



Guia do usuário

Amazon VPC Lattice



Amazon VPC Lattice: Guia do usuário

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon VPC Lattice?	1
Componentes principais	1
Perfis e responsabilidades	4
Atributos	5
Como acessar o VPC Lattice	7
Endpoints de serviço VPC Lattice	7
IPv4 endpoints	7
Endpoints Dualstack (IPv4 e) IPv6	8
Especificar endpoints	8
Preços	9
Funcionamento do VPC Lattice	10
Redes de serviços	14
Criar uma rede de serviços	15
Gerenciar associações	18
Gerenciar associações de serviços	18
Gerenciar associações de configuração de recursos	19
Gerenciar associações de VPC	20
Gerencie associações de endpoints de VPC	21
Editar configurações de acesso	22
Editar detalhes de monitoramento	24
Gerenciar tags	25
Excluir uma rede de serviços	25
Serviços	27
Etapa 1: criar um serviço do VPC Lattice	28
Etapa 2: definir o roteamento	29
Etapa 3: criar associações de rede	30
Etapa 4: revisar e criar	31
Gerenciar associações	31
Editar configurações de acesso	32
Editar detalhes de monitoramento	33
Gerenciar tags	34
Configurar um nome de domínio personalizado	35
Associe um nome de domínio personalizado ao seu serviço	37
BYOC	39

Como proteger a chave privada do seu certificado	41
Excluir um serviço	41
Grupos de destino	43
Criar um grupo de destino	44
Criar um grupo de destino	44
Sub-redes compartilhadas	47
Registrar destinos	47
Instância IDs	48
Endereços IP	49
Funções do Lambda	49
Application Load Balancers	50
Configurar verificações de integridade	50
Configurações de verificação de integridade	51
Verificar a integridade de seus destinos	53
Modificar as configurações de verificação de integridade	54
Configuração de roteamento	54
Algoritmo de roteamento	55
Target type	55
Tipo de endereço IP	57
Destinos HTTP	57
Cabeçalhos x-forwarded	57
Cabeçalhos de identidade do chamador	58
Funções do Lambda como destinos	59
Preparar a função do Lambda	59
Criar um grupo de destino para a função do Lambda	49
Receba eventos do serviço VPC Lattice	61
Responder ao serviço VPC Lattice	64
Cabeçalhos de vários valores	65
parâmetros de string de consulta	65
Cancelar o registro da função do Lambda	66
Application Load Balancers como destinos	66
Pré-requisitos	67
Etapa 1: criar um grupo de destino do tipo ALB	67
Etapa 2: registrar o Application Load Balancer como destino	68
Versão do protocolo	69
Atualizar tags	70

Excluir um grupo de destino	71
Listeners	72
Configuração do receptor	72
Receptores HTTPS	73
Pré-requisitos	73
Adicionar um receptor HTTP	73
Listeners HTTPS	75
Política de segurança	76
Política de ALPN	76
Adicionar um receptor HTTPS	77
ouvintes TLS	79
Considerações	79
Adicionar um listener TLS	80
Regras do listener	81
Regras padrão	81
Prioridade das regras	81
Ação da regra	81
Condições de regra	82
Adicionar uma regra	83
Atualizar uma regra	84
Excluir uma regra	84
Excluir um listener	85
Recursos da VPC	86
Gateways de recursos	86
Considerações	87
Grupos de segurança	87
Tipos de endereço IP	88
Crie um gateway de recursos	88
Excluir um gateway de recursos	89
Configurações de recursos	90
Tipos de configurações de recursos	90
Gateway de recursos	86
Definição de recurso	91
Protocolo	92
Intervalos de portas	92
Acesso a recursos da	92

Associação com o tipo de rede de serviços	93
Tipos de redes de serviços	93
Compartilhando configurações de recursos por meio de AWS RAM	94
Monitoramento	94
Criar uma configuração de recursos	94
Gerenciar associações	95
Compartilhe entidades do VPC Lattice	98
Pré-requisitos	98
Compartilhar entidades	99
Pare de compartilhar entidades	100
Responsabilidades e permissões	101
Proprietários da entidade	101
Consumidores individuais	102
Eventos entre contas	103
Estrutura de VPC para Oracle Database@AWS	107
Considerações	107
Backup gerenciado do Oracle Cloud Infrastructure (OCI) para o Amazon S3	109
Acesso do Amazon S3	110
Considerações	110
Habilite a integração gerenciada do Amazon S3 Access	110
Acesso seguro com uma política de autenticação	110
Acesse e compartilhe entidades do VPC Lattice	111
Acesse os serviços e recursos do VPC Lattice	111
Compartilhe sua rede ODB por meio do VPC Lattice	112
Segurança	113
Gerenciar o acesso aos serviços	114
Políticas de autenticação	115
Grupos de segurança	130
Rede ACLs	136
Solicitações autenticadas	138
Proteção de dados	157
Criptografia em trânsito	157
Criptografia inativa	158
Gerenciamento de identidade e acesso	164
Funcionamento do Amazon VPC Lattice com o IAM	165
Permissões de API	171

Políticas baseadas em identidade	174
Uso de perfis vinculados ao serviço	180
AWS políticas gerenciadas	182
Validação de conformidade	185
Acesse de forma privada o Lattice APIs	187
Considerações sobre endpoints da VPC de interface	187
Como criar um endpoint da VPC de interface para o VPC Lattice	187
Resiliência	187
Segurança da infraestrutura	188
Monitoramento	189
CloudWatch métricas	189
Visualizar as CloudWatch métricas da Amazon	189
Métricas do grupo de destino	190
Métricas de serviço	197
Logs de acesso	199
Permissões do IAM necessárias para habilitar os logs de acesso	200
Destinos de logs de acesso	201
Habilitar logs de acesso	202
Conteúdo dos logs de acesso	203
Conteúdo do log de acesso a recursos	207
Solucionar problemas de logs de acesso	209
CloudTrail troncos	210
Eventos de gerenciamento do VPC Lattice em CloudTrail	212
Exemplos de eventos do VPC Lattice	212
Cotas	215
Histórico de documentos	221
.....	ccxxiv

O que é o Amazon VPC Lattice?

O Amazon VPC Lattice é um serviço de rede de aplicativos totalmente gerenciado que você usa para conectar, proteger e monitorar os serviços e recursos do seu aplicativo. Você pode usar o VPC Lattice com uma única nuvem privada virtual (VPC) ou em várias VPCs de uma ou mais contas.

Os aplicativos modernos podem consistir em vários componentes pequenos e modulares, geralmente chamados de microsserviços, como uma API HTTP, recursos como bancos de dados e recursos personalizados que consistem em endpoints de endereço IP e DNS. Embora a modernização tenha suas vantagens, ela também pode introduzir complexidades e desafios de rede quando você conecta esses microsserviços e recursos. Por exemplo, se os desenvolvedores estiverem espalhados por equipes diferentes, eles poderão criar e implantar microsserviços e recursos em várias contas ou VPCs.

No VPC Lattice, nos referimos a um microsserviço como um serviço e representamos um recurso somente como uma configuração de recurso. Esses são os termos que você vê no guia do usuário do VPC Lattice.

Conteúdo

- [Componentes principais](#)
- [Perfis e responsabilidades](#)
- [Atributos](#)
- [Como acessar o VPC Lattice](#)
- [Endpoints de serviço VPC Lattice](#)
- [Preços](#)

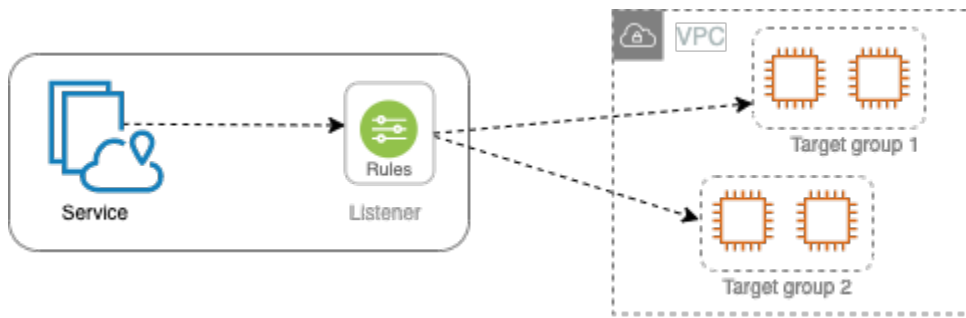
Componentes principais

Para usar o Amazon VPC Lattice, é necessário que você esteja familiarizado com seus principais componentes.

Serviço

Uma unidade de software implantável de maneira independente que fornece uma tarefa ou função específica. Um serviço pode ser executado em EC2 instâncias ou ECS/EKS/Fargate

contêineres, ou como funções Lambda, em uma conta ou em uma nuvem privada virtual (VPC). Um serviço VPC Lattice tem os seguintes componentes: grupos de destino, receptores e regras.



Grupo de destino

Uma coleção de recursos, também conhecidos como destinos, que executam sua aplicação ou serviço. Eles são semelhantes aos grupos de destino fornecidos pelo Elastic Load Balancing, mas não são intercambiáveis. Os tipos de destino compatíveis incluem EC2 instâncias, endereços IP, funções Lambda, Application Load Balancers, tarefas do Amazon ECS e Kubernetes Pods.

Receptor

Um processo que verifica as solicitações de conexão e as encaminha para destinos em um grupo de destino. Você configura um ouvinte com um protocolo e um número de porta.

Regra

Um componente padrão de um receptor que encaminha solicitações para os destinos em um grupo de destinos do VPC Lattice. Cada regra consiste em uma prioridade, uma ou mais ações e uma ou mais condições. As regras determinam como o receptor encaminha as solicitações do cliente.

Recurso

Um recurso é uma entidade como um banco de dados do Amazon Relational Database Service (Amazon RDS), uma instância da EC2 Amazon, um endpoint de aplicativo, um destino de nome de domínio ou um endereço IP. Você pode compartilhar um recurso em sua VPC criando um compartilhamento de recursos em AWS Resource Access Manager (AWS RAM), criando um gateway de recursos e definindo uma configuração de recursos.

Gateway de recursos

Um gateway de recursos é um ponto de entrada na VPC em que os recursos residem.

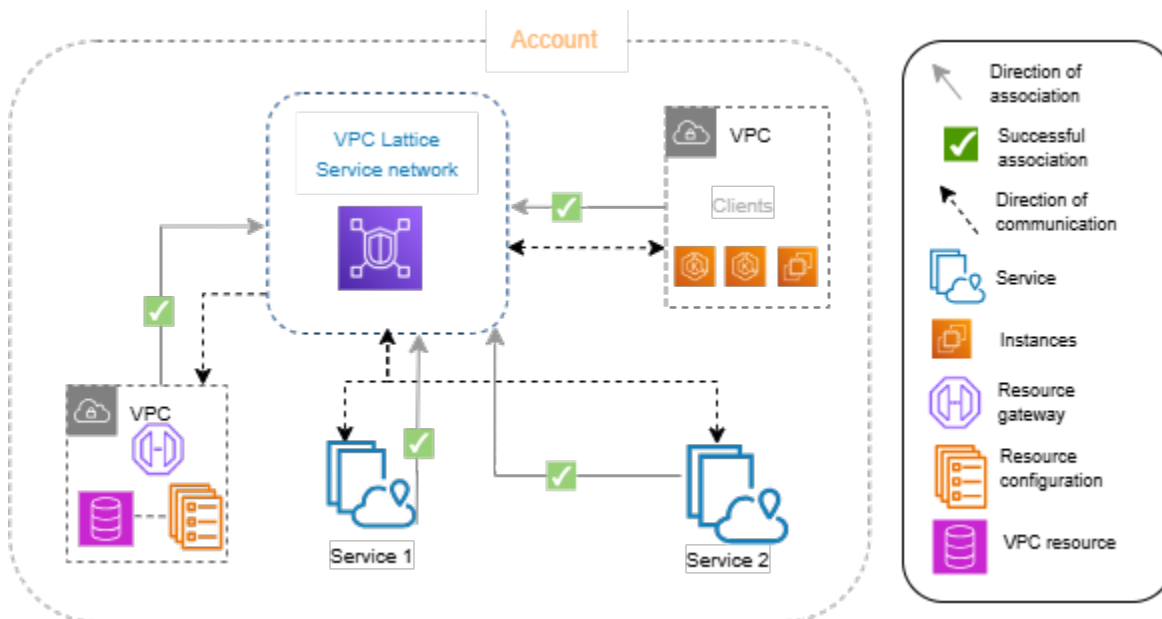
Configuração de recursos

Uma configuração de recurso é um objeto lógico que representa um único recurso ou um grupo de recursos. Um recurso pode ser um endereço IP, um destino de nome de domínio ou um banco de dados do Amazon RDS.

Rede de serviços

Um limite lógico para uma coleção de configurações de serviços e recursos. Um cliente pode estar em uma VPC associada à rede de serviços. Clientes e serviços associados à mesma rede de serviços podem se comunicar entre eles se estiverem autorizados a fazer isso.

Na figura a seguir, os clientes podem se comunicar com os dois serviços, porque a VPC e os serviços estão associados à mesma rede de serviços.



Diretório de serviços

Um registro central de todos os serviços do VPC Lattice que você possui ou por meio dos quais são compartilhados com sua conta. AWS RAM

Políticas de autenticação

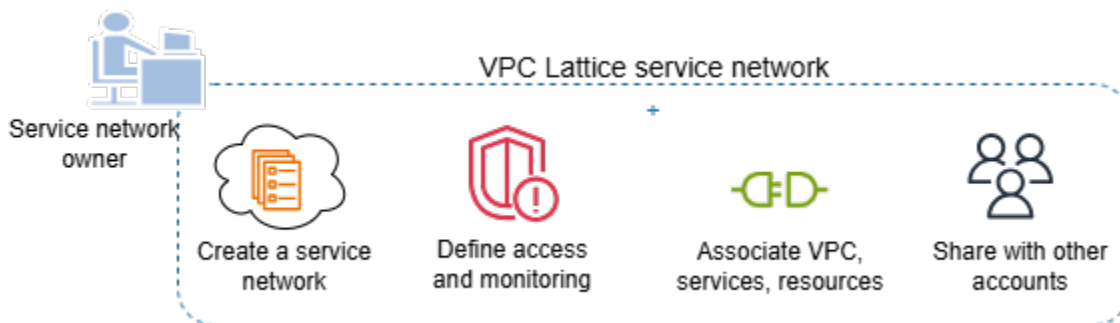
Políticas de autorização refinadas que podem ser usadas para definir o acesso aos serviços. Você pode anexar políticas de autenticação distintas a serviços individuais ou à rede de serviços. Por exemplo, você pode criar uma política de como um serviço de pagamento executado em um grupo de EC2 instâncias de auto scaling deve interagir com um serviço de faturamento em execução. AWS Lambda

As políticas de autenticação não são suportadas nas configurações de recursos. As políticas de autenticação de uma rede de serviços não são aplicáveis às configurações de recursos na rede de serviços.

Perfis e responsabilidades

Um perfil determina quem é responsável pela configuração e pelo fluxo de informações no Amazon VPC Lattice. Normalmente, há dois perfis, proprietário da rede de serviços e proprietário do serviço, e suas responsabilidades podem se sobrepor.

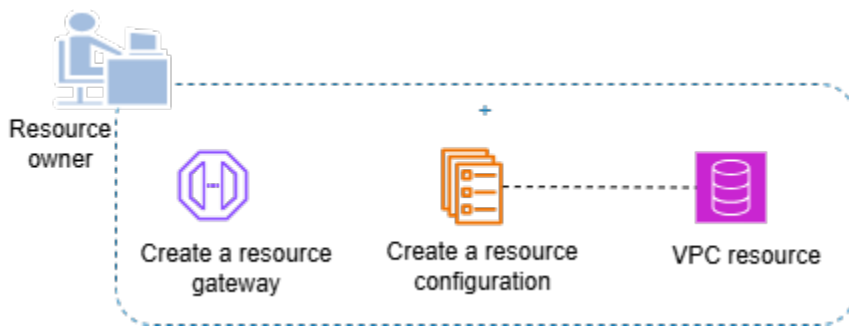
Proprietário da rede de serviços: em geral, o proprietário da rede de serviços é o administrador da rede ou o administrador da nuvem em uma organização. Os proprietários da rede de serviços criam, compartilham e provisionam a rede de serviços. Eles também gerenciam quem pode acessar a rede de serviços ou os serviços no VPC Lattice. O proprietário da rede de serviços pode definir configurações de acesso gerais para os serviços associados à rede de serviços. Esses controles são usados para gerenciar a comunicação entre clientes e serviços usando políticas de autenticação e autorização. O proprietário da rede de serviços também pode associar uma configuração de serviço ou recurso a uma ou várias redes de serviços, se a configuração do serviço ou recurso for compartilhada com a conta do proprietário da rede de serviços.



Proprietário do serviço — O proprietário do serviço geralmente é um desenvolvedor de software em uma organização. Os proprietários de serviço criam serviços no VPC Lattice, definem regras de roteamento e também associam serviços à rede de serviços. Eles também podem definir configurações de acesso refinadas, que podem restringir o acesso somente a serviços e clientes autenticados e autorizados.



Proprietário do recurso — O proprietário do recurso geralmente é um desenvolvedor de software em uma organização e atua como administrador de um recurso, como um banco de dados. O proprietário do recurso cria uma configuração de recurso para o recurso, define as configurações de acesso para a configuração do recurso e associa a configuração do recurso às redes de serviços.



Atributos

Veja a seguir os principais recursos que o VPC Lattice fornece.

Descoberta de serviço

Todos os clientes e serviços VPCs associados à rede de serviços podem se comunicar com outros serviços dentro da mesma rede de serviços. Direcionamentos client-to-service e service-to-service tráfego de DNS por meio do endpoint VPC Lattice. Quando um cliente deseja enviar uma solicitação para um serviço, ele usa o nome de DNS do serviço. O Route 53 Resolver envia o tráfego para o VPC Lattice, que então identifica o serviço de destino.

Conectividade

Client-to-service e a client-to-resource conectividade é estabelecida dentro da infraestrutura AWS de rede. Quando você associa uma VPC à rede de serviços, qualquer cliente dentro da VPC pode se conectar com serviços e recursos (por meio de configurações de recursos) na rede

de serviços, se tiver o acesso necessário. O VPC Lattice oferece suporte à tecnologia CIDR sobreposta.

Acesso no local

Você pode habilitar a conectividade com uma rede de serviços a partir de uma VPC usando um VPC endpoint (desenvolvido por). AWS PrivateLink Um endpoint VPC do tipo rede de serviços permite que você habilite o acesso a serviços e recursos na rede de serviços a partir de redes locais por meio do Direct Connect e da VPN. Tráfego que atravessa o emparelhamento de VPC ou que também AWS Transit Gateway pode acessar recursos e serviços por meio de um VPC endpoint.

Observabilidade

O VPC Lattice gera métricas e logs para cada solicitação e resposta que atravessa a rede de serviços, ajudando você a monitorar e solucionar problemas de aplicações. Por padrão, as métricas são publicadas na conta do proprietário do serviço. Proprietários de serviços e proprietários de recursos têm a opção de ativar o registro e receber registros de todos os clientes access/requests to their services and resources. Service network owners can also turn on logging on the service network, to log all access/requests nos VPCs serviços e recursos dos clientes conectados à rede de serviços.

O VPC Lattice trabalha com as seguintes ferramentas para ajudar você a monitorar e solucionar problemas em seus serviços: Amazon CloudWatch grupos de log, streams de entrega do Firehose e buckets Amazon S3.

Segurança

O VPC Lattice fornece uma estrutura que você pode usar para implementar uma estratégia de defesa em várias camadas da rede. A primeira camada é a combinação de serviço, configuração de recursos, associação de VPC e ponto de extremidade VPC do tipo rede de serviços. Sem uma VPC e uma associação de serviços ou um endpoint VPC do tipo rede de serviços, os clientes não podem acessar os serviços. Da mesma forma, sem uma VPC e uma configuração de recursos e uma associação de serviços ou um endpoint VPC do tipo rede de serviços, os clientes não podem acessar os recursos.

A segunda camada permite que os usuários anexem grupos de segurança à associação entre a VPC e a rede de serviços. A terceira e a quarta camadas são políticas de autenticação que podem ser aplicadas individualmente no nível da rede de serviços e no nível do serviço.

Como acessar o VPC Lattice

É possível criar, acessar e gerenciar o VPC Lattice usando qualquer uma das seguintes interfaces:

- AWS Management Console: fornece uma interface da Web que você pode usar para acessar o VPC Lattice.
- AWS Command Line Interface (AWS CLI) — Fornece comandos para um amplo conjunto de AWS serviços, incluindo o VPC Lattice. O AWS CLI é compatível com Windows, macOS e Linux. Para obter mais informações sobre a CLI, consulte [AWS Command Line Interface](#). Para obter mais informações sobre o APIs, consulte [Amazon VPC Lattice API Reference](#).
- VPC Lattice Controller para Kubernetes: "gerencia os recursos do VPC Lattice para um cluster Kubernetes. Para obter mais informações sobre como usar o VPC Lattice com o Kubernetes, consulte o [Guia do usuário do AWS Gateway API Controller](#).
- AWS CloudFormation: ajuda você a modelar e configurar os recursos da AWS . Para obter mais informações, consulte [Referência de tipo de recursos do Amazon VPC Lattice](#).

Endpoints de serviço VPC Lattice

Um endpoint é uma URL que serve como ponto de entrada para um serviço AWS web. O VPC Lattice é compatível com os seguintes tipos de endpoints:

- [the section called “IPv4 endpoints”](#)
- Endpoints [Dualstack \(suportam ambos\)](#) e IPv4 IPv6

Ao fazer uma solicitação, você pode especificar o endpoint a ser usado. Se você não especificar um endpoint, o IPv4 endpoint será usado por padrão. Para usar outro tipo de endpoint, você deve especificá-lo em sua solicitação. Para obter exemplos de como fazer isso, consulte [the section called “Especificar endpoints”](#). Para ver uma tabela de endpoints disponíveis, consulte os endpoints do [Amazon VPC Lattice](#).

IPv4 endpoints

IPv4 os endpoints oferecem suporte somente ao IPv4 tráfego. IPv4 os endpoints estão disponíveis para todas as regiões.

Se você especificar o endpoint geral, `vpc-lattice.amazonaws.com`, usaremos o endpoint para `us-east-1`. Para usar uma região diferente, especifique o endpoint associado a ela. Por exemplo,

se você especificar `vpc-lattice.us-east-2.amazonaws.com` como endpoint, direcionaremos sua solicitação para o endpoint `us-east-2`.

IPv4 os nomes de endpoints usam a seguinte convenção de nomenclatura:

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

Por exemplo, o nome do IPv4 endpoint para a `eu-west-1` região é `vpc-lattice.eu-west-1.amazonaws.com`.

Endpoints Dualstack (IPv4 e) IPv6

Os endpoints Dualstack oferecem suporte tanto ao tráfego quanto ao tráfego. IPv4 IPv6 Os endpoints Dualstack estão disponíveis para todas as regiões. Quando você faz uma solicitação para um endpoint dualstack, o URL do endpoint é resolvido para um IPv4 endereço IPv6 ou, dependendo do protocolo usado pela rede e pelo cliente.

Os nomes de endpoints de pilha dupla usam a seguinte convenção de nomenclatura:

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

Por exemplo, o nome do endpoint de pilha dupla para a região `eu-west-1` é `vpc-lattice.eu-west-1.api.aws`.

Especificar endpoints

Os exemplos a seguir mostram como especificar um endpoint para a `us-east-2` região usando o AWS CLI `forvpc-lattice`.

- IPv4

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

- Pilha dupla

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

Preços

No VPC Lattice, você paga pelo tempo que um serviço fica provisionado, pela quantidade de dados transferidos por cada serviço e pelo número de solicitações. Como proprietário do recurso, você paga pelos dados transferidos de e para cada recurso. Como proprietário da rede de serviços, você paga por hora pelas configurações de recursos associadas à sua rede de serviços. Como consumidor que tem uma VPC associada a uma rede de serviços, você paga pelos dados transferidos de e para os recursos na rede de serviços da sua VPC. Para obter mais informações, consulte [Preços do Amazon VPC Lattice](#).

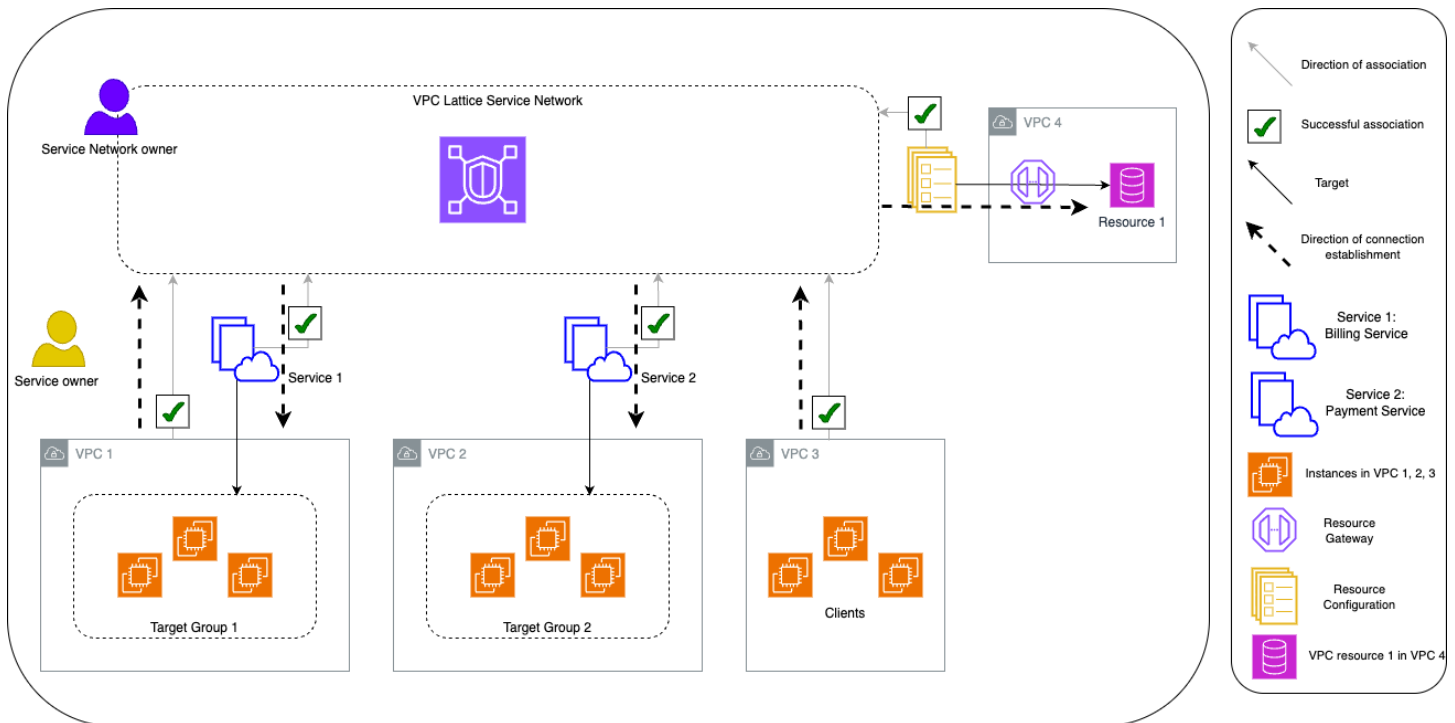
Funcionamento do VPC Lattice

O VPC Lattice foi projetado para ajudá-lo a descobrir, proteger, conectar e monitorar com facilidade e eficácia todos os serviços e recursos contidos nele. Cada componente do VPC Lattice se comunica unidirecionalmente ou bidirecionalmente dentro da rede de serviços com base em sua associação com a rede de serviços e suas configurações de acesso. As configurações de acesso são compostas pelas políticas de autenticação e autorização necessárias para essa comunicação.

O resumo a seguir descreve a comunicação entre componentes no VPC Lattice:

- Há duas maneiras pelas quais uma VPC pode ser conectada a uma rede de serviços: por meio de uma associação de VPC e por meio de um endpoint VPC do tipo rede de serviços.
- Os serviços e recursos associados à rede de serviços podem receber solicitações de clientes que também VPCs estejam conectados à rede de serviços.
- Um cliente pode enviar solicitações para serviços e recursos associados a uma rede de serviços somente se estiver em uma VPC conectada à mesma rede de serviços. O tráfego de clientes que atravessa uma conexão de emparelhamento de VPC, um gateway de trânsito, Direct Connect ou VPN só pode alcançar recursos e serviços se a VPC estiver conectada à rede de serviços por meio de um VPC endpoint.
- Os alvos dos serviços associados à rede de serviços também são clientes e podem enviar solicitações para outros serviços e recursos associados à rede de serviços. VPCs
- Os alvos dos serviços VPCs que não estão associados à rede de serviços não são clientes e não podem enviar solicitações para outros serviços e recursos associados à rede de serviços.
- Clientes VPCs que têm recursos, mas em que a VPC não está associada à rede de serviços, não são clientes e não podem enviar solicitações para outros serviços e recursos associados à rede de serviços.

O diagrama de fluxo a seguir usa um exemplo de cenário para explicar o fluxo de informações e a direção da comunicação entre os componentes no VPC Lattice. Há dois serviços associados a uma rede de serviços. Tanto os serviços quanto todos VPCs foram criados na mesma conta da rede de serviços. Ambos os serviços estão configurados para permitir o tráfego proveniente da rede de serviços.



O serviço 1 é uma aplicação de faturamento executada em um grupo de instâncias registrado com o grupo de destino 1 na VPC 1. O serviço 2 é uma aplicação de pagamento executada em um grupo de instâncias registrado no grupo de destino 2 na VPC 2. A VPC 3 está na mesma conta e tem clientes, mas não tem serviços. O recurso 1 é um banco de dados que tem dados de clientes na VPC 4.

A lista a seguir descreve, em ordem, o fluxo de trabalho habitual de tarefas do VPC Lattice.

1. Criar uma rede de serviços

O proprietário da rede de serviços cria a rede de serviços.

2. Criar um serviço

Os proprietários do serviço criam os respectivos serviços, serviço 1 e serviço 2. Durante a criação, o proprietário do serviço adiciona receptores e define regras para rotear solicitações para o grupo de destino de cada serviço.

3. Definir roteamento

Os proprietários do serviço criam o grupo de destino para cada serviço (grupo de destino 1 e grupo de destino 2). Eles fazem isso especificando as instâncias de destino nas quais os serviços são executados. Eles também especificam o local VPCs em que esses alvos residem.

No diagrama anterior, as setas sólidas representam o tráfego de roteamento de serviços para grupos-alvo e o roteamento de configurações de recursos para recursos.

4. Associar serviços à rede de serviços

O proprietário da rede de serviços ou o proprietário do serviço associa os serviços à rede de serviços. As associações são apresentadas como setas com marcas de verificação apontando para a rede de serviços com base no serviço. Quando você associa um serviço a uma rede de serviços, esse serviço se torna detectável para outros serviços associados à rede de serviços e clientes VPCs conectados à rede de serviços.

As setas tracejadas entre a rede de serviço e os grupos-alvo mostram a direção do estabelecimento da conexão. Os fluxos de tráfego de retorno para os clientes que usam a rede de serviços. As setas que representam o tráfego de retorno não estão incluídas neste diagrama.

5. Crie um gateway de recursos

O proprietário do recurso cria um gateway de recursos na VPC 4 para poder habilitar a conectividade dos clientes com o recurso 1.

6. Criar uma configuração de recursos

O proprietário do recurso cria uma configuração de recurso para representar o recurso 1 e especifica o gateway de recursos para o recurso 1.

7. Associar configurações de recursos à rede de serviços

O proprietário da rede de serviços ou o proprietário do recurso associa a configuração do recurso à rede de serviços. A associação é mostrada como uma seta com uma marca de seleção apontando para a rede de serviços a partir da configuração do recurso. Quando você associa uma configuração de recursos a uma rede de serviços, essa configuração de recursos se torna detectável para outros serviços associados à rede de serviços e clientes VPCs conectados à rede de serviços.

As setas tracejadas da rede de serviços até o recurso representam o recurso que recebe solicitações dos clientes. Os fluxos de tráfego de retorno para o cliente usando a rede de serviços. As setas que representam o tráfego de retorno não estão incluídas neste diagrama.

8. Conecte-se VPCs com a rede de serviços

VPCs pode ser conectado à rede de serviços de duas maneiras: associando a VPC à rede de serviços ou criando um VPC endpoint. Aqui, o proprietário da rede de serviços associa a VPC

1 e a VPC 3 à rede de serviços. As associações são mostradas usando setas com marcas de verificação apontadas para a rede de serviços. Com essas associações, todos os recursos na VPC podem atuar como clientes e fazer solicitações a serviços dentro da rede de serviços. As setas tracejadas entre a VPC 1 e a rede de serviços mostram a direção do estabelecimento da conexão. A rede de serviços só inicia conexões com recursos direcionados aos grupos-alvo do serviço 1. Qualquer recurso na VPC 1 pode atuar como cliente e iniciar conexões com os serviços e recursos da rede de serviços.

A VPC 2 não tem uma seta ou marca de seleção que represente uma associação. Isso significa que o proprietário da rede de serviços ou o proprietário do serviço não associou a VPC 2 à rede de serviços. Isso ocorre porque o serviço 2, neste exemplo, só precisa receber solicitações e enviar respostas usando a mesma solicitação. Em outras palavras, os destino do serviço 2 não são clientes e não precisam fazer solicitações para outros serviços na rede de serviços.

Da mesma forma, a VPC 4 não tem uma seta ou marca de seleção que represente uma associação. Isso significa que o proprietário da rede de serviços ou o proprietário do recurso não associou a VPC 4 à rede de serviços. Isso ocorre porque o recurso 1 só recebe solicitações e envia respostas usando a mesma solicitação. Ele não pode fazer solicitações para outros serviços e recursos na rede de serviços.

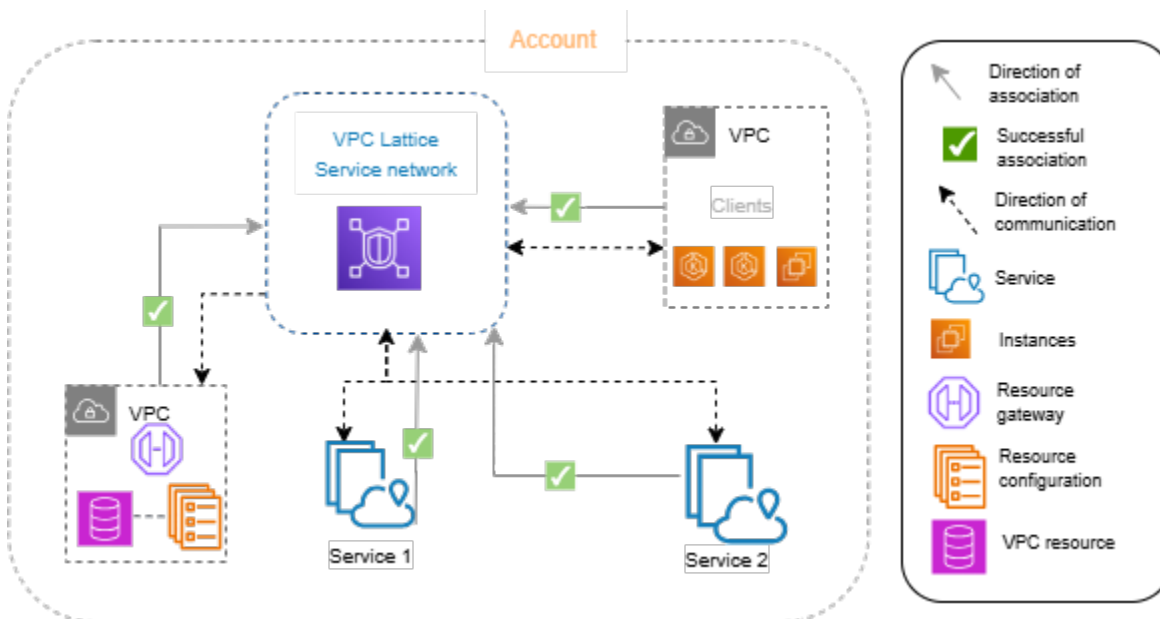
Em resumo, o diagrama de procedimentos mostrou os seguintes cenários:

- VPCs com conexões somente de entrada da VPC Lattice com seus recursos. A VPC 2 e a VPC 4 representam esses cenários.
- Uma VPC com conexões somente de saída de seus recursos para a VPC Lattice. O VPC 3 representa esse cenário.
- Uma VPC com conexões de entrada da VPC Lattice para seus recursos e com conexões de saída de seus recursos para a VPC Lattice. O VPC 1 representa esse cenário.

Redes de serviços no VPC Lattice

Uma rede de serviços é um limite lógico para uma coleção de serviços e configurações de recursos. As configurações de serviços e recursos associados à rede podem ser autorizadas para descoberta, conectividade, acessibilidade e observabilidade. Para fazer solicitações a serviços e configurações de recursos na rede, seu serviço ou cliente deve estar em uma VPC conectada à rede de serviços por meio de uma associação ou por meio de um VPC endpoint.

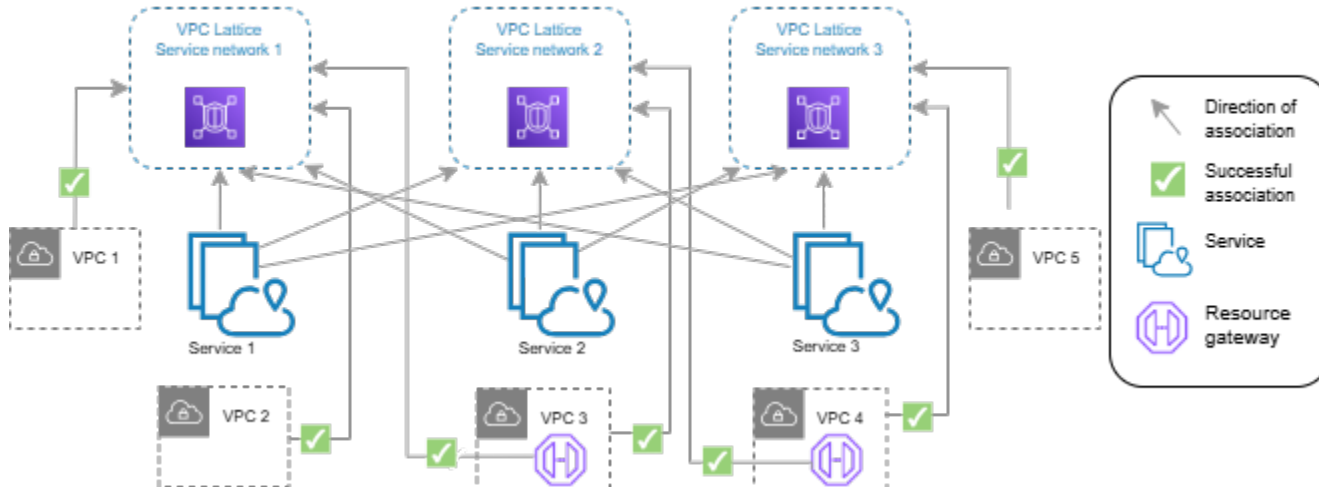
O diagrama a seguir mostra os principais componentes de uma rede de serviços do Amazon VPC Lattice. As marcas de verificação nas setas indicam que os serviços e a VPC estão associados à rede de serviços. Os clientes na VPC associada à rede de serviços podem se comunicar com os dois serviços por meio da rede de serviços.



Você pode associar um ou mais serviços e configurações de recursos a várias redes de serviços. Você também pode conectar vários VPCs com uma rede de serviços. Você pode conectar uma VPC a apenas uma rede de serviços por meio de uma associação. Para conectar uma VPC a várias redes de serviços, você pode usar endpoints VPC do tipo service network. [Para obter mais informações sobre VPC endpoints do tipo service network, consulte o guia do AWS PrivateLink usuário.](#)

No diagrama a seguir, as setas representam as associações entre serviços e redes de serviços, bem como as associações entre as redes VPCs de serviços. Você pode ver que vários serviços estão associados a várias redes de serviços e vários VPCs estão associados a cada rede de serviços. Cada VPC tem exatamente uma associação com uma rede de serviços. No entanto, a VPC 3 e a VPC 4 se conectam a duas redes de serviços. A VPC 3 se conecta à rede de serviços 1 por meio de

um VPC endpoint. Da mesma forma, a VPC 4 se conecta à rede de serviços 2 por meio de um VPC endpoint.



Para obter mais informações, consulte [Cotas do Amazon VPC Lattice](#).

Conteúdo

- [Crie uma rede de serviços VPC Lattice](#)
- [Gerencie as associações para uma rede de serviços VPC Lattice](#)
- [Editar configurações de acesso para uma rede de serviços VPC Lattice](#)
- [Editar detalhes de monitoramento de uma rede de serviços VPC Lattice](#)
- [Gerenciar tags para uma rede de serviços VPC Lattice](#)
- [Excluir uma rede de serviços VPC Lattice](#)

Crie uma rede de serviços VPC Lattice

Use o console para criar uma rede de serviços e, opcionalmente, configurá-la com serviços, associações, configurações de acesso e logs de acesso.

Para criar uma rede de serviços usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Escolha Criar rede de serviços.

4. Em Identificadores, insira um nome, uma descrição opcional e tags opcionais. O nome deve ter entre 3 e 63 caracteres. É possível usar letras minúsculas, números e hifens. O nome deve começar e terminar com uma letra ou um número. Não use hifens consecutivos. A descrição pode ter até 256 caracteres. Para adicionar uma tag, escolha Adicionar nova tag e especifique uma chave e o valor da tag.
5. (Opcional) Para associar um serviço, escolha o serviço em Associações de serviços, Serviços. A lista inclui serviços que estão em sua conta e quaisquer serviços compartilhados com você de uma conta diferente. Se não houver nenhum serviço na lista, você poderá criar um serviço escolhendo Criar um serviço VPC Lattice.

Como alternativa, para associar um serviço após ter criado a rede de serviços, consulte [the section called “Gerenciar associações de serviços”](#).

6. (Opcional) Para associar uma configuração de recursos, escolha o serviço de configuração de recursos em Associações de configuração de recursos, Configuração de recursos. A lista inclui configurações de recursos que estão na sua conta e todas as configurações de recursos que são compartilhadas com você de uma conta diferente. Se não houver nenhuma configuração de recurso na lista, você pode criar uma configuração de recursos escolhendo Criar uma configuração de recurso do Amazon VPC Lattice.

Como alternativa, para associar uma configuração de recurso depois de criar a rede de serviços, consulte [the section called “Gerenciar associações de configuração de recursos”](#).

7. (Opcional) Para associar uma VPC, escolha Adicionar associação à VPC. Selecione a VPC a ser associada em VPC e selecione até cinco grupos de segurança em Grupos de segurança. Para criar um novo grupo de segurança, escolha Criar um novo grupo de segurança.

Como alternativa, você pode pular essa etapa e conectar uma VPC à rede de serviços usando um VPC endpoint (desenvolvido por). AWS PrivateLink Para obter mais informações, consulte [Access service networks](#) no guia AWS PrivateLink do usuário.

8. Ao criar uma rede de serviços, você precisa decidir se pretende compartilhar a rede de serviços com outras contas ou não. Sua seleção é imutável e não pode ser alterada após a criação da rede de serviços. Se você optar por permitir o compartilhamento, a rede de serviços poderá ser compartilhada com outras contas por meio de AWS Resource Access Manager.

Para [compartilhar sua rede de serviços](#) com outras contas, escolha os compartilhamentos de AWS RAM recursos em Compartilhamentos de recursos.

- Para criar um compartilhamento de recursos, acesse o AWS RAM console e escolha Criar um compartilhamento de recursos.
9. Para acesso à rede, você pode deixar o tipo de autenticação padrão, Nenhum, se quiser que os clientes associados VPCs acessem os serviços dessa rede de serviços. Para aplicar uma [política de autenticação](#) para controlar o acesso aos seus serviços, escolha AWS IAM e execute uma das seguintes ações para Política de autenticação:
 - Insira uma política no campo de entrada. Para exemplos de políticas que você pode copiar e colar, escolha Exemplos de política.
 - Escolha Aplicar modelo de política e selecione o modelo Permitir acesso autenticado e não autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço assinando a solicitação (ou seja, autenticado) ou anonimamente (ou seja, não autenticado).
 - Escolha Aplicar modelo de política e selecione o modelo Permitir apenas acesso autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço exclusivamente assinando a solicitação (ou seja, autenticado).
 10. (Opcional) Para ativar os [logs de acesso](#), ative o seletor de Logs de acesso e especifique um destino para seus logs de acesso da seguinte forma:
 - Selecione Grupo de CloudWatch registros e escolha um grupo de CloudWatch registros. Para criar um grupo de registros, escolha Criar um grupo de registros em CloudWatch.
 - Selecione o bucket do S3 e insira o caminho do bucket do S3, incluindo qualquer prefixo. Para pesquisar seus buckets do S3, escolha Procurar S3.
 - Em Fluxo de entrega do Kinesis Data Firehose, selecione um fluxo de entrega. Para criar um fluxo de entrega, escolha Criar um fluxo de entrega no Kinesis.
 11. (Opcional) Para [compartilhar sua rede de serviços](#) com outras contas, escolha os compartilhamentos de AWS RAM recursos em Compartilhamentos de recursos. Para criar um compartilhamento de recursos, escolha Criar um compartilhamento de recursos no console do RAM.
 12. Revise sua configuração na seção Resumo e escolha Criar rede de serviços.

Para criar uma rede de serviços usando o AWS CLI

Use o comando [create-service-network](#). Esse comando cria somente a rede de serviços básicos. Para criar uma rede de serviços totalmente funcional, você também deve usar os comandos que criam [associações de serviços](#), [associações de VPC](#) e [configurações de acesso](#).

Gerencie as associações para uma rede de serviços VPC Lattice

Quando você associa uma configuração de serviço ou recurso à rede de serviços, isso permite que os clientes VPCs conectados à rede de serviços façam solicitações à configuração do serviço e do recurso. Quando você conecta uma VPC à rede de serviços, ela permite que todos os destinos dentro dessa VPC sejam clientes e se comuniquem com outros serviços e configurações de recursos na rede de serviços.

Conteúdo

- [Gerenciar associações de serviços](#)
- [Gerenciar associações de configuração de recursos](#)
- [Gerenciar associações de VPC](#)
- [Gerencie associações de endpoints de VPC](#)

Gerenciar associações de serviços

Você pode associar serviços que residam em sua conta ou serviços que sejam compartilhados com você de contas diferentes. Essa é uma etapa opcional ao criar uma rede de serviços. No entanto, uma rede de serviços não estará totalmente funcional até que você associe um serviço. Os proprietários do serviço podem associar seus serviços a uma rede de serviços se a conta tiver o acesso necessário. Para obter mais informações, consulte [Exemplos de políticas baseadas em identidade para o VPC Lattice](#).

Quando você exclui uma associação de serviço, o serviço não poderá mais se conectar a outros serviços na rede de serviços.

Para gerenciar associações de serviço usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.
4. Escolha a guia Associações de serviço.
5. Para criar uma associação, faça o seguinte:
 - a. Escolha Criar associações.

- b. Selecione um serviço em Serviços. Para criar um serviço, escolha Criar um serviço Amazon VPC Lattice.
 - c. (Opcional) Para adicionar uma tag, expanda Tags de associação de serviço, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
 - d. Escolha Salvar alterações.
6. Para excluir uma associação, marque a caixa de seleção da associação e escolha Ações, Excluir associações de serviço. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para criar uma associação de serviço usando o AWS CLI

Use o comando [create-service-network-service-association](#).

Para excluir uma associação de serviço usando o AWS CLI

Use o comando [delete-service-network-service-association](#).

Gerenciar associações de configuração de recursos

Uma configuração de recurso é um objeto lógico que representa um único recurso ou um grupo de recursos. Você pode associar configurações de recursos que residem em sua conta ou configurações de recursos que são compartilhadas com você de contas diferentes. Essa é uma etapa opcional ao criar uma rede de serviços. Os proprietários da configuração de recursos podem associar suas configurações de recursos a uma rede de serviços se a conta tiver o acesso necessário. Para obter mais informações, consulte [exemplos de políticas baseadas em identidade para o VPC Lattice](#).

Gerencie associações entre redes de serviços e configurações de recursos

Você pode criar ou excluir a associação entre a rede de serviços e a configuração do recurso.

Para gerenciar associações de configuração de recursos usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em PrivateLink e Lattice, escolha Redes de serviços.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.
4. Escolha a guia Associações de configuração de recursos.
5. Para criar uma associação, faça o seguinte:

- a. Escolha Criar associações.
 - b. Selecione uma configuração de recurso em Configurações de recursos. Escolha Criar uma configuração de recursos do Amazon VPC Lattice. .
 - c. (Opcional) Para adicionar uma tag, expanda Tags de associação de serviço, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
 - d. Escolha Salvar alterações.
6. Para excluir uma associação, marque a caixa de seleção da associação e escolha Ações, Excluir. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para criar uma associação de configuração de recursos usando o AWS CLI

Use o comando [create-service-network-resource-association](#).

Para excluir uma associação de configuração de recursos usando o AWS CLI

Use o comando [delete-service-network-resource-association](#).

Gerenciar associações de VPC

Os clientes podem enviar solicitações para serviços e recursos especificados nas configurações de recursos associadas a uma rede de serviços se o cliente estiver VPCs associado à rede de serviços. O tráfego de clientes que atravessa uma conexão de emparelhamento de VPC ou um gateway de trânsito só é permitido por meio de uma rede de serviços usando um endpoint VPC do tipo rede de serviços.

Associar uma VPC é uma etapa opcional quando você cria uma rede de serviços. Os proprietários da rede podem se VPCs associar a uma rede de serviços se sua conta tiver o acesso necessário. Para obter mais informações, consulte [Exemplos de políticas baseadas em identidade para o VPC Lattice](#).

Quando você exclui uma associação de VPC, os clientes do não VPCs podem mais se conectar aos serviços na rede de serviços.

Para gerenciar associações de VPC usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.

4. Escolha a guia Associações de VPC.
5. Para criar uma associação de VPC, faça o seguinte:
 - a. Escolha Criar associações de VPC.
 - b. Escolha Adicionar associação de VPC.
 - c. Selecione uma VPC em VPC e selecione até cinco grupos de segurança em Grupos de segurança. Para criar um novo grupo de segurança, escolha Criar um novo grupo de segurança.
 - d. (Opcional) Para adicionar uma tag, expanda Tags de associação de VPC, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
 - e. Escolha Salvar alterações.
6. Para editar os grupos de segurança de uma associação, marque a caixa de seleção da associação e escolha Ações, Editar grupos de segurança. Adicione e remova grupos de segurança conforme necessário.
7. Para excluir uma associação, marque a caixa de seleção da associação e escolha Ações, Excluir associações de VPC. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para criar uma associação de VPC usando o AWS CLI

Use o comando [create-service-network-vpc-association](#).

Para atualizar os grupos de segurança de uma associação de VPC usando o AWS CLI

Use o comando [update-service-network-vpc-association](#).

Para excluir uma associação de VPC usando o AWS CLI

Use o comando [delete-service-network-vpc-association](#).

Gerencie associações de endpoints de VPC

Os clientes podem enviar solicitações para serviços e recursos especificados nas configurações de recursos por meio de um VPC endpoint (desenvolvido AWS PrivateLink por) em sua VPC. Um endpoint VPC do tipo rede de serviços conecta uma VPC a uma rede de serviços. O tráfego de clientes que vem de fora da VPC por meio de uma conexão de emparelhamento de VPC, Transit Gateway, Direct Connect ou VPN pode usar o VPC endpoint para acessar configurações de serviços e recursos. Com os VPC endpoints, você pode conectar uma VPC a várias redes de serviços.

Quando você cria um VPC endpoint em uma VPC, os endereços IP da VPC (e não os endereços IP da [lista de prefixos gerenciados](#)) são usados para estabelecer conectividade com a rede de serviços.

Para gerenciar associações de endpoints de VPC usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.
4. Escolha a guia Associações de endpoint para visualizar os endpoints VPC conectados à sua rede de serviços.
5. Selecione o ID do endpoint da VPC para abrir sua página de detalhes. Em seguida, modifique ou exclua a associação do VPC endpoint.

Para criar uma nova associação de VPC endpoint usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Endpoints.
3. Escolha Criar endpoints.
4. Em Tipo, escolha Redes de serviço.
5. Selecione a rede de serviços que você deseja conectar à sua VPC.
6. Selecione a VPC, as sub-redes e os grupos de segurança.
7. (Opcional) Para adicionar uma tag, expanda Tags de associação de VPC, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
8. Escolha Criar endpoint.

Para saber mais sobre o VPC endpoint e como se conectar a redes de serviços, consulte [Acesse redes de serviços no guia](#) do AWS PrivateLink usuário.

Editar configurações de acesso para uma rede de serviços VPC Lattice

As configurações de acesso permitem que você configure e gerencie o acesso do cliente a uma rede de serviços. As configurações de acesso incluem tipo de autenticação e políticas de autenticação. As políticas de autenticação ajudam você a autenticar e autorizar o fluxo de tráfego para serviços no

VPC Lattice. As configurações de acesso da rede de serviços não se aplicam às configurações de recursos associadas à rede de serviços.

Você pode aplicar políticas de autenticação no nível da rede de serviços, no nível do serviço ou em ambos. Normalmente, as políticas de autenticação são aplicadas pelos proprietários da rede ou administradores da nuvem. Eles podem implementar uma autorização específica, por exemplo, permitindo chamadas autenticadas de dentro da organização ou permitindo solicitações GET anônimas que correspondam a uma determinada condição. No nível do serviço, os proprietários do serviço podem aplicar controles refinados, que podem ser mais restritivos. Para obter mais informações, consulte [Controle o acesso aos serviços do VPC Lattice usando políticas de autenticação](#).

Para adicionar ou atualizar políticas de acesso usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.
4. Escolha a guia Acesso para verificar as configurações de acesso atuais.
5. Para atualizar as configurações de acesso, escolha Editar configurações de acesso.
6. Se você quiser que os clientes associados VPCs acessem os serviços nessa rede de serviços, escolha Nenhum para o tipo de autenticação.
7. Para aplicar uma política de recursos à rede de serviços, escolha AWS IAM em Tipo de autenticação e faça o seguinte para a Política de autenticação:
 - Insira uma política no campo de entrada. Para exemplos de políticas que você pode copiar e colar, escolha Exemplos de política.
 - Escolha Aplicar modelo de política e selecione o modelo Permitir acesso autenticado e não autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço assinando a solicitação (ou seja, autenticado) ou anonimamente (ou seja, não autenticado).
 - Escolha Aplicar modelo de política e selecione o modelo Permitir apenas acesso autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço exclusivamente assinando a solicitação (ou seja, autenticado).
8. Escolha Salvar alterações.

Para adicionar ou atualizar uma política de acesso usando o AWS CLI

Use o comando [put-auth-policy](#).

Editar detalhes de monitoramento de uma rede de serviços VPC Lattice

O VPC Lattice gera métricas e logs para cada solicitação e resposta, tornando mais eficiente monitorar e solucionar problemas de aplicações.

Você pode habilitar os logs de acesso e especificar o recurso de destino para seus logs. O VPC Lattice pode enviar registros para os seguintes recursos: grupos de CloudWatch registros, fluxos de entrega do Firehose e buckets do S3.

Para habilitar logs de acesso ou atualizar um destino de log usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.
4. Escolha a guia Monitoring (Monitoramento). Verifique Logs de acesso para ver se os logs de acesso estão habilitados.
5. Para habilitar ou desabilitar os logs de acesso, escolha Editar logs de acesso e, em seguida, ative ou desative a opção Logs de acesso.
6. Ao habilitar os logs de acesso, você deverá selecionar o tipo de destino de entrega e, em seguida, criar ou escolher o destino para os logs de acesso. Você também pode alterar o destino da entrega a qualquer momento. Por exemplo:
 - Selecione Grupo de CloudWatch registros e escolha um grupo de CloudWatch registros. Para criar um grupo de registros, escolha Criar um grupo de registros em CloudWatch.
 - Selecione o bucket do S3 e insira o caminho do bucket do S3, incluindo qualquer prefixo. Para pesquisar seus buckets do S3, escolha Procurar S3.
 - Em Fluxo de entrega do Kinesis Data Firehose, selecione um fluxo de entrega. Para criar um fluxo de entrega, escolha Criar um fluxo de entrega no Kinesis.
7. Escolha Salvar alterações.

Para habilitar os registros de acesso usando o AWS CLI

Use o comando [create-access-log-subscription](#).

Para atualizar o destino do registro usando o AWS CLI

Use o comando [update-access-log-subscription](#).

Para desativar os registros de acesso usando o AWS CLI

Use o comando [delete-access-log-subscription](#).

Gerenciar tags para uma rede de serviços VPC Lattice

As tags ajudam a categorizar sua rede de serviços de diferentes formas, por exemplo, por finalidade, por proprietário ou por ambiente.

Você pode adicionar várias tags a cada rede de serviços. As chaves de tag precisam ser exclusivas para cada rede de serviços. Se você adicionar uma tag a uma chave que já esteja associada à rede de serviços, isso atualizará o valor da tag. É possível usar caracteres como letras, espaços, números (em UTF-8) e os seguintes caracteres especiais: + - = . _ : / @. Não use espaços no início nem no fim. Os valores de tags não diferenciam maiúsculas de minúsculas.

Para adicionar ou excluir tags usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.
4. Escolha a guia Tags.
5. Para adicionar uma tag, escolha Adicionar tags e insira a chave e o valor da tag. Para adicionar outra tag, escolha Adicionar nova tag novamente. Quando terminar de adicionar etiquetas, escolha Save changes (Salvar alterações).
6. Para excluir uma tag, marque a caixa de seleção da tag e escolha Excluir. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para adicionar ou excluir tags usando o AWS CLI

Use os comandos [tag-resource](#) e [untag-resource](#).

Excluir uma rede de serviços VPC Lattice

Antes de excluir uma rede de serviços, você deve primeiro excluir todas as associações que a rede de serviços possa ter com qualquer serviço, configuração de recursos, VPC ou VPC endpoint.

Quando você exclui uma rede de serviços, também excluimos todos os recursos relacionados à rede de serviços, como a política de recursos, a política de autenticação e as assinaturas do log de acesso.

Para excluir uma rede de serviços usando o console

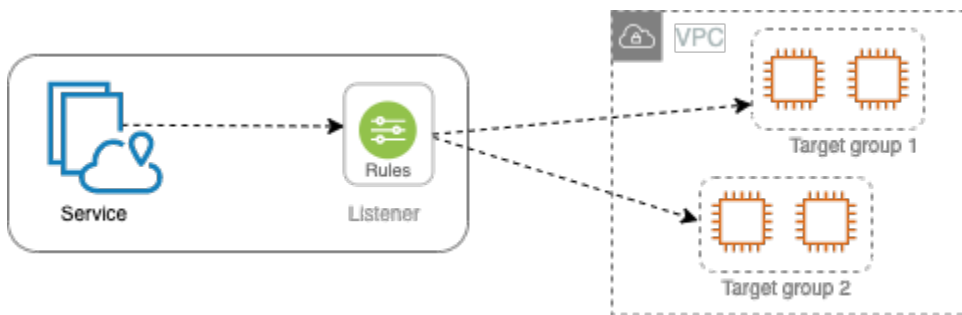
1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Marque a caixa de seleção para a rede de serviços e selecione Ações, Excluir rede de serviços.
4. Quando a confirmação for solicitada, insira **confirm** e escolha Delete.

Para excluir uma rede de serviços usando o AWS CLI

Use o comando [delete-service-network](#).

Serviços no VPC Lattice

Um serviço no VPC Lattice é uma unidade de software implantável de maneira independente que fornece uma tarefa ou função específica. Um serviço pode funcionar em instâncias, contêineres ou como funções com tecnologia sem servidor em uma conta ou em uma nuvem privada virtual (VPC). Um serviço tem um receptor que usa regras, chamadas regras de receptor, que você pode configurar para ajudar a direcionar o tráfego para seus destinos. Os tipos de destino compatíveis incluem EC2 instâncias, endereços IP, funções Lambda, Application Load Balancers, tarefas do Amazon ECS e Kubernetes Pods. Para obter mais informações, consulte [Grupos de destino no VPC Lattice](#). É possível associar um serviço a várias redes de serviços. O diagrama a seguir mostra os principais componentes de um serviço habitual no VPC Lattice.



Você pode criar um serviço dando um nome e uma descrição a ele. No entanto, para controlar e monitorar o tráfego para seu serviço, é importante incluir configurações de acesso e detalhes de monitoramento. Para enviar tráfego do seu serviço para seus destinos, você deverá configurar um receptor e configurar regras. Para permitir que o tráfego flua da rede de serviços para seu serviço, você deverá associar seu serviço à rede de serviços.

Há um tempo limite de inatividade e um tempo limite geral de conexão para conexões com os destinos. O tempo limite da conexão ociosa é de 1 minuto. Depois disso, fecharemos a conexão. A duração máxima é de 10 minutos. Depois disso, não permitiremos novos fluxos na conexão e iniciaremos o processo de fechamento dos fluxos existentes.

Tarefas

- [Etapa 1: criar um serviço do VPC Lattice](#)
- [Etapa 2: definir o roteamento](#)
- [Etapa 3: criar associações de rede](#)
- [Etapa 4: revisar e criar](#)
- [Gerenciar associações de um serviço do VPC Lattice](#)

- [Editar as configurações de acesso para um serviço VPC Lattice](#)
- [Editar os detalhes de monitoramento de um serviço VPC Lattice](#)
- [Gerenciar tags de um serviço VPC Lattice](#)
- [Configure um nome de domínio personalizado para seu serviço VPC Lattice](#)
- [Traga seu próprio certificado \(BYOC\) para o VPC Lattice](#)
- [Excluir um serviço VPC Lattice](#)

Etapa 1: criar um serviço do VPC Lattice

Crie um serviço VPC Lattice básico com configurações de acesso e detalhes de monitoramento. No entanto, o serviço não estará totalmente funcional até que você defina sua configuração de roteamento e o associe a uma rede de serviços.

Para criar um serviço básico usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Escolha Create service.
4. Em Identificadores, faça o seguinte:
 - a. Insira um nome para o serviço. O nome deve ter entre 3 e 63 caracteres e usar letras minúsculas, números e hifens. Ele deve começar e terminar com uma letra ou um número. Não use hifens duplos.
 - b. (Opcional) Insira uma descrição para a rede de serviços. Você pode definir ou alterar a descrição durante ou após a criação. A descrição pode ter até 256 caracteres.
5. Para especificar um nome de domínio personalizado para seu serviço, selecione Especificar uma configuração de domínio personalizada e insira o nome de domínio personalizado.

Para ouvintes HTTPS, você pode selecionar o certificado que o VPC Lattice usará para realizar a terminação de TLS. Se você não selecionar um certificado agora, poderá selecioná-lo ao criar um ouvinte HTTPS para o serviço.

Para ouvintes TCP, você deve especificar um nome de domínio personalizado para seu serviço. Se você especificar um certificado, ele não será usado. Em vez disso, você executa a terminação de TLS em seu aplicativo.

6. Em Acesso ao serviço, escolha Nenhum se quiser que os clientes VPCs associados à rede de serviços acessem seu serviço. Para aplicar uma [política de autenticação](#) para controlar o acesso ao serviço, escolha AWS IAM. Para aplicar uma política de recurso ao serviço, faça o seguinte em Política de autenticação:
 - Insira uma política no campo de entrada. Para exemplos de políticas que você pode copiar e colar, escolha Exemplos de política.
 - Escolha Aplicar modelo de política e selecione o modelo Permitir acesso autenticado e não autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço assinando a solicitação (ou seja, autenticado) ou anonimamente (ou seja, não autenticado).
 - Escolha Aplicar modelo de política e selecione o modelo Permitir apenas acesso autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço exclusivamente assinando a solicitação (ou seja, autenticado).
7. (Opcional) Para habilitar os [logs de acesso](#), ative o seletor de Logs de acesso e especifique um destino para seus logs de acesso da seguinte forma:
 - Selecione Grupo de CloudWatch registros e escolha um grupo de CloudWatch registros. Para criar um grupo de registros, escolha Criar um grupo de registros em CloudWatch.
 - Selecione o bucket do S3 e insira o caminho do bucket do S3, incluindo qualquer prefixo. Para pesquisar seus buckets do S3, escolha Procurar S3.
 - Em Fluxo de entrega do Kinesis Data Firehose, selecione um fluxo de entrega. Para criar um fluxo de entrega, escolha Criar um fluxo de entrega no Kinesis.
8. (Opcional) Para [compartilhar seu serviço](#) com outras contas, escolha um compartilhamento de AWS RAM recursos em Compartilhamentos de recursos. Para criar um compartilhamento de recursos, escolha Criar um compartilhamento de recursos no console do RAM.
9. Para revisar sua configuração e criar o serviço, escolha Pular para a análise e criação. Caso contrário, escolha Próximo para definir a configuração de roteamento do seu serviço.

Etapa 2: definir o roteamento

Defina sua configuração de roteamento usando receptores para que seu serviço possa enviar tráfego para os destinos que você especificar.

Pré-requisito

Antes que possa adicionar um receptor, é necessário criar um grupo de destino do VPC Lattice. Para obter mais informações, consulte [the section called “Criar um grupo de destino”](#).

Para definir o roteamento para seu serviço usando o console

1. Escolha Add listener.
2. Em Nome do receptor, você pode fornecer um nome de receptor personalizado ou usar o protocolo e a porta do seu receptor como o nome do receptor. Um nome personalizado que você especificar pode ter até 63 caracteres e deve ser exclusivo para cada serviço em sua conta. Os caracteres válidos são a-z, 0-9 e hífens (-). Você não pode usar um hífen como primeiro ou último caractere, nem imediatamente após outro hífen. Não é possível alterar o nome de um receptor após criá-lo.
3. Escolha um protocolo e, em seguida, insira um número de porta.
4. Em Ação padrão, escolha o grupo de destino do VPC Lattice para receber tráfego e escolha o peso a ser atribuído a esse grupo de destino. Opcionalmente, você poderá adicionar outro grupo de destino para a ação padrão. Escolha Adicionar ação e, em seguida, escolha outro grupo de destino e especifique seu peso.
5. (Opcional) Para adicionar outra regra, escolha Adicionar regra e insira um nome, uma prioridade, uma condição e uma ação para a regra.

Você pode atribuir um número de prioridade entre 1 e 100 a cada regra. Um listener não pode ter várias regras com a mesma prioridade. As regras são avaliadas em ordem de prioridade, do valor mais baixo para o valor mais alto. A regra padrão é avaliada por último.

Em Condição, insira um padrão de caminho para a condição de correspondência de caminho. O tamanho máximo de cada string é de 200 caracteres. A comparação não diferencia maiúsculas de minúsculas.

6. (Opcional) Para adicionar tags, expanda Tags de receptor, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
7. Para revisar sua configuração e criar o serviço, escolha Pular para a análise e criação. Caso contrário, escolha Próximo para associar seu serviço a uma rede de serviços.

Etapa 3: criar associações de rede

Associe seu serviço a uma rede de serviços para que os clientes possam se comunicar com ele.

Para associar um serviço a uma rede de serviços usando o console

1. Para Redes de serviços VPC Lattice, selecione a rede de serviços. Para criar uma rede de serviços, escolha Criar uma rede VPC Lattice. É possível associar seu serviço a várias redes de serviços.
2. (Opcional) Para adicionar uma tag, expanda Tags de associação de rede de serviços, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
3. Escolha Próximo.

Etapa 4: revisar e criar

Para revisar a configuração e criar o serviço usando o console

1. Revise a configuração do seu serviço.
2. Escolha Editar se precisar modificar qualquer parte da configuração do serviço.
3. Quando terminar de revisar ou editar sua configuração, escolha Criar serviço VPC Lattice.
4. Se você tiver especificado um nome de domínio personalizado para o serviço, será necessário configurar o roteamento de DNS após a criação do serviço. Para obter mais informações, consulte [the section called “Configurar um nome de domínio personalizado”](#).

Gerenciar associações de um serviço do VPC Lattice

Quando você associa um serviço à rede de serviços, isso permite que os clientes (recursos em uma VPC associada à rede de serviços) façam solicitações a esse serviço. Você pode associar serviços que estejam em sua conta ou serviços que sejam compartilhados com você de contas diferentes. Essa etapa é opcional na criação do serviço. No entanto, após a criação, o serviço não poderá se comunicar com outros serviços até que você o associe a uma rede de serviços. Os proprietários do serviço podem associar seus serviços à rede de serviços se a conta tiver o acesso necessário. Para obter mais informações, consulte [Funcionamento do VPC Lattice](#).

Para gerenciar associações de rede de serviços usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.

4. Escolha a guia Associações de rede de serviços.
5. Para criar uma associação, faça o seguinte:
 - a. Escolha Criar associações.
 - b. Selecione uma rede de serviços nas Redes de serviços VPC Lattice. Para criar uma rede de serviços, escolha Criar uma rede VPC Lattice.
 - c. (Opcional) Para adicionar uma tag, expanda Tags de associação de serviço, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
 - d. Escolha Salvar alterações.
6. Para excluir uma associação, marque a caixa de seleção da associação e escolha Ações, Excluir associações de rede. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para criar uma associação de rede de serviços usando o AWS CLI

Use o comando [create-service-network-service-association](#).

Para excluir uma associação de rede de serviços usando o AWS CLI

Use o comando [delete-service-network-service-association](#).

Editar as configurações de acesso para um serviço VPC Lattice

As configurações de acesso permitem que você configure e gerencie o acesso do cliente a um serviço. As configurações de acesso incluem tipo de autenticação e políticas de autenticação. As políticas de autenticação ajudam você a autenticar e autorizar o fluxo de tráfego para serviços no VPC Lattice.

Você pode aplicar políticas de autenticação no nível da rede de serviços, no nível do serviço ou em ambos. No nível do serviço, os proprietários do serviço podem aplicar controles refinados, que podem ser mais restritivos. Normalmente, as políticas de autenticação são aplicadas pelos proprietários da rede ou administradores da nuvem. Eles podem implementar uma autorização específica, por exemplo, permitindo chamadas autenticadas de dentro da organização ou permitindo solicitações GET anônimas que correspondam a uma determinada condição. Para obter mais informações, consulte [Controle o acesso aos serviços do VPC Lattice usando políticas de autenticação](#).

Para adicionar ou atualizar políticas de acesso usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Escolha a guia Acesso para verificar as configurações de acesso atuais.
5. Para atualizar as configurações de acesso, escolha Editar configurações de acesso.
6. Se você quiser que os clientes VPCs na rede de serviços associada acessem seu serviço, escolha Nenhum para o tipo de autenticação.
7. Para aplicar uma política de recursos para controlar o acesso ao serviço, escolha AWS IAM em Tipo de autenticação e faça o seguinte para a Política de autenticação:
 - Insira uma política no campo de entrada. Para exemplos de políticas que você pode copiar e colar, escolha Exemplos de política.
 - Escolha Aplicar modelo de política e selecione o modelo Permitir acesso autenticado e não autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço assinando a solicitação (ou seja, autenticado) ou anonimamente (ou seja, não autenticado).
 - Escolha Aplicar modelo de política e selecione o modelo Permitir apenas acesso autenticado. Esse modelo permite que um cliente de outra conta acesse o serviço exclusivamente assinando a solicitação (ou seja, autenticado).
8. Escolha Salvar alterações.

Para adicionar ou atualizar uma política de acesso usando o AWS CLI

Use o comando [put-auth-policy](#).

Editar os detalhes de monitoramento de um serviço VPC Lattice

O VPC Lattice gera métricas e logs para cada solicitação e resposta, tornando mais eficiente monitorar e solucionar problemas de aplicações.

Você pode habilitar os logs de acesso e especificar o recurso de destino para seus logs. O VPC Lattice pode enviar registros para os seguintes recursos: grupos de CloudWatch registros, fluxos de entrega do Firehose e buckets do S3.

Para habilitar logs de acesso ou atualizar um destino de log usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Escolha a guia Monitor e Logs. Verifique Logs de acesso para ver se os logs de acesso estão habilitados.
5. Para habilitar ou desabilitar os logs de acesso, escolha Editar logs de acesso e, em seguida, ative ou desative a opção Logs de acesso.
6. Ao habilitar os logs de acesso, você deverá selecionar o tipo de destino de entrega e, em seguida, criar ou escolher o destino para os logs de acesso. Você também pode alterar o destino da entrega a qualquer momento. Por exemplo:
 - Selecione Grupo de CloudWatch registros e escolha um grupo de CloudWatch registros. Para criar um grupo de registros, escolha Criar um grupo de registros em CloudWatch.
 - Selecione o bucket do S3 e insira o caminho do bucket do S3, incluindo qualquer prefixo. Para pesquisar seus buckets do S3, escolha Procurar S3.
 - Em Fluxo de entrega do Kinesis Data Firehose, selecione um fluxo de entrega. Para criar um fluxo de entrega, escolha Criar um fluxo de entrega no Kinesis.
7. Escolha Salvar alterações.

Para habilitar os registros de acesso usando o AWS CLI

Use o comando [create-access-log-subscription](#).

Para atualizar o destino do registro usando o AWS CLI

Use o comando [update-access-log-subscription](#).

Para desativar os registros de acesso usando o AWS CLI

Use o comando [delete-access-log-subscription](#).

Gerenciar tags de um serviço VPC Lattice

As tags ajudam a categorizar seu serviço de diferentes formas, por exemplo, por finalidade, por proprietário ou por ambiente.

Você pode adicionar várias tags a cada serviço. As chaves de tag devem ser exclusivas para cada serviço. Se você adicionar uma tag com uma chave que já esteja associada ao serviço, ela atualizará o valor dessa tag. É possível usar caracteres como letras, espaços, números (em UTF-8) e os seguintes caracteres especiais: + - = . _ : / @. Não use espaços no início nem no fim. Os valores de tags não diferenciam maiúsculas de minúsculas.

Para adicionar ou excluir tags usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Escolha a guia Tags.
5. Para adicionar uma tag, escolha Adicionar tags e insira a chave e o valor da tag. Para adicionar outra tag, escolha Adicionar nova tag novamente. Quando terminar de adicionar etiquetas, escolha Save changes (Salvar alterações).
6. Para excluir uma tag, marque a caixa de seleção da tag e escolha Excluir. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para adicionar ou excluir tags usando o AWS CLI

Use os comandos [tag-resource](#) e [untag-resource](#).

Configure um nome de domínio personalizado para seu serviço VPC Lattice

Quando você cria um novo serviço, o VPC Lattice gera um nome de domínio totalmente qualificado (FQDN) exclusivo para o serviço com a seguinte sintaxe.

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

No entanto, os nomes de domínio que o VPC Lattice fornece não são fáceis de lembrar para seus usuários. Os nomes de domínio personalizados são mais simples e intuitivos do URLs que você pode fornecer aos seus usuários. Se você preferir usar um nome de domínio personalizado para seu serviço, como `www.parking.example.com`, em vez do nome DNS gerado pelo VPC Lattice, você poderá configurá-lo ao criar um serviço VPC Lattice. Quando um cliente fizer uma solicitação usando

seu nome de domínio personalizado, o servidor de DNS o resolverá para o nome de domínio gerado pelo VPC Lattice.

Pré-requisitos

- Você deve ter um nome de domínio registrado para o seu serviço. Se ainda não tiver um nome de domínio registrado, você poderá registrar um por meio do Amazon Route 53 ou em dezenas de outros registradores comerciais.
- Para receber solicitações HTTPS, você deverá fornecer seu próprio certificado no AWS Certificate Manager. O VPC Lattice não oferece suporte a um certificado padrão como alternativa. Portanto, se você não fornecer um SSL/TLS certificado correspondente ao seu nome de domínio personalizado, todas as conexões HTTPS com seu nome de domínio personalizado falharão. Para obter mais informações, consulte [Traga seu próprio certificado \(BYOC\) para o VPC Lattice](#).

Limitações e considerações

- Você não pode ter mais de um nome de domínio personalizado para um serviço.
- Você não pode modificar o nome de domínio personalizado após criar o serviço.
- O nome de domínio personalizado deve ser exclusivo para uma rede de serviços. Isso significa que um serviço não poderá ser criado com um nome de domínio personalizado que já exista (para outro serviço) na mesma rede de serviços.

O procedimento a seguir mostra como configurar um nome de domínio personalizado para seu serviço.

AWS Management Console

Para configurar um nome de domínio personalizado para seu serviço

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviço.
3. Escolha Criar serviço. Você seguirá para a Etapa 1: criar um serviço.
4. Na seção Configuração de domínio personalizado, escolha Especificar uma configuração de domínio personalizado.
5. Insira o nome de domínio personalizado.

6. Para atender às solicitações HTTPS, selecione o SSL/TLS certificado correspondente ao seu nome de domínio personalizado em SSL/TLS Certificado personalizado. Se você ainda não tiver um certificado ou não quiser adicionar um agora, poderá adicionar um certificado ao criar seu receptor HTTPS. No entanto, sem um certificado, seu nome de domínio personalizado não poderá atender às solicitações HTTPS. Para obter mais informações, consulte [Adicionar um receptor HTTPS](#).
7. Quando terminar de adicionar todas as outras informações para criar o serviço, escolha Criar.

AWS CLI

Para configurar um nome de domínio personalizado para seu serviço

Use o 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
```

No comando acima, insira um nome para o serviço em `--name`. Em `--custom-domain-name`, insira o nome de domínio do seu serviço, como `parking.example.com`. Em `--certificate-arn`, insira o ARN do seu certificado no ACM. O ARN do certificado está disponível em AWS Certificate Manager na sua conta.

Associe um nome de domínio personalizado ao seu serviço

Primeiro, se você ainda não tiver feito isso, registre seu nome de domínio personalizado. A Sociedade Internet para a Atribuição de Nomes e Números (ICANN, Internet Corporation for Assigned Names and Numbers) gerencia nomes de domínio na Internet. Você registra um nome de domínio usando um registrador de nomes de domínio, uma organização chancelada pela ICANN que gerencia o registro dos nomes de domínio. O site do registrador fornecerá instruções detalhadas e informações sobre a definição de preço para registrar o nome de domínio. Para obter mais informações, consulte os seguintes recursos:

- Para usar o Amazon Route 53 para registrar um nome de domínio, consulte [Registrar nomes de domínio com o Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

- Para obter uma lista de registradores cancelados, consulte [Diretório de registradores cancelados](#).

Em seguida, use seu serviço de DNS, como seu registrador de domínio, para criar um registro para encaminhar consultas para seu serviço. Para obter mais informações, consulte a documentação do serviço DNS. Também é possível usar o Route 53 como seu serviço DNS.

Se você estiver usando o Route 53, poderá usar um registro de alias ou um registro CNAME para encaminhar consultas para seu serviço. Recomendamos que você use um registro de alias, pois você pode criar um registro de alias no nó superior de um namespace DNS, também conhecido como ápice da zona.

Se você estiver usando o Route 53, primeiro crie uma zona hospedada, que contém informações sobre como rotear o tráfego na Internet para seu domínio. Depois de criar a zona hospedada pública ou privada, crie um registro para que seu nome de domínio personalizado, por exemplo `parking.example.com`, seja mapeado para o nome de domínio gerado automaticamente pelo VPC Lattice, por exemplo, `.my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`. Sem esse mapeamento, seu nome de domínio personalizado não funcionará no VPC Lattice.

Os procedimentos a seguir mostram como criar uma zona hospedada pública ou privada usando o Route 53.

AWS Management Console

Para criar um registro de alias para rotear consultas para seu serviço usando o Route 53, consulte [Roteamento de tráfego para o endpoint de domínio do serviço Amazon VPC Lattice](#).

Use o nome de domínio gerado pelo VPC Lattice para seu serviço, por exemplo **`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`**, para o Value. Você pode encontrar esse nome de domínio gerado automaticamente no console do VPC Lattice na sua página de serviço.

AWS CLI

Para criar um registro de alias na sua zona hospedada

1. Obtenha o nome de domínio gerado pelo VPC Lattice para seu serviço (por exemplo, `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`) e o ID da zona hospedada executando o comando `get-service`.

2. Para definir o alias, execute o seguinte comando.

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

Para o arquivo `change-set.json`, crie um arquivo JSON com o conteúdo do exemplo de JSON a seguir e salve-o em sua máquina local. *file:///~/Desktop/change-set.json* Substitua o comando acima pelo caminho do arquivo JSON salvo em sua máquina local. Observe que “Type” no JSON a seguir pode ser um tipo de registro A ou 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
        }
      }
    }
  ]
}
```

Traga seu próprio certificado (BYOC) para o VPC Lattice

Para atender às solicitações HTTPS, você deve ter seu próprio SSL/TLS certificado pronto AWS Certificate Manager (ACM) antes de configurar um nome de domínio personalizado. Esses certificados devem ter um Subject Alternate Name (SAN – Nome alternativo do assunto) ou Common Name (CN – Nome comum) que corresponda ao nome de domínio personalizado do seu serviço. Se houver um SAN presente, verificaremos se há uma correspondência somente na lista de SAN. Se não houver um SAN, verificaremos se há uma correspondência no CN.

O VPC Lattice atenderá às solicitações HTTPS usando a Server Name Indication (SNI – Indicação de nome de servidor). O DNS encaminhará a solicitação HTTPS para seu serviço VPC Lattice com base no nome de domínio personalizado e no certificado correspondente a esse nome de domínio. Para solicitar um SSL/TLS certificado para um nome de domínio no ACM ou importar um para o ACM, consulte [Emissão e gerenciamento de certificados e Importação de certificados](#) no Guia do usuário.AWS Certificate Manager. Se você não puder solicitar ou importar seu próprio certificado no ACM, use o nome de domínio e o certificado gerados pelo VPC Lattice.

O VPC Lattice só aceita um certificado personalizado por serviço. No entanto, você pode usar um certificado personalizado para vários domínios personalizados. Isso significa que você poderá usar o mesmo certificado para todos os serviços VPC Lattice criados com um nome de domínio personalizado.

Para visualizar seu certificado usando o console do ACM, abra Certificados e selecione seu ID de certificado. Você deverá ver o serviço VPC Lattice associado a esse certificado em Recurso associado.

Limitações e considerações

- O VPC Lattice permite combinações de caracteres curinga com um nível de profundidade no nome alternativo do assunto (SAN) ou no nome comum (CN) do certificado associado. Por exemplo, se você criar um serviço com o nome de domínio personalizado `parking.example.com` e associar seu próprio certificado ao SAN `*.example.com`. Quando uma solicitação chegar para `parking.example.com`, o VPC Lattice combinará o SAN com qualquer nome de domínio com o domínio apex `example.com`. No entanto, se você tiver o domínio personalizado `parking.different.example.com` e seu certificado tiver o SAN `*.example.com`, a solicitação falhará.
- O VPC Lattice oferece suporte a um nível de correspondência de domínio curinga. Isso significa que um curinga só pode ser usado como um subdomínio de primeiro nível e que protege apenas um nível de subdomínio. Por exemplo, se o SAN do seu certificado for `*.example.com`, não haverá suporte para `parking.*.example.com`.
- O VPC Lattice oferece suporte a um curinga por nome de domínio. Isso significa que `*.*.example.com` não é válido. Para obter mais informações, consulte [Solicitar um certificado público](#) no Guia do usuário do AWS Certificate Manager.
- O VPC Lattice é compatível somente com certificados com chaves RSA de 2.048 bits.
- O SSL/TLS certificado no ACM deve estar na mesma região do serviço VPC Lattice ao qual você o está associando.

Como proteger a chave privada do seu certificado

Quando você solicita um SSL/TLS certificado usando o ACM, o ACM gera um par de public/private chaves. Ao importar um certificado, você gera o par de chaves. A chave pública se torna parte do certificado. Para armazenar com segurança a chave privada, o ACM cria outra chave usando AWS KMS, chamada de chave KMS, com o alias `aws/acm`. AWS KMS usa essa chave para criptografar a chave privada do seu certificado. Para obter mais informações, consulte [Proteção de dados no AWS Certificate Manager](#), no Guia do usuário do AWS Certificate Manager .

O VPC Lattice usa o Gerenciador de AWS Conexões TLS, um serviço que só pode ser acessado por Serviços da AWS, para proteger e usar as chaves privadas do seu certificado. Quando você usa seu certificado ACM para criar um serviço VPC Lattice, o VPC Lattice associa seu certificado ao Gerenciador de Conexões TLS. AWS faz isso criando uma concessão em AWS KMS relação à sua chave AWS gerenciada. Essa concessão permite que o Gerenciador de Conexões TLS use AWS KMS para descriptografar a chave privada do seu certificado. O TLS Connection Manager usará o certificado e a chave privada descriptografada (texto simples) para estabelecer uma conexão segura (sessão SSL/TLS) com clientes de serviços do VPC Lattice. Quando o certificado for desassociado de um serviço VPC Lattice, a concessão será removida. Para obter mais informações, consulte [Concessões](#) no Guia do desenvolvedor do AWS Key Management Service .

Para obter mais informações, consulte [Criptografia inativa](#).

Excluir um serviço VPC Lattice

Para excluir um serviço VPC Lattice, primeiro você deverá excluir todas as associações que o serviço possa ter com qualquer rede de serviços. Se você excluir um serviço, todos os recursos relacionados ao serviço, como política de recursos, política de autenticação, receptores, regras de receptor e assinaturas de registros de acesso, também serão excluídos.

Para excluir um serviço usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviço.
3. Na página Serviços, selecione o serviço que você deseja excluir e, em seguida, escolha Ações, Excluir serviço.
4. Quando a confirmação for solicitada, escolha Excluir.

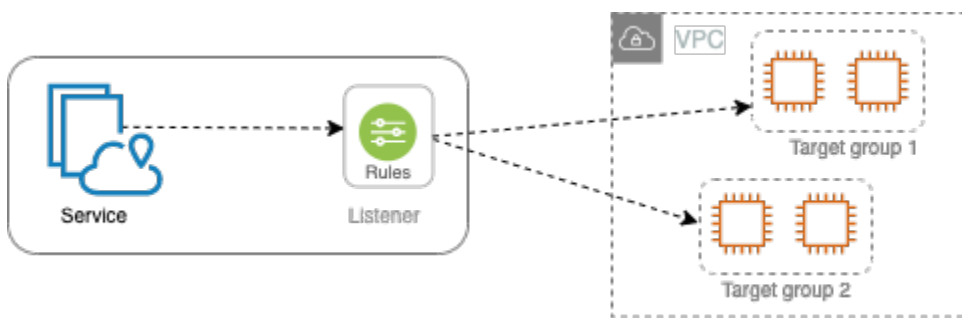
Para excluir um serviço usando o AWS CLI

Use o comando [delete-service](#).

Grupos de destino no VPC Lattice

Um grupo de destino do VPC Lattice é uma coleção de destinos, ou recursos computacionais, que executam sua aplicação ou serviço. Os tipos de destino compatíveis incluem EC2 instâncias, endereços IP, funções do Lambda, Application Load Balancers, tarefas do Amazon ECS e pods do Kubernetes. Você também pode anexar serviços existentes aos seus grupos de destino. Para obter mais informações sobre como usar o Kubernetes com o VPC Lattice, consulte o [Guia do usuário do AWS Gateway API Controller](#).

Cada grupo de destino é usado para rotear solicitações para um ou mais destinos registrados. Ao criar uma regra do receptor, especifique um grupo de destino e as condições. Quando uma condição da regra é atendida, o tráfego é encaminhado para o grupo de destino correspondente. Você pode criar grupos de destino diferentes para tipos de solicitações diferentes. Por exemplo, crie um grupo de destino para solicitações gerais e outros grupos de destino para solicitações que incluam condições de regras específicas, como um valor de caminho ou cabeçalho.



Você define as configurações de verificação de integridade para seu serviço por grupo de destino. Cada grupo de destino usa as configurações de verificação de integridade padrão, a menos que você as substitua ao criar o grupo de destino ou as modifique posteriormente. Após especificar um grupo de destino em uma regra para um receptor, o serviço vai monitorar continuamente a integridade de todos os destinos registrados no grupo de destino. O serviço vai rotear solicitações para os destinos registrados que estiverem íntegros.

Para especificar um grupo de destino em uma regra para um receptor de serviço, o grupo de destino deve estar na mesma conta do serviço.

Os grupos de destino do VPC Lattice são semelhantes aos grupos de destino fornecidos pelo Elastic Load Balancing, mas não são intercambiáveis.

Conteúdo

- [Criar um grupo de destino do VPC Lattice](#)

- [Registrar destinos com um grupo de destino do VPC Lattice](#)
- [Verificações de integridade para seus grupos de destino do VPC Lattice](#)
- [Configuração de roteamento](#)
- [Algoritmo de roteamento](#)
- [Target type](#)
- [Tipo de endereço IP](#)
- [Destinos HTTP no VPC Lattice](#)
- [Funções do Lambda como destinos no VPC Lattice](#)
- [Application Load Balancers como destinos no VPC Lattice](#)
- [Versão do protocolo](#)
- [Tags para seu grupo de destino do VPC Lattice](#)
- [Excluir um grupo de destino do VPC Lattice](#)

Criar um grupo de destino do VPC Lattice

Você registra seus destinos com um grupo de destino. Por padrão, o serviço VPC Lattice envia solicitações para destinos registrados usando a porta e o protocolo especificados por você para o grupo de destino. Você pode substituir essa porta ao registrar cada destino no grupo de destino.

Para rotear o tráfego aos destino em um grupo de destino, especifique o grupo de destino em uma ação quando você criar um listener ou uma regra para o listener. Para obter mais informações, consulte [Regras de receptor para seu serviço VPC Lattice](#). Você pode especificar o mesmo grupo de destino em vários receptores, mas esses receptores deverão pertencer ao mesmo serviço. Para usar um grupo de destino com um serviço, você deverá verificar se o grupo de destino não está sendo usado por um receptor para nenhum outro serviço.

Você pode adicionar ou remover destinos do seu grupo de destino a qualquer momento. Para obter mais informações, consulte [Registrar destinos com um grupo de destino do VPC Lattice](#). Você também pode modificar as configurações de verificação de integridade para seu grupo de destino. Para obter mais informações, consulte [Verificações de integridade para seus grupos de destino do VPC Lattice](#).

Criar um grupo de destino

Você pode criar um grupo de destino e, opcionalmente, registrar destinos da seguinte maneira.

Para criar um grupo de destino usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Selecione Criar grupo de destino.
4. Em Destino de backup, execute uma das seguintes ações:
 - Escolha Instâncias para registrar destinos por ID de instância.
 - Escolha Endereços IP para registrar destinos por endereço IP.
 - Escolha Função do Lambda para registrar uma função do Lambda como destino.
 - Escolha Application Load Balancer para registrar um Application Load Balancer como destino.
5. Em Nome do grupo de destino, insira um nome para o grupo de destino. Esse nome deve ser exclusivo para sua conta em cada AWS região, pode ter o máximo de 32 caracteres, deve conter apenas caracteres alfanuméricos ou hífens, e não deve iniciar nem terminar com hífen.
6. Nos itens Protocolo e Porta, você pode modificar os valores padrão conforme o necessário. O protocolo padrão é HTTPS e a porta padrão é 443.

Se o tipo de destino for função do Lambda, você não poderá especificar um protocolo ou uma porta.

7. Para o tipo de endereço IP, escolha IPv4 para registrar alvos com IPv4 endereços ou IPv6 para optar por registrar alvos com IPv6 endereços. Não é possível alterar essa configuração após a criação do grupo de destino.

Essa opção só estará disponível se o tipo de destino for endereços IP.

8. Em VPC, selecione uma nuvem privada virtual (VPC).

Essa opção não estará disponível se o tipo de destino for função do Lambda.

9. Em Versão do protocolo, modifique os valores padrão conforme necessário. O padrão é HTTP1.

Essa opção não estará disponível se o tipo de destino for função do Lambda.

10. Em Verificações de integridade, modifique as configurações padrão conforme necessário. Para obter mais informações, consulte [Verificações de integridade para seus grupos de destino do VPC Lattice](#).

As verificações de integridade não estarão disponíveis se o tipo de destino for função do Lambda.

11. Em Versão da estrutura de eventos do Lambda, escolha uma versão. Para obter mais informações, consulte [the section called “Receba eventos do serviço VPC Lattice”](#).

Essa opção só estará disponível se o tipo de destino for função do Lambda.

12. (Opcional) Para adicionar tags, escolha Tags, Adicionar nova tag e insira a chave e o valor da tag.
13. Escolha Próximo.
14. Em Registrar destinos, você pode pular essa etapa ou adicionar destinos da seguinte maneira:
 - Se o tipo de destino for Instâncias, selecione as instâncias, insira as portas e escolha Incluir como pendente abaixo.
 - Se o tipo de destino for Endereços IP, faça o seguinte:
 - a. Em Escolher uma rede, mantenha a VPC que você selecionou para o grupo de destino ou escolha Outro endereço IP privado.
 - b. Em Especificar IPs e definir portas, insira o endereço IP e as portas. A porta padrão é a porta do grupo de destino.
 - c. Escolha Incluir como pendente abaixo.
 - Se o tipo de destino for uma função do Lambda, escolha uma função do Lambda. Para criar uma função do Lambda, escolha Criar uma nova função do Lambda.
 - Se o tipo de destino for um Application Load Balancer, escolha um Application Load Balancer. Para criar um Application Load Balancer, escolha Criar um Application Load Balancer.
15. Selecione Criar grupo de destino.

Pode demorar alguns minutos para o VPC Lattice registrar os destinos. Para obter mais informações, consulte [Por que minhas alterações de DNS estão demorando tanto para se propagarem no Route 53 e nos resolvedores públicos?](#)

Para criar um grupo de destino usando a AWS CLI

Use o [create-target-group](#) comando para criar o grupo de destino e o comando [register-targets](#) para adicionar destinos.

Sub-redes compartilhadas

Os participantes podem criar grupos de destinos do VPC Lattice em uma VPC compartilhada. As seguintes regras se aplicam a sub-redes compartilhadas:

- Todas as partes de um serviço VPC Lattice, como receptores, grupos de destino e destinos, devem ser criadas pela mesma conta. É possível criá-las em sub-redes pertencentes ou compartilhadas com o proprietário do serviço VPC Lattice.
- Os destinos registrados com um grupo de destino devem ser criados pela mesma conta do grupo de destino.
- Somente o proprietário de uma VPC pode associar a VPC a uma rede de serviços. Os recursos dos participantes em uma VPC compartilhada associada a uma rede de serviços podem enviar solicitações para serviços associados à rede de serviços. No entanto, o administrador pode evitar isso usando grupos de segurança, políticas de rede ACLs ou de autenticação.

Para obter mais informações sobre os recursos compartilháveis do VPC Lattice, consulte

[Compartilhe entidades do VPC Lattice](#).

Registrar destinos com um grupo de destino do VPC Lattice

O seu serviço atua como um ponto único de contato para clientes e distribui o tráfego de entrada entre os destinos íntegros registrados. Você pode registrar cada destino com um ou mais grupos de destino.

Se a demanda da sua aplicação aumentar, você poderá registrar destinos adicionais com um ou mais grupos de destino para dar conta da demanda. O serviço inicia as solicitações de roteamento para um destino recém-registrado assim que o processo de registro é concluído e o destino passa pelas verificações de integridade iniciais.

Se a demanda na seu aplicativo diminuir, ou se você precisar fazer manutenção nos seus destinos, você pode cancelar o registro dos destinos dos seus grupos de destino. Cancelar o registro de um destino o remove do seu grupo de destino, mas não afeta o destino de outra forma. O serviço interrompe as solicitações de roteamento ao destino assim que o registro dele for cancelado. O destino entra no estado DRAINING até que as solicitações em andamento tenham sido concluídas. Você pode registrar o destino com o grupo de destino novamente quando estiver pronto para retomar o recebimento de solicitações.

O tipo de destino do seu grupo de destino determina como você registra os destinos com esse grupo de destino. Para obter mais informações, consulte [Target type](#).

Use os procedimentos de console a seguir para registrar ou cancelar o registro de destinos. Como alternativa, use os comandos [register-targets](#) e [deregister-targets](#) da AWS CLI.

Conteúdo

- [Registrar ou cancelar o registro de destinos por ID de Instância](#)
- [Registrar ou cancelar o registro de destinos por endereço IP](#)
- [Registrar ou cancelar o registro de uma função do Lambda](#)
- [Registrar ou cancelar o registro de um Application Load Balancer](#)

Registrar ou cancelar o registro de destinos por ID de Instância

As instâncias de destinos devem estar na nuvem privada virtual (VPC) que você especificou para o grupo de destino. A instância também deve estar no estado `running` quando você registrá-la.

Ao registrar destinos por ID de instância, você poderá usar o serviço com um grupo do Auto Scaling. Após anexar um grupo de destino a um grupo do Auto Scaling e o grupo aumentar a escala horizontalmente, as instâncias iniciadas pelo grupo do Auto Scaling serão registradas automaticamente no grupo de destino. Se você desanexar o grupo de destino do grupo do Auto Scaling, as instâncias terão o registro automaticamente cancelado do grupo de destino. Para obter mais informações, consulte [Rotear tráfego para o seu grupo do Auto Scaling com um grupo de destino do VPC Lattice no Guia do usuário do Amazon Auto EC2 Scaling](#).

Para registrar ou cancelar o registro de destinos por ID de instância usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Escolha a guia Destinos.
5. Para registrar instâncias, escolha Registrar destinos. Selecione as instâncias, insira a porta da instância e escolha Incluir como pendente abaixo. Após terminar de adicionar instâncias, escolha Registrar destinos.
6. Para cancelar o registro de instâncias, selecione as instâncias e escolha Cancelar registro.

Registrar ou cancelar o registro de destinos por endereço IP

Os endereços IP de destino devem ser das sub-redes da VPC que você especificou para o grupo de destino. Não é possível registrar os endereços IP de outro serviço na mesma VPC. Não é possível registrar endpoints da VPC ou endereços IP roteáveis publicamente.

Para registrar ou cancelar o registro de destinos por endereço IP usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Escolha a guia Destinos.
5. Para registrar endereços IP, escolha Registrar destinos. Para cada endereço IP, selecione a rede, insira o endereço IP e a porta e, em seguida, escolha Incluir como pendente abaixo. Quando você concluir a especificação de endereços, escolha Registrar destinos.
6. Para cancelar o registro de endereços IP, selecione os endereços IP e escolha Cancelar registro.

Registrar ou cancelar o registro de uma função do Lambda

Você pode registrar uma única função do Lambda com o grupo de destino. Se não precisar mais enviar tráfego para sua função Lambda, você poderá cancelar o registro. Depois de cancelar o registro de uma função Lambda, as solicitações em andamento falham com erros HTTP 5XX. É melhor criar um novo grupo de destino em vez de substituir a função do Lambda em um grupo de destino.

Para registrar ou cancelar o registro de funções do Lambda usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Escolha a guia Destinos.
5. Se não houver nenhuma função do Lambda registrada, escolha Registrar destino. Selecione a função do Lambda e escolha Registrar destino.
6. Para cancelar o registro de uma função Lambda, escolha Deregister (Cancelar registro). Quando receber a solicitação de confirmação, insira **confirm** e escolha Cancelar registro.

Registrar ou cancelar o registro de um Application Load Balancer

Você pode registrar um único Application Load Balancer com cada grupo de destino. Se não precisar mais enviar tráfego para seu balanceador de carga, você poderá cancelar seu registro. Após cancelar o registro de um balanceador de carga, as solicitações em andamento falharão com erros HTTP 5XX. É melhor criar um novo grupo de destino em vez de substituir o Application Load Balancer por um grupo de destino.

Para registrar ou cancelar o registro de um Application Load Balancer usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Escolha a guia Destinos.
5. Se não houver nenhum Application Load Balancer registrado, escolha Registrar destino. Selecione o Application Load Balancer e escolha Registrar destino.
6. Para cancelar o registro de um Application Load Balancer, escolha Cancelar registro. Quando receber a solicitação de confirmação, insira **confirm** e escolha Cancelar registro.

Verificações de integridade para seus grupos de destino do VPC Lattice

Seu serviço enviará periodicamente solicitações para seus destinos registrados a fim de testar o status deles. Esses testes se chamam verificações de integridade.

Cada serviço VPC Lattice encaminha as solicitações somente para os destinos íntegros. Cada serviço verifica a integridade de cada destino usando as configurações de verificação de integridade para os grupos de destino com os quais o destino está registrado. Após o destino ser registrado, ele deverá ser aprovado em uma verificação de integridade para ser considerado íntegro. Após a conclusão de cada verificação de integridade, o serviço fechará a conexão que foi estabelecida para a verificação de integridade.

Limitações e considerações

- Quando a versão do protocolo do grupo de destino for HTTP1, as verificações de integridade estarão habilitadas por padrão.

- Quando a versão do protocolo do grupo de destino for HTTP2, as verificações de integridade não estarão habilitadas por padrão. No entanto, você pode habilitar as verificações de integridade e definir manualmente a versão do protocolo como HTTP1 ou HTTP2.
- As verificações de integridade não oferecem suporte às versões do protocolo de grupo de destino gRPC. No entanto, se você habilitar as verificações de integridade, deverá especificar a versão do protocolo de verificação de integridade como HTTP1 ou HTTP2.
- As verificações de integridade não são compatíveis com grupos de destino do Lambda.
- As verificações de integridade não oferecem suporte a grupos de destino do Application Load Balancer. No entanto, você pode habilitar verificações de integridade para os destinos do seu Application Load Balancer usando o Elastic Load Balancing. Para obter mais informações, consulte [Verificações de integridade do grupo-alvo](#) no Guia do usuário dos Application Load Balancers.

Configurações de verificação de integridade

Você pode configurar verificações de integridade para os destinos em um grupo de destino conforme descrito na tabela a seguir. Os nomes das configurações usados na tabela são os nomes usados na API. O serviço envia uma solicitação de verificação de integridade a todos os destinos registrados a cada `HealthCheckIntervalSeconds` segundo de, usando a porta, o protocolo e o caminho de ping especificados. Cada solicitação de verificação de integridade é independente e o resultado dura por todo o intervalo. O tempo necessário para o destino responder não afeta o intervalo da próxima solicitação de verificação de integridade. Se a verificação de integridade exceder as falhas `UnhealthyThresholdCount` consecutivas, o serviço tornará o destino inoperante. Quando as verificações de integridade excederem os sucessos `HealthyThresholdCount` consecutivos, o serviço tornará o destino operacional novamente.

Configuração	Descrição
<code>HealthCheckProtocol</code>	O protocolo que o serviço usa ao executar verificações de integridade nos destinos. Os protocolos possíveis são HTTP e HTTPS. O padrão é o protocolo HTTP.
<code>HealthCheckPort</code>	A porta que o serviço usa ao executar verificações de integridade nos destinos. O padrão é usar a porta em que cada destino recebe o tráfego do serviço.

Configuração	Descrição
HealthCheckPath	O destino para verificações de integridade nos destinos. Se a versão do protocolo for HTTP1 ou HTTP2, especifique um URI válido (/path? consulta). O padrão é /.
HealthCheckTimeoutSeconds	O tempo, em segundos, durante o qual ausência de resposta de um destino significa uma falha na verificação de integridade. O intervalo é de 1 a 120 segundos. Se o tipo de destino for INSTANCE ou IP, o padrão será de 5 segundos. Especifique 0 para redefinir essa configuração para o valor padrão.
HealthCheckIntervalSeconds	A quantia aproximada de tempo, em segundos, entre as verificações de integridade de um destino individual. O intervalo é de 5 a 300 segundos. Se o tipo de destino for INSTANCE ou IP, o padrão será de 30 segundos. Especifique 0 para redefinir essa configuração para o valor padrão.
HealthyThresholdCount	O número de verificações de integridade bem-sucedidas consecutivas que são necessárias antes que um destino não íntegro seja considerado íntegro. O intervalo é de 2 a 10. O padrão é 5. Especifique 0 para redefinir essa configuração para o valor padrão.
UnhealthyThresholdCount	O número de falhas de verificações de integridade consecutivas necessárias para considerar um destino como não íntegro. O intervalo é de 2 a 10. O padrão é 2. Especifique 0 para redefinir essa configuração para o valor padrão.

Configuração	Descrição
Matcher	O códigos a serem usados ao verificar uma resposta bem-sucedida de um destino. Eles são chamados de códigos de sucesso no console. Se a versão do protocolo for HTTP1 ou HTTP2, os valores possíveis são de 200 a 499. Você pode especificar valores múltiplos (por exemplo, "200,202") ou um intervalo valores (por exemplo, "200-299"). O valor padrão é 200. No momento, não há suporte para a versão do protocolo de verificação de integridade para gRPC. No entanto, se a versão do protocolo do seu grupo de destino for gRPC, você poderá especificar HTTP1 ou versões de HTTP2 protocolo na configuração da verificação de integridade.

Verificar a integridade de seus destinos

Você pode verificar a integridade dos destinos registrados com seus grupos de destino.

Para verificar a integridade dos seus destinos usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Destinos, a coluna Status da integridade indica o status de cada destino. Se o status for qualquer valor diferente de `Healthy`, a coluna Detalhes do status de integridade conterá mais informações.

Para verificar a integridade dos seus destinos usando a AWS CLI

Use o comando [list-targets](#). O resultado desse comando contém o estado de integridade do destino. Se o status for qualquer valor diferente de `Healthy`, a saída também inclui um código de motivo.

Como receber notificações por e-mail sobre destinos não íntegros

Use CloudWatch alarmes para iniciar uma função do Lambda para enviar detalhes sobre destinos não íntegros.

Modificar as configurações de verificação de integridade

Você pode modificar as configurações de verificação de integridade do seu grupo de destino a qualquer momento.

Para modificar as configurações de verificação de integridade usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Verificações de integridade, na seção Configurações de verificação de integridade, selecione Editar.
5. Modifique as configurações de verificação de integridade conforme necessário.
6. Escolha Salvar alterações.

Para modificar as configurações de verificação de integridade usando a AWS CLI

Use o comando [update-target-group](#).

Configuração de roteamento

Por padrão, um serviço roteia solicitações para seus destinos usando o protocolo e o número da porta que você especificou ao criar o grupo de destino. Como alternativa, você pode substituir a porta usada para rotear o tráfego para um destino quando registrá-lo no grupo de destino.

Os grupos de destino são compatíveis com os seguintes protocolos e portas:

- Protocolos: HTTP, HTTPS, TCP
- Ports (Portas): 1-65535

Se um grupo de destino estiver configurado com o protocolo HTTPS ou usar as verificações de integridade de HTTPS, as conexões TLS com os destinos usarão a política de segurança do receptor. O VPC Lattice estabelecerá conexões TLS com os destinos usando certificados instalados nos destinos. O VPC Lattice não valida esses certificados. Portanto, é possível usar certificados autoassinados ou certificados que tenham expirado. O tráfego entre o VPC Lattice e os destinos é autenticado no nível do pacote e, portanto, não corre o risco de man-in-the-middle ataques ou de falsificações mesmo que os certificados nos destinos não sejam válidos.

Os grupos-alvo TCP são compatíveis somente com ouvintes [TLS](#).

Algoritmo de roteamento

Por padrão, o algoritmo de roteamento de ida e volta é usado para rotear solicitações para destinos íntegros.

Quando o serviço VPC Lattice recebe uma solicitação, ele usa o seguinte processo:

1. Avalia as regras de listener em ordem de prioridade para determinar qual regra aplicar.
2. Seleciona um destino do grupo de destino para a ação da regra usando o algoritmo padrão de ida e volta. O roteamento é realizado de forma independente para cada grupo de destino, até mesmo quando um destino é registrado com vários grupos de destino.

Se um grupo de destino contiver somente destinos não íntegros, as solicitações serão roteadas para todos os destinos, independentemente do seu status de integridade. Isso significa que a abertura do serviço VPC Lattice falhará se todos os destinos falharem nas verificações de integridade ao mesmo tempo. O efeito da falha na abertura é permitir o tráfego para todos os destinos com base no algoritmo de ida e volta, independentemente do seu estado de integridade.

Target type

Durante a criação de um grupo de destino, você especifica seu tipo de destino, que determina o tipo de destino especificado ao registrar destinos com esse grupo de destino. Depois de criar um grupo de destino, você não pode mudar o tipo de destino dele.

Os possíveis tipos de destino são os seguintes:

INSTANCE

Os destinos são especificados por ID de instância.

IP

Os destinos são endereços IP.

LAMBDA

O destino é uma função Lambda.

ALB

O destino é um Application Load Balancer.

Considerações

- Quando o tipo de destino for IP, será necessário especificar endereços IP das sub-redes da VPC para o grupo de destino. Se você precisar registrar endereços IP de fora dessa VPC, crie um grupo de destino do tipo ALB e registre os endereços IP com o Application Load Balancer.
- Quando o tipo de destino for IP, não será possível registrar endpoints da VPC ou endereços IP roteáveis publicamente.
- Quando o tipo de destino for LAMBDA, você poderá registrar uma única função do Lambda. Quando o serviço receber uma solicitação para a função do Lambda, ele invocará a função do Lambda. Se você quiser registrar várias funções do Lambda em um serviço, precisará usar vários grupos de destino.
- Quando o tipo de destino for ALB, você poderá registrar um único Application Load Balancer interno como o destino de até dois serviços VPC Lattice. Para fazer isso, registre o Application Load Balancer com dois grupos de destino separados, usados por dois serviços VPC Lattice diferentes. Além disso, o Application Load Balancer de destino deve ter pelo menos um receptor cuja porta corresponda à porta do grupo de destino.
- Você pode registrar automaticamente suas tarefas do ECS com um grupo de destino do VPC Lattice no lançamento. O grupo de destino deve ter um tipo de destino de IP. Para obter mais informações, consulte [Use o VPC Lattice com seus serviços do Amazon ECS no Amazon Elastic Container Service Developer Guide](#).

Como alternativa, registre o Application Load Balancer para seu serviço Amazon ECS com um grupo de destino do VPC Lattice do tipo ALB. Para obter mais informações, consulte [Usar balanceamento de carga para distribuir o tráfego do serviço Amazon ECS](#) no Guia do desenvolvedor do Amazon Elastic Container Service.

- Para registrar um pod do EKS como destino, use o [AWS Gateway API Controller](#), que obtém os endereços IP do serviço Kubernetes.

- Se o protocolo do grupo de destino for TCP, os únicos tipos de destino compatíveis serão INSTANCE e IP.

Tipo de endereço IP

Ao criar um grupo de destino com um tipo de destino IP, você pode especificar um tipo de endereço IP para o grupo de destino. Isso especificará o tipo de endereço que o balanceador de carga usa para enviar solicitações e verificações de integridade aos destinos. Os valores possíveis são IPv4 e IPv6. O padrão é IPv4.

Considerações

- Se você criar um grupo de destino com um tipo de endereço IP de IPv6, a VPC especificada para o grupo de destino deverá ter um intervalo de IPv6 endereços.
- Os endereços IP que você registrar em um grupo de destino deverão corresponder ao tipo de endereço IP do grupo de destino. Por exemplo, você não poderá registrar um IPv6 endereço com um grupo de destino se o tipo de endereço IP for IPv4.
- Os endereços IP que você registrar em um grupo de destino deverão estar no intervalo de endereço IP da VPC especificada para o grupo de destino.

Destinos HTTP no VPC Lattice

As solicitações HTTP e as respostas HTTP usam campos de cabeçalho para enviar informações sobre as mensagens HTTP. Os cabeçalhos HTTP são adicionados automaticamente. Os campos de cabeçalho são pares de nome-valor separados por dois pontos e separados por um retorno de carro (CR) e um avanço de linha (LF). Um conjunto padrão de campos de cabeçalho HTTP está definido na RFC 2616, [Cabeçalhos de mensagem](#). Também há a disponibilidade de cabeçalhos HTTP não padrão que são adicionados automaticamente e amplamente usados pelas aplicações. Por exemplo, há cabeçalhos HTTP não padrão com o prefixo x-forwarded.

Cabeçalhos x-forwarded

O Amazon VPC Lattice adiciona os seguintes cabeçalhos x-forwarded:

x-forwarded-for

O endereço IP de origem.

x-forwarded-for-port

A porta de destino.

x-forwarded-for-proto

O protocolo de conexão (http | https)

Cabeçalhos de identidade do chamador

O Amazon VPC Lattice adiciona os seguintes cabeçalhos de identidade do chamador:

x-amzn-lattice-identity

As informações de identidade. Os campos a seguir estarão presentes se a autenticação da AWS for bem-sucedida.

- **Principal**: a entidade principal autenticada.
- **PrincipalOrgID**: o ID da organização da entidade principal autenticada.
- **SessionName**: o nome da sessão autenticada.

Os campos a seguir estarão presentes se houver o uso de credenciais do Roles Anywhere e a autenticação for bem-sucedida.

- **X509Issuer/OU**: o emissor (OU).
- **X509SAN/DNS**: o nome alternativo do assunto (DNS).
- **X509SAN/NameCN**: o nome alternativo do emissor (nome/CN).
- **X509SAN/URI**: o nome alternativo do assunto (URI).
- **X509Subject/CN**: o nome do assunto (CN).

x-amzn-lattice-network

A VPC. O formato é o seguinte.

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

x-amzn-lattice-target

O destino. O formato é o seguinte.

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

Para obter informações sobre o recurso ARNs do VPC Lattice, consulte [Tipos de recursos definidos pelo Amazon VPC Lattice](#).

Os cabeçalhos de identidade do chamador não podem ser falsificados. O VPC Lattice retira esses cabeçalhos de todas as solicitações recebidas.

Funções do Lambda como destinos no VPC Lattice

Você pode registrar suas funções do Lambda como destinos com um grupo de destino do VPC Lattice e configurar uma regra de receptor para encaminhar solicitações ao grupo de destino para sua função do Lambda. Quando o serviço encaminhar a solicitação para um grupo de destino com uma função do Lambda como um destino, ele invocará sua função do Lambda e transmitirá o conteúdo da solicitação para a função do Lambda em formato JSON.

Limitações

- A função do Lambda e o grupo de destino devem estar na mesma conta e na mesma região.
- O tamanho máximo do corpo da solicitação que você pode enviar para uma função do Lambda é de 6 MB.
- O tamanho máximo da resposta JSON que a função do Lambda pode enviar é de 6 MB.
- O protocolo precisa ser HTTP ou HTTPS.

Preparar a função do Lambda

As recomendações a seguir se aplicam se você estiver usando sua função do Lambda com um serviço VPC Lattice.

Permissões para invocar a função do Lambda

Quando você criar o grupo de destino e registrar a função do Lambda usando o AWS Management Console ou a, o AWS CLI VPC Lattice adicionará as permissões necessárias à sua política de função do Lambda em seu nome.

Você também poderá adicionar permissões por conta própria usando a seguinte chamada de 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
```

Versionamento da função do Lambda

É possível registrar uma função Lambda por grupo de destino. Para garantir que você possa alterar sua função do Lambda e que o serviço VPC Lattice sempre invoque a versão atual da função do Lambda, crie um alias de função e inclua o alias no ARN da função ao registrar a função do Lambda com o serviço VPC Lattice. Para obter mais informações, consulte [Versões da função Lambda](#) e [Criar um alias para uma função Lambda](#) no Guia do desenvolvedor.AWS Lambda

Criar um grupo de destino para a função do Lambda

Crie um grupo de destino, que é usado no roteamento da solicitação. Se o conteúdo da solicitação corresponder a uma regra de receptor com uma ação para encaminhá-la para esse grupo de destino, o serviço VPC Lattice invocará a função do Lambda registrada.

Para criar um grupo de destino e registrar a função do Lambda usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Selecione Criar grupo de destino.
4. Em Selecionar um tipo de destino, escolha Função do Lambda.
5. Em Nome do grupo de destino, insira um nome para o grupo de destino.
6. Em Versão da estrutura de eventos do Lambda, escolha uma versão. Para obter mais informações, consulte [the section called “Receba eventos do serviço VPC Lattice”](#).
7. (Opcional) Para adicionar tags, escolha Tags, Adicionar nova tag e insira a chave e o valor da tag.
8. Escolha Próximo.
9. Em Lambda function (Função Lambda), siga um destes procedimentos
 - Selecione uma função do Lambda existente.
 - Crie uma nova função do Lambda e selecione-a.
 - Registre a função do Lambda mais posteriormente.
10. Selecione Criar grupo de destino.

Para criar um grupo de destino e registrar a função do Lambda usando a AWS CLI

Use os comandos [create-target-groupe](#) [register-targets](#).

Receba eventos do serviço VPC Lattice

O serviço VPC Lattice é compatível com solicitações de invocação do Lambda por HTTP e HTTPS. O serviço envia um evento no formato JSON e adiciona o cabeçalho X-Forwarded-For a cada solicitação.

Codificação base64

O serviço Base64 codifica o corpo se o cabeçalho content-encoding estiver presente e o tipo de conteúdo não for um dos seguintes:

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

Se o cabeçalho content-encoding não estiver presente, a codificação Base64 dependerá do tipo de conteúdo. Para os tipos de conteúdo acima, o serviço envia o corpo como está, sem a codificação Base64.

Formato de estrutura de evento

Ao criar ou atualizar um grupo de destino do tipo LAMBDA, você poderá especificar a versão da estrutura de eventos que sua função do Lambda recebe. As versões possíveis são V1 e V2.

Example Exemplo de evento: 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

O corpo da solicitação. Presente somente se o protocolo for HTTP, HTTPS ou gRPC.

headers

Os cabeçalhos HTTP da solicitação. Presente somente se o protocolo for HTTP, HTTPS ou gRPC.

identity

As informações de identidade. Os seguintes campos são possíveis.

- **principal**: a entidade principal autenticada. Presente somente se a AWS autenticação for bem-sucedida.

- `principalOrgID`: o ID da organização da entidade principal autenticada. Presente somente se a AWS autenticação for bem-sucedida.
- `sessionName`: o nome da sessão autenticada. Presente somente se a AWS autenticação for bem-sucedida.
- `sourceVpcArn`: o ARN da VPC na qual a solicitação teve origem. Presente somente se for possível identificar a VPC de origem.
- `type`— O valor é `AWS_IAM` se uma política de autenticação for usada e a AWS autenticação for bem-sucedida.

Se houver o uso de credenciais do Roles Anywhere e a autenticação for bem-sucedida, os campos a seguir serão possíveis.

- `x509IssuerOu`: o emissor (OU).
- `x509SanDns`: o nome alternativo do assunto (DNS).
- `x509SanNameCn`: o nome alternativo do emissor (nome/CN).
- `x509SanUri`: o nome alternativo do assunto (URI).
- `x509SubjectCn`: o nome do assunto (CN).

`isBase64Encoded`

Indica se o corpo foi codificado em base64. Presente somente se o protocolo for HTTP, HTTPS ou gRPC e o corpo da solicitação ainda não for uma string.

`method`

O método HTTP da solicitação. Presente somente se o protocolo for HTTP, HTTPS ou gRPC.

`path`

O caminho da solicitação. Presente somente se o protocolo for HTTP, HTTPS ou gRPC.

`queryStringParameters`

Os parâmetros da string de consulta HTTP. Presente somente se o protocolo for HTTP, HTTPS ou gRPC.

`serviceArn`

O ARN do serviço que recebe a solicitação.

`serviceNetworkArn`

O ARN da rede de serviço que entrega a solicitação.

targetGroupArn

O ARN do grupo de destino que recebe a solicitação.

timeEpoch

A hora em microssegundos.

Example Exemplo de evento: 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
}
```

Responder ao serviço VPC Lattice

A resposta da função do Lambda deve incluir o status de codificação Base64, o código do status e os cabeçalhos. É possível omitir o corpo.

Para incluir um conteúdo binário no corpo da resposta, você deve codificar o conteúdo em Base64 e definir `isBase64Encoded` como `true`. O serviço decodifica o conteúdo para recuperar o conteúdo binário e o envia ao cliente no corpo da resposta HTTP.

O serviço VPC Lattice não respeita hop-by-hop cabeçalhos, como `ou. Connection Transfer-Encoding`. É possível omitir o cabeçalho `Content-Length` porque o serviço o calcula antes de enviar respostas aos clientes.

Veja a seguir um exemplo de resposta de uma função do Lambda:

```
{
  "isBase64Encoded": false,
  "statusCode": 200,
  "statusDescription": "200 OK",
  "headers": {
    "Set-cookie": "cookies",
```

```
    "Content-Type": "application/json"
  },
  "body": "Hello from Lambda (optional)"
}
```

Cabeçalhos de vários valores

O VPC Lattice oferece suporte a solicitações de um cliente ou respostas de uma função do Lambda que contêm cabeçalhos com vários valores ou contêm o mesmo cabeçalho várias vezes. O VPC Lattice passa todos os valores para os destinos.

No exemplo a seguir, há dois cabeçalhos nomeados header1 com valores diferentes.

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

Com uma estrutura de eventos V2, o VPC Lattice envia os valores em uma lista. Por exemplo:

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

Com uma estrutura de eventos V1, o VPC Lattice combina os valores em uma única string. Por exemplo:

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

parâmetros de string de consulta

O VPC Lattice oferece suporte a parâmetros de consulta com vários valores para a mesma chave.

No exemplo a seguir, há dois parâmetros nomeados QS1 com valores diferentes.

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

Com uma estrutura de eventos V2, o VPC Lattice envia os valores em uma lista. Por exemplo:

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

Com uma estrutura de eventos V1, o VPC Lattice usa o último valor passado. Por exemplo:

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

Cancelar o registro da função do Lambda

Se não precisar mais enviar tráfego para sua função Lambda, você poderá cancelar o registro. Depois de cancelar o registro de uma função Lambda, as solicitações em andamento falham com erros HTTP 5XX.

Para substituir uma função Lambda, recomendamos criar um grupo de destino, registrar a nova função com o novo grupo de destino e atualizar as regras do listener para usar o novo grupo de destino em vez do existente.

Para cancelar o registro de funções do Lambda usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Targets (Destinos), selecione Deregister (Cancelar registro).
5. Quando receber a solicitação de confirmação, insira **confirm** e escolha Cancelar registro.

Para cancelar o registro da função do Lambda usando a AWS CLI

Use o comando [deregister-targets](#).

Application Load Balancers como destinos no VPC Lattice

Você pode criar um grupo de destino do VPC Lattice, registrar um único Application Load Balancer interno como destino e configurar seu serviço VPC Lattice para encaminhar o tráfego para esse grupo de destino. Nesse cenário, o Application Load Balancer assume a decisão de roteamento assim que o tráfego chega até ele. Essa configuração permite que você use o recurso de roteamento baseado em solicitações da camada 7 do Application Load Balancer em combinação com recursos compatíveis com o VPC Lattice, como autenticação e autorização do IAM e conectividade entre contas. VPCs

Limitações

- Você pode registrar um único Application Load Balancer interno como destino em um grupo de destino do VPC Lattice do tipo ALB.

- Você pode registrar um Application Load Balancer como destino de até dois grupos de destino do VPC Lattice, usados por dois serviços VPC Lattice diferentes.
- O VPC Lattice não fornece verificações de integridade para nenhum grupo de destino do tipo ALB. No entanto, você pode configurar verificações de integridade de maneira independente no nível do balanceador de carga para os destinos no Elastic Load Balancing. Para obter mais informações, consulte [Verificações de integridade do grupo-alvo](#) no Guia do usuário para Application Load Balancers

Pré-requisitos

Crie um Application Load Balancer para registrar como destino com seu grupo de destino do VPC Lattice. O balanceador de carga deve atender aos seguintes critérios:

- O esquema do balanceador de carga deve ser Interno.
- O Application Load Balancer deve estar na mesma conta do grupo de destino do VPC Lattice e estar no estado Ativo.
- O Application Load Balancer deve estar na mesma VPC do grupo de destino do VPC Lattice.
- Você pode usar receptores HTTPS no Application Load Balancer para encerrar o TLS, mas somente se o serviço VPC Lattice usar o mesmo certificado SSL/TLS do balanceador de carga.
- Para preservar o IP do cliente do serviço VPC Lattice no cabeçalho da solicitação X-Forwarded-For, você deverá definir o atributo `routing.http.xff_header_processing.mode` do Application Load Balancer como Preserve. Se o valor for Preserve, o balanceador de carga deverá preservar o cabeçalho X-Forwarded-For na solicitação HTTP e enviá-lo para o destino sem nenhuma alteração.

Para obter mais informações, consulte [Criar um Application Load Balancer](#) no Guia do usuário dos Application Load Balancers.

Etapa 1: criar um grupo de destino do tipo ALB

Siga o procedimento abaixo para criar o grupo de destino. Observe que o VPC Lattice não oferece suporte a verificações de integridade para ALB grupos de destino. No entanto, você pode configurar verificações de integridade para os grupos de destino do seu Application Load Balancer. Para obter mais informações, consulte [Verificações de integridade do grupo-alvo](#) no Guia do usuário dos Application Load Balancers.

Para criar o grupo de destino

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Selecione Criar grupo de destino.
4. Na página Especificar detalhes do grupo de destino, em Configuração básica, escolha Application Load Balancer como o tipo de destino.
5. Em Nome do grupo de destino, insira um nome para o grupo de destino.
6. Para Protocol (Protocolo), escolha **HTTP** ou **HTTPS**. O protocolo do grupo de destino deverá corresponder ao protocolo do receptor do seu Application Load Balancer interno.
7. Em Porta, especifique a porta para seu grupo de destino. Essa porta deverá corresponder à porta do receptor do Application Load Balancer interno. Como alternativa, você pode adicionar uma porta de receptor no Application Load Balancer interno para corresponder à porta do grupo de destino especificada aqui.
8. Em VPC, selecione a mesma nuvem privada virtual (VPC) que você selecionou ao criar o Application Load Balancer interno. Essa deverá ser a VPC que contém seus recursos do VPC Lattice.
9. Em Versão do protocolo, escolha a versão do protocolo compatível com seu Application Load Balancer.
10. (Opcional) Adicione qualquer tag necessária.
11. Escolha Próximo.

Etapa 2: registrar o Application Load Balancer como destino

Você pode registrar o balanceador de carga como destino agora ou mais tarde.

Para registrar um Application Load Balancer como destino

1. Escolha Registrar agora.
2. Em Application Load Balancer, escolha seu Application Load Balancer interno.
3. Em Porta, mantenha a porta padrão ou especifique uma porta diferente conforme necessário. Essa porta deverá corresponder à porta de um receptor existente em seu Application Load Balancer. Se você continuar sem uma porta correspondente, o tráfego não alcançará seu Application Load Balancer.

4. Selecione Criar grupo de destino.

Versão do protocolo

Por padrão, os serviços enviam solicitações para destinos usando HTTP/1.1. Você pode usar a versão do protocolo para enviar solicitações aos destinos usando HTTP/2 ou gRPC.

A tabela a seguir resume o resultado das combinações de protocolo de solicitação e versão de protocolo do grupo de destino.

Protocolo de solicitação	Versão do protocolo	Resultado
HTTP/1.1	HTTP/1.1	Bem-sucedida
HTTP/2	HTTP/1.1	Bem-sucedida
gRPC	HTTP/1.1	Erro
HTTP/1.1	HTTP/2	Erro
HTTP/2	HTTP/2	Bem-sucedida
gRPC	HTTP/2	Sucesso se os destinos forem compatíveis com gRPC
HTTP/1.1	gRPC	Erro
HTTP/2	gRPC	Sucesso se for uma solicitação POST
gRPC	gRPC	Bem-sucedida

Considerações sobre a versão do protocolo gRPC

- O único protocolo de receptor compatível é HTTPS.
- Só há compatibilidade com os tipos de destino INSTANCE e IP.
- O serviço analisa as solicitações do gRPC e encaminha as chamadas do gRPC para os grupos de destino adequados com base no pacote, serviço e método.

- Não é possível usar funções do Lambda como destino.

Considerações sobre a versão do protocolo HTTP/2

- O único protocolo de receptor compatível é HTTPS. Você pode escolher HTTP ou HTTPS para o protocolo do grupo de destino.
- As únicas regras de receptor suportadas são encaminhar e resposta fixa.
- Só há compatibilidade com os tipos de destino INSTANCE e IP.
- O serviço é compatível com streaming proveniente dos clientes. O serviço não é compatível com streaming para os destinos.

Tags para seu grupo de destino do VPC Lattice

As tags ajudam a categorizar seus grupos de destino de diferentes formas, como por finalidade, por proprietário ou por ambiente.

Você pode adicionar várias tags a um grupo de destino. As chaves de tag devem ser exclusivas para cada grupo de destino. Se você adicionar uma tag com uma chave que já esteja associada ao grupo de destino, o valor dessa tag será atualizado.

Quando não precisar mais de uma tag, você poderá removê-la.

Restrições

- Número máximo de tags por recurso: 50
- Comprimento máximo da chave: 127 caracteres Unicode
- Comprimento máximo de valor: 255 caracteres Unicode
- As chaves e valores das tags diferenciam maiúsculas de minúsculas. Os caracteres permitidos são letras, espaços e números representáveis em UTF-8, além dos seguintes caracteres especiais: + - = . _ : / @. Não use espaços no início nem no fim.
- Não use o `aws:` prefixo no nome nem no valor das suas tags, pois ele é reservado para AWS uso da. Você não pode editar nem excluir nomes ou valores de tag com esse prefixo. As tags com esse prefixo não contam para as tags por limite de recurso.

Para atualizar as tags de um grupo de destino usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Grupos de destino.
3. Selecione o nome do grupo de destino para abrir sua página de detalhes.
4. Escolha a guia Tags.
5. Para adicionar uma tag, escolha Adicionar tags e insira a chave e o valor da tag. Para adicionar outra tag, escolha Adicionar nova tag novamente. Quando terminar de adicionar etiquetas, escolha Save changes (Salvar alterações).
6. Para excluir uma tag, marque a caixa de seleção da tag e escolha Excluir. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para atualizar as tags de um grupo de destino usando a AWS CLI

Use os comandos [tag-resource](#) e [untag-resource](#).

Excluir um grupo de destino do VPC Lattice

Você pode excluir um grupo de destino se ele não for mencionado pelas ações de encaminhamento de nenhuma regra de receptor. A exclusão de um grupo de destino não afeta os destinos registrados no grupo de destino. Você pode parar ou terminar uma EC2 instância registrada, poderá interrompê-la ou encerrá-la.

Para excluir um grupo de destino usando o console

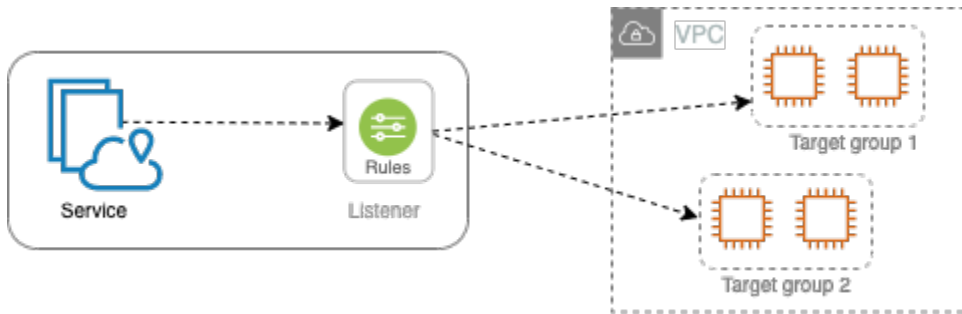
1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Grupos de destino.
3. Marque a caixa de seleção do grupo de destino e selecione Ações, Excluir.
4. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para excluir um grupo de destino usando a AWS CLI

Use o comando [delete-target-group](#).

Receptores do seu serviço VPC Lattice

Antes de começar a usar seu serviço VPC Lattice, você deve adicionar um listener. Um receptor é um processo que verifica solicitações de conexão usando o protocolo e a porta configurados por você. As regras que você define para um receptor determinam como o serviço roteia solicitações para seus destinos registrados.



Conteúdo

- [Configuração do receptor](#)
- [Receptores HTTP para serviços VPC Lattice](#)
- [Receptores HTTPS para serviços VPC Lattice](#)
- [Receptores TLS para serviços VPC Lattice](#)
- [Regras de receptor para seu serviço VPC Lattice](#)
- [Exclua um receptor do seu serviço VPC Lattice](#)

Configuração do receptor

Os listeners são compatíveis com os seguintes protocolos e portas:

- Protocolos: HTTP, HTTPS, TLS
- Ports (Portas): 1-65535

Se o protocolo do receptor for HTTPS, o VPC Lattice provisionará e gerenciará um certificado TLS associado ao FQDN gerado pelo VPC Lattice. O VPC Lattice é compatível com TLS em HTTP/1.1 e HTTP/2. Quando você configurar um serviço com um receptor HTTPS, o VPC Lattice determinará automaticamente o protocolo HTTP usando a Application-Layer Protocol Negotiation (ALPN). Se a

ALPN estiver ausente, o VPC Lattice será padronizado para HTTP/1.1. Para obter mais informações, consulte [Listeners HTTPS](#).

O VPC Lattice pode escutar em HTTP, HTTPS, HTTP/1.1 e HTTP/2 e se comunicar com destinos em qualquer um desses protocolos e versões. Não exigimos que os protocolos do receptor e do grupo de destino correspondam. O VPC Lattice gerencia todo o processo de upgrade e downgrade entre protocolos e versões. Para obter mais informações, consulte [Versão do protocolo](#).

Você pode criar um ouvinte TLS para garantir que seu aplicativo decodifique o tráfego criptografado em vez do VPC Lattice. Para obter mais informações, consulte [ouvintes TLS](#).

O VPC Lattice não é compatível. WebSockets

Receptores HTTP para serviços VPC Lattice

Um listener é um processo que verifica se há solicitações de conexão. Você pode definir um receptor ao criar seu serviço VPC Lattice. Você pode adicionar receptores ao seu serviço a qualquer momento.

As informações dessa página ajudam você a criar um receptor HTTP para o serviço. Para obter informações sobre a criação de ouvintes que usam outros protocolos, consulte [Listeners HTTPS](#) e [ouvintes TLS](#).

Pré-requisitos

- Para adicionar uma ação de encaminhamento à regra do receptor padrão, você deverá especificar um grupo de destino disponível no VPC Lattice. Para obter mais informações, consulte [Criar um grupo de destino do VPC Lattice](#).
- Você pode especificar o mesmo grupo de destino em vários receptores, mas esses receptores deverão pertencer ao mesmo serviço. Para usar um grupo de destino com um serviço VPC Lattice, você deve verificar se ele não está sendo usado por um receptor para nenhum outro serviço VPC Lattice.

Adicionar um receptor HTTP

Você pode adicionar receptores e regras ao seu serviço a qualquer momento. Você configura um receptor com um protocolo e uma porta para as conexões de clientes com o serviço, e um grupo

de destino do VPC Lattice para a regra padrão do receptor. Para obter mais informações, consulte [Configuração do receptor](#).

Para adicionar um listener HTTPS usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Na guia Roteamento, escolha Adicionar receptor.
5. Em Nome do receptor, você pode fornecer um nome de receptor personalizado ou usar o protocolo e a porta do seu receptor como o nome do receptor. Um nome personalizado que você especificar pode ter até 63 caracteres e deve ser exclusivo para cada serviço em sua conta. Os caracteres válidos são a-z, 0-9 e hífens (-). Você não pode usar um hífen como primeiro ou último caractere, nem imediatamente após outro hífen. Não é possível alterar o nome depois de criá-lo.
6. Em Protocolo: porta, escolha HTTP e insira um número de porta.
7. Em Ação padrão, escolha o grupo de destino do VPC Lattice para receber tráfego e escolha o peso a ser atribuído a esse grupo de destino. O peso que você atribui a um grupo de destino define sua prioridade para o recebimento de tráfego. Por exemplo, se dois grupos de destino tiverem o mesmo peso, cada grupo de destino receberá metade do tráfego. Se você tiver especificado apenas um grupo de destino, 100% do tráfego será enviado para um grupo de destino.

Opcionalmente, você poderá adicionar outro grupo de destino para a ação padrão. Escolha Adicionar ação e, em seguida, escolha um grupo de destino e especifique seu peso.

8. (Opcional) Para adicionar outra regra, escolha Adicionar regra e insira um nome, uma prioridade, uma condição e uma ação para a regra.

Você pode atribuir um número de prioridade entre 1 e 100 a cada regra. Um listener não pode ter várias regras com a mesma prioridade. As regras são avaliadas em ordem de prioridade, do valor mais baixo para o valor mais alto. A regra padrão é avaliada por último. Para obter mais informações, consulte [Regras do listener](#).

9. (Opcional) Para adicionar tags, expanda Tags de receptor, escolha Adicionar nova tag e insira uma chave de tag e valor de tag.
10. Revise sua configuração e escolha Adicionar.

Para adicionar um ouvinte HTTP usando o AWS CLI

Use o comando [create-listener](#) para criar o receptor com uma regra padrão, e o comando [create-rule](#) para definir as regras de receptor adicionais.

Receptores HTTPS para serviços VPC Lattice

Um listener é um processo que verifica se há solicitações de conexão. Você define um receptor ao criar seu serviço. Você pode adicionar receptores ao seu serviço no VPC Lattice a qualquer momento.

Você pode criar um listener HTTPS, que usa o TLS versão 1.2 ou o TLS versão 1.3 para encerrar conexões HTTPS diretamente com o VPC Lattice. O VPC Lattice provisionará e gerenciará um certificado TLS associado ao FQDN gerado pelo VPC Lattice. O VPC Lattice é compatível com TLS em HTTP/1.1 e HTTP/2. Quando você configurar um serviço com um receptor HTTPS, o VPC Lattice determinará automaticamente o protocolo HTTP com a Application-Layer Protocol Negotiation (ALPN). Se a ALPN estiver ausente, o VPC Lattice será padronizado para HTTP/1.1.

O VPC Lattice usa uma arquitetura de multilocalização, o que significa que ele pode hospedar vários serviços no mesmo endpoint. O VPC Lattice usa TLS com Server Name Indication (SNI – Indicação de nome do servidor) para cada solicitação de cliente. Não há suporte para Encrypted Client Hello (ECH) e Encrypted Server Name Indication (ESNI).

O VPC Lattice pode escutar em HTTP, HTTPS, HTTP/1.1 e HTTP/2 e se comunicar com destinos em qualquer um desses protocolos e versões. Essas configurações de receptor e grupo de destino não precisam ser correspondentes. O VPC Lattice gerencia todo o processo de upgrade e downgrade entre protocolos e versões. Para obter mais informações, consulte [Versão do protocolo](#).

Para garantir que seu aplicativo decodifique o tráfego, crie um ouvinte TLS em vez disso. Com a passagem TLS, o VPC Lattice não encerra o TLS. Para obter mais informações, consulte [ouvintes TLS](#).

Sumário

- [Política de segurança](#)
- [Política de ALPN](#)
- [Adicionar um receptor HTTPS](#)

Política de segurança

O VPC Lattice usa uma política de segurança que é uma combinação do protocolo TLSv1 1.2 e uma lista de cifras SSL/TLS. O protocolo estabelece uma conexão segura entre um cliente e o servidor, ajudando a garantir que todos os dados transmitidos entre o cliente e seu serviço no VPC Lattice sejam privados. A cifra é um algoritmo de criptografia que usa chaves de criptografia para criar uma mensagem codificada. Os protocolos usam várias cifras para criptografar dados. Durante o processo de negociação de conexão, o cliente e o VPC Lattice apresentam uma lista de cifras e protocolos que cada um suporta, em ordem de preferência. Por padrão, a primeira cifra na lista do servidor que corresponder a qualquer uma das cifras do cliente é selecionada para a conexão segura.

O VPC Lattice usa as seguintes cifras TLS 1.2 SSL/TLS nesta ordem de preferência:

- 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

O VPC Lattice também usa as seguintes cifras TLS 1.3 SSL/TLS nesta ordem de preferência:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Política de ALPN

A Application-Layer Protocol Negotiation (ALPN) é uma extensão TLS que é enviada nas mensagens Hello iniciais de handshake de TLS. ALPN permite que a camada do aplicativo negocie quais protocolos devem ser usados em uma conexão segura, como HTTP/1 e HTTP/2.

Quando o cliente inicia uma conexão ALPN, o serviço VPC Lattice compara a lista de preferências de ALPN do cliente com a política de ALPN. Se o cliente oferecer suporte a um protocolo da política de

ALPN, o serviço VPC Lattice estabelecerá a conexão com base na lista de preferências da política de ALPN. Caso contrário, o serviço não usará a ALPN.

O VPC Lattice oferece suporte à seguinte política de ALPN:

HTTP2Preferred

Prefira HTTP/2 em vez de HTTP/1.1. A lista de preferência de ALPN é h2, http/1.1.

Adicionar um receptor HTTPS

Você configura um receptor com um protocolo e uma porta para as conexões de clientes com o serviço, e um grupo de destino para a regra padrão do receptor. Para obter mais informações, consulte [Configuração do receptor](#).

Pré-requisitos

- Para adicionar uma ação de encaminhamento à regra do receptor padrão, você deverá especificar um grupo de destino disponível no VPC Lattice. Para obter mais informações, consulte [Criar um grupo de destino do VPC Lattice](#).
- Você pode especificar o mesmo grupo de destino em vários receptores, mas esses receptores deverão pertencer ao mesmo serviço VPC Lattice. Para usar um grupo de destino com um serviço VPC Lattice, você deve verificar se ele não está sendo usado por um receptor para nenhum outro serviço VPC Lattice.
- Você pode usar o certificado fornecido pelo VPC Lattice ou importar seu próprio certificado para o AWS Certificate Manager. Para obter mais informações, consulte [the section called “BYOC”](#).

Adicionar um listener HTTPS usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Na guia Roteamento, escolha Adicionar receptor.
5. Em Nome do receptor, você pode fornecer um nome de receptor personalizado ou usar o protocolo e a porta do seu receptor como o nome do receptor. Um nome personalizado que você especificar pode ter até 63 caracteres e deve ser exclusivo para cada serviço em sua conta.

Os caracteres válidos são a-z, 0-9 e hífens (-). Você não pode usar um hífen como primeiro ou último caractere, nem imediatamente após outro hífen. Não é possível alterar o nome de um receptor após criá-lo.

6. Em Protocolo: porta, escolha HTTPS e insira um número de porta.
7. Em Ação padrão, escolha o grupo de destino do VPC Lattice para receber tráfego e escolha o peso a ser atribuído a esse grupo de destino. O peso que você atribui a um grupo de destino define sua prioridade para o recebimento de tráfego. Por exemplo, se dois grupos de destino tiverem o mesmo peso, cada grupo de destino receberá metade do tráfego. Se você tiver especificado apenas um grupo de destino, 100% do tráfego será enviado para um grupo de destino.

Opcionalmente, você poderá adicionar outro grupo de destino para a ação padrão. Escolha Adicionar ação e, em seguida, escolha um grupo de destino e especifique seu peso.

8. (Opcional) Para adicionar outra regra, escolha Adicionar regra e insira um nome, uma prioridade, uma condição e uma ação para a regra.

Você pode atribuir um número de prioridade entre 1 e 100 a cada regra. Um listener não pode ter várias regras com a mesma prioridade. As regras são avaliadas em ordem de prioridade, do valor mais baixo para o valor mais alto. A regra padrão é avaliada por último. Para obter mais informações, consulte [Regras do listener](#).

9. (Opcional) Para adicionar tags, expanda Tags de receptor, escolha Adicionar nova tag e insira uma chave de tag e valor de tag.
10. Em Configurações de certificado de receptor HTTPS, se você não tiver especificado um nome de domínio personalizado ao criar o serviço, o VPC Lattice vai gerar automaticamente um certificado TLS para proteger o tráfego que passa pelo receptor.

Se você tiver criado o serviço com um nome de domínio personalizado, mas não tiver especificado um certificado correspondente, poderá fazer isso agora escolhendo o certificado em Certificado SSL/TLS personalizado. Caso contrário, o certificado que você especificou ao criar o serviço já estará escolhido.

11. Revise sua configuração e escolha Adicionar.

Para adicionar um listener HTTPS usando a AWS CLI

Use o comando [create-listener](#) para criar o receptor com uma regra padrão, e o comando [create-rule](#) para definir as regras de receptor adicionais.

Receptores TLS para serviços VPC Lattice

Um listener é um processo que verifica se há solicitações de conexão. Você pode definir um receptor ao criar seu serviço VPC Lattice. Você pode adicionar receptores ao seu serviço a qualquer momento.

Você pode criar um ouvinte TLS para que o VPC Lattice transmita tráfego criptografado para seus aplicativos sem descriptografá-lo.

Se você preferir que o VPC Lattice descriptografe o tráfego criptografado e envie tráfego não criptografado para seus aplicativos, crie um ouvinte HTTPS em vez disso. Para obter mais informações, consulte [Listeners HTTPS](#).

Considerações

As seguintes considerações se aplicam aos receptores TLS:

- O serviço VPC Lattice deve ter um nome de domínio personalizado. O nome de domínio personalizado do serviço é usado como uma correspondência de Indicação de Nome de Serviço (SNI). Se você especificou um certificado ao criar o serviço, ele não será usado.
- A única regra permitida para um ouvinte TLS é a regra padrão.
- A ação padrão para um ouvinte TLS deve ser uma ação de encaminhamento para um grupo-alvo TCP.
- Por padrão, as verificações de saúde estão desativadas para grupos-alvo TCP. Se você habilitar verificações de integridade para um grupo-alvo TCP, deverá especificar um protocolo e uma versão do protocolo.
- Os ouvintes TLS roteiam solicitações usando o campo SNI da mensagem client-hello. Você pode usar certificados curinga e SAN em seus destinos se a condição correspondente corresponder exatamente ao client-hello.
- Como todo o tráfego permanece criptografado do cliente para o destino, o VPC Lattice não consegue ler os cabeçalhos HTTP e não pode inserir ou remover cabeçalhos HTTP. Portanto, com um ouvinte TLS, existem as seguintes limitações:
 - A duração da conexão é limitada a 10 minutos
 - As políticas de autenticação são limitadas a diretores anônimos
 - Os alvos Lambda não são compatíveis
- Não há suporte ao Encrypted Client Hello (ECH) não é compatível.

- Não há suporte à indicação de nome de servidor criptografado (ESNI) não é compatível.

Adicionar um listener TLS

Você configura um receptor com um protocolo e uma porta para as conexões de clientes com o serviço, e um grupo de destino para a regra padrão do receptor. Para obter mais informações, consulte [Configuração do receptor](#).

Para adicionar um receptor TLS usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Na guia Roteamento, escolha Adicionar receptor.
5. Em Nome do receptor, você pode fornecer um nome de receptor personalizado ou usar o protocolo e a porta do seu receptor como o nome do receptor. Um nome personalizado que você especificar pode ter até 63 caracteres e deve ser exclusivo para cada serviço em sua conta. Os caracteres válidos são a-z, 0-9 e hífens (-). Você não pode usar um hífen como primeiro ou último caractere, nem imediatamente após outro hífen. Não é possível alterar o nome de um receptor após criá-lo.
6. Para Protocolos, escolha TLS. Em Porta, digite um número da porta.
7. Em Encaminhar para o grupo de destino, escolha um grupo de destino do VPC Lattice que usa o protocolo TCP para receber o tráfego e escolha o peso a ser atribuído a esse grupo de destino. Opcionalmente, você poderá adicionar outro grupo de destino. Escolha Adicionar grupo de destino e, em seguida, escolha um grupo de destino e insira seu peso.
8. (Opcional) Para adicionar tags, expanda Tags de receptor, escolha Adicionar nova tag e insira uma chave de tag e valor de tag.
9. Revise sua configuração e escolha Adicionar.

Para adicionar um ouvinte TLS usando o AWS CLI

Use o comando [create-listener](#) para criar um ouvinte com uma regra padrão. Especifique o protocolo TLS_PASSTHROUGH.

Regras de receptor para seu serviço VPC Lattice

Cada receptor tem uma regra padrão e regras adicionais que você pode definir. Cada regra consiste em uma prioridade, uma ou mais ações e uma ou mais condições. Você pode adicionar ou editar regras a qualquer momento.

Conteúdo

- [Regras padrão](#)
- [Prioridade das regras](#)
- [Ação da regra](#)
- [Condições de regra](#)
- [Adicionar uma regra](#)
- [Atualizar uma regra](#)
- [Excluir uma regra](#)

Regras padrão

Ao criar um listener, você define as ações para a regra padrão. As regras padrão não podem ter condições. Se nenhuma das condições das regras do listener for atendida, a ação para a regra padrão será executada.

Prioridade das regras

Cada regra tem uma prioridade. As regras são avaliadas em ordem de prioridade, do valor mais baixo para o valor mais alto. A regra padrão é avaliada por último. Você pode alterar a prioridade de uma regra não padrão a qualquer momento. Você não pode alterar a prioridade da regra padrão.

Ação da regra

Os receptores dos serviços VPC Lattice oferecem suporte a ações de encaminhamento e ações de resposta fixa.

Ações de encaminhamento

É possível usar ações `forward` a fim de rotear solicitações para um ou mais grupos de destino do VPC Lattice. Se especificar vários grupos de destino para uma ação `forward`, você deverá especificar um peso para cada grupo de destino. Cada peso de grupo de destino é um valor de 0 a

999. As solicitações que correspondem a uma regra de listener com grupos de destino ponderados são distribuídas para esses grupos de destino com base em seus pesos. Por exemplo, se você especificar dois grupos de destino, cada um com um peso de 10, cada grupo de destino receberá metade das solicitações. Se você especificar dois grupos de destino, um com peso de 10 e o outro com peso de 20, o grupo de destino com peso de 20 receberá duas vezes mais solicitações do que o outro grupo de destino.

Ações de resposta fixa

Você pode usar ações de `fixed-response` para descartar solicitações do cliente e retornar uma resposta HTTP personalizada. Você pode usar essa ação para retornar um código de resposta 404 ou 500.

Example Exemplo de ação de resposta fixa para a AWS CLI

Você pode especificar uma ação ao criar ou atualizar uma regra. A ação a seguir envia uma resposta fixa com o código de status especificado.

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

```

Condições de regra

Cada condição de regra possui um tipo e informações de configuração. Quando as condições de uma regra forem atendidas, a ação será executada.

Veja a seguir os critérios de correspondência aceitos para uma regra:

Correspondência de cabeçalho

Roteamento com base nos cabeçalhos HTTP de cada solicitação. Você pode usar condições de cabeçalho HTTP para configurar regras que roteiam solicitações com base nos cabeçalhos HTTP da solicitação. Você pode especificar os nomes dos campos de cabeçalho HTTP padrão ou personalizados. O nome do cabeçalho e a avaliação de correspondência não diferenciam maiúsculas de minúsculas. Você pode alterar essa configuração ativando a diferenciação entre maiúsculas e minúsculas. Caracteres curinga não são compatíveis com o nome do cabeçalho. Há suporte para correspondência dos tipos prefixo, exata e contém na correspondência de cabeçalho.

Correspondência de métodos

Roteamento com base no método de solicitação HTTP de cada solicitação.

Você pode usar condições do método de solicitação HTTP para configurar regras que roteiam solicitações com base no método de solicitação HTTP da solicitação. Você pode especificar métodos HTTP padrão ou personalizados. A correspondência de método diferencia maiúsculas de minúsculas. O nome do método deve ser uma correspondência exata. Caracteres curinga não são compatíveis.

Correspondência de caminho

O roteamento é baseado na correspondência dos padrões de caminho na solicitação URLs.

Você pode usar as condições de caminho para definir regras que roteiam solicitações com base no URL da solicitação. Caracteres curinga não são compatíveis. Há suporte para correspondência dos tipos prefixo e exata no caminho.

Adicionar uma regra

Você pode adicionar uma regra de receptor a qualquer momento.

Para adicionar uma regra de receptor usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Na guia Roteamento, escolha Editar receptor.
5. Expanda as Regras do receptor e escolha Adicionar regra.
6. Em Nome da regra, insira um nome para a regra.
7. Em Prioridade, insira uma prioridade entre 1 e 100. As regras são avaliadas em ordem de prioridade, do valor mais baixo para o valor mais alto. A regra padrão é avaliada por último.
8. Em Condição, insira um padrão de caminho para a condição de correspondência de caminho. O tamanho máximo de cada string é de 200 caracteres. A comparação não diferencia maiúsculas de minúsculas. Caracteres curinga não são compatíveis.

Para adicionar uma condição de regra de correspondência de cabeçalho ou de correspondência de método, use a AWS CLI ou um AWS SDK.

9. Em Ação, escolha um grupo de destino do VPC Lattice.
10. Escolha Salvar alterações.

Para adicionar uma regra usando o AWS CLI

Use o comando [create-rule](#).

Atualizar uma regra

Você pode atualizar uma regra de receptor a qualquer momento. Você pode modificar sua prioridade, condição, grupo de destino e o peso de cada grupo de destino. Não é possível modificar o nome da regra.

Para atualizar uma regra de receptor usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Na guia Roteamento, escolha Editar receptor.
5. Modifique as prioridades, condições e ações da regra conforme necessário.
6. Revise as atualizações e escolha Salvar alterações.

Para atualizar uma regra usando a AWS CLI

Use o comando [update-rule](#).

Excluir uma regra

Você pode excluir as regras não padrão para um receptor a qualquer momento. Você não pode excluir a regra padrão do listener. Quando você exclui um receptor, todas as regras são excluídas.

Para excluir uma regra de receptor usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Na guia Roteamento, escolha Editar receptor.

5. Selecione a regra e escolha Remover.
6. Escolha Salvar alterações.

Para excluir uma regra usando a AWS CLI

Use o comando [delete-rule](#).

Exclua um receptor do seu serviço VPC Lattice

Você pode excluir um listener a qualquer momento. Quando você exclui um receptor, todas as regras são excluídas automaticamente.

Para excluir um listener usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços.
3. Selecione o nome do serviço para abrir sua página de detalhes.
4. Na guia Roteamento, escolha Excluir receptor.
5. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para excluir um listener usando a AWS CLI

Use o comando [delete-listener](#).

Recursos de VPC no Amazon VPC Lattice

Você pode compartilhar recursos de VPC com outras equipes em sua organização ou com parceiros externos de fornecedores independentes de software (ISV). Um recurso de VPC pode ser um recurso AWS-nativo, como um banco de dados do Amazon RDS, um nome de domínio ou um endereço IP. O recurso pode estar na sua VPC ou na rede local e não precisa ter balanceamento de carga. Você usa AWS RAM para especificar os principais que podem acessar o recurso. Você cria um gateway de recursos por meio do qual seu recurso pode ser acessado. Você também cria uma configuração de recurso que representa o recurso ou um grupo de recursos que você deseja compartilhar.

Os diretores com os quais você compartilha o recurso podem acessar esses recursos de forma privada usando VPC endpoints. Eles podem usar um endpoint VPC de recursos para acessar um recurso ou agrupar vários recursos em uma rede de serviços VPC Lattice e acessar a rede de serviços usando um endpoint VPC de rede de serviços.

As seções a seguir explicam como criar e gerenciar recursos de VPC no VPC Lattice:

Tópicos

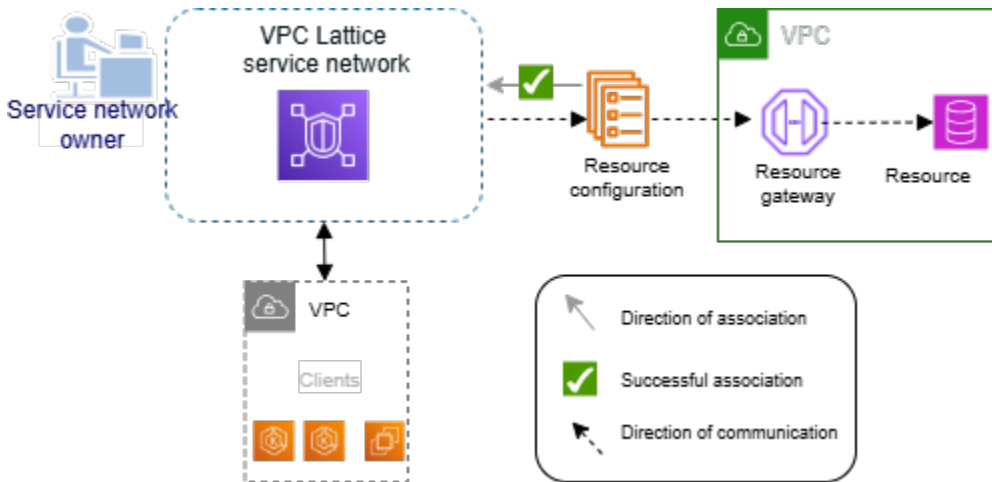
- [Gateways de recursos no VPC Lattice](#)
- [Configurações de recursos para recursos de VPC](#)

Gateways de recursos no VPC Lattice

Um gateway de recursos é o ponto que recebe tráfego na VPC em que o recurso reside. Ela abrange várias zonas de disponibilidade.

Uma VPC deve ter um gateway de recursos se você planeja tornar os recursos dentro da VPC acessíveis a partir de outras contas ou contas. VPCs Cada recurso que você compartilha está associado a um gateway de recursos. Quando clientes em outras VPCs contas acessam um recurso em sua VPC, o recurso vê o tráfego vindo localmente do gateway de recursos nessa VPC. O endereço IP de origem do tráfego é o endereço IP do gateway de recursos em uma zona de disponibilidade. Várias configurações de recursos, cada uma com vários recursos, podem ser anexadas a um gateway de recursos.

O diagrama a seguir mostra como um cliente acessa um recurso por meio do gateway de recursos:



Conteúdo

- [Considerações](#)
- [Grupos de segurança](#)
- [Tipos de endereço IP](#)
- [Crie um gateway de recursos no VPC Lattice](#)
- [Excluir um gateway de recursos na VPC Lattice](#)

Considerações

As considerações a seguir se aplicam aos gateways de recursos:

- Para que seu recurso seja acessível a partir de todas as [zonas de disponibilidade](#), você deve criar seus gateways de recursos para abranger o maior número possível de zonas de disponibilidade.
- Pelo menos uma zona de disponibilidade do VPC endpoint e do gateway de recursos precisa se sobrepor.
- Uma VPC pode ter no máximo 100 gateways de recursos. Para obter mais informações, consulte [Cotas para VPC Lattice](#).
- Você não pode criar um gateway de recursos em uma sub-rede compartilhada.

Grupos de segurança

Você pode anexar grupos de segurança a um gateway de recursos. As regras de grupo de segurança para gateways de recursos controlam o tráfego de saída do gateway de recursos para os recursos.

Regras de saída recomendadas para o tráfego que flui de um gateway de recursos para um recurso de banco de dados

Para que o tráfego flua de um gateway de recursos para um recurso, você deve criar regras de saída para os protocolos de ouvinte e intervalos de portas aceitos pelo recurso.

Destino	Protocolo	Intervalo de portas	Comentário
<i>CIDR range for resource</i>	TCP	3306	Permite o tráfego do gateway de recursos para os bancos de dados.

Tipos de endereço IP

Um gateway de recursos pode ter endereços IPv6 ou IPv4 endereços de pilha dupla. O tipo de endereço IP de um gateway de recursos deve ser compatível com as sub-redes do gateway de recursos e com o tipo de endereço IP do recurso, conforme descrito aqui:

- IPv4— Atribua IPv4 endereços às interfaces de rede do gateway de recursos. Essa opção é suportada somente se todas as sub-redes selecionadas tiverem intervalos de IPv4 endereços e o recurso também tiver um IPv4 endereço.
- IPv6— Atribua IPv6 endereços às interfaces de rede do gateway de recursos. Essa opção é suportada somente se todas as sub-redes selecionadas forem IPv6 somente sub-redes e o recurso também tiver um endereço IPv6.
- Dualstack — atribua IPv6 endereços IPv4 e endereços às interfaces de rede do gateway de recursos. Essa opção é suportada somente se todas as sub-redes selecionadas tiverem intervalos de IPv6 endereços IPv4 e o recurso tiver um endereço IPv4 ou IPv6.

O tipo de endereço IP do gateway de recursos é independente do tipo de endereço IP do cliente ou do VPC endpoint por meio do qual o recurso é acessado.

Crie um gateway de recursos no VPC Lattice

Use o console para criar um gateway de recursos.

Pré-requisito

Para criar um gateway de recursos, você deve ter um bloco /28 disponível em uma sub-rede.

Para criar um gateway de recursos usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em PrivateLink e Lattice, escolha Resource gateways.
3. Escolha Criar gateway de recursos.
4. Insira um nome que seja exclusivo em sua AWS conta.
5. Escolha o tipo de IP para o gateway de recursos.
6. Escolha a VPC na qual o recurso está.
7. Escolha até cinco grupos de segurança para controlar o tráfego de entrada da VPC para a rede de serviços.
8. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
9. Escolha Criar gateway de recursos.

Para criar um gateway de recursos usando o AWS CLI

Use o comando [create-resource-gateway](#).

Excluir um gateway de recursos na VPC Lattice

Use o console para excluir um gateway de recursos.

Para excluir um gateway de recursos usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em PrivateLink e Lattice, escolha Resource gateways.
3. Marque a caixa de seleção do gateway de recursos que você deseja excluir e escolha Ações, Excluir. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para excluir um gateway de recursos usando o AWS CLI

Use o comando [delete-resource-gateway](#).

Configurações de recursos para recursos de VPC

Uma configuração de recurso representa um recurso ou um grupo de recursos que você deseja tornar acessível a clientes em VPCs outras contas. Ao definir uma configuração de recursos, você pode permitir conectividade de rede privada, segura e unidirecional aos recursos em sua VPC de clientes em outras contas. VPCs Uma configuração de recurso está associada a um gateway de recursos por meio do qual ela recebe tráfego. Para que um recurso seja acessado de outra VPC, ele precisa ter uma configuração de recursos.

Conteúdo

- [Tipos de configurações de recursos](#)
- [Gateway de recursos](#)
- [Definição de recurso](#)
- [Protocolo](#)
- [Intervalos de portas](#)
- [Acesso a recursos da](#)
- [Associação com o tipo de rede de serviços](#)
- [Tipos de redes de serviços](#)
- [Compartilhando configurações de recursos por meio de AWS RAM](#)
- [Monitoramento](#)
- [Crie uma configuração de recursos no VPC Lattice](#)
- [Gerenciar associações para uma configuração de recursos do VPC Lattice](#)

Tipos de configurações de recursos

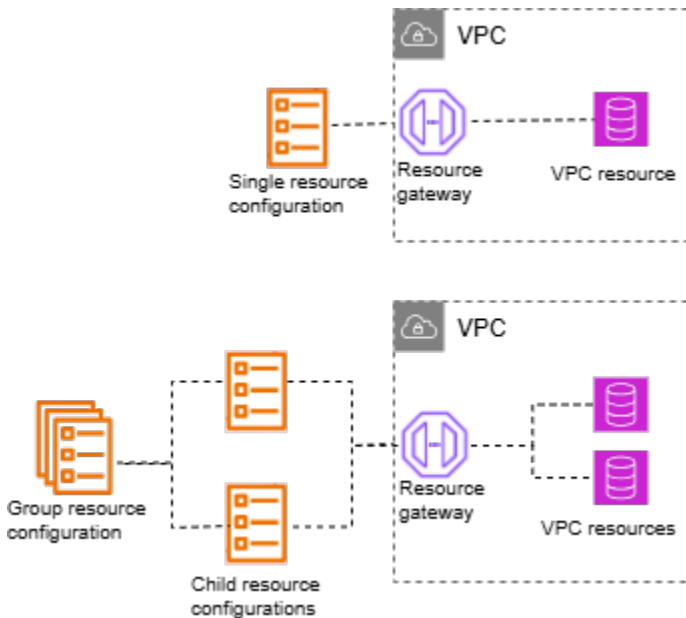
A configuração de um recurso pode ser de vários tipos. Os diferentes tipos ajudam a representar diferentes tipos de recursos. Os tipos são:

- Configuração de recurso único: representa um endereço IP ou nome de domínio. Ele pode ser compartilhado de forma independente.
- Configuração de recursos de grupo: é uma coleção de configurações de recursos secundários. Ele pode ser usado para representar um grupo de endpoints de endereço IP e DNS.
- Configuração de recursos secundários: é membro de uma configuração de recursos de grupo. Ele representa um endereço IP ou nome de domínio. Não pode ser compartilhado de forma

independente; ele só pode ser compartilhado como parte de um grupo. Ele pode ser adicionado e removido de um grupo. Quando adicionado, ele pode ser acessado automaticamente por aqueles que podem acessar o grupo.

- Configuração do recurso ARN: representa um tipo de recurso suportado que é provisionado por um serviço. AWS Qualquer relacionamento grupo-filho é resolvido automaticamente.

A imagem a seguir mostra uma configuração de recurso único, secundário e de grupo:



Gateway de recursos

Uma configuração de recurso está associada a um gateway de recursos. Um gateway de recursos é um conjunto ENIs que serve como um ponto de entrada na VPC na qual o recurso está. Várias configurações de recursos podem ser associadas ao mesmo gateway de recursos. Quando clientes em outras VPCs contam acessar um recurso em sua VPC, o recurso vê o tráfego vindo localmente dos endereços IP do gateway de recursos nessa VPC.

Definição de recurso

Na configuração do recurso, identifique o recurso de uma das seguintes formas:

- Por um nome de recurso da Amazon (ARN): os tipos de recursos compatíveis que são provisionados por AWS serviços podem ser identificados por seu ARN. Somente bancos de dados do Amazon RDS são compatíveis. Você não pode criar uma configuração de recursos para um cluster acessível ao público.

- Por um alvo de nome de domínio: você pode usar qualquer nome de domínio que possa ser resolvido publicamente. Se seu nome de domínio apontar para um IP que esteja fora da sua VPC, você deverá ter um gateway NAT na sua VPC.
- Por endereço IP: Para IPv4, especifique um IP privado dos seguintes intervalos: 10.0.0.0/8, 100.64.0.0/10, 172.16.0.0/12, 192.168.0.0/16. Para IPv6, especifique um IP da VPC. O público IPs não é suportado.

Protocolo

Ao criar uma configuração de recurso, você pode definir os protocolos que o recurso suportará. Atualmente, somente o protocolo TCP é suportado.

Intervalos de portas

Ao criar uma configuração de recurso, você pode definir as portas nas quais ela aceitará solicitações. O acesso do cliente em outras portas não será permitido.

Acesso a recursos da

Os consumidores podem acessar as configurações de recursos diretamente de sua VPC usando um VPC endpoint ou por meio de uma rede de serviços. Como consumidor, você pode habilitar o acesso da sua VPC a uma configuração de recursos que esteja em sua conta ou que tenha sido compartilhada com você por meio de outra conta por meio de. AWS RAM

- Acessando a configuração de um recurso diretamente

Você pode criar um AWS PrivateLink VPC endpoint do tipo resource (endpoint de recurso) na sua VPC para acessar uma configuração de recursos de forma privada a partir da sua VPC. Para obter mais informações sobre como criar um endpoint de recursos, consulte Como [acessar recursos de VPC](#) no guia AWS PrivateLink do usuário.

- Acessando uma configuração de recursos por meio de uma rede de serviços

Você pode associar uma configuração de recursos a uma rede de serviços e conectar sua VPC à rede de serviços. Você pode conectar sua VPC à rede de serviços por meio de uma associação ou usando um endpoint VPC de AWS PrivateLink rede de serviços.

Para obter mais informações sobre associações de redes de serviços, consulte [Gerenciar as associações de uma rede de serviços VPC Lattice](#).

Para obter mais informações sobre os endpoints VPC da rede de serviços, consulte [Acesse redes de serviços no guia](#) do AWS PrivateLink usuário.

Quando o DNS privado está habilitado para sua VPC, você não pode criar um endpoint de recursos e um endpoint de rede de serviços para a mesma configuração de recursos.

Associação com o tipo de rede de serviços

Quando você compartilha uma configuração de recurso com uma conta de consumidor, por exemplo, Conta-B, por meio AWS RAM de, a Conta B pode acessar a configuração do recurso diretamente por meio de um endpoint VPC de recursos ou por meio de uma rede de serviços.

Para acessar uma configuração de recursos por meio de uma rede de serviços, a Conta B precisaria associar a configuração do recurso a uma rede de serviços. As redes de serviços podem ser compartilhadas entre contas. Assim, a Conta B pode compartilhar sua rede de serviços (à qual a configuração do recurso está associada) com a Conta C, tornando seu recurso acessível a partir da Conta C.

Para evitar esse compartilhamento transitivo, você pode especificar que sua configuração de recursos não pode ser adicionada às redes de serviços que podem ser compartilhadas entre contas. Se você especificar isso, a Conta B não poderá adicionar sua configuração de recursos às redes de serviços que são compartilhadas ou podem ser compartilhadas com outra conta no futuro.

Tipos de redes de serviços

Quando você compartilha uma configuração de recurso com outra conta, por exemplo, Conta-B, por meio AWS RAM de, a Conta-B pode acessar os recursos especificados na configuração do recurso de uma das três maneiras:

- Usando um endpoint VPC do tipo recurso (recurso VPC endpoint).
- Usando um endpoint VPC do tipo service network (rede de serviços VPC endpoint).
- Usando uma associação VPC de rede de serviços.

Quando você usa uma associação de serviço-rede, cada recurso recebe um IP por sub-rede do bloco 129.224.0.0/17, que é próprio e não roteável. AWS Isso é um acréscimo à [lista de prefixos gerenciados](#) que o VPC Lattice usa para rotear o tráfego para serviços pela rede VPC Lattice.

Ambos IPs são atualizados na tabela de rotas da sua VPC.

Para o endpoint VPC da rede de serviços e a associação VPC da rede de serviços, a configuração do recurso precisaria estar associada a uma rede de serviços na Conta B. As redes de serviços podem ser compartilhadas entre contas. Assim, a Conta B pode compartilhar sua rede de serviços (que contém a configuração do recurso) com a Conta C, tornando seu recurso acessível a partir da Conta C. Para evitar esse compartilhamento transitivo, você pode impedir que sua configuração de recursos seja adicionada às redes de serviços que podem ser compartilhadas entre contas. Se você não permitir isso, a Conta B não poderá adicionar sua configuração de recursos a uma rede de serviços que seja compartilhada ou possa ser compartilhada com outra conta.

Compartilhando configurações de recursos por meio de AWS RAM

As configurações de recursos são integradas com o AWS Resource Access Manager. Você pode compartilhar sua configuração de recursos com outra conta por meio de AWS RAM. Quando você compartilha uma configuração de recurso com uma AWS conta, os clientes dessa conta podem acessar o recurso de forma privada. Você pode compartilhar uma configuração de recursos usando um [compartilhamento de recursos](#) em AWS RAM.

Use o AWS RAM console para ver os compartilhamentos de recursos aos quais você foi adicionado, os recursos compartilhados que você pode acessar e as AWS contas que compartilharam recursos com você. Para obter mais informações, consulte [Recursos compartilhados com você](#) no Guia AWS RAM do usuário.

Para acessar um recurso de outra VPC na mesma conta da configuração do recurso, você não precisa compartilhar a configuração do recurso por meio de AWS RAM.

Monitoramento

Você pode ativar os registros de monitoramento na configuração do seu recurso. Você pode escolher um destino para o qual enviar os registros.

Crie uma configuração de recursos no VPC Lattice

Use o console para criar uma configuração de recursos.

Para criar uma configuração de recursos usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em PrivateLink e Lattice, escolha Configurações de recursos.
3. Escolha Criar configuração de recursos.

4. Insira um nome que seja exclusivo em sua AWS conta. Você não pode alterar esse nome após a criação da configuração do recurso.
5. Em Tipo de configuração, escolha Recurso para um recurso único ou secundário ou Grupo de recursos para um grupo de recursos secundários.
6. Escolha um gateway de recursos que você criou anteriormente ou crie um agora.
7. Escolha o identificador do recurso que você deseja que essa configuração represente.
8. Escolha os intervalos de portas por meio dos quais você deseja compartilhar o recurso.
9. Em Configurações de associação, especifique se essa configuração de recurso pode ser associada a redes de serviços compartilháveis.
10. Em Configuração de recursos de compartilhamento, escolha os compartilhamentos de recursos que identificam os principais que podem acessar esse recurso.
11. (Opcional) Para monitoramento, ative os registros de acesso a recursos e o destino de entrega se quiser monitorar solicitações e respostas de e para a configuração do recurso.
12. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
13. Escolha Criar configuração de recursos.

Para criar uma configuração de recursos usando o AWS CLI

Use o comando [create-resource-configuration](#).

Gerenciar associações para uma configuração de recursos do VPC Lattice

As contas de consumidor com as quais você compartilha uma configuração de recursos e os clientes em sua conta podem acessar a configuração do recurso diretamente usando um endpoint VPC do tipo recurso ou por meio de um endpoint VPC do tipo service-network. Como resultado, sua configuração de recursos terá associações de endpoints e associações de rede de serviços.

Gerenciar associações de rede de serviços

Crie ou exclua uma associação de rede de serviços.

Note

Se você receber uma mensagem de acesso negado ao criar a associação entre a rede de serviços e a configuração do recurso, verifique a versão da AWS RAM política e certifique-se de que seja a versão 2. Para obter mais informações, consulte o [guia AWS RAM do usuário](#).

Para gerenciar uma associação de serviço-rede usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em PrivateLink e Lattice, escolha Configurações de recursos.
3. Selecione o nome da configuração do recurso para abrir sua página de detalhes.
4. Selecione a guia Associações de rede de serviços.
5. Escolha Criar associações.
6. Selecione uma rede de serviços nas Redes de serviços VPC Lattice. Para criar uma rede de serviços, escolha Criar uma rede VPC Lattice.
7. (Opcional) Para adicionar uma tag, expanda Tags de associação de serviço, escolha Adicionar nova tag e insira uma chave de tag e um valor de tag.
8. Escolha Salvar alterações.
9. Para excluir uma associação, marque a caixa de seleção da associação e escolha Ações, Excluir. Quando a confirmação for solicitada, insira **confirm** e selecione Excluir.

Para criar uma associação de rede de serviços usando o AWS CLI

Use o comando [create-service-network-resource-association](#).

Para excluir uma associação de rede de serviços usando o AWS CLI

Use o comando [delete-service-network-resource-association](#).

Gerencie associações de endpoints de VPC

Gerencie uma associação de VPC endpoint.

Para gerenciar uma associação de VPC endpoint usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em PrivateLink e Lattice, escolha Configurações de recursos.
3. Selecione o nome da configuração do recurso para abrir sua página de detalhes.
4. Escolha a guia Associações de endpoints.
5. Selecione o ID da associação para abrir sua página de detalhes. A partir daqui, você pode modificar ou excluir a associação.
6. Para criar uma nova associação de endpoint, acesse PrivateLink e Lattice no painel de navegação esquerdo e escolha Endpoints.

7. Escolha Criar endpoints.
8. Selecione a configuração do recurso que você deseja conectar à sua VPC.
9. Selecione a VPC, as sub-redes e os grupos de segurança.
10. (Opcional) Para marcar seu VPC endpoint, escolha Adicionar nova tag e insira uma chave e um valor de tag.
11. Escolha Criar endpoint.

Para criar uma associação de VPC endpoint usando o AWS CLI

Use o comando [create-vpc-endpoint](#).

Para excluir uma associação de VPC endpoint usando o AWS CLI

Use o comando [delete-vpc-endpoint](#).

Compartilhe suas entidades do VPC Lattice

O Amazon VPC Lattice se integra com AWS Resource Access Manager (AWS RAM) para permitir o compartilhamento de serviços, configurações de recursos e redes de serviços. AWS RAM é um serviço que permite que você compartilhe algumas entidades do VPC Lattice com outras Contas da AWS ou por meio de. AWS Organizations Com AWS RAM, você compartilha entidades de sua propriedade criando um compartilhamento de recursos. Um compartilhamento de recursos especifica as entidades a serem compartilhadas e os consumidores com quem compartilhá-las. Os consumidores podem incluir:

- Específico Contas da AWS dentro ou fora de sua organização em AWS Organizations.
- Uma unidade organizacional dentro da sua organização no AWS Organizations.
- Uma organização inteira no AWS Organizations.

Para obter mais informações sobre AWS RAM, consulte o [Guia AWS RAM do usuário](#).

Conteúdo

- [Pré-requisitos para compartilhar entidades do VPC Lattice](#)
- [Compartilhe entidades do VPC Lattice](#)
- [Pare de compartilhar entidades do VPC Lattice](#)
- [Responsabilidades e permissões](#)
- [Eventos entre contas](#)

Pré-requisitos para compartilhar entidades do VPC Lattice

- Para compartilhar uma entidade, você deve possuí-la em seu Conta da AWS. Isso significa que a entidade deve ser alocada ou provisionada em sua conta. Você não pode compartilhar uma entidade que tenha sido compartilhada com você.
- Para compartilhar uma entidade com sua organização ou unidade organizacional em AWS Organizations, você deve habilitar o compartilhamento com AWS Organizations. Para obter mais informações, consulte [Habilitar o compartilhamento de recursos no AWS Organizations](#) no Guia do usuário do AWS RAM .

Compartilhe entidades do VPC Lattice

Para compartilhar uma entidade, comece criando um compartilhamento de recursos usando AWS Resource Access Manager. Um compartilhamento de recursos especifica as entidades a serem compartilhadas, os consumidores com quem elas são compartilhadas e quais ações os diretores podem realizar.

Ao compartilhar uma entidade do VPC Lattice que você possui com outra pessoa Contas da AWS, você permite que essas contas associem suas entidades às entidades em sua conta. Quando você cria uma associação com uma entidade compartilhada, geramos um nome de recurso da Amazon (ARN) na conta do proprietário da entidade e na conta que criou a associação. Portanto, tanto o proprietário da entidade quanto a conta que criou a associação podem excluir a associação.

Se você faz parte de uma organização AWS Organizations e o compartilhamento dentro de sua organização está ativado, os consumidores em sua organização recebem automaticamente acesso à entidade compartilhada. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e terão acesso à entidade compartilhada após aceitarem o convite.

Considerações

- Você pode compartilhar três tipos de entidades do VPC Lattice: redes de serviços, serviços e configurações de recursos.
- Você pode compartilhar suas entidades do VPC Lattice com qualquer uma. Conta da AWS
- Você não pode compartilhar suas entidades do VPC Lattice com usuários e funções individuais do IAM.
- O VPC Lattice oferece suporte a permissões gerenciadas pelo cliente para serviços, configurações de recursos e redes de serviços.

Para compartilhar uma entidade que você possui usando o console VPC Lattice

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços, Redes de serviços ou Configurações de recursos.
3. Escolha o nome da entidade para abrir sua página de detalhes e, em seguida, escolha Compartilhar serviço, Compartilhar rede de serviços ou Compartilhar configuração de recursos na guia Compartilhamento.

4. Escolha os compartilhamentos AWS RAM de recursos em Compartilhamentos de recursos. Para criar um compartilhamento de recursos, escolha Criar um compartilhamento de recursos no console do RAM.
5. Escolha Compartilhar serviço, Compartilhar rede de serviços ou Compartilhar configuração de recursos.

Para compartilhar uma entidade que você possui usando o AWS RAM console

Siga o procedimento descrito em [Criar um compartilhamento de recursos](#) no Guia do usuário do AWS RAM .

Para compartilhar uma entidade que você possui usando o AWS CLI

Use o comando [associate-resource-share](#).

Pare de compartilhar entidades do VPC Lattice

Para parar de compartilhar uma entidade VPC Lattice de sua propriedade, você deve removê-la do compartilhamento de recursos. As associações existentes persistem depois que você para de compartilhar sua entidade. Novas associações a uma entidade compartilhada anteriormente não são permitidas. Quando o proprietário da entidade ou o proprietário da associação exclui uma associação, ela é excluída de ambas as contas. Se o proprietário da conta quiser sair de um compartilhamento de recursos, ele deverá pedir ao proprietário do compartilhamento de recursos que remova sua conta da lista de contas com as quais esse recurso foi compartilhado.

Para parar de compartilhar uma entidade que você possui usando o console VPC Lattice

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Serviços, Redes de serviços ou Configurações de recursos.
3. Escolha o nome da entidade para abrir sua página de detalhes.
4. Na guia Compartilhamento, marque a caixa de seleção do compartilhamento de recursos e escolha Remover.

Para parar de compartilhar uma entidade que você possui usando o AWS RAM console

Consulte [Atualizar um compartilhamento de recursos](#) no Guia do usuário do AWS RAM .

Para parar de compartilhar uma entidade que você possui usando o AWS CLI

Use o comando [disassociate-resource-share](#).

Responsabilidades e permissões

As responsabilidades e permissões a seguir se aplicam ao uso de entidades compartilhadas do VPC Lattice.

Proprietários da entidade

- O proprietário da rede de serviços não pode modificar um serviço criado por um consumidor.
- O proprietário da rede de serviços não pode excluir um serviço criado por um consumidor.
- O proprietário da rede de serviços pode descrever todas as associações de serviços da rede de serviços.
- O proprietário da rede de serviços pode desassociar qualquer serviço associado à rede de serviços, independentemente de quem tenha criado a associação.
- O proprietário da rede de serviços pode descrever todas as associações de VPC da rede de serviços.
- O proprietário da rede de serviços pode desassociar qualquer VPC que um consumidor tenha associado à rede de serviços.
- O proprietário da rede de serviços pode descrever todas as associações de configuração de recursos da rede de serviços.
- O proprietário da rede de serviços pode desassociar qualquer configuração de recurso associada à rede de serviços, independentemente de quem criou a associação.
- O proprietário da rede de serviços pode descrever todas as associações de endpoints da rede de serviços.
- O proprietário da rede de serviços pode desassociar qualquer endpoint associado à rede de serviços, independentemente de quem criou a associação.
- O proprietário do serviço pode descrever todas as associações de rede de serviços com o serviço.
- O proprietário do serviço pode desassociar um serviço de qualquer rede de serviços à qual ele esteja associado.
- O proprietário da configuração do recurso pode descrever todas as associações de rede com a configuração do recurso.

- O proprietário da configuração do recurso pode desassociar uma configuração de recurso de qualquer rede de serviços à qual ela esteja associada.
- O proprietário do VPC endpoint pode descrever a rede de serviços à qual ele está associado.
- O proprietário do VPC endpoint pode dissociar um endpoint da rede de serviços.
- Somente a conta que criou uma associação pode atualizar a associação entre a rede de serviços e a VPC.

Consumidores individuais

- O consumidor não pode excluir uma configuração de serviço ou recurso que ele não criou.
- O consumidor pode desassociar somente os serviços ou configurações de recursos que ele associou a uma rede de serviços.
- O consumidor e o proprietário da rede podem descrever todas as associações entre uma rede de serviços e uma configuração de serviços ou recursos.
- O consumidor não pode recuperar informações de serviço de um serviço ou informações de configuração de recursos de uma configuração de recursos que não seja de sua propriedade.
- O consumidor pode descrever todas as associações de serviços e associações de configurações de recursos com uma rede de serviços compartilhados.
- O consumidor pode associar um serviço ou uma configuração de recursos a uma rede de serviços compartilhados.
- O consumidor pode ver todas as associações de VPC com uma rede de serviços compartilhados.
- O consumidor pode associar uma VPC a uma rede de serviços compartilhados.
- O consumidor pode desassociar somente o VPCs que ele associou a uma rede de serviços.
- O consumidor pode criar um endpoint VPC de rede de serviços para conectar sua VPC a uma rede de serviços compartilhada.
- O consumidor pode excluir somente o endpoint VPC da rede de serviços que criou para conectar sua VPC a uma rede de serviços compartilhada.
- O consumidor de um serviço compartilhado não pode associar um serviço a uma rede de serviços que não seja de sua propriedade.
- O consumidor de uma rede de serviços compartilhados não pode associar uma VPC ou um serviço que não seja de sua propriedade.
- O consumidor de uma configuração de recurso compartilhado não pode associar uma configuração de recursos a uma rede de serviços que não seja de sua propriedade.

- O consumidor de uma rede de serviços compartilhados não pode associar uma VPC ou uma configuração de serviço ou recurso que não seja de sua propriedade.
- O consumidor pode descrever um serviço, uma rede de serviços ou uma configuração de recursos que é compartilhada com ele.
- O consumidor não pode associar duas entidades se ambas forem compartilhadas com elas.

Eventos entre contas

Quando proprietários e consumidores de entidades realizam ações em uma entidade compartilhada, essas ações são registradas como eventos entre contas em AWS CloudTrail.

CreateServiceNetworkResourceAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga `CreateServiceNetworkResourceAssociation` com uma entidade compartilhada. Se o chamador possuir a configuração do recurso, o evento será enviado ao proprietário da rede de serviço. Se o chamador for proprietário da rede de serviço, o evento será enviado ao proprietário da configuração do recurso.

CreateServiceNetworkServiceAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [CreateServiceNetworkServiceAssociation](#) com uma entidade compartilhada. Se o chamador for proprietário do serviço, o evento será enviado ao proprietário da rede de serviços. Se o chamador for proprietário da rede de serviços, o evento será enviado ao proprietário do serviço.

CreateServiceNetworkVpcAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [CreateServiceNetworkVpcAssociation](#) com uma rede de serviços compartilhados.

DeleteServiceNetworkResourceAssociationByOwner

Enviado ao proprietário da associação quando o proprietário da entidade liga `DeleteServiceNetworkResourceAssociation` com uma entidade compartilhada. Se o chamador possuir a configuração do recurso, o evento será enviado ao proprietário da associação de rede de serviço. Se o chamador for proprietário da rede de serviços, o evento será enviado ao proprietário da associação de recursos.

DeleteServiceNetworkResourceAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga `DeleteServiceNetworkResourceAssociation` com uma entidade compartilhada. Se o chamador possuir a configuração do recurso, o evento será enviado ao proprietário da rede de serviço. Se o chamador for proprietário da rede de serviço, o evento será enviado ao proprietário da configuração do recurso.

DeleteServiceNetworkServiceAssociationByOwner

Enviado ao proprietário da associação quando o proprietário da entidade liga [DeleteServiceNetworkServiceAssociation](#) com uma entidade compartilhada. Se o chamador for proprietário do serviço, o evento será enviado ao proprietário da associação da rede de serviços. Se o chamador for proprietário da rede de serviços, o evento será enviado ao proprietário da associação de serviço.

DeleteServiceNetworkServiceAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [DeleteServiceNetworkServiceAssociation](#) com uma entidade compartilhada. Se o chamador for proprietário do serviço, o evento será enviado ao proprietário da rede de serviços. Se o chamador for proprietário da rede de serviços, o evento será enviado ao proprietário do serviço.

DeleteServiceNetworkVpcAssociationByOwner

Enviado ao proprietário da associação quando o proprietário da entidade liga [DeleteServiceNetworkVpcAssociation](#) com uma rede de serviços compartilhados.

DeleteServiceNetworkVpcAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [DeleteServiceNetworkVpcAssociation](#) com uma rede de serviços compartilhados.

GetServiceBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [GetService](#) com um serviço compartilhado.

GetServiceNetworkBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [GetServiceNetwork](#) com uma rede de serviços compartilhados.

GetServiceNetworkResourceAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [GetServiceNetworkResourceAssociation](#) com uma entidade compartilhada. Se o chamador possuir a configuração do recurso, o evento será enviado ao proprietário da rede de serviço. Se o chamador for proprietário da rede de serviço, o evento será enviado ao proprietário da configuração do recurso.

GetServiceNetworkServiceAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [GetServiceNetworkServiceAssociation](#) com uma entidade compartilhada. Se o chamador for proprietário do serviço, o evento será enviado ao proprietário da rede de serviços. Se o chamador for proprietário da rede de serviços, o evento será enviado ao proprietário do serviço.

GetServiceNetworkVpcAssociationBySharee

Enviado ao proprietário da entidade quando um consumidor da entidade liga [GetServiceNetworkVpcAssociation](#) com uma rede de serviços compartilhados.

O seguinte é um exemplo da entrada para o evento `CreateServiceNetworkServiceAssociationBySharee`.

```
{
  "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-eea89f4a47cd",
  "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"  
  }  
]
```

Estrutura de VPC para Oracle Database@AWS

O VPC Lattice potencializa as integrações de serviços AWS gerenciados para [Oracle Database@AWS](#) (ODB) e fornece conectividade simplificada entre a rede ODB e o local. AWS VPCs Para oferecer suporte a essa conectividade, a VPC Lattice provisiona as seguintes entidades em seu nome:

Rede de serviços padrão

A rede de serviços padrão usa a convenção de nomenclatura `default-odb-network-randomHash`

Endpoint de rede de serviço padrão

Não há nome para esse AWS recurso.

Gateway de recursos

O gateway de recursos usa a convenção de nomenclatura `default-odb-network-randomHash`

O VPC Lattice oferece suporte a integrações de serviços AWS gerenciados, chamadas de integrações gerenciadas à sua rede ODB. Por padrão, o Oracle Cloud Infrastructure (OCI) Managed Backup to Amazon S3 está habilitado. Você pode optar por habilitar o acesso autogerenciado ao Amazon S3.

Depois de criar sua rede ODB, você pode visualizar os recursos provisionados usando o ou. AWS Management Console AWS CLI O exemplo de comando a seguir lista as integrações gerenciadas padrão da rede ODB e quaisquer outros recursos que você possa ter para essa rede de serviços:

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

Considerações

As considerações a seguir se aplicam ao VPC Lattice para: Oracle Database@AWS

- Você não pode excluir a rede de serviços padrão, o endpoint da rede de serviços, o gateway de recursos ou qualquer integração gerenciada de ODB provisionada pelo VPC Lattice. Para excluir essas entidades, exclua sua rede ODB ou desative as integrações gerenciadas.

- Os clientes só podem acessar as integrações gerenciadas na rede ODB. Clientes fora da rede ODB, como na sua VPCs, não podem usar essas integrações gerenciadas para acessar o S3.
- Você não pode se conectar a nenhuma das integrações gerenciadas fora da rede ODB provisionada pelo VPC Lattice.
- Todo o tráfego para o Amazon S3 passa pelo endpoint padrão da rede de serviços e são aplicadas taxas de processamento padrão para acessar os recursos. Para obter mais informações, consulte os preços do [VPC Lattice](#).
- Não há cobranças por hora para integrações Oracle Database@AWS gerenciadas.
- Você pode gerenciar os recursos provisionados pelo VPC Lattice da mesma forma que qualquer outra rede de serviços. Você pode compartilhar a rede de serviços padrão com outras pessoas Contas da AWS ou organizações e adicionar novos endpoints, associações de VPC, serviços e recursos do VPC Lattice à rede padrão.
- As seguintes permissões são necessárias para que o VPC Lattice provisione recursos: Oracle Database@AWS

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

```

```

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

```

Para usar o VPC Lattice para Oracle Database@AWS, recomendamos que você esteja familiarizado com redes de serviços, [associações de redes de serviços e gateways de](#) recursos no VPC Lattice.

Tópicos

- [the section called “Backup gerenciado do Oracle Cloud Infrastructure \(OCI\) para o Amazon S3”](#)
- [the section called “Acesso do Amazon S3”](#)
- [the section called “Acesse e compartilhe entidades do VPC Lattice”](#)

Backup gerenciado do Oracle Cloud Infrastructure (OCI) para o Amazon S3

Quando você cria um Oracle Database@AWS banco de dados, o VPC Lattice cria uma configuração de recursos chamada. odb-managed-s3-backup-access Essa configuração de recursos representa um backup gerenciado pela OCI de seus bancos de dados para o Amazon S3 e só

permite a conectividade com buckets do Amazon S3 de propriedade da OCI. O tráfego entre a rede ODB e o S3 nunca sai da rede Amazon.

Acesso do Amazon S3

Além do OCI Managed Backup to Amazon S3, você pode criar uma integração gerenciada que permite o acesso ao Amazon S3 a partir da rede ODB. Quando você modifica a Oracle Database@AWS rede para permitir a integração gerenciada do Amazon S3 Access, o VPC Lattice provisiona uma configuração de recursos chamada `odb-s3-access` na rede de serviços padrão. Você pode usar essa integração para acessar o Amazon S3 de acordo com suas próprias necessidades, incluindo backups ou restaurações autogerenciados. Você pode estabelecer o controle de perímetro fornecendo uma política de autenticação.

Considerações

A seguir estão algumas considerações sobre a integração gerenciada do Amazon S3 Access:

- Você pode criar somente uma integração gerenciada do Amazon S3 Access para a rede ODB.
- Essa integração gerenciada permite o acesso ao Amazon S3 somente a partir da rede ODB, e não de outras associações VPC ou endpoints de rede de serviços na rede de serviços padrão.
- Você não pode acessar buckets do S3 em regiões diferentes AWS .

Habilite a integração gerenciada do Amazon S3 Access

Use o comando a seguir para habilitar a integração gerenciada do Amazon S3 Access:

```
aws odb modify-odb-network --enable-s3-access
```

Acesso seguro com uma política de autenticação

Você pode proteger o acesso aos buckets do S3 definindo uma política de autenticação usando a API ODB. O exemplo de política a seguir concede acesso a buckets específicos do S3 pertencentes a uma organização específica.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1515115909152",
```

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

Note

As chaves de `aws:VpcSourceIp` condição `aws:SourceVpc` `aws:SourceVpce`, e não são suportadas pelas políticas de bucket do S3 ao usar integrações gerenciadas pelo ODB.

Acesse e compartilhe entidades do VPC Lattice

Você também pode conectar sua rede ODB a serviços, recursos e outros clientes VPCs usando o VPC Lattice. Essas opções de conectividade são alimentadas por meio da rede de serviços padrão, do gateway de recursos e do endpoint da rede de serviços provisionados pela VPC Lattice.

Acesse os serviços e recursos do VPC Lattice

Para acessar outras entidades, associe serviços ou recursos que você possui ou que estão compartilhados com você à rede de serviços padrão. Os clientes na rede ODB podem acessar os serviços ou recursos por meio do endpoint padrão da rede de serviços.

Considerações

Veja a seguir algumas considerações para se conectar a outras entidades do VPC Lattice:

- Você pode adicionar novos endpoints de rede de serviços, associações de VPC, recursos e serviços do VPC Lattice à rede de serviços, mas não pode modificar os recursos provisionados pelo VPC Lattice em nome da rede ODB. Eles devem ser gerenciados por meio do Oracle Database@AWS APIs.

Compartilhe sua rede ODB por meio do VPC Lattice

Você pode compartilhar seus recursos de rede ODB com clientes em outras VPCs contos ou no local. Para começar, crie uma configuração de recursos para os recursos que você deseja compartilhar. As configurações de recursos devem usar o gateway de recursos padrão para sua rede ODB. Em seguida, você pode associar os recursos à sua rede de serviços padrão.

Clientes em outra rede de serviços VPCs ou com Contas da AWS os quais você compartilhou sua rede de serviços podem acessar esses recursos por meio de seus próprios endpoints de rede de serviços ou associações de VPC. Para obter mais informações, consulte [the section called “Gerenciar associações”](#).

Considerações

A seguir estão algumas considerações para compartilhar sua rede ODB:

- Recomendamos compartilhar somente instâncias de rede ODB como recursos baseados em IP.
- O VPC Lattice não é compatível com o DNS do ouvinte Single Client Access Name (SCAN) da OCI.

Segurança no Amazon VPC Lattice

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon VPC Lattice, consulte [AWS Services in Scope by Compliance Program Scope by Compliance Program](#).
- **Segurança na nuvem**: você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o VPC Lattice. Os tópicos a seguir mostram como configurar o VPC Lattice para atender aos seus objetivos de segurança e de conformidade. Você também aprende a usar outros AWS serviços, que ajudam você a monitorar e proteger seu serviço VPC Lattice, redes de serviços e configurações de recursos.

Conteúdo

- [Gerencie o acesso aos serviços do VPC Lattice](#)
- [Proteção de dados no Amazon VPC Lattice](#)
- [Identity and Access Management para o Amazon VPC Lattice](#)
- [Validação de conformidade para o Amazon VPC Lattice](#)
- [Acesse o Amazon VPC Lattice usando endpoints de interface \(\)AWS PrivateLink](#)
- [Resiliência no Amazon VPC Lattice](#)
- [Segurança da infraestrutura no Amazon VPC Lattice](#)

Gerencie o acesso aos serviços do VPC Lattice

O VPC Lattice é seguro por padrão porque você precisa ser explícito sobre quais serviços e configurações de recursos fornecer acesso e com quais. VPCs Você pode acessar os serviços por meio de uma associação VPC ou de um endpoint VPC do tipo rede de serviços. Para cenários de várias contas, você pode usar [AWS Resource Access Manager](#) para compartilhar serviços, configurações de recursos e redes de serviços entre os limites da conta.

O VPC Lattice fornece uma estrutura que permite implementar uma estratégia de defense-in-depth em várias camadas da rede.

- Primeira camada — A associação de serviços, recursos, VPC e VPC endpoints com uma rede de serviços. Uma VPC pode estar conectada a uma rede de serviços por meio de uma associação ou por meio de um VPC endpoint. Se uma VPC não estiver conectada a uma rede de serviços, os clientes na VPC não poderão acessar as configurações de serviços e recursos associadas à rede de serviços.
- Segunda camada — proteções de segurança opcionais em nível de rede para a rede de serviços, como grupos de segurança e rede. ACLs Ao usá-los, você pode permitir o acesso a grupos específicos de clientes em uma VPC em vez de a todos os clientes na VPC.
- Terceira camada: política de autenticação opcional do VPC Lattice. Você pode aplicar uma política de autenticação a redes de serviços e serviços individuais. Normalmente, a política de autenticação na rede de serviços é operada pelo administrador da rede ou da nuvem, que implementa uma autorização granular. Por exemplo, permitir somente solicitações autenticadas de uma organização específica no AWS Organizations. Para uma política de autenticação no nível do serviço, normalmente o proprietário do serviço define controles refinados, que podem ser mais restritivos do que a autorização geral aplicada no nível da rede de serviço.

Note

A política de autenticação na rede de serviços não se aplica às configurações de recursos na rede de serviços.

Métodos de controle de acesso

- [Políticas de autenticação](#)
- [Grupos de segurança](#)

- [Rede ACLs](#)

Controle o acesso aos serviços do VPC Lattice usando políticas de autenticação

As políticas de autenticação do VPC Lattice são documentos de política do IAM que você anexa a redes ou serviços de serviços para controlar se uma entidade principal específica tem acesso a um grupo de serviços ou a um serviço específico. Você pode anexar uma política de autenticação a cada rede de serviços ou serviço ao qual você deseja controlar o acesso.

Note

A política de autenticação na rede de serviços não se aplica às configurações de recursos na rede de serviços.

As políticas de autorização são diferentes das políticas baseadas em identidade do IAM. As políticas baseadas em identidade do IAM são anexadas usuários, grupos ou perfis do IAM e definem quais ações essas entidades podem de executar em quais recursos. As políticas de autenticação são anexadas a serviços e redes de serviços. Para que a autorização seja bem-sucedida, tanto as políticas de autenticação quanto as políticas baseadas em identidade precisam ter declarações explícitas de permissão. Para obter mais informações, consulte [Funcionamento da autorização](#).

Você pode usar o console AWS CLI e para visualizar, adicionar, atualizar ou remover políticas de autenticação em serviços e redes de serviços. Quando você adiciona, atualiza ou remove uma política de autenticação, ela pode levar alguns minutos para ficar pronta. Ao usar o AWS CLI, verifique se você está na região correta. Você pode alterar a região padrão do seu perfil ou usar o `--region` parâmetro com o comando.

Conteúdo

- [Elementos comuns em uma política de autorização](#)
- [Formato de recurso para políticas de autenticação](#)
- [Chaves de condição que podem ser usadas em políticas de autenticação](#)
- [Entidades principais anônimas \(não autenticadas\)](#)
- [Exemplos de políticas de autenticação](#)
- [Funcionamento da autorização](#)

Para começar a usar as políticas de autenticação, siga o procedimento para criar uma política de autenticação que se aplique a uma rede de serviços. Para obter permissões mais restritivas que você não deseje aplicar a outros serviços, você pode, como opção, definir políticas de autenticação em serviços individuais.

Gerenciar o acesso a uma rede de serviços com políticas de autenticação

As AWS CLI tarefas a seguir mostram como gerenciar o acesso a uma rede de serviços usando políticas de autenticação. Para obter instruções usando o console, consulte [Redes de serviços no VPC Lattice](#).

Tarefas

- [Adicionar uma política de autenticação a uma rede de serviços](#)
- [Alterar o tipo de autenticação de uma rede de serviços](#)
- [Remover uma política de autenticação de uma rede de serviços](#)

Adicionar uma política de autenticação a uma rede de serviços

Siga as etapas desta seção para usar o AWS CLI para:

- Habilitar o controle de acesso em uma rede de serviços usando o IAM.
- Adicionar uma política de autenticação à rede de serviços. Se você não adicionar uma política de autenticação, todo o tráfego receberá um erro de acesso negado.

Para habilitar o controle de acesso e adicionar uma política de autenticação a uma nova rede de serviços

1. Para habilitar o controle de acesso em uma rede de serviços para que ela possa usar uma política de autenticação, use o comando `create-service-network` com a opção `--auth-type` e um valor de `AWS_IAM`.

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

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

```
{  
  "arn": "arn",
```

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

2. Use o comando `put-auth-policy`, especificando o ID da rede de serviços à qual você deseja adicionar a política de autenticação e a política de autenticação que deseja adicionar.

Por exemplo, use o comando a seguir para criar uma política de autenticação para a rede de serviços com o ID *sn-0123456789abcdef0*.

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

Use JSON para criar uma definição de política. Para obter mais informações, consulte [Elementos comuns em uma política de autorização](#).

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

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

Para habilitar o controle de acesso e adicionar uma política de autenticação a uma rede de serviços existente

1. Para habilitar o controle de acesso em uma rede de serviços para que ela possa usar uma política de autenticação, use o comando `update-service-network` com a opção `--auth-type` e um valor de `AWS_IAM`.

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

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

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

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

2. Use o comando `put-auth-policy`, especificando o ID da rede de serviços à qual você deseja adicionar a política de autenticação e a política de autenticação que deseja adicionar.

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

Use JSON para criar uma definição de política. Para obter mais informações, consulte [Elementos comuns em uma política de autorização](#).

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

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

Alterar o tipo de autenticação de uma rede de serviços

Para desabilitar a política de autenticação de uma rede de serviços

Use o `update-service-network` comando com a `--auth-type` opção e um valor de `NONE`.

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

Se você precisar habilitar a política de autenticação novamente posteriormente, execute esse comando com `AWS_IAM` especificado para a opção `--auth-type`.

Remover uma política de autenticação de uma rede de serviços

Para remover uma política de autenticação de uma rede de serviços

Use o comando `delete-auth-policy`.

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

A solicitação falhará se você remover uma política de autenticação antes de alterar o tipo de autenticação de uma rede de serviços para NONE.

Gerenciar o acesso a um serviço com políticas de autenticação

As AWS CLI tarefas a seguir mostram como gerenciar o acesso a um serviço usando políticas de autenticação. Para obter instruções usando o console, consulte [Serviços no VPC Lattice](#).

Tarefas

- [Adicionar uma política de autenticação a um serviço](#)
- [Alterar o tipo de autenticação de um serviço](#)
- [Remover uma política de autenticação de um serviço](#)

Adicionar uma política de autenticação a um serviço

Siga estas etapas para usar o AWS CLI para:

- Habilitar o controle de acesso em um serviço usando o IAM.
- Adicionar uma política de autenticação ao serviço. Se você não adicionar uma política de autenticação, todo o tráfego receberá um erro de acesso negado.

Para habilitar o controle de acesso e adicionar uma política de autenticação a um novo serviço

1. Para habilitar o controle de acesso em um serviço para que ele possa usar uma política de autenticação, use o comando `create-service` com a opção `--auth-type` e um valor de `AWS_IAM`.

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

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

```
{  
  "arn": "arn",  
  "authType": "AWS_IAM",  
  "dnsEntry": {  
    ...  
  },  
}
```

```
{
  "id": "svc-0123456789abcdef0",
  "name": "Name",
  "status": "CREATE_IN_PROGRESS"
}
```

2. Use o comando `put-auth-policy`, especificando o ID do serviço ao qual você deseja adicionar a política de autenticação e a política de autenticação que deseja adicionar.

Por exemplo, use o comando a seguir para criar uma política de autenticação para o serviço com o ID `svc-0123456789abcdef0`.

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

Use JSON para criar uma definição de política. Para obter mais informações, consulte [Elementos comuns em uma política de autorização](#).

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

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

Para habilitar o controle de acesso e adicionar uma política de autenticação a um serviço existente

1. Para habilitar o controle de acesso em um serviço para que ele possa usar uma política de autenticação, use o comando `update-service` com a opção `--auth-type` e um valor de `AWS_IAM`.

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

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

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

```
}
```

2. Use o comando `put-auth-policy`, especificando o ID do serviço ao qual você deseja adicionar a política de autenticação e a política de autenticação que deseja adicionar.

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

Use JSON para criar uma definição de política. Para obter mais informações, consulte [Elementos comuns em uma política de autorização](#).

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

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

Alterar o tipo de autenticação de um serviço

Para desabilitar a política de autenticação de um serviço

Use o `update-service` comando com a `--auth-type` opção e um valor de `NONE`.

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

Se você precisar habilitar a política de autenticação novamente posteriormente, execute esse comando com `AWS_IAM` especificado para a opção `--auth-type`.

Remover uma política de autenticação de um serviço

Para remover uma política de autenticação de um serviço

Use o comando `delete-auth-policy`.

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

A solicitação falhará se você remover uma política de autenticação antes de alterar o tipo de autenticação do serviço para `NONE`.

Se você habilitar políticas de autenticação que exijam solicitações autenticadas para um serviço, todas as solicitações para esse serviço deverão conter uma assinatura de solicitação válida que seja calculada usando o Signature Version 4 (SigV4). Para obter mais informações, consulte [SIGv4 solicitações autenticadas para o Amazon VPC Lattice](#).

Elementos comuns em uma política de autorização

As políticas de autorização do VPC Lattice são especificadas usando a mesma sintaxe das políticas do IAM. Para obter mais informações, consulte [Políticas baseadas em identidade e em recurso](#) no Guia do usuário do IAM.

A política de autorização contém os seguintes elementos:

- **Entidade principal:** a pessoa ou aplicação que tem permissão de acesso a ações e recursos na instrução. Em uma política de autorização, a entidade principal é a entidade do IAM que será a destinatária dessa permissão. A entidade principal é autenticada como uma entidade do IAM para fazer solicitações a um recurso específico ou grupo de recursos, como no caso de serviços em uma rede de serviços.
- Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou AWS serviços. Para obter mais informações, consulte [Elementos de política JSON da AWS : entidade principal](#) no Guia do usuário do IAM.
- **Efeito:** o efeito resultante quando a entidade principal especificada solicita a ação específica. Pode ser Allow ou Deny. Por padrão, quando você habilita o controle de acesso em um serviço ou rede de serviços usando o IAM, as entidades principais não têm permissão para fazer solicitações ao serviço ou à rede de serviços.
- **Ações** — A ação específica da API para a qual você está concedendo ou negando permissão. O VPC Lattice suporta ações que usam o prefixo. `vpc-lattice-svcs` Para obter mais informações, consulte [Ações definidas pelo Amazon VPC Lattice Services](#) na Referência de autorização de serviço.
- **Recursos:** os serviços afetados pela ação.
- **Condição:** as condições são opcionais. Você pode usá-los para controlar quando sua política está em vigor. Para obter mais informações, consulte [Chaves de condição para serviços do Amazon VPC Lattice](#) na Referência de autorização de serviço.

Conforme cria e gerencia políticas de autenticação, talvez você queira usar o [Gerador de políticas do IAM](#).

Requisito

A política em JSON não deve conter novas linhas ou linhas em branco.

Formato de recurso para políticas de autenticação

Você pode restringir o acesso a recursos específicos criando uma política de autenticação que use um esquema correspondente com um padrão `<serviceARN>/<path>` e codifique o elemento `Resource` conforme mostrado nos exemplos a seguir.

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

Use o seguinte formato de recurso de nome do recurso da Amazon (ARN) para o `<serviceARN>`:

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

Por exemplo:

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

Chaves de condição que podem ser usadas em políticas de autenticação

O acesso pode ser controlado adicionalmente com chaves de condição no elemento Condição das políticas de autenticação. Essas chaves de condição estão presentes para avaliação, dependendo do protocolo e se a solicitação está assinada com [Signature Version 4 \(SigV4\)](#) ou anônima. As chaves de condição fazem distinção entre maiúsculas e minúsculas.

AWS fornece chaves de condição globais que você pode usar para controlar o acesso, como `aws:PrincipalOrgID` `aws:SourceIp` e. Para ver uma lista das chaves de condição AWS globais, consulte as chaves de [contexto de condição AWS global](#) no Guia do usuário do IAM.

A tabela a seguir lista as chaves de condição do VPC Lattice. Para obter mais informações, consulte [Chaves de condição para serviços do Amazon VPC Lattice](#) na Referência de autorização de serviço.

Chaves de condição	Descrição	Exemplo	Disponível para chamador anônimo (não autenticado)?	Disponível para gRPC?
<code>vpc-lattice-svcs:Port</code>	Filtra o acesso por porta do serviço para a qual a solicitação é feita	80	Sim	Sim
<code>vpc-lattice-svcs:RequestMethod</code>	Filtra o acesso pelo método da solicitação	GET	Sim	Sempre POST
<code>vpc-lattice-svcs:RequestHeader/ <i>header-name</i> : <i>value</i></code>	Filtra o acesso por um par nome-valor de cabeçalho nos cabeçalhos da solicitação	<code>content-type: application/json</code>	Sim	Sim

Chaves de condição	Descrição	Exemplo	Disponível para chamador anônimo (não autenticado)?	Disponível para gRPC?
<code>vpc-lattice-svcs:RequestQueryString/ <i>key-name</i>: <i>value</i></code>	Filtra o acesso pelos pares de chave-valor da string de consulta no URL de solicitação	<code>quux: [corge, grault]</code>	Sim	Não
<code>vpc-lattice-svcs:ServiceNetworkArn</code>	Filtra o acesso pelo ARN da rede de serviços do serviço que recebe a solicitação	<code>arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/sn-0123456789abcdef0</code>	Sim	Sim
<code>vpc-lattice-svcs:ServiceArn</code>	Filtra o acesso pelo ARN do serviço que recebe a solicitação	<code>arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0</code>	Sim	Sim
<code>vpc-lattice-svcs:SourceVpc</code>	Filtra o acesso pela VPC de onde a solicitação é feita	<code>vpc-1a2b3c4d</code>	Sim	Sim

Chaves de condição	Descrição	Exemplo	Disponível para chamador anônimo (não autenticado)?	Disponível para gRPC?
<code>vpc-lattice-svcs:SourceVpcOwnerAccount</code>	Filtra o acesso pela conta proprietária da VPC da qual a solicitação é feita	123456789012	Sim	Sim

Entidades principais anônimas (não autenticadas)

Os diretores anônimos são chamadores que não assinam suas AWS solicitações com o [Signature Version 4 \(SigV4\)](#) e estão dentro de uma VPC conectada à rede de serviços. Essas entidades principais anônimas podem fazer solicitações não autenticadas a serviços na rede de serviços se isso for permitido por uma política de autenticação.

Exemplos de políticas de autenticação

Veja a seguir exemplos de políticas de autenticação que exigem que as solicitações sejam feitas por entidades principais autenticadas.

Todos os exemplos usam a us-west-2 Região e contêm uma conta fictícia. IDs

Exemplo 1: Restringir o acesso aos serviços por uma AWS organização específica

O exemplo de política de autenticação a seguir concede permissões a qualquer solicitação autenticada para acessar quaisquer serviços na rede de serviços à qual a política se aplique. No entanto, a solicitação deve ser originada de diretores que pertençam à AWS organização especificada na condição.

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

```

    "Principal": "*",
    "Action": "vpc-lattice-svcs:Invoke",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": [
          "o-123456example"
        ]
      }
    }
  }
]
}

```

Exemplo 2: restringir acesso a um serviço por um perfil do IAM específico

O exemplo de política de autenticação a seguir concede permissões a qualquer solicitação autenticada que use o perfil do IAM `rates-client` para fazer solicitações HTTP GET no serviço especificado no elemento `Resource`. O recurso no elemento `Resource` é igual ao serviço ao qual a política está vinculada.

```

{
  "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"
        }
      }
    }
  ]
}

```

```
}
```

Exemplo 3: restringir o acesso aos serviços por entidades principais autenticadas em uma VPC específica

O exemplo de política de autenticação a seguir só permite solicitações autenticadas de entidades principais na VPC cujo ID de VPC seja *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"
        }
      }
    }
  ]
}
```

Funcionamento da autorização

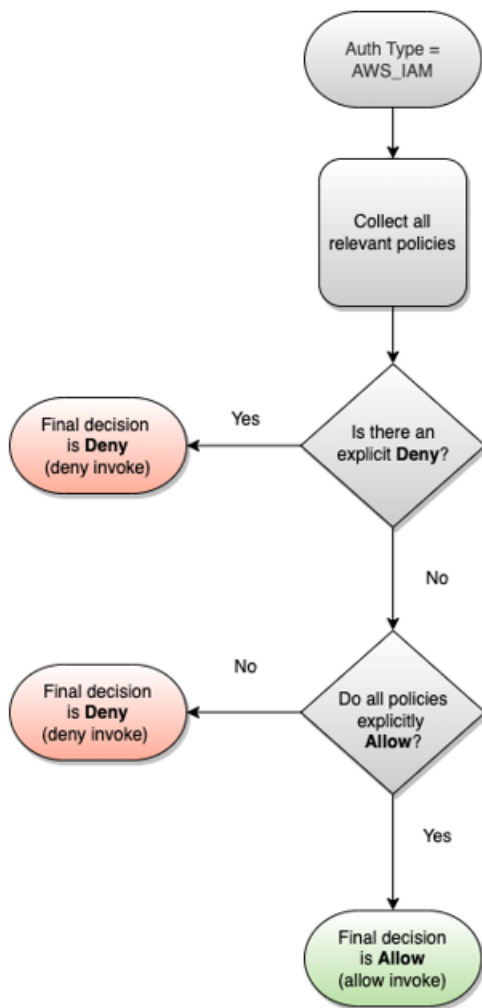
Quando um serviço VPC Lattice recebe uma solicitação, o código de AWS fiscalização avalia todas as políticas de permissões relevantes em conjunto para determinar se autoriza ou nega a solicitação. Ele avalia todas as políticas baseadas em identidade e políticas de autenticação do IAM que são aplicáveis no contexto da solicitação durante a autorização. Por padrão, todas as solicitações serão implicitamente negadas quando o tipo de autenticação for `AWS_IAM`. Uma permissão explícita de todas as políticas relevantes substitui o padrão.

A autorização inclui:

- Coletar todas as políticas relevantes do IAM baseadas em identidade e políticas de autenticação.
- Avaliação do conjunto de políticas resultante:

- Verificar se o solicitante (como um perfil ou usuário do IAM) tem permissões para executar a operação na conta à qual o solicitante pertence. Se não houver uma declaração de permissão explícita, AWS não autoriza a solicitação.
- Verificar se a solicitação é permitida pela política de autenticação da rede de serviços. Se uma política de autenticação estiver habilitada, mas não houver uma declaração de permissão explícita, AWS não autoriza a solicitação. Se houver uma instrução explícita de permissão, ou se o tipo de autenticação for NONE, o código continuará.
- Verificar se a solicitação é permitida pela política de autenticação para o serviço. Se uma política de autenticação estiver habilitada, mas não houver uma declaração de permissão explícita, AWS não autoriza a solicitação. Se houver uma declaração explícita de permissão, ou se o tipo de autenticação for NONE, o código de imposição retornará uma decisão final de Permitir.
- Uma negação explícita em qualquer política substitui todas as permissões.

O diagrama mostra o fluxo de trabalho de autorização. Quando uma solicitação é feita, as políticas relevantes permitem ou negam o acesso da solicitação a um determinado serviço.



Controlar o tráfego no VPC Lattice usando grupos de segurança

AWS grupos de segurança atuam como firewalls virtuais, controlando o tráfego de rede de e para as entidades às quais estão associados. Com o VPC Lattice, você pode criar grupos de segurança e atribuí-los à associação VPC que conecta uma VPC a uma rede de serviços para aplicar proteções adicionais de segurança em nível de rede para sua rede de serviços. Se você conectar uma VPC a uma rede de serviços usando um VPC endpoint, também poderá atribuir grupos de segurança ao VPC endpoint. Da mesma forma, você pode atribuir grupos de segurança aos gateways de recursos que você cria para permitir o acesso aos recursos em sua VPC.

Conteúdo

- [Listas de prefixos gerenciados](#)
- [Regras de grupos de segurança](#)
- [Gerenciar grupos de segurança para uma associação de VPC](#)

Listas de prefixos gerenciados

O VPC Lattice fornece listas de prefixos gerenciados que incluem os endereços IP usados para rotear o tráfego pela rede VPC Lattice quando você usa uma associação de rede de serviços para conectar sua VPC a uma rede de serviços usando uma associação VPC. Eles IPs são links privados locais IPs ou públicos não roteáveis. IPs

É possível fazer referência à lista de prefixos gerenciados do VPC Lattice nas regras do seu grupo de segurança. Isso permite que o tráfego flua dos clientes por meio da rede de serviços do VPC Lattice e para os destinos do serviço VPC Lattice.

Por exemplo, suponha que você tenha uma EC2 instância registrada como destino na região Oeste dos EUA (Oregon) (us-west-2). Você pode adicionar uma regra ao grupo de segurança da instância que permita acesso HTTPS de entrada da lista de prefixos gerenciados do VPC Lattice, para que o tráfego do VPC Lattice nessa região possa chegar na instância. Se você remover todas as outras regras de entrada do grupo de segurança, poderá impedir a chegada à instância de qualquer outro tráfego que não seja do VPC Lattice.

Os nomes das listas de prefixos gerenciados para o VPC Lattice são os seguintes:

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

Para obter mais informações, consulte [listaS de prefixos gerenciados da AWS](#) no Guia do usuário da Amazon VPC.

Clientes Windows e macOS

Os endereços nas listas de prefixos do VPC Lattice são endereços locais de link e endereços públicos não roteáveis. Se você se conectar à VPC Lattice a partir desses clientes, deverá atualizar suas configurações para que ela encaminhe os endereços IP na lista de prefixos gerenciados para o endereço IP primário do cliente. Veja a seguir um exemplo de comando que atualiza a configuração do cliente Windows, onde 169.254.171.0 está um dos endereços na lista de prefixos gerenciados.

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

Veja a seguir um exemplo de comando que atualiza a configuração do cliente macOS, onde 169.254.171.0 está um dos endereços na lista de prefixos gerenciados.

```
sudo route -n add -net 169.254.171.0 primary-ip-address 255.255.255.0
```

Para evitar a criação de uma rota estática, recomendamos que você use um endpoint de rede de serviços em uma VPC para estabelecer conectividade. Para obter mais informações, consulte [the section called “Gerencie associações de endpoints de VPC”](#).

Regras de grupos de segurança

Usar o VPC Lattice com ou sem grupos de segurança não afetará sua configuração de grupo de segurança da VPC existente. No entanto, você pode adicionar seus próprios grupos de segurança a qualquer momento.

Considerações importantes

- As regras do grupo de segurança para clientes controlam o tráfego de saída para o VPC Lattice.
- As regras do grupo de segurança para alvos controlam o tráfego de entrada do VPC Lattice para os alvos, incluindo o tráfego de verificação de integridade.
- As regras do grupo de segurança para a associação entre a rede de serviços e a VPC controlam quais clientes podem acessar a rede de serviços do VPC Lattice.
- As regras de grupo de segurança para o gateway de recursos controlam o tráfego de saída do gateway de recursos para os recursos.

Regras de saída recomendadas para tráfego que flui do gateway de recursos para um recurso de banco de dados

Para que o tráfego flua do gateway de recursos para os recursos, você deve criar regras de saída para as portas abertas e protocolos de escuta aceitos para os recursos.

Destino	Protocolo	Intervalo de portas	Comentário
<i>CIDR range for resource</i>	<i>TCP</i>	<i>3306</i>	Permitir tráfego do gateway de recursos para bancos de dados

Regras de entrada recomendadas para redes de serviço e associações de VPC

Para que o tráfego flua do cliente VPCs para os serviços associados à rede de serviços, você deve criar regras de entrada para as portas do listener e protocolos do listener para os serviços.

Origem	Protocolo	Intervalo de portas	Comentário
<i>VPC CIDR</i>	<i>listener</i>	<i>listener</i>	Permita o tráfego de clientes para o VPC Lattice

Regras de saída recomendadas para o fluxo de tráfego das instâncias do cliente para o VPC Lattice

Por padrão, os grupos de segurança permitem todo o tráfego de saída. No entanto, se você tiver regras de saída personalizadas, deverá permitir o tráfego de saída para o prefixo VPC Lattice para portas e protocolos de ouvinte para que as instâncias do cliente possam se conectar a todos os serviços associados à rede de serviços VPC Lattice. Você pode permitir esse tráfego fazendo referência ao ID da lista de prefixos do VPC Lattice.

Destino	Protocolo	Intervalo de portas	Comentário
<i>ID of the VPC Lattice prefix list</i>	<i>listener</i>	<i>listener</i>	Permita o tráfego de clientes para o VPC Lattice

Regras de entrada recomendadas para o fluxo de tráfego do VPC Lattice para as instâncias de destino

Você não pode usar o grupo de segurança do cliente como origem para os grupos de segurança do seu destino, porque o tráfego é proveniente do VPC Lattice. Você pode fazer referência ao ID da lista de prefixos do VPC Lattice.

Origem	Protocolo	Intervalo de portas	Comentário
<i>ID of the VPC Lattice prefix list</i>	<i>target</i>	<i>target</i>	Permitir tráfego do VPC Lattice para os destinos

Origem	Protocolo	Intervalo de portas	Comentário
<i>ID of the VPC Lattice prefix list</i>	<i>health check</i>	<i>health check</i>	Permitir a verificação de integridade do tráfego do VPC Lattice para os destinos

Gerenciar grupos de segurança para uma associação de VPC

Você pode usar o AWS CLI para visualizar, adicionar ou atualizar grupos de segurança na VPC para atender à associação de rede. Ao usar o AWS CLI, lembre-se de que seus comandos são Região da AWS executados no configurado para seu perfil. Se você deseja executar os comandos em uma região diferente, altere a região padrão para o seu perfil ou use o parâmetro `--region` com o comando.

Antes de começar, confirme se você criou o grupo de segurança na mesma VPC que você deseja adicionar à rede de serviços. Para obter mais informações, consulte [Controle o tráfego para seus recursos usando grupos de segurança](#) no Guia do usuário da Amazon VPC

Para adicionar um grupo de segurança ao criar uma associação de VPC usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.
4. Na guia Associações de VPC, escolha Criar associações de VPC e, em seguida, escolha Adicionar associação de VPC.
5. Selecione uma VPC e até cinco grupos de segurança.
6. Escolha Salvar alterações.

Para adicionar ou atualizar grupos de segurança para uma associação de VPC existente usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, em VPC Lattice, escolha Redes de serviço.
3. Selecione o nome da rede de serviços para abrir sua página de detalhes.

4. Na guia Associações de VPC, marque a caixa de seleção da associação e escolha Ações, Editar grupos de segurança.
5. Adicione e remova grupos de segurança conforme necessário.
6. Escolha Salvar alterações.

Para adicionar um grupo de segurança ao criar uma associação de VPC usando o AWS CLI

Use o comando [create-service-network-vpc-association](#), especificando a ID da VPC para a associação da VPC e a ID dos grupos de segurança a serem adicionados.

```
aws vpc-lattice create-service-network-vpc-association \
  --service-network-identifier sn-0123456789abcdef0 \
  --vpc-identifier vpc-1a2b3c4d \
  --security-group-ids sg-7c2270198example
```

Se houver êxito, o comando gerará uma saída semelhante à seguinte.

```
{
  "arn": "arn",
  "createdBy": "464296918874",
  "id": "snva-0123456789abcdef0",
  "status": "CREATE_IN_PROGRESS",
  "securityGroupIds": ["sg-7c2270198example"]
}
```

Para adicionar ou atualizar grupos de segurança para uma associação de VPC existente usando a AWS CLI

Use o comando [update-service-network-vpc-association](#), especificando o ID da rede de serviços e dos grupos IDs de segurança. Esses grupos de segurança substituem qualquer outro grupo de segurança anteriormente associado. Defina pelo menos um grupo de segurança ao atualizar a lista.

```
aws vpc-lattice update-service-network-vpc-association
  --service-network-vpc-association-identifier sn-903004f88example \
  --security-group-ids sg-7c2270198example sg-903004f88example
```

⚠ Warning

Não é possível remover todos os grupos de segurança. Em vez disso, primeiro você deve excluir a associação de VPC e, em seguida, recriar a associação de VPC sem nenhum grupo de segurança. Tenha cuidado ao excluir a associação de VPC. Isso impede que o tráfego chegue aos serviços que estão nessa rede de serviços.

Controle o tráfego para o VPC Lattice usando a rede ACLs

Uma lista de controle de acesso (ACL) de rede permite ou não determinado tráfego de entrada ou de saída no nível da sub-rede. A ACL de rede padrão permite todo o tráfego de entrada e saída. Você pode criar uma rede personalizada ACLs para suas sub-redes para fornecer uma camada adicional de segurança. Para obter mais informações, consulte [Rede ACLs](#) no Guia do usuário da Amazon VPC.

Conteúdo

- [Rede ACLs para suas sub-redes de clientes](#)
- [Rede ACLs para suas sub-redes de destino](#)

Rede ACLs para suas sub-redes de clientes

A rede ACLs para sub-redes de clientes deve permitir tráfego entre clientes e o VPC Lattice. Você pode obter os intervalos de endereços IP permitidos na [lista de prefixos gerenciados](#) do VPC Lattice.

Veja a seguir um exemplo de regra de entrada.

Origem	Protocolo	Intervalo de portas	Comentário
<i>vpc_lattice_cidr_block</i>	TCP	1025-65535	Permitir tráfego do VPC Lattice para clientes

Veja a seguir um exemplo de uma regra de saída.

Destino	Protocolo	Intervalo de portas	Comentário
<i>vpc_lattice_cidr_block</i>	<i>listener</i>	<i>listener</i>	Permita o tráfego de clientes para o VPC Lattice

Rede ACLs para suas sub-redes de destino

A rede das sub-redes ACLs de destino deve permitir o tráfego entre os destinos e o VPC Lattice na porta de destino e na porta de verificação de integridade. Você pode obter os intervalos de endereços IP permitidos na [lista de prefixos gerenciados](#) do VPC Lattice.

Veja a seguir um exemplo de regra de entrada.

Origem	Protocolo	Intervalo de portas	Comentário
<i>vpc_lattice_cidr_block</i>	<i>target</i>	<i>target</i>	Permitir tráfego do VPC Lattice para os destinos
<i>vpc_lattice_cidr_block</i>	<i>health check</i>	<i>health check</i>	Permitir a verificação de integridade do tráfego do VPC Lattice para os destinos

Veja a seguir um exemplo de uma regra de saída.

Destino	Protocolo	Intervalo de portas	Comentário
<i>vpc_lattice_cidr_block</i>	<i>target</i>	1024-65535	Permitir tráfego de destinos para o VPC Lattice
<i>vpc_lattice_cidr_block</i>	<i>health check</i>	1024-65535	Permitir tráfego de verificação de

Destino	Protocolo	Intervalo de portas	Comentário
			integridade de destinos para o VPC Lattice

SIGv4 solicitações autenticadas para o Amazon VPC Lattice

O VPC Lattice usa Signature Version 4 (SIGv4) ou Signature Version 4A (A) para autenticação do SIGv4 cliente. Para obter mais informações, consulte [AWS Signature versão 4 para solicitações de API](#) no Guia do usuário do IAM.

Considerações

- O VPC Lattice tenta autenticar qualquer solicitação assinada com ou A. SIGv4 SIGv4 Solicitações sem autenticação falharão.
- O VPC Lattice não oferece suporte à assinatura de carga útil. Você deve enviar um cabeçalho x-amz-content-sha256 com o valor definido como "UNSIGNED-PAYLOAD".

Exemplos

- [Python](#)
- [Java](#)
- [Node.js](#)
- [Golang](#)
- [Golang - GRPC](#)

Python

Este exemplo envia as solicitações assinadas por uma conexão segura com um serviço registrado na rede. Se você preferir usar [solicitações](#), o pacote [botocore](#) simplifica o processo de autenticação, mas não é estritamente obrigatório. Para obter mais informações, consulte [Credenciais](#) na documentação do Boto3.

Para instalar os awscrt pacotes botocore e, use o comando a seguir. Para obter mais informações, consulte [AWS CRT Python](#).

```
pip install botocore awscrt
```

Se você executar o aplicativo cliente no Lambda, instale os módulos necessários usando [camadas do Lambda](#) ou inclua-os em seu pacote de implantação.

No exemplo a seguir, substitua os valores do espaço reservado pelos seus próprios valores.

SIGv4

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

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtSigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
    'us-west-2')
    endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-
    west-2.on.aws'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':
    'UNSIGNED-PAYLOAD'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False
    signer.add_auth(request)

    prepped = request.prepare()

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

SIGv4A

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

if __name__ == '__main__':
    session = botocore.session.Session()
```

```
signer = crt.auth.CrtSigV4AsymAuth(session.get_credentials(), 'vpc-lattice-  
svcs', '*')  
endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-  
west-2.on.aws'  
data = "some-data-here"  
headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':  
'UNSIGNED-PAYLOAD'}  
request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)  
request.context["payload_signing_enabled"] = False  
signer.add_auth(request)  
  
prepped = request.prepare()  
  
response = requests.post(prepped.url, headers=prepped.headers, data=data)  
print(response.text)
```

Java

Este exemplo mostra como você pode realizar a assinatura de solicitações usando interceptores personalizados. Ele usa a classe de provedor de credenciais padrão do [AWS SDK for Java 2.x](#), que obtém as credenciais corretas para você. Se você preferir usar um provedor de credenciais específico, você pode selecionar um no [AWS SDK for Java 2.x](#). O AWS SDK para Java permite somente cargas não assinadas por HTTPS. No entanto, você pode estender o signatário para oferecer suporte a cargas úteis não assinadas por HTTP.

SIGv4

```
package com.example;  
  
import software.amazon.awssdk.http.auth.aws.signer.AwsV4HttpSigner;  
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;  
  
import software.amazon.awssdk.http.SdkHttpMethod;  
import software.amazon.awssdk.http.SdkHttpClient;  
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;  
import software.amazon.awssdk.http.SdkHttpRequest;  
import software.amazon.awssdk.http.apache.ApacheHttpClient;  
import software.amazon.awssdk.http.HttpExecuteRequest;  
import software.amazon.awssdk.http.HttpExecuteResponse;  
import java.io.IOException;  
import java.net.URI;
```

```

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

public class sigv4 {

    public static void main(String[] args) {
        AwsV4HttpSigner signer = AwsV4HttpSigner.create();

        AwsCredentialsIdentity credentials =
DefaultCredentialsProvider.create().resolveCredentials();

        if (args.length < 2) {
            System.out.println("Usage: sample <url> <region>");
            System.exit(1);
        }
        // Create the HTTP request to be signed
        var url = args[0];
        SdkHttpRequest httpRequest = SdkHttpRequest.builder()
            .uri(URI.create(url))
            .method(SdkHttpMethod.GET)
            .build();

        SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
            .request(httpRequest)
            .putProperty(AwsV4HttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")

            .putProperty(AwsV4HttpSigner.PAYLOAD_SIGNING_ENABLED, false)
            .putProperty(AwsV4HttpSigner.REGION_NAME, args[1]));

        System.out.println("[*] Raw request headers:");
        signedRequest.request().headers().forEach((key, values) -> {
            values.forEach(value -> System.out.println("  " + key + ": " + value));
        });

        try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
            HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
                .request(signedRequest.request())
                .contentStreamProvider(signedRequest.payload().orElse(null))
                .build();

            System.out.println("[*] Sending request to: " + url);

            HttpExecuteResponse httpResponse =
httpClient.prepareRequest(httpExecuteRequest).call();

```

```

        System.out.println("[*] Request sent");

        System.out.println("[*] Response status code: " +
        httpResponse.httpResponse().statusCode());
        // Read and print the response body
        httpResponse.responseBody().ifPresent(inputStream -> {
            try {
                String responseBody = new String(inputStream.readAllBytes());
                System.out.println("[*] Response body: " + responseBody);
            } catch (IOException e) {
                System.err.println("[*] Failed to read response body");
                e.printStackTrace();
            } finally {
                try {
                    inputStream.close();
                } catch (IOException e) {
                    System.err.println("[*] Failed to close input stream");
                    e.printStackTrace();
                }
            }
        });
    } catch (IOException e) {
        System.err.println("[*] HTTP Request Failed.");
        e.printStackTrace();
    }
}
}

```

SIGv4A

Este exemplo requer uma dependência adicional de `software.amazon.awssdk:http-auth-aws-crt`

```

package com.example;

import software.amazon.awssdk.http.auth.aws.signer.AwsV4aHttpSigner;
import software.amazon.awssdk.http.auth.aws.signer.RegionSet;
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;

import software.amazon.awssdk.http.SdkHttpMethod;

```

```

import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;
import software.amazon.awssdk.http.SdkHttpRequest;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.http.HttpExecuteRequest;
import software.amazon.awssdk.http.HttpExecuteResponse;
import java.io.IOException;
import java.net.URI;
import java.util.Arrays;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

public class sigv4a {

    public static void main(String[] args) {
        AwsV4aHttpSigner signer = AwsV4aHttpSigner.create();

        AwsCredentialsIdentity credentials =
DefaultCredentialsProvider.create().resolveCredentials();

        if (args.length < 2) {
            System.out.println("Usage: sample <url> <regionset>");
            System.exit(1);
        }
        // Create the HTTP request to be signed
        var url = args[0];
        SdkHttpRequest httpRequest = SdkHttpRequest.builder()
            .uri(URI.create(url))
            .method(SdkHttpMethod.GET)
            .build();

        SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
            .request(httpRequest)
            .putProperty(AwsV4aHttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
            .putProperty(AwsV4aHttpSigner.PAYLOAD_SIGNING_ENABLED, false)
            .putProperty(AwsV4aHttpSigner.REGION_SET,
RegionSet.create(String.join(" ",Arrays.copyOfRange(args, 1, args.length)))));

        System.out.println("[*] Raw request headers:");
        signedRequest.request().headers().forEach((key, values) -> {
            values.forEach(value -> System.out.println("  " + key + ": " + value));
        });
    }
}

```

```

try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
    HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
        .request(signedRequest.request())
        .contentStreamProvider(signedRequest.payload().orElse(null))
        .build();

    System.out.println("[*] Sending request to: " + url);

    HttpExecuteResponse httpResponse =
httpClient.prepareRequest(httpExecuteRequest).call();

    System.out.println("[*] Request sent");

    System.out.println("[*] Response status code: " +
httpClient.httpResponse().statusCode());
    // Read and print the response body
    httpResponse.responseBody().ifPresent(inputStream -> {
        try {
            String responseBody = new String(inputStream.readAllBytes());
            System.out.println("[*] Response body: " + responseBody);
        } catch (IOException e) {
            System.err.println("[*] Failed to read response body");
            e.printStackTrace();
        } finally {
            try {
                inputStream.close();
            } catch (IOException e) {
                System.err.println("[*] Failed to close input stream");
                e.printStackTrace();
            }
        }
    });
} catch (IOException e) {
    System.err.println("[*] HTTP Request Failed.");
    e.printStackTrace();
}
}
}

```

Node.js

Este exemplo usa [vinculações NodeJS aws-crt](#) para enviar uma solicitação assinada usando HTTPS.

Para instalar o pacote `aws-crt`, execute o comando a seguir.

```
npm -i aws-crt
```

Se a variável de ambiente `AWS_REGION` existir, o exemplo usará a região especificada por `AWS_REGION`. A região padrão é `us-east-1`.

SIGv4

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
  const host = new URL(endpoint).host
  const request = new HttpRequest(method, endpoint)
  request.headers.add('host', host)
  // crt.io.enable_logging(crt.io.LogLevel.INFO)
  const config = {
    service: service,
    region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
    algorithm: algorithm,
    signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
    signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
    signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
    provider: crt.auth.AwsCredentialsProvider.newDefault()
  }

  return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs', algorithm).then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
```

```

    headers[sigv4header[0]] = sigv4header[1]
  }

  const options = {
    hostname: new URL(process.argv[2]).host,
    path: new URL(process.argv[2]).pathname,
    method: 'GET',
    headers: headers
  }

  req = https.request(options, res => {
    console.log('statusCode:', res.statusCode)
    console.log('headers:', res.headers)
    res.on('data', d => {
      process.stdout.write(d)
    })
  })
  req.on('error', err => {
    console.log('Error: ' + err)
  })
  req.end()
}
)

```

SIGv4A

```

const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
  const host = new URL(endpoint).host
  const request = new HttpRequest(method, endpoint)
  request.headers.add('host', host)
  // crt.io.enable_logging(crt.io.LogLevel.INFO)
  const config = {
    service: service,
    region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
    algorithm: algorithm,
    signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
    signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
    signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
    provider: crt.auth.AwsCredentialsProvider.newDefault()
  }
}

```

```
    }

    return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4Asymmetric;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs', algorithm).then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: new URL(process.argv[2]).pathname,
      method: 'GET',
      headers: headers
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)
```

Golang

Este exemplo usa os [geradores de código Smithy para Go](#) e o [AWS SDK para a linguagem de programação Go](#) para lidar com solicitações de assinatura de solicitações. O exemplo requer uma versão Go de 1.21 ou superior.

SIGv4

```
package main

import (
    "context"
    "flag"
    "fmt"
    "io"
    "log"
    "net/http"
    "net/http/httputil"
    "os"
    "strings"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/smithy-go/aws-http-auth/credentials"
    "github.com/aws/smithy-go/aws-http-auth/sigv4"
    v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
    io.ReadSeeker
}

func (nopCloser) Close() error {
    return nil
}

type stringFlag struct {
    set    bool
    value  string
}

flag.PrintDefaults()
```

```
    os.Exit(1)
}

func main() {
    flag.Parse()
    if !url.set || !region.set {
        Usage()
    }

    cfg, err := config.LoadDefaultConfig(context.TODO(),
config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    if len(os.Args) < 2 {
        log.Fatalf("Usage: go run main.go <url>")
    }

    // Retrieve credentials from an SDK source, such as the instance profile
    sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
    if err != nil {
        log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
    }

    creds := credentials.Credentials{
        AccessKeyID:      sdkCreds.AccessKeyID,
        SecretAccessKey:  sdkCreds.SecretAccessKey,
        SessionToken:     sdkCreds.SessionToken,
    }

    // Add a payload body, which will not be part of the signature calculation
    body := nopCloser{strings.NewReader(`Example payload body`)}

    req, _ := http.NewRequest(http.MethodPost, url.value, body)

    // Create a sigv4a signer with specific options
    signer := sigv4.New(func(o *v4.SignerOptions) {
        o.DisableDoublePathEscape = true
        // This will add the UNSIGNED-PAYLOAD sha256 header
        o.AddPayloadHashHeader = true
        o.DisableImplicitPayloadHashing = true
    })
```

```

SDK      // Perform the signing on req, using the credentials we retrieved from the

err = signer.SignRequest(&sigv4.SignRequestInput{
    Request:    req,
    Credentials: creds,
    Service:    "vpc-lattice-svcs",
    Region:    region.String(),
})

if err != nil {
    log.Fatalf("%s", err)
}

res, err := httputil.DumpRequest(req, true)

if err != nil {
    log.Fatalf("%s", err)
}

log.Printf("[*] Raw request\n%s\n", string(res))

log.Printf("[*] Sending request to %s\n", url.value)

resp, err := http.DefaultClient.Do(req)
if err != nil {
    log.Fatalf("%s", err)
}

log.Printf("[*] Request sent\n")

log.Printf("[*] Response status code: %d\n", resp.StatusCode)

respBody, err := io.ReadAll(resp.Body)
if err != nil {
    log.Fatalf("%s", err)
}

log.Printf("[*] Response body: \n%s\n", respBody)
}

```

SIGv4A

```
package main
```

```
import (
    "context"
    "flag"
    "fmt"
    "io"
    "log"
    "net/http"
    "net/http/httputil"
    "os"
    "strings"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/smithy-go/aws-http-auth/credentials"
    "github.com/aws/smithy-go/aws-http-auth/sigv4a"
    v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
    io.ReadSeeker
}

func (nopCloser) Close() error {
    return nil
}

type stringFlag struct {

func main() {
    flag.Parse()
    if !url.set || !regionSet.set {
        Usage()
    }

    cfg, err := config.LoadDefaultConfig(context.TODO(),
config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    if len(os.Args) < 2 {
        log.Fatalf("Usage: go run main.go <url>")
    }
}
```

```

// Retrieve credentials from an SDK source, such as the instance profile
sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
if err != nil {
    log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
}

creds := credentials.Credentials{
    AccessKeyID:    sdkCreds.AccessKeyID,
    SecretAccessKey: sdkCreds.SecretAccessKey,
    SessionToken:   sdkCreds.SessionToken,
}

// Add a payload body, which will not be part of the signature calculation
body := nopCloser{strings.NewReader(`Example payload body`)}

req, _ := http.NewRequest(http.MethodPost, url.value, body)

// Create a sigv4a signer with specific options
signer := sigv4a.New(func(o *v4.SignerOptions) {
    o.DisableDoublePathEscape = true
    // This will add the UNSIGNED-PAYLOAD sha256 header
    o.AddPayloadHashHeader = true
    o.DisableImplicitPayloadHashing = true
})

// Create a slice out of the provided regionset
rs := strings.Split(regionSet.value, ",")

// Perform the signing on req, using the credentials we retrieved from the
SDK
err = signer.SignRequest(&sigv4a.SignRequestInput{
    Request:    req,
    Credentials: creds,
    Service:    "vpc-lattice-svcs",
    RegionSet:  rs,
})

if err != nil {
    log.Fatalf("%s", err)
}

res, err := httputil.DumpRequest(req, true)

```

```
    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Raw request\n%s\n", string(res))

    log.Printf("[*] Sending request to %s\n", url.value)

    resp, err := http.DefaultClient.Do(req)
    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Request sent\n")

    log.Printf("[*] Response status code: %d\n", resp.StatusCode)

    respBody, err := io.ReadAll(resp.Body)
    if err != nil {
        log.Fatalf("%s", err)
    }

    log.Printf("[*] Response body: \n%s\n", respBody)
}
```

Golang - GRPC

Este exemplo usa o [AWS SDK para a linguagem de programação Go](#) para lidar com a assinatura de solicitações de GRPC. Isso pode ser usado com o [servidor de eco do repositório](#) de código de amostra do GRPC.

```
package main

import (
    "context"
    "crypto/tls"
    "crypto/x509"

    "flag"
    "fmt"
    "log"
    "net/http"
```

```

"net/url"
"strings"
"time"

"google.golang.org/grpc"
"google.golang.org/grpc/credentials"

"github.com/aws/aws-sdk-go-v2/aws"
v4 "github.com/aws/aws-sdk-go-v2/aws/signer/v4"
"github.com/aws/aws-sdk-go-v2/config"

ecpb "google.golang.org/grpc/examples/features/proto/echo"
)

const (
    headerContentSha      = "x-amz-content-sha256"
    headerSecurityToken   = "x-amz-security-token"
    headerDate            = "x-amz-date"
    headerAuthorization   = "authorization"
    unsignedPayload       = "UNSIGNED-PAYLOAD"
)

type SigV4GrpcSigner struct {
    service      string
    region       string
    credProvider aws.CredentialsProvider
    signer       *v4.Signer
}

func NewSigV4GrpcSigner(service string, region string, credProvider
aws.CredentialsProvider) *SigV4GrpcSigner {
    signer := v4.NewSigner()
    return &SigV4GrpcSigner{
        service:      service,
        region:       region,
        credProvider: credProvider,
        signer:       signer,
    }
}

func (s *SigV4GrpcSigner) GetRequestMetadata(ctx context.Context, uri ...string)
(map[string]string, error) {
    ri, _ := credentials.RequestInfoFromContext(ctx)
    creds, err := s.credProvider.Retrieve(ctx)

```

```

    if err != nil {
        return nil, fmt.Errorf("failed to load credentials: %w", err)
    }

    // The URI we get here is scheme://authority/service/ - for signing we want to
    include the RPC name
    // But RequestInfoFromContext only has the combined /service/rpc-name - so read the
    URI, and
    // replace the Path with what we get from RequestInfo.
    parsed, err := url.Parse(uri[0])
    if err != nil {
        return nil, err
    }
    parsed.Path = ri.Method

    // Build a request for the signer.
    bodyReader := strings.NewReader("")
    req, err := http.NewRequest("POST", uri[0], bodyReader)
    if err != nil {
        return nil, err
    }
    date := time.Now()
    req.Header.Set(headerContentSha, unsignedPayload)
    req.Header.Set(headerDate, date.String())
    if creds.SessionToken != "" {
        req.Header.Set(headerSecurityToken, creds.SessionToken)
    }
    // The signer wants this as //authority/path
    // So get this by trimming off the scheme and the colon before the first slash.
    req.URL.Opaque = strings.TrimPrefix(parsed.String(), parsed.Scheme+":")

    err = s.signer.SignHTTP(context.Background(), creds, req, unsignedPayload,
s.service, s.region, date)
    if err != nil {
        return nil, fmt.Errorf("failed to sign request: %w", err)
    }

    // Pull the relevant headers out of the signer, and return them to get
    // included in the request we make.
    reqHeaders := map[string]string{
        headerContentSha: req.Header.Get(headerContentSha),
        headerDate:       req.Header.Get(headerDate),
        headerAuthorization: req.Header.Get(headerAuthorization),
    }

```

```

    if req.Header.Get(headerSecurityToken) != "" {
        reqHeaders[headerSecurityToken] = req.Header.Get(headerSecurityToken)
    }

    return reqHeaders, nil
}

func (c *SigV4GrpcSigner) RequireTransportSecurity() bool {
    return true
}

var addr = flag.String("addr", "some-lattice-service:443", "the address to connect to")
var region = flag.String("region", "us-west-2", "region")

func callUnaryEcho(client ecpb.EchoClient, message string) {
    ctx, cancel := context.WithTimeout(context.Background(), 10*time.Second)
    defer cancel()
    resp, err := client.UnaryEcho(ctx, &ecpb.EchoRequest{Message: message})
    if err != nil {
        log.Fatalf("client.UnaryEcho(_) = _, %v: ", err)
    }
    fmt.Println("UnaryEcho: ", resp.Message)
}

func main() {
    flag.Parse()
    cfg, err := config.LoadDefaultConfig(context.TODO(),
    config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    pool, _ := x509.SystemCertPool()
    tlsConfig := &tls.Config{
        RootCAs: pool,
    }

    authority, _, _ := strings.Cut(*addr, ":") // Remove the port from the addr
    opts := []grpc.DialOption{
        grpc.WithTransportCredentials(credentials.NewTLS(tlsConfig)),

        // Lattice needs both the Authority to be set (without a port), and the SigV4
    signer
    grpc.WithAuthority(authority),

```

```
    grpc.WithPerRPCCredentials(NewSigV4GrpcSigner("vpc-lattice-svcs", *region,
cfg.Credentials)),
}

conn, err := grpc.Dial(*addr, opts...)

if err != nil {
    log.Fatalf("did not connect: %v", err)
}
defer conn.Close()
rgc := ecgp.NewEchoClient(conn)

callUnaryEcho(rgc, "hello world")
}
```

Proteção de dados no Amazon VPC Lattice

O [modelo de responsabilidade AWS compartilhada](#) se aplica à proteção de dados no Amazon VPC Lattice. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas Frequentes sobre Privacidade de Dados](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) no Blog de segurança da AWS.

Criptografia em trânsito

O VPC Lattice é um serviço totalmente gerenciado que consiste em um ambiente de gerenciamento e um plano de dados. Cada ambiente serve a um propósito distinto no serviço. O plano de controle fornece o administrativo APIs usado para criar, ler/descrever, atualizar, excluir e listar recursos (CRUDL) (por exemplo, `CreateService` e `UpdateService`). As comunicações com o plano de controle do VPC Lattice são protegidas em trânsito pelo TLS. O plano de dados é a API VPC Lattice `Invoke`, que fornece a interconexão entre os serviços. O TLS criptografa as comunicações com o plano de dados do VPC Lattice quando você usa HTTPS ou TLS. O conjunto de cifras e a versão do protocolo usam os padrões fornecidos pelo VPC Lattice e não são configuráveis. Para obter mais informações, consulte [Receptores HTTPS para serviços VPC Lattice](#).

Criptografia inativa

Por padrão, a criptografia de dados em repouso reduz a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, isso permite que você crie aplicações seguras que atendam aos rigorosos requisitos regulatórios e de conformidade de criptografia.

Conteúdo

- [Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 \(SSE-S3\)](#)
- [Criptografia do lado do servidor com AWS KMS chaves armazenadas em AWS KMS \(SSE-KMS\)](#)

Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)

Quando você usa criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3), cada objeto é criptografado com uma chave exclusiva. Como proteção adicional, criptografamos a chave em si com uma chave raiz que rotacionamos regularmente. A criptografia no lado do servidor do Amazon S3 usa uma das criptografias de bloco mais fortes disponíveis, o GCM padrão de criptografia avançada de 256 bits (AES-256), para criptografar seus dados. Sobre objetos criptografados antes do AES-GCM, o AES-CBC ainda é compatível com a descriptografia desses objetos. Para obter mais informações, consulte [Como usar criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 \(SSE-S3\)](#).

Se você habilitar a criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) para seu bucket do S3 para registros de acesso do VPC Lattice, nós criptografamos automaticamente cada arquivo de log de acesso antes que ele seja armazenado em seu bucket do S3. Para obter mais informações, consulte [Registros enviados para o Amazon S3 no Guia CloudWatch](#) do usuário da Amazon.

Criptografia do lado do servidor com AWS KMS chaves armazenadas em AWS KMS (SSE-KMS)

A criptografia do lado do servidor com AWS KMS chaves (SSE-KMS) é semelhante à SSE-S3, mas com benefícios e cobranças adicionais pelo uso desse serviço. Há permissões separadas para a AWS KMS chave que fornecem proteção adicional contra o acesso não autorizado de seus objetos no Amazon S3. O SSE-KMS também fornece uma trilha de auditoria que mostra quando e por quem sua AWS KMS chave foi usada. Para obter mais informações, consulte [Utilização da criptografia no lado do servidor com o AWS Key Management Service \(SSE-KMS\)](#).

Conteúdo

- [Criptografia e decodificação da chave privada do seu certificado](#)
- [Contexto de criptografia para o VPC Lattice](#)
- [Monitoramento das suas chaves de criptografia para o VPC Lattice](#)

Criptografia e decodificação da chave privada do seu certificado

Seu certificado ACM e sua chave privada são criptografados usando uma chave KMS AWS gerenciada que tem o alias `aws/acm`. Você pode ver o ID da chave com esse alias no AWS KMS console, em chaves AWS gerenciadas.

O VPC Lattice não acessa diretamente seus recursos do ACM. Ele usa o Gerenciador de AWS Conexões TLS para proteger e acessar as chaves privadas do seu certificado. Quando você usa seu certificado do ACM para criar um serviço VPC Lattice, o VPC Lattice associa seu certificado ao AWS TLS Connection Manager. Isso é feito criando uma concessão em AWS KMS relação à sua chave AWS gerenciada com o prefixo `aws/acm`. Uma concessão é um instrumento de política que permite que o TLS Connection Manager usem chaves do KMS em operações de criptografia. A concessão permite que a entidade principal autorizada (TLS Connection Manager) chame as operações de concessão especificadas na chave do KMS para decifrar a chave privada do seu certificado. Em seguida, o TLS Connection Manager usará o certificado e a chave privada descriptografada (texto simples) para estabelecer uma conexão segura (sessão SSL/TLS) com clientes de serviços do VPC Lattice. Quando o certificado for desassociado de um serviço VPC Lattice, a concessão será removida.

Se você quiser remover o acesso à chave KMS, recomendamos que você substitua ou exclua o certificado do serviço usando o AWS Management Console ou o `update-service` comando no AWS CLI

Contexto de criptografia para o VPC Lattice

Um [contexto de criptografia](#) é um conjunto opcional de pares de valores-chave que contêm informações contextuais sobre para que sua chave privada pode ser usada. AWS KMS vincula o contexto de criptografia aos dados criptografados e os usa como dados autenticados adicionais para oferecer suporte à criptografia autenticada.

Quando suas chaves TLS são usadas com o VPC Lattice e o TLS Connection manager, o nome do seu serviço VPC Lattice é incluído no contexto de criptografia usado para criptografar sua chave em repouso. Você pode verificar para qual serviço VPC Lattice seu certificado e sua chave privada

estão sendo usados visualizando o contexto de criptografia em seus CloudTrail registros, conforme mostrado na próxima seção, ou examinando a guia Recursos associados no console do ACM.

Para descriptografar os dados, o mesmo contexto de criptografia é incluído na solicitação. O VPC Lattice usa o mesmo contexto de criptografia em todas as operações criptográficas do AWS KMS, onde a chave está `aws:vpc-lattice:arn` e o valor é o Amazon Resource Name (ARN) do serviço VPC Lattice.

O seguinte exemplo mostra o contexto de criptografia na saída de uma operação como `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"
}
```

Monitoramento das suas chaves de criptografia para o VPC Lattice

Quando você usa uma chave AWS gerenciada com seu serviço VPC Lattice, você pode usá-la [AWS CloudTrail](#) para rastrear solicitações enviadas pela VPC Lattice. AWS KMS

CreateGrant

Quando você adiciona seu certificado do ACM a um serviço VPC Lattice, uma solicitação `CreateGrant` é enviada em seu nome para que o TLS Connection manager possa descriptografar a chave privada associada ao seu certificado do ACM.

Você pode ver a `CreateGrant` operação como um evento em CloudTrail, Histórico de eventos, `CreateGrant`.

Veja a seguir um exemplo de registro de CloudTrail evento no histórico de eventos da `CreateGrant` operação.

```
{
  "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"
  }
}

```

No `CreateGrant` exemplo acima, o principal beneficiário é o Gerenciador de Conexões TLS, e o contexto de criptografia tem o ARN do serviço VPC Lattice.

ListGrants

Você pode usar o ID da chave do KMS e o ID da conta para chamar a API `ListGrants`. Ela fornecerá uma lista de todas as concessões para a chave do KMS especificada. Para obter mais informações, consulte [ListGrants](#).

Use o `ListGrants` comando a seguir no AWS CLI para ver os detalhes de todas as concessões.

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

O seguinte é um exemplo de saída.

```

{
  "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"
            }
        }
    }
}

```

No ListGrants exemplo acima, o principal beneficiário é o Gerenciador de Conexões TLS e o contexto de criptografia tem o ARN do serviço VPC Lattice.

Decrypt

O VPC Lattice usa o TLS Connection manager para chamar a operação Decrypt para descriptografar sua chave privada a fim de atender conexões TLS em seu serviço VPC Lattice. Você pode ver a Decrypt operação como um evento em Histórico de CloudTrail eventos, Decrypt.

Veja a seguir um exemplo de registro de CloudTrail evento no histórico de eventos da Decrypt operação.

```

{
    "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"
}
```

Identity and Access Management para o Amazon VPC Lattice

As seções a seguir descrevem como você pode usar o AWS Identity and Access Management (IAM) para ajudar a proteger seus recursos do VPC Lattice, controlando quem pode realizar ações da API do VPC Lattice.

Tópicos

- [Funcionamento do Amazon VPC Lattice com o IAM](#)
- [Permissões da API Amazon VPC Lattice](#)
- [Políticas baseadas em identidade para o Amazon VPC Lattice](#)
- [Usando funções vinculadas a serviços para Amazon VPC Lattice](#)
- [AWS políticas gerenciadas para Amazon VPC Lattice](#)

Funcionamento do Amazon VPC Lattice com o IAM

Antes de usar o IAM para gerenciar o acesso ao VPC Lattice, saiba quais recursos do IAM estão disponíveis para uso com o VPC Lattice.

Atributo do IAM	Compatibilidade com o VPC Lattice
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para uma visão de alto nível de como o VPC Lattice e AWS outros serviços funcionam com a maioria dos recursos do IAM, [AWS consulte os serviços que funcionam com](#) o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para o VPC Lattice

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elemento de política JSON do IAM](#) no Guia do usuário do IAM.

Políticas baseadas em recursos no VPC Lattice

Compatível com políticas baseadas em recursos: sim

Políticas baseadas em recursos são documentos de política JSON que você anexa a um recurso em AWS. Em AWS serviços que oferecem suporte a políticas baseadas em recursos, os administradores de serviços podem usá-las para controlar o acesso a um recurso específico desse serviço. AWS Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos.

O VPC Lattice oferece suporte a políticas de autenticação, uma política baseada em recursos que permite controlar o acesso aos serviços em sua rede de serviços. Para obter mais informações, consulte [Controle o acesso aos serviços do VPC Lattice usando políticas de autenticação](#).

O VPC Lattice também oferece suporte a políticas de permissões baseadas em recursos para integração com o AWS Resource Access Manager. Você pode usar essas políticas baseadas em recursos para conceder permissão para gerenciar a conectividade com outras AWS contas ou organizações para serviços, configurações de recursos e redes de serviços. Para obter mais informações, consulte [Compartilhe suas entidades do VPC Lattice](#).

Ações de políticas para o VPC Lattice

Compatível com ações de políticas: sim

Em uma declaração de política do IAM, é possível especificar qualquer ação de API de qualquer serviço que dê suporte ao IAM. Para o VPC Lattice, use o seguinte prefixo com o nome da ação de API `vpc-lattice:`. Por exemplo: `vpc-lattice:CreateService`, `vpc-lattice:CreateTargetGroup` e `vpc-lattice:PutAuthPolicy`.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, da seguinte maneira:

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

Também é possível especificar várias ações usando asteriscos. Por exemplo, é possível especificar todas as ações cujos nomes comecem com a palavra Get, da seguinte maneira:

```
"Action": "vpc-lattice:Get*"
```

Para obter uma lista completa das ações de API do VPC Lattice, consulte [Ações definidas pelo Amazon VPC Lattice](#) na Referência de autorização de serviço.

Recursos de políticas para o VPC Lattice

Compatível com recursos de políticas: sim

Em uma instrução de política do IAM, o elemento Resource especifica o objeto ou os objetos abrangidos pela instrução. Para o VPC Lattice, cada declaração de política do IAM se aplica aos recursos que você especifica usando eles. ARNs

O formato específico do nome do recurso da Amazon (ARN) dependerá do recurso. Ao fornecer um ARN, substitua o *italicized* texto pelas informações específicas do recurso.

- Inscrições em log de acesso:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:accesslogsubscription/access-log-subscription-id"
```

- Receptores:

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

- Gateways de recursos

```
"Resource": "arn:aws:vpc-lattice:region:account-id:resourcegateway/resource-gateway-id"
```

- Configuração de recursos

```
"Resource": "arn:aws:vpc-lattice:region:account-id:resourceconfiguration/resource-configuration-id"
```

- Regras:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/listener/listener-id/rule/rule-id"
```

- Serviços:

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

- Redes de serviços:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetwork/service-network-id"
```

- Associações a serviço de rede de serviços:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetworkserviceassociation/service-network-service-association-id"
```

- Associações de configuração de recursos de rede de serviços

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetworkresourceassociation/service-network-resource-association-id"
```

- Associações a VPC de rede de serviços:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetworkvpcassociation/service-network-vpc-association-id"
```

- Grupos de destino:

```
"Resource": "arn:aws:vpc-lattice:region:account-id:targetgroup/target-group-id"
```

Chaves de condição de política do VPC Lattice

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento Condition (ou bloco Condition) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento Condition é opcional. É possível criar expressões

condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos de Condition em uma declaração ou várias chaves em um único elemento de Condition, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos da política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do VPC Lattice, consulte Chaves de [condição do Amazon VPC Lattice](#) na Referência de autorização de serviço.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para obter informações sobre chaves de condição AWS globais, consulte [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Listas de controle de acesso (ACLs) na VPC Lattice

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso por atributos (ABAC) com o VPC Lattice

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é

a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte [Definir permissões com autorização do ABAC](#) no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Usar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

Usar credenciais temporárias com o VPC Lattice

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “[Trabalhe com o IAM](#)” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte [Alternar para um perfil do IAM \(console\)](#) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte [Credenciais de segurança temporárias no IAM](#).

Perfis de serviço para o VPC Lattice

Compatível com perfis de serviço: não

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

 Warning

Alterar as permissões de um perfil de serviço pode prejudicar a funcionalidade do VPC Lattice. Apenas edite os perfis de serviço quando o VPC Lattice orientar você a fazer isso.

Perfis vinculados a serviço para o VPC Lattice

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados a serviço.

Para obter informações sobre como criar ou gerenciar perfis vinculadas a serviço do VPC Lattice, consulte [Usando funções vinculadas a serviços para Amazon VPC Lattice](#).

Permissões da API Amazon VPC Lattice

Você deve conceder permissão para que identidade do IAM (como usuários ou perfis) chamem as ações de API do VPC Lattice necessárias, conforme indicado em [Ações de políticas para o VPC Lattice](#). Além disso, para algumas ações do VPC Lattice, você deve conceder permissão às identidades do IAM para chamar ações específicas de outras. AWS APIs

Permissões necessárias para a API

Ao chamar as seguintes ações da API, você deverá conceder permissões para que os usuários do IAM chamem as ações especificadas.

CreateResourceConfiguration

- `vpc-lattice:CreateResourceConfiguration`
- `ec2:DescribeSubnets`

- `rds:DescribeDBInstances`
- `rds:DescribeDBClusters`

CreateResourceGateway

- `vpc-lattice>CreateResourceGateway`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssignIpv6Addresses`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`

DeleteResourceGateway

- `vpc-lattice>DeleteResourceGateway`
- `ec2>DeleteNetworkInterface`

UpdateResourceGateway

- `vpc-lattice:UpdateResourceGateway`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssignIpv6Addresses`
- `ec2:UnassignPrivateIpAddresses`
- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`

CreateServiceNetworkResourceAssociation

- `vpc-lattice>CreateServiceNetworkResourceAssociation`
- `ec2:AssignIpv6Addresses`

- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeNetworkInterfaces`

`CreateServiceNetworkVpcAssociation`

- `vpc-lattice:CreateServiceNetworkVpcAssociation`
- `ec2:DescribeVpcs`
- `ec2:DescribeSecurityGroups` (necessária somente ao fornecer grupos de segurança)

`UpdateServiceNetworkVpcAssociation`

- `vpc-lattice:UpdateServiceNetworkVpcAssociation`
- `ec2:DescribeSecurityGroups` (necessária somente ao fornecer grupos de segurança)

`CreateTargetGroup`

- `vpc-lattice:CreateTargetGroup`
- `ec2:DescribeVpcs`

`RegisterTargets`

- `vpc-lattice:RegisterTargets`
- `ec2:DescribeInstances` (necessária somente quando INSTANCE for o tipo de grupo de destino)
- `ec2:DescribeVpcs` (necessária somente quando INSTANCE ou IP for o tipo de grupo de destino)
- `ec2:DescribeSubnets` (necessária somente quando INSTANCE ou IP for o tipo de grupo de destino)
- `lambda:GetFunction` (necessária somente quando LAMBDA for o tipo de grupo de destino)
- `lambda:AddPermission` (necessária somente se o grupo de destino ainda não tiver permissão para invocar a função do Lambda especificada)

`DeregisterTargets`

- `vpc-lattice:DeregisterTargets`

`CreateAccessLogSubscription`

- `vpc-lattice:CreateAccessLogSubscription`
- `logs:GetLogDelivery`
- `logs:CreateLogDelivery`

DeleteAccessLogSubscription

- `vpc-lattice:DeleteAccessLogSubscription`
- `logs:DeleteLogDelivery`

UpdateAccessLogSubscription

- `vpc-lattice:UpdateAccessLogSubscription`
- `logs:UpdateLogDelivery`

Políticas baseadas em identidade para o Amazon VPC Lattice

Por padrão, os usuários e os perfis não têm permissão para criar ou modificar os recursos do VPC Lattice. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte [Criar políticas do IAM \(console\)](#) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo VPC Lattice, incluindo o formato do ARNs para cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição do Amazon VPC Lattice](#) na Referência de autorização de serviço.

Conteúdo

- [Práticas recomendadas de política](#)
- [Permissões adicionais necessárias para acesso total](#)
- [Exemplos de políticas baseadas em identidade para o VPC Lattice](#)

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do VPC Lattice em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas

AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte [Elementos da política JSON do IAM: condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

Permissões adicionais necessárias para acesso total

Para usar outros AWS serviços aos quais o VPC Lattice está integrado e todo o conjunto de recursos do VPC Lattice, você deve ter permissões adicionais específicas. Essas permissões não estão

incluídas na política gerenciada pela `VPCLatticeFullAccess` devido ao risco de escalonamento de privilégios conhecido por [“confused deputy”](#).

Você deverá anexar a política a seguir ao seu perfil e usá-la junto com a política gerenciada pela `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*"
  }
]
```

Essa política fornece as seguintes permissões adicionais:

- `iam:AttachRolePolicy`: permite que você anexe a política gerenciada especificada ao perfil do IAM especificado.
- `iam:PutRolePolicy`: permite que você adicione ou atualize um documento de política em linha que esteja incorporado ao perfil do IAM especificado.
- `s3:PutBucketPolicy`: permite que você aplique uma política de bucket a um bucket do Amazon S3.
- `firehose:TagDeliveryStream`: permite que você adicione ou atualize tags para fluxos de entrega do Firehose.

Exemplos de políticas baseadas em identidade para o VPC Lattice

Tópicos

- [Exemplo de política: gerenciar associações de VPC a uma rede de serviços](#)
- [Exemplo de política: criar associações de serviços a uma rede de serviços](#)
- [Exemplo de política: adicionar tags aos recursos](#)
- [Exemplo de política: criar uma função vinculada ao serviço](#)

Exemplo de política: gerenciar associações de VPC a uma rede de serviços

O exemplo a seguir demonstra uma política que concede aos usuários dessa política a permissão para criar, atualizar e excluir as associações de VPC a uma rede de serviços, mas somente para a VPC e a rede de serviços especificadas na condição. Para obter mais informações sobre como especificar chaves de condição, consulte [Chaves de condição de política do 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"
        }
      }
    }
  ]
}

```

Exemplo de política: criar associações de serviços a uma rede de serviços

Se você não estiver usando chaves de condição para controlar o acesso aos recursos do VPC Lattice, você pode especificar o número ARNs de recursos no Resource elemento para controlar o acesso em vez disso.

O exemplo a seguir demonstra uma política que limita as associações de serviços a uma rede de serviços que os usuários com essa política podem criar especificando o serviço e a rede ARNs de serviços que podem ser usados com a ação da `CreateServiceNetworkServiceAssociation` API. Para obter mais informações sobre como especificar os valores de ARN, consulte [Recursos de políticas para o 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"
    ]
}
]
}

```

Exemplo de política: adicionar tags aos recursos

O exemplo a seguir demonstra uma política que dá permissão para que usuários com essa política de permissão criem tags nos recursos do VPC Lattice.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc-lattice:TagResource"
      ],
      "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/*"
    }
  ]
}

```

Exemplo de política: criar uma função vinculada ao serviço

O VPC Lattice exige permissões para criar uma função vinculada ao serviço na primeira vez em que qualquer usuário cria Conta da AWS recursos do VPC Lattice. Se o perfil vinculada a serviço ainda não existir, o VPC Lattice o criará em sua conta. A função vinculada ao serviço concede permissões à VPC Lattice para que ela possa ligar para outras pessoas em seu nome. Serviços da AWS Para obter mais informações, consulte [the section called “Uso de perfis vinculados ao serviço”](#).

Para que a criação automática da função seja bem-sucedida, os usuários devem ter permissões para a ação `iam:CreateServiceLinkedRole`.

```

"Action": "iam:CreateServiceLinkedRole"

```

O exemplo a seguir demonstra uma política que dá permissão para que usuários com essa política de permissão criem um perfil vinculado a serviço para o 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"
        }
      }
    }
  ]
}
```

Para obter mais informações, consulte [Service-linked role permissions](#) (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Usando funções vinculadas a serviços para Amazon VPC Lattice

O Amazon VPC Lattice usa uma função vinculada ao serviço para as permissões necessárias para ligar para outras pessoas em seu nome. Serviços da AWS Para obter mais informações, consulte [Perfis vinculados ao serviço](#) no Guia do usuário do IAM.

O VPC Lattice usa a função vinculada ao serviço chamada. `AWSServiceRoleForVpcLattice`

Permissões de perfil vinculado a serviço para o VPC Lattice

A função vinculada ao serviço `AWSServiceRoleForVpcLattice` confia no seguinte serviço para assumir a função:

- `vpc-lattice.amazonaws.com`

A política de permissões de função nomeada `AWSVpcLatticeServiceRolePolicy` permite que o VPC Lattice publique CloudWatch métricas no namespace. `AWS/VpcLattice` Para obter mais informações, consulte [AWSVpcLatticeServiceRolePolicy](#) na Referência de política AWS gerenciada.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte [the section called “Exemplo de política: criar uma função vinculada ao serviço”](#).

Crie uma função vinculada a serviços para o VPC Lattice

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você cria recursos do VPC Lattice na, no ou na AWS Management Console API AWS CLI, o VPC Lattice cria a AWS função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria recursos do VPC Lattice, o VPC Lattice cria o perfil vinculado a serviço para você novamente.

Editar uma função vinculada a serviços para VPC Lattice

Você pode editar a descrição do `AWSServiceRoleForVpcLattice` do IAM. Para obter mais informações, consulte [Editar uma descrição de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para VPC Lattice

Se você não precisar mais usar o Amazon VPC Lattice, recomendamos que você exclua `AWSServiceRoleForVpcLattice`.

Você só pode excluir esse perfil vinculado a serviço após excluir todos os recursos do VPC Lattice em sua Conta da AWS.

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForVpcLattice` vinculada ao serviço. Para obter mais informações, consulte [Excluir uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Depois que você excluir um perfil vinculado a serviço, o VPC Lattice criará o perfil novamente quando você criar recursos do VPC Lattice na sua Conta da AWS.

Regiões compatíveis com perfis vinculados a serviço do VPC Lattice

O VPC Lattice oferece suporte a perfis vinculados a serviço em todas as regiões nas quais o serviço esteja disponível.

AWS políticas gerenciadas para Amazon VPC Lattice

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as [políticas gerenciadas pelo cliente](#) que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte [Políticas gerenciadas pela AWS](#) no Manual do usuário do IAM.

AWS política gerenciada: VPCLattice FullAccess

Essa política concede acesso total ao Amazon VPC Lattice e acesso limitado a outros serviços dependentes. Ela inclui permissões para fazer o seguinte:

- ACM — Recupere o SSL/TLS ARN do certificado para nomes de domínio personalizados.
- CloudWatch — Visualize registros de acesso e dados de monitoramento.
- CloudWatch Registros — configure e envie registros de acesso para o CloudWatch Logs.
- Amazon EC2 — Configure interfaces de rede e recupere informações sobre EC2 instâncias e VPCs Isso é usado para criar configurações de recursos, gateways de recursos e grupos de destino, configurar associações de entidades do VPC Lattice e registrar destinos.
- Elastic Load Balancing: recupere informações sobre um Application Load Balancer para registrá-lo como destino.
- Firehose — Recupere informações sobre fluxos de entrega usados para armazenar registros de acesso.
- Lambda: recupere informações sobre uma função do Lambda para registrá-la como destino.
- Amazon RDS — Recupere informações sobre clusters e instâncias do RDS.

- Amazon S3: recupere informações sobre buckets do S3 usados para armazenar logs de acesso.

Para visualizar as permissões para esta política, consulte [VPC_Lattice_Full_Access](#) na Referência de políticas gerenciadas pela AWS .

Para usar outros AWS serviços aos quais o VPC Lattice está integrado e todo o conjunto de recursos do VPC Lattice, você deve ter permissões adicionais específicas. Essas permissões não estão incluídas na política gerenciada pela `VPC_Lattice_Full_Access` devido ao risco de escalonamento de privilégios conhecido por [“confused deputy”](#). Para obter mais informações, consulte [Permissões adicionais necessárias para acesso total](#).

AWS política gerenciada: `VPC_Lattice_ReadOnly_Access`

Essa política concede acesso somente leitura ao Amazon VPC Lattice e acesso limitado a outros serviços dependentes. Ela inclui permissões para fazer o seguinte:

- ACM — Recupere o SSL/TLS ARN do certificado para nomes de domínio personalizados.
- CloudWatch — Visualize registros de acesso e dados de monitoramento.
- CloudWatch Registros — Visualize as informações de entrega de registros para assinaturas de registros de acesso.
- Amazon EC2 — Recupere VPCs informações sobre EC2 instâncias, crie grupos-alvo e registre alvos.
- Elastic Load Balancing: recupere informações sobre um Application Load Balancer.
- Firehose — Recupere informações sobre fluxos de entrega para entrega de registros de acesso.
- Lambda: veja informações sobre uma função do Lambda.
- Amazon RDS — Recupere informações sobre clusters e instâncias do RDS.
- Amazon S3: recupere informações sobre buckets do S3 para entrega de logs de acesso.

Para visualizar as permissões para esta política, consulte [VPC_Lattice_ReadOnly_Access](#) na Referência de políticas gerenciadas pela AWS .

AWS política gerenciada: `VPC_Lattice_Services_Invoke_Access`

Essa política fornece acesso à invocação de serviços do Amazon VPC Lattice.

Para visualizar as permissões para esta política, consulte [VPC_Lattice_Services_Invoke_Access](#) na Referência de políticas gerenciadas pela AWS .

AWS política gerenciada: AWSVpcLatticeServiceRolePolicy

Essa política é anexada a uma função vinculada ao serviço chamada `AWSServiceRoleForVpcLattice` para permitir que a VPC Lattice execute ações em seu nome. Não é possível anexar essa política a suas entidades do IAM. Para obter mais informações, consulte [Usando funções vinculadas a serviços para Amazon VPC Lattice](#).

Para visualizar as permissões para esta política, consulte [AWSVpcLatticeServiceRolePolicy](#) na Referência de políticas gerenciadas pela AWS .

Atualizações do VPC Lattice nas políticas gerenciadas AWS

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do VPC Lattice desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS do Guia do usuário do VPC Lattice.

Alteração	Descrição	Data
VPC Lattice Full Access	O VPC Lattice adiciona permissões somente de leitura para descrever clusters e instâncias do Amazon RDS.	1.º de dezembro de 2024
VPC Lattice Read Only Access	O VPC Lattice adiciona permissões somente de leitura para descrever clusters e instâncias do Amazon RDS.	1.º de dezembro de 2024
AWSVpcLatticeServiceRolePolicy	O VPC Lattice adiciona permissões para permitir que o VPC Lattice crie uma interface de rede gerenciada pelo solicitante.	1.º de dezembro de 2024
VPC Lattice Full Access	O VPC Lattice adiciona uma nova política para conceder permissões de acesso total ao Amazon VPC Lattice e acesso limitado a outros serviços dependentes.	31 de março de 2023

Alteração	Descrição	Data
VPC LatticeReadOnlyAccess	O VPC Lattice adiciona uma nova política para conceder permissões de acesso somente leitura ao Amazon VPC Lattice e acesso limitado a outros serviços dependentes.	31 de março de 2023
VPC LatticeServicesInvokeAccess	O VPC Lattice adiciona uma nova política para conceder acesso para invocar serviços do Amazon VPC Lattice.	31 de março de 2023
AWSVpcLatticeServiceRolePolicy	O VPC Lattice adiciona permissões à sua função vinculada ao serviço para permitir que o VPC Lattice publique métricas no namespace. CloudWatch AWS/VpcLattice. A AWSVpcLatticeServiceRolePolicy política inclui permissão para chamar a ação CloudWatch PutMetricData API. Para obter mais informações, consulte Usando funções vinculadas a serviços para Amazon VPC Lattice .	5 de dezembro de 2022
O VPC Lattice começou a monitorar alterações	A VPC Lattice começou a monitorar as mudanças em suas AWS políticas gerenciadas.	5 de dezembro de 2022

Validação de conformidade para o Amazon VPC Lattice

Audidores terceirizados avaliam a segurança e a conformidade do Amazon VPC Lattice como parte de vários programas de AWS conformidade.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#)

[Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Governança e conformidade de segurança](#): esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- [Referência de serviços qualificados para HIPAA](#): lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#)— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Acesse o Amazon VPC Lattice usando endpoints de interface ([AWS PrivateLink](#))

É possível estabelecer uma conexão privada entre a VPC e o Amazon VPC Lattice criando uma endpoint da VPC de interface. Os endpoints de interface são alimentados por [AWS PrivateLink](#) uma tecnologia que permite acessar de forma privada o VPC Lattice APIs sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias na sua VPC não precisam de endereços IP públicos para se comunicar com a VPC Lattice. APIs

Cada endpoint de interface é representado por uma ou mais [interfaces de rede](#) em suas sub-redes.

Considerações sobre endpoints da VPC de interface

[Antes de configurar uma interface VPC endpoint para o VPC Lattice, certifique-se de revisar o Access no Guia. Serviços da AWS AWS PrivateLink AWS PrivateLink](#)

O VPC Lattice oferece suporte à realização de chamadas para todas as ações de API da sua VPC.

Como criar um endpoint da VPC de interface para o VPC Lattice

Você pode criar um VPC endpoint para o serviço VPC Lattice usando o console Amazon VPC ou o ([AWS Command Line Interface AWS CLI](#)). Para obter mais informações, consulte [Criar uma interface VPC endpoint no Guia](#). AWS PrivateLink

Crie um endpoint da VPC para o VPC Lattice usando o seguinte nome de serviço:

`com.amazonaws.region.vpc-lattice`

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o VPC Lattice usando seu nome de DNS padrão para a região, por exemplo, `vpc-lattice.us-east-1.amazonaws.com`.

Resiliência no Amazon VPC Lattice

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade.

Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância.

Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

Segurança da infraestrutura no Amazon VPC Lattice

Como um serviço gerenciado, o Amazon VPC Lattice é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o VPC Lattice pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Monitoramento do Amazon VPC Lattice

Use os recursos desta seção para monitorar suas redes de serviços, serviços, grupos de destino e conexões de VPC do Amazon VPC Lattice.

Conteúdo

- [CloudWatch métricas do Amazon VPC Lattice](#)
- [Registros de acesso para Amazon VPC Lattice](#)
- [CloudTrail registros para Amazon VPC Lattice](#)

CloudWatch métricas do Amazon VPC Lattice

O Amazon VPC Lattice envia dados relacionados aos grupos de destino e serviços para a Amazon CloudWatch e os processa em métricas legíveis praticamente em tempo real. Essas métricas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor sobre o desempenho da aplicação Web ou do serviço. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

O Amazon VPC Lattice usa uma perfil vinculado a serviço em sua AWS conta da para enviar métricas para a Amazon. CloudWatch Para obter mais informações, consulte [Usando funções vinculadas a serviços para Amazon VPC Lattice](#).

Conteúdo

- [Visualizar as CloudWatch métricas da Amazon](#)
- [Métricas do grupo de destino](#)
- [Métricas de serviço](#)

Visualizar as CloudWatch métricas da Amazon

Você pode visualizar as CloudWatch métricas da Amazon para seus grupos de destino e serviços usando o CloudWatch console ou a AWS CLI.

Para visualizar as métricas usando o CloudWatch console

1. Abra o CloudWatch console da Amazon em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Métricas.
3. Selecione o namespace AWS/VpcLattice.
4. (Opcional) Para visualizar uma métrica em todas as dimensões, digite o nome no campo de pesquisa.
5. (Opcional) Para filtrar por dimensão, selecione uma das seguintes ações:
 - Para exibir somente as métricas relatadas para seus grupos de destino, escolha Grupos de destino. Para visualizar uma métrica para um só grupo de destino, digite o nome no campo de pesquisa.
 - Para exibir somente as métricas relatadas para seus serviços, escolha Serviços. Para visualizar uma métrica para um só serviço, digite seu nome no campo de pesquisa.

Para visualizar métricas usando o AWS CLI

Use o AWS CLI comando [CloudWatch list-metrics](#) para listar as métricas disponíveis:

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

Para obter informações sobre cada métricas e suas dimensões, consulte [Métricas do grupo de destino](#) e [Métricas de serviço](#).

Métricas do grupo de destino

[O VPC Lattice armazena automaticamente métricas relacionadas aos grupos de destino no namespace do AmazonAWS/VpcLattice. CloudWatch](#) Para obter mais informações sobre grupos de destino, consulte [Grupos de destino no VPC Lattice](#).

Dimensões

Para filtrar as métricas dos grupos de destino, use as dimensões a seguir:

- AvailabilityZone
- TargetGroup

Métrica	Descrição
TotalConnectionCount	Total de conexões. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.
ActiveConnectionCount	Conexões ativas. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.
ConnectionErrorCount	Total de falhas de conexão. Critérios de relatórios Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego.

Métrica	Descrição
	Frequência de relatórios • Uma vez por minuto. Estatísticas • A estatística mais útil é Sum.
HTTP1_ConnectionCount	Total de conexões HTTP/1.1. Critérios de relatórios • Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios • Uma vez por minuto. Estatísticas • A estatística mais útil é Sum.
HTTP2_ConnectionCount	Total de conexões HTTP/2. Critérios de relatórios • Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios • Uma vez por minuto. Estatísticas • A estatística mais útil é Sum.

Métrica	Descrição
ConnectionTimeoutCount	Total de tempos limite de conexão esgotados. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.
TotalReceivedConnectionBytes	Total de bytes de conexão recebidos. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.

Métrica	Descrição
TotalSentConnectionBytes	Total de bytes de conexão enviados. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.
TotalRequestCount	Total de solicitações. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.

Métrica	Descrição
ActiveRequestCount	Total de solicitações ativas. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.
RequestTime	Tempo de solicitação até o último byte em milissegundos. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - As estatísticas mais úteis são Average e pNN.NN (percentis).

Métrica	Descrição
HTTPCode_2XX_Count, HTTPCode_3XX_Count, HTTPCode_4XX_Count, HTTPCode_5XX_Count	Códigos de resposta HTTP agregados. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.
TLSConnectionError Count	Total de erros de conexão TLS, sem incluir falhas nas verificações de certificado. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.

Métrica	Descrição
TotalTLSConnectionHandshakeCount	Total de handshakes de conexão TLS bem-sucedidos. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.

Métricas de serviço

[O VPC Lattice armazena automaticamente métricas relacionadas a serviços namespace do AmazonAWS/VpcLattice. CloudWatch](#) Para obter mais informações sobre os serviços, consulte [Serviços no VPC Lattice](#).

Dimensões

Para filtrar as métricas dos grupos de destino, use as dimensões a seguir:

- AvailabilityZone
- Service

Métrica	Descrição
RequestTimeoutCount	Total de solicitações que atingiram o tempo limite à espera de uma resposta.

Métrica	Descrição
	Critérios de relatórios • Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios • Uma vez por minuto. Estatísticas • A estatística mais útil é Sum.
TotalRequestCount	Total de solicitações. Critérios de relatórios • Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios • Uma vez por minuto. Estatísticas • A estatística mais útil é Sum.

Métrica	Descrição
RequestTime	Tempo de solicitação em milissegundos. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - As estatísticas mais úteis são Average e pNN.NN (percentis).
HTTPCode_2XX_Count , HTTPCode_3XX_Count , HTTPCode_4XX_Count , HTTPCode_5XX_Count	Códigos de resposta HTTP agregados. Critérios de relatórios - Sempre relatado (seja um valor zero ou diferente de zero) a partir do momento em que o recurso recebe tráfego. Frequência de relatórios - Uma vez por minuto. Estatísticas - A estatística mais útil é Sum.

Registros de acesso para Amazon VPC Lattice

Os registros de acesso capturam informações detalhadas sobre seus serviços e configurações de recursos do VPC Lattice. Você pode usar esses logs de acesso para analisar padrões de tráfego e auditar todos os serviços na rede. Para serviços VPC Lattice, publicamos VpcLatticeAccessLogs

e para configurações de recursos, publicamos o `VpcLatticeResourceAccessLogs` que precisa ser configurado separadamente.

Logs de acesso são opcionais e estão desabilitados por padrão. Após ativar os logs de acesso, você poderá desabilitá-los a qualquer momento.

Preços

Haverá cobranças quando os logs de acesso forem publicados. Os registros que são publicados AWS nativamente em seu nome são chamados de registros vendidos. Para obter mais informações sobre preços de registros vendidos, consulte [Amazon CloudWatch Pricing](#), escolha Logs e veja os preços em Vended Logs.

Conteúdo

- [Permissões do IAM necessárias para habilitar os logs de acesso](#)
- [Destinos de logs de acesso](#)
- [Habilitar logs de acesso](#)
- [Conteúdo dos logs de acesso](#)
- [Conteúdo do log de acesso a recursos](#)
- [Solucionar problemas de logs de acesso](#)

Permissões do IAM necessárias para habilitar os logs de acesso

Para habilitar os logs de acesso e enviá-los para seus destinos, você deverá ter as seguintes ações na política anexadas ao usuário, grupo ou perfil do IAM que você estiver usando.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Sid": "ManageVPC_LatticeAccessLogSetup",
      "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": [
        "*"
    ]
}
]
}

```

Para obter mais informações, consulte [Adicionar e remover permissões de identidade do IAM](#) no Guia do usuário do AWS Identity and Access Management .

Após atualizar a política anexada ao usuário, grupo ou perfil do IAM que você estiver usando, acesse [Habilitar logs de acesso](#).

Destinos de logs de acesso

Você pode enviar logs de acesso para os seguintes destinos.

CloudWatch Registros da Amazon

- O VPC Lattice normalmente entrega registros para o Logs em CloudWatch 2 minutos. No entanto, lembre-se de que o tempo efetivo de entrega dos logs é baseado no melhor esforço possível e pode haver latência adicional.
- Uma política de recursos é criada automaticamente e adicionada ao grupo de CloudWatch registros se o grupo de registros não tiver determinadas permissões. Para obter mais informações, consulte [Registros enviados para CloudWatch Logs](#) no Guia CloudWatch do usuário da Amazon.
- Você pode encontrar registros de acesso que são enviados CloudWatch em Grupos de registros no CloudWatch console. Para obter mais informações, consulte [Exibir dados de log enviados para CloudWatch Logs](#) no Guia CloudWatch do usuário da Amazon.

Amazon S3

- Normalmente, o VPC Lattice entrega logs para o Amazon S3 em até 6 minutos. No entanto, lembre-se de que o tempo efetivo de entrega dos logs é baseado no melhor esforço possível e pode haver latência adicional.

- Uma política de bucket será criada automaticamente e adicionada ao seu bucket do Amazon S3 se o bucket não tiver determinadas permissões. Para obter mais informações, consulte [Registros enviados para o Amazon S3 no Guia CloudWatch](#) do usuário da Amazon.
- Logs de acesso que são enviados ao Amazon S3 usam a seguinte convenção de nomenclatura:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/AccessLogs/[region]/[YYYY/MM/DD]/[resource-id]/[accountId]_VpcLatticeAccessLogs_[region]_[resource-id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

- VpcLatticeResourceAccessLogs que são enviados para o Amazon S3 usam a seguinte convenção de nomenclatura:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/ResourceAccessLogs/[region]/[YYYY/MM/DD]/[resource-id]/[accountId]_VpcLatticeResourceAccessLogs_[region]_[resource-id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

Amazon Data Firehose

- O VPC Lattice normalmente entrega registros para o Firehose em 2 minutos. No entanto, lembre-se de que o tempo efetivo de entrega dos logs é baseado no melhor esforço possível e pode haver latência adicional.
- Um perfil vinculado a serviço é criado automaticamente e concede permissão para que o VPC Lattice envie logs de acesso para o Amazon Data Firehose. Para que a criação automática da função seja bem-sucedida, os usuários devem ter permissão para a ação `iam:CreateServiceLinkedRole`. Para obter mais informações, consulte [Registros enviados Amazon Data Firehose](#) no Guia do CloudWatch usuário da Amazon.
- Para obter mais informações sobre como visualizar os logs enviados ao Amazon Data Firehose, consulte [Como monitorar o Amazon Kinesis Data Streams](#) no Guia do desenvolvedor do Amazon Data Firehose .

Habilitar logs de acesso

Execute o procedimento a seguir para configurar logs de acesso a fim de capturar e entregar logs de acesso ao destino que você escolher.

Conteúdo

- [Habilitar os logs de acesso usando o console](#)

- [Habilitar os logs de acesso usando a AWS CLI](#)

Habilitar os logs de acesso usando o console

Você pode ativar os registros de acesso para uma rede de serviços, um serviço ou uma configuração de recursos durante a criação. Você também pode ativar os registros de acesso depois de criar uma rede de serviços, um serviço ou uma configuração de recursos, conforme descrito no procedimento a seguir.

Para criar um serviço básico usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. Selecione a rede de serviços, o serviço ou a configuração do recurso.
3. Escolha Ações, Editar configurações de log.
4. Ative o seletor de Logs de acesso.
5. Adicione um destino de entrega para seus logs de acesso da seguinte forma:
 - Selecione Grupo de CloudWatch registros e escolha um grupo de registros. Para criar um grupo de registros, escolha Criar um grupo de registros em CloudWatch.
 - Selecione o bucket do S3 e insira o caminho do bucket do S3, incluindo qualquer prefixo. Para pesquisar seus buckets do S3, escolha Procurar S3.
 - Em Fluxo de entrega do Kinesis Data Firehose, selecione um fluxo de entrega. Para criar um fluxo de entrega, escolha Criar um fluxo de entrega no Kinesis.
6. Escolha Salvar alterações.

Habilitar os logs de acesso usando a AWS CLI

Use o comando CLI [create-access-log-subscription](#) para habilitar registros de acesso para redes ou serviços de serviços.

Conteúdo dos logs de acesso

A tabela a seguir descreve os campos de uma entrada no log de acesso.

Campo	Descrição	Formato
hostHeader	O cabeçalho da autoridade da solicitação.	string
sslCipher	O nome OpenSSL do conjunto de cifras usado para estabelecer a conexão TLS do cliente.	string
serviceNetworkArn	O ARN da rede de serviços.	arn:aws:vpc-lattice: ::service network/ <i>region account id</i>
resolvedUser	O ARN do usuário quando a autenticação estiver habilitada e a autenticação acontecer.	null ARN "Anonymous" "Unknown"
authDeniedReason	O motivo pelo qual o acesso é negado quando a autenticação estiver habilitada.	null "Service" "Network" "Identity"
requestMethod	O cabeçalho do método da solicitação.	string
targetGroupArn	O grupo de hosts de destino ao qual o host de destino pertence.	string
tlsVersion	A versão do TLS.	TLSv <i>x</i>
userAgent	O cabeçalho user-agent.	string
ServerNameIndication	[Somente HTTPS] O valor definido no soquete de conexão SSL para a Indicação de nome de servidor (SNI).	string
destinationVpcId	O ID da VPC de destino.	pvc- <i>xxxxxxxxx</i>

Campo	Descrição	Formato
sourceIpPort	O endereço IP e a porta da origem.	<i>ip:port</i>
targetIpPort	O endereço IP e a porta do destino.	<i>ip:port</i>
serviceArn	O ARN do serviço.	arn:aws:vpc-lattice: ::service/ <i>region account id</i>
sourceVpcId	O ID da VPC de origem.	pvc- <i>xxxxxxxxx</i>
requestPath	O caminho da solicitação.	LatticePath?: <i>path</i>
startTime	O horário inicial da solicitação.	<i>YYYY-MM-DD T HHMM:SS Z</i>
protocol	O protocolo. Atualmente, HTTP/1.1 ou HTTP/2.	string
responseCode	O código HTTP da resposta. Somente o código de resposta para os cabeçalhos finais é registrado em log. Para obter mais informações, consulte Solucionar problemas de logs de acesso .	integer
bytesReceived	Os bytes do corpo e do cabeçalho recebidos.	integer
bytesSent	Os bytes do corpo e do cabeçalho enviados.	integer
duration	Duração total em milissegundos da solicitação desde a hora de início até o último byte de saída.	integer

Campo	Descrição	Formato
<code>requestToTargetDuration</code>	Duração total em milissegundos da solicitação desde a hora de início até o último byte enviado ao destino.	integer
<code>responseFromTargetDuration</code>	Duração total em milissegundos da solicitação desde o primeiro byte lido do host de destino até o último byte enviado ao cliente.	integer
<code>grpcResponseCode</code>	O código da resposta gRPC. Para obter mais informações, consulte Códigos de status e seu uso no gRPC . Esse campo só será registrado em log se o serviço for compatível com gRPC.	integer
<code>callerPrincipal</code>	A entidade principal autenticada.	string
<code>callerX509SubjectCN</code>	O nome do assunto (CN).	string
<code>callerX509IssuerOU</code>	O emissor (OU).	string
<code>callerX509SANNameCN</code>	O nome alternativo do emissor (nome/CN).	string
<code>callerX509SANDNS</code>	O nome alternativo do assunto (DNS).	string
<code>callerX509SANURI</code>	O nome alternativo do assunto (URI).	string
<code>sourceVpcArn</code>	O ARN da VPC na qual a solicitação teve origem.	arn:aws:ec2: ::vpc/ <i>region</i> <i>account id</i>

Exemplo

Este é um exemplo de entrada de 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
}
```

Conteúdo do log de acesso a recursos

A tabela a seguir descreve os campos de uma entrada de registro de acesso a recursos.

Campo	Descrição	Formato
serviceNetworkArn	O ARN da rede de serviços.	Arquivo: <i>partition</i> vpc-lattice: ::servicenetwork/ <i>region</i> <i>account id</i>
serviceNetworkResourceAssociationId	O ID do recurso da rede de serviços.	<i>snra-xxx</i>
vpcEndpointId	O ID do endpoint usado para acessar o recurso.	string
sourceVpcArn	O ARN da VPC de origem ou a VPC de onde a conexão foi iniciada.	string
resourceConfigurationArn	O ARN da configuração do recurso que foi acessado.	string
protocol	O protocolo usado para se comunicar com a configuração do recurso. Atualmente, somente o tcp é suportado.	string
sourceIpPort	O endereço IP e a porta da fonte que iniciou a conexão.	<i>ip:port</i>
destinationIpPort	O endereço IP e a porta na qual a conexão foi iniciada. Esse será o IP do SN-E/SN-A.	<i>ip:port</i>
gatewayIpPort	O endereço IP e a porta usados pelo gateway de recursos para acessar o recurso.	<i>ip:port</i>
resourceIpPort	O endereço IP e a porta do recurso.	<i>ip:port</i>

Exemplo

Este é um exemplo de entrada de log.

```
{
  "eventTimestamp": "2024-12-02T10:10:10.123Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:1234567890:servicenetwork/sn-1a2b3c4d",
  "serviceNetworkResourceAssociationId": "snra-1a2b3c4d",
  "vpcEndpointId": "vpce-01a2b3c4d",
  "sourceVpcArn": "arn:aws:ec2:us-west-2:1234567890:vpc/vpc-01a2b3c4d",
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-west-2:0987654321:resourceconfiguration/rcfg-01a2b3c4d",
  "protocol": "tcp",
  "sourceIpPort": "172.31.23.56:44076",
  "destinationIpPort": "172.31.31.226:80",
  "gatewayIpPort": "10.0.28.57:49288",
  "resourceIpPort": "10.0.18.190:80"
}
```

Solucionar problemas de logs de acesso

Esta seção contém uma explicação dos códigos de erro HTTP que você pode ver nos logs de acesso.

Código de erro	Possíveis causas
HTTP 400: solicitação inválida	- O cliente enviou uma solicitação malformada que não atende às especificações de HTTP. - O cabeçalho da solicitação excedeu 60K para todo o cabeçalho da solicitação ou mais de 100 cabeçalhos. - O cliente fechou a conexão antes de enviar o corpo completo da solicitação.
HTTP 403: negado	A autenticação foi configurada para o serviço, mas a solicitação recebida não está autenticada nem autorizada.
HTTP 404: serviço inexistente	Você está tentando se conectar a um serviço que não existe ou não está registrado na rede de serviços correta.

Código de erro	Possíveis causas
HTTP 500: Erro interno do servidor	O VPC Lattice encontrou um erro, como falha na conexão com os destinos.
HTTP 502: Bad Gateway	O VPC Lattice encontrou um erro.

CloudTrail registros para Amazon VPC Lattice

O Amazon VPC Lattice está integrado com [AWS CloudTrail](#), um serviço que fornece um registro das ações realizadas por um usuário, função ou um. AWS service (Serviço da AWS) CloudTrail captura todas as chamadas de API para o VPC Lattice como eventos. As chamadas capturadas incluem chamadas do console VPC Lattice e chamadas de código para as operações da API VPC Lattice. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à VPC Lattice, o endereço IP a partir do qual a solicitação foi feita, quando foi feita e detalhes adicionais.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais de usuário raiz ou credenciais de usuário.
- Se a solicitação foi feita em nome de um usuário do Centro de Identidade do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

CloudTrail está ativo Conta da AWS quando você cria a conta e você tem acesso automático ao histórico de CloudTrail eventos. O histórico de CloudTrail eventos fornece um registro visível, pesquisável, baixável e imutável dos últimos 90 dias de eventos de gerenciamento registrados em um. Região da AWS Para obter mais informações, consulte [Trabalhando com o histórico de CloudTrail eventos](#) no Guia AWS CloudTrail do usuário. Não há CloudTrail cobrança pela visualização do histórico de eventos.

Para um registro contínuo dos eventos dos Conta da AWS últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do [CloudTrailLake](#).

CloudTrail trilhas

Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Todas as trilhas criadas usando o AWS Management Console são multirregionais. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. É recomendável criar uma trilha multirregional porque você captura todas as atividades Regiões da AWS em sua conta. Ao criar uma trilha de região única, é possível visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte [Criar uma trilha para a Conta da AWS](#) e [Criar uma trilha para uma organização](#) no Guia do usuário do AWS CloudTrail .

Você pode entregar uma cópia dos seus eventos de gerenciamento contínuos para o bucket do Amazon S3 sem nenhum custo CloudTrail criando uma trilha. No entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre CloudTrail preços, consulte [AWS CloudTrail Preços](#). Para receber informações sobre a definição de preços do Amazon S3, consulte [Definição de preços do Amazon S3](#).

CloudTrail Armazenamentos de dados de eventos em Lake

CloudTrail O Lake permite que você execute consultas baseadas em SQL em seus eventos. CloudTrail O Lake converte eventos existentes no formato JSON baseado em linhas para o formato [Apache](#) ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de [seletores de eventos avançados](#). Os seletores que aplicados a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para consulta. Para obter mais informações sobre o CloudTrail Lake, consulte [Trabalhando com o AWS CloudTrail Lake](#) no Guia AWS CloudTrail do Usuário.

CloudTrail Os armazenamentos e consultas de dados de eventos em Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a [opção de preço](#) que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre CloudTrail preços, consulte [AWS CloudTrail Preços](#).

Para monitorar ações adicionais, use logs de acesso. Para obter mais informações, consulte [Logs de acesso](#).

Eventos de gerenciamento do VPC Lattice em CloudTrail

[Os eventos de gerenciamento](#) fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. Também são conhecidas como operações de ambiente de gerenciamento. Por padrão, CloudTrail registra eventos de gerenciamento.

O Amazon VPC Lattice registra as operações do plano de controle do VPC Lattice como eventos de gerenciamento. [Para obter uma lista das operações do plano de controle do Amazon VPC Lattice nas quais o VPC Lattice se registra, consulte a Referência da API CloudTrail do Amazon VPC Lattice.](#)

Exemplos de eventos do VPC Lattice

Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação de API solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, os eventos não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra um CloudTrail evento para a [CreateService](#) operação.

```
{
  "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"
  }
}

```

O exemplo a seguir mostra um CloudTrail evento para a [DeleteService](#) operação.

```

{
  "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"
}
```

Para obter informações sobre o conteúdo do CloudTrail registro, consulte [o conteúdo do CloudTrail registro](#) no Guia AWS CloudTrail do usuário.

Cotas do Amazon VPC Lattice

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. AWS service (Serviço da AWS) A menos que especificado de outra forma, cada cota é específica da região. É possível solicitar aumentos para algumas cotas, enquanto outras cotas não podem ser aumentadas.

Para visualizar as cotas do VPC Lattice, abra o [Console do Service Quotas](#). No painel de navegação, escolha Serviços da AWS e selecione o VPC Lattice.

Para solicitar um aumento da cota, consulte [Requesting a quota increase](#) no Guia do usuário do Service Quotas.

Você Conta da AWS tem as seguintes cotas relacionadas ao VPC Lattice.

Name	Padrão	Ajuste	Descrição
Tamanho da política de autenticação	Cada região compatível: 10 kilobytes	Não	O tamanho máximo de um arquivo JSON em uma política de Auth.
Configurações de recursos secundários por configuração de recursos de grupo	Cada região compatível: 40	Sim	O número máximo de configurações de recursos secundários em uma configuração de recursos de grupo. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Ouvintes por serviço	Cada região compatível: 2	Sim	O número máximo de ouvintes que você pode criar para um serviço. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.

Name	Padrão	Ajuste	Descrição
Configurações de recursos por rede de serviço	Cada região compatível: 100	Sim	O número máximo de configurações de recursos associadas a uma rede de serviços. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Configurações de recursos por região AWS	Cada região com suporte: 500	Sim	O número máximo de configurações de recursos que uma AWS conta pode ter por AWS região. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Gateways de recursos por VPC	Cada região compatível: 100	Sim	O número máximo de gateways de recursos em uma VPC. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Regras por ouvinte	Cada região compatível: 5	Sim	O número máximo de regras que você pode definir para o seu ouvinte do serviço. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.

Name	Padrão	Ajuste	Descrição
Grupos de segurança por associação	Cada região compatível: 5	Não	O número máximo de grupos de segurança que você pode adicionar a uma associação entre uma VPC e uma rede de serviços.
Associações de serviços por rede de serviços	Cada região com suporte: 500	Sim	O número máximo de serviços que você pode associar a uma única rede de serviços. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Redes de serviços por região	Cada região com suporte: 10	Sim	O número máximo de redes de serviços por região. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Serviços por região da	Cada região com suporte: 500	Sim	O número máximo de serviços por região. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.

Name	Padrão	Ajuste	Descrição
Grupos de destino por região	Cada região com suporte: 500	Sim	O número máximo de grupos de destino por região. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Número de grupos de destino por serviço	Cada região compatível: 5	Sim	O número máximo de grupos-alvo que você pode associar a um serviço. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Destinos por grupo de destino	Cada região com suporte: 1.000	Sim	O número máximo de destinos que você pode associar a um único grupo de destinos. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.
Associações VPC por rede de serviço	Cada região com suporte: 500	Sim	O número máximo VPCs que você pode associar a uma única rede de serviços. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.

Name	Padrão	Ajuste	Descrição
Endpoints VPC do tipo rede de serviço por rede de serviço	Cada região compatível: 50	Sim	O número máximo de endpoints de rede de serviço associados a uma rede de serviços. Para aumentos adicionais de capacidade e limite, entre em contato com o AWS Support.

As seguintes zonas de disponibilidade não são compatíveis com o VPC Lattice: use1-az3,, usw1-az2, apne1-az3,, apne2-az2, euc1-az2, euw1-az4. cac1-az3 ilc1-az2

Os limites a seguir também são aplicáveis.

Limite	Valor	Descrição
Largura de banda por serviço por zona de disponibilidade	10 Gbps	A largura de banda máxima alocada por serviço por zona de disponibilidade.
Largura de banda por gateway de recursos por zona de disponibilidade	100 Gbps	A largura de banda máxima alocada por gateway de recursos por zona de disponibilidade.
A unidade de transmissão máxima (MTU) por conexão	8500 bytes	O tamanho do maior pacote de dados que um serviço pode aceitar.
Solicitações por segundo por serviço por zona de disponibilidade	10.000	Para serviços HTTP, esse é o número máximo de solicitações por segundo por serviço por zona de disponibilidade.
Tempo de inatividade da conexão por conexão	1 minuto	O tempo máximo em que uma conexão pode ficar ociosa sem solicitações ativas (para HTTP e

Limite	Valor	Descrição
		GRPC) ou sem transferência ativa de dados (para TLS-PASSTHROUGH).
Vida útil máxima de conexão por conexão	10 minutos	O tempo máximo em que uma conexão pode ser aberta.
Rede de serviços por VPC	1 rede de serviços	Você pode conectar uma VPC a apenas uma rede de serviços por meio de uma associação. Para conectar uma VPC a várias redes de serviços, você pode usar endpoints VPC do tipo service network.

Histórico de documentos do Guia do usuário do Amazon VPC Lattice

A tabela a seguir descreve as versões de documentação para o VPC Lattice.

Alteração	Descrição	Data
Estrutura de VPC adicionada para Oracle Database@AWS	Lançamento do VPC Lattice. Oracle Database@AWS	26 de junho de 2025
Foi adicionado suporte de pilha dupla para endpoints de gerenciamento	O VPC Lattice agora oferece suporte a IPv6 endpoints de pilha dupla (eIPv4) para todo o gerenciamento do VPC Lattice. APIs	30 de abril de 2025
Compartilhe e acesse recursos	O VPC Lattice agora oferece suporte ao compartilhamento e ao acesso a recursos entre os limites da VPC e da conta. Isso inclui atualizações nas VPC Lattice Full Access políticas VPC Lattice Read Only Access .	1.º de dezembro de 2024
Passagem TLS	O VPC Lattice agora oferece suporte à passagem de TLS, o que permite que você execute o encerramento de TLS em seu aplicativo para autenticação. end-to-end	14 de maio de 2024
Versão da estrutura de eventos do Lambda	Agora, o VPC Lattice oferece suporte a uma nova versão da estrutura de eventos do Lambda.	7 de setembro de 2023

Support for shared VPCs	Os participantes podem criar grupos de destinos do VPC Lattice em uma VPC compartilhada.	5 de julho de 2023
Versão de disponibilidade geral	O lançamento do Guia do usuário do VPC Lattice para disponibilidade geral (GA)	31 de março de 2023
A VPC Lattice agora relata mudanças em suas políticas gerenciadas AWS	As alterações nas políticas gerenciadas são relatadas em “políticas AWS gerenciadas para VPC Lattice” no capítulo “Segurança”.	29 de março de 2023
Suporte para tipo de destino do Application Load Balancer	Agora, o VPC Lattice oferece suporte à criação de um grupo de destino do tipo Application Load Balancer.	29 de março de 2023
Compatibilidade com todos os tipos de instâncias	Agora, o VPC Lattice oferece suporte a todos os tipos de instâncias.	27 de março de 2023
IPv6 apoio	O VPC Lattice agora oferece suporte a ambos IPv4 e a grupos-alvo IPv6 IP.	27 de março de 2023
HTTP2 versão do protocolo para verificações de saúde	As verificações de saúde agora são suportadas quando a versão do protocolo do grupo-alvo é HTTP2.	27 de março de 2023
Ação de resposta fixa para regras de receptor	Agora, os receptores dos serviços VPC Lattice oferecem suporte a ações de resposta fixa, além de ações de encaminhamento.	27 de março de 2023

Suporte para nomes de domínio personalizados	Agora, você pode configurar um nome de domínio personalizado para um serviço VPC Lattice	14 de fevereiro de 2023
Suporte para Traga seu próprio certificado (BYOC)	O VPC Lattice suporta o uso de seu próprio SSL/TLS certificado no ACM para nomes de domínio personalizados.	14 de fevereiro de 2023
Agora, o VPC Lattice relata uma lista atualizada de tipos de instância não compatíveis	Três instâncias adicionais foram adicionadas à lista de instâncias não compatíveis.	26 de janeiro de 2023
A VPC Lattice agora relata mudanças em suas políticas gerenciadas AWS	A partir de 5 de dezembro de 2022, alterações nas políticas gerenciadas são relatadas no tópico “políticas gerenciadas pela AWS para o VPC Lattice” no capítulo “Segurança”. A primeira alteração listada é a adição das permissões necessárias para o CloudWatch monitoramento.	5 de dezembro de 2022
Lançamento inicial	A versão inicial do Guia do usuário do VPC Lattice	5 de dezembro de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.