aws

Guida per l'utente

Amazon VPC Lattice

Amazon VPC Lattice: Guida per l'utente

Table of Contents

Cos'è Amazon VPC Lattice? 1
Componenti chiave 1
Ruoli e responsabilità 3
Funzionalità 4
Come funziona VPC Lattice 5
Accesso a VPC Lattice 8
Prezzi 8
Reti di servizio 9
Creare una rete di servizi 10
Gestisci le associazioni 12
Gestisci le associazioni di servizi 12
Gestisci le associazioni VPC 13
Modifica le impostazioni di accesso 14
Modifica i dettagli del monitoraggio 15
Gestione dei tag 17
Eliminare una rete di servizi 17
Servizi 19
Fase 1: Creare un servizio VPC Lattice 20
Fase 2: Definizione del routing 21
Fase 3: Creare associazioni di rete 22
Fase 4: Revisione e creazione 23
Gestisci le associazioni 23
Modifica le impostazioni di accesso 24
Modifica i dettagli del monitoraggio 25
Gestione dei tag 26
Configura un nome di dominio personalizzato 27
Associa un nome di dominio personalizzato al tuo servizio 29
BYOC 32
Protezione della chiave privata del certificato 33
Eliminazione di un servizio 34
Gruppi target 35
Creazione di un gruppo target 36
Creazione di un gruppo target 36
Sottoreti condivise 38

Registrazione di destinazioni ... 39
ID di istanza ... 40
Indirizzi IP ... 41
Funzioni Lambda ... 41
Application Load Balancer ... 42
Configurazione dei controlli dello stato ... 42
Impostazioni del controllo dello stato ... 43
Controllo dello stato delle destinazioni ... 45
Modifica le impostazioni del controllo sanitario ... 46
Configurazione dell'instradamento ... 46
Algoritmo di instradamento ... 47
Target type (Tipo di destinazione) ... 47
Tipo di indirizzo IP ... 49
Obiettivi HTTP ... 49
x-forwardedintestazioni ... 49
Intestazioni relative all'identità del chiamante ... 50
Funzioni Lambda come destinazioni ... 51
Preparazione della funzione Lambda ... 51
Creazione di un gruppo di destinazioni per la funzione Lambda ... 41
Ricevi eventi dal servizio VPC Lattice ... 53
Rispondi al servizio VPC Lattice ... 56
Intestazioni con più valori ... 57
Annullamento della registrazione della funzione Lambda ... 57
Application Load Balancer come destinazioni ... 58
Prerequisiti ... 58
Fase 1: Creare un gruppo target di tipo ALB ... 59
Fase 2: Registrare l'Application Load Balancer come destinazione ... 60
Versione del protocollo ... 60
Aggiornamento dei tag ... 62
Eliminazione di un gruppo target ... 63
Listener ... 64
Configurazione dei listener ... 64
Creare un listener ... 65
Listener HTTP ... 65
Prerequisiti ... 66
Aggiunta di un ascoltatore HTTP ... 66

Listener HTTPS ... 67
Policy di sicurezza ... 68
Politica ALPN ... 69
Aggiunta di un ascoltatore HTTPS ... 69
Ascoltatori TLS ... 71
Considerazioni ... 71
Aggiungi un listener TLS ... 72
Regole dei listener ... 73
Regole predefinite ... 73
Priorità regola ... 73
Operazione delle regole ... 73
Condizioni della regola ... 74
Aggiungere una regola ... 75
Aggiorna una regola ... 76
Eliminare una regola ... 76
Aggiornamento di un listener ... 77
Eliminazione di un listener ... 77
Condividi le risorse VPC Lattice ... 79
Prerequisiti ... 79
Condividi le risorse ... 80
Smetti di condividere risorse ... 81
Responsabilità e autorizzazioni ... 81
Proprietari delle risorse ... 82
Consumatori di risorse ... 82
Eventi tra account ... 83
Sicurezza ... 86
Gestisci l'accesso ai servizi ... 87
Politiche di autenticazione ... 87
Gruppi di sicurezza ... 102
Liste di controllo accessi (ACL) di rete ... 107
Richieste autenticate ... 109
Protezione dei dati ... 117
Crittografia in transito ... 117
Crittografia a riposo ... 117
Gestione dell'identità e degli accessi ... 124
Come funziona Amazon VPC Lattice con IAM ... 124

Autorizzazioni API 131
Policy basate su identità 132
Uso di ruoli collegati ai servizi 139
AWS politiche gestite 140
Convalida della conformità 144
AWS PrivateLink 145
Considerazioni sugli endpoint VPC di interfaccia 145
Creazione di un endpoint VPC di interfaccia per VPC Lattice 146
Resilienza 146
Sicurezza dell'infrastruttura 146
Monitoraggio 148
CloudWatch metriche 148
Visualizza i CloudWatch parametri di Amazon 148
Metriche del gruppo target 149
Parametri del servizio 162
Log di accesso 166
Autorizzazioni IAM necessarie per abilitare i log di accesso 167
Accedi alle destinazioni dei log 168
Abilitare log di accesso 169
Accedere al contenuto del registro 170
Risolvi i problemi relativi ai log di accesso 174
CloudTrail registri 175
Comprendi le voci dei file di registro VPC Lattice 175
Quote 179
Cronologia dei documenti 182
..... clxxxv

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 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 servizi piccoli e modulari, spesso chiamati microservizi. Sebbene la modernizzazione abbia i suoi vantaggi, può anche introdurre complessità e sfide di rete quando si connettono questi microservizi. Ad esempio, se gli sviluppatori sono distribuiti in diversi team, potrebbero creare e distribuire microservizi su più account o VPC.

In VPC Lattice, ci riferiamo a un microservizio come a un servizio. Questa è la dicitura che vedi nella documentazione di VPC Lattice.

Indice

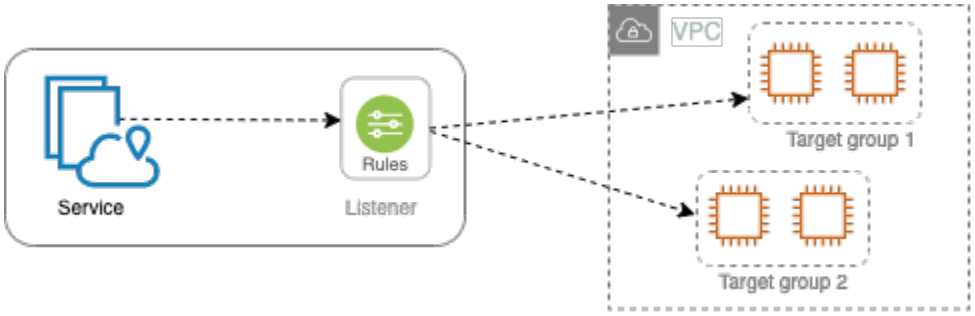
- Componenti chiave
- Ruoli e responsabilità
- Funzionalità
- Come funziona VPC Lattice
- Accesso a VPC Lattice
- Prezzi

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 EC2 o contenitori ECS 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. Le destinazioni possono essere istanze EC2, indirizzi IP, funzioni Lambda, Application Load Balancer o Kubernetes Pods. Questi sono simili ai gruppi target forniti da Elastic Load Balancing, ma non sono intercambiabili.

Listener

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

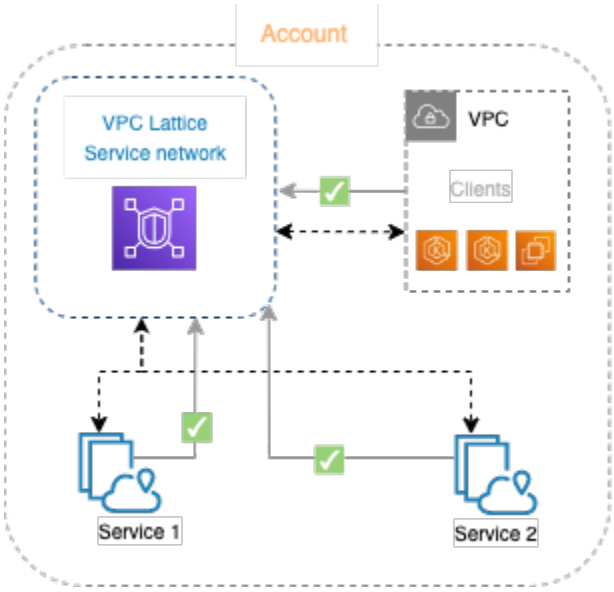
Regola

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.

Rete di servizi

Un limite logico per un insieme di servizi. Un client è qualsiasi risorsa distribuita in un VPC associata 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 di tua proprietà o condivisi con il tuo account tramite AWS Resource Access Manager ().AWS RAM

Politiche di autenticazione

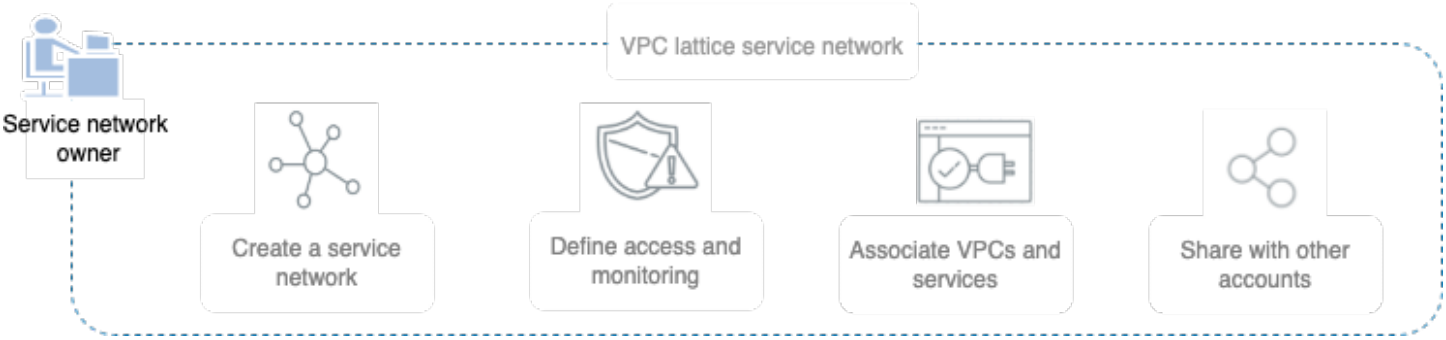
Politiche di autorizzazione granulari che possono essere utilizzate per definire l'accesso ai servizi. È possibile allegare politiche di autenticazione separate ai singoli servizi o alla rete di servizi. Ad esempio, puoi creare una policy che stabilisca come un servizio di pagamento in esecuzione su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

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 un servizio alla rete di servizio, se il servizio è condiviso con l'account del proprietario della rete di servizio.



Proprietario del servizio: il proprietario del servizio è in genere uno sviluppatore di software all'interno di 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.

Funzionalità

Le seguenti sono 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. Indirizzi client-to-service e service-to-service traffico DNS 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

La lient-to-service connettività C viene stabilita utilizzando il piano dati VPC Lattice all'interno dell' AWS infrastruttura di rete. Quando associ un VPC alla rete di servizi, qualsiasi client all'interno del VPC può connettersi ai servizi della rete di servizio, se dispone dell'accesso richiesto.

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, VPC Lattice pubblica le metriche nell'account del proprietario del servizio e offre la possibilità di attivare la registrazione. Se i client sono associati anche alla stessa rete di servizi, il proprietario della rete di servizi riceve i registri per tutti i servizi associati alla rete di servizi. Il proprietario del servizio riceve i registri di tutti i client che effettuano richieste al proprio servizio.

VPC Lattice funziona con i seguenti strumenti per aiutarti a monitorare e risolvere i problemi dei tuoi servizi: CloudWatch gruppi di log, flussi di distribuzione Firehose e bucket 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 l'associazione tra servizio e VPC. Senza un VPC e un'associazione di servizi, i clienti non possono accedere al servizio. 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.

Come funziona VPC Lattice

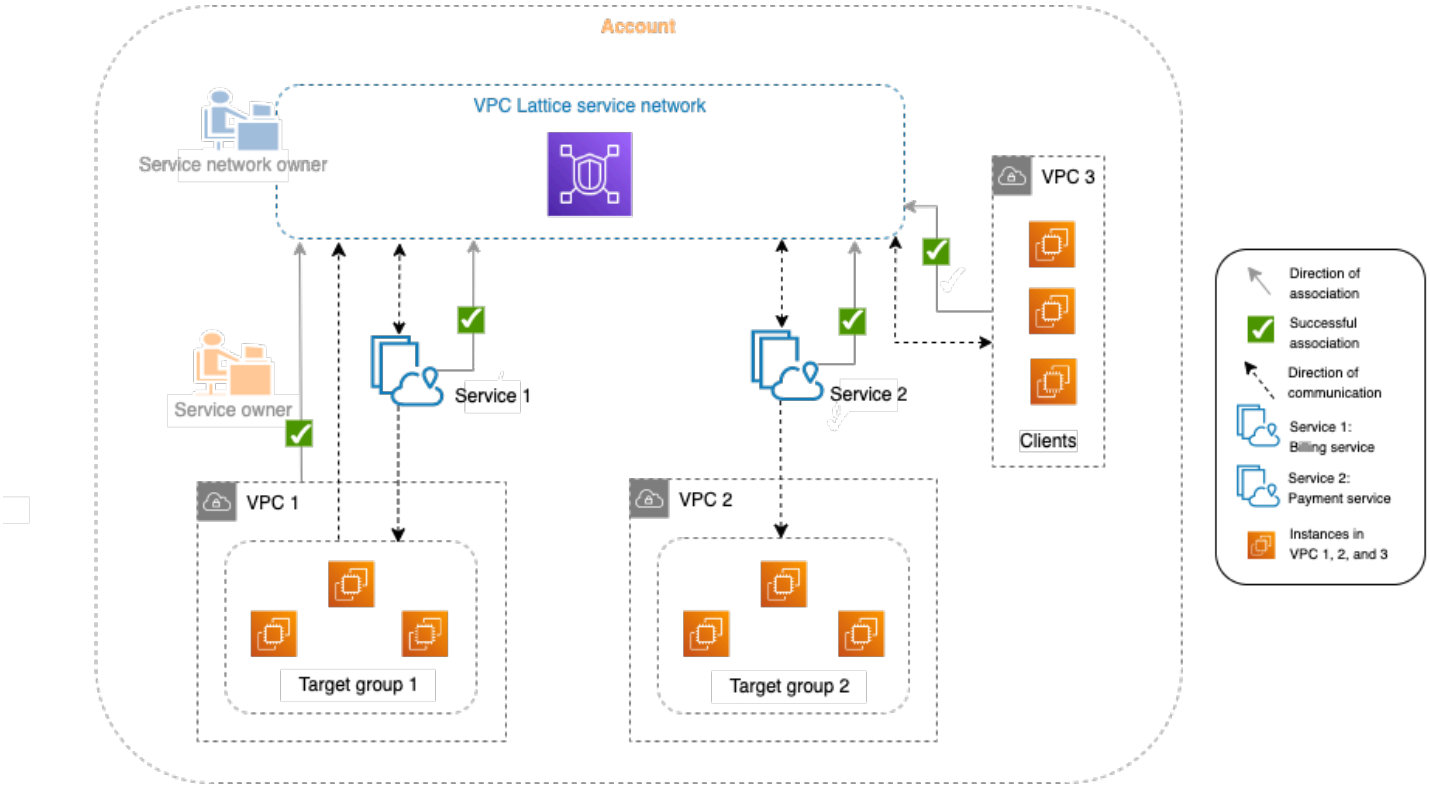
VPC Lattice è progettato per aiutarti a scoprire, proteggere, connettere e monitorare in modo semplice ed efficace tutti i servizi al suo interno. Ogni componente all'interno di VPC Lattice comunica in modo unidirezionale o bidirezionale all'interno della rete di servizi in base alla sua associazione 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:

- I servizi associati alla rete di servizi possono ricevere richieste da client i cui VPC sono associati anche alla rete di servizi.

- Un client può inviare richieste ai servizi associati a una rete di servizi solo se si trova in un VPC associato alla stessa rete di servizi. Il traffico client che attraversa una connessione peering VPC o un gateway di transito viene negato.
- Un client non può inviare richieste ai client in altri VPC associati alla rete di servizi.
- Gli obiettivi dei servizi nei VPC associati alla rete di servizi sono anche client e possono inviare richieste ad altri servizi associati alla rete di servizi.
- Le destinazioni dei servizi nei VPC che non sono associati alla rete di servizi non sono client e non possono inviare richieste ad altri servizi 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 e tre i VPC sono stati creati nello stesso account della rete di assistenza. 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.

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

1. Creare una rete di servizi

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

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 risorse mirate su cui vengono eseguiti i servizi, ad esempio le istanze. Specificano inoltre i VPC in cui risiedono questi obiettivi.

   Nel diagramma precedente, le frecce punteggiate che indicano i gruppi destinatari dei servizi rappresentano il traffico che scorre da ciascun servizio al rispettivo gruppo target. Le frecce punteggiate rappresentano la direzione della comunicazione tra il servizio e il gruppo target.

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 da altri servizi e client nei VPC associati alla rete di servizi.

   Le frecce punteggiate bidirezionali tra il servizio e la rete di servizi rappresentano la comunicazione bidirezionale risultante dall'associazione. Le frecce punteggiate dalla rete di servizi ai servizi rappresentano i servizi che ricevono richieste dai client. Le frecce punteggiate nella direzione opposta, ovvero dai servizi alla rete di servizi, rappresentano i servizi che rispondono alle richieste dei client attraverso la rete di servizi.

5. Associa i VPC alla rete di servizi

   Il proprietario della rete di assistenza associa VPC 1 e VPC 3 alla rete di servizio. Alle associazioni vengono mostrate frecce con segni di spunta puntati verso la rete di assistenza. Con queste associazioni, gli obiettivi di questi VPC diventano client e possono effettuare richieste ai servizi associati. La freccia punteggiata bidirezionale tra VPC 3 e la rete di servizi rappresenta la comunicazione bidirezionale tra i client (ad esempio, le istanze) in VPC 3 e la rete di servizi come

risultato dell'associazione. Allo stesso modo, la freccia punteggiata che punta dal gruppo target 1 alla rete di servizi rappresenta i client che effettuano richieste ad altri servizi associati alla rete di servizi.

Nota che VPC 2 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 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.

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
- 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.

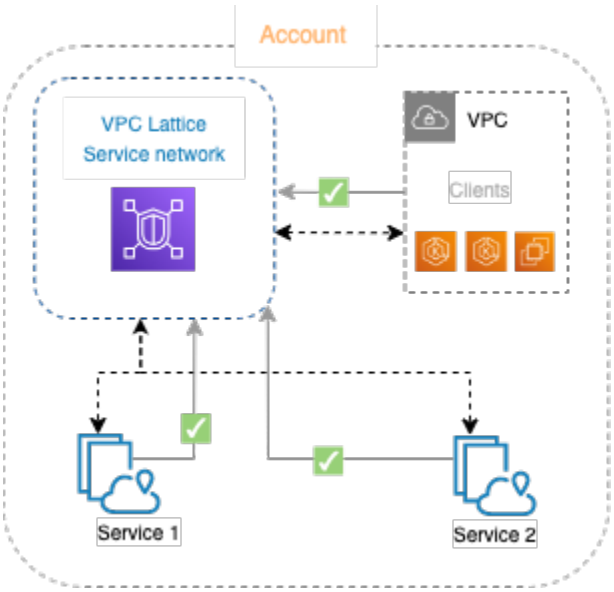
Prezzi

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. Per ulteriori informazioni, consulta i prezzi di Amazon VPC Lattice.

Reti di servizio in VPC Lattice

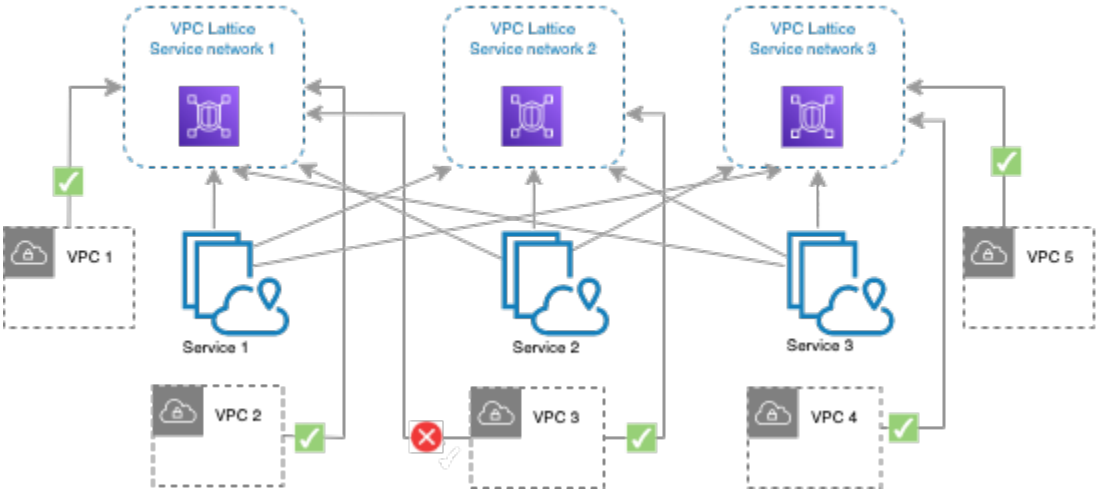
Una rete di servizi è un limite logico per una raccolta di servizi. I servizi associati alla rete possono essere autorizzati per il rilevamento, la connettività, l'accessibilità e l'osservabilità. Per effettuare richieste ai servizi della rete, il servizio o il client deve trovarsi in un VPC associato alla rete di servizi.

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 a più reti di servizi. Puoi anche associare più VPC a una rete di servizi. Tuttavia, ogni VPC può essere associato a una sola rete di servizi.

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. Tuttavia, il segno x rosso nel diagramma mostra che ogni VPC non può avere più di un'associazione a una rete di servizi.



Per ulteriori informazioni, consulta Quote per Amazon VPC Lattice.

Creare una rete di servizi

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 alla 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 di servizi”

6. (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, per associare i VPC dopo aver creato la rete di servizi, consultathe section called "Gestisci le associazioni VPC".

7. 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 AWS IAM 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).
8. (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.
9. (Facoltativo) 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, scegli Crea una condivisione di risorse nella console RAM.
10. Controlla la configurazione nella sezione Riepilogo, quindi scegli Crea rete di servizi.

Per creare una rete di servizi utilizzando il AWS CLI

Utilizza 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 alla rete di servizi, consente ai client (risorse in un VPC associato alla rete di servizi) di effettuare richieste al servizio. Quando si associa un VPC alla rete di servizi, si consente a tutte le destinazioni all'interno di quel VPC di essere client e comunicare con altri servizi nella rete di servizi.

Indice

- Gestisci le associazioni di servizi
- Gestisci le associazioni VPC

Gestisci le associazioni di servizi

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 Come funziona 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 alla 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. Seleziona Salvataggio delle 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 il AWS CLI

Utilizzare il comando create-service-network-service-association.

Per eliminare un'associazione di servizi utilizzando il AWS CLI

Utilizzare il comando delete-service-network-service-association.

Gestisci le associazioni VPC

I client possono inviare richieste ai servizi associati alla rete di servizi solo se si trovano in VPC associati alla rete di servizi. Il traffico client che attraversa una connessione peering VPC o un gateway di transito viene negato.

L'associazione di un VPC è un passaggio facoltativo quando si crea una rete di servizi. Tuttavia, la rete di servizi non è completamente funzionante finché non si associa un VPC. I proprietari della rete possono associare i VPC a una rete di servizi se il loro account dispone dell'accesso richiesto. Per ulteriori informazioni, consulta Come funziona VPC Lattice.

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 alla 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 aggiungere un tag, espandi i tag di associazione VPC, scegli Aggiungi nuovo tag e inserisci una chiave e un valore per il tag.

e. Seleziona Salvataggio delle 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.

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.

È possibile applicare le politiche 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 dettagliate, 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 alla 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 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. Seleziona Salvataggio delle modifiche.

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

Utilizza 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 alla 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. Scegliere la scheda Monitoring (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. Per 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. Seleziona Salvataggio delle modifiche.

Per abilitare i log di accesso utilizzando il AWS CLI

Utilizza il comando create-access-log-subscription.

Per aggiornare la destinazione del registro utilizzando il AWS CLI

Utilizza il comando update-access-log-subscription.

Per disabilitare i registri di accesso utilizzando il AWS CLI

Utilizza 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 uniche per ogni rete di servizi. Se aggiungi un tag con una chiave già associata alla rete di servizi, 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 alla 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. Seleziona la scheda Tags (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.

Eliminare una rete di servizi

Prima di poter eliminare una rete di servizi, è necessario eliminare tutte le associazioni che la rete di servizi potrebbe avere con qualsiasi servizio o VPC. Quando elimini una rete di servizi, eliminiamo anche tutte le risorse relative alla rete di servizio, 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 alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

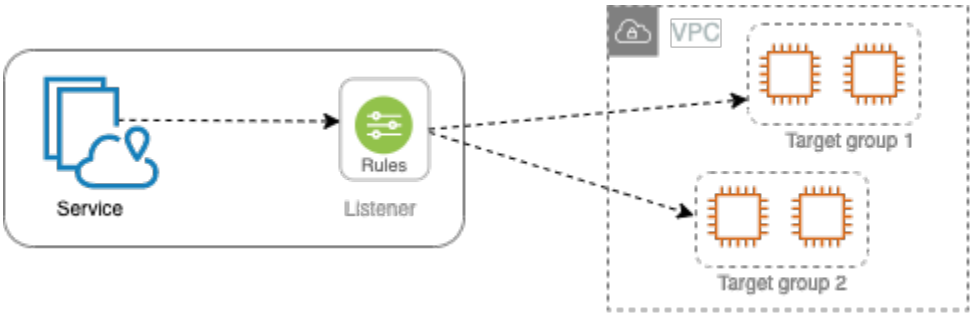
2. Nel pannello di navigazione, in VPC Lattice, scegli Reti di servizio.
3. Seleziona la casella di controllo relativa alla rete di servizio, quindi scegli Azioni, Elimina rete di servizi.
4. Quando viene richiesta la conferma, inserisci **`confirm`** e scegli Delete (Elimina).

Per eliminare una rete di servizi utilizzando il AWS CLI

Utilizza 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, contenitori 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, denominate regole di ascolto, che puoi configurare per indirizzare il traffico verso i tuoi obiettivi. Le destinazioni possono essere istanze EC2, indirizzi IP, funzioni Lambda serverless, Application Load Balancer o 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 di 1 minuto, dopodiché chiudiamo la connessione. La durata massima è di 10 minuti, dopodiché non consentiamo nuovi stream tramite la connessione e iniziamo il processo di chiusura degli stream esistenti.

Attività

- 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
- Eliminazione di un servizio

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 alla 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 63 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.

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. Seleziona 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. Una volta terminata la revisione o la 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, 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 alla 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. Seleziona Salvataggio delle 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 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 alla 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. Seleziona Salvataggio delle modifiche.

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

Utilizza 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 alla 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. Per 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. Seleziona Salvataggio delle modifiche.

Per abilitare i log di accesso utilizzando il AWS CLI

Utilizza il comando create-access-log-subscription.

Per aggiornare la destinazione del registro utilizzando il AWS CLI

Utilizza il comando update-access-log-subscription.

Per disabilitare i registri di accesso utilizzando il AWS CLI

Utilizza il comando delete-access-log-subscription.

Gestire i tag per un servizio VPC Lattice

I tag ti aiutano a classificare il tuo servizio in diversi modi, ad esempio per 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 alla 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. Seleziona la scheda Tags (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 crei 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 intuitivi che puoi fornire ai tuoi 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.

Tuttavia, ciò accade solo se mappi il tuo nome di dominio personalizzato al nome di dominio generato da VPC Lattice con un record CNAME per indirizzare le query al tuo servizio. Per ulteriori informazioni, consulta Associa un nome di dominio personalizzato al tuo servizio.

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 certificato SSL/TLS 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 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.

Per configurare un nome di dominio personalizzato per il servizio utilizzando il AWS Management Console

1. Apri alla 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 certificato SSL/TLS corrispondente al tuo nome di dominio personalizzato in Certificato SSL/TLS personalizzato. Se non disponi ancora di un certificato o non desideri aggiungerne uno ora, puoi aggiungere un certificato quando crei il tuo 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.

Per configurare un nome di dominio personalizzato per il tuo servizio utilizzando il AWS CLI

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, for`--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

Se non disponi di un certificato SSL/TLS in AWS Certificate Manager (ACM), puoi crearne o importarne uno prima di configurare un nome di dominio personalizzato. Tuttavia, il certificato è necessario solo se desideri soddisfare le richieste HTTPS utilizzando il tuo nome di dominio personalizzato. Per ulteriori informazioni, consulta Porta il tuo certificato (BYOC) per VPC Lattice.

Associa un nome di dominio personalizzato al tuo servizio

Innanzitutto, se non l'hai già fatto, registra il tuo nome di dominio personalizzato. La Internet Corporation for Assigned Names and Numbers (ICANN) gestisce i nomi di dominio su Internet. Puoi registrare un nome di dominio utilizzando un registrar nome dominio, un'organizzazione accreditata ICANN 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 ulteriori 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 CNAME 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, 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 CNAME 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. Per ulteriori informazioni, consulta Creazione di record utilizzando la console Amazon Route 53 nella Amazon Route 53 Developer Guide. Inoltre, puoi fare riferimento ai passaggi seguenti per creare una zona ospitata e un record CNAME per mappare il tuo nome di dominio personalizzato all'endpoint VPC Lattice.

Per creare una zona ospitata privata o pubblica con un record CNAME utilizzando la console Amazon Route 53

1. Apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.
2. Nel pannello di navigazione, scegli Zone ospitate, quindi Crea zona ospitata.
3. Per Nome di dominio, scegli il nome della zona ospitata che desideri utilizzare per indirizzare il traffico verso il tuo servizio VPC Lattice. Ad esempio, se il nome di dominio personalizzato è `parking.example.com` (http://parking.example.com/), il nome di dominio per la zona ospitata sarà `example.com` (http://example.com/), noto anche come nome di dominio apex. Puoi quindi creare un record CNAME per questa zona ospitata per indirizzare il traffico verso il tuo servizio VPC Lattice. Nota: non puoi modificare il nome di una zona ospitata dopo averla creata.
4. Per Tipo, scegli Private Hosted Zone o Public Hosted Zone come richiesto.
5. Scegli la tua regione e seleziona l'ID VPC per un VPC che desideri associare a questa zona ospitata.
6. Aggiungi i tag se necessario e scegli Crea zona ospitata. Dopo la creazione, la zona ospitata viene elencata in Zone ospitate.
7. Per creare un record CNAME nella zona ospitata appena creata, seleziona la zona ospitata, quindi seleziona Crea record.
8. Specificate i seguenti valori in Crea record:

    a. In Record name, inserisci il nome che desideri utilizzare come nome di dominio personalizzato. Se desideri utilizzare `parking.example.com` (http://acme.example.com/) come nome di dominio personalizzato, `parking` inserisci*. Ciò significa che devi inserire il nome del sottodominio `parking` ma senza il nome di dominio della zona ospitata `example.com` (http://example.com/).

b. Per Tipo di record, scegli CNAME.

c. Mantieni l'alias disattivato.

d. Per Value, inserisci il VPC Lattice che ha generato il nome di dominio per il tuo servizio (ad esempio,). `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws` Troverai questo nome di dominio generato automaticamente nella console VPC Lattice nella pagina del tuo servizio. Se si utilizza il AWS CLI, l'output dei `list-services` comandi `create-service` o restituirà questo nome di dominio generato automaticamente.

e. Per TTL (secondi), accettate il valore predefinito di 300.

f. Per Politica di routing, scegli la politica di routing applicabile. Per ulteriori informazioni, consulta la sezione Choose a routing policy nella Amazon Route 53 Developer Guide.

9. Scegli Crea record.

   In genere le modifiche si propagano a tutti i server Route 53 entro 60 secondi. Al termine della propagazione, sarai in grado di indirizzare il traffico verso il tuo servizio utilizzando il nome di dominio personalizzato.

Per creare un record di alias nella tua zona ospitata utilizzando il AWS CLI

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

```
aws route53 change-resource-record-sets --hosted-zone-id hosted-zone-id-for-your-service-domain --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 nel 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-service-domain.com alias",
    "Changes": [
        {
```

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

Porta il tuo certificato (BYOC) per VPC Lattice

Per soddisfare le richieste HTTPS, devi disporre del tuo certificato SSL/TLS pronto all'uso 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 certificato SSL/TLS 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 corrispondenze con caratteri jolly che si trovano a un livello profondo 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 del dominio wildcard. Ciò significa che un wildcard può essere utilizzato solo come sottodominio di primo livello e che protegge solo un livello di sottodominio. Ad esempio, se la SAN del certificato lo è`*.example.com`, allora non è supportata. `parking.*.example.com`
- VPC Lattice supporta una wildcard 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 certificato SSL/TLS in ACM deve trovarsi nella stessa regione del servizio VPC Lattice a cui lo stai associando.

Protezione della chiave privata del certificato

Quando richiedi un certificato SSL/TLS utilizzando ACM, ACM genera una coppia di chiavi pubblica/privata. Quando si importa un certificato, si genera la key pair. 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 la sezione Protezione dei dati AWS Certificate Manager nella Guida per l'AWS Certificate Manager utente.

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 (sessione SSL/TLS) 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 Developer Guide.AWS Key Management Service

Per ulteriori informazioni, consulta Crittografia a riposo.

Eliminazione di un servizio

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, gli ascoltatori, le regole dei listener e le sottoscrizioni ai registri di accesso.

Per eliminare un servizio utilizzando la console

1. Apri alla 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 Delete (Elimina).

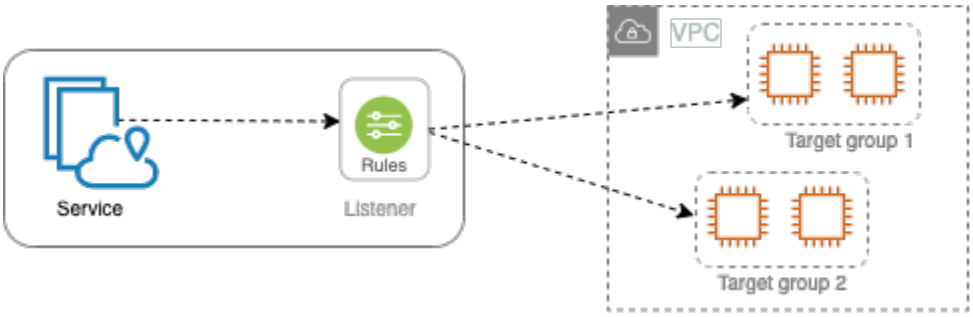
Per eliminare un servizio utilizzando il AWS CLI

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. Le destinazioni possono essere istanze EC2, indirizzi IP, funzioni Lambda, Application Load Balancer o 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 alla 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. Seleziona 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.

Per creare un gruppo target utilizzando il AWS CLI

Utilizzare il create-target-groupcomando 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 le risorse 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
- Registrazione o annullamento della 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 alla 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 alla 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 alla 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.

Registrazione o annullamento della 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 alla 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 lo stato del gruppo target nella Guida per l'utente di 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 HealthCheckIntervalSecondssecondo, 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 UnhealthyThresholdCountconsecutivi, il servizio mette fuori servizio l'obiettivo. Quando i controlli di integrità superano i successi HealthyThresholdCountconsecutivi, il servizio rimette l'obiettivo in servizio.

Impostazione	Descrizione
HealthCheckProtocol	Il protocollo utilizzato dal servizio per eseguire i controlli di integrità 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'imposta zione predefinita prevede l'utilizzo della porta

Impostazione	Descrizione
	su cui ogni destinazione riceve il traffico dal servizio.
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 predefini to è 5. Specificare 0 per ripristinare questa impostazione al valore predefinito.

Impostazione	Descrizione
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 impostazi one al valore predefinito.
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 configura zione 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 alla 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 alla 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. Seleziona Salvataggio delle modifiche.

Per modificare le impostazioni del controllo sanitario utilizzando il AWS CLI

Utilizza 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 man-in-the-middle attacchi o spoofing anche se i certificati sulle destinazioni 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.

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 VPC Lattice Services. 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.
- Per registrare un'attività ECS come destinazione, utilizza il tipo di `ALB` destinazione e registra l'Application Load Balancer per il tuo servizio Amazon ECS. Per ulteriori informazioni, consulta Service load balancing nella Guida per gli sviluppatori di Amazon Elastic Container Service.
- Per registrare un pod EKS come destinazione, utilizza il AWS Gateway 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 e. `INSTANCE` `IP`

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 costituti 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-forwardedintestazioni

Amazon VPC Lattice aggiunge le seguenti intestazioni: `x-forwarded`

`x-forwarded-for`

L'indirizzo IP di origine.

`x-forwarded-for-port`

La porta di destinazione.

`x-forwarded-for-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.
- `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 (nome/CN).
- `X509SAN/URI`— Il nome alternativo del soggetto (URI).
- `X509Subject/CN`— Il nome del soggetto (CN).

`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.

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. Per ulteriori informazioni, consulta Using AWS Lambda with Amazon VPC Lattice nella Developer Guide.AWS Lambda

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 alla 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. Seleziona 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 di destinazioni e registrare la funzione Lambda tramite AWS CLI

Usa i comandi create-target-groupe 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-encoding`intestazione 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 target`LAMBDA`, 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": "/",
    "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 (nome/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. 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",
    "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 hop-by-hop intestazioni, 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,
    "statusDescription": "200 OK",
    "headers": {
        "Set-cookie": "cookies",
        "Content-Type": "application/json"
    },
    "body": "Hello from Lambda (optional)"
}
```

Intestazioni con più valori

Per impostazione predefinita, VPC Lattice supporta le richieste provenienti da un client o le risposte da una funzione Lambda contenente intestazioni con più valori o contenenti la stessa intestazione più volte. VPC Lattice supporta anche parametri di interrogazione con più valori per la stessa chiave.

Per le intestazioni di richiesta, se più parametri condividono lo stesso nome, VPC Lattice passerà entrambi i valori ai target. Di seguito è riportato un esempio in cui `header 1` è riportato il nome di due intestazioni separate:

```
header1 = foo
header1 = bar
```

Quindi VPC Lattice invia entrambi i valori ai target:

```
"header1": ["foo", "bar"]
```

Per le stringhe di query, se più parametri condividono lo stesso nome, vince l'ultimo valore. Ciò significa che i parametri `_not_ coalesced` rientrano in un unico valore se condividono lo stesso nome di chiave.

Di seguito è riportato un esempio in cui `foo` e `bar` sono i valori dei parametri con lo stesso nome`QS1`:

```
http://www.example.com?&QS1=foo&QS1=bar
```

Quindi VPC Lattice invia l'ultimo valore ai target:

```
"QS1": "bar"
```

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 alla 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 AWS 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 la sezione Health checks for your target group nella User Guide for 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 SSL/TLS del load balancer.
- 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 X-Forwarded-For nella User Guide for Application Load Balancers.

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 i gruppi target ALB. Tuttavia, puoi configurare i controlli di integrità per i gruppi target per il tuo Application Load Balancer. Per ulteriori informazioni, consulta lo stato del gruppo Target nella Guida per l'utente di Application Load Balancers.

Per creare il gruppo target

1. Apri alla 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 Protocol (Protocollo), selezionare **HTTP** o **HTTPS**. 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. Seleziona 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	Riuscito
HTTP/2	HTTP/1.1	Riuscito
gRPC	HTTP/1.1	Errore
HTTP/1.1	HTTP/2	Errore
HTTP/2	HTTP/2	Riuscito
gRPC	HTTP/2	Riuscito se le destinazioni supportano gRPC
HTTP/1.1	gRPC	Errore
HTTP/2	gRPC	Riuscito se la richiesta è POST
gRPC	gRPC	Riuscito

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. Puoi scegliere HTTP o HTTPS per il protocollo del gruppo di destinazione.
- Le uniche regole di ascolto 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 formato UTF-8, più i caratteri speciali + - = . _ : / @. Non utilizzare spazi iniziali o finali.
- Non utilizzate il `aws:` prefisso nei nomi o nei valori dei tag perché è riservato all'uso. AWS 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 alla 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. Seleziona la scheda Tags (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 il AWS 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

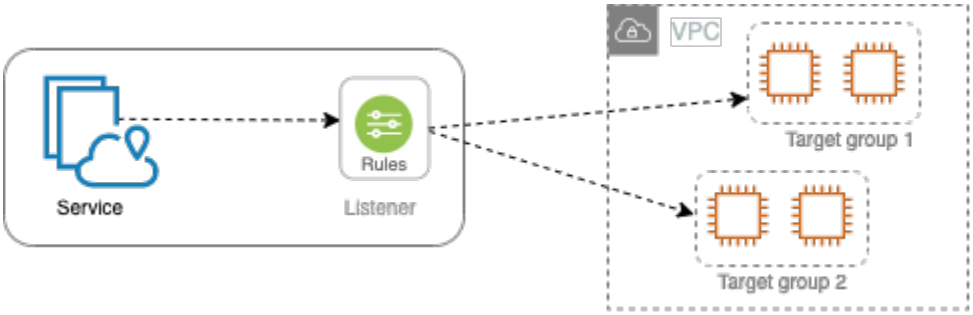
1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, scegli Target groups.
3. Seleziona la casella di controllo per il gruppo target, quindi scegli Azioni, Elimina.
4. Quando viene richiesta la conferma, immettere **`confirm`** e quindi scegliere Elimina.

Per eliminare un gruppo target utilizzando il AWS 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 che definisci per un listener determinano il modo in cui il servizio indirizza le richieste verso le destinazioni registrate.



Indice

- Configurazione dei listener
- Creare un listener
- Listener HTTP per i servizi VPC Lattice
- Listener HTTPS per servizi VPC Lattice
- Listener TLS per i servizi VPC Lattice
- Regole di ascolto per il tuo servizio VPC Lattice
- Aggiornamento di un listener
- Eliminazione di un listener

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 HTTP/1.1 e HTTP/2. Quando si configura un servizio con un listener HTTPS, VPC Lattice determinerà automaticamente il protocollo HTTP

utilizzando Application-Layer 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, HTTPS, HTTP/1.1 e 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. WebSockets

Creare un listener

Puoi creare listener per il tuo servizio VPC Lattice. Quando si crea un listener, è necessario specificare un nome, un'azione e un protocollo predefiniti. Un listener viene fornito con una regola predefinita. Puoi anche creare regole aggiuntive per il tuo ascoltatore.

Per creare un ascoltatore utilizzando la console

- the section called “Aggiunta di un ascoltatore HTTP ”
- the section called “Aggiunta di un ascoltatore HTTPS”
- the section called “Aggiungi un listener TLS”
- the section called “Aggiungere una regola”

Per creare un ascoltatore utilizzando AWS CLI

Utilizzate i comandi create-listener e create-rule.

Listener HTTP per i 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 alla 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 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.

È possibile creare un listener HTTPS, che utilizza la versione TLS 1.2 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 HTTP/1.1 e HTTP/2. Quando si configura un servizio con un listener HTTPS, VPC Lattice determinerà automaticamente il protocollo HTTP tramite Application-Layer 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.

VPC Lattice può ascoltare su HTTP, HTTPS, HTTP/1.1 e 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 del protocollo TLSv1.2 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 il protocollo TLSv1.2 e i seguenti cifrari SSL/TLS in questo ordine 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`

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 HTTP/1 e 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`

Preferisci HTTP/2 a 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 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 alla 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 tra Certificato SSL/TLS personalizzato. 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 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 i 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

- Le politiche di autenticazione sono limitate ai principali anonimi
- I target Lambda non sono supportati

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 alla 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 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 regola
- 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 regola

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 di inoltro e azioni di 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.

Operazioni con risposta fissa

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.

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.

Metodi match

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 alla 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. Seleziona Salvataggio delle 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 alla 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 in base alle esigenze.
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 alla 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. Seleziona Salvataggio delle modifiche.

Per eliminare una regola utilizzando il AWS CLI

Utilizzare il comando delete-rule.

Aggiornamento di un listener

Dopo aver creato un listener, è possibile sostituire il gruppo target per l'azione predefinita. È inoltre possibile aggiungere un gruppo target all'azione predefinita e assegnare pesi ai gruppi target. Non è possibile aggiornare il nome del listener, il protocollo del listener o la porta del listener.

Per aggiornare un listener utilizzando la console

1. Apri alla 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. Per l'azione predefinita, puoi aggiornare il gruppo target o il peso in base alle esigenze.
6. Per aggiungere altri gruppi target, scegli Aggiungi azione, quindi scegli un gruppo target e specificane il peso.
7. Puoi anche aggiungere, modificare o eliminare le regole del listener. Per ulteriori informazioni, consulta Regole dei listener.
8. Controlla gli aggiornamenti e scegli Salva modifiche.

Per aggiornare l'azione predefinita per un ascoltatore utilizzando il AWS CLI

Utilizzate il comando update-listener.

Eliminazione di un listener

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

Per eliminare un listener utilizzando la console

1. Apri alla 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 AWS CLI

Utilizza il comando delete-listener.

Condividi le tue risorse VPC Lattice

Amazon VPC Lattice si integra con AWS Resource Access Manager (AWS RAM) per consentire la condivisione delle risorse. AWS RAMè un servizio che consente di condividere alcune risorse VPC Lattice con altri Account AWS o tramite. AWS Organizations Con AWS RAM, condividi le risorse di cui sei proprietario creando una condivisione delle risorse. Una condivisione delle risorse specifica le risorse da condividere e i consumatori con cui condividerle. I consumatori possono includere:

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

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

Indice

- Prerequisiti per la condivisione delle risorse VPC Lattice
- Condividi le risorse VPC Lattice
- Smetti di condividere le risorse VPC Lattice
- Responsabilità e autorizzazioni
- Eventi tra account

Prerequisiti per la condivisione delle risorse VPC Lattice

- Per condividere una risorsa, devi possederla nel tuo. Account AWS Ciò significa che la risorsa deve essere allocata o fornita nel tuo account. Non puoi condividere una risorsa che è stata condivisa con te.
- Per condividere una risorsa con la tua organizzazione o un'unità organizzativa inAWS Organizations, devi abilitare la condivisione conAWS Organizations. Per ulteriori informazioni, consulta Abilitare la condivisione delle risorse AWS Organizations all'interno della Guida AWS RAM per l'utente.

Condividi le risorse VPC Lattice

Per condividere una risorsa, inizia creando una condivisione di risorse utilizzandoAWS Resource Access Manager. Una condivisione di risorse specifica le risorse da condividere, i consumatori con cui vengono condivise e le azioni che i responsabili possono eseguire.

Quando condividi una risorsa VPC Lattice di tua proprietà con altriAccount AWS, consenti a tali account di associare le proprie risorse alle risorse del tuo account. Quando crei un'associazione con una risorsa condivisa, generiamo un Amazon Resource Name (ARN) nell'account del proprietario della risorsa e più un ARN nell'account che ha creato l'associazione. In questo modo, sia il proprietario della risorsa 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 alla risorsa condivisa. In caso contrario, i consumatori ricevono un invito a partecipare alla condivisione di risorse e ottengono l'accesso alla risorsa condivisa dopo aver accettato l'invito.

Considerazioni

- Puoi condividere due tipi di risorse VPC Lattice: reti di servizi e servizi.
- Puoi condividere le tue risorse VPC Lattice con chiunque. Account AWS
- Non puoi condividere le tue risorse VPC Lattice con singoli utenti e ruoli IAM.
- VPC Lattice supporta le autorizzazioni gestite dai clienti sia per le reti di servizio che per i servizi.

Per condividere una risorsa di tua proprietà utilizzando la console VPC Lattice

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi o Reti di servizio.
3. Scegli il nome della risorsa per aprire la relativa pagina dei dettagli, quindi scegli Share service o Share service network 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 Share service o Share service network.

Per condividere una risorsa di tua proprietà utilizzando la AWS RAM console

Utilizza la procedura descritta in Creare una condivisione di risorse nella Guida AWS RAM per l'utente.

Per condividere una risorsa di tua proprietà utilizzando il AWS CLI

Utilizza il comando associate-resource-share.

Smetti di condividere le risorse VPC Lattice

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

Per interrompere la condivisione di una risorsa di tua proprietà utilizzando la console VPC Lattice

1. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, in VPC Lattice, scegli Servizi o Reti di servizio.
3. Scegli il nome della risorsa 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 una risorsa di tua proprietà utilizzando la AWS RAM console

Vedi Aggiornare una condivisione di risorse nella Guida AWS RAM per l'utente.

Per interrompere la condivisione di una risorsa di tua proprietà, utilizza il AWS CLI

Utilizza il comando disassociate-resource-share.

Responsabilità e autorizzazioni

Le seguenti responsabilità e autorizzazioni si applicano all'utilizzo di risorse VPC Lattice condivise.

Proprietari delle risorse

- 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 del servizio può descrivere tutte le associazioni di rete con il servizio.
- Il proprietario del servizio può dissociare un servizio da qualsiasi rete di assistenza a cui è associato.
- Solo l'account che ha creato un'associazione può aggiornare l'associazione tra la rete di servizi e il VPC.

Consumatori di risorse

- Il consumatore non può eliminare un servizio che non ha creato.
- Il consumatore può dissociare solo i servizi 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 un servizio.
- Il consumatore non può recuperare le informazioni di servizio di un servizio di cui non è proprietario.
- Il consumatore può descrivere tutte le associazioni di servizi con una rete di servizi condivisa.
- Il consumatore può associare un servizio 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 i VPC che ha associato a una rete di servizi.
- 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.
- Il consumatore può descrivere un servizio o una rete di servizi condivisa con lui.
- Il consumatore non può associare due risorse se entrambe sono condivise con lui.

Eventi tra account

Quando i proprietari e i consumatori delle risorse eseguono azioni su una risorsa condivisa, tali azioni vengono registrate come eventi tra account in. AWS CloudTrail

`CreateServiceNetworkServiceAssociationBySharee`

Inviato al proprietario della risorsa quando un utente di risorse chiama CreateServiceNetworkServiceAssociationcon una risorsa 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 della risorsa quando un utente di risorse chiama CreateServiceNetworkVpcAssociationcon una rete di servizi condivisa.

`DeleteServiceNetworkServiceAssociationByOwner`

Inviato al proprietario dell'associazione quando il proprietario della risorsa chiama DeleteServiceNetworkServiceAssociationcon una risorsa 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 della risorsa quando un utente di risorse chiama DeleteServiceNetworkServiceAssociationcon una risorsa 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 della risorsa chiama DeleteServiceNetworkVpcAssociationcon una rete di servizi condivisa.

`DeleteServiceNetworkVpcAssociationBySharee`

Inviato al proprietario della risorsa quando un utente di risorse chiama DeleteServiceNetworkVpcAssociationcon una rete di servizi condivisa.

`GetServiceBySharee`

Inviato al proprietario della risorsa quando un consumatore di risorse chiama GetServicecon un servizio condiviso.

`GetServiceNetworkBySharee`

Inviato al proprietario della risorsa quando un consumatore di risorse chiama GetServiceNetworkcon una rete di servizi condivisa.

`GetServiceNetworkServiceAssociationBySharee`

Inviato al proprietario della risorsa quando un consumatore di risorse chiama GetServiceNetworkServiceAssociationcon una risorsa 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 della risorsa quando un utente di risorse chiama GetServiceNetworkVpcAssociationcon una rete di servizi condivisa.

Di seguito è riportato un esempio di voce relativa all'`CreateServiceNetworkServiceAssociationByShareee`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-eaa89f4a47cd",
    "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"
}
```

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 di mantenere il controllo sui 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. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità 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. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua 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 le tue risorse VPC Lattice.

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 dell'interfaccia () 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 fornire l'accesso e con quali VPC. Per gli scenari con più account, puoi utilizzarli per condividere le risorse oltre AWS Resource Access Manageri confini degli account. VPC Lattice fornisce un framework che consente di implementare una defense-in-depth strategia su più livelli della rete.

- Primo livello: l'associazione del servizio e del VPC con una rete di servizi. Se un VPC o un servizio specifico non è associato alla rete di servizi, i client nel VPC non hanno accesso al servizio.
- 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 risorse in un VPC anziché a tutte le risorse 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.

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 policy di autenticazione a ogni rete di servizio o servizio a cui si desidera controllare l'accesso.

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 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.

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
- 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 politiche 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, consultaReti di servizio in VPC Lattice.

Attività

- 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 i passaggi descritti 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, consultaServizi in VPC Lattice.

Attività

- 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-type`opzione 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 Politiche basate sull'identità e politiche basate sulle risorse nella Guida per l'utente IAM.

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.

È necessario specificare un principale in una policy basata sulle risorse. 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'`Resource`elemento come illustrato negli esempi seguenti.

Esempi di risorse per le politiche di autenticazione

Protocollo	Esempi
HTTP	• `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/rates"` • `"Resource": "*/rates"`

Protocollo	Esempi
	• `"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
```

Per 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 e`aws: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 VPC Lattice. Per ulteriori informazioni, consulta Condition keys for Amazon VPC Lattice Services nel Service Authorization Reference.

Chiavi condizionali per le politiche di autenticazione

Chiavi di condizione	Descrizione	Esempio	Disponibile per chiamanti anonimi (non autenticati)?	Disponibile per gRPC?
`vpc-lattice-svcs:Port`	Filtra l'accesso tramite la porta di servizio a cui viene effettuata la richiesta	80	Sì	Sì
`vpc-lattice-svcs:RequestMethod`	Filtra l'accesso in base al metodo della richiesta	GET	Sì	PUBBLICA sempre
`vpc-lattice-svcs:RequestHeader/` *`header-name`* `:` *`value`*	Filtra l'accesso in base a una coppia nome-valore dell'intestazione nelle intestazioni della richiesta	content-type: application/json	Sì	Sì
`vpc-lattice-svcs:RequestQueryString/` *`key-name`*`:` *`value`*	Filtra l'accesso dalle coppie chiave-valore della stringa di query nell'URL della richiesta	quux: [corge, grault]	Sì	No
`vpc-lattice-svcs:ServiceNetworkArn`	Filtra l'accesso tramite l'ARN della rete di servizi del servizio che riceve la richiesta	arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/sn-0123456789abcdef0	Sì	Sì

Chiavi di condizione	Descrizione	Esempio	Disponibile per chiamanti anonimi (non autenticati)?	Disponibile per gRPC?
`vpc-lattice-svcs:ServiceArn`	Filtra l'accesso in base all'ARN del servizio che riceve la richiesta	arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0	Sì	Sì
`vpc-lattice-svcs:SourceVpc`	Filtra l'accesso in base al VPC da cui proviene la richiesta	vpc-1a2b3c4d	Sì	Sì
`vpc-lattice-svcs:SourceVpcOwnerAccount`	Filtra l'accesso in base all'account proprietario del VPC da cui viene effettuata la richiesta	123456789012	Sì	Sì

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: limitare l'accesso ai servizi da parte di un'organizzazione specifica AWS

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.

```
{
   "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'`Resource`elemento è la stessa del servizio a cui è allegata la policy.

```
{
   "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*

```
{
   "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"
            }
         }
      }
   ]
}
```

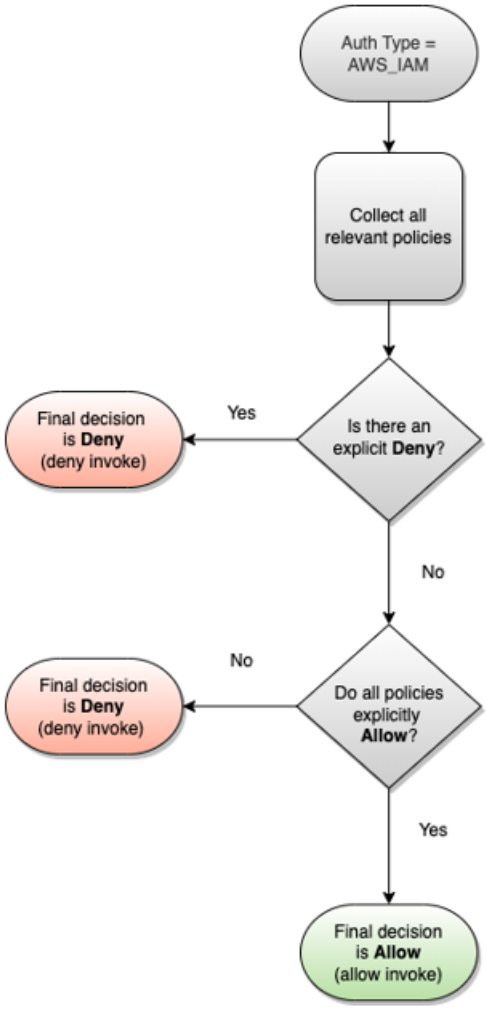
Come funziona l'autorizzazione

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 risorse 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.

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. 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.*regione*.vpc-lattice
- com.amazonaws.*region*.ipv6.vpc-lattice

Per maggiori informazioni, consulta Elenchi di prefissi gestiti da AWS nella Guida dell'utente di Amazon VPC.

Client Windows

Gli indirizzi negli elenchi di prefissi VPC Lattice sono indirizzi locali del collegamento. Se ti connetti a VPC Lattice da un client Windows, devi aggiornare la configurazione del client Windows in modo che inoltri gli indirizzi locali del collegamento utilizzati da VPC Lattice all'indirizzo IP primario del client. Di seguito è riportato un comando di esempio che aggiorna la configurazione del client Windows, 169.254.171.0 dov'è l'indirizzo locale del collegamento utilizzato da VPC Lattice.

```
C:\> route add 169.254.171.0 mask 255.255.255.0 primary-ip-address
```

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 di controllo dello stato.
- 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.

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.

In entrata

Crea	Protocollo	Intervallo porte	Commento
CIDR VPC	*listener*	*listener*	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.

In uscita

Destinazione	Protocollo	Intervallo porte	Commento
ID dell'elenco dei prefissi VPC Lattice	*listener*	*listener*	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.

In entrata

Crea	Protocollo	Intervallo porte	Commento
ID dell'elenco dei prefissi VPC Lattice	*target*	*target*	Consenti il traffico da VPC Lattice agli obiettivi
ID dell'elenco dei prefissi VPC Lattice	*health check*	*health check*	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 alla 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. Seleziona Salvataggio delle modifiche.

Per aggiungere o aggiornare gruppi di sicurezza per un'associazione VPC esistente utilizzando la console

1. Apri alla 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 secondo necessità.
6. Seleziona Salvataggio delle 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": "snva-0123456789abcdef0",
  "status": "CREATE_IN_PROGRESS",
  "securityGroupIds": ["sg-7c2270198example"]
}
```

Per aggiungere o aggiornare gruppi di sicurezza per un'associazione VPC esistente utilizzando AWS CLI

Utilizzare 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 l'intervallo di indirizzi IP da consentire dall'elenco dei prefissi gestiti per VPC Lattice.

In entrata

Crea	Protocollo	Intervallo porte	Commento
vpc_lattice_cidr_block	TCP	1025-65535	Consenti il traffico da VPC Lattice ai client

In uscita

Destinazione	Protocollo	Intervallo porte	Commento
vpc_latti ce_cidr_block	*listener*	*listener*	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 l'intervallo di indirizzi IP da consentire dall'elenco dei prefissi gestiti per VPC Lattice.

In entrata

Crea	Protocollo	Intervallo porte	Commento
vpc_latti ce_cidr_block	*target*	*target*	Consenti il traffico da VPC Lattice agli obiettivi
vpc_latti ce_cidr_block	*health check*	*health check*	Consenti il traffico di health check da VPC Lattice agli obiettivi

In uscita

Destinazione	Protocollo	Intervallo porte	Commento
vpc_latti ce_cidr_block	*target*	1024-65535	Consenti il traffico dai target a VPC Lattice
vpc_latti ce_cidr_block	*health check*	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 Signing AWS API request nella IAM User Guide.

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 con interceptor
- Java senza interceptor
- Node.js

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 `awscrt` pacchetti `botocore` and, utilizzare il comando seguente. Per ulteriori informazioni, consulta AWS CRT Python.

```
pip install botocore awscrt
```

Nell'esempio seguente, sostituite i valori segnaposto con i vostri valori.

SIGv4

```
from botocore import crt
import requests
```

```
from botocore.awsrequest import AWSRequest
from botocore.credentials import Credentials
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtS3SigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
 'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["has_streaming_input"] = True # payload signing is not supported
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
```

SIGv4A

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
from botocore.credentials import Credentials
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtS3SigV4AsymAuth(session.get_credentials(), 'vpc-lattice-
svcs', 'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["has_streaming_input"] = True # payload signing is not supported
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
```

Java con interceptor

Questo esempio utilizza Amazon Request Signing Interceptor per gestire la firma delle richieste.

```
import com.amazonaws.http.AwsRequestSigningApacheInterceptor;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
import software.amazon.awssdk.regions.Region;

import java.nio.charset.StandardCharsets;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {
    public static void main(String[] args) {
      var interceptor = new AwsRequestSigningApacheInterceptor(
          "vpc-lattice-svcs",
          Aws4UnsignedPayloadSigner.create(), // requires HTTPS
          DefaultCredentialsProvider.create(),
          Region.US_WEST_2.id()
          );
      CloseableHttpClient client = HttpClients.custom()
        .addInterceptorLast(interceptor)
        .build();

      var httpPost = new HttpPost("https://user-02222f67d3a427111.1234abc.vpc-lattice-
svcs.us-west-2.on.aws/create");
      httpPost.addHeader("content-type", "application/json");

      var body = """
      {
        "name": "Jane Doe",
        "job": "Engineer"
      }
      """;
      httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

      try (var response = client.execute(httpPost)) {
        System.out.println(new
 String(response.getEntity().getContent().readAllBytes()));
      } catch (Exception e) {
```

```
            throw new RuntimeException(e);
        }
    }
}
```

Java senza interceptor

Questo esempio mostra come 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 for Java Consente solo payload non firmati su HTTPS. Tuttavia, puoi estendere il firmatario per supportare payload non firmati tramite HTTP.

```
import java.io.ByteArrayInputStream;
import java.io.IOException;
import java.nio.charset.StandardCharsets;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
import software.amazon.awssdk.auth.signer.AwsSignerExecutionAttribute;
import software.amazon.awssdk.core.interceptor.ExecutionAttributes;
import software.amazon.awssdk.http.SdkHttpFullRequest;
import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.regions.Region;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {

    public static void main(String[] args) {
        var signer = Aws4UnsignedPayloadSigner.create(); // requires HTTPS

        Map<String, String> headers = new HashMap<>();
        headers.put("content-type", "application/json");
        var body = """
        {
            "name": "Jane Doe",
            "job": "Engineer"
```

```
        }
        """;

        String endpoint = "https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create";

        var sdkRequest = SdkHttpFullRequest.builder().method(SdkHttpMethod.POST);

        sdkRequest.host("user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws");
        sdkRequest.protocol("HTTPS");
        sdkRequest.encodedPath("/create");
        sdkRequest.contentStreamProvider(() -> new
 ByteArrayInputStream(body.getBytes(StandardCharsets.UTF_8)));


        for (Map.Entry<String, String> header : headers.entrySet()) {
            sdkRequest.putHeader(header.getKey(), header.getValue());
        }

        ExecutionAttributes attributes = ExecutionAttributes.builder()
                .put(AwsSignerExecutionAttribute.AWS_CREDENTIALS,
 DefaultCredentialsProvider.create().resolveCredentials())
                .put(AwsSignerExecutionAttribute.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
                .put(AwsSignerExecutionAttribute.SIGNING_REGION, Region.US_WEST_2)
                .build();

        SdkHttpFullRequest prepRequest = signer.sign(sdkRequest.build(), attributes);

        HttpPost httpPost = new HttpPost(endpoint);
        for (Map.Entry<String, List<String>> header : prepRequest.headers().entrySet())
 {
            if (header.getKey().equalsIgnoreCase("host")) { continue; }
            for(var value : header.getValue()) {
                httpPost.addHeader(header.getKey(), value);
            }
        }

        CloseableHttpClient client = HttpClients.custom().build();

        httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

        try (var response = client.execute(httpPost)){
```

```
            System.out.println(new
 String(response.getEntity().getContent().readAllBytes()));
        } catch (IOException e) {
            throw new RuntimeException(e);
        }
    }
}
```

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').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: '/',
      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').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: '/',
      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()
  }
)
```

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 Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Crittografia 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, leggere/descrivere, aggiornare, eliminare ed elencare le risorse (CRUDL) (ad esempio e. `CreateService` `UpdateService` Le comunicazioni verso il piano di controllo di VPC Lattice sono protette in transito da TLS. Il piano dati è l'API Invoke di VPC Lattice che fornisce l'interconnessione tra i servizi. TLS crittografa anche le comunicazioni sul piano dati di VPC Lattice. 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 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

- Crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3)
- Crittografia lato server con AWS KMS chiavi memorizzate in (SSE-KMS) AWS KMS

Crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3)

Quando usi la crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3), ogni oggetto viene crittografato con una chiave univoca. Come ulteriore tutela, crittografa la chiave con una chiave root che ruota con regolarità. Per crittografare i dati, la crittografia lato server di Simple Storage Service (Amazon S3) utilizza una delle crittografie di blocco più complesse disponibili, lo standard di crittografia avanzata a 256 bit (AES-256). Per gli oggetti crittografati prima di AES-GCM, è ancora supportato AES-CBC per decrittare tali oggetti. Per ulteriori informazioni, consulta Uso della crittografia lato server con le chiavi di crittografia gestite da Amazon S3 (SSE-S3).

Se abiliti la crittografia lato server con chiavi di crittografia gestite da Amazon S3 (SSE-S3) per il tuo bucket S3 per i log di accesso VPC Lattice, crittografa AWS automaticamente ogni file di log di accesso prima che venga archiviato nel bucket S3. Per ulteriori informazioni, consulta Logs sent to Amazon S3 nella CloudWatch Amazon User Guide.

Crittografia lato server con AWS KMS chiavi memorizzate in (SSE-KMS) AWS KMS

La crittografia lato server con AWS KMS chiavi (SSE-KMS) è simile a SSE-S3, ma con alcuni vantaggi e costi aggiuntivi per l'utilizzo di questo servizio. Esistono autorizzazioni separate per l'uso di una AWS KMS chiave che fornisce una protezione aggiuntiva contro l'accesso non autorizzato ai tuoi oggetti in Amazon S3. SSE-KMS fornisce anche una pista di controllo che mostra quando la AWS KMS chiave è stata utilizzata e da chi. Per ulteriori informazioni, vedere Utilizzo della crittografia lato server con (SSE-KMS). AWS Key Management Service

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 con una chiave KMS AWS gestita con l'alias aws/acm. Puoi visualizzare l'ID della chiave con questo alias nella console sotto chiavi gestite. AWS KMS AWS

VPC Lattice non accede direttamente alle 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 per la tua Managed Key con il prefisso AWS KMS aws/acm AWS . Una concessione è uno strumento politico che consente a TLS Connection Manager di utilizzare le chiavi KMS nelle operazioni crittografiche. La concessione consente al destinatario (TLS Connection Manager) di richiamare le operazioni di concessione specificate sulla 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 (sessione SSL/TLS) 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 con il comando utilizzando il. `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 aggiuntive sullo scopo per cui può 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, nella richiesta viene incluso 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 seguente 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 CloudTrailper 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**>>**. CloudTrail **`CreateGrant`**

Di seguito è riportato un esempio di record di eventi nella cronologia CloudTrail 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 si noterà che 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, vedere. ListGrants

Usa il seguente `ListGrants` comando AWS CLI per vedere i dettagli di tutte le sovvenzioni:

```
aws kms list-grants –key-id your-kms-key-id
```

Il risultato dovrebbe essere simile a questo 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'`ListGrants`esempio precedente si noterà che 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 evento in **>>** Cronologia eventi **>>**. CloudTrail **`Decrypt`**

Di seguito è riportato un esempio di record di CloudTrail eventi nella cronologia 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
- Policy basate sull'identità 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 che puoi utilizzare con Amazon VPC Lattice

Funzionalità IAM	Supporto VPC Lattice
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	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.

Policy basate sull'identità per VPC Lattice

Supporta le policy basate su identità	Sì

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

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica

all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Policy basate sulle risorse all'interno di VPC Lattice

Supporta le policy basate su risorse	Sì

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse.

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 ManagerÈ possibile utilizzare queste politiche basate sulle risorse per concedere l'autorizzazione di utilizzo ad altri account o organizzazioni per consentire la condivisione delle risorse. AWS Per ulteriori informazioni, consulta Condividi le tue risorse 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 singola istruzione, separale con virgole, come segue:

```
"Action": [ "vpc-lattice:action1", "vpc-lattice:action2" ]
```

Puoi anche specificare più operazioni tramite caratteri jolly. Ad esempio, è possibile specificare tutte le azioni i cui nomi iniziano con la parola`Get`, nel modo seguente:

```
"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 di 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 testo in *`corsivo con le informazioni specifiche`* della risorsa.

- Abbonamenti ai registri di accesso:

```
"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"
```

- 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 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. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

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

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

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome

utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

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

Per visualizzare un elenco delle chiavi di condizione di 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.

Controllo degli accessi basato sugli attributi (ABAC) con VPC Lattice

Supporta ABAC (tag nelle policy)	Sì

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

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

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

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

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

Utilizzo di credenziali temporanee con VPC Lattice

Supporta le credenziali temporanee	Sì

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

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

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

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 Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella 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.

Ruoli collegati ai servizi 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 per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni 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.

`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`

Policy basate sull'identità per Amazon VPC Lattice

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

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

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

Per 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
- Esempi di policy basate sull'identità per VPC Lattice

Best practice per le policy

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

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

utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

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

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

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`

```
{
    "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.

Esempi di policy basate sull'identità per VPC Lattice

Argomenti

- Gestisci le associazioni VPC a una rete di servizi
- Creare associazioni di servizi su una rete di servizi
- Aggiunge tag a risorse
- Creazione di un ruolo collegato ai servizi

Gestisci le 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.

```
{
   "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"
            }
         }
```

```
      }
   ]
}
```

Creare associazioni di servizi su 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

```
{
   "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"
         ]
      }
   ]
}
```

Aggiunge tag a risorse

L'esempio seguente mostra una politica che offre agli utenti con questa politica il permesso di creare tag sulle risorse VPC Lattice.

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

```
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:TagResource"
         ],
         "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/*"
      }
   ]
}
```

Creazione di un ruolo collegato ai servizi

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

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.

```
{
   "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"
            }
         }
      }
   ]
}
```

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 Utilizzo di ruoli collegati a servizi nella Guida per l'utente di IAM .

Autorizzazioni di ruolo collegate ai servizi per VPC Lattice

VPC Lattice utilizza il ruolo collegato al servizio denominato. AWSServiceRoleForVpcLattice

Il ruolo AWSServiceRoleForVpcLatticecollegato al servizio si affida al seguente servizio per l'assunzione del ruolo:

- `vpc-lattice.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AWSVpcLatticeServiceRolePolicy` consente a VPC Lattice di CloudWatch pubblicare metriche nel namespace. `AWS/VpcLattice`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/VpcLattice"
                }
            }
        }
    ]
}
```

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

Creazione di un ruolo collegato ai servizi per 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 ai servizi, puoi 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 di un ruolo collegato ai servizi per VPC Lattice

È possibile modificare la descrizione dell'utilizzo di IAM. AWSServiceRoleForVpcLattice Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di 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 informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di 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 AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

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

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

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

AWS policy gestita: VPC LatticeFullAccess

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'ARN del certificato SSL/TLS 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: recupera informazioni sulle istanze EC2 e sui VPC per creare gruppi target e registrarli.
- 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 S3: recupera informazioni sui bucket S3 utilizzati per archiviare i log di accesso.

Per visualizzare le autorizzazioni per questa politica, consulta LatticeFullAccessVPC nel Managed Policy AWS Reference.

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. Per ulteriori informazioni, consulta Autorizzazioni aggiuntive richieste per l'accesso completo.

AWS policy gestita: VPC LatticeReadOnlyAccess

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'ARN del certificato SSL/TLS 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 S3: recupera informazioni sui bucket S3 per la consegna dei log di accesso.

Per visualizzare le autorizzazioni per questa politica, consulta LatticeReadOnlyAccessVPC nel Managed Policy AWS Reference.

AWS policy gestita: VPC LatticeServicesInvokeAccess

Questa policy fornisce l'accesso per richiamare i servizi Amazon VPC Lattice.

Per visualizzare le autorizzazioni per questa politica, consulta LatticeServicesInvokeAccessVPC nel Managed Policy AWS Reference.

AWS politica gestita: AWSVpcLatticeServiceRolePolicy

Questa policy è associata a un ruolo collegato al servizio denominato AWSServiceRoleForVpcLatticeper 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 visualizzare le autorizzazioni per questa politica, consulta il Managed Policy Reference AWSVpcLatticeServiceRolePolicy.AWS

VPC Lattice si aggiorna alle policy gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per VPC Lattice da quando questo servizio ha iniziato a tracciare queste modifiche. Per avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS per la VPC Lattice User Guide.

Modifica	Descrizione	Data
VPC LatticeFullAccess	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 LatticeReadOnlyAccess	VPC Lattice aggiunge una nuova policy per concedere le autorizza zioni per l'accesso in sola lettura ad Amazon VPC Lattice e l'accesso limitato ad altri servizi dipendenti.	31 marzo 2023
VPC LatticeServicesInvokeAccess	VPC Lattice aggiunge una nuova policy per concedere l'accesso per richiamare i servizi Amazon VPC Lattice.	31 marzo 2023
AWSVpcLatticeServiceRolePolicy	VPC Lattice aggiunge le autorizza zioni 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. `AWSVpcLatticeServiceRolePolicy` CloudWatch PutMetricData Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon VPC Lattice.	5 dicembre 2022

Modifica	Descrizione	Data
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

I revisori di terze parti 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. AWS fornisce le seguenti risorse per contribuire alla conformità:

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

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

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.

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

Accedi ad Amazon VPC Lattice utilizzando gli endpoint dell'interfaccia () 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. AWS 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 CLIPer 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, puoi 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 cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

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

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 i CloudWatch parametri 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

Potresti voler monitorare le `HTTP code` `RequestTime` metriche per i gruppi target. Puoi filtrare queste metriche per Zona di disponibilità (AZ) per determinare in quale AZ si trova il gruppo target.

Parametro	Descrizione
`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.

Parametro	Descrizione
	Frequenza di segnalazione • Una volta al minuto Statistiche • La statistica più utile è`Sum`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.
`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 Statistiche • La statistica più utile è`Sum`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`HTTP1_ConnectionCount`	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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome: `TargetGroup` , Valore: Il nome del gruppo target. • Nome: `AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`TotalSentConnectionBytes`	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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`RequestTime`	Tempo di richiesta in millisecondi. 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). Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`TLSConnectionErrorCount`	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`. Dimensioni • Nome: `TargetGroup` , Valore: Il nome del gruppo target. • Nome: `AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`TotalTLSConnection HandshakeCount`	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`. Dimensioni • Nome:`TargetGroup` , Valore: Il nome del gruppo target. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

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

Potresti voler monitorare `HTTP code` e `RequestTime` misurare i servizi. Puoi filtrare queste metriche in base alla zona di disponibilità (AZ) per determinare in quale zona si trova il servizio.

Parametro	Descrizione
`RequestTimeoutCount`	Richieste totali scadute in attesa di una risposta. Criteri per la creazione di report

Parametro	Descrizione
	• 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`. Dimensioni • Nome:`Service`, Valore: l'ID del servizio. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`Service`, Valore: l'ID del servizio. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`RequestTime`	Tempo di richiesta in millisecondi. 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). Dimensioni • Nome:`Service`, Valore: l'ID del servizio. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Parametro	Descrizione
`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`. Dimensioni • Nome:`Service`, Valore: l'ID del servizio. • Nome:`AvailabilityZone` , Valore: L'AZ in cui si trova il gruppo target.

Log di accesso per Amazon VPC Lattice

I log di accesso acquisiscono informazioni dettagliate sui tuoi servizi VPC Lattice. Puoi utilizzare questi log di accesso per analizzare i modelli di traffico e controllare tutti i servizi della rete.

I registri 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
- Accedere al contenuto del registro
- 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.

```
{
    "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 inviati alla CloudWatch sezione Log Groups nella console. CloudWatch Per ulteriori informazioni, consulta Visualizza i dati di registro inviati ai CloudWatch registri nella Amazon CloudWatch User Guide.

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 al massimo e che 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
```

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 o per un servizio durante la creazione. È inoltre possibile abilitare i log di accesso dopo aver creato una rete o un servizio di assistenza, come descritto nella procedura seguente.

Per creare un servizio di base utilizzando la console

1. Apri alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Seleziona la rete o il servizio di assistenza.
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. Seleziona Salvataggio delle modifiche.

Abilita i log di accesso utilizzando il AWS CLI

Utilizza il comando CLI create-access-log-subscriptionper abilitare i log di accesso per reti o servizi di servizio.

Accedere al contenuto del registro

La seguente tabella descrive i campi di una voce di un log di accesso.

Campo	Descrizione	Formato
`hostHeader`	L'intestazione dell'autorità della richiesta.	string
`sslCipher`	Il nome OpenSSL per il set di cifrari utilizzati per stabilire la connessione TLS del client.	string
`serviceNetworkArn`	La rete di assistenza ARN.	*arn:aws:vpc-lattic e: region: account:s ervicenetwork/ id*
`resolvedUser`	L'ARN dell'utente quando l'autenticazione è abilitata e l'autenticazione è stata effettuata.	null | ARN | «Anonimo» | «Sconosciuto»

Campo	Descrizione	Formato
`authDeniedReason`	Il motivo per cui l'accesso viene negato quando l'autenticazione è abilitata.	null | «Servizio» | «Rete» | «Identità»
`requestMethod`	L'intestazione del metodo della richiesta.	string
`targetGroupArn`	Il gruppo di host di destinazione a cui appartiene l'host di destinazione.	string
`tlsVersion`	La versione TLS.	*`TLSv x`*
`userAgent`	L'intestazione user-agent.	string
`ServerNameIndication`	[Solo HTTPS] Il valore impostato sul socket di connessione ssl per Server Name Indication (SNI).	string
`destinationVpcId`	L'ID VPC di destinazione.	*`vpc- xxxxxxxx`*
`sourceIpPort`	L'indirizzo IP e la porta della sorgente.	*`ip: porta`*
`targetIpPort`	L'indirizzo IP e la porta della destinazione.	*`ip`*: *`porta`*
`serviceArn`	Il servizio ARN.	*`arn:aws:vpc-lattice: region: account:service/ id`*
`sourceVpcId`	L'ID VPC di origine.	*`vpc- xxxxxxxx`*
`requestPath`	Il percorso della richiesta.	LatticePath? : *`percorso`*
`startTime`	L'ora di inizio della richiesta.	*`YYYY - MM - DA GG A A HH: MM: SS Z`*

Campo	Descrizione	Formato
`protocol`	Il protocollo. Attualmente HTTP/1.1 o HTTP/2.	string
`responseCode`	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.	integer
`bytesReceived`	I byte del corpo e dell'intestazione ricevuti.	integer
`bytesSent`	I byte del corpo e dell'intestazione inviati.	integer
`duration`	Durata totale in millisecondi della richiesta dall'ora di inizio all'ultimo byte in uscita.	integer
`requestToTargetDuration`	Durata totale in millisecondi della richiesta dall'ora di inizio all'ultimo byte inviato alla destinazione.	integer
`responseFromTargetDuration`	Durata totale in millisecondi della richiesta dal primo byte letto dall'host di destinazione all'ultimo byte inviato al client.	integer
`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.	integer

Campo	Descrizione	Formato
`callerPrincipal`	Il principale autenticato.	string
`callerX509SubjectCN`	Il nome del soggetto (CN).	string
`callerX509IssuerOU`	L'emittente (OU).	string
`callerX509SANNameCN`	L'alternativa all'emittente (nome/CN).	string
`callerX509SANDNS`	Il nome alternativo del soggetto (DNS).	string
`callerX509SANURI`	Il nome alternativo dell'oggetto (URI).	string
`sourceVpcArn`	L'ARN del VPC da cui ha avuto origine la richiesta.	*arn:aws:ec2: region: account:vpc/ id*

Esempio

Nell'esempio seguente viene mostrata una voce di log.


```
{
    "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
}
```

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

AWS CloudTrail è un AWS servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio. CloudTrail acquisisce le chiamate API per VPC Lattice come eventi. CloudTrail è abilitato sul tuo Account AWS quando lo crei. Quando si verifica un'attività in VPC Lattice, tale attività viene registrata come CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Le chiamate acquisite includono chiamate dalla console VPC Lattice e chiamate in codice alle operazioni dell'API VPC Lattice. Per ulteriori informazioni in merito CloudTrail, consulta la Guida per l'utente.AWS CloudTrail

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

Per monitorare azioni aggiuntive, utilizza i log di accesso. Per ulteriori informazioni, consulta Log di accesso.

Comprendi le voci dei file di registro VPC Lattice

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

Per informazioni relative alle coppie chiave-valore nei log, consultate il contenuto dei CloudTrail record nella Guida per l'utente.AWS CloudTrail

Di seguito è riportato un esempio di voce di registro per una chiamata all'CreateServiceazione API.

```
{
  "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"
}
```


Di seguito è riportato un esempio di voce di registro per una chiamata all'azione DeleteServiceAPI.

```
{
  "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"
}
```

Quote per Amazon VPC Lattice

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWSSalvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare le quote per VPC Lattice, apri la console Service Quotas. Nel pannello di navigazione, scegli Servizi AWSe seleziona VPC Lattice.

Per richiedere un aumento della quota, contatta l' AWS assistenza o consulta la sezione Richiesta di aumento della quota nella Service Quotas User Guide.

Hai Account AWS le seguenti quote relative a VPC Lattice.

Nome	Predefinita	Adattabile	Descrizione
Dimensioni della politica di autenticazione	Ogni regione supportata: 10 KB	No	La dimensione massima di un file JSON in una politica di autenticazione.
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.
Regole per ascoltatore	Ogni regione supportata: 5	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.

Nome	Predefinita	Adatta e	Descrizione
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: 10	Sì	Il numero massimo di reti di servizi per regione. Per ulteriori aumenti della capacità e dei limiti, contatta l' AWS assistenza.
Servizi per regione	Ogni regione supportata: 500	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.

Nome	Predefinita	Adatta e	Descrizione
Gruppi di destinazione per servizio	Ogni regione supportata: 5	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.
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.

Si applicano anche i seguenti limiti.

Limite	Valore
Larghezza di banda per servizio per zona di disponibilità	10 Gb/s
Unità di trasmissione massima (MTU) per connessione	8500 byte
Richieste al secondo per servizio per zona di disponibilità	10.000

Cronologia dei documenti per la Amazon VPC Lattice User Guide

La tabella seguente descrive le versioni della documentazione per VPC Lattice.

Modifica	Descrizione	Data
Passthrough TLS	VPC Lattice ora supporta il passthrough TLS, che consente di eseguire la terminazione TLS nell'appl icazione 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 VPC condivisi	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
Supporto IPv6	VPC Lattice ora supporta sia i gruppi target IP IPv4 che IPv6.	27 marzo 2023
Versione del protocollo HTTP2 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 del listener	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 di un certificato SSL/TLS in ACM per nomi di dominio personalizzati.	14 febbraio 2023
VPC Lattice ora riporta un elenco aggiornato di tipi di istanze non supportati	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.