risorse e con connessioni in uscita dalle proprie risorse a VPC Lattice. VPC 1 rappresenta questo scenario.

Reti di servizio in VPC Lattice

Una rete di servizi è un limite logico per una raccolta di configurazioni di servizi e risorse. Le configurazioni di servizi e risorse associate alla rete possono essere autorizzate per il rilevamento, la connettività, l'accessibilità e l'osservabilità. Per effettuare richieste ai servizi e alle configurazioni delle risorse nella rete, il servizio o il client deve trovarsi in un VPC connesso alla rete di servizi tramite un'associazione o tramite un endpoint VPC.

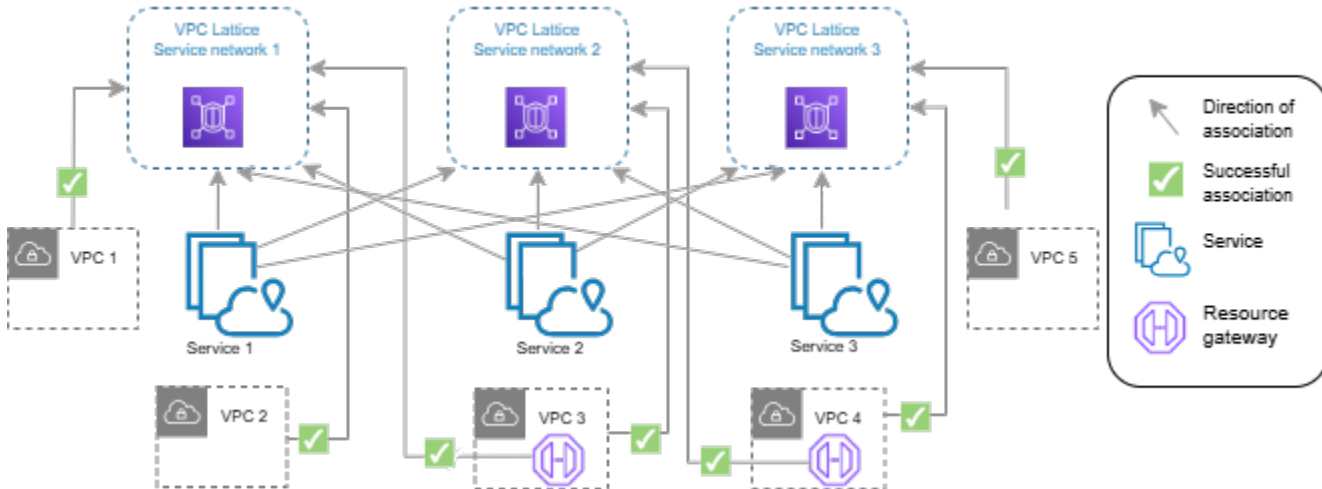
Il diagramma seguente mostra i componenti chiave di una tipica rete di servizi all'interno di Amazon VPC Lattice. I segni di spunta sulle frecce indicano che i servizi e il VPC sono associati alla rete di servizi. I client nel VPC associato alla rete di servizi possono comunicare con entrambi i servizi tramite la rete di servizi.



È possibile associare uno o più servizi e configurazioni di risorse a più reti di servizi. Puoi anche connettere più VPC a una rete di servizi. È possibile connettere un VPC a una sola rete di servizi tramite un'associazione. Per connettere un VPC a più reti di servizi, puoi utilizzare endpoint VPC di tipo service network. [Per ulteriori informazioni sugli endpoint VPC di tipo service network, consulta la guida per l'AWS PrivateLinkutente.](#)

Nel diagramma seguente, le frecce rappresentano le associazioni tra servizi e reti di servizi, nonché le associazioni tra i VPC e le reti di servizi. Puoi vedere che più servizi sono associati a più reti di servizi e più VPC sono associati a ciascuna rete di servizi. Ogni VPC ha esattamente un'associazione a una rete di servizi. VPC 3 e VPC 4 si connettono tuttavia a due reti di servizi. VPC 3 si connette alla

rete di servizi 1 tramite un endpoint VPC. Allo stesso modo, VPC 4 si connette alla rete di servizi 2 tramite un endpoint VPC.



Per ulteriori informazioni, consulta [Quote per Amazon VPC Lattice](#).

Indice

- [Crea una rete di servizi VPC Lattice](#)
- [Gestisci le associazioni per una rete di servizi VPC Lattice](#)
- [Modifica le impostazioni di accesso per una rete di servizi VPC Lattice](#)
- [Modifica i dettagli di monitoraggio per una rete di servizi VPC Lattice](#)
- [Gestisci i tag per una rete di servizi VPC Lattice](#)
- [Eliminare una rete di servizi VPC Lattice](#)

Crea una rete di servizi VPC Lattice

Utilizza la console per creare una rete di servizi e, facoltativamente, configurala con servizi, associazioni, impostazioni di accesso e registri di accesso.

Per creare una rete di servizi utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Scegli Crea rete di servizi.

4. Per Identificatori, inserisci un nome, una descrizione opzionale e tag opzionali. Il nome deve contenere tra 3 e 63 caratteri. È possibile utilizzare lettere minuscole, numeri e trattini. Il nome deve iniziare e terminare con una lettera o un numero. Non utilizzare trattini consecutivi. La descrizione può contenere fino a 256 caratteri. Per aggiungere un tag, scegli Aggiungi nuovo tag e specifica una chiave e un valore per il tag.
5. (Facoltativo) Per associare un servizio, scegliete il servizio da Associazioni di servizi, Servizi. L'elenco include i servizi presenti nel tuo account e tutti i servizi condivisi con te da un altro account. Se non ci sono servizi nell'elenco, puoi creare un servizio scegliendo Crea un servizio VPC Lattice.

In alternativa, per associare un servizio dopo aver creato la rete di servizi, vedi. [the section called “Gestisci le associazioni dei servizi di rete di servizio”](#)

6. (Facoltativo) Per associare una configurazione delle risorse, scegli il servizio di configurazione delle risorse da Associazioni di configurazione delle risorse, Configurazione delle risorse. L'elenco include le configurazioni delle risorse presenti nel tuo account e tutte le configurazioni delle risorse condivise con te da un account diverso. Se non ci sono configurazioni di risorse nell'elenco, puoi creare una configurazione delle risorse scegliendo Crea una configurazione di risorse Amazon VPC Lattice.

In alternativa, per associare una configurazione delle risorse dopo aver creato la rete di servizi, consulta. [the section called “Gestisci le associazioni di risorse di rete di servizio”](#)

7. (Facoltativo) Per associare un VPC, scegli Aggiungi associazione VPC. Seleziona il VPC da associare da VPC e seleziona fino a cinque gruppi di sicurezza dai gruppi di sicurezza. Per creare un gruppo di sicurezza, scegli Crea nuovo gruppo di sicurezza.

In alternativa, puoi saltare questo passaggio e connettere un VPC alla rete di servizio utilizzando un endpoint VPC (fornito da). AWS PrivateLink Per ulteriori informazioni, consulta [Access service networks](#) nella guida per l'utente. AWS PrivateLink

8. Quando si crea una rete di servizi, è necessario decidere se condividere la rete di servizio con altri account o meno. La selezione è immutabile e non può essere modificata dopo aver creato la rete di servizi. Se scegli di consentire la condivisione, la rete di servizi può essere condivisa con altri account tramite. AWS Resource Access Manager

Per [condividere la rete di servizi](#) con altri account, scegli le condivisioni di AWS RAM risorse da Condivisioni di risorse.

Per creare una condivisione di risorse, vai alla AWS RAM console e scegli Crea una condivisione di risorse.

9. Per l'accesso alla rete, puoi lasciare il tipo di autenticazione predefinito, Nessuno, se desideri che i client nei VPC associati accedano ai servizi di questa rete di servizi. Per applicare una [politica di autenticazione](#) per controllare l'accesso ai tuoi servizi, scegli AWSIAM ed esegui una delle seguenti operazioni per la politica di autenticazione:
 - Inserisci una policy nel campo di immissione. Ad esempio politiche che puoi copiare e incollare, scegli Esempi di politiche.
 - Scegli Applica modello di policy e seleziona il modello Consenti accesso autenticato e non autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio firmando la richiesta (ovvero autenticato) o in modo anonimo (ovvero non autenticato).
 - Scegli Applica modello di policy e seleziona il modello Consenti solo l'accesso autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio solo firmando la richiesta (ovvero autenticato).
10. (Facoltativo) Per attivare [i log di accesso](#), selezionate l'interruttore Access logs e specificate una destinazione per i log di accesso come segue:
 - Seleziona Gruppo di CloudWatch log e scegli un gruppo di log. CloudWatch Per creare un gruppo di log, scegli Crea un gruppo di log in CloudWatch.
 - Seleziona il bucket S3 e inserisci il percorso del bucket S3, incluso qualsiasi prefisso. Per cercare nei bucket S3, scegli Browse S3.
 - Seleziona il flusso di distribuzione di Kinesis Data Firehose e scegli un flusso di distribuzione. Per creare un flusso di distribuzione, scegli Crea un flusso di distribuzione in Kinesis.
11. (Facoltativo) Per [condividere la tua rete di servizi](#) con altri account, scegli le condivisioni di AWS RAM risorse da Condivisioni di risorse. Per creare una condivisione di risorse, scegli Crea una condivisione di risorse nella console RAM.
12. Controlla la configurazione nella sezione Riepilogo, quindi scegli Crea rete di servizi.

Per creare una rete di servizi utilizzando ilAWS CLI

Utilizzare il comando [create-service-network](#). Questo comando crea solo la rete di servizi di base. Per creare una rete di servizi completamente funzionante, è necessario utilizzare anche i comandi che creano [associazioni di servizi](#), [associazioni VPC e impostazioni](#) di [accesso](#).

Gestisci le associazioni per una rete di servizi VPC Lattice

Quando si associa un servizio o una configurazione di risorse alla rete di servizi, si consente ai client nei VPC collegati alla rete di servizio di effettuare richieste alla configurazione del servizio e delle risorse. Quando si collega un VPC alla rete di servizi, consente a tutte le destinazioni all'interno di quel VPC di essere client e comunicare con altri servizi e configurazioni di risorse nella rete di servizi.

La proprietà DNS privata abilitata dell'associazione di risorse di rete di servizio ha la precedenza sulla proprietà DNS privata abilitata dell'endpoint della rete di servizio e dell'associazione VPC della rete di servizio.

Se il proprietario di una rete di servizi crea un'associazione di risorse di rete di servizio e non abilita il DNS privato, VPC Lattice non fornirà zone ospitate private per quella configurazione di risorse in nessun VPC a cui è connessa la rete di servizio, anche se il DNS privato è abilitato sull'endpoint della rete di servizio o sulle associazioni VPC della rete di servizio.

Indice

- [Gestisci le associazioni dei servizi di rete di servizio](#)
- [Gestisci le associazioni di risorse di rete di servizio](#)
- [Gestisci le associazioni VPC della rete di assistenza](#)
- [Gestisci le associazioni di endpoint VPC della rete di assistenza](#)

Gestisci le associazioni dei servizi di rete di servizio

Puoi associare servizi che risiedono nel tuo account o servizi condivisi con te da account diversi. Si tratta di un passaggio facoltativo durante la creazione di una rete di servizi. Tuttavia, una rete di assistenza non è completamente funzionante finché non si associa un servizio. I proprietari dei servizi possono associare i propri servizi a una rete di servizi se il loro account dispone dell'accesso richiesto. Per ulteriori informazioni, consulta [Identity-based esempi di policy per VPC Lattice](#).

Quando si elimina un'associazione di servizi, il servizio non può più connettersi ad altri servizi nella rete di servizi.

Per gestire le associazioni di servizi utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.

3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Associazioni di servizio.
5. Per creare un'associazione, procedi come segue:
 - a. Scegliete Crea associazioni.
 - b. Seleziona un servizio da Servizi. Per creare un servizio, scegli Crea un servizio Amazon VPC Lattice.
 - c. (Facoltativo) Per aggiungere un tag, espandi Service Association tags, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
 - d. Scegli Save changes (Salva modifiche).
6. Per eliminare un'associazione, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Elimina associazioni di servizi. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per creare un'associazione di servizi utilizzando ilAWS CLI

Utilizzare il comando [create-service-network-service-association](#).

Per eliminare un'associazione di servizi utilizzandoAWS CLI

Utilizzare il comando [delete-service-network-service-association](#).

Gestisci le associazioni di risorse di rete di servizio

Una configurazione di risorse è un oggetto logico che rappresenta una singola risorsa o un gruppo di risorse. Puoi associare configurazioni di risorse che risiedono nel tuo account o configurazioni di risorse condivise con te da account diversi. Si tratta di un passaggio facoltativo durante la creazione di una rete di servizi. I proprietari della configurazione delle risorse possono associare le proprie configurazioni delle risorse a una rete di servizi se il loro account dispone dell'accesso richiesto. Per ulteriori informazioni, consulta [esempi di Identity-based policy per VPC](#) Lattice.

Gestisci le associazioni tra reti di servizi e configurazioni di risorse

È possibile creare o eliminare l'associazione tra la rete di servizi e la configurazione delle risorse.

Per gestire le associazioni di configurazione delle risorse utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.

2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Reti di servizio.
3. Seleziona il nome della rete di servizi per aprirne la pagina dei dettagli.
4. Scegli la scheda Associazioni di configurazione delle risorse.
5. Per creare un'associazione, procedi come segue:
 - a. Scegliete Crea associazioni.
 - b. Per Configurazioni delle risorse, seleziona una configurazione delle risorse.
 - c. Per il nome DNS, seleziona DNS privato abilitato per consentire a VPC Lattice di fornire una zona ospitata privata per le associazioni di configurazione delle risorse in base al nome di dominio della configurazione della risorsa.
 - d. (Facoltativo) Per aggiungere un tag, espandi Service association tags, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
 - e. Scegli Save changes (Salva modifiche).
6. Per eliminare un'associazione, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Elimina. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per creare un'associazione di configurazione delle risorse utilizzando ilAWS CLI

Utilizzare il comando [create-service-network-resource-association](#).

Per eliminare un'associazione di configurazione di risorse utilizzandoAWS CLI

Utilizzare il comando [delete-service-network-resource-association](#).

Gestisci le associazioni VPC della rete di assistenza

I client possono inviare richieste ai servizi e alle risorse specificati nelle configurazioni delle risorse associate a una rete di servizi se il client si trova in VPC associati alla rete di servizi. Il traffico client che attraversa una connessione peering VPC o un gateway di transito è consentito solo attraverso una rete di servizi che utilizza un endpoint VPC di tipo rete di servizio.

L'associazione di un VPC è un passaggio facoltativo quando si crea una rete di servizi. I proprietari di rete possono associare i VPC a una rete di servizi se il loro account dispone dell'accesso richiesto. Per ulteriori informazioni, consulta [Identity-based esempi di policy per VPC Lattice](#).

Quando si crea un'associazione VPC a una configurazione di risorse, è possibile specificare la preferenza DNS privata. Questa preferenza consente a VPC Lattice di fornire zone ospitate private

per conto del consumatore di risorse. Per ulteriori informazioni, consulta [the section called “Nomi di dominio personalizzati per i provider di risorse”](#).

Quando si elimina un'associazione VPC, i client nei VPC non possono più connettersi ai servizi nella rete di servizi.

Per gestire le associazioni VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Associazioni VPC.
5. Per creare un'associazione VPC, procedi come segue:
 - a. Scegli Crea associazioni VPC.
 - b. Scegli Aggiungi associazione VPC.
 - c. Seleziona un VPC da VPC e seleziona fino a cinque gruppi di sicurezza dai gruppi di sicurezza. Per creare un gruppo di sicurezza, scegli Crea nuovo gruppo di sicurezza.
 - d. (Facoltativo) Per consentire a VPC Lattice di fornire una zona ospitata privata in base al nome di dominio di una configurazione di risorsa, per il nome DNS, seleziona Abilita nome DNS ed esegui quanto segue:
 - i. Per la preferenza DNS privata, seleziona una preferenza.

Se scegli Tutti i domini, VPC Lattice fornisce una zona ospitata privata per qualsiasi nome di dominio personalizzato per una configurazione di risorse.

- ii. (Facoltativo) Se scegli Domini verificati e specificati o Domini specificati, inserisci un elenco separato da virgole di domini per i quali desideri che VPC Lattice esegua il provisioning delle zone ospitate. VPC Lattice effettua il provisioning di una zona ospitata solo se corrisponde al tuo elenco di domini privati. Puoi usare la corrispondenza con i caratteri jolly.
 - e. (Facoltativo) Per aggiungere un tag, espandi i tag di associazione VPC, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
 - f. Scegli Save changes (Salva modifiche).

6. Per modificare i gruppi di sicurezza per un'associazione, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Modifica gruppi di sicurezza. Aggiungi e rimuovi i gruppi di sicurezza secondo necessità.
7. Per eliminare un'associazione, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Elimina associazioni VPC. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per creare un'associazione VPC utilizzando AWS CLI

Utilizzare il comando [create-service-network-vpc-association](#).

Per aggiornare i gruppi di sicurezza per un'associazione VPC utilizzando AWS CLI

Utilizzare il comando [update-service-network-vpc-association](#).

Per eliminare un'associazione VPC utilizzando AWS CLI

Utilizzare il comando [delete-service-network-vpc-association](#).

Gestisci le associazioni di endpoint VPC della rete di assistenza

I clienti possono inviare richieste a servizi e risorse specificati nelle configurazioni delle risorse su un endpoint VPC (con tecnologia AWS PrivateLink) nel proprio VPC. Un endpoint VPC di tipo service network collega un VPC a una rete di servizi. Il traffico client proveniente dall'esterno del VPC tramite una connessione peering VPC, Transit Gateway, Direct Connect o VPN può utilizzare l'endpoint VPC per raggiungere le configurazioni di servizi e risorse. Con gli endpoint VPC, puoi connettere un VPC a più reti di servizi. Quando si crea un endpoint VPC in un VPC, gli indirizzi IP del VPC (e non gli indirizzi IP dell'[elenco dei prefissi gestiti](#)) vengono utilizzati per stabilire la connettività alla rete di servizi.

Quando si crea un'associazione VPC a una configurazione di risorse, è possibile specificare la preferenza DNS privata. Questa preferenza consente a VPC Lattice di fornire zone ospitate private per conto del consumatore di risorse. Per ulteriori informazioni, consulta [the section called “Nomi di dominio personalizzati per i provider di risorse”](#).

Per gestire le associazioni degli endpoint VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.

3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Associazioni endpoint per visualizzare gli endpoint VPC collegati alla tua rete di servizi.
5. Seleziona l'ID endpoint dell'endpoint VPC per aprire la relativa pagina dei dettagli. Quindi modifica o elimina l'associazione degli endpoint VPC.

Per creare una nuova associazione di endpoint VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Endpoints.
3. Scegli Crea endpoint.
4. Per Tipo, scegli Reti di servizio.
5. Seleziona la rete di servizi che desideri connettere al tuo VPC.
6. Seleziona il VPC, le sottoreti e i gruppi di sicurezza.
7. (Facoltativo) Per abilitare il DNS privato, scegli Abilita DNS privato.
8. (Facoltativo) Per aggiungere un tag, espandi i tag di associazione VPC, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
9. Seleziona Crea endpoint.

Per saperne di più sugli endpoint VPC e su come connettersi alle reti di servizi, consulta [Access service networks](#) nella guida per l'AWS PrivateLinkutente.

Modifica le impostazioni di accesso per una rete di servizi VPC Lattice

Le impostazioni di accesso consentono di configurare e gestire l'accesso dei client a una rete di servizi. Le impostazioni di accesso includono il tipo di autenticazione e i criteri di autenticazione. Le politiche di autenticazione ti aiutano ad autenticare e autorizzare il traffico che fluisce verso i servizi all'interno di VPC Lattice. Le impostazioni di accesso della rete di servizio non si applicano alle configurazioni delle risorse associate alla rete di servizio.

È possibile applicare i criteri di autenticazione a livello di rete di servizio, a livello di servizio o entrambi. In genere, le politiche di autenticazione vengono applicate dai proprietari della rete o dagli amministratori del cloud. Possono implementare autorizzazioni generiche, ad esempio, consentire

chiamate autenticate dall'interno dell'organizzazione o consentire richieste GET anonime che soddisfano una determinata condizione. A livello di servizio, i proprietari dei servizi possono applicare controlli granulari, che possono essere più restrittivi. Per ulteriori informazioni, consulta [Controlla l'accesso ai servizi VPC Lattice utilizzando le policy di autenticazione](#).

Per aggiungere o aggiornare le politiche di accesso utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Accesso per verificare le impostazioni di accesso correnti.
5. Per aggiornare le impostazioni di accesso, scegli Modifica impostazioni di accesso.
6. Se desideri che i client nei VPC associati accedano ai servizi di questa rete di servizi, scegli Nessuno come tipo di autenticazione.
7. Per applicare una politica delle risorse alla rete di servizi, scegli AWSIAM per il tipo di autenticazione ed esegui una delle seguenti operazioni per la politica di autenticazione:
 - Inserisci una politica nel campo di immissione. Ad esempio politiche che puoi copiare e incollare, scegli Esempi di politiche.
 - Scegli Applica modello di policy e seleziona il modello Consenti accesso autenticato e non autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio firmando la richiesta (ovvero autenticato) o in modo anonimo (ovvero non autenticato).
 - Scegli Applica modello di policy e seleziona il modello Consenti solo l'accesso autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio solo firmando la richiesta (ovvero autenticato).
8. Scegli Save changes (Salva modifiche).

Per aggiungere o aggiornare una politica di accesso utilizzando ilAWS CLI

Utilizzate il comando [put-auth-policy](#).

Modifica i dettagli di monitoraggio per una rete di servizi VPC Lattice

VPC Lattice genera metriche e log per ogni richiesta e risposta, rendendo più efficiente il monitoraggio e la risoluzione dei problemi delle applicazioni.

È possibile abilitare i log di accesso e specificare la risorsa di destinazione per i log. VPC Lattice può inviare i log alle seguenti risorse: CloudWatch gruppi di log, flussi di distribuzione Firehose e bucket S3.

Per abilitare i log di accesso o aggiornare una destinazione di log utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Monitoraggio. Controlla i registri di accesso per vedere se i registri di accesso sono abilitati.
5. Per abilitare o disabilitare i registri di accesso, scegli Modifica registri di accesso, quindi attiva o disattiva l'interruttore dei registri di accesso.
6. Quando abiliti i log di accesso, devi selezionare il tipo di destinazione di consegna e quindi creare o scegliere la destinazione per i log di accesso. Puoi anche modificare la destinazione di consegna in qualsiasi momento. Esempio:
 - Seleziona Gruppo di CloudWatch log e scegli un gruppo di CloudWatch log. Per creare un gruppo di log, scegli Crea un gruppo di log in CloudWatch.
 - Seleziona il bucket S3 e inserisci il percorso del bucket S3, incluso qualsiasi prefisso. Per cercare nei bucket S3, scegli Browse S3.
 - Seleziona il flusso di distribuzione di Kinesis Data Firehose e scegli un flusso di distribuzione. Per creare un flusso di distribuzione, scegli Crea un flusso di distribuzione in Kinesis.
7. Scegli Save changes (Salva modifiche).

Per abilitare i log di accesso utilizzando ilAWS CLI

Utilizzare il comando [create-access-log-subscription](#).

Per aggiornare la destinazione del registro utilizzando ilAWS CLI

Utilizzare il comando [update-access-log-subscription](#).

Per disabilitare i registri di accesso utilizzandoAWS CLI

Utilizzare il comando [delete-access-log-subscription](#).

Gestisci i tag per una rete di servizi VPC Lattice

I tag consentono di classificare la rete di servizi in diversi modi, ad esempio per scopo, proprietario o ambiente.

È possibile aggiungere più tag a ciascuna rete di servizi. Le chiavi dei tag devono essere univoche per ogni rete di servizi. Se aggiungi un tag con una chiave già associata alla rete del servizio, il valore del tag viene aggiornato. È possibile utilizzare caratteri come lettere, spazi, numeri (in UTF-8) e i seguenti caratteri speciali: + - =. _ : / @. Non utilizzare spazi iniziali o finali. I valori di tag fanno distinzione tra maiuscole e minuscole.

Per aggiungere o eliminare tag utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Selezionare la scheda Tag.
5. Per aggiungere un tag, scegli Aggiungi tag e inserisci la chiave e il valore del tag. Per aggiungere un altro tag, scegli Aggiungi nuovo tag. Una volta completata l'aggiunta di tag, scegli Save changes (Salva modifiche).
6. Per eliminare un tag, seleziona la relativa casella di controllo e scegli Elimina. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per aggiungere o eliminare tag utilizzando ilAWS CLI

Utilizzate i comandi [tag-resource](#) e [untag-resource](#).

Eliminare una rete di servizi VPC Lattice

Prima di poter eliminare una rete di servizi, è necessario eliminare tutte le associazioni che la rete di servizi potrebbe avere con qualsiasi servizio, configurazione di risorse, VPC o endpoint VPC. Quando elimini una rete di servizi, eliminiamo anche tutte le risorse relative alla rete di servizi, come la politica delle risorse, la politica di autenticazione e le sottoscrizioni ai registri di accesso.

Per eliminare una rete di servizi utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.

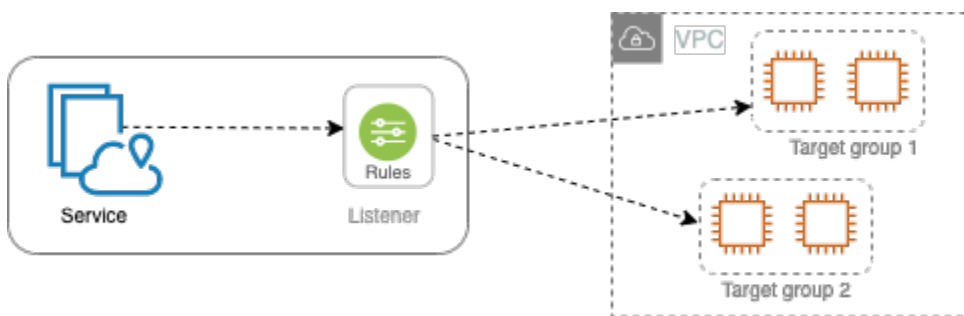
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona la casella di controllo relativa alla rete di servizio, quindi scegli Azioni, Elimina rete di servizi.
4. Quando viene richiesta la conferma, inserisci **confirm** e scegli Delete (Elimina).

Per eliminare una rete di servizi utilizzando ilAWS CLI

Utilizzare il comando [delete-service-network](#).

Servizi in VPC Lattice

Un servizio all'interno di VPC Lattice è un'unità software distribuibile in modo indipendente che fornisce un'attività o una funzione specifica. Un servizio può essere eseguito su istanze, container o come funzioni serverless all'interno di un account o di un cloud privato virtuale (VPC). Un servizio dispone di un listener che utilizza regole, chiamate regole listener, che puoi configurare per indirizzare il traffico verso i tuoi obiettivi. I tipi di destinazione supportati includono istanze EC2, indirizzi IP, funzioni Lambda, Application Load Balancer, attività Amazon ECS e Kubernetes Pods. Per ulteriori informazioni, consulta [Gruppi target in VPC Lattice](#). È possibile associare un servizio a più reti di servizi. Il diagramma seguente mostra i componenti chiave di un servizio tipico all'interno di VPC Lattice.



È possibile creare un servizio assegnandogli un nome e una descrizione. Tuttavia, per controllare e monitorare il traffico verso il servizio, è importante includere le impostazioni di accesso e i dettagli di monitoraggio. Per inviare il traffico dal servizio ai destinatari, è necessario impostare un listener e configurare le regole. Per consentire il flusso del traffico dalla rete di servizi al servizio, è necessario associare il servizio alla rete di servizi.

È previsto un timeout di inattività e un timeout complessivo di connessione per le connessioni alle destinazioni. Il timeout della connessione inattiva è predefinito a 60 secondi ed è regolabile in base al servizio utilizzando il parametro nell'API `idleTimeoutSeconds` [CreateServiceUpdateService](#). Si applica a tutti gli ascoltatori e ai gruppi target di quel servizio. L'intervallo valido è compreso tra 60 e 600 secondi. VPC Lattice chiude la connessione dopo la scadenza del timeout di inattività. La durata massima della connessione è di 10 minuti, dopodiché VPC Lattice smette di accettare nuovi flussi e chiude i flussi esistenti. Questo valore massimo si applica indipendentemente dal valore del timeout di inattività.

Processi

- [Fase 1: Creare un servizio VPC Lattice](#)
- [Fase 2: Definizione del routing](#)

- [Fase 3: Creare associazioni di rete](#)
- [Fase 4: Revisione e creazione](#)
- [Gestisci le associazioni per un servizio VPC Lattice](#)
- [Modifica le impostazioni di accesso per un servizio VPC Lattice](#)
- [Modifica i dettagli di monitoraggio per un servizio VPC Lattice](#)
- [Gestire i tag per un servizio VPC Lattice](#)
- [Configura un nome di dominio personalizzato per il tuo servizio VPC Lattice](#)
- [Porta il tuo certificato \(BYOC\) per VPC Lattice](#)
- [Eliminare un servizio VPC Lattice](#)

Fase 1: Creare un servizio VPC Lattice

Crea un servizio VPC Lattice di base con impostazioni di accesso e dettagli di monitoraggio. Tuttavia, il servizio non è completamente funzionante finché non ne definisci la configurazione di routing e lo associ a una rete di servizi.

Per creare un servizio di base utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Selezionare Create service (Crea servizio).
4. Per gli identificatori, procedi come segue:
 - a. Immettete un nome per il servizio. Il nome deve contenere da 3 a 40 caratteri e utilizzare lettere minuscole, numeri e trattini. Deve iniziare e terminare con una lettera o un numero. Non utilizzare trattini doppi.
 - b. (Facoltativo) Immettere una descrizione per la rete di assistenza. È possibile impostare o modificare la descrizione durante o dopo la creazione. La descrizione può contenere fino a 256 caratteri.
5. Per specificare un nome di dominio personalizzato per il tuo servizio, seleziona Specificare una configurazione di dominio personalizzata e inserisci il nome di dominio personalizzato.

Per i listener HTTPS, puoi selezionare il certificato che VPC Lattice utilizzerà per eseguire la terminazione TLS. Se non si seleziona un certificato ora, è possibile selezionarlo quando si crea un listener HTTPS per il servizio.

Per i listener TCP, è necessario specificare un nome di dominio personalizzato per il servizio. Se si specifica un certificato, questo non viene utilizzato. Invece, esegui la terminazione TLS nella tua applicazione.

6. Per l'accesso al servizio, scegli Nessuno se desideri che i client nei VPC associati alla rete di servizi accedano al tuo servizio. Per applicare una [politica di autenticazione](#) per controllare l'accesso al servizio, scegli AWS IAM. Per applicare una politica delle risorse al servizio, esegui una delle seguenti operazioni per la politica di autenticazione:
 - Inserisci una politica nel campo di immissione. Ad esempio politiche che puoi copiare e incollare, scegli Esempi di politiche.
 - Scegli Applica modello di policy e seleziona il modello Consenti accesso autenticato e non autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio firmando la richiesta (ovvero autenticato) o in modo anonimo (ovvero non autenticato).
 - Scegli Applica modello di policy e seleziona il modello Consenti solo l'accesso autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio solo firmando la richiesta (ovvero autenticato).
7. (Facoltativo) Per abilitare [i log di accesso](#), attiva l'interruttore Access logs e specifica una destinazione per i log di accesso come segue:
 - Seleziona Gruppo di CloudWatch log e scegli un gruppo di log. CloudWatch Per creare un gruppo di log, scegli Crea un gruppo di log in CloudWatch.
 - Seleziona il bucket S3 e inserisci il percorso del bucket S3, incluso qualsiasi prefisso. Per cercare nei bucket S3, scegli Browse S3.
 - Seleziona il flusso di distribuzione di Kinesis Data Firehose e scegli un flusso di distribuzione. Per creare un flusso di distribuzione, scegli Crea un flusso di distribuzione in Kinesis.
8. (Facoltativo) Per [condividere il servizio](#) con altri account, scegli una condivisione di AWS RAM risorse tra Condivisioni di risorse. Per creare una condivisione di risorse, scegli Crea una condivisione di risorse nella console RAM.
9. Per rivedere la configurazione e creare il servizio, scegli Salta per rivedere e creare. Altrimenti, scegli Avanti per definire la configurazione di routing per il tuo servizio.

Note

Per configurare un timeout di inattività personalizzato per il tuo servizio, utilizza la AWS CLI o l'API. Specificate il `idleTimeoutSeconds` parametro quando create o aggiornate

il servizio. L'impostazione predefinita è 60 secondi con un intervallo di 60-600 secondi. Per ulteriori informazioni, consulta [CreateService](#) Amazon VPC Lattice API Reference.

Fase 2: Definizione del routing

Definite la configurazione del routing utilizzando i listener in modo che il servizio possa inviare traffico verso gli obiettivi specificati.

Prerequisito

Prima di poter aggiungere un listener, devi creare un gruppo target VPC Lattice. Per ulteriori informazioni, consulta [the section called "Creazione di un gruppo target"](#).

Per definire il routing per il servizio utilizzando la console

1. Scegli Add listener (Aggiungi listener).
2. Per il nome del listener, puoi fornire un nome di listener personalizzato o utilizzare il protocollo e la porta del listener come nome del listener. Un nome personalizzato che specifichi può contenere fino a 63 caratteri e deve essere univoco per ogni servizio del tuo account. I caratteri validi sono a-z, 0-9 e trattini (-). Non è possibile utilizzare un trattino come primo o ultimo carattere o immediatamente dopo un altro trattino. Non è possibile modificare il nome di un ascoltatore dopo averlo creato.
3. Scegliete un protocollo e inserite un numero di porta.
4. Per Azione predefinita, scegli il gruppo target VPC Lattice per ricevere il traffico e scegli il peso da assegnare a questo gruppo target. Facoltativamente, puoi aggiungere un altro gruppo target per l'azione predefinita. Scegli Aggiungi azione, quindi scegli un altro gruppo target e specificane il peso.
5. (Facoltativo) Per aggiungere un'altra regola, scegli Aggiungi regola, quindi inserisci un nome, una priorità, una condizione e un'azione per la regola.

Puoi assegnare a ciascuna regola un numero di priorità compreso tra 1 e 100. Un listener non può avere più regole con la stessa priorità. Le regole vengono valutate in base all'ordine di priorità, dal valore più basso a quello più alto. La regola predefinita è valutata per ultima.

In Condizione, inserite un modello di percorso per la condizione di corrispondenza del percorso. La dimensione massima di ogni stringa è di 200 caratteri. Il confronto non fa distinzione tra maiuscole e minuscole.

6. (Facoltativo) Per aggiungere tag, espandi i tag Listener, scegli Aggiungi nuovo tag e inserisci una chiave di tag e un valore per il tag.
7. Per rivedere la configurazione e creare il servizio, scegli Salta per rivedere e creare. Altrimenti, scegli Avanti per associare il servizio a una rete di assistenza.

Fase 3: Creare associazioni di rete

Associa il tuo servizio a una rete di servizi in modo che i client possano comunicare con esso.

Per associare un servizio a una rete di servizi utilizzando la console

1. Per le reti di servizi VPC Lattice, seleziona la rete di servizio. Per creare una rete di servizi, scegli Crea una rete VPC Lattice. Puoi associare il tuo servizio a più reti di servizi.
2. (Facoltativo) Per aggiungere un tag, espandi i tag di associazione della rete di servizi, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
3. Scegli Next (Successivo).

Fase 4: Revisione e creazione

Per rivedere la configurazione e creare il servizio utilizzando la console

1. Controlla la configurazione del tuo servizio.
2. Scegli Modifica se devi modificare qualsiasi parte della configurazione del servizio.
3. Al termine della revisione o della modifica della configurazione, scegli il servizio Create VPC Lattice.
4. Se hai specificato un nome di dominio personalizzato per il servizio, devi configurare il routing DNS dopo la creazione del servizio. Per ulteriori informazioni, consulta [the section called "Configura un nome di dominio personalizzato"](#).

Gestisci le associazioni per un servizio VPC Lattice

Quando si associa un servizio alla rete di servizi, si consente ai client (risorse in un VPC associato alla rete di servizi) di effettuare richieste a questo servizio. Puoi associare servizi presenti nel tuo account o servizi condivisi con te da account diversi. Questo passaggio è facoltativo durante la creazione del servizio. Tuttavia, dopo la creazione, il servizio non può comunicare con altri servizi

finché non lo si associa a una rete di servizi. I proprietari dei servizi possono associare i propri servizi alla rete di servizi se il loro account dispone dell'accesso richiesto. Per ulteriori informazioni, consulta [Come funziona VPC Lattice](#).

Per gestire le associazioni delle reti di servizio utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Associazioni di rete di servizio.
5. Per creare un'associazione, procedi come segue:
 - a. Scegliete Crea associazioni.
 - b. Seleziona una rete di servizi dalle reti di servizi VPC Lattice. Per creare una rete di servizi, scegli Crea una rete VPC Lattice.
 - c. (Facoltativo) Per aggiungere un tag, espandi Service Association tags, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
 - d. Scegli Save changes (Salva modifiche).
6. Per eliminare un'associazione, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Elimina associazioni di rete. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per creare un'associazione di rete di servizi utilizzando il AWS CLI

Utilizzare il comando [create-service-network-service-association](#).

Per eliminare un'associazione di rete di servizi utilizzando il AWS CLI

Utilizzare il comando [delete-service-network-service-association](#).

Modifica le impostazioni di accesso per un servizio VPC Lattice

Le impostazioni di accesso consentono di configurare e gestire l'accesso dei client a un servizio. Le impostazioni di accesso includono il tipo di autenticazione e i criteri di autenticazione. Le politiche di autenticazione ti aiutano ad autenticare e autorizzare il traffico che fluisce verso i servizi all'interno di VPC Lattice.

È possibile applicare le politiche di autenticazione a livello di rete di servizio, a livello di servizio o entrambi. A livello di servizio, i proprietari dei servizi possono applicare controlli dettagliati, che possono essere più restrittivi. In genere, le politiche di autenticazione vengono applicate dai proprietari della rete o dagli amministratori del cloud. Possono implementare autorizzazioni dettagliate, ad esempio, consentire chiamate autenticate dall'interno dell'organizzazione o consentire richieste GET anonime che soddisfano una determinata condizione. Per ulteriori informazioni, consulta [Controlla l'accesso ai servizi VPC Lattice utilizzando le policy di autenticazione](#).

Per aggiungere o aggiornare le politiche di accesso utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Accesso per verificare le impostazioni di accesso correnti.
5. Per aggiornare le impostazioni di accesso, scegli Modifica impostazioni di accesso.
6. Se desideri che i client in VPC nella rete di servizi associata accedano al tuo servizio, scegli Nessuno come tipo di autenticazione.
7. Per applicare una politica delle risorse per controllare l'accesso al servizio, scegli AWS IAM per il tipo di autenticazione ed esegui una delle seguenti operazioni per la politica di autenticazione:
 - Inserisci una politica nel campo di immissione. Ad esempio politiche che puoi copiare e incollare, scegli Esempi di politiche.
 - Scegli Applica modello di policy e seleziona il modello Consenti accesso autenticato e non autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio firmando la richiesta (ovvero autenticato) o in modo anonimo (ovvero non autenticato).
 - Scegli Applica modello di policy e seleziona il modello Consenti solo l'accesso autenticato. Questo modello consente a un cliente di un altro account di accedere al servizio solo firmando la richiesta (ovvero autenticato).
8. Scegli Save changes (Salva modifiche).

Per aggiungere o aggiornare una politica di accesso utilizzando il AWS CLI

Utilizzate il comando [put-auth-policy](#).

Modifica i dettagli di monitoraggio per un servizio VPC Lattice

VPC Lattice genera metriche e log per ogni richiesta e risposta, rendendo più efficiente il monitoraggio e la risoluzione dei problemi delle applicazioni.

È possibile abilitare i log di accesso e specificare la risorsa di destinazione per i log. VPC Lattice può inviare i log alle seguenti risorse: CloudWatch gruppi di log, flussi di distribuzione Firehose e bucket S3.

Per abilitare i log di accesso o aggiornare una destinazione di log utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Scegli la scheda Monitoraggio, quindi scegli Registri. Controlla i registri di accesso per vedere se i registri di accesso sono abilitati.
5. Per abilitare o disabilitare i registri di accesso, scegli Modifica registri di accesso, quindi attiva o disattiva l'interruttore dei registri di accesso.
6. Quando abiliti i log di accesso, devi selezionare il tipo di destinazione di consegna e quindi creare o scegliere la destinazione per i log di accesso. Puoi anche modificare la destinazione di consegna in qualsiasi momento. Ad esempio:
 - Seleziona Gruppo di CloudWatch log e scegli un gruppo di CloudWatch log. Per creare un gruppo di log, scegli Crea un gruppo di log in CloudWatch.
 - Seleziona il bucket S3 e inserisci il percorso del bucket S3, incluso qualsiasi prefisso. Per cercare nei bucket S3, scegli Browse S3.
 - Seleziona il flusso di distribuzione di Kinesis Data Firehose e scegli un flusso di distribuzione. Per creare un flusso di distribuzione, scegli Crea un flusso di distribuzione in Kinesis.
7. Scegli Save changes (Salva modifiche).

Per abilitare i log di accesso utilizzando il AWS CLI

Utilizzare il comando [create-access-log-subscription](#).

Per aggiornare la destinazione del registro utilizzando il AWS CLI

Utilizzare il comando [update-access-log-subscription](#).

Per disabilitare i registri di accesso utilizzando il AWS CLI

Utilizzare il comando [delete-access-log-subscription](#).

Gestire i tag per un servizio VPC Lattice

I tag ti aiutano a classificare il servizio in modi diversi, ad esempio in base a scopo, proprietario o ambiente.

Puoi aggiungere più tag a ciascun servizio. Le chiavi dei tag devono essere uniche per ogni servizio. Se aggiungi un tag con una chiave già associata al servizio, il valore di quel tag viene aggiornato. È possibile utilizzare caratteri come lettere, spazi, numeri (in UTF-8) e i seguenti caratteri speciali: + - =. _ : / @. Non utilizzare spazi iniziali o finali. I valori di tag fanno distinzione tra maiuscole e minuscole.

Per aggiungere o eliminare tag utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Selezionare la scheda Tag.
5. Per aggiungere un tag, scegli Aggiungi tag e inserisci la chiave del tag e il valore del tag. Per aggiungere un altro tag, scegli Aggiungi nuovo tag. Una volta completata l'aggiunta di tag, scegli Save changes (Salva modifiche).
6. Per eliminare un tag, seleziona la relativa casella di controllo e scegli Elimina. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per aggiungere o eliminare tag utilizzando il AWS CLI

Utilizzate i comandi [tag-resource](#) e [untag-resource](#).

Configura un nome di dominio personalizzato per il tuo servizio VPC Lattice

Quando si crea un nuovo servizio, VPC Lattice genera un nome di dominio completo (FQDN) univoco per il servizio con la seguente sintassi.

```
service_name-service_id.partition_id.vpc-lattice-svcs.region.on.aws
```

Tuttavia, i nomi di dominio forniti da VPC Lattice non sono facili da ricordare per gli utenti. I nomi di dominio personalizzati sono URL più semplici e più intuitivi per gli utenti. Se preferisci utilizzare un nome di dominio personalizzato per il tuo servizio, ad esempio `www.parking.example.com` al posto del nome DNS generato da VPC Lattice, puoi configurarlo quando crei un servizio VPC Lattice. Quando un client effettua una richiesta utilizzando il nome di dominio personalizzato, il server DNS la risolve nel nome di dominio generato da VPC Lattice.

Prerequisiti

- È necessario disporre di un nome di dominio registrato per il servizio. Se non disponi già di un nome di dominio registrato, puoi registrarne uno tramite Amazon Route 53 o qualsiasi altro registrar commerciale.
- Per ricevere richieste HTTPS, devi fornire il tuo certificato in AWS Certificate Manager. VPC Lattice non supporta un certificato predefinito come fallback. Pertanto, se non fornisci un SSL/TLS certificato corrispondente al tuo nome di dominio personalizzato, tutte le connessioni HTTPS al tuo nome di dominio personalizzato falliranno. Per ulteriori informazioni, consulta [Porta il tuo certificato \(BYOC\) per VPC Lattice](#).

Limitazioni e considerazioni

- Non puoi avere più di un nome di dominio personalizzato per un servizio.
- Non puoi modificare il nome di dominio personalizzato dopo aver creato il servizio.
- Il nome di dominio personalizzato deve essere univoco per una rete di servizi. Ciò significa che non è possibile creare un servizio con un nome di dominio personalizzato già esistente (per un altro servizio) nella stessa rete di servizi.

La procedura seguente mostra come configurare un nome di dominio personalizzato per il servizio.

AWS Management Console

Per configurare un nome di dominio personalizzato per il servizio

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Service.
3. Scegli Crea servizio. Si passa alla Fase 1: Creazione di un servizio.
4. Nella sezione Configurazione personalizzata del dominio, scegli Specificare una configurazione di dominio personalizzata.

5. Inserisci il tuo nome di dominio personalizzato.
6. Per soddisfare le richieste HTTPS, seleziona il SSL/TLS certificato corrispondente al tuo nome di dominio personalizzato in SSL/TLS Certificato personalizzato. Se non disponi ancora di un certificato o non desideri aggiungerne uno ora, puoi aggiungere un certificato quando crei il listener HTTPS. Tuttavia, senza un certificato, il tuo nome di dominio personalizzato non sarà in grado di soddisfare le richieste HTTPS. Per ulteriori informazioni, consulta [Aggiunta di un ascoltatore HTTPS](#).
7. Dopo aver aggiunto tutte le altre informazioni per la creazione del servizio, scegli Crea.

AWS CLI

Per configurare un nome di dominio personalizzato per il tuo servizio

Usa il comando [create-service](#).

```
aws vpc-lattice create-service --name service_name --custom-domain-name your_custom_domain_name --type https --certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Nel comando precedente, per `--name`, inserisci un nome per il tuo servizio.

Per `--custom-domain-name`, inserisci il nome di dominio del tuo servizio, ad esempio, `parking.example.com`. Per `--certificate-arn` inserire l'ARN del certificato in ACM. L'ARN del certificato è disponibile nel tuo account in AWS Certificate Manager

Associa il tuo nome di dominio personalizzato al tuo servizio

Innanzitutto, se non l'hai ancora fatto, registra il tuo nome di dominio personalizzato. La Internet Corporation for Assigned Names and Numbers (ICANN) gestisce i nomi di dominio su Internet. Registra un nome di dominio utilizzando un registrar di nomi di dominio, un' ICANN-accredited organizzazione che gestisce il registro dei nomi di dominio. Il sito Web per il tuo registrar fornirà istruzioni dettagliate e informazioni sui prezzi per la registrazione del tuo nome dominio. Per maggiori informazioni, consulta le seguenti risorse:

- Per utilizzare Amazon Route 53 per registrare un nome di dominio, consulta [Registrazione dei nomi di dominio utilizzando Route 53](#) nella Guida per gli sviluppatori di Amazon Route 53.
- Per un elenco dei registrar accreditati, consulta la [directory dei registrar accreditati](#).

Successivamente, utilizza il tuo servizio DNS, ad esempio il registrar di domini, per creare un record per indirizzare le richieste al tuo servizio. Per ulteriori informazioni, consulta la documentazione per il servizio DNS. In alternativa, puoi utilizzare Route 53 come servizio DNS.

Se utilizzi Route 53, puoi utilizzare un record alias o un record CNAME per indirizzare le query al tuo servizio. Ti consigliamo di utilizzare un record di alias in quanto puoi creare un record di alias nel nodo superiore di uno spazio dei nomi DNS, noto anche come apice della zona.

Se utilizzi Route 53, devi prima creare una zona ospitata, che contenga informazioni su come indirizzare il traffico su Internet per il tuo dominio. Dopo aver creato la zona ospitata privata o pubblica, crea un record in modo che il tuo nome di dominio personalizzato, ad esempio `parking.example.com`, sia mappato al nome di dominio generato automaticamente da VPC Lattice, ad esempio `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`. Senza questa mappatura, il tuo nome di dominio personalizzato non funzionerà in VPC Lattice.

Le seguenti procedure mostrano come creare una zona ospitata privata o pubblica utilizzando Route 53

AWS Management Console

Per creare un record di alias per indirizzare le query al tuo servizio utilizzando Route 53, consulta [Routing del traffico verso l'endpoint del dominio del servizio Amazon VPC Lattice](#).

Usa il nome di dominio generato da VPC Lattice per il tuo servizio, ad esempio **`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`** per Value. Puoi trovare questo nome di dominio generato automaticamente nella console VPC Lattice nella pagina del tuo servizio.

AWS CLI

Per creare un record di alias nella tua zona ospitata

1. Ottieni il nome di dominio generato da VPC Lattice per il tuo servizio (ad esempio,). `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`
2. Per impostare l'alias, usa il seguente comando.

```
aws route53 change-resource-record-sets --hosted-zone-id your-hosted-zone-ID --change-batch file:///~/Desktop/change-set.json
```

Per il `change-set.json` file, create un file JSON con il contenuto del seguente esempio JSON e salvalo sul computer locale. Sostituisci `file:///~/Desktop/change-set.json` il comando precedente con il percorso del file JSON salvato nel computer locale. Nota che «Tipo» nel seguente codice JSON può essere un tipo di record A o AAAA.

```
{
  "Comment": "my-custom-domain-name.com alias",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "my-custom-domain-name.com",
        "Type": "alias-record-type",
        "AliasTarget": {
          "HostedZoneId": "your-hosted-zone-ID",
          "DNSName": "lattice-generated-domain-name",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

Porta il tuo certificato (BYOC) per VPC Lattice

Per soddisfare le richieste HTTPS, è necessario disporre del proprio SSL/TLS certificato pronto in AWS Certificate Manager (ACM) prima di configurare un nome di dominio personalizzato. Questi certificati devono avere un Subject Alternate Name (SAN) o Common Name (CN) che corrisponda al nome di dominio personalizzato del servizio. Se il SAN è presente, controlliamo la corrispondenza solo nell'elenco SAN. Se il SAN è assente, controlliamo la presenza di una corrispondenza nel CN.

VPC Lattice serve le richieste HTTPS utilizzando Server Name Indication (SNI). Il DNS indirizza la richiesta HTTPS al servizio VPC Lattice in base al nome di dominio personalizzato e al certificato che corrisponde a questo nome di dominio. Per richiedere un SSL/TLS certificato per un nome di dominio in ACM o importarne uno in ACM, consulta [Emissione e gestione dei certificati e importazione di certificati](#) nella Guida per l'utente AWS Certificate Manager. Se non puoi richiedere o importare il tuo certificato in ACM, usa il nome di dominio e il certificato generati da VPC Lattice.

VPC Lattice accetta solo un certificato personalizzato per servizio. Tuttavia, puoi utilizzare un certificato personalizzato per più domini personalizzati. Ciò significa che puoi utilizzare lo stesso certificato per tutti i servizi VPC Lattice che crei con un nome di dominio personalizzato.

Per visualizzare il certificato utilizzando la console ACM, apri Certificati e seleziona l'ID del certificato. Dovresti vedere il servizio VPC Lattice associato a quel certificato in Risorsa associata.

Considerazioni e limitazioni

- VPC Lattice consente abbinamenti con caratteri jolly che si trovano a un livello di profondità nel Subject Alternate Name (SAN) o nel Common Name (CN) del certificato associato. Ad esempio, se si crea un servizio con il nome di dominio personalizzato `parking.example.com` e si associa il proprio certificato alla SAN `*.example.com`. Quando arriva una richiesta `parking.example.com`, VPC Lattice abbina la SAN a qualsiasi nome di dominio con il dominio apex `example.com`. Tuttavia, se hai il dominio personalizzato `parking.different.example.com` e il tuo certificato ha la SAN `*.example.com`, la richiesta ha esito negativo.
- VPC Lattice supporta un livello di corrispondenza tra domini con caratteri jolly. Ciò significa che un carattere jolly può essere utilizzato solo come sottodominio di primo livello e che protegge solo un livello di sottodominio. Ad esempio, se la rete SAN del certificato lo è `*.example.com`, allora non `parking.*.example.com` è supportata.
- VPC Lattice supporta un carattere jolly per nome di dominio. Ciò significa che non `*.*.example.com` è valido. Per ulteriori informazioni, consulta [Richiedere un certificato pubblico](#) nella Guida AWS Certificate Manager per l'utente.
- VPC Lattice supporta solo certificati con chiavi RSA a 2048 bit.
- Il SSL/TLS certificato in ACM deve trovarsi nella stessa regione del servizio VPC Lattice a cui lo stai associando.

Proteggere la chiave privata del certificato

Quando richiedi un SSL/TLS certificato utilizzando ACM, ACM genera una public/private key pair. La coppia di chiavi viene generata al momento dell'importazione di un certificato. La chiave di accesso pubblica diventa parte del certificato. Per archiviare in modo sicuro la chiave privata, ACM crea un'altra chiave utilizzando AWS KMS, chiamata chiave KMS, l'alias `aws/acm`. AWS KMS utilizza questa chiave per crittografare la chiave privata del certificato. Per ulteriori informazioni, consulta [Data protection in AWS Certificate Manager](#) nella Guida per l'utente di AWS Certificate Manager.

VPC Lattice utilizza AWS TLS Connection Manager, un servizio accessibile solo a Servizi AWS, per proteggere e utilizzare le chiavi private del certificato. Quando si utilizza il certificato ACM per creare un servizio VPC Lattice, VPC Lattice associa il certificato a TLS Connection Manager. AWS Lo facciamo creando una sovvenzione a fronte della tua chiave gestita. AWS KMS AWS Questa concessione consente di utilizzare AWS KMS TLS Connection Manager per decrittografare la chiave privata del certificato. TLS Connection Manager utilizza il certificato e la chiave privata decrittografata (testo semplice) per stabilire una connessione sicura (SSL/TLS sessione) con i client dei servizi VPC Lattice. Quando il certificato viene dissociato da un servizio VPC Lattice, la concessione viene ritirata. Per ulteriori informazioni, consulta [Grants](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni, consulta [Crittografia dei dati a riposo](#).

Eliminare un servizio VPC Lattice

Per eliminare un servizio VPC Lattice, devi prima eliminare tutte le associazioni che il servizio potrebbe avere con qualsiasi rete di servizi. Se si elimina un servizio, vengono eliminate anche tutte le risorse correlate al servizio, come la politica delle risorse, la politica di autenticazione, i listener, le regole dei listener e le sottoscrizioni ai registri di accesso.

Per eliminare un servizio utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Service.
3. Nella pagina Servizi, seleziona il servizio che desideri eliminare, quindi scegli Azioni, Elimina servizio.
4. Quando viene richiesta la conferma, seleziona Elimina.

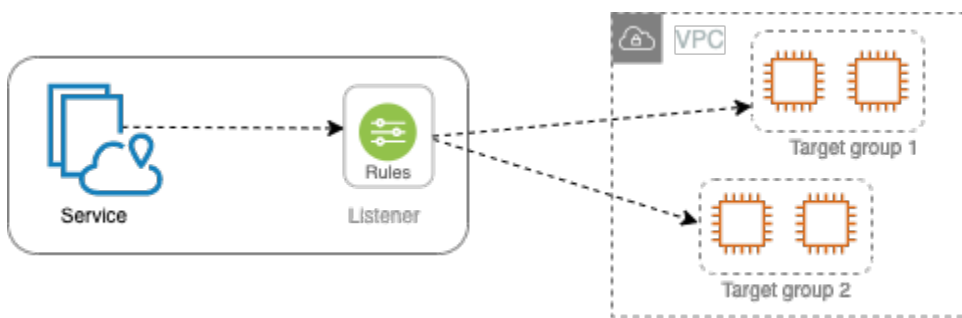
Per eliminare un servizio utilizzando il AWS CLI

Utilizzare il comando [delete-service](#).

Gruppi target in VPC Lattice

Un gruppo target VPC Lattice è una raccolta di obiettivi, o risorse di calcolo, che eseguono l'applicazione o il servizio. I tipi di destinazione supportati includono istanze EC2, indirizzi IP, funzioni Lambda, Application Load Balancer, attività Amazon ECS e Kubernetes Pods. Puoi anche collegare i servizi esistenti ai tuoi gruppi target. [Per ulteriori informazioni sull'utilizzo di Kubernetes con VPC Lattice, consulta la Gateway API Controller User Guide. AWS](#)

Ogni gruppo target viene utilizzato per instradare le richieste a uno o più target registrati. Quando crei una regola listener, specifichi un gruppo target e delle condizioni. Quando una condizione di una regola viene soddisfatta, il traffico viene instradato al gruppo target corrispondente. È possibile creare diversi gruppi target per diversi tipi di richieste. Ad esempio, create un gruppo target per le richieste generali e altri gruppi target per le richieste che includono condizioni di regole specifiche, come un percorso o un valore di intestazione.



Le impostazioni di controllo dello stato del servizio vengono definite in base al gruppo target. Ogni gruppo target utilizza le impostazioni di controllo dello stato predefinite, a meno che non vengano sostituite al momento della creazione del gruppo target o modificate in un secondo momento. Dopo aver specificato un gruppo target in una regola per un listener, il servizio monitora continuamente lo stato di tutti i target registrati con il gruppo target. Il servizio indirizza le richieste verso le destinazioni registrate che sono integre.

Per specificare un gruppo target in una regola per un service listener, il gruppo target deve appartenere allo stesso account del servizio.

I gruppi target VPC Lattice sono simili ai gruppi target forniti da Elastic Load Balancing, ma non sono intercambiabili.

Indice

- [Crea un gruppo target VPC Lattice](#)

- [Registra gli obiettivi con un gruppo target VPC Lattice](#)
- [Controlli sanitari per i gruppi target di VPC Lattice](#)
- [Configurazione dell'instradamento](#)
- [Algoritmo di instradamento](#)
- [Target type \(Tipo di destinazione\)](#)
- [Tipo di indirizzo IP](#)
- [Obiettivi HTTP in VPC Lattice](#)
- [Lambda funge da obiettivi in VPC Lattice](#)
- [Application Load Balancer come obiettivi in VPC Lattice](#)
- [Versione del protocollo](#)
- [Tag per il tuo gruppo target VPC Lattice](#)
- [Eliminare un gruppo target VPC Lattice](#)

Crea un gruppo target VPC Lattice

Puoi registrare le destinazioni con un gruppo di destinazioni. Per impostazione predefinita, il servizio VPC Lattice invia le richieste alle destinazioni registrate utilizzando la porta e il protocollo specificati per il gruppo di destinazione. È possibile sostituire questa porta al momento della registrazione di ogni target con il gruppo target.

Per instradare il traffico verso le destinazioni in un gruppo, specifica il gruppo in un'operazione al momento della creazione di un listener oppure crea una regola per il listener. Per ulteriori informazioni, consulta [Regole di ascolto per il tuo servizio VPC Lattice](#). È possibile specificare lo stesso gruppo target in più listener, ma questi listener devono appartenere allo stesso servizio. Per utilizzare un gruppo target con un servizio, è necessario verificare che il gruppo target non sia utilizzato da un listener per nessun altro servizio.

È possibile aggiungere o rimuovere target dal gruppo target in qualsiasi momento. Per ulteriori informazioni, consulta [Registra gli obiettivi con un gruppo target VPC Lattice](#). È anche possibile modificare le impostazioni di controllo dello stato per il gruppo target. Per ulteriori informazioni, consulta [Controlli sanitari per i gruppi target di VPC Lattice](#).

Creazione di un gruppo target

È possibile creare un gruppo target e, facoltativamente, registrare gli obiettivi come segue.

Per creare un gruppo target tramite la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegliere Crea gruppo target.
4. Per Scegli un tipo di destinazione, esegui una delle seguenti operazioni:
 - Scegli Istanze per registrare le destinazioni in base all'ID dell'istanza.
 - Scegli gli indirizzi IP per registrare le destinazioni in base all'indirizzo IP.
 - Scegli la funzione Lambda per registrare una funzione Lambda come destinazione.
 - Scegliete Application Load Balancer per registrare un Application Load Balancer come destinazione.
5. In Nome gruppo di destinazione, immetti un nome per il gruppo di destinazione. Questo nome deve essere univoco per l'account in ogni AWS regione, può avere un massimo di 32 caratteri, deve contenere solo caratteri alfanumerici o trattini e non deve iniziare o terminare con un trattino.
6. Per Protocol e Port, è possibile modificare i valori predefiniti in base alle esigenze. Il protocollo predefinito è HTTPS e la porta predefinita è 443.

Se il tipo di destinazione è la funzione Lambda, non è possibile specificare un protocollo o una porta.

7. Per il tipo di indirizzo IP, scegli IPv4 per registrare le destinazioni con indirizzi IPv4 o scegli IPv6 per registrare le destinazioni con indirizzi IPv6. Non è possibile modificare questa impostazione dopo la creazione del gruppo target.

Questa opzione è disponibile solo se il tipo di destinazione sono gli indirizzi IP.

8. Per VPC, selezionare un cloud privato virtuale (VPC, Virtual Private Cloud).

Questa opzione non è disponibile se il tipo di destinazione è la funzione Lambda.

9. Per la versione del protocollo, modificate il valore predefinito in base alle esigenze. L'impostazione predefinita è HTTP1.

Questa opzione non è disponibile se il tipo di destinazione è la funzione Lambda.

10. Per i controlli Health, modificare le impostazioni predefinite in base alle esigenze. Per ulteriori informazioni, consulta [Controlli sanitari per i gruppi target di VPC Lattice](#).

I controlli Health non sono disponibili se il tipo di destinazione è la funzione Lambda.

11. Per la versione della struttura degli eventi Lambda, scegli una versione. Per ulteriori informazioni, consulta [the section called “Ricevi eventi dal servizio VPC Lattice”](#).

Questa opzione è disponibile solo se il tipo di destinazione è la funzione Lambda

12. (Facoltativo) Per aggiungere tag, espandi Tag, scegli Aggiungi nuovo tag e inserisci la chiave e il valore del tag.
13. Scegli Next (Successivo).
14. Per Register targets, puoi saltare questo passaggio o aggiungere obiettivi come segue:
 - Se il tipo di destinazione è Istanze, seleziona le istanze, inserisci le porte, quindi scegli Includi come in sospeso di seguito.
 - Se il tipo di destinazione è Indirizzi IP, procedere nel seguente modo:
 - a. Per Scegli una rete, mantieni il VPC selezionato per il gruppo di destinazione o scegli Altro indirizzo IP privato.
 - b. Per Specificare gli IP e definire le porte, inserisci l'indirizzo IP e inserisci le porte. La porta predefinita è la porta del gruppo di destinazione.
 - c. Seleziona Includi come in sospeso di seguito.
 - Se il tipo di destinazione è una funzione Lambda, scegli una funzione Lambda. Per creare una funzione Lambda, scegli Crea una nuova funzione Lambda.
 - Se il tipo di destinazione è un Application Load Balancer, scegli un Application Load Balancer. Per creare un Application Load Balancer, scegli crea un Application Load Balancer.
15. Scegliere Crea gruppo target.

VPC Lattice potrebbe impiegare alcuni minuti per registrare gli obiettivi. Per ulteriori informazioni, consulta, [Perché ci vuole così tanto tempo prima che le mie modifiche DNS si propaghino in Route 53 e nei resolver](#) pubblici?

Per creare un gruppo target utilizzando AWS CLI

Utilizzate il comando [create-target-group](#) per creare il gruppo target e il comando [register-targets](#) per aggiungere obiettivi.

Sottoreti condivise

I partecipanti possono creare gruppi target VPC Lattice in un VPC condiviso. Le seguenti regole si applicano alle sottoreti condivise:

- Tutte le parti di un servizio VPC Lattice, come ascoltatori, gruppi target e destinazioni, devono essere create dallo stesso account. Possono essere creati in sottoreti possedute o condivise con il proprietario del servizio VPC Lattice.
- Le destinazioni registrate con un gruppo target devono essere create dallo stesso account del gruppo target.
- Solo il proprietario di un VPC può associare il VPC a una rete di servizi. Le risorse dei partecipanti in un VPC condiviso associato a una rete di servizi possono inviare richieste ai servizi associati alla rete di servizi. Tuttavia, l'amministratore può evitare che ciò accada utilizzando gruppi di sicurezza, ACL di rete o politiche di autenticazione.

Per ulteriori informazioni sulle risorse condivisibili per VPC Lattice, vedere [Condividi entità VPC Lattice](#)

Registra gli obiettivi con un gruppo target VPC Lattice

Il tuo servizio funge da unico punto di contatto per i clienti e distribuisce il traffico in entrata tra i suoi target registrati validi. È possibile registrare ogni target con uno o più gruppi target.

Se la domanda della tua applicazione aumenta, puoi registrare obiettivi aggiuntivi con uno o più gruppi target per gestire la domanda. Il servizio inizia a indirizzare le richieste a un target appena registrato non appena il processo di registrazione viene completato e il target supera i controlli di integrità iniziali.

Se il carico di richieste per l'applicazione diminuisce o devi eseguire la manutenzione dei target, puoi annullare la loro registrazione dai gruppi target. L'annullamento della registrazione di un target rimuove il target dal gruppo target, ma non influisce in altro modo sul target stesso. Il servizio interrompe l'instradamento delle richieste verso una destinazione non appena viene annullata la registrazione. Il target passa allo stato DRAINING fino a quando non vengono completate le richieste in transito. Puoi registrare di nuovo la destinazione con il gruppo di destinazioni quando è possibile riprendere la ricezione delle richieste.

Il tipo di destinazione del gruppo di destinazioni determina il modo in cui si registrano le destinazioni con quel gruppo di destinazioni. Per ulteriori informazioni, consulta [Target type \(Tipo di destinazione\)](#).

Utilizza le seguenti procedure della console per registrare o annullare la registrazione delle destinazioni. [In alternativa, utilizza i comandi register-targets e deregister-targets di AWS CLI](#)

Indice

- [Registrazione o annullamento della registrazione di destinazioni in base all'ID istanza](#)
- [Registrazione o annullamento della registrazione di destinazioni in base all'indirizzo IP](#)
- [Registrazione o annullamento della registrazione di una funzione Lambda](#)
- [Registrare o annullare la registrazione di un Application Load Balancer](#)

Registrazione o annullamento della registrazione di destinazioni in base all'ID istanza

Le istanze di destinazione devono trovarsi nel cloud privato virtuale (VPC) specificato per il gruppo di destinazione. Quando la registri, l'istanza deve inoltre trovarsi nello stato `running`.

Quando registri le destinazioni in base all'ID dell'istanza, puoi utilizzare il tuo servizio con un gruppo Auto Scaling. Dopo aver associato un gruppo target a un gruppo Auto Scaling e il gruppo si è ridimensionato, le istanze avviate dal gruppo Auto Scaling vengono automaticamente registrate con il gruppo di destinazione. Se distacchi il gruppo di destinazioni dal gruppo con dimensionamento automatico, viene automaticamente annullata la registrazione delle istanze dal gruppo di destinazioni. Per ulteriori informazioni, consulta [Routing del traffico verso il tuo gruppo Auto Scaling con un gruppo target VPC Lattice](#) nella Amazon EC2 Auto Scaling User Guide.

Per registrare le destinazioni o annullarne la registrazione in base all'ID istanza tramite la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Scegliere la scheda Destinazioni.
5. Per registrare le istanze, scegli Registra destinazioni. Seleziona le istanze, inserisci la porta dell'istanza, quindi scegli Includi come in sospeso di seguito. Quando hai finito di aggiungere le istanze, scegli Registra obiettivi.
6. Per annullare la registrazione delle istanze, selezionate le istanze, quindi scegliete Annulla registrazione.

Registrazione o annullamento della registrazione di destinazioni in base all'indirizzo IP

Gli indirizzi IP di destinazione devono provenire dalle sottoreti del VPC specificate per il gruppo di destinazione. Non è possibile registrare gli indirizzi IP di un altro servizio nello stesso VPC. Non puoi registrare endpoint VPC o indirizzi IP instradabili pubblicamente.

Per registrare le destinazioni o annullarne la registrazione in base all'indirizzo IP tramite la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Scegliere la scheda Destinazioni.
5. Per registrare gli indirizzi IP, scegli Registrare destinazioni. Per ogni indirizzo IP, seleziona la rete, inserisci l'indirizzo IP e la porta, quindi scegli Includi come in sospeso di seguito. Quando hai finito di specificare gli indirizzi, scegli Registra obiettivi.
6. Per annullare la registrazione degli indirizzi IP, seleziona gli indirizzi e scegliere Annulla registrazione.

Registrazione o annullamento della registrazione di una funzione Lambda

È possibile registrare una singola funzione Lambda con il gruppo target. Se non hai più bisogno di inviare traffico alla funzione Lambda, puoi annullare la relativa registrazione. Dopo avere annullato la registrazione di una funzione Lambda, le richieste in transito hanno esito negativo con 5XX errori HTTP. È preferibile creare un nuovo gruppo target anziché sostituire la funzione Lambda per un gruppo target.

Per registrare o annullare la registrazione di una funzione Lambda utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Scegliere la scheda Destinazioni.
5. Se non è registrata alcuna funzione Lambda, scegli Registra destinazione. Seleziona la funzione Lambda e scegli Register target.

6. Per annullare la registrazione di una funzione Lambda, scegli Annulla registrazione. Quando viene richiesta la conferma, immettete **confirm** e scegliete Annulla registrazione.

Registrare o annullare la registrazione di un Application Load Balancer

È possibile registrare un singolo Application Load Balancer per ogni gruppo target. Se non è più necessario inviare traffico al sistema di bilanciamento del carico, è possibile annullarne la registrazione. Dopo aver annullato la registrazione di un sistema di bilanciamento del carico, le richieste in corso hanno esito negativo con errori HTTP 5XX. È preferibile creare un nuovo gruppo target anziché sostituire l'Application Load Balancer per un gruppo target.

Per registrare o annullare la registrazione di un Application Load Balancer utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Scegliere la scheda Destinazioni.
5. Se non è registrato alcun Application Load Balancer, scegli Register target. Seleziona Application Load Balancer e scegli Register target.
6. Per annullare la registrazione di un Application Load Balancer, scegli Annulla registrazione. Quando viene richiesta la conferma, inserisci e scegli Annulla registrazione. **confirm**

Controlli sanitari per i gruppi target di VPC Lattice

Il tuo servizio invia periodicamente richieste ai destinatari registrati per verificarne lo stato. Questi test sono chiamati controlli dello stato.

Ogni servizio VPC Lattice indirizza le richieste solo verso gli obiettivi integri. Ogni servizio verifica lo stato di salute di ciascun target, utilizzando le impostazioni di controllo dello stato per i gruppi target con cui il target è registrato. Una volta che un target viene registrato, deve essere sottoposto a un controllo dello stato per essere considerato integro. Al termine di ogni controllo sanitario, il servizio chiude la connessione stabilita per il controllo sanitario.

Limitazioni e considerazioni

- Quando la versione del protocollo del gruppo di destinazione è HTTP1, i controlli di integrità sono abilitati per impostazione predefinita.

- Quando la versione del protocollo del gruppo di destinazione è HTTP2, i controlli sanitari non sono abilitati per impostazione predefinita. Tuttavia, è possibile abilitare i controlli sanitari e impostare manualmente la versione del protocollo su HTTP1 o HTTP2.
- I controlli Health non supportano le versioni del protocollo gRPC per gruppi target. Tuttavia, se si abilitano i controlli sanitari, è necessario specificare la versione del protocollo di controllo dello stato come HTTP1 o HTTP2.
- I controlli Health non supportano i gruppi target Lambda.
- I controlli dello stato di salute non supportano i gruppi target di Application Load Balancer. Tuttavia, puoi abilitare i controlli di integrità per gli obiettivi del tuo Application Load Balancer utilizzando Elastic Load Balancing. Per ulteriori informazioni, consulta [Target group health controls](#) nella User Guide for Application Load Balancers.

Impostazioni del controllo dello stato

È possibile configurare controlli dell'integrità per le destinazioni all'interno di un gruppo di destinazioni come viene descritto nella tabella seguente. I nomi delle impostazioni utilizzati nella tabella sono i nomi usati nell'API. Il servizio invia una richiesta di controllo dello stato di salute a ciascun target registrato ogni `HealthCheckIntervalSeconds`secondo, utilizzando la porta, il protocollo e il percorso ping specificati. Ogni richiesta di controllo dello stato è indipendente e il risultato dura per l'intero intervallo. Il tempo di risposta del target non influenza l'intervallo per la richiesta di controllo dello stato successiva. Se i controlli di integrità superano gli errori `UnhealthyThresholdCount`consecutivi, il servizio mette fuori servizio l'obiettivo. Quando i controlli di integrità superano i successi `HealthyThresholdCount`consecutivi, il servizio rimette l'obiettivo in servizio.

Impostazione	Description
HealthCheckProtocol	Il protocollo utilizzato dal servizio per eseguire i controlli sanitari sugli obiettivi. I protocolli possibili sono HTTP e HTTPS. L'impostazione predefinita è il protocollo HTTP.
HealthCheckPort	La porta utilizzata dal servizio per eseguire i controlli di integrità sugli obiettivi. L'impostazione predefinita prevede l'utilizzo della porta su cui ogni destinazione riceve il traffico dal servizio.

Impostazione	Description
HealthCheckPath	La destinazione dei controlli dell'integrità sulle destinazioni. Se la versione del protocollo è HTTP1 o HTTP2, specifica un URI (/path) valido? (interrogazione). Il valore di default è /.
HealthCheckTimeoutSeconds	Il periodo di tempo, in secondi, durante il quale l'assenza di risposta da un target indica che un controllo dello stato non è riuscito. L'intervallo è compreso tra 1 e 120 secondi. L'impostazione predefinita è 5 secondi se il tipo di destinazione è INSTANCE o IP. Specificare 0 per ripristinare questa impostazione al valore predefinito.
HealthCheckIntervalSeconds	Il periodo di tempo approssimativo, in secondi, tra i controlli dell'integrità di una singola destinazione. L'intervallo è compreso tra 5 e 300 secondi. L'impostazione predefinita è 30 secondi se il tipo di destinazione è INSTANCE o IP. Specificare 0 per ripristinare questa impostazione al valore predefinito.
HealthyThresholdCount	Il numero di controlli sanitari consecutivi che hanno avuto esito positivo prima che un bersaglio non sano venga considerato sano. L'intervallo è compreso tra 2 e 10. Il predefinito è 5. Specificare 0 per ripristinare questa impostazione al valore predefinito.
UnhealthyThresholdCount	Numero di controlli dello stato consecutivi non riusciti necessari prima di considerare una destinazione non integra. L'intervallo è compreso tra 2 e 10. Il valore predefinito è 2. Specificare 0 per ripristinare questa impostazione al valore predefinito.

Impostazione	Description
Matcher	I codici da utilizzare durante la verifica di una risposta con esito positivo ricevuta da una destinazione. Tali codici si chiamano Codici di successo nella console. Se la versione del protocollo è HTTP1 o HTTP2, i valori possibili sono compresi tra 200 e 499. Puoi specificare più valori (ad esempio "200,202") o un intervallo di valori (ad esempio "200-299"). Il valore predefinito è 200. La versione del protocollo Health check per gRPC non è attualmente supportata. Tuttavia, se la versione del protocollo del gruppo target è gRPC, è possibile specificare le versioni del protocollo HTTP1 o HTTP2 nella configurazione del controllo dello stato.

Controllo dello stato delle destinazioni

È possibile controllare lo stato dei target registrato con i gruppi target.

Per controllare lo stato dei target utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella scheda Destinazioni, la colonna Stato di integrità indica lo stato di ogni destinazione. Se lo stato è un valore diverso da `Healthy`, la colonna Health status details contiene ulteriori informazioni.

Per controllare lo stato di salute dei tuoi bersagli, usa il `AWS CLI`

Usa il comando [list-targets](#). L'output di questo comando contiene lo stato del target. Se lo stato è un valore diverso da `Healthy`, il risultato comprende anche un codice di motivo.

Per ricevere notifiche via e-mail su destinazioni non integre

Usa gli CloudWatch allarmi per avviare una funzione Lambda per inviare dettagli su obiettivi non sani.

Modifica le impostazioni del controllo sanitario

Puoi modificare le impostazioni di controllo dello stato per il tuo gruppo di target in qualsiasi momento.

Per modificare le impostazioni del controllo dello stato utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella scheda Health checks, nella sezione Impostazioni Health check, scegli Modifica.
5. Modifica le impostazioni del controllo sanitario in base alle esigenze.
6. Scegli Save changes (Salva modifiche).

Per modificare le impostazioni del controllo sanitario utilizzando ilAWS CLI

Usa il comando [update-target-group](#).

Configurazione dell'instradamento

Per impostazione predefinita, un servizio indirizza le richieste verso le sue destinazioni utilizzando il protocollo e il numero di porta specificati al momento della creazione del gruppo di destinazione. In alternativa, è possibile sostituire la porta utilizzata per l'instradamento del traffico a un target al momento della registrazione con il gruppo target.

I gruppi di destinazioni supportano i seguenti protocolli e porte:

- Protocolli: HTTP, HTTPS, TCP
- Porte: 1-65535

Se un gruppo target è configurato con il protocollo HTTPS o utilizza i controlli di integrità HTTPS, le connessioni TLS alle destinazioni utilizzano la politica di sicurezza del listener. VPC Lattice stabilisce connessioni TLS con le destinazioni utilizzando i certificati che installi sulle destinazioni. VPC Lattice

non convalida questi certificati. Pertanto, è possibile utilizzare certificati autofirmati o certificati scaduti. Il traffico tra VPC Lattice e le destinazioni è autenticato a livello di pacchetto, quindi non è a rischio di attacchi o spoofing man-in-the-middle anche se i certificati sugli obiettivi non sono validi.

[I gruppi target TCP sono supportati solo con listener TLS.](#)

Algoritmo di instradamento

Per impostazione predefinita, l'algoritmo di routing round robin viene utilizzato per indirizzare le richieste verso obiettivi sani.

Quando il servizio VPC Lattice riceve una richiesta, utilizza il seguente processo:

1. Valuta le regole del listener in ordine di priorità per determinare quale regola applicare.
2. Seleziona un bersaglio dal gruppo target per l'azione della regola, utilizzando l'algoritmo round robin predefinito. L'instradamento avviene in maniera indipendente per ogni gruppo di destinazioni, anche nel caso in cui una destinazione sia registrata con più gruppi.

Se un gruppo target contiene solo obiettivi non integri, le richieste vengono indirizzate a tutte le destinazioni, indipendentemente dal loro stato di salute. Ciò significa che se tutti gli obiettivi non superano i controlli di integrità contemporaneamente, il servizio VPC Lattice non si apre. L'effetto del fail-open è quello di consentire il traffico verso tutti gli obiettivi, indipendentemente dal loro stato di salute, sulla base dell'algoritmo round robin.

VPC Lattice supporta l'affinità Availability Zone (AZ) per il routing del traffico. Quando un client invia una richiesta a VPC Lattice, VPC Lattice risponde con l'indirizzo IP del servizio o della risorsa dalla stessa AZ del client. Se quella AZ non è disponibile, VPC Lattice risponde con gli indirizzi IP di altre AZ. Da VPC Lattice alla destinazione, il routing è verso le destinazioni, che potrebbero essere distribuite tra AZ. Inoltre, non sono previsti costi di trasferimento dati Inter-AZ in VPC Lattice.

Target type (Tipo di destinazione)

Quando si crea un gruppo di destinazioni, occorre specificare il relativo tipo, che determina il tipo di destinazione specificato al momento della registrazione delle destinazioni con tale gruppo di destinazioni. Dopo aver creato un gruppo di destinazione, non è possibile modificarne il tipo di destinazione.

I tipi di target possibili sono i seguenti:

INSTANCE

I target vengono specificati in base all'ID istanza.

IP

Le destinazioni sono indirizzi IP.

LAMBDA

La destinazione è una funzione Lambda.

ALB

La destinazione è un sistema Application Load Balancer.

Considerazioni

- Se il tipo di destinazione è IP, è necessario specificare gli indirizzi IP delle sottoreti del VPC per il gruppo di destinazione. Se devi registrare indirizzi IP dall'esterno di questo VPC, crea un gruppo target di tipo ALB e registra gli indirizzi IP con Application Load Balancer.
- Se il tipo di destinazione è IP, non puoi registrare endpoint VPC o indirizzi IP instradabili pubblicamente.
- Se il tipo di destinazione è LAMBDA, puoi registrare una singola funzione Lambda. Quando il servizio riceve una richiesta per la funzione Lambda, richiama la funzione Lambda. Se desideri registrare più funzioni lambda in un servizio, devi utilizzare più gruppi target.
- Se il tipo di destinazione è ALB, puoi registrare un singolo Application Load Balancer interno come destinazione di un massimo di due servizi VPC Lattice. Per fare ciò, registra l'Application Load Balancer con due gruppi target separati, utilizzati da due diversi servizi VPC Lattice. Inoltre, l'Application Load Balancer di destinazione deve avere almeno un listener la cui porta corrisponda alla porta del gruppo di destinazione.
- Puoi registrare automaticamente le tue attività ECS con un gruppo target VPC Lattice al momento del lancio. Il tipo di destinazione del gruppo di destinazione deve essere IP. Per ulteriori informazioni, consulta [Usa VPC Lattice con i tuoi servizi Amazon ECS nella Amazon Elastic Container Service Developer Guide](#).

In alternativa, registra l'Application Load Balancer per il tuo servizio Amazon ECS con un gruppo target di tipo VPC Lattice. ALB Per ulteriori informazioni, consulta [Utilizzare il bilanciamento del carico per distribuire il traffico del servizio Amazon ECS](#) nella Amazon Elastic Container Service Developer Guide.

- Per registrare un pod EKS come destinazione, utilizza il [AWSGateway API Controller](#), che ottiene gli indirizzi IP dal servizio Kubernetes.
- Se il protocollo del gruppo di destinazione è TCP, gli unici tipi di destinazione supportati sono INSTANCE, o. IP ALB

Tipo di indirizzo IP

Quando si crea un gruppo di destinazione con un tipo di destinazione di IP, è possibile specificare un tipo di indirizzo IP per il gruppo di destinazione. Questo specifica il tipo di indirizzi utilizzato dal load balancer per inviare richieste e controlli di integrità alle destinazioni. I valori possibili sono IPv4 e IPv6. Il valore di default è IPv4.

Considerazioni

- Se si crea un gruppo target con un tipo di indirizzo IP di IPv6, il VPC specificato per il gruppo di destinazione deve avere un intervallo di indirizzi IPv6.
- Gli indirizzi IP registrati presso un gruppo di destinazione devono corrispondere al tipo di indirizzo IP del gruppo di destinazione. Ad esempio, non è possibile registrare un indirizzo IPv6 presso un gruppo target se il tipo di indirizzo IP è IPv4
- Gli indirizzi IP registrati presso un gruppo target devono rientrare nell'intervallo di indirizzi IP del VPC specificato per il gruppo di destinazione.

Obiettivi HTTP in VPC Lattice

Le richieste e le risposte HTTP utilizzano i campi intestazione per inviare informazioni sui messaggi HTTP. Le intestazioni HTTP vengono aggiunte automaticamente. I campi intestazione sono costituiti da coppie nome-valore separati da due punti e intervallati da un ritorno a capo e un avanzamento riga. Un insieme standard di campi dell'intestazione HTTP è definito nella RFC 2616 [intestazioni di messaggi](#). Sono anche disponibili intestazioni HTTP non standard che vengono aggiunte automaticamente e sono ampiamente utilizzate dalle applicazioni. Ad esempio, esistono intestazioni HTTP non standard con il prefisso. x-forwarded

x-forwarded headers

Amazon VPC Lattice aggiunge le seguenti intestazioni: x-forwarded

x-forwarded-for

L'indirizzo IP di origine.

x-forwarded-port

La porta di destinazione.

x-forwarded-proto

Il protocollo di connessione (http|https).

Intestazioni relative all'identità del chiamante

Amazon VPC Lattice aggiunge le seguenti intestazioni di identità del chiamante:

x-amzn-lattice-identity

Le informazioni sull'identità. I seguenti campi sono presenti se AWS l'autenticazione ha esito positivo.

- **Principal**— Il principale autenticato.
- **PrincipalOrgID**— L'ID dell'organizzazione per il principale autenticato.
- **PrincipalOrgPath**— I percorsi organizzativi per il principale autenticato.
- **SessionName**— Il nome della sessione autenticata.

I seguenti campi sono presenti se vengono utilizzate le credenziali Roles Anywhere e l'autenticazione ha esito positivo.

- **X509Issuer/OU**— L'emittente (OU).
- **X509SAN/DNS**— Il nome alternativo del soggetto (DNS).
- **X509SAN/NameCN**— Il nome alternativo dell'emittente ()Name/CN.
- **X509SAN/URI**— Il nome alternativo del soggetto (URI).
- **X509Subject/CN**— Il nome del soggetto (CN).

x-amzn-lattice-identity-tags

L'ID principale e gli eventuali tag principali. Il formato è il seguente:

```
principal=principal;principalorgid=orgid;principalorgpath=orgpath;principal-tag1=value1; ...;principal-tag99=value99
```

VPC Lattice sfugge a qualsiasi punto e virgola (;) in un valore con barre rovesciate (\).

x-amzn-lattice-network

Il VPC. Il formato è il seguente:

```
SourceVpcArn=arn:aws:ec2:region:account:vpc/id
```

x-amzn-lattice-target

La destinazione. Il formato è il seguente:

```
ServiceArn=arn;ServiceNetworkArn=arn;TargetGroupArn=arn
```

Per informazioni sugli ARN delle risorse per VPC Lattice, [consulta Tipi di risorse definiti da Amazon VPC Lattice](#).

Le intestazioni dell'identità del chiamante non possono essere falsificate. VPC Lattice rimuove queste intestazioni da qualsiasi richiesta in arrivo. Queste intestazioni di identità esprimono una mappa che supporta valori vuoti utilizzando il seguente formato. Durante l'analisi, non dovresti fare affidamento sull'ordine specifico delle CHIAVI in queste intestazioni, dovresti aspettarti che nuove KEY possano essere aggiunte in qualsiasi momento e dovresti essere pronto a gestire valori vuoti.

Il formato è il seguente:

```
key-0=value-0;key-1=value-1;...;key-n=value-n;
```

Lambda funge da obiettivi in VPC Lattice

Puoi registrare le tue funzioni Lambda come destinazioni con un gruppo di destinazione VPC Lattice e configurare una regola listener per inoltrare le richieste al gruppo target per la tua funzione Lambda. Quando il servizio inoltra la richiesta a un gruppo target con una funzione Lambda come destinazione, richiama la funzione Lambda e passa il contenuto della richiesta alla funzione Lambda, in formato JSON.

Limitazioni

- La funzione Lambda e il gruppo di destinazioni devono trovarsi nello stesso account e nella stessa regione.

- La dimensione massima del corpo della richiesta che puoi inviare a una funzione Lambda è di 6 MB.
- La dimensione massima della risposta JSON che la funzione Lambda può inviare è di 6 MB.
- Il protocollo deve essere HTTP o HTTPS.

Preparazione della funzione Lambda

I seguenti consigli si applicano se si utilizza la funzione Lambda con un servizio VPC Lattice.

Autorizzazioni a richiamare la funzione Lambda

Quando crei il gruppo target e registri la funzione Lambda utilizzando AWS Management Console o il, AWS CLI VPC Lattice aggiunge le autorizzazioni richieste alla politica della funzione Lambda per tuo conto.

Puoi anche aggiungere le autorizzazioni da solo utilizzando la seguente chiamata API:

```
aws lambda add-permission \  
  --function-name lambda-function-arn-with-alias-name \  
  --statement-id vpc-lattice \  
  --principal vpc-lattice.amazonaws.com \  
  --action lambda:InvokeFunction \  
  --source-arn target-group-arn
```

Controllo delle versioni della funzione Lambda

Puoi registrare una funzione Lambda per gruppo di destinazioni. Per assicurarti di poter modificare la funzione Lambda e che il servizio VPC Lattice richiami sempre la versione corrente della funzione Lambda, crea un alias di funzione e includi l'alias nella funzione ARN quando registri la funzione Lambda con il servizio VPC Lattice. Per ulteriori informazioni, consulta [Versioni della funzione Lambda](#) e [Creazione di un alias per una funzione Lambda](#) nella Guida per gli sviluppatori. AWS Lambda

Creazione di un gruppo di destinazioni per la funzione Lambda

Creare un gruppo target, che viene utilizzato nell'instradamento delle richieste. Se il contenuto della richiesta corrisponde a una regola del listener con un'azione per inoltrarlo a questo gruppo di destinazione, il servizio VPC Lattice richiama la funzione Lambda registrata.

Per creare un gruppo target e registrare la funzione Lambda utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegliere Crea gruppo target.
4. Per Seleziona destinazione, scegli Funzione Lambda.
5. In Nome gruppo di destinazione, immetti un nome per il gruppo di destinazione.
6. Per la versione della struttura degli eventi Lambda, scegli una versione. Per ulteriori informazioni, consulta [the section called “Ricevi eventi dal servizio VPC Lattice”](#).
7. (Facoltativo) Per aggiungere tag, espandi Tag, scegli Aggiungi nuovo tag e inserisci la chiave e il valore del tag.
8. Scegli Next (Successivo).
9. In Funzione Lambda, esegui una delle seguenti operazioni:
 - Seleziona una funzione Lambda esistente.
 - Crea una nuova funzione Lambda e selezionala.
 - Registra la funzione Lambda in un secondo momento.
10. Scegliere Crea gruppo target.

Per creare un gruppo target e registrare la funzione Lambda utilizzando ilAWS CLI

Utilizza i comandi [create-target-group](#) e [register-targets](#).

Ricevi eventi dal servizio VPC Lattice

Il servizio VPC Lattice supporta la chiamata Lambda per le richieste su HTTP e HTTPS. Il servizio invia un evento in formato JSON e aggiunge l'intestazione a ogni richiesta. X-Forwarded-For

Codifica Base64

Il servizio Base64 codifica il corpo se l'content-encodingintestazione è presente e il tipo di contenuto non è uno dei seguenti:

- text/*
- application/json
- application/xml
- application/javascript

Se l'intestazione content-encoding non è presente, la codifica Base64 dipende dal tipo di contenuto. Per i tipi di contenuto sopra indicati, il servizio invia il corpo così com'è, senza codifica Base64.

Formato della struttura degli eventi

Quando crei o aggiorni un tipo di gruppo targetLAMBDA, puoi specificare la versione della struttura degli eventi ricevuta dalla funzione Lambda. Le versioni possibili sono V1 e V2.

Example Evento di esempio: V2

```
{
  "version": "2.0",
  "path": "/?query1=value1&query2=value2",
  "method": "GET|POST|HEAD|...",
  "headers": {
    "header-key": ["header-value", ...],
    ...
  },
  "queryStringParameters": {
    "key": ["value", ...]
  },
  "body": "request-body",
  "isBase64Encoded": true|false,
  "requestContext": {
    "serviceNetworkArn": "arn:aws:vpc-
lattice:region:123456789012:servicenetwork/sn-0bf3f2882e9cc805a",
    "serviceArn": "arn:aws:vpc-
lattice:region:123456789012:service/svc-0a40eebed65f8d69c",
    "targetGroupArn": "arn:aws:vpc-
lattice:region:123456789012:targetgroup/tg-6d0ecf831eec9f09",
    "identity": {
      "sourceVpcArn":
"arn:aws:ec2:region:123456789012:vpc/vpc-0b8276c84697e7339",
      "type": "AWS_IAM",
      "principal": "arn:aws:iam::123456789012:assumed-role/my-role/my-session",
      "principalOrgID": "o-50dc6c495c0c9188",
      "sessionName": "i-0c7de02a688bde9f7",
      "x509IssuerOu": "string",
      "x509SanDns": "string",
      "x509SanNameCn": "string",
      "x509SanUri": "string",
      "x509SubjectCn": "string"
    }
  }
}
```

```
    },  
    "region": "region",  
    "timeEpoch": "1690497599177430"  
  }  
}
```

body

Il corpo della richiesta. Presente solo se il protocollo è HTTP, HTTPS o gRPC.

headers

Le intestazioni HTTP della richiesta. Presente solo se il protocollo è HTTP, HTTPS o gRPC.

identity

Le informazioni sull'identità. I campi possibili sono i seguenti.

- `principal`— Il principale autenticato. Presente solo se AWS l'autenticazione ha esito positivo.
- `principalOrgID`— L'ID dell'organizzazione per il principale autenticato. Presente solo se AWS l'autenticazione ha esito positivo.
- `sessionName`— Il nome della sessione autenticata. Presente solo se AWS l'autenticazione ha esito positivo.
- `sourceVpcArn`— L'ARN del VPC da cui ha avuto origine la richiesta. Presente solo se è possibile identificare il VPC di origine.
- `type`— Il valore è `AWS_IAM` se viene utilizzata una politica di AWS autenticazione e l'autenticazione ha esito positivo.

Se vengono utilizzate le credenziali Roles Anywhere e l'autenticazione ha esito positivo, i seguenti sono i campi possibili.

- `x509IssuerOu`— L'emittente (OU).
- `x509SanDns`— Il nome alternativo del soggetto (DNS).
- `x509SanNameCn`— Il nome alternativo dell'emittente ()Name/CN.
- `x509SanUri`— Il nome alternativo del soggetto (URI).
- `x509SubjectCn`— Il nome del soggetto (CN).

isBase64Encoded

Indica se il corpo è codificato in base64. Presente solo se il protocollo è HTTP, HTTPS o gRPC e il corpo della richiesta non è già una stringa.

method

Metodo HTTP nella richiesta. Presente solo se il protocollo è HTTP, HTTPS o gRPC.

path

Il percorso della richiesta proveniente dal client che include i parametri della stringa di query.

Presente solo se il protocollo è HTTP, HTTPS o gRPC.

queryStringParameters

I parametri della stringa di query HTTP. Presente solo se il protocollo è HTTP, HTTPS o gRPC.

serviceArn

L'ARN del servizio che riceve la richiesta.

serviceNetworkArn

L'ARN della rete di servizi che consegna la richiesta.

targetGroupArn

L'ARN del gruppo target che riceve la richiesta.

timeEpoch

Il tempo, in microsecondi.

Example Evento di esempio: V1

```
{
  "raw_path": "/path/to/resource?query1=value1&query2=value2",
  "method": "GET|POST|HEAD|...",
  "headers": {"header-key": "header-value", ... },
  "query_string_parameters": {"key": "value", ...},
  "body": "request-body",
  "is_base64_encoded": true|false
}
```

Rispondi al servizio VPC Lattice

La risposta dalla funzione Lambda deve includere lo stato della codifica Base64, il codice di stato e le intestazioni. Puoi omettere il corpo della risposta.

Per includere un contenuto binario nel corpo della risposta, devi sottoporre a codifica Base64 il contenuto e impostare `isBase64Encoded` su `true`. Il servizio decodifica il contenuto per recuperare il contenuto binario e lo invia al client nel corpo della risposta HTTP.

Il servizio VPC Lattice non rispetta le intestazioni hop-by-hop, come `o. Connection Transfer-Encoding`. È possibile omettere l'`Content-Length` intestazione perché il servizio la calcola prima di inviare le risposte ai client.

Di seguito è riportato un esempio di risposta da una funzione Lambda:

```
{
  "isBase64Encoded": false,
  "statusCode": 200,
  "headers": {
    "Set-cookie": "cookies",
    "Content-Type": "application/json"
  },
  "body": "Hello from Lambda (optional)"
}
```

Multi-value intestazioni

VPC Lattice supporta le richieste di un client o le risposte di una funzione Lambda che contengono intestazioni con più valori o contengono la stessa intestazione più volte. VPC Lattice passa tutti i valori agli obiettivi.

Nell'esempio seguente, ci sono due intestazioni denominate `header1` con valori diversi.

```
header1 = value1
header1 = value2
```

Con una struttura di eventi V2, VPC Lattice invia i valori in un elenco. Esempio:

```
"header1": ["value1", "value2"]
```

Con una struttura di eventi V1, VPC Lattice combina i valori in un'unica stringa. Esempio:

```
"header1": "value1, value2"
```

Multi-value parametri della stringa di interrogazione

VPC Lattice supporta parametri di interrogazione con più valori per la stessa chiave.

Nell'esempio seguente, ci sono due parametri denominati QS1 con valori diversi.

```
http://www.example.com?&QS1=value1&QS1=value2
```

Con una struttura di eventi V2, VPC Lattice invia i valori in un elenco. Esempio:

```
"QS1": ["value1", "value2"]
```

Con una struttura di eventi V1, VPC Lattice utilizza l'ultimo valore passato. Esempio:

```
"QS1": "value2"
```

Annullamento della registrazione della funzione Lambda

Se non hai più bisogno di inviare traffico alla funzione Lambda, puoi annullare la relativa registrazione. Dopo avere annullato la registrazione di una funzione Lambda, le richieste in transito hanno esito negativo con 5XX errori HTTP.

Per sostituire una funzione Lambda, ti consigliamo di creare un nuovo gruppo di destinazioni, registrare la nuova funzione con il nuovo gruppo e aggiornare le regole del listener per utilizzare il nuovo gruppo di destinazioni invece di quello esistente.

Per annullare la registrazione di una funzione Lambda utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegli il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Nella scheda Destinazioni, scegli Annulla registrazione.
5. Quando viene richiesta la conferma, inserisci **confirm** e scegli Annulla registrazione.

Per annullare la registrazione della funzione Lambda utilizzando ilAWS CLI

Utilizza il comando [deregister-targets](#).

Application Load Balancer come obiettivi in VPC Lattice

Puoi creare un gruppo target VPC Lattice, registrare un singolo Application Load Balancer interno come destinazione e configurare il servizio VPC Lattice per inoltrare il traffico a questo gruppo target. In questo scenario, l'Application Load Balancer prende in carico la decisione di routing non appena il traffico la raggiunge. Questa configurazione consente di utilizzare la funzionalità di routing basato su richieste di livello 7 dell'Application Load Balancer in combinazione con le funzionalità supportate da VPC Lattice, come l'autenticazione e l'autorizzazione IAM e la connettività tra VPC e account.

Limitazioni

- È possibile registrare un singolo Application Load Balancer interno come destinazione in un gruppo target di tipo VPC Lattice. ALB
- È possibile registrare un Application Load Balancer come destinazione di un massimo di due gruppi di target VPC Lattice, utilizzati da due diversi servizi VPC Lattice.
- VPC Lattice non fornisce controlli dello stato di salute per un ALB tipo di gruppo target. Tuttavia, puoi configurare i controlli di integrità in modo indipendente a livello di load balancer per gli obiettivi in Elastic Load Balancing. Per ulteriori informazioni, consulta i [controlli dello stato del gruppo Target](#) nella Guida per l'utente di Application Load Balancers

Prerequisiti

Crea un Application Load Balancer per registrarti come target con il tuo gruppo target VPC Lattice. Il load balancer deve soddisfare i seguenti criteri:

- Lo schema di bilanciamento del carico è interno.
- L'Application Load Balancer deve trovarsi nello stesso account del gruppo target VPC Lattice e deve essere nello stato Attivo.
- L'Application Load Balancer deve trovarsi nello stesso VPC del gruppo target VPC Lattice.
- Puoi utilizzare i listener HTTPS sull'Application Load Balancer per terminare TLS, ma solo se il servizio VPC Lattice utilizza lo stesso certificato del load balancer. SSL/TLS
- Per preservare l'IP client del servizio VPC Lattice nell'intestazione della X-Forwarded-For richiesta, è necessario impostare l'attributo per Application Load Balancer su `routing.http.xff_header_processing.mode Preserve`. Se il valore è `Preserve`, il load balancer conserva l'X-Forwarded-For intestazione nella richiesta HTTP e la invia alle destinazioni senza alcuna modifica.

Per ulteriori informazioni, consulta [Create an Application Load Balancer](#) nella User Guide for Application Load Balancer.

Fase 1: Creare un gruppo target di tipo ALB

Utilizzare la procedura seguente per creare il gruppo target. Tieni presente che VPC Lattice non supporta i controlli sanitari per ALB i gruppi target. Tuttavia, puoi configurare i controlli di integrità per i gruppi target per il tuo Application Load Balancer. Per ulteriori informazioni, consulta [Target group health checks](#) nella User Guide for Application Load Balancers.

Per creare il gruppo target

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Scegliere Crea gruppo target.
4. Nella pagina Specificare i dettagli del gruppo target, in Configurazione di base, scegli Application Load Balancer come tipo di destinazione.
5. In Nome gruppo di destinazione, immetti un nome per il gruppo di destinazione.
6. Per Protocollo, scegliete **HTTPHTTPS**, o **TCP**. Il protocollo del gruppo target deve corrispondere al protocollo del listener per l'Application Load Balancer interno.
7. Per Port, specificate la porta per il vostro gruppo di destinazione. Questa porta deve corrispondere alla porta del listener per l'Application Load Balancer interno. In alternativa, è possibile aggiungere una porta listener sull'Application Load Balancer interno in modo che corrisponda alla porta del gruppo di destinazione specificata qui.
8. Per VPC, seleziona lo stesso cloud privato virtuale (VPC) che hai selezionato quando hai creato l'Application Load Balancer interno. Dovrebbe essere il VPC che contiene le tue risorse VPC Lattice.
9. Per la versione del protocollo, scegli la versione del protocollo supportata dall'Application Load Balancer.
10. (Facoltativo) Aggiungi i tag richiesti.
11. Scegli Next (Successivo).

Fase 2: Registrare l'Application Load Balancer come destinazione

È possibile registrare il load balancer come destinazione ora o in un secondo momento.

Per registrare un Application Load Balancer come destinazione

1. Scegli Registrati ora.
2. Per Application Load Balancer, scegli il tuo Application Load Balancer interno.
3. Per Port, mantieni l'impostazione predefinita o specifica una porta diversa in base alle esigenze. Questa porta deve corrispondere a una porta listener esistente sull'Application Load Balancer. Se continui senza una porta corrispondente, il traffico non raggiungerà il tuo Application Load Balancer.
4. Scegliere Crea gruppo target.

Versione del protocollo

Per impostazione predefinita, i servizi inviano richieste alle destinazioni utilizzando HTTP/1.1. È possibile utilizzare la versione del protocollo per inviare richieste alle destinazioni utilizzando HTTP/2 o gRPC.

La tabella seguente riassume il risultato per le combinazioni di protocollo della richiesta e versione del protocollo del gruppo di destinazioni.

Protocollo della richiesta	Versione del protocollo	Risultato
HTTP/1.1	HTTP/1.1	Completato
HTTP/2	HTTP/1.1	Completato
gRPC	HTTP/1.1	Errore
HTTP/1.1	HTTP/2	Errore
HTTP/2	HTTP/2	Completato
gRPC	HTTP/2	Riuscito se le destinazioni supportano gRPC
HTTP/1.1	gRPC	Errore
HTTP/2	gRPC	Riuscito se la richiesta è POST

Protocollo della richiesta	Versione del protocollo	Risultato
gRPC	gRPC	Completato

Considerazioni sulla versione del protocollo gRPC

- L'unico protocollo dell'ascoltatore supportato è HTTPS.
- Gli unici tipi di istanza supportati sono INSTANCE e IP.
- Il servizio analizza le richieste gRPC e indirizza le chiamate gRPC ai gruppi target appropriati in base al pacchetto, al servizio e al metodo.
- Non puoi usare le funzioni Lambda come obiettivi.

Considerazioni sulla versione del protocollo HTTP/2

- L'unico protocollo dell'ascoltatore supportato è HTTPS. È possibile scegliere HTTP o HTTPS per il protocollo del gruppo di destinazione.
- Le uniche regole per i listener supportate sono la risposta diretta e la risposta fissa.
- Gli unici tipi di istanza supportati sono INSTANCE e IP.
- Il servizio supporta lo streaming dai client. Il servizio non supporta lo streaming verso le destinazioni.

Tag per il tuo gruppo target VPC Lattice

I tag ti aiutano a classificare i gruppi target in modi diversi, ad esempio in base a scopo, proprietario o ambiente.

È possibile aggiungere più tag a ciascun gruppo target. Le chiavi dei tag devono essere univoche per ogni gruppo target. Se aggiungi un tag con una chiave già associata al gruppo target, il valore del tag viene aggiornato.

Quando un tag non serve più, è possibile rimuoverlo.

Restrizioni

- Numero massimo di tag per risorsa: 50
- Lunghezza massima della chiave: 127 caratteri Unicode

- Lunghezza massima del valore: 255 caratteri Unicode
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. I caratteri consentiti sono lettere, spazi e numeri rappresentabili in UTF-8, più i seguenti caratteri speciali: + - =. _ : / @. Non utilizzare spazi iniziali o finali.
- Non utilizzate il `aws:` prefisso nei nomi o nei valori dei tag perché è AWS riservato all'uso. Non è possibile modificare né eliminare i nomi o i valori di tag con tale prefisso. I tag con questo prefisso non vengono conteggiati per il limite del numero di tag per risorsa.

Per aggiornare i tag per un gruppo target tramite la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Target groups.
3. Seleziona il nome del gruppo di destinazione per visualizzarne i dettagli.
4. Selezionare la scheda Tag.
5. Per aggiungere un tag, scegli Aggiungi tag e inserisci la chiave del tag e il valore del tag. Per aggiungere un altro tag, scegli Aggiungi nuovo tag. Una volta completata l'aggiunta di tag, scegli Save changes (Salva modifiche).
6. Per eliminare un tag, seleziona la relativa casella di controllo e scegli Elimina. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per aggiornare i tag per un gruppo target utilizzando ilAWS CLI

Utilizzate i comandi [tag-resource](#) e [untag-resource](#).

Eliminare un gruppo target VPC Lattice

È possibile eliminare un gruppo di destinazioni se non ci sono operazioni di inoltro di alcuna regola dell'ascoltatore che vi fanno riferimento. L'eliminazione di un gruppo target non influisce sui target registrati con il gruppo target. Se non hai più bisogno di un'istanza EC2 registrata, puoi arrestarla o terminarla.

Per eliminare un gruppo target tramite la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, scegli Target groups.

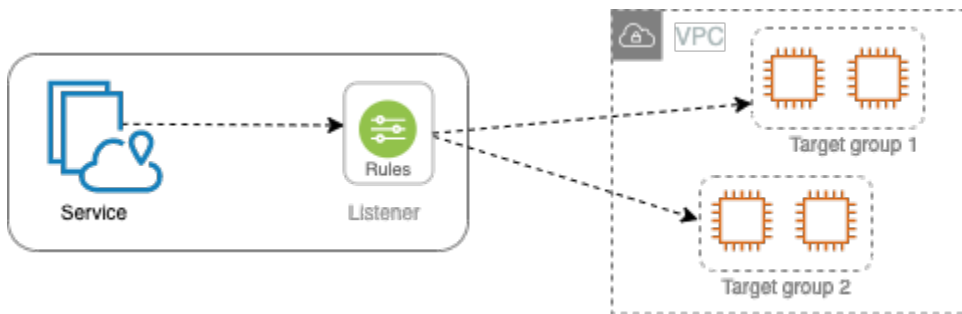
3. Seleziona la casella di controllo per il gruppo target, quindi scegli Azioni, Elimina.
4. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per eliminare un gruppo target utilizzando ilAWS CLI

Utilizza il comando [delete-target-group](#).

Listener per il tuo servizio VPC Lattice

Prima di iniziare a utilizzare il servizio VPC Lattice, devi aggiungere un listener. Un ascoltatore è un processo che controlla le richieste di connessione utilizzando il protocollo e la porta configurata. Le regole definite per un listener determinano il modo in cui il sistema di bilanciamento del carico instrada le richieste alle destinazioni registrate.



Indice

- [Configurazione dei listener](#)
- [Listener HTTP per servizi VPC Lattice](#)
- [Listener HTTPS per servizi VPC Lattice](#)
- [Listener TLS per servizi VPC Lattice](#)
- [Regole di ascolto per il tuo servizio VPC Lattice](#)
- [Elimina un listener per il tuo servizio VPC Lattice](#)

Configurazione dei listener

I listener supportano i seguenti protocolli e porte:

- Protocolli: HTTP, HTTPS, TLS
- Porte: 1-65535

Se il protocollo listener è HTTPS, VPC Lattice fornirà e gestirà un certificato TLS associato all'FQDN generato da VPC Lattice. VPC Lattice supporta TLS su e. HTTP/1.1 HTTP/2 Quando si configura un servizio con un listener HTTPS, VPC Lattice determinerà automaticamente il protocollo HTTP Application-Layer utilizzando Protocol Negotiation (ALPN). Se ALPN è assente, il valore predefinito di VPC Lattice è. HTTP/1.1 Per ulteriori informazioni, consulta [Listener HTTPS](#).

VPC Lattice può ascoltare su HTTP HTTP/1.1, HTTPS HTTP/2 e comunicare con i target in uno qualsiasi di questi protocolli e versioni. Non è necessario che i protocolli del listener e del gruppo target corrispondano. VPC Lattice gestisce l'intero processo di aggiornamento e downgrade tra protocolli e versioni. Per ulteriori informazioni, consulta [Versione del protocollo](#).

È possibile creare un listener TLS per garantire che l'applicazione decrittografi il traffico crittografato anziché VPC Lattice. Per ulteriori informazioni, consulta [Ascoltatori TLS](#).

VPC Lattice non supporta nativamente. WebSockets Tuttavia, puoi comunque connetterti ai Websocket-based servizi utilizzando listener TLS o eseguendo il routing tramite risorse VPC Lattice.

Listener HTTP per servizi VPC Lattice

Si definisce listener il processo che verifica la presenza di richieste di connessione. Puoi definire un listener quando crei il tuo servizio VPC Lattice. Puoi aggiungere ascoltatori al tuo servizio in qualsiasi momento.

Le informazioni contenute in questa pagina consentono di creare un listener HTTP per il servizio. Per informazioni sulla creazione di listener che utilizzano altri protocolli, [Listener HTTPS](#) consultate e.

[Ascoltatori TLS](#)

Prerequisiti

- Per aggiungere un'azione di inoltro alla regola listener predefinita, è necessario specificare un gruppo target VPC Lattice disponibile. Per ulteriori informazioni, consulta [Crea un gruppo target VPC Lattice](#).
- È possibile specificare lo stesso gruppo target in più listener, ma questi listener devono appartenere allo stesso servizio. Per utilizzare un gruppo target con un servizio VPC Lattice, è necessario verificare che non venga utilizzato da un listener per nessun altro servizio VPC Lattice.

Aggiunta di un ascoltatore HTTP

Puoi aggiungere listener e regole al tuo servizio in qualsiasi momento. Si configura un listener con un protocollo e una porta per le connessioni dai client al servizio e un gruppo target VPC Lattice per la regola listener predefinita. Per ulteriori informazioni, consulta [Configurazione dei listener](#).

Aggiunta di un listener HTTP mediante la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.

2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Nella scheda Routing, scegli Aggiungi listener.
5. Per il nome del listener, puoi fornire un nome di listener personalizzato o utilizzare il protocollo e la porta del listener come nome del listener. Un nome personalizzato che specifichi può contenere fino a 63 caratteri e deve essere univoco per ogni servizio del tuo account. I caratteri validi sono a-z, 0-9 e trattini (-). Non è possibile utilizzare un trattino come primo o ultimo carattere o immediatamente dopo un altro trattino. Non è possibile modificare il nome dopo averlo creato.
6. Per Protocollo: porta, scegli HTTP e inserisci un numero di porta.
7. Per Azione predefinita, scegli il gruppo target VPC Lattice per ricevere il traffico e scegli il peso da assegnare a questo gruppo target. Il peso che assegni a un gruppo target ne imposta la priorità rispetto alla ricezione del traffico. Ad esempio, se due gruppi target hanno lo stesso peso, ogni gruppo target riceve metà del traffico. Se hai specificato un solo gruppo target, il 100% del traffico viene inviato a quell'unico gruppo target.

Facoltativamente, puoi aggiungere un altro gruppo target per l'azione predefinita. Scegli Aggiungi azione, quindi scegli un gruppo target e specificane il peso.

8. (Facoltativo) Per aggiungere un'altra regola, scegli Aggiungi regola, quindi inserisci un nome, una priorità, una condizione e un'azione per la regola.

Puoi assegnare a ciascuna regola un numero di priorità compreso tra 1 e 100. Un listener non può avere più regole con la stessa priorità. Le regole vengono valutate in base all'ordine di priorità, dal valore più basso a quello più alto. La regola predefinita è valutata per ultima. Per ulteriori informazioni, consulta [Regole dei listener](#).

9. (Facoltativo) Per aggiungere tag, espandi i tag Listener, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
10. Controlla la configurazione, quindi scegli Aggiungi.

Per aggiungere un listener HTTP utilizzando il AWS CLI

Utilizzate il comando [create-listener](#) per creare un listener con una regola predefinita e il comando [create-rule](#) per creare regole di listener aggiuntive.

Listener HTTPS per servizi VPC Lattice

Si definisce listener il processo che verifica la presenza di richieste di connessione. Definisci un listener quando crei il tuo servizio. Puoi aggiungere ascoltatori al tuo servizio in VPC Lattice in qualsiasi momento.

Puoi creare un listener HTTPS, che utilizza la versione TLS 1.2 o la versione TLS 1.3 per terminare direttamente le connessioni HTTPS con VPC Lattice. VPC Lattice fornirà e gestirà un certificato TLS associato al nome di dominio completo (FQDN) generato da VPC Lattice. VPC Lattice supporta TLS su e. HTTP/1.1 HTTP/2 Quando si configura un servizio con un listener HTTPS, VPC Lattice determinerà automaticamente il protocollo HTTP Application-Layer tramite Protocol Negotiation (ALPN). Se ALPN è assente, il valore predefinito di VPC Lattice è. HTTP/1.1

VPC Lattice utilizza un'architettura multi-tenancy, il che significa che può ospitare più servizi sullo stesso endpoint. VPC Lattice utilizza TLS con Server Name Indication (SNI) per ogni richiesta del client. Encrypted Client Hello (ECH) e Encrypted Server Name Indication (ESNI) non sono supportati.

VPC Lattice può ascoltare su HTTP HTTP/1.1, HTTPS HTTP/2 e comunicare con i target in uno qualsiasi di questi protocolli e versioni. Non è necessario che queste configurazioni del listener e del gruppo target corrispondano. VPC Lattice gestisce l'intero processo di aggiornamento e downgrade tra protocolli e versioni. Per ulteriori informazioni, consulta [Versione del protocollo](#).

Per garantire che la tua applicazione decrittografi il traffico, crea invece un listener TLS. Con il passthrough TLS, VPC Lattice non termina TLS. Per ulteriori informazioni, consulta [Ascoltatori TLS](#).

Indice

- [Policy di sicurezza](#)
- [Politica ALPN](#)
- [Aggiunta di un ascoltatore HTTPS](#)

Policy di sicurezza

VPC Lattice utilizza una politica di sicurezza che è una combinazione di un TLSv1.2 protocollo e un elenco di cifrari. SSL/TLS Il protocollo stabilisce una connessione sicura tra un client e un server e aiuta a garantire che tutti i dati trasmessi tra il client e il servizio in VPC Lattice siano privati. Un codice è un algoritmo di crittografia che utilizza chiavi di crittografia per creare un messaggio codificato. I protocolli utilizzano diversi codici per crittografare i dati. Durante il processo di negoziazione della connessione, il client e VPC Lattice presentano un elenco di cifrari e protocolli

supportati ciascuno, in ordine di preferenza. Per impostazione predefinita, la prima crittografia nell'elenco del server che corrisponde a una qualsiasi delle crittografie del client viene selezionata per la connessione sicura.

VPC Lattice utilizza i seguenti codici TLS 1.2 in questo ordine SSL/TLS di preferenza:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA
- AES256-GCM-SHA384
- AES256-SHA

VPC Lattice utilizza anche i seguenti SSL/TLS cifrari TLS 1.3 in questo ordine di preferenza:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Politica ALPN

Application-Layer Protocol Negotiation (ALPN) è un'estensione TLS che viene inviata nei messaggi di saluto iniziali dell'handshake TLS. ALPN consente al livello dell'applicazione di negoziare quali protocolli devono essere utilizzati su una connessione sicura, ad esempio e. HTTP/1 HTTP/2

Quando il client avvia una connessione ALPN, il servizio VPC Lattice confronta l'elenco delle preferenze ALPN del client con la sua politica ALPN. Se il client supporta un protocollo dalla politica ALPN, il servizio VPC Lattice stabilisce la connessione in base all'elenco delle preferenze della politica ALPN. Altrimenti, il servizio non utilizza ALPN.

VPC Lattice supporta la seguente politica ALPN:

HTTP2Preferred

Preferisco. HTTP/2 HTTP/1.1 L'elenco delle preferenze ALPN è h2, http/1 .1.

Aggiunta di un ascoltatore HTTPS

Si configura un listener con un protocollo e una porta per le connessioni dai client al servizio e un gruppo target per la regola del listener predefinita. Per ulteriori informazioni, consulta [Configurazione dei listener](#).

Prerequisiti

- Per aggiungere un'azione di inoltro alla regola listener predefinita, è necessario specificare un gruppo target VPC Lattice disponibile. Per ulteriori informazioni, consulta [Crea un gruppo target VPC Lattice](#).
- È possibile specificare lo stesso gruppo target in più listener, ma questi listener devono appartenere allo stesso servizio VPC Lattice. Per utilizzare un gruppo target con un servizio VPC Lattice, è necessario verificare che non venga utilizzato da un listener per nessun altro servizio VPC Lattice.
- Puoi utilizzare il certificato fornito da VPC Lattice o importare il tuo certificato in. AWS Certificate Manager Per ulteriori informazioni, consulta [the section called "BYOC"](#).

Aggiunta di un listener HTTPS mediante la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Nella scheda Routing, scegli Aggiungi listener.
5. Per il nome del listener, puoi fornire un nome di listener personalizzato o utilizzare il protocollo e la porta del listener come nome del listener. Un nome personalizzato che specifichi può contenere fino a 63 caratteri e deve essere univoco per ogni servizio del tuo account. I caratteri validi sono a-z, 0-9 e trattini (-). Non è possibile utilizzare un trattino come primo o ultimo carattere o immediatamente dopo un altro trattino. Non è possibile modificare il nome di un ascoltatore dopo averlo creato.
6. Per Protocollo: porta, scegliete HTTPS e immettete un numero di porta.
7. Per Azione predefinita, scegli il gruppo target VPC Lattice per ricevere il traffico e scegli il peso da assegnare a questo gruppo target. Il peso che assegni a un gruppo target ne imposta la priorità rispetto alla ricezione del traffico. Ad esempio, se due gruppi target hanno lo stesso peso, ogni gruppo target riceve metà del traffico. Se hai specificato un solo gruppo target, il 100% del traffico viene inviato a quell'unico gruppo target.

Facoltativamente, puoi aggiungere un altro gruppo target per l'azione predefinita. Scegli Aggiungi azione, quindi scegli un gruppo target e specificane il peso.

8. (Facoltativo) Per aggiungere un'altra regola, scegli Aggiungi regola, quindi inserisci un nome, una priorità, una condizione e un'azione per la regola.

Puoi assegnare a ciascuna regola un numero di priorità compreso tra 1 e 100. Un listener non può avere più regole con la stessa priorità. Le regole vengono valutate in base all'ordine di priorità, dal valore più basso a quello più alto. La regola predefinita è valutata per ultima. Per ulteriori informazioni, consulta [Regole dei listener](#).

9. (Facoltativo) Per aggiungere tag, espandi i tag Listener, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
10. Per le impostazioni del certificato del listener HTTPS, se non hai specificato un nome di dominio personalizzato al momento della creazione del servizio, VPC Lattice genera automaticamente un certificato TLS per proteggere il traffico che scorre attraverso il listener.

Se hai creato il servizio con un nome di dominio personalizzato, ma non hai specificato un certificato corrispondente, puoi farlo ora scegliendo il certificato da Certificato personalizzato. SSL/TLS. Altrimenti, il certificato specificato al momento della creazione del servizio è già stato scelto.

11. Controlla la configurazione, quindi scegli Aggiungi.

Per aggiungere un listener HTTPS utilizzando il AWS CLI

Utilizzate il comando [create-listener](#) per creare un listener con una regola predefinita e il comando [create-rule](#) per creare regole di listener aggiuntive.

Listener TLS per servizi VPC Lattice

Si definisce listener il processo che verifica la presenza di richieste di connessione. Puoi definire un listener quando crei il tuo servizio VPC Lattice. Puoi aggiungere ascoltatori al tuo servizio in qualsiasi momento.

Puoi creare un listener TLS in modo che VPC Lattice trasmetta il traffico crittografato alle tue applicazioni senza decrittografarlo.

Se preferisci che VPC Lattice decrittografi il traffico crittografato e invii traffico non crittografato alle tue applicazioni, crea invece un listener HTTPS. Per ulteriori informazioni, consulta [Listener HTTPS](#).

Considerazioni

Le seguenti considerazioni si applicano ai listener TLS:

- Il servizio VPC Lattice deve avere un nome di dominio personalizzato. Il nome di dominio personalizzato del servizio viene utilizzato come corrispondenza SNI (Service Name Indication). Se hai specificato un certificato quando hai creato il servizio, questo non viene utilizzato.
- L'unica regola consentita per un listener TLS è la regola predefinita.
- L'azione predefinita per un listener TLS deve essere un'azione di inoltro a un gruppo target TCP.
- Per impostazione predefinita, i controlli di integrità sono disabilitati per i gruppi target TCP. Se si abilitano i controlli di integrità per un gruppo target TCP, è necessario specificare un protocollo e una versione del protocollo.
- I listener TLS instradano le richieste utilizzando il campo SNI del messaggio client-hello. Puoi utilizzare certificati wildcard e SAN sui tuoi obiettivi se la condizione di corrispondenza corrisponde esattamente a quella del client-hello.
- Poiché tutto il traffico rimane crittografato dal client alla destinazione, VPC Lattice non può leggere le intestazioni HTTP e non può inserire o rimuovere le intestazioni HTTP. Pertanto, con un listener TLS, esistono le seguenti limitazioni:
 - La durata della connessione è limitata a 10 minuti
 - Il timeout di inattività configurabile per il servizio si applica anche alle connessioni del listener TLS. Se non viene trasferito alcun dato per la durata del timeout di inattività, VPC Lattice chiude la connessione. È possibile regolare il timeout di inattività (60-600 secondi) utilizzando il parametro quando si crea o si aggiorna il `idleTimeoutSeconds` servizio.
 - Le politiche di autenticazione sono limitate ai principali anonimi
 - I target Lambda non sono supportati
- Le connessioni Websocket possono utilizzare i listener TLS per connettersi ai servizi VPC Lattice. Esistono le seguenti limitazioni:
 - La durata della connessione è limitata a 10 minuti
 - Le politiche di autenticazione sono limitate ai principali anonimi
 - I target Lambda non sono supportati
- Encrypted Client Hello (ECH) non è supportato.
- L'Encrypted Server Name Indication (ESNI) non è supportata.

Aggiungi un listener TLS

Si configura un listener con un protocollo e una porta per le connessioni dai client al servizio e un gruppo target per la regola del listener predefinita. Per ulteriori informazioni, consulta [Configurazione dei listener](#).

Per aggiungere un listener TLS utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Nella scheda Routing, scegli Aggiungi listener.
5. Per il nome del listener, puoi fornire un nome di listener personalizzato o utilizzare il protocollo e la porta del listener come nome del listener. Un nome personalizzato che specifichi può contenere fino a 63 caratteri e deve essere univoco per ogni servizio del tuo account. I caratteri validi sono a-z, 0-9 e trattini (-). Non è possibile utilizzare un trattino come primo o ultimo carattere o immediatamente dopo un altro trattino. Non è possibile modificare il nome di un ascoltatore dopo averlo creato.
6. Per Protocollo, scegli TLS. Per Porta, inserisci un numero di porta.
7. Per Inoltra al gruppo target, scegli un gruppo target VPC Lattice che utilizza il protocollo TCP per ricevere il traffico e scegli il peso da assegnare a questo gruppo target. Facoltativamente, puoi aggiungere un altro gruppo target. Scegli Aggiungi gruppo target, quindi scegli un gruppo target e inserisci il suo peso.
8. (Facoltativo) Per aggiungere tag, espandi i tag Listener, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
9. Controlla la configurazione, quindi scegli Aggiungi.

Per aggiungere un listener TLS utilizzando il AWS CLI

Utilizzate il comando [create-listener](#) per creare un listener con una regola predefinita. Specificate il protocollo TLS_PASSTHROUGH.

Regole di ascolto per il tuo servizio VPC Lattice

Ogni listener ha una regola predefinita e regole aggiuntive che puoi definire. Ogni regola consiste in una priorità, una o più operazioni e una o più condizioni. Puoi aggiungere o modificare le regole in qualsiasi momento.

Indice

- [Regole predefinite](#)
- [Priorità delle regole](#)
- [Operazione delle regole](#)
- [Condizioni della regola](#)
- [Aggiungere una regola](#)
- [Aggiorna una regola](#)
- [Eliminare una regola](#)

Regole predefinite

Le operazioni per la regola predefinita vengono definite al momento della creazione del listener. Le regole predefinite non possono avere condizioni. Se non viene soddisfatta nessuna condizione per qualsiasi regola del listener, viene eseguita l'operazione per la regola predefinita.

Priorità delle regole

Ogni regola ha una priorità. Le regole vengono valutate in base all'ordine di priorità, dal valore più basso a quello più alto. La regola predefinita è valutata per ultima. È possibile modificare la priorità di una regola non predefinita in qualsiasi momento. Non è possibile modificare la priorità della regola di default.

Operazione delle regole

I listener per i servizi VPC Lattice supportano azioni dirette e azioni a risposta fissa.

Operazioni di inoltro

Puoi utilizzare `forward` le azioni per indirizzare le richieste a uno o più gruppi target VPC Lattice. Se si specificano più gruppi di destinazioni per un'operazione `forward`, è necessario specificare un peso per ciascun gruppo di destinazioni. Ogni peso del gruppo di destinazioni è un valore compreso

tra 0 e 999. Le richieste che corrispondono a una regola del listener con gruppi di destinazioni ponderati vengono distribuite a questi gruppi di destinazioni in base ai rispettivi pesi. Ad esempio, se specifichi due gruppi di destinazioni, ciascuno con un peso di 10, ogni gruppo di destinazioni riceve la metà delle richieste. Se specifichi due gruppi di destinazioni, uno con un peso di 10 e l'altro con un peso di 20, il gruppo di destinazioni con un peso di 20 riceve il doppio delle richieste rispetto all'altro gruppo di destinazioni.

Fixed-response azioni

È possibile utilizzare le operazioni `fixed-response` per archiviare le richieste client e restituire una risposta HTTP personalizzata. È possibile utilizzare questa azione per restituire un codice di risposta 404 o 500.

Example Esempio di azione a risposta fissa per AWS CLI

È possibile specificare un'azione quando si crea o si aggiorna una regola. L'azione seguente invia una risposta fissa con il codice di stato specificato.

```
"action": {
  "fixedResponse": {
    "statusCode": 404
  },

```

Condizioni della regola

Ogni condizione della regola ha informazioni su tipo e configurazione. Quando le condizioni di una regola vengono soddisfatte, l'operazione viene eseguita.

Di seguito sono riportati i criteri di corrispondenza supportati per una regola:

Corrispondenza dell'intestazione

Il routing si basa sulle intestazioni HTTP per ogni richiesta. Puoi usare le condizioni dell'intestazione HTTP per configurare le regole che instradano le richieste in base alle intestazioni HTTP per la richiesta. Puoi specificare i nomi dei campi delle intestazioni HTTP standard o personalizzate. Il nome dell'intestazione e la valutazione della corrispondenza non fanno distinzione tra maiuscole e minuscole. È possibile modificare questa impostazione attivando la distinzione tra maiuscole e minuscole. I caratteri jolly non sono supportati nel nome dell'intestazione. La corrispondenza tra prefisso, esatto e contiene sono supportate nell'intestazione match.

Match del metodo

Il routing si basa sul metodo di richiesta HTTP di ogni richiesta.

Puoi usare le condizioni del metodo di richiesta HTTP per configurare le regole che instradano le richieste in base al metodo di richiesta HTTP della richiesta. Puoi specificare metodi HTTP standard o personalizzati. Il metodo match fa distinzione tra maiuscole e minuscole. Il nome del metodo deve corrispondere esattamente. I caratteri jolly non sono supportati.

Percorso corrispondente

Il routing si basa sulla corrispondenza dei modelli di percorso negli URL della richiesta.

È possibile utilizzare le condizioni del percorso per definire regole che indirizzano le richieste in base all'URL contenuto nella richiesta. I caratteri jolly non sono supportati. Sono supportati il prefisso e la corrispondenza esatta sul percorso.

Aggiungere una regola

Puoi aggiungere una regola di ascolto in qualsiasi momento.

Per aggiungere una regola di ascolto utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Nella scheda Routing, scegli Modifica listener.
5. Espandi le regole del listener e scegli Aggiungi regola.
6. In Nome regola, immettere un nome per la regola.
7. Per Priorità, inserisci una priorità compresa tra 1 e 100. Le regole vengono valutate in base all'ordine di priorità, dal valore più basso a quello più alto. La regola predefinita è valutata per ultima.
8. Per Condizione, inserite un modello di percorso per la condizione di corrispondenza del percorso. La dimensione massima di ogni stringa è di 200 caratteri. Il confronto non fa distinzione tra maiuscole e minuscole. I caratteri jolly non sono supportati.

Per aggiungere una condizione di corrispondenza dell'intestazione o della regola di corrispondenza del metodo, usa AWS CLI o un AWS SDK.

9. Per Action, scegli un gruppo target VPC Lattice.
10. Scegli Save changes (Salva modifiche).

Per aggiungere una regola usando il AWS CLI

Utilizzate il comando [create-rule](#).

Aggiorna una regola

Puoi aggiornare una regola del listener in qualsiasi momento. È possibile modificarne la priorità, la condizione, il gruppo target e il peso di ciascun gruppo target. Non è possibile modificare il nome della regola.

Per aggiornare una regola del listener utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Nella scheda Routing, scegli Modifica listener.
5. Modifica le priorità, le condizioni e le azioni delle regole secondo necessità.
6. Controlla gli aggiornamenti e scegli Salva modifiche.

Per aggiornare una regola utilizzando il AWS CLI

Utilizzare il comando [update-rule](#).

Eliminare una regola

È possibile eliminare le regole non predefinite per un listener in qualsiasi momento. Non è possibile eliminare la regola predefinita per un listener. Quando si elimina un listener, vengono eliminate tutte le relative regole.

Per eliminare una regola del listener utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.

4. Nella scheda Routing, scegli Modifica listener.
5. Trova la regola e scegli Rimuovi.
6. Scegli Save changes (Salva modifiche).

Per eliminare una regola utilizzando il AWS CLI

Utilizzare il comando [delete-rule](#).

Elimina un listener per il tuo servizio VPC Lattice

Puoi eliminare un listener in qualsiasi momento. Quando si elimina un listener, tutte le sue regole vengono eliminate automaticamente.

Per eliminare un listener utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi.
3. Seleziona il nome del servizio per aprirne la pagina dei dettagli.
4. Nella scheda Routing, scegli Elimina listener.
5. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per eliminare un ascoltatore utilizzando il AWS CLI

Utilizza il comando [delete-listener](#).

Risorse VPC in Amazon VPC Lattice

Puoi condividere le risorse VPC con altri team della tua organizzazione o con partner ISV (Independent Software Vendor) esterni. Una risorsa VPC può essere una risorsa AWS nativa come un database Amazon RDS, un nome di dominio o un indirizzo IP. La risorsa può trovarsi nel tuo VPC o nella rete locale e non è necessario che il carico sia bilanciato. Si usa AWS RAM per specificare i responsabili che possono accedere alla risorsa. Si crea un gateway di risorse attraverso il quale è possibile accedere alla risorsa. È inoltre possibile creare una configurazione di risorse che rappresenti la risorsa o un gruppo di risorse che si desidera condividere.

I responsabili con cui condividi la risorsa possono accedere a queste risorse privatamente utilizzando gli endpoint VPC. Possono utilizzare un endpoint VPC di risorse per accedere a una risorsa o raggruppare più risorse in una rete di servizi VPC Lattice e accedere alla rete di servizi utilizzando un endpoint VPC di rete di servizio.

Le seguenti sezioni spiegano come creare e gestire risorse VPC in VPC Lattice:

Argomenti

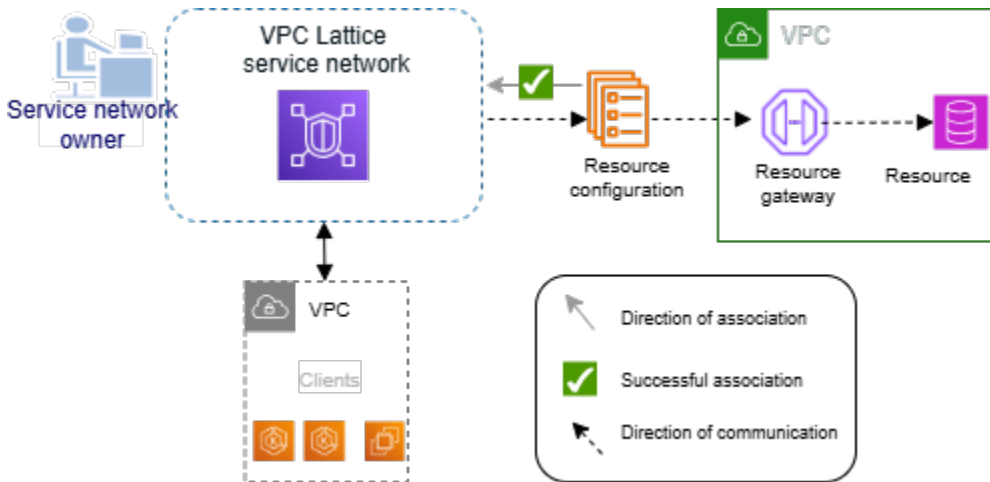
- [Gateway per le risorse in VPC Lattice](#)
- [Configurazioni delle risorse per le risorse VPC](#)

Gateway per le risorse in VPC Lattice

Un gateway di risorse è il punto che riceve il traffico nel VPC in cui risiede una risorsa. Si estende su più zone di disponibilità.

Un VPC deve disporre di un gateway di risorse se prevedi di rendere accessibili le risorse all'interno del VPC da altri VPC o account. Ogni risorsa condivisa è associata a un gateway di risorse. Quando i client di altri VPC o account accedono a una risorsa nel tuo VPC, la risorsa vede il traffico proveniente localmente dal gateway di risorse in quel VPC. L'indirizzo IP di origine del traffico è l'indirizzo IP del gateway di risorse in una zona di disponibilità. È possibile collegare più configurazioni di risorse, ciascuna con più risorse, a un gateway di risorse.

Il diagramma seguente mostra come un client accede a una risorsa tramite il gateway di risorse:



Indice

- [Considerazioni](#)
- [Gruppi di sicurezza](#)
- [Tipi di indirizzi IP](#)
- [Indirizzi IPv4 per ENI](#)
- [Risoluzione DNS di Resource Config](#)
- [Creare un gateway per le risorse in VPC Lattice](#)
- [Eliminare un gateway per le risorse in VPC Lattice](#)

Considerazioni

Le seguenti considerazioni si applicano ai gateway di risorse:

- Affinché la risorsa sia accessibile da tutte le [zone di disponibilità](#), è necessario creare gateway di risorse che coprano il maggior numero possibile di zone di disponibilità.
- Almeno una zona di disponibilità dell'endpoint VPC e del gateway di risorse deve sovrapporsi.
- Un VPC può avere un massimo di 100 gateway di risorse. Per ulteriori informazioni, consulta [Quotas for VPC Lattice](#).
- VPC Lattice potrebbe aggiungere nuovi ENI al tuo gateway di risorse.
- Gateway di risorse con sottoreti VPC condivise:
 - Un gateway di risorse può essere distribuito in una sottorete VPC condivisa solo dall'account proprietario del VPC.

- Una configurazione delle risorse per un gateway di risorse può essere creata solo dall'account proprietario del gateway di risorse.

Gruppi di sicurezza

È possibile collegare gruppi di sicurezza a un gateway di risorse. Le regole dei gruppi di sicurezza per i gateway di risorse controllano il traffico in uscita dal gateway di risorse alle risorse.

Regole in uscita consigliate per il traffico che scorre da un gateway di risorse a una risorsa di database

Affinché il traffico fluisca da un gateway di risorse a una risorsa, è necessario creare regole in uscita per i protocolli di listener e gli intervalli di porte accettati dalla risorsa.

Destinazione	Protocollo	Intervallo porte	Comment
<i>CIDR range for resource</i>	TCP	3306	Consente il traffico dal gateway di risorse ai database.

Tipi di indirizzi IP

Un gateway di risorse può avere indirizzi IPv4, IPv6 o dual-stack. Il tipo di indirizzo IP di un Resource Gateway deve essere compatibile con le sottoreti del Resource Gateway e il tipo di indirizzo IP della risorsa, come descritto di seguito:

- IPv4: assegna gli indirizzi IPv4 alle interfacce di rete del Resource Gateway. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di indirizzi IPv4 e la risorsa dispone anche di un indirizzo IPv4. Quando si utilizza questa opzione, è possibile configurare il numero di indirizzi IPv4 per gateway di risorse ENI.
- IPv6: assegna gli indirizzi IPv6 alle interfacce di rete del tuo Resource Gateway. Questa opzione è supportata solo se tutte le sottoreti selezionate sono subnet solo IPv6 e la risorsa dispone anche di un indirizzo IPv6. Quando si utilizza questa opzione, gli indirizzi IPv6 vengono assegnati automaticamente e non devono essere gestiti.
- Dualstack: assegna indirizzi IPv4 e IPv6 alle interfacce di rete del Resource Gateway. Questa opzione è supportata solo se tutte le sottoreti selezionate hanno intervalli di indirizzi IPv4 e IPv6

e la risorsa dispone di un indirizzo IPv4 o IPv6. Quando si utilizza questa opzione, è possibile configurare il numero di indirizzi IPv4 per gateway di risorse ENI.

Il tipo di indirizzo IP del Resource Gateway è indipendente dal tipo di indirizzo IP del client o dell'endpoint VPC tramite il quale si accede alla risorsa.

Indirizzi IPv4 per ENI

Se il tuo Resource Gateway ha un tipo di indirizzo IP IPv4 o dual-stack, puoi configurare il numero di indirizzi IPv4 assegnati a ciascun ENI del tuo Resource Gateway. Quando crei un resource gateway, scegli da 1 a 62 indirizzi IPv4. Una volta impostato il numero di indirizzi IPv4, il valore non può essere modificato.

Gli indirizzi IPv4 vengono utilizzati per la conversione degli indirizzi di rete e determinano il numero massimo di connessioni IPv4 simultanee a una risorsa. Ogni indirizzo IPv4 può supportare fino a 55.000 connessioni simultanee per IP di destinazione. Per impostazione predefinita, a tutti i gateway di risorse vengono assegnati 16 indirizzi IPv4 per ENI.

Se il gateway di risorse utilizza il tipo di indirizzo IPv6, il gateway di risorse riceve automaticamente un CIDR /80 per ENI. Questo valore non può essere modificato. L'unità di trasmissione massima (MTU) per connessione è di 8500 byte.

Risoluzione DNS di Resource Config

È possibile specificare in che modo un gateway per le risorse esegue la risoluzione DNS per le configurazioni di risorse che sono destinazioni con nomi di dominio. Questa proprietà non è modificabile. È possibile scegliere:

- **PUBLIC** (impostazione predefinita): i nomi di dominio vengono risolti utilizzando resolver DNS pubblici.
- **IN_VPC** - I nomi di dominio vengono risolti utilizzando il server DNS configurato nel set di opzioni DHCP del VPC in cui si trova il gateway di risorse. È consigliabile utilizzarlo se si utilizza un server DNS privato o se le destinazioni dei nomi di dominio si trovano in una zona ospitata privata di Route53.

Se la risoluzione DNS è **IN_VPC**, non è possibile collegare configurazioni di risorse definite da ARN al gateway per le risorse. Non è possibile impostare la risoluzione DNS su **IN_VPC** se il gateway di risorse utilizza sottoreti. IPv6-only

Creare un gateway per le risorse in VPC Lattice

Usa la console per creare un gateway di risorse.

Per creare un gateway di risorse utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Resource gateway.
3. Scegli Crea gateway di risorse.
4. Per il nome del Resource gateway, inserisci un nome univoco all'interno AWS del tuo account.
5. Per Tipo di indirizzo IP, scegli il tipo di indirizzo IP per il Resource Gateway.

- Se hai selezionato IPv4 o Dualstack per il tipo di indirizzo IP, puoi inserire il numero di indirizzi IPv4 per ENI per il tuo Resource Gateway.

L'impostazione predefinita è 16 indirizzi IPv4 per ENI. Si tratta di un numero adeguato di IP per creare connessioni con le risorse di backend.

6. Per VPC, scegli il VPC e le sottoreti in cui creare il tuo gateway di risorse.
7. Per i gruppi di sicurezza, scegli fino a cinque gruppi di sicurezza per controllare il traffico in entrata dal VPC alla rete di servizi.
8. Per Resource Config DNS Resolution, scegli come vuoi che il DNS venga risolto per le destinazioni dei nomi di dominio.
 - Se utilizzi un server DNS privato o le destinazioni dei nomi di dominio si trovano in una zona ospitata privata di Route53, imposta su IN_VPC
9. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
10. Scegli Crea gateway di risorse.

Per creare un gateway di risorse utilizzando ilAWS CLI

Utilizzare il comando [create-resource-gateway](#).

Eliminare un gateway per le risorse in VPC Lattice

Usa la console per eliminare un gateway di risorse.

Per eliminare un gateway di risorse utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Resource gateway.
3. Seleziona la casella di controllo relativa al gateway di risorse che desideri eliminare e scegli Azioni, Elimina. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per eliminare un gateway di risorse utilizzando ilAWS CLI

Utilizzare il comando [delete-resource-gateway](#).

Configurazioni delle risorse per le risorse VPC

Una configurazione di risorse rappresenta una risorsa o un gruppo di risorse che desideri rendere accessibili ai client in altri VPC e account. Definendo una configurazione delle risorse, puoi consentire la connettività di rete privata, sicura e unidirezionale alle risorse del tuo VPC dai client di altri VPC e account. Una configurazione delle risorse è associata a un gateway di risorse attraverso il quale riceve il traffico. Affinché una risorsa sia accessibile da un altro VPC, deve disporre di una configurazione delle risorse.

Indice

- [Tipi di configurazioni delle risorse](#)
- [Protocollo](#)
- [Gateway per le risorse](#)
- [Nomi di dominio personalizzati per i provider di risorse](#)
- [Nomi di dominio personalizzati per consumatori di risorse](#)
- [Nomi di dominio personalizzati per i proprietari di reti di servizi](#)
- [Definizione della risorsa](#)
- [Intervalli di porte](#)
- [Accesso alle risorse](#)
- [Associazione con il tipo di rete di servizi](#)
- [Tipi di reti di servizio](#)
- [Condivisione delle configurazioni delle risorse tramiteAWS RAM](#)

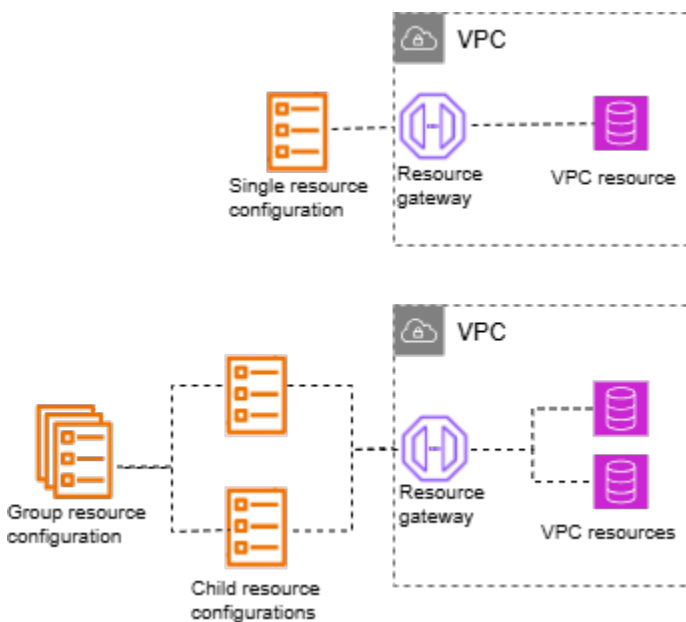
- [Monitoraggio](#)
- [Crea e verifica un dominio](#)
- [Creare una configurazione delle risorse in VPC Lattice](#)
- [Gestire le associazioni per una configurazione di risorse VPC Lattice](#)

Tipi di configurazioni delle risorse

Una configurazione delle risorse può essere di diversi tipi. I diversi tipi aiutano a rappresentare diversi tipi di risorse. I tipi sono:

- Configurazione a risorsa singola: rappresenta un indirizzo IP o un nome di dominio. Può essere condivisa indipendentemente.
- Configurazione delle risorse di gruppo: è una raccolta di configurazioni di risorse secondarie. Può essere utilizzato per rappresentare un gruppo di endpoint DNS e indirizzi IP.
- Configurazione delle risorse secondarie: è un membro di una configurazione di risorse di gruppo. Rappresenta un indirizzo IP o un nome di dominio. Non può essere condiviso indipendentemente; può essere condiviso solo come parte di un gruppo. Può essere aggiunto e rimosso da un gruppo. Una volta aggiunto, è automaticamente accessibile a coloro che possono accedere al gruppo.
- Configurazione delle risorse ARN: rappresenta un tipo di risorsa supportato fornito da un servizio. AWS Qualsiasi relazione gruppo-figlio viene gestita automaticamente.

L'immagine seguente mostra una configurazione di risorse singole, secondarie e di gruppo:



Protocollo

Quando si crea una configurazione delle risorse, è possibile definire i protocolli che la risorsa supporterà. Attualmente è supportato solo il protocollo TCP.

Gateway per le risorse

Una configurazione delle risorse è associata a un gateway di risorse. Un gateway di risorse è un insieme di ENI che fungono da punto di ingresso nel VPC in cui si trova la risorsa. È possibile associare più configurazioni di risorse allo stesso gateway di risorse. Quando i client di altri VPC o account accedono a una risorsa nel tuo VPC, la risorsa vede il traffico proveniente localmente dagli indirizzi IP del gateway di risorse in quel VPC.

Nomi di dominio personalizzati per i provider di risorse

I provider di risorse possono assegnare un nome di dominio personalizzato a una configurazione di risorse, ad esempio `example.com`, quali risorse possono utilizzare gli utenti per accedere alla configurazione delle risorse. Il nome di dominio personalizzato può essere di proprietà e verificato dal provider di risorse oppure può essere di terze parti o di un AWS dominio. I provider di risorse possono utilizzare le configurazioni delle risorse per condividere cluster di cache e cluster Kafka, TLS-based applicazioni o altre risorse. AWS

Le seguenti considerazioni si applicano ai fornitori di configurazioni di risorse:

- Una configurazione di risorse può avere solo un dominio personalizzato.
- Il nome di dominio personalizzato di una configurazione di risorse non può essere modificato.
- Il nome di dominio personalizzato è visibile a tutti gli utenti della configurazione delle risorse.
- Puoi verificare il tuo nome di dominio personalizzato utilizzando il processo di verifica del nome di dominio in VPC Lattice. Per ulteriori informazioni, vedere [the section called "Crea e verifica un dominio"](#)
- Per le configurazioni delle risorse di tipo group e child, è necessario innanzitutto specificare un dominio di gruppo nella configurazione delle risorse di gruppo. Successivamente, le configurazioni delle risorse secondarie possono avere domini personalizzati che sono sottodomini del dominio del gruppo. Se il gruppo non ha un dominio di gruppo, puoi utilizzare qualsiasi nome di dominio personalizzato per il figlio, ma VPC Lattice non fornirà alcuna zona ospitata per i nomi di dominio figlio nel VPC del consumatore di risorse.

Nomi di dominio personalizzati per consumatori di risorse

Quando i consumatori di risorse abilitano la connettività a una configurazione di risorse con un nome di dominio personalizzato, possono consentire a VPC Lattice di gestire una zona ospitata privata Route 53 nel proprio VPC. I consumatori di risorse hanno opzioni granulari per i domini per cui desiderano consentire a VPC Lattice di gestire zone ospitate private.

I consumatori di risorse possono impostare il `private-dns-enabled` parametro quando abilitano la connettività alle configurazioni delle risorse tramite un endpoint di risorse, un endpoint di rete di servizi o un'associazione VPC di rete di servizi. Oltre al `private-dns-enabled` parametro, i consumatori possono utilizzare le opzioni DNS per specificare per quali domini desiderano che VPC Lattice gestisca le zone ospitate private. I consumatori possono scegliere tra le seguenti preferenze DNS private:

ALL_DOMAINS

VPC Lattice fornisce zone ospitate private per tutti i nomi di dominio personalizzati.

VERIFIED_DOMAINS_ONLY

VPC Lattice fornisce una zona ospitata privata solo se il nome di dominio personalizzato è stato verificato dal provider.

VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS

VPC Lattice fornisce zone ospitate private per tutti i nomi di dominio personalizzati verificati e altri nomi di dominio specificati dal consumatore di risorse. Il consumatore di risorse specifica i nomi di dominio nel parametro `private DNS specified domains`

SPECIFIED_DOMAINS_ONLY

VPC Lattice fornisce una zona ospitata privata per i nomi di dominio specificati dal consumatore di risorse. Il consumatore di risorse specifica i nomi di dominio nel parametro `private DNS specified domains`

Quando abiliti il DNS privato, VPC Lattice crea una zona ospitata privata nel tuo VPC per il nome di dominio personalizzato associato alla configurazione delle risorse. Per impostazione predefinita, la preferenza DNS privata è impostata su `VERIFIED_DOMAINS_ONLY`. Ciò significa che le zone private ospitate vengono create solo se il nome di dominio personalizzato è stato verificato dal provider di risorse. Se imposti la preferenza DNS privata su `ALL_DOMAINS` o `SPECIFIED_DOMAINS_ONLY` allora VPC Lattice crea zone ospitate private indipendentemente

dallo stato di verifica del nome di dominio personalizzato. Quando viene creata una zona ospitata privata per un determinato dominio, tutto il traffico verso quel dominio dal tuo VPC viene instradato tramite VPC Lattice. Ti consigliamo di utilizzare le `SPECIFIED_DOMAINS_ONLY` preferenze `ALL_DOMAINS`, `VERIFIED_DOMAINS`, o `AND_SPECIFIED_DOMAINS`, o solo quando desideri che il traffico verso questi nomi di dominio personalizzati passi attraverso VPC Lattice.

Consigliamo ai consumatori di risorse di impostare la propria preferenza DNS privata su `VERIFIED_DOMAINS_ONLY`. Ciò consente ai consumatori di rafforzare il proprio perimetro di sicurezza consentendo a VPC Lattice di fornire zone private ospitate per domini verificati nell'account del consumatore di risorse.

Per selezionare i domini nei domini privati specificati dal DNS, i consumatori di risorse possono inserire un nome di dominio completo, ad esempio o utilizzare un carattere jolly come `my.example.com` o `*.example.com`.

Le seguenti considerazioni si applicano agli utenti che utilizzano configurazioni di risorse:

- Il parametro DNS privato abilitato non può essere modificato.
- Il DNS privato deve essere abilitato su un'associazione di risorse di rete di servizio per l'hosting privato da creare in un VPC. Per una configurazione di risorse, lo stato di abilitazione DNS privato dell'associazione di risorse di rete di servizio ha la precedenza sullo stato di abilitazione DNS privato dell'endpoint della rete di servizio o dell'associazione VPC della rete di servizio.

Per le configurazioni di risorse che sono destinazioni basate su nomi di dominio, non viene creata una voce di zona ospitata privata se sono soddisfatte le seguenti condizioni:

- Il gateway di risorse si trova nello stesso VPC dell'associazione VPC di rete VPC della endpoint/service rete di servizio.
- La risoluzione DNS è impostata su `IN_VPC` sul gateway di risorse.
- Il nome di dominio o il dominio di gruppo personalizzato è lo stesso dominio o il dominio di livello superiore della destinazione del nome di dominio.

Per le configurazioni di risorse di tipo ARN, VPC Lattice non crea una voce di zona ospitata privata se è vero quanto segue:

- Il gateway di risorse si trova nello stesso VPC dell'endpoint VPC della rete di servizio o dell'associazione VPC della rete di servizio.

Nomi di dominio personalizzati per i proprietari di reti di servizi

La proprietà DNS privata abilitata dell'associazione di risorse di rete di servizio ha la precedenza sulla proprietà DNS privata abilitata dell'endpoint della rete di servizio e dell'associazione VPC della rete di servizio.

Se il proprietario di una rete di servizi crea un'associazione di risorse di rete di servizio e non abilita il DNS privato, VPC Lattice non fornirà zone ospitate private per quella configurazione di risorse in nessun VPC a cui è connessa la rete di servizio, anche se il DNS privato è abilitato sull'endpoint della rete di servizio o sulle associazioni VPC della rete di servizio.

Per le configurazioni delle risorse di tipo ARN, il flag DNS privato è vero e immutabile. VPC Lattice fornisce zone ospitate private per i tipi di risorse ARN indipendentemente dall'impostazione della proprietà DNS privata dell'endpoint della rete di servizio e dall'associazione VPC della rete di servizio. L'eccezione è quando il gateway di risorse si trova nello stesso VPC. In altre parole, quando un VPC è sia un consumatore che un provider per una configurazione di risorse di tipo ARN, VPC Lattice salta la creazione delle zone ospitate private in quel VPC.

Definizione della risorsa

Nella configurazione della risorsa, identificate la risorsa in uno dei seguenti modi:

- Con un Amazon Resource Name (ARN): i tipi di risorse supportati, forniti dai AWS servizi, possono essere identificati dal relativo ARN. Sono supportati solo i database Amazon RDS. Non è possibile creare una configurazione delle risorse per un cluster accessibile pubblicamente.
- Per destinazione con nome di dominio: puoi utilizzare qualsiasi nome di dominio. Se utilizzi un server DNS privato o il tuo dominio si trova in una zona ospitata privata di Route53, il gateway di risorse deve avere la risoluzione DNS impostata su IN_VPC. Se il tuo nome di dominio punta a un IP esterno al tuo VPC, devi avere un gateway NAT nel tuo VPC. Domain-name gli obiettivi che si risolvono in indirizzi IPv6 pubblici non sono supportati.
- Con un IP-address: Per IPv4, specificare un IP privato tra i seguenti intervalli: 10.0.0. 0/8, 100.64.0. 0/10, 172,16,0. 0/12, 192,168,0. 0/16. Per IPv6, specifica un IP dal VPC. Gli IP pubblici non sono supportati.

Intervalli di porte

Quando si crea una configurazione di risorse, è possibile definire le porte su cui verranno accettate le richieste. L'accesso del client su altre porte non sarà consentito.

Accesso alle risorse

I consumatori possono accedere alle configurazioni delle risorse direttamente dal proprio VPC utilizzando un endpoint VPC o tramite una rete di servizi. In qualità di consumatore, puoi abilitare l'accesso dal tuo VPC a una configurazione di risorse presente nel tuo account o che è stata condivisa con te da un altro account tramite AWS RAM.

- Accesso diretto a una configurazione delle risorse

Puoi creare un endpoint AWS PrivateLink VPC di tipo risorsa (endpoint di risorse) nel tuo VPC per accedere a una configurazione di risorse in modo privato dal tuo VPC. Per ulteriori informazioni su come creare un endpoint di risorse, consulta [Accesso alle risorse VPC](#) nella guida per AWS PrivateLink l'utente.

- Accesso a una configurazione di risorse tramite una rete di servizi

Puoi associare una configurazione di risorse a una rete di servizi e connettere il tuo VPC alla rete di servizi. Puoi connettere il tuo VPC alla rete di servizio tramite un'associazione o utilizzando un endpoint VPC AWS PrivateLink della rete di servizi.

Per ulteriori informazioni sulle associazioni delle reti di servizio, consulta [Gestire le associazioni per una rete di servizi VPC Lattice](#).

Per ulteriori informazioni sugli endpoint VPC della rete di servizio, consulta [Accedere alle reti di servizio](#) nella guida per l'AWS PrivateLink utente.

Quando il DNS privato è abilitato per il tuo VPC, non puoi creare un endpoint di risorse e un endpoint di rete di servizi per la stessa configurazione di risorse.

Associazione con il tipo di rete di servizi

Quando condividi una configurazione di risorse con un account consumer, ad esempio Account-A AWS RAM, Account-B puoi accedere alla configurazione delle risorse direttamente tramite un endpoint VPC di risorse o tramite una rete di servizi.

Per accedere a una configurazione di risorse tramite una rete di servizi, Account-B è necessario associare la configurazione delle risorse a una rete di servizi. Le reti di servizi sono condivisibili tra account. Quindi, Account-B possono condividere la propria rete di servizi (a cui è associata la configurazione delle risorse) Account-C, rendendo la risorsa accessibile da Account-C.

Per evitare tale condivisione transitiva, è possibile specificare che la configurazione delle risorse non può essere aggiunta alle reti di servizi condivisibili tra account. Se lo specifichi, Account-B non sarà possibile aggiungere la configurazione delle risorse alle reti di servizi che sono condivise o che possono essere condivise con un altro account in futuro.

Tipi di reti di servizio

Quando condividi una configurazione di risorse con un altro account Account-B, ad esempio AWS RAM, tramite Account-B puoi accedere alle risorse specificate nella configurazione delle risorse in tre modi:

- Utilizzo di un endpoint VPC di tipo risorsa (endpoint VPC di risorsa).
- Utilizzo di un endpoint VPC di tipo service network (endpoint VPC della rete di assistenza).
- Utilizzo di un'associazione VPC di rete di servizi.

Quando si utilizza un'associazione di rete di servizio, a ciascuna risorsa viene assegnato un IP per sottorete a partire dalla 129.224.0. 0/17 blocco, che è di proprietà e non è instradabile. AWS Questo si aggiunge all'[elenco di prefissi gestiti](#) che VPC Lattice utilizza per indirizzare il traffico verso i servizi sulla rete VPC Lattice. Entrambi questi IP vengono aggiornati nella tabella di routing VPC.

Per l'endpoint VPC della rete di servizio e l'associazione VPC della rete di servizio, la configurazione delle risorse dovrebbe essere associata a una rete di servizio in Account-B. Le reti di servizi sono condivisibili tra account. Quindi, Account-B possono condividere la loro rete di servizi (che contiene la configurazione delle risorse) con Account-C, rendendo la risorsa accessibile da Account-C. Per evitare tale condivisione transitiva, puoi impedire che la configurazione delle risorse venga aggiunta alle reti di servizi che sono condivisibili tra account. Se non consentite questa opzione, Account-B non sarete in grado di aggiungere la configurazione delle risorse a una rete di servizi condivisa o condivisa con un altro account.

Condivisione delle configurazioni delle risorse tramite AWS RAM

Le configurazioni delle risorse sono integrate con AWS Resource Access Manager. È possibile condividere la configurazione delle risorse con un altro account tramite AWS RAM. Quando condividi una configurazione di risorse con un AWS account, i client di quell'account possono accedere privatamente alla risorsa. È possibile condividere una configurazione di risorse utilizzando una [condivisione di risorse](#) in AWS RAM.

Usa la AWS RAM console per visualizzare le condivisioni di risorse a cui sei stato aggiunto, le risorse condivise a cui puoi accedere e gli AWS account che hanno condiviso risorse con te. Per ulteriori informazioni, consulta [Risorse condivise con te](#) nella Guida AWS RAM per l'utente.

Per accedere a una risorsa da un altro VPC nello stesso account della configurazione della risorsa, non è necessario condividere la configurazione della risorsa tramite AWS RAM.

Monitoraggio

È possibile abilitare i log di monitoraggio sulla configurazione delle risorse. È possibile scegliere una destinazione a cui inviare i log.

Crea e verifica un dominio

Una verifica del nome di dominio è un'entità che ti consente di dimostrare la tua proprietà di un determinato dominio. In qualità di provider di risorse, puoi utilizzare il dominio e i relativi sottodomini come nomi di dominio personalizzati per le configurazioni delle risorse. I consumatori di risorse possono vedere lo stato di verifica del nome di dominio personalizzato quando descrivono la configurazione delle risorse.

Avvia la verifica del dominio

Si avvia la verifica del nome di dominio utilizzando VPC Lattice, quindi si utilizza la zona DNS per completare il processo.

AWS Management Console

Per iniziare la verifica del nome di dominio

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, sotto PrivateLink e Lattice, scegli Verifiche del dominio.
3. Scegli Avvia la verifica del dominio.
4. Per Nome di dominio, inserisci un nome di dominio di tua proprietà.
5. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
6. Scegli Avvia la verifica del nome di dominio.

Dopo aver avviato con successo la verifica del nome di dominio, VPC Lattice restituisce e ilId. txtMethodConfig Utilizzi il txtMethodConfig per completare la verifica del tuo nome di dominio.

AWS CLI

Il start-domain-verification comando seguente avvia una verifica del nome di dominio:

```
aws vpc-lattice start-domain-verification \
  --domain-name example.com
```

L'output sarà simile al seguente:

```
{
  "id": "dv-aaaa00000000111111",
  "arn": "arn:aws:vpc-lattice:us-west-2:111122223333:domainverification/dv-aaaa00000000111111",
  "domainName": "example.com",
  "status": "PENDING",
  "txtMethodConfig": {
    "value": "vpc-lattice:1111aaaaaaaa",
    "name": "_11111aaaaaaaaaa"
  }
}
```

VPC Lattice restituisce e ilId. txtMethodConfig Utilizzi il txtMethodConfig per completare la verifica del tuo nome di dominio. In questo esempio, txtMethodConfig è il seguente:

```
txtMethodConfig": {
  "value": "vpc-lattice:1111aaaaaaaa",
  "name": "_11111aaaaaaaaaa"
}
```

Completa la verifica del nome di dominio

Per completare la verifica del nome di dominio, aggiungi un record TXT nella tua zona DNS. Se usi Route 53, usa la zona ospitata del tuo nome di dominio. Quando verifichi un nome di dominio, vengono verificati anche tutti i sottodomini. Ad esempio, se effettui la verificaexample.com, puoi associare una configurazione di risorse con alpha.example.com e beta.example.com senza eseguire alcuna verifica aggiuntiva.

Per creare un record TXT utilizzando ilAWS Management Console, consulta [Creazione di record utilizzando la console Amazon Route 53](#).

Per creare un record TXT utilizzandoAWS CLIper Route 53

1. Utilizzate il comando [change-resource-record-sets](#) con il seguente file di esempio: TXT-record.json

```
{
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "_1111aaaaaaaa",
        "Type": "TXT",
        "ResourceRecords": [
          {
            "value": "vpc-lattice:1111aaaaaaa"
          }
        ]
      }
    ]
  }
}
```

2. Usa il AWS CLI comando seguente per aggiungere il record TXT del passaggio precedente a una zona ospitata da Route 53:

```
aws route53 change-resource-record-sets \
  --hosted-zone-id ABCD123456 \
  --change-batch file://path/to/your/TXT-record.json
```

hosted-zone-idSostituiscilo con l'ID della zona ospitata Route 53 della zona ospitata nel tuo account. Il valore del parametro change-batch punta a un file JSON (TXT-record.json) in una cartella (path/to/your).

Per verificare lo stato di verifica del tuo nome di dominio, puoi utilizzare la console VPC Lattice o il comando. `get-domain-verification`

Una volta verificato il nome di dominio, questo rimane verificato finché non lo elimini. Se elimini il record TXT dalla tua zona DNS, VPC Lattice lo elimina `verification-id` e devi verificare

nuovamente il nome di dominio. Se elimini il record TXT nella tua zona DNS, VPC Lattice imposta lo stato di verifica del nome di dominio su. UNVERIFIED Ciò non ha alcun impatto sugli endpoint di risorse, sugli endpoint della rete di servizio o sulle associazioni VPC della rete di servizio esistenti alle configurazioni delle risorse. Per verificare nuovamente il tuo nome di dominio, riavvia la procedura di verifica del nome di dominio.

Creare una configurazione delle risorse in VPC Lattice

Crea una configurazione delle risorse.

AWS Management Console

Per creare una configurazione delle risorse utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Configurazioni delle risorse.
3. Scegli Crea configurazione delle risorse.
4. Inserisci un nome univoco all'interno del tuo AWS account. Non puoi modificare questo nome dopo aver creato la configurazione delle risorse.
5. Per Tipo di configurazione, scegli Risorsa per una risorsa singola o secondaria o Gruppo di risorse per un gruppo di risorse secondarie.
6. Scegli un gateway di risorse che hai creato in precedenza o creane uno ora.
7. (Facoltativo) Per inserire un nome di dominio personalizzato, effettuate una delle seguenti operazioni:
 - Se disponi di una configurazione delle risorse di tipo single, puoi inserire un nome di dominio personalizzato. I consumatori di risorse possono utilizzare questo nome di dominio per accedere alle configurazioni delle risorse.
 - Se disponi di una configurazione delle risorse di tipo group e child, devi prima specificare un dominio di gruppo nella configurazione delle risorse di gruppo. Successivamente, le configurazioni delle risorse secondarie possono avere domini personalizzati che sono sottodomini del dominio del gruppo.
8. (Facoltativo) Inserisci l'ID di verifica.

Fornisci un ID di verifica se desideri che il tuo nome di dominio venga verificato. Ciò consente ai consumatori di risorse di sapere che il nome di dominio è tuo.

9. Scegliete l'identificatore per la risorsa che desiderate che questa configurazione di risorse rappresenti.
10. Scegliete gli intervalli di porte attraverso i quali desiderate condividere la risorsa.
11. Per le impostazioni di associazione, specifica se questa configurazione delle risorse può essere associata a reti di servizi condivisibili.
12. Per la configurazione di condivisione delle risorse, scegli le condivisioni di risorse che identificano i principali che possono accedere a questa risorsa.
13. (Facoltativo) Per il monitoraggio, abilita i registri di accesso alle risorse e la destinazione di consegna se desideri monitorare le richieste e le risposte da e verso la configurazione delle risorse.
14. (Facoltativo) Per aggiungere un tag, scegliere Add new tag (Aggiungi nuovo tag) e immettere la chiave e il valore del tag.
15. Scegli Crea configurazione delle risorse.

AWS CLI

Il seguente comando [create-resource-configuration crea una singola configurazione](#) di risorse e la associa al nome di dominio personalizzato. `example.com`

```
aws vpc-lattice create-resource-configuration \
  --name my-resource-config \
  --type SINGLE \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}' \
  --custom-domain-name example.com \
  --verification-id dv-aaaa000000011111
```

Il seguente comando [create-resource-configuration crea una configurazione di risorse di gruppo e la associa al nome di](#) dominio personalizzato. `example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-group \
  --type GROUP \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --domain-verification-identifier dv-aaaa000000011111
```

Il seguente comando [create-resource-configuration crea una configurazione di risorse secondarie e la associa al nome di](#) dominio personalizzato. `child.example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \  
  --name my-custom-dns-resource-config-child \  
  --type CHILD \  
  --resource-configuration-definition 'dnsResource={domainName=my-alb-123456789.us-  
west-2.elb.amazonaws.com,ipAddressType=IPv4}' \  
  --resource-configuration-group-identifier rcfg-07129f3acded87626 \  
  --custom-domain-name child.example.com
```

Gestire le associazioni per una configurazione di risorse VPC Lattice

Gli account consumer con cui condividi una configurazione di risorse e i client del tuo account possono accedere alla configurazione delle risorse direttamente utilizzando un endpoint VPC di tipo risorsa o tramite un endpoint VPC di tipo servizio-rete. Di conseguenza, la configurazione delle risorse avrà associazioni di endpoint e associazioni di reti di servizi.

Gestisci le associazioni di risorse della rete di servizio

Creare o eliminare un'associazione di rete di servizio.

Note

Se ricevi un messaggio di accesso negato durante la creazione dell'associazione tra la rete di servizio e la configurazione delle risorse, controlla la versione AWS RAM della tua policy e assicurati che sia la versione 2. Per ulteriori informazioni, consulta la guida per l'[AWS RAM utente](#).

Per gestire un'associazione servizio-rete utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, sotto PrivateLink e Lattice, scegli Configurazioni delle risorse.
3. Seleziona il nome della configurazione della risorsa per aprirne la pagina dei dettagli.
4. Seleziona la scheda Associazioni di rete di servizio.
5. Scegli Crea associazioni.
6. Seleziona una rete di servizi dalle reti di servizi VPC Lattice. Per creare una rete di servizi, scegli Crea una rete VPC Lattice.

7. (Facoltativo) Per aggiungere un tag, espandi Service Association tags, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
8. (Facoltativo) Per abilitare i nomi DNS privati per questa associazione di risorse di rete di servizio, scegli abilita il nome DNS privato. Per ulteriori informazioni, consulta [the section called “Nomi di dominio personalizzati per i proprietari di reti di servizi”](#).
9. Scegli Salva modifiche.
10. Per eliminare un'associazione, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Elimina. Quando viene richiesta la conferma, immettere **confirm** e quindi scegliere Elimina.

Per creare un'associazione di rete di servizi utilizzando AWS CLI

Utilizzare il comando [create-service-network-resource-association](#).

Per eliminare un'associazione di rete di servizi utilizzando il AWS CLI

Utilizzare il comando [delete-service-network-resource-association](#).

Gestisci le associazioni degli endpoint VPC delle risorse

Gli account consumer con accesso alla configurazione delle risorse o i client nel tuo account possono accedere alla configurazione delle risorse utilizzando un endpoint VPC di risorse. Se la configurazione delle risorse ha un nome di dominio personalizzato, puoi utilizzare abilita il DNS privato per consentire a VPC Lattice di fornire zone ospitate private per l'endpoint di risorse o l'endpoint della rete di servizi. In questo modo, i client possono modificare direttamente il nome di dominio per accedere alla configurazione delle risorse. Per ulteriori informazioni, consulta [the section called “Nomi di dominio personalizzati per consumatori di risorse”](#).

AWS Management Console

1. Per creare una nuova associazione di endpoint, vai su PrivateLink and Lattice nel riquadro di navigazione a sinistra e scegli Endpoints.
2. Scegli Crea endpoint.
3. Seleziona la configurazione delle risorse che desideri connettere al tuo VPC.
4. Seleziona il VPC, le sottoreti e i gruppi di sicurezza.
5. (Facoltativo) Per attivare il DNS privato e configurare le opzioni DNS, seleziona Abilita nome DNS privato.

6. (Facoltativo) Per taggare il tuo endpoint VPC, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.
7. Seleziona Crea endpoint.

AWS CLI

Il seguente comando [create-vpc-endpoint crea un endpoint](#) VPC che utilizza DNS privato. Le preferenze DNS private sono impostate su e i domini selezionati sono e. VERIFIED_AND_SELECTED example.com example.org VPC Lattice fornisce solo zone ospitate private per qualsiasi dominio verificato o o. example.com example.org

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Resource \
  --vpc-id vpc-111122223333aabbcc \
  --subnet-ids subnet-0011aabbcc2233445 \
  --resource-configuration-arn arn:aws:vpc-lattice:us-
west-2:111122223333:resourceconfiguration/rcfg-07129f3acded87625 \
  --private-dns-enabled \
  --private-dns-preferences VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS \
  --private-domains-set example.com, example.org
```

Per creare un'associazione di endpoint VPC utilizzando AWS CLI

Utilizzare il comando [create-vpc-endpoint](#).

Per eliminare un'associazione di endpoint VPC utilizzando AWS CLI

Utilizzare il comando [delete-vpc-endpoint](#).

Condivisione delle entità di VPC Lattice

Amazon VPC Lattice si integra con AWS Resource Access Manager (AWS RAM) per consentire la condivisione di servizi, configurazioni di risorse e reti di servizi. AWS RAM è un servizio che consente di condividere alcune entità VPC Lattice con altre Account AWS o tramite AWS Organizations. Con AWS RAM, condividi le entità di tua proprietà creando una condivisione di risorse. Una condivisione di risorse specifica le entità da condividere e i consumatori con cui condividerle. I consumatori includono:

- Specifico Account AWS all'interno o all'esterno della sua organizzazione in AWS Organizations.
- Un'unità organizzativa all'interno dell'organizzazione in AWS Organizations.
- Un'intera organizzazione in AWS Organizations.

Per ulteriori informazioni in merito AWS RAM, consulta la [Guida AWS RAM per l'utente](#).

Indice

- [Prerequisiti per la condivisione di entità VPC Lattice](#)
- [Condividi entità VPC Lattice](#)
- [Interrompi la condivisione di entità VPC Lattice](#)
- [Responsabilità e autorizzazioni](#)
- [Eventi multi-account](#)

Prerequisiti per la condivisione di entità VPC Lattice

- Per condividere un'entità, devi possederla nel tuo Account AWS. Ciò significa che l'entità deve essere allocata o fornita nel tuo account. Non puoi condividere un'entità che è stata condivisa con te.
- Per condividere un'entità con la tua organizzazione o un'unità organizzativa AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta [Abilitare la condivisione delle risorse con AWS Organizations](#) nella Guida per l'utente di AWS RAM.

Condividi entità VPC Lattice

Per condividere un'entità, inizia creando una condivisione di risorse utilizzando AWS Resource Access Manager. Una condivisione di risorse specifica le entità da condividere, i consumatori con cui vengono condivise e quali azioni possono eseguire i responsabili.

Quando condividi un'entità VPC Lattice di tua proprietà con altri Account AWS, consenti a tali account di associare le loro entità alle entità del tuo account. Quando crei un'associazione con un'entità condivisa, generiamo un Amazon Resource Name (ARN) nell'account del proprietario dell'entità e nell'account che ha creato l'associazione. Pertanto, sia il proprietario dell'entità che l'account che ha creato l'associazione possono eliminare l'associazione.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso all'entità condivisa. In caso contrario, i consumatori ricevono un invito a partecipare alla condivisione delle risorse e ottengono l'accesso all'entità condivisa dopo aver accettato l'invito.

Considerazioni

- Puoi condividere tre tipi di entità VPC Lattice: reti di servizi, servizi e configurazioni di risorse.
- Puoi condividere le tue entità VPC Lattice con chiunque. Account AWS
- Non puoi condividere le tue entità VPC Lattice con singoli utenti e ruoli IAM.
- VPC Lattice supporta le autorizzazioni gestite dal cliente per servizi, configurazioni di risorse e reti di servizi.

Per condividere un'entità di tua proprietà utilizzando la console VPC Lattice

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi, Reti di servizio o Configurazioni di risorse.
3. Scegli il nome dell'entità per aprire la relativa pagina dei dettagli, quindi scegli Condividi servizio, Condividi rete di servizi o Condividi configurazione delle risorse dalla scheda Condivisione.
4. Scegli le condivisioni di AWS RAM risorse da Condivisioni di risorse. Per creare una condivisione di risorse, scegli Crea una condivisione di risorse nella console RAM.
5. Scegli Condividi servizio, Condividi rete di servizi o Condividi configurazione delle risorse.

Per condividere un'entità di tua proprietà utilizzando la AWS RAM console

Usa la procedura descritta in [Creare una condivisione di risorse](#) nella Guida AWS RAM per l'utente.

Per condividere un'entità di tua proprietà utilizzando il AWS CLI

Utilizza il comando [associate-resource-share](#).

Interrompi la condivisione di entità VPC Lattice

Per interrompere la condivisione di un'entità VPC Lattice di tua proprietà, devi rimuoverla dalla condivisione di risorse. Le associazioni esistenti persistono dopo l'interruzione della condivisione dell'entità. Non sono consentite nuove associazioni a un'entità precedentemente condivisa. Quando il proprietario dell'entità o il proprietario dell'associazione elimina un'associazione, questa viene eliminata da entrambi gli account. Se il proprietario di un account desidera abbandonare una condivisione di risorse, deve chiedere al proprietario della condivisione di risorse di rimuovere il proprio account dall'elenco degli account con cui è stata condivisa la risorsa.

Per interrompere la condivisione di un'entità di tua proprietà utilizzando la console VPC Lattice

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi, Reti di servizio o Configurazioni di risorse.
3. Scegli il nome dell'entità per aprire la pagina dei dettagli.
4. Nella scheda Condivisione, seleziona la casella di controllo relativa alla condivisione delle risorse, quindi scegli Rimuovi.

Per interrompere la condivisione di un'entità di tua proprietà utilizzando la AWS RAM console

Consulta [Update a resource share](#) nella Guida per l'utente di AWS RAM .

Per interrompere la condivisione di un'entità di tua proprietà, utilizza il AWS CLI

Utilizza il comando [disassociate-resource-share](#).

Responsabilità e autorizzazioni

Le seguenti responsabilità e autorizzazioni si applicano quando si utilizzano entità VPC Lattice condivise.

Proprietari delle entità

- Il proprietario della rete di servizi non può modificare un servizio creato da un consumatore.
- Il proprietario della rete di assistenza non può eliminare un servizio creato da un consumatore.
- Il proprietario della rete di assistenza può descrivere tutte le associazioni di servizi per la rete di assistenza.
- Il proprietario della rete di assistenza può dissociare qualsiasi servizio associato alla rete di servizi, indipendentemente da chi ha creato l'associazione.
- Il proprietario della rete di servizi può descrivere tutte le associazioni VPC per la rete di servizi.
- Il proprietario della rete di servizi può dissociare qualsiasi VPC associato da un consumatore alla rete di servizio.
- Il proprietario della rete di assistenza può descrivere tutte le associazioni di configurazione delle risorse per la rete di servizio.
- Il proprietario della rete di servizi può dissociare qualsiasi configurazione di risorse associata alla rete di servizio, indipendentemente da chi ha creato l'associazione.
- Il proprietario della rete di servizi può descrivere tutte le associazioni di endpoint per la rete di servizi.
- Il proprietario della rete di servizi può dissociare qualsiasi endpoint associato alla rete di servizio, indipendentemente da chi ha creato l'associazione.
- Il proprietario del servizio può descrivere tutte le associazioni della rete di servizio con il servizio.
- Il proprietario del servizio può dissociare un servizio da qualsiasi rete di assistenza a cui è associato.
- Il proprietario della configurazione delle risorse può descrivere tutte le associazioni di rete con la configurazione delle risorse.
- Il proprietario della configurazione delle risorse può dissociare una configurazione di risorse da qualsiasi rete di servizio a cui è associata.
- Il proprietario dell'endpoint VPC può descrivere la rete di servizi a cui è associato.
- Il proprietario dell'endpoint VPC può dissociare un endpoint dalla rete di servizi.
- Solo l'account che ha creato un'associazione può aggiornare l'associazione tra la rete di servizi e il VPC.

Consumatori dell'entità

- Il consumatore non può eliminare una configurazione di servizio o di risorse che non ha creato.
- Il consumatore può dissociare solo i servizi o le configurazioni di risorse che ha associato a una rete di servizi.
- Il consumatore e il proprietario della rete possono descrivere tutte le associazioni tra una rete di servizi e una configurazione di servizi o risorse.
- Il consumatore non può recuperare le informazioni di servizio relative a un servizio o le informazioni sulla configurazione di una risorsa di cui non è proprietario.
- Il consumatore può descrivere tutte le associazioni di servizi e le associazioni di configurazioni di risorse con una rete di servizi condivisa.
- Il consumatore può associare una configurazione di servizio o di risorse a una rete di servizi condivisa.
- Il consumatore può vedere tutte le associazioni VPC con una rete di servizi condivisa.
- Il consumatore può associare un VPC a una rete di servizi condivisa.
- Il consumatore può dissociare solo VPCs ciò che ha associato a una rete di servizi.
- Il consumatore può creare un endpoint VPC della rete di servizio per connettere il proprio VPC a una rete di servizi condivisa.
- Il consumatore può eliminare solo l'endpoint VPC della rete di servizio che ha creato per connettere il proprio VPC a una rete di servizi condivisa.
- Il consumatore di un servizio condiviso non può associare un servizio a una rete di servizi di cui non è proprietario.
- L'utente di una rete di servizi condivisa non può associare un VPC o un servizio di cui non è proprietario.
- L'utente di una configurazione di risorse condivise non può associare una configurazione di risorse a una rete di servizi di cui non è proprietario.
- L'utente di una rete di servizi condivisa non può associare un VPC o una configurazione di servizi o risorse di cui non è proprietario.
- Il consumatore può descrivere un servizio, una rete di servizi o una configurazione di risorse condivisa con lui.
- Il consumatore non può associare due entità se entrambe sono condivise con lui.

Eventi multi-account

Quando i proprietari e i consumatori dell'entità eseguono azioni su un'entità condivisa, tali azioni vengono registrate come eventi interaccount in AWS CloudTrail.

CreateServiceNetworkResourceAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama `CreateServiceNetworkResourceAssociation` con un'entità condivisa. Se il chiamante possiede la configurazione delle risorse, l'evento viene inviato al proprietario della rete di servizi. Se il chiamante è proprietario della rete di servizi, l'evento viene inviato al proprietario della configurazione delle risorse.

CreateServiceNetworkServiceAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [CreateServiceNetworkServiceAssociation](#) con un'entità condivisa. Se il chiamante è proprietario del servizio, l'evento viene inviato al proprietario della rete di assistenza. Se il chiamante è proprietario della rete di assistenza, l'evento viene inviato al proprietario del servizio.

CreateServiceNetworkVpcAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [CreateServiceNetworkVpcAssociation](#) con una rete di servizi condivisa.

DeleteServiceNetworkResourceAssociationByOwner

Inviato al proprietario dell'associazione quando il proprietario dell'entità chiama `DeleteServiceNetworkResourceAssociation` con un'entità condivisa. Se il chiamante possiede la configurazione delle risorse, l'evento viene inviato al proprietario dell'associazione della rete di servizio. Se il chiamante è proprietario della rete di servizi, l'evento viene inviato al proprietario dell'associazione di risorse.

DeleteServiceNetworkResourceAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama `DeleteServiceNetworkResourceAssociation` con un'entità condivisa. Se il chiamante possiede la configurazione delle risorse, l'evento viene inviato al proprietario della rete di servizi. Se il chiamante è proprietario della rete di servizi, l'evento viene inviato al proprietario della configurazione delle risorse.

DeleteServiceNetworkServiceAssociationByOwner

Inviato al proprietario dell'associazione quando il proprietario dell'entità chiama [DeleteServiceNetworkServiceAssociation](#) con un'entità condivisa. Se il chiamante è proprietario del servizio, l'evento viene inviato al proprietario dell'associazione della rete di servizio. Se il chiamante è proprietario della rete di servizi, l'evento viene inviato al proprietario dell'associazione di servizio.

DeleteServiceNetworkServiceAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [DeleteServiceNetworkServiceAssociation](#) con un'entità condivisa. Se il chiamante è proprietario del servizio, l'evento viene inviato al proprietario della rete di assistenza. Se il chiamante è proprietario della rete di assistenza, l'evento viene inviato al proprietario del servizio.

DeleteServiceNetworkVpcAssociationByOwner

Inviato al proprietario dell'associazione quando il proprietario dell'entità chiama [DeleteServiceNetworkVpcAssociation](#) con una rete di servizi condivisa.

DeleteServiceNetworkVpcAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [DeleteServiceNetworkVpcAssociation](#) con una rete di servizi condivisa.

GetServiceBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [GetService](#) con un servizio condiviso.

GetServiceNetworkBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [GetServiceNetwork](#) con una rete di servizi condivisa.

GetServiceNetworkResourceAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [GetServiceNetworkResourceAssociation](#) con un'entità condivisa. Se il chiamante possiede la configurazione delle risorse, l'evento viene inviato al proprietario della rete di servizi. Se il chiamante è proprietario della rete di servizi, l'evento viene inviato al proprietario della configurazione delle risorse.

GetServiceNetworkServiceAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [GetServiceNetworkServiceAssociation](#) con un'entità condivisa. Se il chiamante è proprietario del servizio, l'evento viene inviato al proprietario della rete di assistenza. Se il chiamante è proprietario della rete di assistenza, l'evento viene inviato al proprietario del servizio.

GetServiceNetworkVpcAssociationBySharee

Inviato al proprietario dell'entità quando un consumatore dell'entità chiama [GetServiceNetworkVpcAssociation](#) con una rete di servizi condivisa.

Di seguito è riportato un esempio di voce relativa all'`CreateServiceNetworkServiceAssociationBySharee` evento.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown"
  },
  "eventTime": "2023-04-27T17:12:46Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateServiceNetworkServiceAssociationBySharee",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "vpc-lattice.amazonaws.com",
  "userAgent": "ec2.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "callerAccountId": "111122223333"
  },
  "requestID": "ddabb0a7-70c6-4f70-a6c9-00cbe8a6a18b",
  "eventID": "bd03cdca-7edd-4d50-b9c9-aaa89f4a47cd",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::VpcLattice::ServiceNetworkServiceAssociation",
      "ARN": "arn:aws:vpc-lattice:region:123456789012:servicenetworkserviceassociation/snsa-0d5ea7bc72EXAMPLE"
    }
  ],
  "eventType": "AwsServiceEvent",
}
```

```
"managementEvent": true,  
"recipientAccountId": "123456789012",  
"eventCategory": "Management"  
}
```

Lattice VPC per Oracle Database@AWS

VPC Lattice AWS alimenta le integrazioni di servizi gestiti per [Oracle Database@AWS](#) (ODB) e offre una connettività semplificata tra la rete ODB e on-premise. AWS VPCs Per supportare questa connettività, VPC Lattice fornisce le seguenti entità per tuo conto:

Rete di servizio predefinita

La rete di servizi predefinita utilizza la convenzione di denominazione `default-odb-network-randomHash`

Endpoint di rete di servizio predefinito

Non esiste un nome per questa risorsa. AWS

Gateway per le risorse

Il Resource Gateway utilizza la convenzione di denominazione `default-odb-network-randomHash`

VPC Lattice supporta integrazioni di servizi AWS gestiti, denominate integrazioni gestite nella rete ODB. Per impostazione predefinita, il backup gestito di Oracle Cloud Infrastructure (OCI) su Amazon S3 è abilitato. Puoi scegliere di abilitare l'accesso autogestito ad Amazon S3 e Zero-ETL.

Una volta creata la rete ODB, puoi visualizzare le risorse fornite utilizzando o. AWS Management Console AWS CLI Il comando di esempio seguente elenca le integrazioni gestite predefinite della rete ODB e tutte le altre risorse disponibili per questa rete di servizi:

```
aws vpc-lattice list-service-network-resource-associations \
  --service-network-identifier default-odb-network-randomHash
```

Considerazioni

Le seguenti considerazioni si applicano a VPC Lattice per: Oracle Database@AWS

- Non è possibile eliminare la rete di servizio predefinita, l'endpoint della rete di servizi, il gateway di risorse o qualsiasi integrazione gestita ODB fornita da VPC Lattice. Per eliminare queste entità, elimina la rete ODB o disabilita le integrazioni gestite.

- I client possono accedere solo alle integrazioni gestite nella rete ODB. I client esterni alla rete ODB, ad esempio la tua VPCs, non possono utilizzare queste integrazioni gestite per accedere a S3 o Zero-ETL.
- Non è possibile connettersi a nessuna delle integrazioni gestite al di fuori della rete ODB fornita da VPC Lattice.
- Tutto il traffico verso Amazon S3 passa attraverso l'endpoint di rete di servizio predefinito e vengono applicati i costi di elaborazione standard per l'accesso alle risorse. Tutto il traffico zero-ETL passa attraverso il gateway di risorse e vengono applicate le tariffe standard di elaborazione dei dati per le risorse condivise. Per ulteriori informazioni, consulta i prezzi di [VPC Lattice](#).
- Non sono previsti costi orari per Oracle Database@AWS le integrazioni gestite.
- Puoi gestire le risorse fornite da VPC Lattice proprio come qualsiasi altra rete di servizi. È possibile condividere la rete di servizi predefinita con altre Account AWS organizzazioni e aggiungere nuovi endpoint, associazioni VPC, servizi e risorse VPC Lattice alla rete predefinita.
- Le seguenti autorizzazioni sono necessarie per consentire a VPC Lattice di effettuare il provisioning delle risorse: Oracle Database@AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowODBEC2andLatticeActions",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:CreateTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateOdbNetworkPeering",
        "ec2>DeleteOdbNetworkPeering",
        "ec2:ModifyOdbNetworkPeering",
        "ec2:DescribeVpcEndpointAssociations",
        "ec2:CreateVpcEndpoint",
        "ec2>DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "vpc-lattice:CreateServiceNetwork",
        "vpc-lattice>DeleteServiceNetwork",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:CreateServiceNetworkResourceAssociation",
        "vpc-lattice>DeleteServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkResourceAssociation",

```

```

        "vpc-lattice:CreateResourceGateway",
        "vpc-lattice:DeleteResourceGateway",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:CreateServiceNetworkVpcEndpointAssociation"
    ],
    "Effect": "Allow",
    "Resource": "*"
  },
  {
    "Sid": "AllowSLRActionsForLattice",
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "vpc-lattice.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Per utilizzare VPC Lattice for Oracle Database@AWS, ti consigliamo di conoscere le reti di servizio, le [associazioni di reti di servizio e i gateway di](#) risorse in VPC Lattice.

Argomenti

- [the section called “Backup gestito dell'infrastruttura Oracle Cloud \(OCI\) su Amazon S3”](#)
- [the section called “Accesso ad Amazon S3”](#)
- [the section called “Zero-ETL per Amazon Redshift”](#)
- [the section called “Accedi e condividi entità VPC Lattice”](#)

Backup gestito dell'infrastruttura Oracle Cloud (OCI) su Amazon S3

Quando si crea un Oracle Database@AWS database, VPC Lattice crea una configurazione di risorse chiamata. odb-managed-s3-backup-access Questa configurazione delle risorse rappresenta un

backup gestito da OCI dei database su Amazon S3 e consente solo la connettività ai bucket Amazon S3 di proprietà di OCI. Il traffico tra la rete ODB e S3 non esce mai dalla rete Amazon.

Accesso ad Amazon S3

Oltre a OCI Managed Backup to Amazon S3, puoi creare un'integrazione gestita che consente l'accesso ad Amazon S3 dalla rete ODB. Quando modifichi la Oracle Database@AWS rete per abilitare l'integrazione gestita di Amazon S3 Access, VPC Lattice fornisce una configurazione delle risorse chiamata `odb-s3-access` nella rete di servizio predefinita. Puoi utilizzare questa integrazione per accedere ad Amazon S3 per le tue esigenze, inclusi backup o ripristini autogestiti. Puoi stabilire il controllo perimetrale fornendo una politica di autenticazione.

Considerazioni

Di seguito sono riportate le considerazioni relative all'integrazione gestita di Amazon S3 Access:

- Puoi creare una sola integrazione gestita di Amazon S3 Access per la rete ODB.
- Questa integrazione gestita consente l'accesso ad Amazon S3 solo dalla rete ODB e non da altre associazioni VPC o endpoint di rete di servizi nella rete di servizi predefinita.
- Non puoi accedere ai bucket S3 in diverse regioni. AWS

Abilita l'integrazione gestita di Amazon S3 Access

Utilizza il seguente comando per abilitare l'integrazione gestita di Amazon S3 Access:

```
aws odb update-odb-network \  
  --odb-network-id odb-network-id \  
  --s3-access ENABLED
```

Accesso sicuro con una politica di autenticazione

Puoi proteggere l'accesso ai bucket S3 definendo una politica di autenticazione utilizzando l'API ODB. La seguente politica di esempio concede l'accesso a specifici bucket S3 di proprietà di un'organizzazione specifica.

JSON

```
{
```

```
"Version": "2012-10-17",
"Id": "Policy1515115909152",
"Statement": [
  {
    "Sid": "GrantAccessToMyOrgS3",
    "Principal": "*",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::awsexamplebucket1",
      "arn:aws:s3:::awsexamplebucket1/*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:ResourceOrgID": "o-abcd1234"
      }
    }
  }
]
```

Note

Le chiavi `aws:SourceVpc`, `aws:SourceVpcId`, e `aws:VpcSourceIp` condition non sono supportate per le policy dei bucket S3 quando si utilizzano integrazioni gestite da ODB.

Zero-ETL per Amazon Redshift

[È possibile utilizzare la rete di servizi fornita da VPC Lattice per abilitare Zero-ETL.](#) Questa integrazione gestita collega i database di rete ODB ad Amazon Redshift per facilitare l'analisi dei dati su diversi database. Puoi avviare la configurazione zero-ETL utilizzando l' AWS Glue integrazione APIs e utilizzare l'ODB APIs per attivare l'integrazione gestita e configurare il percorso di rete. Per ulteriori informazioni, consulta l'[integrazione Zero-ETL con Amazon Redshift](#).

Considerazioni

Di seguito sono riportate le considerazioni relative all'integrazione zero-ETL gestita:

- Se abiliti l'integrazione zero-ETL gestita, puoi utilizzare zero-ETL solo per accedere alle istanze nella tua rete ODB. Gli altri servizi e risorse associati alla rete di assistenza sono isolati da Zero-ETL.

Accedi e condividi entità VPC Lattice

Puoi anche connettere la tua rete ODB a servizi, risorse e altri client VPCs utilizzando VPC Lattice. Queste opzioni di connettività sono alimentate tramite la rete di servizio predefinita, il gateway di risorse e l'endpoint della rete di servizi forniti da VPC Lattice.

Accedi ai servizi e alle risorse VPC Lattice

Per accedere ad altre entità, associa servizi o risorse di tua proprietà o condivisi con te alla rete di servizi predefinita. I client nella rete ODB possono accedere ai servizi o alle risorse tramite l'endpoint di rete di servizio predefinito.

Considerazioni

Di seguito sono riportate le considerazioni relative alla connessione ad altre entità VPC Lattice:

- È possibile aggiungere nuovi endpoint di rete di servizi, associazioni VPC, risorse e servizi VPC Lattice alla rete di servizi, ma non è possibile modificare le risorse fornite da VPC Lattice per conto della rete ODB. Queste Oracle Database@AWS APIs devono essere gestite tramite.

Condividi la tua rete ODB tramite VPC Lattice

È possibile condividere le risorse di rete ODB con i clienti che utilizzano altri VPCs account o in locale. Per iniziare, crea una configurazione delle risorse per le risorse che desideri condividere. Le configurazioni delle risorse devono utilizzare il gateway di risorse predefinito per la rete ODB. È quindi possibile associare le risorse alla rete di servizi predefinita.

I clienti di un'altra rete di servizi VPCs o con Account AWS cui hai condiviso la tua rete di servizi possono accedere a queste risorse tramite i propri endpoint della rete di servizio o le associazioni VPC. Per ulteriori informazioni, consulta [the section called "Gestisci le associazioni"](#).

Considerazioni

Di seguito sono riportate alcune considerazioni sulla condivisione della rete ODB:

- Consigliamo di condividere solo le istanze di rete ODB come risorse basate su IP.
- VPC Lattice non supporta il DNS del listener SCAN (Single Client Access Name) di OCI.

Sicurezza in Amazon VPC Lattice

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

L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi in. AWS Cloud AWS AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. Third-party i revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei [AWS Programmi di AWS conformità dei Programmi di conformità](#) dei di . Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon VPC Lattice, consulta [AWS Services in Scope by Compliance Program by Compliance Program](#).
- Sicurezza nel cloud: sei responsabile del mantenimento del controllo sui contenuti ospitati su questa infrastruttura. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi VPC Lattice. I seguenti argomenti mostrano come configurare VPC Lattice per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi, che ti aiutano a monitorare e proteggere il servizio VPC Lattice, le reti di servizio e le configurazioni delle risorse.

Indice

- [Gestisci l'accesso ai servizi VPC Lattice](#)
- [Protezione dei dati in Amazon VPC Lattice](#)
- [Gestione delle identità e degli accessi per Amazon VPC Lattice](#)
- [Convalida della conformità per Amazon VPC Lattice](#)
- [Accedi ad Amazon VPC Lattice utilizzando gli endpoint di interfaccia \(AWS PrivateLink\)](#)
- [Resilienza in Amazon VPC Lattice](#)
- [Sicurezza dell'infrastruttura in Amazon VPC Lattice](#)

Gestisci l'accesso ai servizi VPC Lattice

VPC Lattice è sicuro di default perché devi essere esplicito su quali servizi e configurazioni di risorse fornire l'accesso e con quali VPC. È possibile accedere ai servizi tramite un'associazione VPC o un endpoint VPC di tipo rete di servizio. Per scenari con più account, è possibile utilizzare [AWS Resource Access Manager](#) per condividere servizi, configurazioni di risorse e reti di servizi oltre i limiti degli account.

VPC Lattice fornisce un framework che consente di implementare una defense-in-depth strategia su più livelli della rete.

- Primo livello: associazione del servizio, della risorsa, del VPC e dell'endpoint VPC con una rete di servizi. Un VPC può essere connesso a una rete di servizi tramite un'associazione o tramite un endpoint VPC. Se un VPC non è connesso a una rete di servizi, i client nel VPC non possono accedere alle configurazioni di servizi e risorse associate alla rete di servizi.
- Secondo livello: protezioni di sicurezza opzionali a livello di rete per la rete di servizi, come gruppi di sicurezza e ACL di rete. Usandoli, puoi consentire l'accesso a gruppi specifici di client in un VPC anziché a tutti i client nel VPC.
- Terzo livello: policy di autenticazione VPC Lattice opzionale. È possibile applicare una politica di autenticazione alle reti di servizi e ai singoli servizi. In genere, la politica di autenticazione sulla rete di servizi viene gestita dall'amministratore di rete o del cloud, che implementa un'autorizzazione granulare. Ad esempio, consente l'accesso solo alle richieste autenticate provenienti da un'organizzazione specifica. AWS Organizations Per una politica di autenticazione a livello di servizio, in genere il proprietario del servizio imposta controlli granulari, che potrebbero essere più restrittivi rispetto all'autorizzazione granulare applicata a livello di rete di servizio.

Note

La politica di autenticazione sulla rete di servizi non si applica alle configurazioni delle risorse nella rete di servizi.

Metodi di controllo degli accessi

- [Politiche di autenticazione](#)
- [Gruppi di sicurezza](#)
- [Liste di controllo accessi \(ACL\) di rete](#)

Controlla l'accesso ai servizi VPC Lattice utilizzando le policy di autenticazione

Le policy di autenticazione VPC Lattice sono documenti di policy IAM da allegare a reti o servizi di servizio per controllare se uno specifico principale ha accesso a un gruppo di servizi o a un servizio specifico. È possibile allegare una politica di autenticazione a ogni rete o servizio di servizio a cui si desidera controllare l'accesso.

Note

La politica di autenticazione sulla rete di servizi non si applica alle configurazioni delle risorse nella rete di servizi.

Le politiche di autenticazione sono diverse dalle politiche basate sull'identità IAM. Le policy basate sull'identità IAM sono associate agli utenti, ai gruppi o ai ruoli IAM e definiscono quali azioni tali identità possono eseguire su quali risorse. Le politiche di autenticazione sono collegate ai servizi e alle reti di servizi. Affinché l'autorizzazione abbia esito positivo, sia le politiche di autenticazione che le politiche basate sull'identità devono avere istruzioni di autorizzazione esplicite. Per ulteriori informazioni, consulta [Come funziona l'autorizzazione](#).

È possibile utilizzare la console AWS CLI and per visualizzare, aggiungere, aggiornare o rimuovere i criteri di autenticazione su servizi e reti di servizi. Quando aggiungi, aggiorni o rimuovi un criterio di autenticazione, potrebbero essere necessari alcuni minuti prima che sia pronto. Quando usi il AWS CLI, assicurati di trovarti nella regione corretta. Puoi modificare la regione predefinita per il tuo profilo o utilizzare il `--region` parametro con il comando.

Indice

- [Elementi comuni in una politica di autenticazione](#)
- [Formato delle risorse per le politiche di autenticazione](#)
- [Chiavi di condizione che possono essere utilizzate nelle politiche di autenticazione](#)
- [Tag delle risorse](#)
- [Tag principali](#)
- [Principi anonimi \(non autenticati\)](#)
- [Esempi di politiche di autenticazione](#)
- [Come funziona l'autorizzazione](#)

Per iniziare a utilizzare i criteri di autenticazione, segui la procedura per creare un criterio di autenticazione applicabile a una rete di servizi. Per autorizzazioni più restrittive che non desideri applicare ad altri servizi, puoi facoltativamente impostare criteri di autenticazione su singoli servizi.

Gestisci l'accesso a una rete di servizi con politiche di autenticazione

Le seguenti AWS CLI attività mostrano come gestire l'accesso a una rete di servizi utilizzando le politiche di autenticazione. Per istruzioni sull'utilizzo della console, consulta [Reti di servizio in VPC Lattice](#).

Processi

- [Aggiungere un criterio di autenticazione a una rete di servizi](#)
- [Modifica il tipo di autenticazione di una rete di servizi](#)
- [Rimuovi una politica di autenticazione da una rete di servizi](#)

Aggiungere un criterio di autenticazione a una rete di servizi

Segui la procedura descritta in questa sezione per utilizzare: AWS CLI

- Abilita il controllo degli accessi su una rete di servizi utilizzando IAM.
- Aggiungi una politica di autenticazione alla rete di servizi. Se non aggiungi un criterio di autenticazione, tutto il traffico riceverà un errore di accesso negato.

Per abilitare il controllo degli accessi e aggiungere una politica di autenticazione a una nuova rete di servizi

1. Per abilitare il controllo degli accessi su una rete di servizi in modo che possa utilizzare una politica di autenticazione, usa il `create-service-network` comando con l'`--auth-type` opzione e il valore di `AWS_IAM`

```
aws vpc-lattice create-service-network --name Name --auth-type AWS_IAM [--  
tags TagSpecification]
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "arn": "arn",  
  "authType": "AWS_IAM",
```

```
{
  "id": "sn-0123456789abcdef0",
  "name": "Name"
}
```

2. Usa il `put-auth-policy` comando, specificando l'ID della rete di servizi in cui desideri aggiungere la politica di autenticazione e la politica di autenticazione che desideri aggiungere.

Ad esempio, utilizzate il comando seguente per creare una politica di autenticazione per la rete di servizi con l'ID. *sn-0123456789abcdef0*

```
aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --
policy file://policy.json
```

Utilizzate JSON per creare una definizione di policy. Per ulteriori informazioni, consulta [Elementi comuni in una politica di autenticazione](#).

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{
  "policy": "policy",
  "state": "Active"
}
```

Per abilitare il controllo degli accessi e aggiungere una politica di autenticazione a una rete di servizi esistente

1. Per abilitare il controllo degli accessi su una rete di servizi in modo che possa utilizzare una politica di autenticazione, usa il `update-service-network` comando con l'`--auth-type` opzione e il valore di `AWS_IAM`

```
aws vpc-lattice update-service-network --service-network-
identifier sn-0123456789abcdef0 --auth-type AWS_IAM
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{
  "arn": "arn",
  "authType": "AWS_IAM",
  "id": "sn-0123456789abcdef0",
}
```

```
"name": "Name"
}
```

2. Usa il `put-auth-policy` comando, specificando l'ID della rete di servizi in cui desideri aggiungere la politica di autenticazione e la politica di autenticazione che desideri aggiungere.

```
aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --  
policy file:///policy.json
```

Usa JSON per creare una definizione di policy. Per ulteriori informazioni, consulta [Elementi comuni in una politica di autenticazione](#).

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "policy": "policy",  
  "state": "Active"  
}
```

Modifica il tipo di autenticazione di una rete di servizi

Per disabilitare la politica di autenticazione per una rete di servizi

Utilizzare il `update-service-network` comando con l'`--auth-type` opzione e il valore di `NONE`.

```
aws vpc-lattice update-service-network --service-network-  
identifier sn-0123456789abcdef0 --auth-type NONE
```

Se è necessario abilitare nuovamente la politica di autenticazione in un secondo momento, esegui questo comando con `AWS_IAM` specified for the `--auth-type` option.

Rimuovi una politica di autenticazione da una rete di servizi

Per rimuovere una politica di autenticazione da una rete di servizi

Utilizza il comando `delete-auth-policy`.

```
aws vpc-lattice delete-auth-policy --resource-identifier sn-0123456789abcdef0
```

La richiesta ha esito negativo se si rimuove una politica di autenticazione prima di modificare il tipo di autenticazione di una rete di servizi in `NONE`

Gestisci l'accesso a un servizio con politiche di autenticazione

Le seguenti AWS CLI attività mostrano come gestire l'accesso a un servizio utilizzando le politiche di autenticazione. Per istruzioni sull'utilizzo della console, consulta [Servizi in VPC Lattice](#).

Processi

- [Aggiungere un criterio di autenticazione a un servizio](#)
- [Modifica il tipo di autenticazione di un servizio](#)
- [Rimuovi una politica di autenticazione da un servizio](#)

Aggiungere un criterio di autenticazione a un servizio

Segui questi passaggi per utilizzare il file AWS CLI per:

- Abilita il controllo degli accessi su un servizio utilizzando IAM.
- Aggiungi una politica di autenticazione al servizio. Se non aggiungi una politica di autenticazione, tutto il traffico riceverà un errore di accesso negato.

Per abilitare il controllo degli accessi e aggiungere una politica di autenticazione a un nuovo servizio

1. Per abilitare il controllo degli accessi su un servizio in modo che possa utilizzare una politica di autenticazione, usa il create-service comando con l'--auth-typeopzione e il valore di.
AWS_IAM

```
aws vpc-lattice create-service --name Name --auth-type AWS_IAM [--  
tags TagSpecification]
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "arn": "arn",  
  "authType": "AWS_IAM",  
  "dnsEntry": {  
    ...  
  },  
  "id": "svc-0123456789abcdef0",  
  "name": "Name",  
  "status": "CREATE_IN_PROGRESS"
```

```
}
```

2. Usa il `put-auth-policy` comando, specificando l'ID del servizio a cui desideri aggiungere la politica di autenticazione e la politica di autenticazione che desideri aggiungere.

Ad esempio, utilizzate il comando seguente per creare una politica di autenticazione per il servizio con l'ID. *svc-0123456789abcdef0*

```
aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --  
policy file://policy.json
```

Utilizzate JSON per creare una definizione di policy. Per ulteriori informazioni, consulta [Elementi comuni in una politica di autenticazione](#).

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "policy": "policy",  
  "state": "Active"  
}
```

Per abilitare il controllo degli accessi e aggiungere una politica di autenticazione a un servizio esistente

1. Per abilitare il controllo degli accessi su un servizio in modo che possa utilizzare una politica di autenticazione, usa il `update-service` comando con l'`--auth-type` opzione e il valore di `AWS_IAM`

```
aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-  
type AWS_IAM
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "arn": "arn",  
  "authType": "AWS_IAM",  
  "id": "svc-0123456789abcdef0",  
  "name": "Name"  
}
```

2. Usa il `put-auth-policy` comando, specificando l'ID del servizio a cui desideri aggiungere la politica di autenticazione e la politica di autenticazione che desideri aggiungere.

```
aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --  
policy file://policy.json
```

Usa JSON per creare una definizione di policy. Per ulteriori informazioni, consulta [Elementi comuni in una politica di autenticazione](#).

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "policy": "policy",  
  "state": "Active"  
}
```

Modifica il tipo di autenticazione di un servizio

Per disabilitare la politica di autenticazione per un servizio

Utilizzare il `update-service` comando con l' `--auth-type` opzione e il valore di `NONE`.

```
aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-type  
NONE
```

Se è necessario abilitare nuovamente la politica di autenticazione in un secondo momento, esegui questo comando con `AWS_IAM` specified for the `--auth-type` option.

Rimuovi una politica di autenticazione da un servizio

Per rimuovere una politica di autenticazione da un servizio

Utilizza il comando `delete-auth-policy`.

```
aws vpc-lattice delete-auth-policy --resource-identifier svc-0123456789abcdef0
```

La richiesta ha esito negativo se si rimuove una politica di autenticazione prima di modificare il tipo di autenticazione del servizio in `NONE`

Se abiliti i criteri di autenticazione che richiedono richieste autenticate a un servizio, tutte le richieste a quel servizio devono contenere una firma di richiesta valida calcolata utilizzando Signature Version 4 (SigV4). Per ulteriori informazioni, consulta [Richieste autenticate SigV4 per Amazon VPC Lattice](#).

Elementi comuni in una politica di autenticazione

Le policy di autenticazione VPC Lattice vengono specificate utilizzando la stessa sintassi delle policy IAM. Per ulteriori informazioni, consulta le [Identity-based policy e le policy basate sulle risorse](#) nella IAM User Guide.

Una policy di autenticazione contiene i seguenti elementi:

- **Principale:** la persona o l'applicazione a cui è consentito l'accesso alle azioni e alle risorse contenute nella dichiarazione. In una politica di autenticazione, il principale è l'entità IAM che è il destinatario di questa autorizzazione. Il principale viene autenticato come entità IAM per effettuare richieste a una risorsa o a un gruppo di risorse specifico, come nel caso dei servizi in una rete di servizi.

In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o servizi. AWS Per ulteriori informazioni, consulta [AWS JSON Policy elements: Principal](#) nella IAM User Guide.

- **Effetto:** l'effetto quando il principale specificato richiede l'azione specifica. Ciò può essere Allow o Deny. Per impostazione predefinita, quando si abilita il controllo degli accessi su un servizio o su una rete di servizi utilizzando IAM, i principali non dispongono delle autorizzazioni per effettuare richieste al servizio o alla rete di servizi.
- **Azioni:** l'azione API specifica per la quale concedi o neghi l'autorizzazione. VPC Lattice supporta azioni che utilizzano il prefisso `vpc-lattice-svcs` Per ulteriori informazioni, consulta [Azioni definite da Amazon VPC Lattice Services](#) nel Service Authorization Reference.
- **Risorse:** i servizi interessati dall'azione.
- **Condizione:** le condizioni sono facoltative. Puoi usarle per controllare quando la tua politica è in vigore. Per ulteriori informazioni, consulta [Condition keys for Amazon VPC Lattice Services](#) nel Service Authorization Reference.

Durante la creazione e la gestione delle politiche di autenticazione, potresti voler utilizzare [IAM](#) Policy Generator.

Requisito

La policy in JSON non deve contenere nuove righe o righe vuote.

Formato delle risorse per le politiche di autenticazione

È possibile limitare l'accesso a risorse specifiche creando una politica di autenticazione che utilizzi uno schema corrispondente con uno `<serviceARN>/<path>` schema e codifichi l'Resourceelemento come illustrato negli esempi seguenti.

Protocollo	Esempi
HTTP	"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/rates" "Resource": "*/rates" "Resource": "*/"
gRPC	"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/GetRates" "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/*" "Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/*"

Utilizza il seguente formato di risorse Amazon Resource Name (ARN) per: `<serviceARN>`

```
arn:aws:vpc-lattice:region:account-id:service/service-id
```

Ad esempio:

```
"Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0"
```

Chiavi di condizione che possono essere utilizzate nelle politiche di autenticazione

L'accesso può essere ulteriormente controllato mediante i tasti condizionali nell'elemento Condition delle politiche di autenticazione. Queste chiavi di condizione sono disponibili per la valutazione a seconda del protocollo e del fatto che la richiesta sia firmata con [Signature Version 4 \(SigV4\)](#) o anonima. Le chiavi di condizione fanno distinzione tra maiuscole e minuscole.

AWS fornisce chiavi di condizione globali che è possibile utilizzare per controllare l'accesso, come `eaws:PrincipalOrgID`. `aws:SourceIp` Per visualizzare un elenco delle chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali](#) nella Guida per l'utente IAM.

La seguente tabella elenca le chiavi delle condizioni di VPC Lattice. Per ulteriori informazioni, consulta [Condition keys for Amazon VPC Lattice Services](#) nel Service Authorization Reference.

Chiavi di condizione	Description	Esempio	Disponibile per chiamanti anonimi (non autenticati)?	Disponibile per gRPC?
<code>vpc-lattice-svcs:Port</code>	Filtra l'accesso tramite la porta di servizio a cui viene effettuata la richiesta	80	Sì	Sì
<code>vpc-lattice-svcs:RequestMethod</code>	Filtra l'accesso in base al metodo della richiesta	GET	Sì	PUBBLICA sempre
<code>vpc-lattice-svcs:RequestPath</code>	Filtra l'accesso in base alla parte del percorso dell'URL della richiesta	/path	Sì	Sì
<code>vpc-lattice-svcs:RequestHeader/ <i>header-name</i> : <i>value</i></code>	Filtra l'accesso in base a una coppia nome-valore dell'intestazione nelle intestazioni della richiesta	content-type: application/json	Sì	Sì

Chiavi di condizione	Description	Esempio	Disponibile per chiamanti anonimi (non autenticati)?	Disponibile per gRPC?
<code>vpc-lattice-svcs:QueryString/ <i>key-name</i>: <i>value</i></code>	Filtra l'accesso dalle coppie chiave-valore della stringa di query nell'URL della richiesta	<code>quux: [corge, grault]</code>	Sì	No
<code>vpc-lattice-svcs:ServiceNetworkArn</code>	Filtra l'accesso tramite l'ARN della rete di servizi del servizio che riceve la richiesta	<code>arn:aws:vpc-lattice:us-west-2:123456789012:service-network/sn-0123456789abcdef0</code>	Sì	Sì
<code>vpc-lattice-svcs:ServiceArn</code>	Filtra l'accesso in base all'ARN del servizio che riceve la richiesta	<code>arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0</code>	Sì	Sì
<code>vpc-lattice-svcs:SourceVpc</code>	Filtra l'accesso in base al VPC da cui proviene la richiesta	<code>vpc-1a2b3c4d</code>	Sì	Sì

Chiavi di condizione	Description	Esempio	Disponibile per chiamanti anonimi (non autenticati)?	Disponibile per gRPC?
<code>vpc-lattice-svcs:SourceVpcOwnerAccount</code>	Filtra l'accesso in base all'account proprietario del VPC da cui viene effettuata la richiesta	123456789012	Sì	Sì

Tag delle risorse

Un tag è un'etichetta di metadati che si assegna o che si assegna a AWS una risorsa. AWS Ogni tag è costituito da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un campo facoltativo noto come valore del tag (ad esempio, `111122223333` o `Production`). Non specificare il valore del tag equivale a utilizzare una stringa vuota. Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra maiuscole e minuscole.

Per ulteriori informazioni sull'etichettatura, consulta [Controllo dell'accesso alle](#) risorse mediante i tag AWS

Puoi utilizzare i tag nelle tue politiche di autenticazione utilizzando la chiave di contesto `aws:ResourceTag/key` AWS global condition.

La seguente politica di esempio concede l'accesso ai servizi con il tag `Environment=Gamma`. Questa policy consente di fare riferimento a servizi senza ARN o ID di servizio con codifica fissa.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGammaAccess",
```

```

    "Effect": "Allow",
    "Principal": "*",
    "Action": "vpc-lattice-svcs:Invoke",
    "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:service/
svc-0124446789abcdef0/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Environment": "Gamma",
      }
    }
  }
]
}

```

Tag principali

Puoi controllare l'accesso ai tuoi servizi e alle tue risorse in base ai tag allegati all'identità del chiamante. VPC Lattice supporta il controllo degli accessi basato su qualsiasi tag principale sui tag utente, ruolo o sessione utilizzando le variabili. `aws:PrincipalTag/context` Per ulteriori informazioni, consulta [Controlling access for IAM principals](#).

La seguente policy di esempio concede l'accesso solo alle identità con il tag. `Team=Payments` Questa policy consente di controllare l'accesso senza codificare gli ID degli account o gli ARN dei ruoli.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPaymentsTeam",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "vpc-lattice-svcs:Invoke",
      "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:service/
svc-0123456789abcdef0/*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalTag/Team": "Payments",
        }
      }
    }
  ]
}

```

```
}
```

Principi anonimi (non autenticati)

I principali anonimi sono chiamanti che non firmano AWS le loro richieste con [Signature Version 4 \(SigV4\)](#) e si trovano all'interno di un VPC connesso alla rete di servizi. I responsabili anonimi possono effettuare richieste non autenticate ai servizi della rete di servizi se una politica di autenticazione lo consente.

Esempi di politiche di autenticazione

Di seguito sono riportati alcuni esempi di politiche di autenticazione che richiedono l'invio di richieste da parte di responsabili autenticati.

Tutti gli esempi utilizzano la us-west-2 regione e contengono ID di account fittizi.

Esempio 1: limita l'accesso ai servizi a una persona specifica AWS organizzazione

Il seguente esempio di politica di autenticazione concede le autorizzazioni a qualsiasi richiesta autenticata di accesso a qualsiasi servizio della rete di servizi a cui si applica la politica. Tuttavia, la richiesta deve provenire da responsabili che appartengono all' AWS organizzazione specificata nella condizione.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "vpc-lattice-svcs:Invoke",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": [
            "o-123456example"
          ]
        }
      }
    }
  ]
}
```

```
}
```

Esempio 2: limita l'accesso a un servizio tramite un ruolo IAM specifico

Il seguente esempio di politica di autenticazione concede le autorizzazioni a qualsiasi richiesta autenticata che utilizza il ruolo IAM `rates-client` per effettuare richieste HTTP GET sul servizio specificato nell'elemento. Resource La risorsa nell'Resourceelemento è la stessa del servizio a cui è allegata la policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/rates-client"
        ]
      },
      "Action": "vpc-lattice-svcs:Invoke",
      "Resource": [
        "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0/*"
      ],
      "Condition": {
        "StringEquals": {
          "vpc-lattice-svcs:RequestMethod": "GET"
        }
      }
    ]
  ]
}
```

Esempio 3: Limita l'accesso ai servizi tramite principali autenticati in un VPC specifico

Il seguente esempio di policy di autenticazione consente solo le richieste autenticate dai principali nel VPC il cui ID VPC è. `vpc-1a2b3c4d`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "vpc-lattice-svcs:Invoke",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalType": "Anonymous"
        },
        "StringEquals": {
          "vpc-lattice-svcs:SourceVpc": "vpc-1a2b3c4d"
        }
      }
    }
  ]
}
```

Come funziona l'autorizzazione

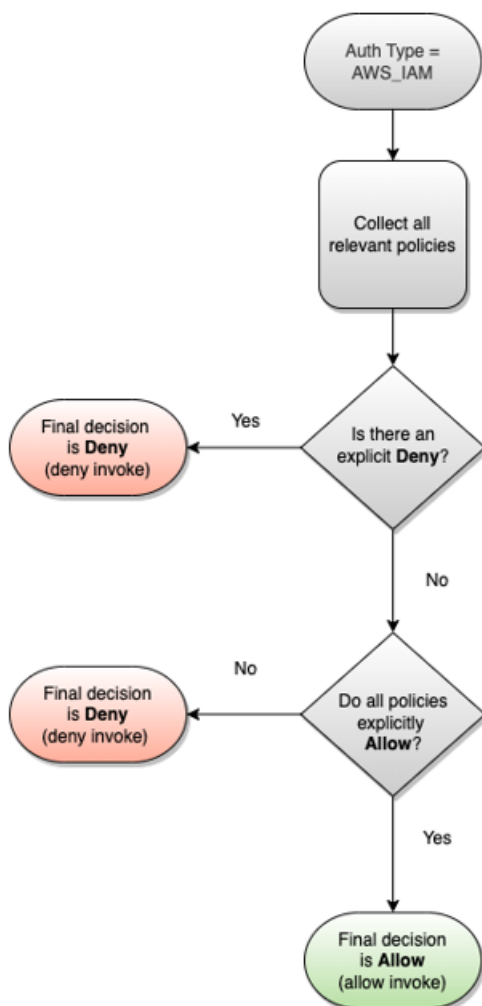
Quando un servizio VPC Lattice riceve una richiesta, il codice di AWS applicazione valuta insieme tutte le politiche di autorizzazione pertinenti per determinare se autorizzare o rifiutare la richiesta. Valuta tutte le politiche basate sull'identità e le politiche di autenticazione IAM applicabili nel contesto della richiesta durante l'autorizzazione. Per impostazione predefinita, tutte le richieste vengono negate implicitamente quando il tipo di autenticazione è `AWS_IAM`. Un'autorizzazione esplicita da parte di tutte le politiche pertinenti ha la precedenza sull'impostazione predefinita.

L'autorizzazione include:

- Raccolta di tutte le policy e le policy di autenticazione basate sull'identità IAM pertinenti.
- Valutazione del set di politiche risultante:
 - Verifica che il richiedente (ad esempio un utente o un ruolo IAM) disponga delle autorizzazioni per eseguire l'operazione dall'account a cui appartiene il richiedente. Se non esiste un'istruzione di autorizzazione esplicita, AWS non autorizza la richiesta.

- Verifica che la richiesta sia consentita dalla politica di autenticazione per la rete di servizi. Se un criterio di autenticazione è abilitato, ma non esiste un'istruzione di autorizzazione esplicita, la richiesta AWS non viene autorizzata. Se esiste un'istruzione di autorizzazione esplicita o il tipo di autenticazione è **NONE**, il codice continua.
- Verifica che la richiesta sia consentita dalla politica di autenticazione del servizio. Se un criterio di autenticazione è abilitato, ma non esiste un'istruzione di autorizzazione esplicita, la richiesta AWS non viene autorizzata. Se è presente un'istruzione di autorizzazione esplicita o il tipo di autenticazione lo è **NONE**, il codice di applicazione restituisce la decisione finale di Allow.
- Un rifiuto esplicito in una policy sostituisce qualsiasi permesso.

Il diagramma mostra il flusso di lavoro di autorizzazione. Quando viene effettuata una richiesta, le politiche pertinenti consentono o negano l'accesso della richiesta a un determinato servizio.



Controlla il traffico in VPC Lattice utilizzando gruppi di sicurezza

AWS i gruppi di sicurezza agiscono come firewall virtuali, controllando il traffico di rete da e verso le entità a cui sono associati. Con VPC Lattice, puoi creare gruppi di sicurezza e assegnarli all'associazione VPC che collega un VPC a una rete di servizi per applicare protezioni di sicurezza aggiuntive a livello di rete per la tua rete di servizi. Se connetti un VPC a una rete di servizi utilizzando un endpoint VPC, puoi assegnare gruppi di sicurezza anche all'endpoint VPC. Allo stesso modo, puoi assegnare gruppi di sicurezza ai gateway di risorse che crei per consentire l'accesso alle risorse nel tuo VPC.

Indice

- [Elenco di prefissi gestiti](#)
- [Regole del gruppo di sicurezza](#)
- [Gestire i gruppi di sicurezza per un'associazione VPC](#)

Elenco di prefissi gestiti

VPC Lattice fornisce elenchi di prefissi gestiti che includono gli indirizzi IP utilizzati per instradare il traffico sulla rete VPC Lattice quando si utilizza un'associazione di rete di servizio per connettere il VPC a una rete di servizi utilizzando un'associazione VPC. Questi IP sono IP locali di collegamento privati o IP pubblici non instradabili.

Puoi fare riferimento agli elenchi di prefissi gestiti da VPC Lattice nelle regole del tuo gruppo di sicurezza. Ciò consente al traffico di fluire dai client, attraverso la rete di servizi VPC Lattice, e verso gli obiettivi del servizio VPC Lattice.

Ad esempio, supponiamo di avere un'istanza EC2 registrata come destinazione nella regione degli Stati Uniti occidentali (Oregon) (). `us-west-2` Puoi aggiungere una regola al gruppo di sicurezza dell'istanza che consente l'accesso HTTPS in entrata dall'elenco dei prefissi gestiti di VPC Lattice, in modo che il traffico VPC Lattice in questa regione possa raggiungere l'istanza. Se rimuovi tutte le altre regole in entrata dal gruppo di sicurezza, puoi impedire a qualsiasi traffico diverso dal traffico VPC Lattice di raggiungere l'istanza.

I nomi degli elenchi di prefissi gestiti per VPC Lattice sono i seguenti:

- `com.amazonaws. region.vpc-reticolo`
- `com.amazonaws. region.ipv6.vpc-reticolo`

Per maggiori informazioni, consulta [Elenchi di prefissi gestiti da AWS](#) nella Guida dell'utente di Amazon VPC.

Client Windows e macOS

Gli indirizzi negli elenchi di prefissi VPC Lattice sono indirizzi locali del collegamento e indirizzi pubblici non instradabili. Se ti connetti a VPC Lattice da questi client, devi aggiornare le loro configurazioni in modo da inoltrare gli indirizzi IP nell'elenco dei prefissi gestiti all'indirizzo IP primario del client. Di seguito è riportato un comando di esempio che aggiorna la configurazione del client Windows, dove si 169.254.171.0 trova uno degli indirizzi nell'elenco dei prefissi gestiti.

```
C:\> route add 169.254.171.0 mask 255.255.255.0 primary-ip-address
```

Di seguito è riportato un comando di esempio che aggiorna la configurazione del client macOS, dove si 169.254.171.0 trova uno degli indirizzi nell'elenco dei prefissi gestiti.

```
sudo route -n add -net 169.254.171.0 primary-ip-address 255.255.255.0
```

Per evitare di creare una route statica, ti consigliamo di utilizzare un endpoint di rete di servizio in un VPC per stabilire la connettività. Per ulteriori informazioni, consulta [the section called “Gestisci le associazioni di endpoint VPC della rete di assistenza”](#).

Regole del gruppo di sicurezza

L'utilizzo di VPC Lattice con o senza gruppi di sicurezza non influirà sulla configurazione del gruppo di sicurezza VPC esistente. Tuttavia, puoi aggiungere i tuoi gruppi di sicurezza in qualsiasi momento.

Considerazioni chiave

- Le regole dei gruppi di sicurezza per i client controllano il traffico in uscita verso VPC Lattice.
- Le regole dei gruppi di sicurezza per le destinazioni controllano il traffico in entrata da VPC Lattice alle destinazioni, incluso il traffico per il controllo dello stato di salute.
- Le regole del gruppo di sicurezza per l'associazione tra la rete di servizi e il VPC controllano quali client possono accedere alla rete di servizi VPC Lattice.
- Le regole dei gruppi di sicurezza per il Resource Gateway controllano il traffico in uscita dal Resource Gateway alle risorse.

Regole in uscita consigliate per il traffico che scorre dal Resource Gateway a una risorsa di database

Affinché il traffico fluisca dal gateway di risorse alle risorse, è necessario creare regole in uscita per le porte aperte e protocolli di ascolto accettati per le risorse.

Destinazione	Protocollo	Intervallo porte	Comment
<i>CIDR range for resource</i>	<i>TCP</i>	<i>3306</i>	Consenti il traffico dal gateway di risorse ai database

Regole in entrata consigliate per le associazioni di reti di servizi e VPC

Affinché il traffico possa fluire dai VPC client ai servizi associati alla rete di servizi, è necessario creare regole in entrata per le porte dei listener e i protocolli di ascolto per i servizi.

Crea	Protocollo	Intervallo porte	Comment
<i>VPC CIDR</i>	<i>listener</i>	<i>listener</i>	Consenti il traffico dai client a VPC Lattice

Regole in uscita consigliate per il flusso di traffico dalle istanze client a VPC Lattice

Per impostazione predefinita, i gruppi di sicurezza autorizzano tutto il traffico in uscita. Tuttavia, se disponi di regole in uscita personalizzate, devi consentire il traffico in uscita al prefisso VPC Lattice per le porte e i protocolli del listener in modo che le istanze client possano connettersi a tutti i servizi associati alla rete di servizi VPC Lattice. Puoi consentire questo traffico facendo riferimento all'ID dell'elenco dei prefissi per VPC Lattice.

Destinazione	Protocollo	Intervallo porte	Comment
<i>ID of the VPC Lattice prefix list</i>	<i>listener</i>	<i>listener</i>	Consenti il traffico dai client a VPC Lattice

Regole in entrata consigliate per il traffico che fluisce da VPC Lattice alle istanze di destinazione

Non puoi utilizzare il gruppo di sicurezza del client come fonte per i gruppi di sicurezza del tuo target, perché il traffico proviene da VPC Lattice. Puoi fare riferimento all'ID dell'elenco dei prefissi per VPC Lattice.

Crea	Protocollo	Intervallo porte	Comment
<i>ID of the VPC Lattice prefix list</i>	<i>target</i>	<i>target</i>	Consenti il traffico da VPC Lattice agli obiettivi
<i>ID of the VPC Lattice prefix list</i>	<i>health check</i>	<i>health check</i>	Consenti il traffico di health check da VPC Lattice agli obiettivi

Gestire i gruppi di sicurezza per un'associazione VPC

È possibile utilizzare l'associazione AWS CLI di rete da VPC a service per visualizzare, aggiungere o aggiornare i gruppi di sicurezza sul VPC. Quando usi il AWS CLI, ricorda che i comandi vengono eseguiti nella Regione AWS configurazione per il tuo profilo. Per eseguire i comandi in un'altra regione, modificare la regione predefinita per il profilo oppure utilizzare il parametro `--region` con il comando.

Prima di iniziare, conferma di aver creato il gruppo di sicurezza nello stesso VPC del VPC che desideri aggiungere alla rete di servizi. Per ulteriori informazioni, consulta [Controlla il traffico verso le tue risorse utilizzando i gruppi di sicurezza](#) nella Amazon VPC User Guide

Per aggiungere un gruppo di sicurezza quando si crea un'associazione VPC utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Nella scheda Associazioni VPC, scegli Crea associazioni VPC, quindi scegli Aggiungi associazione VPC.
5. Seleziona un VPC e fino a cinque gruppi di sicurezza.
6. Scegli Save changes (Salva modifiche).

Per aggiungere o aggiornare gruppi di sicurezza per un'associazione VPC esistente utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona il nome della rete di servizio per aprirne la pagina dei dettagli.
4. Nella scheda Associazioni VPC, seleziona la casella di controllo relativa all'associazione, quindi scegli Azioni, Modifica gruppi di sicurezza.
5. Aggiungi e rimuovi i gruppi di sicurezza in base alle esigenze.
6. Scegli Save changes (Salva modifiche).

Per aggiungere un gruppo di sicurezza quando si crea un'associazione VPC utilizzando AWS CLI

Utilizza il comando [create-service-network-vpc-association](#), specificando l'ID del VPC per l'associazione VPC e l'ID dei gruppi di sicurezza da aggiungere.

```
aws vpc-lattice create-service-network-vpc-association \  
  --service-network-identifier sn-0123456789abcdef0 \  
  --vpc-identifier vpc-1a2b3c4d \  
  --security-group-ids sg-7c2270198example
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "arn": "arn",  
  "createdBy": "464296918874",  
  "id": "sna-0123456789abcdef0",  
  "status": "CREATE_IN_PROGRESS",  
  "securityGroupIds": ["sg-7c2270198example"]  
}
```

Per aggiungere o aggiornare gruppi di sicurezza per un'associazione VPC esistente utilizzando AWS CLI

Utilizza il comando [update-service-network-vpc-association](#), specificando l'ID della rete di servizi e gli ID dei gruppi di sicurezza. Questi gruppi di sicurezza sostituiscono tutti i gruppi di sicurezza precedentemente associati. Definisci almeno un gruppo di sicurezza durante l'aggiornamento dell'elenco.

```
aws vpc-lattice update-service-network-vpc-association
--service-network-vpc-association-identifier sn-903004f88example \
--security-group-ids sg-7c2270198example sg-903004f88example
```

Warning

Non puoi rimuovere tutti i gruppi di sicurezza. È invece necessario prima eliminare l'associazione VPC e quindi ricreare l'associazione VPC senza gruppi di sicurezza. Fai attenzione quando elimini l'associazione VPC. Ciò impedisce al traffico di raggiungere i servizi che si trovano in quella rete di servizi.

Controlla il traffico verso VPC Lattice utilizzando gli ACL di rete

Una lista di controllo degli accessi (ACL) di rete consente o nega traffico specifico in entrata o in uscita a livello di sottorete. L'ACL di rete predefinita consente tutto il traffico in entrata e in uscita. Puoi creare ACL di rete personalizzati per le tue sottoreti per fornire un ulteriore livello di sicurezza. Per ulteriori informazioni, consulta la sezione relativa alle [Liste di controllo degli accessi di rete](#) nella Guida per l'utente di Amazon VPC.

Indice

- [ACL di rete per le sottoreti client](#)
- [ACL di rete per le sottoreti di destinazione](#)

ACL di rete per le sottoreti client

Gli ACL di rete per le sottoreti client devono consentire il traffico tra i client e VPC Lattice. È possibile ottenere gli intervalli di indirizzi IP da consentire dall'[elenco dei prefissi gestiti](#) per VPC Lattice.

Di seguito è riportato un esempio di regola in entrata.

Crea	Protocollo	Intervallo porte	Comment
<i>vpc_lattice_cidr_block</i>	TCP	1025-65535	Consenti il traffico da VPC Lattice ai client

Di seguito è riportato un esempio di una regola di uscita.

Destinazione	Protocollo	Intervallo porte	Comment
<i>vpc_latti</i> <i>ce_cidr_block</i>	<i>listener</i>	<i>listener</i>	Consenti il traffico dai client a VPC Lattice

ACL di rete per le sottoreti di destinazione

Gli ACL di rete per le sottoreti di destinazione devono consentire il traffico tra i target e VPC Lattice sia sulla porta di destinazione che sulla porta di controllo dello stato. È possibile ottenere gli intervalli di indirizzi IP da consentire dall'[elenco dei prefissi gestiti](#) per VPC Lattice.

Di seguito è riportato un esempio di regola in entrata.

Crea	Protocollo	Intervallo porte	Comment
<i>vpc_latti</i> <i>ce_cidr_block</i>	<i>target</i>	<i>target</i>	Consenti il traffico da VPC Lattice agli obiettivi
<i>vpc_latti</i> <i>ce_cidr_block</i>	<i>health check</i>	<i>health check</i>	Consenti il traffico di health check da VPC Lattice agli obiettivi

Di seguito è riportato un esempio di una regola di uscita.

Destinazione	Protocollo	Intervallo porte	Comment
<i>vpc_latti</i> <i>ce_cidr_block</i>	<i>target</i>	1024-65535	Consenti il traffico dai target a VPC Lattice
<i>vpc_latti</i> <i>ce_cidr_block</i>	<i>health check</i>	1024-65535	Consenti il traffico di health check dai target a VPC Lattice

Richieste autenticate SigV4 per Amazon VPC Lattice

VPC Lattice utilizza Signature Version 4 (SigV4) o Signature Version 4A (SigV4A) per l'autenticazione del client. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Considerazioni

- VPC Lattice tenta di autenticare qualsiasi richiesta firmata con SigV4 o SigV4A. La richiesta fallisce senza autenticazione.
- VPC Lattice non supporta la firma del payload. È necessario inviare un'`x-amz-content-sha256` intestazione con il valore impostato su. `"UNSIGNED-PAYLOAD"`

Esempi

- [Python](#)
- [Java](#)
- [Node.js](#)
- [Golang](#)
- [Golang - GRPC](#)

Python

Questo esempio invia le richieste firmate tramite una connessione sicura a un servizio registrato nella rete. Se si preferisce utilizzare [le richieste](#), il pacchetto [botocore](#) semplifica il processo di autenticazione, ma non è strettamente necessario. Per ulteriori informazioni, consulta [Credenziali](#) nella documentazione di Boto3.

Per installare i `awscli` pacchetti `botocore` and, utilizzare il comando seguente. Per ulteriori informazioni, consulta [AWS CRT Python](#).

```
pip install botocore awscli
```

Se esegui l'applicazione client su Lambda, installa i moduli richiesti utilizzando i [livelli Lambda](#) o includili nel pacchetto di distribuzione.

Nell'esempio seguente, sostituisci i valori segnaposto con i tuoi valori.

SIGv4

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtSigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
    'us-west-2')
    endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-
west-2.on.aws'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':
'UNSIGNED-PAYLOAD'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
    print(response.text)
```

SIGv4A

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtSigV4AsymAuth(session.get_credentials(), 'vpc-lattice-
svcs', '*')
    endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-
west-2.on.aws'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':
'UNSIGNED-PAYLOAD'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False
```

```
signer.add_auth(request)

prepped = request.prepare()

response = requests.post(prepped.url, headers=prepped.headers, data=data)
print(response.text)
```

Java

Questo esempio mostra come è possibile eseguire la firma delle richieste utilizzando intercettori personalizzati. Utilizza la classe di provider di credenziali predefinita da [AWS SDK for Java 2.x](#), che ottiene le credenziali corrette per te. Se preferisci utilizzare un provider di credenziali specifico, puoi selezionarne uno da [AWS SDK for Java 2.x](#). AWS SDK per Java Consente solo payload non firmati su HTTPS. Tuttavia, puoi estendere il firmatario per supportare payload non firmati tramite HTTP.

SIGv4

```
package com.example;

import software.amazon.awssdk.http.auth.aws.signer.AwsV4HttpSigner;
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;

import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;
import software.amazon.awssdk.http.SdkHttpRequest;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.http.HttpExecuteRequest;
import software.amazon.awssdk.http.HttpExecuteResponse;
import java.io.IOException;
import java.net.URI;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

public class sigv4 {

    public static void main(String[] args) {
        AwsV4HttpSigner signer = AwsV4HttpSigner.create();

        AwsCredentialsIdentity credentials =
            DefaultCredentialsProvider.create().resolveCredentials();
```

```

    if (args.length < 2) {
        System.out.println("Usage: sample <url> <region>");
        System.exit(1);
    }
    // Create the HTTP request to be signed
    var url = args[0];
    SdkHttpRequest httpRequest = SdkHttpRequest.builder()
        .uri(URI.create(url))
        .method(SdkHttpMethod.GET)
        .build();

    SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
        .request(httpRequest)
        .putProperty(AwsV4HttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")

        .putProperty(AwsV4HttpSigner.PAYLOAD_SIGNING_ENABLED, false)
        .putProperty(AwsV4HttpSigner.REGION_NAME, args[1]));

    System.out.println("[*] Raw request headers:");
    signedRequest.request().headers().forEach((key, values) -> {
        values.forEach(value -> System.out.println("  " + key + ": " + value));
    });

    try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
        HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
            .request(signedRequest.request())
            .contentStreamProvider(signedRequest.payload().orElse(null))
            .build();

        System.out.println("[*] Sending request to: " + url);

        HttpExecuteResponse httpResponse =
httpClient.prepareRequest(httpExecuteRequest).call();

        System.out.println("[*] Request sent");

        System.out.println("[*] Response status code: " +
httpClient.httpResponse().statusCode());
        // Read and print the response body
        httpResponse.responseBody().ifPresent(inputStream -> {
            try {
                String responseBody = new String(inputStream.readAllBytes());
                System.out.println("[*] Response body: " + responseBody);
            } catch (IOException e) {

```

```

        System.err.println("[*] Failed to read response body");
        e.printStackTrace();
    } finally {
        try {
            inputStream.close();
        } catch (IOException e) {
            System.err.println("[*] Failed to close input stream");
            e.printStackTrace();
        }
    }
});
} catch (IOException e) {
    System.err.println("[*] HTTP Request Failed.");
    e.printStackTrace();
}
}
}
}

```

SIGv4A

Questo esempio richiede una dipendenza aggiuntiva da `software.amazon.awssdk:http-auth-aws-crt`

```

package com.example;

import software.amazon.awssdk.http.auth.aws.signer.AwsV4aHttpSigner;
import software.amazon.awssdk.http.auth.aws.signer.RegionSet;
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;

import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;
import software.amazon.awssdk.http.SdkHttpRequest;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.http.HttpExecuteRequest;
import software.amazon.awssdk.http.HttpExecuteResponse;
import java.io.IOException;
import java.net.URI;
import java.util.Arrays;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

```

```

public class sigv4a {

    public static void main(String[] args) {
        AwsV4aHttpSigner signer = AwsV4aHttpSigner.create();

        AwsCredentialsIdentity credentials =
DefaultCredentialsProvider.create().resolveCredentials();

        if (args.length < 2) {
            System.out.println("Usage: sample <url> <regionset>");
            System.exit(1);
        }
        // Create the HTTP request to be signed
        var url = args[0];
        SdkHttpRequest httpRequest = SdkHttpRequest.builder()
            .uri(URI.create(url))
            .method(SdkHttpMethod.GET)
            .build();

        SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
            .request(httpRequest)
            .putProperty(AwsV4aHttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
            .putProperty(AwsV4aHttpSigner.PAYLOAD_SIGNING_ENABLED, false)
            .putProperty(AwsV4aHttpSigner.REGION_SET,
RegionSet.create(String.join(" ",Arrays.copyOfRange(args, 1, args.length)))));

        System.out.println("[*] Raw request headers:");
        signedRequest.request().headers().forEach((key, values) -> {
            values.forEach(value -> System.out.println("  " + key + ": " + value));
        });

        try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
            HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
                .request(signedRequest.request())
                .contentStreamProvider(signedRequest.payload().orElse(null))
                .build();

            System.out.println("[*] Sending request to: " + url);

            HttpExecuteResponse httpResponse =
httpClient.prepareRequest(httpExecuteRequest).call();

```

```

        System.out.println("[*] Request sent");

        System.out.println("[*] Response status code: " +
        httpResponse.httpResponse().statusCode());
        // Read and print the response body
        httpResponse.responseBody().ifPresent(inputStream -> {
            try {
                String responseBody = new String(inputStream.readAllBytes());
                System.out.println("[*] Response body: " + responseBody);
            } catch (IOException e) {
                System.err.println("[*] Failed to read response body");
                e.printStackTrace();
            } finally {
                try {
                    inputStream.close();
                } catch (IOException e) {
                    System.err.println("[*] Failed to close input stream");
                    e.printStackTrace();
                }
            }
        });
    } catch (IOException e) {
        System.err.println("[*] HTTP Request Failed.");
        e.printStackTrace();
    }
}
}

```

Node.js

Questo esempio utilizza le associazioni [aws-crt NodeJS per inviare una richiesta](#) firmata tramite HTTPS.

Per installare il pacchetto, utilizzare il seguente comando. `aws-crt`

```
npm -i aws-crt
```

Se la variabile di `AWS_REGION` ambiente esiste, l'esempio utilizza la regione specificata da `AWS_REGION`. La regione predefinita è `us-east-1`.

SIGv4

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
  const host = new URL(endpoint).host
  const request = new HttpRequest(method, endpoint)
  request.headers.add('host', host)
  // crt.io.enable_logging(crt.io.LogLevel.INFO)
  const config = {
    service: service,
    region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
    algorithm: algorithm,
    signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
    signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
    signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
    provider: crt.auth.AwsCredentialsProvider.newDefault()
  }

  return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs', algorithm).then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: new URL(process.argv[2]).pathname,
      method: 'GET',
      headers: headers
    }
```

```

    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)

```

SIGv4A

```

const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
  const host = new URL(endpoint).host
  const request = new HttpRequest(method, endpoint)
  request.headers.add('host', host)
  // crt.io.enable_logging(crt.io.LogLevel.INFO)
  const config = {
    service: service,
    region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
    algorithm: algorithm,
    signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
    signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
    signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
    provider: crt.auth.AwsCredentialsProvider.newDefault()
  }

  return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

```

```

}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4Asymmetric;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs', algorithm).then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: new URL(process.argv[2]).pathname,
      method: 'GET',
      headers: headers
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)

```

Golang

Questo esempio utilizza i [generatori di codice Smithy per Go](#) e l'[AWS SDK per il linguaggio di programmazione Go per gestire le](#) richieste di firma delle richieste. L'esempio richiede una versione Go 1.21 o successiva.

SIGv4

```
package main
```

```
import (
    "context"
    "flag"
    "fmt"
    "io"
    "log"
    "net/http"
    "net/http/httputil"
    "os"
    "strings"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/smithy-go/aws-http-auth/credentials"
    "github.com/aws/smithy-go/aws-http-auth/sigv4"
    v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
    io.ReadSeeker
}

func (nopCloser) Close() error {
    return nil
}

type stringFlag struct {
    set    bool
    value  string
}

    flag.PrintDefaults()
    os.Exit(1)
}

func main() {
    flag.Parse()
    if !url.set || !region.set {
        Usage()
    }
}
```

```

    cfg, err := config.LoadDefaultConfig(context.TODO(),
config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    if len(os.Args) < 2 {
        log.Fatalf("Usage: go run main.go <url>")
    }

    // Retrieve credentials from an SDK source, such as the instance profile
    sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
    if err != nil {
        log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
    }

    creds := credentials.Credentials{
        AccessKeyID:      sdkCreds.AccessKeyID,
        SecretAccessKey:  sdkCreds.SecretAccessKey,
        SessionToken:     sdkCreds.SessionToken,
    }

    // Add a payload body, which will not be part of the signature calculation
    body := nopCloser{strings.NewReader(`Example payload body`)}

    req, _ := http.NewRequest(http.MethodPost, url.value, body)

    // Create a sigv4a signer with specific options
    signer := sigv4.New(func(o *v4.SignerOptions) {
        o.DisableDoublePathEscape = true
        // This will add the UNSIGNED-PAYLOAD sha256 header
        o.AddPayloadHashHeader = true
        o.DisableImplicitPayloadHashing = true
    })

    // Perform the signing on req, using the credentials we retrieved from the
    SDK
    err = signer.SignRequest(&sigv4.SignRequestInput{
        Request:      req,
        Credentials:  creds,
        Service:      "vpc-lattice-svcs",
        Region:      region.String(),
    })

```

```
    if err != nil {
        log.Fatalf("%s", err)
    }

    res, err := httputil.DumpRequest(req, true)

    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Raw request\n%s\n", string(res))

    log.Printf("[*] Sending request to %s\n", url.value)

    resp, err := http.DefaultClient.Do(req)
    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Request sent\n")

    log.Printf("[*] Response status code: %d\n", resp.StatusCode)

    respBody, err := io.ReadAll(resp.Body)
    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Response body: \n%s\n", respBody)
}
```

SIGv4A

```
package main

import (
    "context"
    "flag"
    "fmt"
    "io"
    "log"
    "net/http"
    "net/http/httputil"
```

```

    "os"
    "strings"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/smithy-go/aws-http-auth/credentials"
    "github.com/aws/smithy-go/aws-http-auth/sigv4a"
    v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
    io.ReadSeeker
}

func (nopCloser) Close() error {
    return nil
}

type stringFlag struct {

func main() {
    flag.Parse()
    if !url.set || !regionSet.set {
        Usage()
    }

    cfg, err := config.LoadDefaultConfig(context.TODO(),
config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    if len(os.Args) < 2 {
        log.Fatalf("Usage: go run main.go <url>")
    }

    // Retrieve credentials from an SDK source, such as the instance profile
    sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
    if err != nil {
        log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
    }

    creds := credentials.Credentials{
        AccessKeyID:      sdkCreds.AccessKeyID,

```

```

        SecretAccessKey: sdkCreds.SecretAccessKey,
        SessionToken:    sdkCreds.SessionToken,
    }

    // Add a payload body, which will not be part of the signature calculation
    body := nopCloser{strings.NewReader(`Example payload body`)}

    req, _ := http.NewRequest(http.MethodPost, url.value, body)

    // Create a sigv4a signer with specific options
    signer := sigv4a.New(func(o *v4.SignerOptions) {
        o.DisableDoublePathEscape = true
        // This will add the UNSIGNED-PAYLOAD sha256 header
        o.AddPayloadHashHeader = true
        o.DisableImplicitPayloadHashing = true
    })

    // Create a slice out of the provided regionset
    rs := strings.Split(regionSet.value, ",")

    // Perform the signing on req, using the credentials we retrieved from the
    SDK err = signer.SignRequest(&sigv4a.SignRequestInput{
        Request:    req,
        Credentials: creds,
        Service:     "vpc-lattice-svcs",
        RegionSet: rs,
    })

    if err != nil {
        log.Fatalf("%s", err)
    }

    res, err := httputil.DumpRequest(req, true)

    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Raw request\n%s\n", string(res))

    log.Printf("[*] Sending request to %s\n", url.value)

    resp, err := http.DefaultClient.Do(req)

```

```
    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Request sent\n")

    log.Printf("[*] Response status code: %d\n", resp.StatusCode)

    respBody, err := io.ReadAll(resp.Body)
    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Response body: \n%s\n", respBody)
}
```

Golang - GRPC

Questo esempio utilizza l'[AWS SDK per il linguaggio di programmazione Go per gestire la](#) firma delle richieste per le richieste GRPC. Questo può essere usato con il [server echo](#) del repository di codici di esempio GRPC.

```
package main

import (
    "context"
    "crypto/tls"
    "crypto/x509"

    "flag"
    "fmt"
    "log"
    "net/http"
    "net/url"
    "strings"
    "time"

    "google.golang.org/grpc"
    "google.golang.org/grpc/credentials"

    "github.com/aws/aws-sdk-go-v2/aws"
    v4 "github.com/aws/aws-sdk-go-v2/aws/signer/v4"
```

```

    "github.com/aws/aws-sdk-go-v2/config"

    ecpb "google.golang.org/grpc/examples/features/proto/echo"
)

const (
    headerContentSha      = "x-amz-content-sha256"
    headerSecurityToken    = "x-amz-security-token"
    headerDate             = "x-amz-date"
    headerAuthorization    = "authorization"
    unsignedPayload        = "UNSIGNED-PAYLOAD"
)

type SigV4GrpcSigner struct {
    service      string
    region       string
    credProvider aws.CredentialsProvider
    signer       *v4.Signer
}

func NewSigV4GrpcSigner(service string, region string, credProvider
aws.CredentialsProvider) *SigV4GrpcSigner {
    signer := v4.NewSigner()
    return &SigV4GrpcSigner{
        service:      service,
        region:       region,
        credProvider: credProvider,
        signer:       signer,
    }
}

func (s *SigV4GrpcSigner) GetRequestMetadata(ctx context.Context, uri ...string)
(map[string]string, error) {
    ri, _ := credentials.RequestInfoFromContext(ctx)
    creds, err := s.credProvider.Retrieve(ctx)
    if err != nil {
        return nil, fmt.Errorf("failed to load credentials: %w", err)
    }

    // The URI we get here is scheme://authority/service/ - for signing we want to
    include the RPC name
    // But RequestInfoFromContext only has the combined /service/rpc-name - so read the
    URI, and
    // replace the Path with what we get from RequestInfo.

```

```

    parsed, err := url.Parse(uri[0])
    if err != nil {
        return nil, err
    }
    parsed.Path = ri.Method

    // Build a request for the signer.
    bodyReader := strings.NewReader("")
    req, err := http.NewRequest("POST", uri[0], bodyReader)
    if err != nil {
        return nil, err
    }
    date := time.Now()
    req.Header.Set(headerContentSha, unsignedPayload)
    req.Header.Set(headerDate, date.String())
    if creds.SessionToken != "" {
        req.Header.Set(headerSecurityToken, creds.SessionToken)
    }
    // The signer wants this as //authority/path
    // So get this by trimming off the scheme and the colon before the first slash.
    req.URL.Opaque = strings.TrimPrefix(parsed.String(), parsed.Scheme+":")

    err = s.signer.SignHTTP(context.Background(), creds, req, unsignedPayload,
s.service, s.region, date)
    if err != nil {
        return nil, fmt.Errorf("failed to sign request: %w", err)
    }

    // Pull the relevant headers out of the signer, and return them to get
    // included in the request we make.
    reqHeaders := map[string]string{
        headerContentSha: req.Header.Get(headerContentSha),
        headerDate:       req.Header.Get(headerDate),
        headerAuthorization: req.Header.Get(headerAuthorization),
    }
    if req.Header.Get(headerSecurityToken) != "" {
        reqHeaders[headerSecurityToken] = req.Header.Get(headerSecurityToken)
    }

    return reqHeaders, nil
}

func (c *SigV4GrpcSigner) RequireTransportSecurity() bool {
    return true
}

```

```

}

var addr = flag.String("addr", "some-lattice-service:443", "the address to connect to")
var region = flag.String("region", "us-west-2", "region")

func callUnaryEcho(client ecspb.EchoClient, message string) {
    ctx, cancel := context.WithTimeout(context.Background(), 10*time.Second)
    defer cancel()
    resp, err := client.UnaryEcho(ctx, &ecspb.EchoRequest{Message: message})
    if err != nil {
        log.Fatalf("client.UnaryEcho(_) = _, %v: ", err)
    }
    fmt.Println("UnaryEcho: ", resp.Message)
}

func main() {
    flag.Parse()
    cfg, err := config.LoadDefaultConfig(context.TODO(),
    config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    pool, _ := x509.SystemCertPool()
    tlsConfig := &tls.Config{
        RootCAs: pool,
    }

    authority, _, _ := strings.Cut(*addr, ":") // Remove the port from the addr
    opts := []grpc.DialOption{
        grpc.WithTransportCredentials(credentials.NewTLS(tlsConfig)),

        // Lattice needs both the Authority to be set (without a port), and the SigV4
    signer
        grpc.WithAuthority(authority),
        grpc.WithPerRPCCredentials(NewSigV4GrpcSigner("vpc-lattice-svcs", *region,
    cfg.Credentials)),
    }

    conn, err := grpc.Dial(*addr, opts...)

    if err != nil {
        log.Fatalf("did not connect: %v", err)
    }
}

```

```
defer conn.Close()
rgc := ecpb.NewEchoClient(conn)

callUnaryEcho(rgc, "hello world")
}
```

Protezione dei dati in Amazon VPC Lattice

Il modello di [responsabilità AWS condivisa modello](#) si applica alla protezione dei dati in Amazon VPC Lattice. 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. Questi contenuti comprendono la configurazione della protezione e le attività di gestione per i Servizi AWS utilizzati. 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 [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

Crittografia dei dati in transito

VPC Lattice è un servizio completamente gestito che consiste in un piano di controllo e un piano dati. Ogni piano ha uno scopo distinto nel servizio. Il piano di controllo fornisce le API amministrative utilizzate per creare, aggiornare read/describe, eliminare ed elencare le risorse (CRUDL) (ad esempio e). CreateService UpdateService Le comunicazioni verso il piano di controllo VPC Lattice sono protette in transito da TLS. Il piano dati è l'API VPC Lattice Invoke, che fornisce l'interconnessione tra i servizi. TLS crittografa le comunicazioni sul piano dati VPC Lattice quando utilizzi HTTPS o TLS. La suite di crittografia e la versione del protocollo utilizzano i valori predefiniti forniti da VPC Lattice e non sono configurabili. Per ulteriori informazioni, consulta [Listener HTTPS per servizi VPC Lattice](#).

Crittografia dei dati a riposo

Per impostazione predefinita, la crittografia dei dati inattivi aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili. Allo stesso tempo, consente di creare applicazioni sicure che soddisfano i rigorosi requisiti normativi e di conformità alla crittografia.

Indice

- [Server-side crittografia con chiavi gestite Amazon S3 \(\) SSE-S3](#)
- [Server-side crittografia con AWS KMS chiavi memorizzate in AWS KMS \(SSE-KMS\)](#)

Server-side crittografia con chiavi gestite Amazon S3 () SSE-S3

Quando utilizzi la crittografia lato server con chiavi gestite di Amazon S3 SSE-S3 (), ogni oggetto viene crittografato con una chiave unica. Come ulteriore protezione, crittografiamo la chiave stessa con una chiave radice che ruotiamo regolarmente. La crittografia lato server di Amazon S3 utilizza uno dei cifrari a blocchi più potenti disponibili, l'Advanced Encryption Standard () GCM a 256 bit, per crittografare i dati. AES-256 Per gli oggetti crittografati in precedenza, è ancora supportata la decrittografia di tali oggetti. AES-GCM AES-CBC Per ulteriori informazioni, consulta [Usare la crittografia lato server con le chiavi di S3-managed crittografia Amazon \(\) SSE-S3](#).

Se abiliti la crittografia lato server con le chiavi di S3-managed crittografia Amazon (SSE-S3) per il tuo bucket S3 per i log di accesso VPC Lattice, crittografiamo automaticamente ogni file di registro di accesso prima che venga archiviato nel tuo bucket S3. Per ulteriori informazioni, consulta [Logs sent to Amazon S3 nella CloudWatch Amazon User Guide](#).

Server-side crittografia con AWS KMS chiavi memorizzate in AWS KMS (SSE-KMS)

Server-side la crittografia con AWS KMS keys (SSE-KMS) è simile a SSE-S3, ma comporta vantaggi e costi aggiuntivi per l'utilizzo di questo servizio. Esistono autorizzazioni separate per la AWS KMS chiave che forniscono una protezione aggiuntiva contro l'accesso non autorizzato ai tuoi oggetti in Amazon S3. SSE-KMS ti fornisce anche una pista di controllo che mostra quando è stata utilizzata la AWS KMS chiave e da chi. Per ulteriori informazioni, consulta [Utilizzo della crittografia lato server con AWS Key Management Service \(\) SSE-KMS](#).

Indice

- [Crittografia e decrittografia della chiave privata del certificato](#)
- [Contesto di crittografia per VPC Lattice](#)
- [Monitoraggio delle chiavi di crittografia per VPC Lattice](#)

Crittografia e decrittografia della chiave privata del certificato

Il certificato ACM e la chiave privata sono crittografati utilizzando una chiave KMS AWS gestita con l'alias. aws/acm Puoi visualizzare l'ID della chiave con questo alias nella AWS KMS console in Chiavi gestite.AWS

VPC Lattice non accede direttamente alle tue risorse ACM. Utilizza AWS TLS Connection Manager per proteggere e accedere alle chiavi private del certificato. Quando si utilizza il certificato ACM

per creare un servizio VPC Lattice, VPC Lattice associa il certificato a TLS Connection Manager. AWS Questo viene fatto creando una concessione in base alla tua Managed Key con il AWS KMS prefisso. AWS aws/acm La concessione è uno strumento delle policy che permette a TLS Connection Manager di usare le chiavi KMS nelle operazioni di crittografia. La concessione consente al principale assegnatario (TLS Connection Manager) di chiamare le operazioni di concessione specificate nella chiave KMS per decrittografare la chiave privata del certificato. TLS Connection Manager utilizza quindi il certificato e la chiave privata decrittografata (testo semplice) per stabilire una connessione sicura (SSL/TLS sessione) con i client dei servizi VPC Lattice. Quando il certificato viene dissociato da un servizio VPC Lattice, la concessione viene ritirata.

Se desideri rimuovere l'accesso alla chiave KMS, ti consigliamo di sostituire o eliminare il certificato dal servizio utilizzando AWS Management Console o il comando `update-service` AWS CLI

Contesto di crittografia per VPC Lattice

Un [contesto di crittografia](#) è un insieme opzionale di coppie chiave-valore che contengono informazioni contestuali sullo scopo per cui potrebbe essere utilizzata la chiave privata. AWS KMS associa il contesto di crittografia ai dati crittografati e lo utilizza come dati autenticati aggiuntivi per supportare la crittografia autenticata.

Quando le chiavi TLS vengono utilizzate con VPC Lattice e TLS Connection Manager, il nome del servizio VPC Lattice viene incluso nel contesto di crittografia utilizzato per crittografare la chiave inattiva. Puoi verificare per quale servizio VPC Lattice vengono utilizzati il tuo certificato e la tua chiave privata visualizzando il contesto di crittografia nei tuoi CloudTrail log, come mostrato nella sezione successiva, o consultando la scheda Risorse associate nella console ACM.

Per decrittografare i dati, includere nella richiesta lo stesso contesto di crittografia. VPC Lattice utilizza lo stesso contesto di crittografia in tutte le operazioni crittografiche AWS KMS, in cui la chiave è `aws:vpc-lattice:arn` e il valore è l'Amazon Resource Name (ARN) del servizio VPC Lattice.

L'esempio illustrato di seguito mostra il contesto di crittografia nell'output di un'operazione come `CreateGrant`.

```
"encryptionContextEquals": {
  "aws:acm:arn": "arn:aws:acm:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/svc-0b23c1234567890ab"
}
```

Monitoraggio delle chiavi di crittografia per VPC Lattice

Quando utilizzi una chiave AWS gestita con il tuo servizio VPC Lattice, puoi utilizzarla [AWS CloudTrail](#) per tenere traccia delle richieste a cui invia VPC Lattice. AWS KMS

CreateGrant

Quando aggiungi il tuo certificato ACM a un servizio VPC Lattice, viene inviata CreateGrant una richiesta per tuo conto affinché TLS Connection Manager sia in grado di decrittografare la chiave privata associata al tuo certificato ACM

È possibile visualizzare l'**CreateGrant** operazione come evento in, Cronologia eventi, CloudTrailCreateGrant

Di seguito è riportato un esempio di record di CloudTrail eventi nella cronologia degli eventi dell'CreateGrant operazione.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accountId": "111122223333",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "userName": "Alice"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-02-06T23:30:50Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "acm.amazonaws.com"
  },
  "eventTime": "2023-02-07T00:07:18Z",
  "eventSource": "kms.amazonaws.com",
```

```

    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "acm.amazonaws.com",
    "userAgent": "acm.amazonaws.com",
    "requestParameters": {
      "granteePrincipal": "tlsconnectionmanager.amazonaws.com",
      "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "operations": [
        "Decrypt"
      ],
      "constraints": {
        "encryptionContextEquals": {
          "aws:acm:arn": "arn:aws:acm:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/svc-0b23c1234567890ab"
        }
      },
      "retiringPrincipal": "acm.us-west-2.amazonaws.com"
    },
    "responseElements": {
      "grantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
      "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ba178361-8ab6-4bdd-9aa2-0d1a44b2974a",
    "eventID": "8d449963-1120-4d0c-9479-f76de11ce609",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  }
}

```

Nell'`CreateGrant` esempio precedente, il principale beneficiario è TLS Connection Manager e il contesto di crittografia ha il servizio VPC Lattice ARN.

ListGrants

Puoi usare l'ID della tua chiave KMS e l'ID del tuo account per chiamare l'API. `ListGrants` In questo modo otterrai un elenco di tutte le concessioni per la chiave KMS specificata. Per ulteriori informazioni, consulta [ListGrants](#).

Usa il seguente `ListGrants` comando in AWS CLI per vedere i dettagli di tutte le sovvenzioni.

```
aws kms list-grants --key-id your-kms-key-id
```

Di seguito è riportato un output di esempio.

```
{
  "Grants": [
    {
      "Operations": [
        "Decrypt"
      ],
      "KeyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "Name": "IssuedThroughACM",
      "RetiringPrincipal": "acm.us-west-2.amazonaws.com",
      "GranteePrincipal": "tlsconnectionmanager.amazonaws.com",
      "GrantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
      "IssuingAccount": "arn:aws:iam::111122223333:root",
      "CreationDate": "2023-02-06T23:30:50Z",
      "Constraints": {
        "encryptionContextEquals": {
          "aws:acm:arn": "arn:aws:acm:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/svc-0b23c1234567890ab"
        }
      }
    }
  ]
}
```

Nell'`ListGrant` esempio precedente, il principale beneficiario è TLS Connection Manager e il contesto di crittografia ha il servizio VPC Lattice ARN.

Decrypt

VPC Lattice utilizza TLS Connection Manager per richiamare l'Decrypt operazione di decrittografia della chiave privata al fine di servire le connessioni TLS nel servizio VPC Lattice. È possibile visualizzare l'**Decrypt** operazione come un evento in Cronologia eventi, Decrypt. CloudTrail

Di seguito è riportato un esempio di record di eventi nella cronologia CloudTrail degli eventi dell'Decrypt operazione.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "tlsconnectionmanager.amazonaws.com"
  },
  "eventTime": "2023-02-07T00:07:23Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "tlsconnectionmanager.amazonaws.com",
  "userAgent": "tlsconnectionmanager.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws:acm:arn": "arn:aws:acm:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/svc-0b23c1234567890ab"
    },
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "12345126-30d5-4b28-98b9-9153da559963",
  "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

```
}  
],  
"eventType": "AwsApiCall",  
"managementEvent": true,  
"recipientAccountId": "111122223333",  
"sharedEventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",  
"eventCategory": "Management"  
}
```

Gestione delle identità e degli accessi per Amazon VPC Lattice

Le sezioni seguenti descrivono come utilizzare AWS Identity and Access Management (IAM) per proteggere le risorse VPC Lattice, controllando chi può eseguire le azioni dell'API VPC Lattice.

Argomenti

- [Come funziona Amazon VPC Lattice con IAM](#)
- [Autorizzazioni dell'API Amazon VPC Lattice](#)
- [Identity-based politiche per Amazon VPC Lattice](#)
- [Utilizzo di ruoli collegati ai servizi per Amazon VPC Lattice](#)
- [AWS politiche gestite per Amazon VPC Lattice](#)

Come funziona Amazon VPC Lattice con IAM

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

Funzionalità IAM	Supporto VPC Lattice
Identity-based politiche	Sì
Resource-based politiche	Sì
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì

Funzionalità IAM	Supporto VPC Lattice
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Ruoli di servizio	No
Service-linked ruoli	Sì

Per una visione di alto livello di come VPC Lattice e AWS altri servizi funzionano con la maggior parte delle funzionalità IAM, [AWS consulta i servizi che funzionano con](#) IAM nella IAM User Guide.

Identity-based politiche per VPC Lattice

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti di policy sulle autorizzazioni JSON che puoi allegare a un'identità, ad esempio un utente IAM, un gruppo di utenti o un ruolo. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'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. 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 IAM.

Resource-based politiche all'interno di VPC Lattice

Supporta le policy basate sulle risorse: sì

Resource-based le politiche sono documenti di policy JSON allegati a una risorsa in AWS. Nei AWS servizi che supportano le politiche basate sulle risorse, gli amministratori del servizio possono utilizzarle per controllare l'accesso a una risorsa specifica di quel servizio. AWS Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

VPC Lattice supporta le politiche di autenticazione, una politica basata sulle risorse che consente di controllare l'accesso ai servizi nella rete di servizi. Per ulteriori informazioni, consulta [Controlla l'accesso ai servizi VPC Lattice utilizzando le policy di autenticazione](#).

VPC Lattice supporta anche politiche di autorizzazione basate sulle risorse per l'integrazione con AWS Resource Access Manager. È possibile utilizzare queste politiche basate sulle risorse per concedere l'autorizzazione a gestire la connettività ad altri AWS account o organizzazioni per servizi, configurazioni di risorse e reti di servizi. Per ulteriori informazioni, consulta [Condivisione delle entità di VPC Lattice](#).

Azioni politiche per VPC Lattice

Supporta le operazioni di policy: sì

In una dichiarazione di policy IAM, è possibile specificare qualsiasi operazione API per qualsiasi servizio che supporta IAM. Per VPC Lattice, utilizza il seguente prefisso con il nome dell'azione API: `vpc-lattice`. For example: `vpc-lattice:CreateService`, `vpc-lattice:CreateTargetGroup` e `vpc-lattice:PutAuthPolicy`.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola, come mostrato di seguito:

```
"Action": [ "vpc-lattice:action1", "vpc-lattice:action2" ]
```

Puoi anche specificare più operazioni tramite caratteri jolly. Ad esempio, puoi specificare tutte le operazioni i cui nomi iniziano con la parola `Get` come segue:

```
"Action": "vpc-lattice:Get*"
```

Per un elenco completo delle azioni dell'API VPC Lattice, consulta Azioni definite [da Amazon VPC Lattice](#) nel Service Authorization Reference.

Risorse politiche per VPC Lattice

Supporta le risorse relative alle policy: sì

In una dichiarazione di policy IAM, l'elemento `Resource` specifica l'oggetto o gli oggetti coperti dall'istruzione. Per VPC Lattice, ogni dichiarazione di policy IAM si applica alle risorse specificate utilizzando i relativi ARN.

Il formato specifico di Amazon Resource Name (ARN) dipende dalla risorsa. Quando fornisci un ARN, sostituisci il *italicized* testo con le informazioni specifiche della risorsa.

- Accedi agli abbonamenti ai registri:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:accesslogsubscription/access-log-subscription-id"
```

- Ascoltatori:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/listener/listener-id"
```

- Gateway per le risorse

```
"Resource": "arn:aws:vpc-lattice:region:account-id:resourcegateway/resource-gateway-id"
```

- Configurazione delle risorse

```
"Resource": "arn:aws:vpc-lattice:region:account-id:resourceconfiguration/resource-configuration-id"
```

- Regole:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/listener/listener-id/rule/rule-id"
```

- Servizi:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id"
```

- Reti di servizio:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetwork/service-network-id"
```

- Associazioni di servizi di rete di servizi:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetworkserviceassociation/service-network-service-association-id"
```

- Associazioni di configurazione delle risorse di rete di servizio

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetworkresourceassociation/service-network-resource-association-id"
```

- Associazioni VPC della rete di assistenza:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetworkvpcassociation/service-network-vpc-association-id"
```

- Gruppi target:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:targetgroup/target-group-id"
```

Chiavi relative alle condizioni delle policy per VPC Lattice

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

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

L'elemento Condition specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. 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 VPC Lattice, consulta Condition keys [for Amazon VPC Lattice](#) nel Service Authorization Reference.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per informazioni sulle chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Elenchi di controllo degli accessi (ACL) in VPC Lattice

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.

Attribute-based controllo accessi (ABAC) con VPC Lattice

Supporta ABAC (tag nelle policy): sì

Attribute-based il controllo degli accessi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. È possibile allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di 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 VPC Lattice

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

Ruoli di servizio per VPC Lattice

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 [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

 Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità VPC Lattice. Modifica i ruoli di servizio solo quando VPC Lattice fornisce indicazioni in tal senso.

Service-linked ruoli per VPC Lattice

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 di eseguire un'azione per conto dell'utente. Service-linked i ruoli appaiono nel tuo Account AWS account e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni sulla creazione o la gestione di ruoli collegati ai servizi VPC Lattice, vedere. [Utilizzo di ruoli collegati ai servizi per Amazon VPC Lattice](#)

Autorizzazioni dell'API Amazon VPC Lattice

È necessario concedere alle identità IAM (come utenti o ruoli) l'autorizzazione a richiamare le azioni dell'API VPC Lattice di cui hanno bisogno, come descritto in. [Azioni politiche per VPC Lattice](#) Inoltre, per alcune azioni VPC Lattice, devi concedere alle identità IAM l'autorizzazione a richiamare azioni specifiche da altre API. AWS

Autorizzazioni richieste per le API

Quando richiami le seguenti azioni dall'API, devi concedere agli utenti IAM l'autorizzazione a chiamare le azioni specificate.

CreateResourceConfiguration

- vpc-lattice:CreateResourceConfiguration
- ec2:DescribeSubnets
- rds:DescribeDBInstances
- rds:DescribeDBClusters

CreateResourceGateway

- vpc-lattice:CreateResourceGateway

- `ec2:AssignPrivateIpAddresses`
- `ec2:AssignIpv6Addresses`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`

DeleteResourceGateway

- `vpc-lattice>DeleteResourceGateway`
- `ec2>DeleteNetworkInterface`

UpdateResourceGateway

- `vpc-lattice:UpdateResourceGateway`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssignIpv6Addresses`
- `ec2:UnassignPrivateIpAddresses`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`

CreateServiceNetworkResourceAssociation

- `vpc-lattice>CreateServiceNetworkResourceAssociation`
- `ec2:AssignIpv6Addresses`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeNetworkInterfaces`

CreateServiceNetworkVpcAssociation

- `vpc-lattice:CreateServiceNetworkVpcAssociation`
- `ec2:DescribeVpcs`
- `ec2:DescribeSecurityGroups`(Necessario solo quando vengono forniti gruppi di sicurezza)

UpdateServiceNetworkVpcAssociation

- `vpc-lattice:UpdateServiceNetworkVpcAssociation`
- `ec2:DescribeSecurityGroups`(Necessario solo quando vengono forniti gruppi di sicurezza)

CreateTargetGroup

- `vpc-lattice:CreateTargetGroup`
- `ec2:DescribeVpcs`

RegisterTargets

- `vpc-lattice:RegisterTargets`
- `ec2:DescribeInstances`(Necessario solo quando INSTANCE si tratta del tipo di gruppo target)
- `ec2:DescribeVpcs`(Necessario solo quando INSTANCE o IP è il tipo di gruppo target)
- `ec2:DescribeSubnets`(Necessario solo quando INSTANCE o IP è il tipo di gruppo target)
- `lambda:GetFunction`(Necessario solo quando LAMBDA si tratta del tipo di gruppo target)
- `lambda:AddPermission`(Necessario solo se il gruppo target non dispone già dell'autorizzazione per richiamare la funzione Lambda specificata)

DeregisterTargets

- `vpc-lattice:DeregisterTargets`

CreateAccessLogSubscription

- `vpc-lattice:CreateAccessLogSubscription`
- `logs:GetLogDelivery`
- `logs:CreateLogDelivery`

DeleteAccessLogSubscription

- `vpc-lattice>DeleteAccessLogSubscription`
- `logs>DeleteLogDelivery`

UpdateAccessLogSubscription

- `vpc-lattice:UpdateAccessLogSubscription`
- `logs:UpdateLogDelivery`

Identity-based politiche per Amazon VPC Lattice

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse VPC Lattice. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

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

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da VPC Lattice, incluso il formato degli ARN per ciascun tipo di risorsa, consulta [Actions, Resources and Condition Keys for Amazon VPC Lattice](#) nel Service Authorization Reference.

Indice

- [Best practice per le policy](#)
- [Autorizzazioni aggiuntive richieste per l'accesso completo](#)
- [Identity-based esempi di policy per VPC Lattice](#)

Best practice per le policy

Identity-based le politiche determinano se qualcuno può creare, accedere o eliminare le risorse VPC Lattice nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

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

Autorizzazioni aggiuntive richieste per l'accesso completo

Per utilizzare altri AWS servizi con cui è integrato VPC Lattice e l'intera suite di funzionalità VPC Lattice, è necessario disporre di autorizzazioni aggiuntive specifiche. [Queste autorizzazioni non sono incluse nella policy VPCLatticeFullAccess gestita a causa del rischio confuso di un'escalation dei privilegi secondari.](#)

È necessario allegare la seguente politica al proprio ruolo e utilizzarla insieme alla politica gestita. VPCLatticeFullAccess

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

        "Action": [
            "firehose:TagDeliveryStream",
            "lambda:AddPermission",
            "s3:PutBucketPolicy"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "logs:PutResourcePolicy"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:CalledVia": [
                    "vpc-lattice.amazonaws.com"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/AWSServiceRoleForVpcLattice"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:AttachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery*"
    }
]
}

```

Questa politica fornisce le seguenti autorizzazioni aggiuntive:

- `iam:AttachRolePolicy`: consente di allegare la politica gestita specificata al ruolo IAM specificato.
- `iam:PutRolePolicy`: Consente di aggiungere o aggiornare un documento di policy in linea incorporato nel ruolo IAM specificato.
- `s3:PutBucketPolicy`: consente di applicare una policy sui bucket a un bucket Amazon S3.
- `firehose:TagDeliveryStream`: consente di aggiungere o aggiornare i tag per i flussi di distribuzione di Firehose.

Identity-based esempi di policy per VPC Lattice

Argomenti

- [Politica di esempio: gestione delle associazioni VPC a una rete di servizi](#)
- [Politica di esempio: creare associazioni di servizi a una rete di servizi](#)
- [Esempio di politica: aggiungere tag alle risorse](#)
- [Politica di esempio: creare un ruolo collegato al servizio](#)

Politica di esempio: gestione delle associazioni VPC a una rete di servizi

L'esempio seguente mostra una politica che offre agli utenti con questa politica l'autorizzazione a creare, aggiornare ed eliminare le associazioni VPC su una rete di servizi, ma solo per il VPC e la rete di servizi specificati nella condizione. Per ulteriori informazioni su come specificare le chiavi di condizione, consulta [Chiavi relative alle condizioni delle policy per VPC Lattice](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc-lattice:CreateServiceNetworkVpcAssociation",
        "vpc-lattice:UpdateServiceNetworkVpcAssociation",
        "vpc-lattice>DeleteServiceNetworkVpcAssociation"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringEquals": {
        "vpc-lattice:ServiceNetworkArn": "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetwork/sn-903004f88example",
        "vpc-lattice:VpcId": "vpc-1a2b3c4d"
      }
    }
  }
]
}

```

Politica di esempio: creare associazioni di servizi a una rete di servizi

Se non utilizzi le chiavi di condizione per controllare l'accesso alle risorse VPC Lattice, puoi invece specificare gli ARN delle risorse nell'`Resource` elemento per controllare l'accesso.

L'esempio seguente mostra una politica che limita le associazioni di servizi a una rete di servizi che gli utenti con questa politica possono creare specificando gli ARN del servizio e della rete di servizi che possono essere utilizzati con l'azione `API. CreateServiceNetworkServiceAssociation`. Per ulteriori informazioni sulla specificazione dei valori ARN, vedere. [Risorse politiche per VPC Lattice](#)

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc-lattice:CreateServiceNetworkServiceAssociation"
      ],
      "Resource": [
        "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetworkserviceassociation/*",
        "arn:aws:vpc-lattice:us-west-2:123456789012:service/
svc-04d5cc9b88example",
        "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/
sn-903004f88example"
      ]
    }
  ]
}

```

```
}  
]  
}
```

Esempio di politica: aggiungere tag alle risorse

L'esempio seguente mostra una politica che offre agli utenti con questa politica il permesso di creare tag sulle risorse VPC Lattice.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "vpc-lattice:TagResource"  
      ],  
      "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/**"  
    }  
  ]  
}
```

Politica di esempio: creare un ruolo collegato al servizio

VPC Lattice richiede le autorizzazioni per creare un ruolo collegato ai servizi la prima volta che un utente crea risorse VPC Lattice. Account AWS Se il ruolo collegato al servizio non esiste già, VPC Lattice lo crea nel tuo account. Il ruolo collegato al servizio fornisce le autorizzazioni a VPC Lattice in modo che possa chiamare altri utenti per tuo conto. Servizi AWS Per ulteriori informazioni, consulta [the section called “Uso di ruoli collegati ai servizi”](#).

Affinché la creazione automatica di un ruolo riesca, gli utenti devono disporre delle autorizzazioni per l'operazione `iam:CreateServiceLinkedRole`.

```
"Action": "iam:CreateServiceLinkedRole"
```

L'esempio seguente mostra una politica che fornisce agli utenti con questa politica l'autorizzazione a creare un ruolo collegato al servizio per VPC Lattice.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/AWSServiceRoleForVpcLattice",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "vpc-lattice.amazonaws.com"
        }
      }
    }
  ]
}
```

Per ulteriori informazioni, consulta le [autorizzazioni dei Service-linked ruoli nella Guida per l'utente IAM](#).

Utilizzo di ruoli collegati ai servizi per Amazon VPC Lattice

Amazon VPC Lattice utilizza un ruolo collegato al servizio per le autorizzazioni necessarie per chiamare altri utenti per tuo conto. Servizi AWS Per ulteriori informazioni, consulta i [Service-linked ruoli](#) nella IAM User Guide.

VPC Lattice utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForVpcLattice`

Service-linked autorizzazioni di ruolo per VPC Lattice

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForVpcLattice` considera attendibile il seguente servizio:

- `vpc-lattice.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AWSVpcLatticeServiceRolePolicy` consente a VPC Lattice di CloudWatch pubblicare metriche nel namespace. `AWS/VpcLattice` Per ulteriori informazioni, consulta [AWSVpcLatticeServiceRolePolicy](#) il Managed Policy Reference. `AWS`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [the section called “Politica di esempio: creare un ruolo collegato al servizio”](#).

Crea un ruolo collegato ai servizi per VPC Lattice

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei risorse VPC Lattice nell'API AWS Management Console AWS , VPC Lattice crea automaticamente il ruolo collegato al servizio. AWS CLI

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei risorse VPC Lattice, VPC Lattice crea nuovamente il ruolo collegato al servizio per te.

Modifica un ruolo collegato ai servizi per VPC Lattice

Puoi modificare la descrizione dell'utilizzo di IAM. `AWSServiceRoleForVpcLattice` Per ulteriori informazioni, consulta [Edit a service-linked role description](#) nella Guida per l'utente IAM.

Eliminare un ruolo collegato al servizio per VPC Lattice

Se non hai più bisogno di usare Amazon VPC Lattice, ti consigliamo di eliminarlo.
`AWSServiceRoleForVpcLattice`

Puoi eliminare questo ruolo collegato al servizio solo dopo aver eliminato tutte le risorse VPC Lattice presenti nel tuo. Account AWS

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al servizio. `AWSServiceRoleForVpcLattice` Per ulteriori dettagli, consulta [Delete a service-linked role](#) nella Guida per l'utente IAM.

Dopo aver eliminato un ruolo collegato al servizio, VPC Lattice crea nuovamente il ruolo quando crei risorse VPC Lattice nel tuo. Account AWS

Regioni supportate per i ruoli collegati ai servizi VPC Lattice

VPC Lattice supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile.

AWS politiche gestite per Amazon VPC Lattice

Una policy AWS gestita è una policy autonoma creata e amministrata da 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 si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. 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 nel Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: VPCLatticeFullAccess

Questa policy fornisce l'accesso completo ad Amazon VPC Lattice e un accesso limitato ad altri servizi dipendenti. Include le autorizzazioni per eseguire le seguenti operazioni:

- ACM: recupera l' SSL/TLS ARN del certificato per i nomi di dominio personalizzati.
- CloudWatch — Visualizza i registri di accesso e i dati di monitoraggio.
- CloudWatch Registri: configura e invia i registri di accesso ai registri. CloudWatch
- Amazon EC2: configura le interfacce di rete e recupera informazioni sulle istanze EC2 e sui VPC. Viene utilizzato per creare configurazioni di risorse, gateway di risorse e gruppi target, configurare associazioni di entità VPC Lattice e registrare destinazioni.
- Elastic Load Balancing: recupera informazioni su un Application Load Balancer per registrarlo come destinazione.
- Firehose: recupera informazioni sui flussi di consegna utilizzati per archiviare i log di accesso.
- Lambda — Recupera informazioni su una funzione Lambda per registrarla come destinazione.
- Amazon RDS: recupera informazioni su cluster e istanze RDS.
- Amazon S3: recupera informazioni sui bucket S3 utilizzati per archiviare i log di accesso.

Per vedere le autorizzazioni per questa policy, consulta [VPC_Lattice_Full_Access](#) nella Guida di riferimento sulle policy gestite da AWS .

Per utilizzare altri AWS servizi con cui è integrato VPC Lattice e l'intera suite di funzionalità VPC Lattice, è necessario disporre di autorizzazioni aggiuntive specifiche. [Queste autorizzazioni non sono incluse nella policy VPC_Lattice_Full_Access gestita a causa del rischio confuso di un'escalation dei privilegi secondari](#). Per ulteriori informazioni, consulta [Autorizzazioni aggiuntive richieste per l'accesso completo](#).

AWS politica gestita: VPC_Lattice_Read_Only_Access

Questa policy fornisce l'accesso in sola lettura ad Amazon VPC Lattice e l'accesso limitato ad altri servizi dipendenti. Include le autorizzazioni per eseguire le seguenti operazioni:

- ACM: recupera l' SSL/TLS ARN del certificato per i nomi di dominio personalizzati.
- CloudWatch — Visualizza i registri di accesso e i dati di monitoraggio.
- CloudWatch Registri: visualizza le informazioni sulla consegna dei log per le sottoscrizioni ai log di accesso.
- Amazon EC2: recupera informazioni sulle istanze EC2 e sui VPC per creare gruppi target e registrarli.
- Elastic Load Balancing: recupera informazioni su un Application Load Balancer.
- Firehose: recupera informazioni sui flussi di consegna per la consegna dei log di accesso.
- Lambda: visualizza informazioni su una funzione Lambda.
- Amazon RDS: recupera informazioni su cluster e istanze RDS.
- Amazon S3: recupera informazioni sui bucket S3 per la consegna dei log di accesso.

Per vedere le autorizzazioni per questa policy, consulta [VPC_Lattice_Read_Only_Access](#) nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: VPC_Lattice_Services_Invoke_Access

Questa policy fornisce l'accesso per richiamare i servizi Amazon VPC Lattice.

Per vedere le autorizzazioni per questa policy, consulta [VPC_Lattice_Services_Invoke_Access](#) nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSVpcLatticeServiceRolePolicy

Questa policy è associata a un ruolo collegato al servizio denominato `AWSServiceRoleForVpcLattice` per consentire a VPC Lattice di eseguire azioni per tuo conto. Non è possibile attribuire questa policy alle entità IAM. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per Amazon VPC Lattice](#).

Per vedere le autorizzazioni per questa policy, consulta [AWSVpcLatticeServiceRolePolicy](#) nella Guida di riferimento sulle policy gestite da AWS.

VPC Lattice si aggiorna a AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per VPC Lattice da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS per la VPC Lattice User Guide.

Modifica	Descrizione	Data
VPC Lattice Full Access	VPC Lattice aggiunge autorizzazioni di sola lettura per descrivere i cluster e le istanze di Amazon RDS.	1 dicembre 2024
VPC Lattice Read Only Access	VPC Lattice aggiunge autorizzazioni di sola lettura per descrivere i cluster e le istanze di Amazon RDS.	1 dicembre 2024
AWSVpcLatticeServiceRolePolicy	VPC Lattice aggiunge le autorizzazioni per consentire a VPC Lattice di creare un'interfaccia di rete gestita dal richiedente.	1 dicembre 2024
VPC Lattice Full Access	VPC Lattice aggiunge una nuova policy per concedere le autorizzazioni per l'accesso completo ad Amazon VPC Lattice e l'accesso limitato ad altri servizi dipendenti.	31 marzo 2023
VPC Lattice Read Only Access	VPC Lattice aggiunge una nuova policy per concedere le autorizza	31 marzo 2023

Modifica	Descrizione	Data
	zioni per l'accesso in sola lettura ad Amazon VPC Lattice e l'accesso limitato ad altri servizi dipendenti.	
VPC Lattice Services Invoke Access	VPC Lattice aggiunge una nuova policy per concedere l'accesso per richiamare i servizi Amazon VPC Lattice.	31 marzo 2023
AWS VPC Lattice Service Role Policy	VPC Lattice aggiunge le autorizzazioni al suo ruolo collegato ai servizi per consentire a VPC Lattice di pubblicare metriche nel namespace. CloudWatch AWS/VpcLattice La policy include il permesso di richiamare l'azione dell'API. <code>AWSVpcLatticeServiceRolePolicy</code> CloudWatch PutMetricData Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon VPC Lattice .	5 dicembre 2022
VPC Lattice ha iniziato a tracciare le modifiche	VPC Lattice ha iniziato a tracciare le modifiche per le sue AWS politiche gestite.	5 dicembre 2022

Convalida della conformità per Amazon VPC Lattice

Third-party i revisori valutano la sicurezza e la conformità di Amazon VPC Lattice nell'ambito di diversi programmi di AWS conformità.

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. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta [AWS la documentazione sulla sicurezza](#).

Accedi ad Amazon VPC Lattice utilizzando gli endpoint di interfaccia (AWS PrivateLink)

Puoi stabilire una connessione privata tra il tuo VPC e Amazon VPC Lattice creando un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono alimentati da [AWS PrivateLink](#), una tecnologia che consente di accedere privatamente alle API VPC Lattice senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le API VPC Lattice.

[Ogni endpoint di interfaccia è rappresentato da una o più interfacce di rete nelle sottoreti.](#)

Considerazioni sugli endpoint VPC di interfaccia

[Prima di configurare un endpoint VPC di interfaccia per VPC Lattice, assicurati di leggere Access through nella Guida. Servizi AWS AWS PrivateLinkAWS PrivateLink](#)

VPC Lattice supporta l'esecuzione di chiamate a tutte le sue azioni API dal tuo VPC.

Creazione di un endpoint VPC di interfaccia per VPC Lattice

Puoi creare un endpoint VPC per il servizio VPC Lattice utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta [Creare un endpoint VPC di interfaccia nella Guida](#).AWS PrivateLink

Crea un endpoint VPC per VPC Lattice utilizzando il seguente nome di servizio:

`com.amazonaws.region.vpc-lattice`

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API a VPC Lattice utilizzando il nome DNS predefinito per la regione, ad esempio. `vpc-lattice.us-east-1.amazonaws.com`

Resilienza in Amazon VPC Lattice

L'infrastruttura AWS globale è costruita attorno a zone di disponibilità. Regioni AWS

Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti.

Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

Sicurezza dell'infrastruttura in Amazon VPC Lattice

In quanto servizio gestito, Amazon VPC Lattice 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 VPC Lattice 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 crittografia con Perfect Forward Secrecy (PFS) come DHE (Ephemeral) o ECDHE (Elliptic Curve Diffie-Hellman Ephemeral). Diffie-Hellman La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Monitoraggio di Amazon VPC Lattice

Utilizza le funzionalità di questa sezione per monitorare le reti di servizi Amazon VPC Lattice, i servizi, i gruppi target e le connessioni VPC.

Indice

- [CloudWatch metriche per Amazon VPC Lattice](#)
- [Log di accesso per Amazon VPC Lattice](#)
- [CloudTrail registri per Amazon VPC Lattice](#)

CloudWatch metriche per Amazon VPC Lattice

Amazon VPC Lattice invia i dati relativi ai tuoi gruppi target e ai tuoi servizi ad Amazon CloudWatch e li elabora in metriche leggibili quasi in tempo reale. Questi parametri vengono conservati per 15 mesi, in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni della tua applicazione o del tuo servizio web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).

Amazon VPC Lattice utilizza un ruolo collegato al servizio nel tuo AWS account per inviare parametri ad Amazon CloudWatch. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per Amazon VPC Lattice](#).

Indice

- [Visualizza i CloudWatch parametri di Amazon](#)
- [Metriche del gruppo target](#)
- [Parametri del servizio](#)

Visualizza i CloudWatch parametri di Amazon

Puoi visualizzare le CloudWatch metriche di Amazon per i tuoi gruppi target e i tuoi servizi utilizzando la CloudWatch console o AWS CLI.

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console Amazon all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.

2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare lo spazio dei nomi AWS/VpcLattice.
4. (Opzionale) Per visualizzare tutte le dimensioni di un parametro, inseriscine il nome nel campo di ricerca.
5. (Facoltativo) Per filtrare per dimensione, selezionare una delle opzioni seguenti:
 - Per visualizzare solo le metriche riportate per i tuoi gruppi target, scegli Gruppi target. Per visualizzare i parametri di un singolo gruppo di destinazioni, inserisci il relativo nome nel campo di ricerca.
 - Per visualizzare solo le metriche riportate per i tuoi servizi, scegli Servizi. Per visualizzare le metriche per un singolo servizio, inserisci il nome nel campo di ricerca.

Per visualizzare le metriche utilizzando il AWS CLI

Utilizzate il seguente AWS CLI comando [CloudWatch list-metrics](#) per elencare le metriche disponibili:

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

Per informazioni su ciascuna metrica e le relative dimensioni, consulta e. [Metriche del gruppo target Parametri del servizio](#)

Metriche del gruppo target

[VPC Lattice memorizza automaticamente le metriche relative ai gruppi target nello spazio dei nomi Amazon. AWS/VpcLattice CloudWatch](#) Per ulteriori informazioni sui gruppi target, consulta. [Gruppi target in VPC Lattice](#)

Dimensioni

Per filtrare le metriche per i gruppi target, utilizza le seguenti dimensioni:

- AvailabilityZone
- TargetGroup

Metrica	Description	TargetGroup Protocollo
TotalConnectionCount	Connessioni totali. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS, TCP
ActiveConnectionCount	Connessioni attive. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto	HTTP, HTTPS, TCP

Metrica	Description	TargetGroup Protocollo
	Statistiche La statistica più utile è Sum.	
ConnectionErrorCount	Errori di connessione totali. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS, TCP

Metrica	Description	TargetGroup Protocollo
HTTP1_Con nectionCo unt	Connessioni HTTP/1.1 totali. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS

Metrica	Description	TargetGroup Protocollo
HTTP2_ConnectionCount	Connessioni HTTP/2 totali. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS

Metrica	Description	TargetGroup Protocollo
ConnectionTimeoutCount	Timeout totali di connessione. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS, TCP

Metrica	Description	TargetGroup Protocollo
TotalReceivedConnectionBytes	Byte di connessione totali ricevuti. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS, TCP

Metrica	Description	TargetGroup Protocollo
TotalSent Connectio nBytes	Byte di connessione totali inviati. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS, TCP

Metrica	Description	TargetGroup Protocollo
TotalRequestCount	Richieste totali. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS

Metrica	Description	TargetGroup Protocollo
ActiveRequestCount	Richieste attive totali. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS

Metrica	Description	TargetGroup Protocollo
RequestTime	Tempo di richiesta fino all'ultimo byte in millisecondi. Criteri per la creazione di report - Viene sempre riportato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - Le statistiche più utili sono Average e pNN.NN (percentili).	HTTP, HTTPS

Metrica	Description	TargetGroup Protocollo
HTTPCode_2XX_Count , HTTPCode_3XX_Count , HTTPCode_4XX_Count , HTTPCode_5XX_Count	Codici di risposta HTTP aggregati. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS

Metrica	Description	TargetGroup Protocollo
TLSConnectionError Count	Errori totali di connessione TLS, escluse le verifiche dei certificati non riuscite. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS, TCP

Metrica	Description	TargetGroup Protocollo
TotalTLSC onnection Handshake Count	Handshake di connessione TLS riusciti in totale. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.	HTTP, HTTPS, TCP

Parametri del servizio

[VPC Lattice memorizza automaticamente le metriche relative ai servizi nel namespace Amazon.](#)
[AWS/VpcLattice CloudWatch](#) Per ulteriori informazioni sui servizi, consulta. [Servizi in VPC Lattice](#)

Dimensioni

Per filtrare le metriche per i gruppi target, utilizza le seguenti dimensioni:

- AvailabilityZone
- Service

Metrica	Description
RequestTimeoutCount	Totale delle richieste scadute in attesa di una risposta. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.
TotalRequestCount	Richieste totali. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.
RequestTime	Tempo di richiesta in millisecondi.

Metrica	Description
	Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - Le statistiche più utili sono Average e pNN.NN (percentili).
HTTPCode_2XX_Count , HTTPCode_3XX_Count , HTTPCode_4XX_Count , HTTPCode_5XX_Count	Codici di risposta HTTP aggregati. Criteri per la creazione di report - Viene sempre segnalato (indipendentemente dal fatto che si tratti di un valore zero o diverso da zero) dal momento in cui la risorsa riceve traffico. Frequenza di segnalazione - Una volta al minuto Statistiche - La statistica più utile è Sum.

Log di accesso per Amazon VPC Lattice

I log di accesso acquisiscono informazioni dettagliate sui servizi VPC Lattice e sulle configurazioni delle risorse. È possibile utilizzare questi log di accesso per analizzare i modelli di traffico e controllare tutti i servizi della rete. Per i servizi VPC Lattice, pubblichiamo VpcLatticeAccessLogs

e per le configurazioni delle risorse, pubblichiamo quelle `VpcLatticeResourceAccessLogs` che devono essere configurate separatamente.

I log di accesso sono opzionali e sono disabilitati per impostazione predefinita. Dopo aver abilitato i registri di accesso, è possibile disabilitarli in qualsiasi momento.

Prezzi

Quando i registri di accesso vengono pubblicati, vengono applicati dei costi. I log pubblicati AWS in modo nativo per conto dell'utente sono denominati registri venduti. Per ulteriori informazioni sui prezzi dei log venduti, consulta la pagina [CloudWatch Prezzi di Amazon](#), scegli Logs e visualizza i prezzi in Vended Logs.

Indice

- [Autorizzazioni IAM necessarie per abilitare i log di accesso](#)
- [Accedi alle destinazioni dei log](#)
- [Abilitare log di accesso](#)
- [Richiedi il tracciamento](#)
- [Accedere al contenuto del registro](#)
- [Contenuto del registro di accesso alle risorse](#)
- [Risolvi i problemi relativi ai log di accesso](#)

Autorizzazioni IAM necessarie per abilitare i log di accesso

Per abilitare i log di accesso e inviarli alle relative destinazioni, devi avere le seguenti azioni nella policy allegate all'utente, al gruppo o al ruolo IAM che stai utilizzando.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Sid": "ManageVPCLatticeAccessLogSetup",
      "Action": [
```

```

        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "vpc-lattice:CreateAccessLogSubscription",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:UpdateAccessLogSubscription",
        "vpc-lattice>DeleteAccessLogSubscription",
        "vpc-lattice:ListAccessLogSubscriptions"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

Per ulteriori informazioni, consulta [Aggiunta e rimozione di autorizzazioni per identità IAM](#) nella Guida per l'utente di AWS Identity and Access Management .

Dopo aver aggiornato la policy allegata all'utente, al gruppo o al ruolo IAM che stai utilizzando, vai a [Abilitare log di accesso](#)

Accedi alle destinazioni dei log

È possibile inviare i log di accesso alle seguenti destinazioni.

CloudWatch Registri Amazon

- VPC Lattice in genere consegna i log ai CloudWatch log entro 2 minuti. Tuttavia, tenete presente che i tempi effettivi di consegna dei log vengono effettuati con la massima diligenza possibile e che potrebbe esserci una latenza aggiuntiva.
- Una politica delle risorse viene creata automaticamente e aggiunta al gruppo di CloudWatch log se il gruppo di log non dispone di determinate autorizzazioni. Per ulteriori informazioni, consulta [Logs sent to CloudWatch Logs](#) nella Amazon CloudWatch User Guide.
- Puoi trovare i log di accesso che vengono inviati alla CloudWatch sezione Log Groups nella console. CloudWatch Per ulteriori informazioni, consulta [Visualizza i dati di log inviati a CloudWatch Logs](#) nella Amazon CloudWatch User Guide.

Simple Storage Service (Amazon S3)

- VPC Lattice in genere consegna i log ad Amazon S3 entro 6 minuti. Tuttavia, tieni presente che i tempi effettivi di consegna dei log vengono effettuati con la massima diligenza possibile e potrebbe esserci una latenza aggiuntiva.
- Una policy relativa ai bucket verrà creata automaticamente e aggiunta al bucket Amazon S3 se il bucket non dispone di determinate autorizzazioni. Per ulteriori informazioni, consulta [Logs sent to Amazon S3 nella CloudWatchAmazon User Guide](#).
- I log di accesso inviati ad Amazon S3 utilizzano la seguente convenzione di denominazione:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/AccessLogs/[region]/[YYYY/MM/DD]/[resource-id]/[accountId]_VpcLatticeAccessLogs_[region]_[resource-id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

- VpcLatticeResourceAccessLogs che vengono inviati ad Amazon S3 utilizzano la seguente convenzione di denominazione:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/ResourceAccessLogs/[region]/[YYYY/MM/DD]/[resource-id]/[accountId]_VpcLatticeResourceAccessLogs_[region]_[resource-id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

Amazon Data Firehose

- VPC Lattice in genere consegna i log a Firehose entro 2 minuti. Tuttavia, tenete presente che il tempo effettivo di consegna dei log viene effettuato con la massima diligenza possibile e potrebbe esserci una latenza aggiuntiva.
- Viene creato automaticamente un ruolo collegato al servizio che concede a VPC Lattice l'autorizzazione a inviare i log di accesso. Amazon Data Firehose Affinché la creazione automatica di un ruolo riesca, gli utenti devono disporre dell'autorizzazione per l'operazione `iam:CreateServiceLinkedRole`. Per ulteriori informazioni, consulta [Logs sent to Amazon Data Firehose](#) nella Amazon CloudWatch User Guide.
- Per ulteriori informazioni sulla visualizzazione dei log inviati a Amazon Data Firehose, consulta [Monitoring Amazon Kinesis Data Streams](#) nella Developer Guide. Amazon Data Firehose

Abilitare log di accesso

Completa la seguente procedura per configurare i log di accesso per acquisire e consegnare i log di accesso alla destinazione prescelta.

Indice

- [Abilita i log di accesso utilizzando la console](#)
- [Abilita i log di accesso utilizzando il AWS CLI](#)

Abilita i log di accesso utilizzando la console

È possibile abilitare i log di accesso per una rete di servizi, un servizio o una configurazione di risorse durante la creazione. È inoltre possibile abilitare i log di accesso dopo aver creato una rete di servizi, un servizio o una configurazione di risorse, come descritto nella procedura seguente.

Per creare un servizio di base utilizzando la console

1. Apri la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Seleziona la rete di servizio, il servizio o la configurazione delle risorse.
3. Scegli Azioni, Modifica impostazioni di registro.
4. Attiva l'interruttore dei registri di accesso.
5. Aggiungi una destinazione di consegna per i registri di accesso come segue:
 - Seleziona Gruppo di CloudWatch log e scegli un gruppo di log. Per creare un gruppo di log, scegli Crea un gruppo di log in CloudWatch.
 - Seleziona il bucket S3 e inserisci il percorso del bucket S3, incluso qualsiasi prefisso. Per cercare nei bucket S3, scegli Browse S3.
 - Seleziona il flusso di distribuzione di Kinesis Data Firehose e scegli un flusso di distribuzione. Per creare un flusso di distribuzione, scegli Crea un flusso di distribuzione in Kinesis.
6. Scegli Save changes (Salva modifiche).

Abilita i log di accesso utilizzando il AWS CLI

Utilizza il comando CLI [create-access-log-subscription](#) per abilitare i log di accesso per reti o servizi di servizio.

Richiedi il tracciamento

VPC Lattice supporta il tracciamento e la correlazione delle richieste tra client, target e log per l'osservabilità e il debug con l'intestazione. `x-amzn-requestid` Questa intestazione può essere impostata e inviata dal client o generata da VPC Lattice e viene inviata alle destinazioni ed è disponibile anche nei log di accesso.

Comportamento predefinito

- VPC Lattice genera automaticamente questa intestazione per ogni richiesta.
- Il valore è un identificatore generato casualmente (di default in stile UUID).
- L'identificatore generato è:
 - Propagato verso obiettivi a valle.
 - Restituito nelle intestazioni di risposta ai client.
 - Registri di accesso registrati

Esempio (risposta predefinita)

Di seguito è riportato un esempio di risposta inviata al client con il comportamento predefinito di VPC Lattice che genera un valore casuale per l'intestazione `x-amzn-requestid`.

```
{
  "HTTP/1.1 200 OK
  x-amzn-requestid: a9f2c7a1-6b4f-4c79-9e87-ff5a1234a001"
}
```

Client che imposta il valore

- I client possono facoltativamente impostare questa intestazione sulle richieste in arrivo per sovrascrivere il valore generato automaticamente.
- Considerazioni
 - Il valore dell'intestazione non deve necessariamente seguire un formato UUID.
 - Se il valore dell'intestazione supera i 512 byte, VPC Lattice lo troncherà a 512.
- Se sovrascritto correttamente, il valore dell'intestazione fornito sarà:
 - Apparirà nelle intestazioni di risposta

- Essere propagato ai bersagli
- Compaiono nei log di accesso e nelle metriche

Esempio (sovrascrivi la richiesta del cliente)

Di seguito è riportato un esempio di richiesta inviata dal client con un valore di intestazione.

```
{
  "GET /my-service/endpoint HTTP/1.1
  Host: my-api.example.com
  x-amzn-requestid: trace-request-foobar"
}
```

Esempio (risposta di override predefinita)

Di seguito è riportato un esempio di risposta inviata al client con il valore sovrascritto.

```
{
  "HTTP/1.1 200 OK
  x-amzn-requestid: trace-request-foobar"
}
```

Accedere al contenuto del registro

La seguente tabella descrive i campi di una voce di un log di accesso.

Campo	Description	Formato
callerPrincipalTags	Il PrincipalTags nella richiesta.	JSON
hostHeader	L'intestazione dell'autorità della richiesta.	stringa
sslCipher	Il nome OpenSSL per il set di cifrari utilizzati per stabilire la connessione TLS del client.	stringa
serviceNetworkArn	La rete di assistenza ARN.	arn:aws:vpc-lattice: ::service network/ <i>region account id</i>

Campo	Description	Formato
<code>resolvedUser</code>	L'ARN dell'utente quando l'autenticazione è abilitata e l'autenticazione è stata effettuata.	null ARN «Anonimo» «Sconosciuto»
<code>authDeniedReason</code>	Il motivo per cui l'accesso viene negato quando l'autenticazione è abilitata.	null «Servizio» «Rete» «Identità»
<code>requestMethod</code>	L'intestazione del metodo della richiesta.	stringa
<code>targetGroupArn</code>	Il gruppo di host di destinazione a cui appartiene l'host di destinazione.	stringa
<code>tlsVersion</code>	La versione TLS.	TLSv x
<code>userAgent</code>	L'intestazione user-agent.	stringa
<code>serverNameIndication</code>	[Solo HTTPS] Il valore impostato sul socket di connessione ssl per Server Name Indication (SNI).	stringa
<code>destinationVpcId</code>	L'ID VPC di destinazione.	vpc- xxxxxxxx
<code>sourceIpPort</code>	L'indirizzo IP e la porta della sorgente.	ip:port
<code>targetIpPort</code>	L'indirizzo IP e la porta della destinazione.	ip:port
<code>serviceArn</code>	Il servizio ARN.	arn:aws:vpc-lattice: ::service/ region account id
<code>sourceVpcId</code>	L'ID VPC di origine.	vpc- xxxxxxxx

Campo	Description	Formato
<code>requestPath</code>	Il percorso della richiesta.	<code>LatticePath?:<i>path</i></code>
<code>startTime</code>	L'ora di inizio della richiesta.	<code>YYYY-MM-DD T HHMM:SS Z</code>
<code>protocol</code>	Il protocollo. Attualmente HTTP/1.1 o HTTP/2.	stringa
<code>responseCode</code>	Il codice di risposta HTTP. Viene registrato solo il codice di risposta per le intestazioni finali. Per ulteriori informazioni, consulta Risolvi i problemi relativi ai log di accesso .	intero
<code>bytesReceived</code>	I byte del corpo e dell'intestazione ricevuti.	intero
<code>bytesSent</code>	I byte del corpo e dell'intestazione inviati.	intero
<code>duration</code>	Durata totale in millisecondi della richiesta dall'ora di inizio all'ultimo byte in uscita.	intero
<code>requestToTargetDuration</code>	Durata totale in millisecondi della richiesta dall'ora di inizio all'ultimo byte inviato alla destinazione.	intero
<code>responseFromTargetDuration</code>	Durata totale in millisecondi della richiesta dal primo byte letto dall'host di destinazione all'ultimo byte inviato al client.	intero

Campo	Description	Formato
grpcResponseCode	Il codice di risposta gRPC. Per ulteriori informazioni, vedere Codici di stato e loro utilizzo in gRPC . Questo campo viene registrato solo se il servizio supporta gRPC.	intero
requestId	Si tratta di un identificatore univoco incluso automaticamente nelle risposte come valore dell'intestazione. x-amzn-requestid Consente la correlazione delle richieste tra client, destinazioni e registri per l'osservabilità e il debug.	stringa
callerPrincipal	Il principale autenticato.	stringa
callerX509SubjectCN	Il nome del soggetto (CN).	stringa
callerX509IssuerOU	L'emittente (OU).	stringa
callerX509SANNameCN	L'alternativa all'emittente (nome/CN).	stringa
callerX509SANDNS	Il nome alternativo del soggetto (DNS).	stringa
callerX509SANURI	Il nome alternativo dell'oggetto (URI).	stringa
sourceVpcArn	L'ARN del VPC da cui ha avuto origine la richiesta.	arn:aws:ec2: :vpc/ <i>region</i> <i>account id</i>

Campo	Description	Formato
<code>failureReason</code>	Indica il motivo per cui una richiesta non è riuscita. Di seguito sono riportati i valori possibili: • <code>TargetConnectionError</code> - La richiesta non è riuscita a connettersi a una destinazione nel gruppo di destinazione. • <code>TargetProtocolError</code> - La destinazione non ha risposto con dati validi. Ciò potrebbe indicare che la destinazione ha record TLS non validi o ha utilizzato un protocollo per gruppi di destinazione non valido. • <code>TargetDataTimeout</code> - È stato raggiunto il timeout di inattività. • <code>TargetConnectionClosed</code> - Il bersaglio ha chiuso la connessione prima di completare la risposta. • <code>ClientConnectionClosed</code> - Il client ha chiuso la connessione prima di ricevere la risposta completa. • <code>ClientRateLimited</code> - Il client ha superato il limite di connessione e VPC Lattice ha limitato la velocità.	stringa

Campo	Description	Formato
	• ClientAccessDenied - VPC Lattice ha negato l'accesso alla risorsa. authDeniedReason Per ulteriori informazioni sul motivo per cui VPC Lattice ha negato l'accesso. • ClientProtocolError - Il client ha inviato dati che non sono stati compresi. Ciò potrebbe indicare che il client ha utilizzato record TLS non validi o un protocollo non valido. • ConnectionDurationExceeded - La connessione ha raggiunto il limite massimo di durata della connessione. • InternalError - Si è verificato un errore interno durante l'elaborazione della richiesta.	

Esempio

Nell'esempio seguente viene mostrata una voce di log.

```
{
  "callerPrincipalTags" : "{ \"TagA\": \"ValA\", \"TagB\": \"ValB\", ... }",
  "hostHeader": "example.com",
  "sslCipher": "-",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/svn-1a2b3c4d",
}
```

```

    "resolvedUser": "Unknown",
    "authDeniedReason": "null",
    "requestMethod": "GET",
    "targetGroupArn": "arn:aws:vpc-lattice:us-west-2:123456789012:targetgroup/tg-1a2b3c4d",
    "tlsVersion": "-",
    "userAgent": "-",
    "serverNameIndication": "-",
    "destinationVpcId": "vpc-0abcdef1234567890",
    "sourceIpPort": "178.0.181.150:80",
    "targetIpPort": "131.31.44.176:80",
    "serviceArn": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-1a2b3c4d",
    "sourceVpcId": "vpc-0abcdef1234567890",
    "requestPath": "/billing",
    "startTime": "2023-07-28T20:48:45Z",
    "protocol": "HTTP/1.1",
    "responseCode": 200,
    "bytesReceived": 42,
    "bytesSent": 42,
    "duration": 375,
    "requestToTargetDuration": 1,
    "responseFromTargetDuration": 1,
    "grpcResponseCode": 1,
    "requestId": "a9f2c7a1-6b4f-4c79-9e87-ff5a1234a001"
  }

```

Contenuto del registro di accesso alle risorse

La tabella seguente descrive i campi di una voce del registro di accesso alle risorse.

Campo	Description	Formato
serviceNetworkArn	La rete di assistenza ARN.	arn: <i>partition</i> vpc-lattice: ::servicenetwork/ <i>region</i> <i>account id</i>
serviceNetworkResourceAssociationId	L'ID della risorsa di rete del servizio.	<i>snra-xxx</i>
vpcEndpointId	L'ID dell'endpoint utilizzato per accedere alla risorsa.	stringa

Campo	Description	Formato
sourceVpcArn	L'ARN VPC di origine o il VPC da cui è stata avviata la connessione.	stringa
resourceConfigurationArn	L'ARN della configurazione delle risorse a cui è stato effettuato l'accesso.	stringa
protocol	Il protocollo utilizzato per comunicare con la configurazione delle risorse. Attualmente è supportato solo tcp.	stringa
sourceIpPort	L'indirizzo IP e la porta della fonte che ha avviato la connessione.	<i>ip:port</i>
destinationIpPort	L'indirizzo IP e la porta con cui è stata avviata la connessione. Questo sarà l'IP di SN-E/SN-A.	<i>ip:port</i>
gatewayIpPort	L'indirizzo IP e la porta utilizzati dal gateway di risorse per accedere alla risorsa.	<i>ip:port</i>
resourceIpPort	L'indirizzo IP e la porta della risorsa.	<i>ip:port</i>

Esempio

Nell'esempio seguente viene mostrata una voce di log.

```
{
  "eventTimestamp": "2024-12-02T10:10:10.123Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:1234567890:servicenetwork/sn-1a2b3c4d",
```

```

    "serviceNetworkResourceAssociationId": "snra-1a2b3c4d",
    "vpcEndpointId": "vpce-01a2b3c4d",
    "sourceVpcArn": "arn:aws:ec2:us-west-2:1234567890:vpc/vpc-01a2b3c4d",
    "resourceConfigurationArn": "arn:aws:vpc-lattice:us-west-2:0987654321:resourceconfiguration/rcfg-01a2b3c4d",
    "protocol": "tcp",
    "sourceIpPort": "172.31.23.56:44076",
    "destinationIpPort": "172.31.31.226:80",
    "gatewayIpPort": "10.0.28.57:49288",
    "resourceIpPort": "10.0.18.190:80"
  }

```

Risolvi i problemi relativi ai log di accesso

Questa sezione contiene una spiegazione dei codici di errore HTTP che è possibile visualizzare nei log di accesso.

Codice di errore	Possibili cause
HTTP 400: Bad Request	- Il client ha inviato una richiesta non valida che non soddisfa la specifica HTTP. - L'intestazione della richiesta ha superato i 60K per l'intera intestazione della richiesta o più di 100 intestazioni. - Il client ha chiuso la connessione prima di inviare l'intero corpo della richiesta.
HTTP 403: Forbidden	L'autenticazione è stata configurata per il servizio, ma la richiesta in arrivo non è autenticata o autorizzata.
HTTP 404: servizio inesistente	Stai tentando di connetterti a un servizio che non esiste o non è registrato nella rete di assistenza corretta.
HTTP 500: Internal Server Error	VPC Lattice ha riscontrato un errore, ad esempio la mancata connessione ai target.
HTTP 502: Bad Gateway	VPC Lattice ha riscontrato un errore.

CloudTrail registri per Amazon VPC Lattice

Amazon VPC Lattice è integrato con [AWS CloudTrail](#), un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un. Servizio AWS CloudTrail acquisisce tutte le chiamate API per VPC Lattice come eventi. Le chiamate acquisite includono chiamate dalla console VPC Lattice e chiamate in codice alle operazioni dell'API VPC Lattice. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a VPC Lattice, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWS Per ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi [CloudTrailLake](#).

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il AWS Management Console sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta [Creating a trail for your Account AWS](#) e [Creating a trail for an organization](#) nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail](#) Per informazioni sui prezzi di Amazon S3, consulta [Prezzi di Amazon S3](#).

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail [Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC](#). ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i [selettori di eventi avanzati](#). I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta [Working with AWS CloudTrail Lake](#) nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'[opzione di prezzo](#) da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. [Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail](#)

Per monitorare azioni aggiuntive, utilizza i registri di accesso. Per ulteriori informazioni, consulta [Log di accesso](#).

Eventi di gestione VPC Lattice in CloudTrail

[Gli eventi di gestione](#) forniscono informazioni sulle operazioni di gestione eseguite sulle risorse del tuo Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Amazon VPC Lattice registra le operazioni del piano di controllo VPC Lattice come eventi di gestione. [Per un elenco delle operazioni del piano di controllo di Amazon VPC Lattice a cui VPC Lattice effettua l'accesso, CloudTrail consulta l'Amazon VPC Lattice API Reference.](#)

Esempi di eventi VPC Lattice

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via.

CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra un CloudTrail evento per l'[CreateService](#) operazione.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "abcdef01234567890",
        "arn": "arn:abcdef01234567890",
        "accountId": "abcdef01234567890",
        "userName": "abcdef01234567890"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-08-16T03:34:54Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-08-16T03:36:12Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateService",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "abcdef01234567890",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "name": "rates-service"
  },
  "responseElements": {
    "name": "rates-service",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "CREATE_IN_PROGRESS"
  },
  "requestID": "abcdef01234567890",
```

```
"eventID": "abcdef01234567890",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "abcdef01234567890",
"eventCategory": "Management"
}
```

L'esempio seguente mostra un CloudTrail evento per l'[DeleteService](#) operazione.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:ABCXYZ123456",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "abcdef01234567890",
        "arn": "arn:aws:iam::AIDACKCEVSQ6C2EXAMPLE:role/Admin",
        "accountId": "abcdef01234567890",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-27T17:42:36Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-27T17:56:41Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "DeleteService",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "72.21.198.64",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "serviceIdentifier": "abcdef01234567890"
  },
  "responseElements": {
```

```
    "name": "test",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "DELETE_IN_PROGRESS"
  },
  "requestID": "abcdef01234567890",
  "eventID": "abcdef01234567890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "abcdef01234567890",
  "eventCategory": "Management"
}
```

Per informazioni sul contenuto dei CloudTrail record, vedere il [contenuto dei CloudTrail record](#) nella Guida AWS CloudTrail per l'utente.

Quote per Amazon VPC Lattice

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Salvo diversa indicazione, ogni quota è. Region-specific Se per alcune quote è possibile richiedere aumenti, per altre non è possibile.

Per visualizzare le quote per VPC Lattice, apri la console Service [Quotas](#). Nel pannello di navigazione, scegli Servizi AWS e seleziona VPC Lattice.

Per richiedere un aumento delle quote, consultare [Richiesta di aumento delle quote](#) nella Guida dell'utente di Service Quotas.

Hai Account AWS le seguenti quote relative a VPC Lattice.

Nome	Predefinita	Adattate	Description
Dimensioni della politica di autenticazione	Ogni regione supportata: 10 KB	No	La dimensione massima di un file JSON in una politica di autenticazione.
Configurazioni delle risorse secondarie per configurazione delle risorse di gruppo	Ogni regione supportata: 60	Sì	Il numero massimo di configurazioni di risorse secondarie in una configurazione di risorse di gruppo. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Verifiche del dominio per regione AWS	Ogni regione supportata: 5	Sì	Il numero massimo di verifiche di dominio che è possibile creare per account. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.

Nome	Predefinita	Adattate	Description
Ascoltatori per servizio	Ogni regione supportata: 2	Sì	Il numero massimo di ascoltatori che è possibile creare per un servizio. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Configurazioni delle risorse per rete di servizio	Ogni regione supportata: 500	Sì	Il numero massimo di configurazioni di risorse associate a una rete di servizi. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Configurazioni delle risorse per regione AWS	Ogni regione supportata: 2.000	Sì	Il numero massimo di configurazioni di risorse che un AWS account può avere per regione. AWS Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Gateway di risorse per VPC	Ogni regione supportata: 500	Sì	Il numero massimo di gateway di risorse in un VPC. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.

Nome	Predefinita	Adatta e	Description
Regole per ascoltatore	Ogni regione supportata: 10	Sì	Il numero massimo di regole che puoi definire per il tuo service listener. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Gruppi di sicurezza per associazione	Ogni Regione supportata: 5	No	Il numero massimo di gruppi di sicurezza che è possibile aggiungere a un'associazione tra un VPC e una rete di servizi.
Associazioni di servizi per rete di servizi	Ogni regione supportata: 500	Sì	Il numero massimo di servizi che è possibile associare a una singola rete di servizi. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Reti di assistenza per regione	Ogni Regione supportata: 50	Sì	Il numero massimo di reti di servizi per regione. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.

Nome	Predefinita	Adatta e	Description
Servizi per regione	Ogni regione supportata: 2.000	Sì	Il numero massimo di servizi per regione. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Gruppi di destinazione per regione	Ogni regione supportata: 500	Sì	Il numero massimo di gruppi target per regione. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Gruppi di destinazione per servizio	Ogni regione supportata: 10	Sì	Il numero massimo di gruppi target che puoi associare a un servizio. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Destinazioni per gruppo di destinazione	Ogni regione supportata: 1.000	Sì	Il numero massimo di obiettivi che è possibile associare a un singolo gruppo target. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.

Nome	Predefinita	Adattata	Description
Associazioni VPC per rete di servizi	Ogni regione supportata: 500	Sì	Il numero massimo di VPC che è possibile associare a una singola rete di servizi. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Endpoint VPC di tipo rete di servizio per rete di servizio	Ogni Regione supportata: 200	Sì	Il numero massimo di endpoint della rete di servizio associati a una rete di servizi. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.

Note

Quando si utilizzano le associazioni di reti di servizio, il numero massimo di configurazioni di risorse per rete di servizio è 1.000 (mille).

Le seguenti zone di disponibilità non sono supportate per VPC Lattice: use1-az3,,, usw1-az2apne1-az3,euw1-az4. cac1-az3 ilc1-az2

Si applicano anche i seguenti limiti.

Limite	Valore	Description
Larghezza di banda per servizio per zona di disponibilità	10 Gb/s	La larghezza di banda predefinita allocata per servizio per zona di disponibilità. Questo limite può essere aumentato, contattate il vostro Solutions Architect (SA) o il Technical

Limite	Valore	Description
		Account Manager (TAM) per ulteriore assistenza.
Unità di trasmissione massima (MTU) per connessione	8500 byte	La dimensione del pacchetto di dati più grande che un servizio può accettare.
Richieste al secondo per servizio per zona di disponibilità	10.000	Per i servizi HTTP, questo è il numero predefinito di richieste al secondo per servizio per zona di disponibilità. Questo numero può essere aumentato, contattate il vostro Solutions Architect (SA) o il Technical Account Manager (TAM) per ulteriore assistenza.
Tempo di inattività della connessione per connessione per i servizi VPC Lattice	Configurabile con un valore predefinito di 60 secondi (intervallo: 60-600 secondi)	Il tempo in cui una connessione può rimanere inattiva senza richieste attive (per HTTP e gRPC) o senza trasferimento di dati attivo (per il passthrough TLS). È possibile configurare questo valore per servizio utilizzando il <code>idleTimeoutSeconds</code> parametro nell'API CreateServiceUpdateService . Puoi anche utilizzare HTTP e keepalive a livello di applicazione per mantenere attive le connessioni fino alla durata massima della connessione di 10 minuti.
Durata massima della connessione per connessione per i servizi VPC Lattice	10 minuti	Il tempo massimo di apertura di una connessione tra il client e il server per i servizi VPC Lattice.

Limite	Valore	Description
Durata massima della connessione per connessione per risorse VPC Lattice	N/A	VPC Lattice non impone limiti di connessione a vita per le risorse. Il client e il server determinano la durata della connessione a vita pur essendo consapevoli del timeout di inattività per le risorse VPC Lattice, che è di 350 secondi.
Tempo di inattività della connessione per connessione per risorse VPC Lattice	350 secondi	È possibile utilizzare i keepalive TCP per estendere questo timeout di inattività.
Rete di assistenza per VPC	1 rete di assistenza	È possibile connettere un VPC a una sola rete di servizi tramite un'associazione. Per connettere un VPC a più reti di servizi, puoi utilizzare endpoint VPC di tipo service network.

Cronologia dei documenti per la Amazon VPC Lattice User Guide

La tabella seguente descrive le versioni della documentazione per VPC Lattice.

Modifica	Descrizione	Data
Sono stati aggiunti indirizzi IP configurabili per i gateway di risorse	VPC Lattice ora supporta indirizzi IP configurabili per gateway di risorse.	7 ottobre 2025
Aggiunto VPC Lattice per Oracle Database@AWS	VPC Lattice è pronto per essere rilasciato. Oracle Database@AWS	26 giugno 2025
Aggiunto il supporto dual-stack per gli endpoint di gestione	VPC Lattice ora supporta gli IPv6 endpoint dual-stack (eIPv4) per tutta la gestione di VPC Lattice. APIs	30 aprile 2025
Condividi e accedi alle risorse	VPC Lattice ora supporta la condivisione e l'accesso alle risorse attraverso i confini del VPC e dell'account. Ciò include gli aggiornamenti alle politiche e. VPCLatticeReadOnlyAccessVPCLatticeFullAccess	1 dicembre 2024
Passthrough TLS	VPC Lattice ora supporta il passthrough TLS, che consente di eseguire la terminazione TLS nell'applicazione per l'autenticazione end-to-end	14 maggio 2024

Versione della struttura degli eventi Lambda	VPC Lattice ora supporta una nuova versione della struttura degli eventi Lambda.	7 settembre 2023
Support per la condivisione VPCs	I partecipanti possono creare gruppi target VPC Lattice in un VPC condiviso.	5 luglio 2023
Versione General Availability	Il rilascio della VPC Lattice User Guide for General Availability (GA)	31 marzo 2023
VPC Lattice ora segnala le modifiche alle sue politiche gestite AWS	Le modifiche alle policy gestite sono riportate in "policy AWS gestite per VPC Lattice» nel capitolo «Sicurezza».	29 marzo 2023
Supporto per il tipo di destinazione Application Load Balancer	VPC Lattice ora supporta la creazione di un gruppo target di tipo Application Load Balancer.	29 marzo 2023
Support per tutti i tipi di istanze	VPC Lattice ora supporta tutti i tipi di istanze.	27 marzo 2023
IPv6 supporto	VPC Lattice ora supporta entrambi i gruppi target IPv4 IPv6 IP.	27 marzo 2023
HTTP2 versione del protocollo per i controlli sanitari	I controlli Health sono ora supportati quando la versione del protocollo del gruppo target è HTTP2.	27 marzo 2023
Azione di risposta fissa per le regole degli ascoltatori	I listener per i servizi VPC Lattice ora supportano azioni di risposta fissa oltre alle azioni di inoltro.	27 marzo 2023

Support per nomi di dominio personalizzati	Ora puoi configurare un nome di dominio personalizzato per il tuo servizio VPC Lattice	14 febbraio 2023
Support per BYOC (Bring Your Own Certificate)	VPC Lattice supporta l'utilizzo del proprio SSL/TLS certificato in ACM per nomi di dominio personalizzati.	14 febbraio 2023
VPC Lattice ora riporta un elenco aggiornato di tipi di istanze non supportate	Sono state aggiunte tre istanze aggiuntive all'elenco delle istanze non supportate.	26 gennaio 2023
VPC Lattice ora segnala le modifiche alle sue politiche gestite AWS	A partire dal 5 dicembre 2022, le modifiche alle politiche gestite sono riportate nell'argomento "politiche AWS gestite per VPC Lattice» nel capitolo «Sicurezza». La prima modifica elencata è l'aggiunta delle autorizzazioni necessarie per il monitoraggio. CloudWatch	5 dicembre 2022
Versione iniziale	Versione iniziale della VPC Lattice User Guide	5 dicembre 2022

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.