aws

Network Load Balancers

Elastic Load Balancing

Elastic Load Balancing: Network Load Balancers

Table of Contents

O que é um Network Load Balancer?

O Elastic Load Balancing distribui automaticamente seu tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Ele monitora a integridade dos destinos registrados e roteia o tráfego apenas para os destinos íntegros. O Elastic Load Balancing escala seu balanceador de carga conforme seu tráfego de entrada muda com o tempo. Ele pode ser dimensionado automaticamente para a vasta maioria das cargas de trabalho.

O Elastic Load Balancing oferece suporte aos seguintes balanceadores de carga: balanceadores de carga da aplicação, balanceadores de carga da rede, balanceadores de carga do gateway e balanceadores de carga clássicos. Você pode selecionar o tipo de balanceador de carga que melhor se adapte às suas necessidades. Este guia discute Network Load Balancers. Para obter mais informações sobre os outros balanceadores de carga, consulte o Guia do usuário de Application Load Balancers, o Guia do usuário de Gateway Load Balancers e o Guia do usuário de Classic Load Balancers.

Componentes do Network Load Balancer

Um load balancer serve como ponto único de contato para os clientes. O balanceador de carga distribui o tráfego de entrada entre vários destinos, como instâncias do Amazon EC2. Isso aumenta a disponibilidade do seu aplicativo. Você adiciona um ou mais listeners ao seu load balancer.

Um listener verifica as solicitações de conexão de clientes, usando o protocolo e a porta que você configurar e encaminha solicitações para um grupo de destino.

Um grupo de destino roteia solicitações a um ou mais destinos registrados, como instâncias do EC2, usando o protocolo e o número de porta que você especifica. Os grupos de destino do Network Load Balancer são compatíveis com os protocolos TCP, UDP, TCP_UDP, TLS, QUIC e TCP_QUIC. Você pode registrar um destino com vários grupos de destino. Você pode configurar verificações de integridade em cada grupo de destino. As verificações de integridade são executadas em todos os destinos registrados para os grupos de destino especificados na ação padrão para o balanceador de carga.

Para saber mais, consulte a documentação a seguir:

- balanceador de cargas
- Listeners

- Grupos de destino

Visão geral do Network Load Balancer

Um Network Load Balancer funciona na quarta camada do modelo Open Systems Interconnection (OSI - interconexão de sistemas abertos). Ele pode lidar com milhões de solicitações por segundo. Após o balanceador de carga receber uma solicitação de um cliente, ele seleciona um destino a partir de um grupo de destino na ação padrão. Ele tenta enviar a solicitação para o destino selecionado usando o protocolo e a porta especificados.

Quando você habilita uma zona de disponibilidade para o balanceador de carga, o Elastic Load Balancing cria um nó de balanceador de carga na zona de disponibilidade. Por padrão, cada nó do load balancer distribui tráfego aos destinos registrados somente na sua zona de disponibilidade. Se você habilitar o balanceamento de carga entre zonas, cada nó do load balancer distribuirá o tráfego aos destinos registrados em todas as zonas de disponibilidade habilitadas. Para obter mais informações, consulte Atualizar as zonas de disponibilidade do Network Load Balancer.

Para aumentar a tolerância a falhas das suas aplicações, você pode habilitar várias zonas de disponibilidade para seu balanceador de carga e garantir que cada grupo de destino tenha pelo menos um destino em cada zona de disponibilidade habilitada. Por exemplo, se um ou mais grupos de destino não têm um destino íntegro em uma zona de disponibilidade, removemos o endereço IP da sub-rede correspondente do DNS, mas os nós do load balancer em outras zonas de disponibilidade permanecerão disponíveis para rotear o tráfego. Se um cliente não honrar o time-to-live (TTL) e enviar solicitações para o endereço IP depois que ele for removido do DNS, as solicitações falharão.

Para o tráfego TCP, o load balancer seleciona um destino usando um algoritmo de hash de fluxo baseado no protocolo, no endereço IP de origem, na porta de origem, no endereço IP de destino, na porta de destino e no número de sequência do TCP. As conexões TCP de um cliente têm diferentes portas de origem e números de sequência e podem ser direcionadas para destinos diferentes. Cada conexão TCP individual é roteada para um único destino para a vida útil da conexão.

Para o tráfego UDP, o load balancer seleciona um destino usando um algoritmo de hash de fluxo baseado no protocolo, no endereço IP de origem, na porta de origem, no endereço IP de destino e na porta de destino. Um fluxo UDP tem a mesma origem e o mesmo destino, portanto, ele é roteado de forma consistente para um único destino durante toda sua vida útil. Diferentes fluxos UDP têm diferentes portas e endereços IP de origem. Assim, eles podem ser roteados para destinos diferentes.

Para o tráfego QUIC, o balanceador de carga seleciona um destino usando a ID do servidor especificada na ID de conexão (CID). Em relação às tentativas iniciais de conexão que não têm uma ID de servidor, é usado um algoritmo de hash de fluxo baseado no protocolo, no endereço IP de origem, na porta de origem, no endereço IP de destino e na porta de destino. Depois de estabelecer uma ID de conexão, o tráfego para esse CID é roteado para o mesmo destino durante a vida útil do CID.

O Elastic Load Balancing cria uma interface de rede para cada zona de disponibilidade que você habilita. Cada nó de load balancer na Zona de disponibilidade usa essa interface de rede para obter um endereço IP estático. Quando você criar um load balancer voltado para a Internet, opcionalmente, poderá associar um endereço IP elástico por sub-rede.

Quando você cria um grupo de destino, especifica o tipo de destino, o que determina como você registra os destinos. Por exemplo, você pode registrar uma instância IDs, endereços IP ou um Application Load Balancer. O tipo de destino também afeta se os endereços IP do cliente são preservados. Para obter mais informações, consulte the section called “Preservação do IP do cliente”.

Você pode adicionar e remover destinos do balanceador de carga conforme suas necessidades mudarem, sem perturbar o fluxo geral de solicitações para sua aplicação. O Elastic Load Balancing escala seu balanceador de carga à medida que o tráfego para sua aplicação muda com o tempo. O Elastic Load Balancing pode ser escalado para a vasta maioria de workloads automaticamente.

Você pode configurar verificações de integridade, que são usadas para monitorar a integridade dos destinos registrados para que o load balancer possa enviar solicitações apenas para os destinos íntegros.

Para obter mais informações, consulte Como o Elastic Load Balancing funciona no Manual do usuário do Elastic Load Balancing.

Benefícios da migração de um Classic Load Balancer

O uso de um Network Load Balancer em vez de um Classic Load Balancer tem os seguintes benefícios:

- Capacidade de processar cargas de trabalho voláteis e de alterar a escala para milhões de solicitações por segundo.
- Suporte para endereços IP estáticos para o load balancer. Também é possível atribuir um endereço IP elástico por sub-rede habilitado para o load balancer.

- Suporte para registrar destinos por endereço IP, incluindo destinos fora da VPC para o load balancer.
- Suporte para solicitações de roteamento para vários aplicativos em uma única instância do EC2. Você pode registrar cada instância ou endereço IP com o mesmo grupo de destino usando várias portas.
- Suporte para aplicativos em contêineres. O Amazon Elastic Container Service (Amazon ECS) pode selecionar uma porta não utilizada ao programar uma tarefa e registrá-la em um grupo de destino usando essa porta. Isso permite que você faça um uso eficiente dos seus clusters.
- Support para monitorar a integridade de cada serviço de forma independente, pois as verificações de saúde são definidas no nível do grupo-alvo e muitas CloudWatch métricas da Amazon são relatadas no nível do grupo-alvo. Anexar um grupo de destino a um grupo do Auto Scaling permite que você escale cada serviço dinamicamente com base na demanda.
- Suporte para os protocolos QUIC e TCP_QUIC com controle avançado de congestionamento, menos estabelecimento de conexão de ida e volta, TLS integrado e migração da conexão entre redes.

Para obter mais informações sobre os recursos compatíveis com cada tipo de balanceador de carga, consulte a Comparação de produtos do Elastic Load Balancing.

Introdução

Para criar um Network Load Balancer usando o Console de gerenciamento da AWS,, ou AWS CLI AWS CloudFormation, consulte. Criar um Network Load Balancer

Para demonstrações de configurações comuns do balanceador de carga, consulte Elastic Load Balancing Demos.

Preços

Para obter mais informações, consulte Preço do Elastic Load Balancing.

Network Load Balancers

Um Network Load Balancer atua como ponto único de contato para os clientes. Os clientes enviam solicitações para o Network Load Balancer, e o Network Load Balancer as envia para destinos, EC2 como instâncias, em uma ou mais zonas de disponibilidade.

Para configurar o Network Load Balancer, você cria grupos de destino e, em seguida, registra os destinos nesses grupos. O Network Load Balancer será mais eficaz se você garantir que cada zona de disponibilidade habilitada tenha pelo menos um destino registrado. Você também pode criar listeners para verificar a solicitações de conexão de clientes e rotear solicitações dos clientes para os destinos em seus grupos de destino.

Os Network Load Balancers oferecem suporte a conexões de clientes por meio de emparelhamento de VPC AWS Direct Connect, VPN gerenciada e soluções VPN de terceiros.

Conteúdo

- Reservas de capacidade para seu Network Load Balancer

Estado do load balancer

Um Network Load Balancer pode estar em um dos seguintes estados:

`provisioning`

O Network Load Balancer está sendo configurado.

`active`

O Network Load Balancer está totalmente configurado e pronto para rotear tráfego.

`failed`

Não foi possível configurar o Network Load Balancer.

Tipo de endereço IP

É possível definir os tipos de endereços IP que os clientes podem usar com seu Network Load Balancer.

Os Network Load Balancers oferecem suporte aos seguintes tipos de endereço IP:

`ipv4`

Os clientes devem se conectar usando IPv4 endereços (por exemplo, 192.0.2.1).

`dualstack`

Os clientes podem se conectar ao Network Load Balancer usando IPv4 endereços (por exemplo, 192.0.2.1) e endereços (por exemplo, 2001:0 db 8:85 a 3:0:0:8 a2e IPv6 : 0370:7334).

Considerações

- O Network Load Balancer se comunica com os destinos com base no tipo de endereço IP do grupo de destino.
- Para oferecer suporte à preservação do IP de origem para IPv6 ouvintes UDP, certifique-se de que o prefixo Enable for IPv6 Source NAT esteja ativado.

- Quando você habilita o modo dualstack para o Network Load Balancer, o Elastic Load Balancing fornece um registro de DNS AAAA para o Network Load Balancer. Os clientes que se comunicam com o Network Load Balancer usando IPv4 endereços resolvem o registro DNS A. Os clientes que se comunicam com o Network Load Balancer usando IPv6 endereços resolvem o registro DNS AAAA.
- O acesso aos Network Load Balancers dualstack internos por meio do gateway da Internet é bloqueado para impedir acesso não intencional à Internet. No entanto, isso não impede outros acessos à Internet (por exemplo, por meio de peering, Transit Gateway ou Site-to-Site VPN). AWS Direct Connect

Para obter mais informações, consulte Atualizar os tipos de endereço IP para o Network Load Balancer.

Tempo limite de inatividade da conexão

Para cada solicitação de TCP que um cliente faz por meio de um Network Load Balancer, o estado da conexão é rastreado. Se não há dados enviados do cliente nem do destino por um período que ultrapasse o tempo limite de inatividade, a conexão não é mais acompanhada. Se um cliente ou um destino envia dados depois do tempo limite de inatividade, o cliente recebe um pacote TCP RST para indicar que a conexão não é mais válida.

O valor padrão do tempo limite de inatividade para fluxos TCP é 350 segundos, mas pode ser atualizado para qualquer valor entre 60 e 6.000 segundos. Os clientes ou destinos podem usar pacotes keepalive de TCP para reiniciar o tempo limite de natividade. Pacotes Keepalive enviados para manter conexões TLS não podem conter dados ou carga.

O tempo limite de inatividade da conexão para receptores TLS é de 350 segundos e não pode ser modificado. Quando um receptor TLS recebe um pacote TCP keepalive de um cliente ou de um destino, o balanceador de carga gera pacotes TCP keepalive e os envia para as conexões de frontend e backend a cada 20 segundos. Não é possível modificar esse comportamento.

Embora o UDP não tenha conexão, o balanceador de carga mantém o estado do fluxo de UDP com base nos endereços IP e nas portas. Isso garante que os pacotes que pertencem ao mesmo fluxo sejam enviados consistentemente para o mesmo destino. Depois do tempo limite de inatividade, o balanceador de carga considerará o pacote UDP de entrada como um novo fluxo e o roteará para um novo destino. O Elastic Load Balancing define o valor do tempo limite de inatividade para fluxos de UDP como 120 segundos. Elas não podem ser alteradas.

EC2 as instâncias devem responder a uma nova solicitação em 30 segundos para estabelecer um caminho de retorno.

Para obter mais informações, consulte Atualizar o tempo limite de inatividade.

Atributos do load balancer

É possível configurar o Network Load Balancer editando seus atributos. Para obter mais informações, consulte Editar atributos do Network Load Balancer.

Os atributos de balanceador de carga para Network Load Balancers são:

`access_logs.s3.enabled`

Indica se os logs de acesso armazenados no Amazon S3 estão habilitados. O padrão é `false`.

`access_logs.s3.bucket`

O nome do bucket do Amazon S3 para os logs de acesso. Esse atributo é necessário se os logs de acesso estiverem habilitados. Para obter mais informações, consulte Requisitos do bucket.

`access_logs.s3.prefix`

O prefixo para o local no bucket do Amazon S3.

`deletion_protection.enabled`

Indica se a proteção contra exclusão está habilitada. O padrão é `false`.

`ipv6.deny_all_igw_traffic`

Bloqueia o acesso do gateway da Internet (IGW) ao Network Load Balancer, impedindo o acesso não intencional ao Network Load Balancer interno por meio de um gateway da Internet. Ele é definido como `false` para Network Load Balancers voltados para a Internet e `true` para Network Load Balancers internos. Esse atributo não impede o acesso à Internet que não seja IGW (por exemplo, por meio de peering, AWS Direct Connect Transit Gateway ou). Site-to-Site VPN

`load_balancing.cross_zone.enabled`

Indica se o balanceamento de carga entre zonas está habilitado. O padrão é `false`.

`dns_record.client_routing_policy`

Indica como o tráfego é distribuído entre as zonas de disponibilidade de Network Load Balancers. Os valores possíveis são `availability_zone_affinity` com 100% de

afinidade zonal, `partial_availability_zone_affinity` com 85% de afinidade zonal e `any_availability_zone` com 0% de afinidade zonal.

`secondary_ips.auto_assigned.per_subnet`

O número de endereços IP secundários a serem configurados. Use para resolver erros de alocação de portas se você não puder adicionar destinos. O intervalo válido é de 0 a 7. O padrão é 0. Depois de definir esse valor, não será possível diminuí-lo.

`zonal_shift.config.enabled`

Indica se a mudança de zona está habilitada. O padrão é `false`.

Balanceamento de carga entre zonas

Por padrão, cada nó de Network Load Balancer distribui tráfego aos destinos registrados somente na própria zona de disponibilidade. Se você ativar o balanceamento de carga entre zonas, cada nó de Network Load Balancer distribuirá tráfego aos destinos registrados em todas as zonas de disponibilidade habilitadas. Você também pode ativar o balanceamento de carga entre zonas no nível de grupo de destino. Para mais informações, consulte the section called “Balanceamento de carga entre zonas” e Balanceamento de carga entre zonas no Guia do usuário do Elastic Load Balancing.

Nome DNS

Cada Network Load Balancer recebe um nome de Sistema de Nomes de Domínio (DNS) padrão com a seguinte sintaxe: - .elb. *name id region*.amazonaws.com. Por exemplo, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com.

Se preferir usar um nome DNS que seja mais fácil de lembrar, é possível criar um nome de domínio personalizado e associá-lo ao nome DNS do seu Network Load Balancer. Quando um cliente faz uma solicitação usando esse nome de domínio personalizado, o servidor DNS o resolverá para o nome DNS para seu Network Load Balancer.

Primeiro, registre um nome de domínio com um registrador de nomes de domínio credenciado. Em seguida, use o serviço de DNS, como o registrador de domínios, para criar um registro de DNS para rotear solicitações para o Network Load Balancer. Para obter mais informações, consulte a documentação do serviço DNS. Por exemplo, se você usar o Amazon Route 53 como serviço de DNS, criará um registro de alias que apontará para o Network Load Balancer. Para obter mais

informações, consulte Rotear tráfego para um balanceador de carga ELB no Guia do desenvolvedor do Amazon Route 53.

O Network Load Balancer tem um endereço IP por zona de disponibilidade habilitada. Esses são os endereços IP dos nós do Network Load Balancer. O nome de DNS do Network Load Balancer é resolvido nesses endereços. Por exemplo, vamos supor que o nome de domínio personalizado para seu Network Load Balancer seja `example.networkloadbalancer.com`. Use o comando dig ou nslookup a seguir para determinar os endereços IP dos nós do Network Load Balancer.

Linux ou Mac

```
$ dig +short example.networkloadbalancer.com
```

Windows

```
C:\> nslookup example.networkloadbalancer.com
```

O Network Load Balancer tem registros de DNS para seus nós. Você pode usar nomes DNS com a seguinte sintaxe para determinar os endereços IP dos nós do Network Load Balancer:. *az* *name*-... *id* coelho. *region*.amazonaws.com.

Linux ou Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Integridade de zona do balanceador de carga

Os Network Load Balancers têm registros DNS de zonas e endereços IP no Route 53 para cada zona de disponibilidade habilitada. Quando um Network Load Balancer falha em uma verificação de integridade de zona para uma zona de disponibilidade específica, seu registro DNS é removido do Route 53. A integridade zonal do balanceador de carga é monitorada usando a CloudWatch métrica da Amazon`ZonalHealthStatus`, oferecendo mais informações sobre eventos que causam uma falha na implementação de medidas preventivas para garantir a disponibilidade ideal do aplicativo. Para obter mais informações, consulte, Métricas do Network Load Balancer.

Os Network Load Balancers podem falhar nas verificações de integridade de zonas por vários motivos, o que faz com que eles se tornem não íntegros. Veja abaixo as causas comuns de Network Load Balancers não íntegros decorrentes de falhas nas verificações de integridade de zonas.

Verifique as seguintes causas possíveis:

- Não há destinos íntegros para o balanceador de carga
- O número de destinos íntegros é menor que o mínimo configurado
- Há uma mudança de zona ou mudança de zona automática em andamento
- O tráfego está sendo migrado automaticamente para zonas íntegros devido a problemas detectados

Criar um Network Load Balancer

Um Network Load Balancer recebe solicitações de clientes e as distribui entre destinos em um grupo-alvo, como instâncias. EC2 Para obter mais informações, consulte o the section called “Visão geral do Network Load Balancer”.

Tarefas

Pré-requisitos

- Decida quais zonas de disponibilidade e tipos de endereço IP seu aplicativo suportará. Configure a VPC do balanceador de carga com sub-redes em cada uma dessas zonas de disponibilidade. Se o aplicativo oferecer suporte a ambos IPv4 e ao IPv6 tráfego, certifique-se de que as sub-redes tenham ambos e. IPv4 IPv6 CIDRs Implante pelo menos um destino em cada zona de disponibilidade.
- Certifique-se de que grupos de segurança associados às instâncias de destino permitam tráfego na porta do receptor de endereços IP do cliente (se os destinos são especificados por ID de instância) ou nós do balanceador de carga (se os destinos são especificados por endereço IP). Para obter mais informações, consulte the section called “Grupos de segurança de destino”.

- Certifique-se de que os grupos de segurança associados a uma instância permitem tráfego do balanceador de carga usando a porta de verificação de integridade e o protocolo de verificação de integridade.
- Se você planeja fornecer endereços IP estáticos ao seu balanceador de carga, certifique-se de que cada endereço IP elástico seja do pool de IPv4 endereços da Amazon e que tenha o mesmo grupo de borda de rede que o balanceador de carga.
- Se você planeja utilizar receptores QUIC ou TCP_QUIC, assegure-se de que o Network Load Balancer use o tipo de endereço `ipv4` e não tenha grupos de segurança associados a ele.

Criar o balanceador de carga

Como parte da criação de um Network Load Balancer, você criará o balanceador de carga, pelo menos um receptor e pelo menos um grupo de destino. Seu balanceador de carga estará pronto para lidar com as solicitações do cliente quando houver pelo menos um destino registrado íntegro em cada uma das zonas de disponibilidade habilitadas.

Console

Para criar um Network Load Balancer

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Selecione Criar um balanceador de carga.
4. Em Network Load Balancer, escolha Criar.
5. Configuração básica

    a. Em Nome do balanceador de carga, insira um nome para o seu Network Load Balancer. O nome deve ser exclusivo em seu conjunto de balanceadores de carga na região. Os nomes podem ter no máximo 32 caracteres e conter somente caracteres alfanuméricos e hifens. Eles não podem começar nem terminar com hífen ou com `internal-`.

    b. Em Scheme (Esquema), escolha Internet-facing (Voltado para a Internet) ou Internal (Interno). Um Network Load Balancer voltado para a Internet roteia solicitações de clientes até destinos na Internet. Um Network Load Balancer interno roteia solicitações para destinos usando endereços IP privados.

    c. Para o tipo de endereço IP do balanceador de carga, escolha IPv4se seus clientes usam IPv4 endereços para se comunicar com o Network Load Balancer ou Dualstack se seus

clientes usam IPv4 ambos IPv6 e endereços para se comunicar com o Network Load Balancer.

6. Mapeamento de rede

   a. Para VPC, selecione a VPC que você preparou para seu balanceador de carga. Com um balanceador de carga voltado para a Internet, somente VPCs com um gateway de Internet estão disponíveis para seleção.

   b. Com um balanceador de carga de pilha dupla, você não pode adicionar um ouvinte UDP a menos que o prefixo Enable for SOURCE NAT esteja Ativado (prefixos NAT de IPv6 origem por sub-rede).

   c. Para Zonas de disponibilidade e sub-redes, selecione pelo menos uma zona de disponibilidade e selecione uma sub-rede por zona. Observe que sub-redes que foram compartilhadas com você estão disponíveis para seleção.

      Se você selecionar várias zonas de disponibilidade e garantir destinos registrados em cada zona selecionada, isso aumentará a tolerância a falhas da sua aplicação.

   d. Para um balanceador de carga voltado para a internet, você pode selecionar um endereço IP elástico para cada zona de disponibilidade. Isso fornece o balanceador de carga com endereços IP estáticos.

      Com um balanceador de carga interno, você pode inserir um IPv4 endereço privado do intervalo de endereços de cada sub-rede ou deixar AWS selecionar um para você.

      Com um balanceador de carga de pilha dupla, você pode inserir um IPv6 endereço do intervalo de endereços de cada sub-rede ou deixar AWS selecionar um para você.

      Para um balanceador de carga com NAT de origem habilitado, você pode inserir um IPv6 prefixo personalizado ou deixar AWS selecionar um para você.

7. Grupos de segurança

   Nós selecionamos previamente o grupo de segurança padrão para a VPC do balanceador de carga. Você pode selecionar grupos de segurança adicionais, conforme necessário. Se você não tiver um grupo de segurança que atenda a suas necessidades, escolha criar um novo grupo de segurança para criar um. Para saber mais, consulte Criar um grupo de segurança no Guia do usuário da Amazon VPC.

> **Warning**
>
> Se você não associar grupos de segurança ao Network Load Balancer agora, não poderá associá-los posteriormente.

> **Warning**
>
> Para utilizar receptores QUIC ou TCP_QUIC, seu Network Load Balancer não deve ter grupos de segurança.

8. Receptores e roteamento

   a. O padrão é um receptor que aceite tráfego TCP na porta 80. Você pode manter as configurações padrão do receptor ou modificar o Protocolo e a Porta conforme a necessidade.

   b. Em Ação padrão, selecione um grupo de destino para encaminhar o tráfego.

      Para adicionar outro grupo de destino, selecione Adicionar grupo de destino e atualize os pesos conforme necessário.

      Caso você não tenha um grupo de destino que responda às suas necessidades, escolha Criar grupo de destino para criar um agora. Para obter mais informações, consulte Criar um grupo de destino.

   c. (Opcional) Escolha Adicionar tag de receptor e digite uma chave de tag e um valor de tag.

   d. (Opcional) Escolha Adicionar receptor para adicionar outro receptor (por exemplo, um receptor TLS).

9. Configurações seguras do receptor

   Essa seção aparece somente se você adicionar um receptor TLS.

   a. Em Política de segurança, escolha uma política de segurança que atenda aos seus requisitos. Para obter mais informações, consulte Políticas de segurança.

   b. Em Certificado de SSL/TLS servidor padrão, escolha Do ACM como a fonte do certificado. Selecione um certificado que você provisionou ou importou usando AWS Certificate Manager. Caso você não tenha um certificado disponível no ACM, mas

tenha um certificado para uso com seu balanceador de carga, selecione Importar certificado e insira as informações necessárias. Caso contrário, escolha Solicitar um novo certificado do ACM. Para obter mais informações, consulte Certificados do AWS Certificate Manager no Guia do usuário do AWS Certificate Manager .

c. (Opcional) Para Política ALPN, escolha uma política para habilitar ALPN. Para obter mais informações, consulte the section called “Políticas ALPN”.

10. Tags do balanceador de carga

    (Opcional) Expanda as Tags do balanceador de carga. Escolha Adicionar nova tag e digite uma chave de tag e um valor de tag. Para obter mais informações, consulte Etiquetas.

11. Resumo

    Revise sua configuração e escolha Create load balancer (Criar um balanceador de carga). Alguns atributos padrão são aplicados ao Network Load Balancer durante a criação. Você pode visualizá-los e editá-los depois de criar o Network Load Balancer. Para obter mais informações, consulte Atributos do load balancer.

AWS CLI

Para criar um Network Load Balancer

Use o comando create-load-balancer.

O exemplo mostrado a seguir cria um balanceador de carga voltado para a internet com duas zonas de disponibilidade habilitadas e um grupo de segurança.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para criar um Network Load Balancer interno

Inclua a opção `--scheme`, como mostrado no exemplo a seguir.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
```

```
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para criar um Network Load Balancer de pilha dupla

Inclua a opção `--ip-address-type`, como mostrado no exemplo a seguir.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --ip-address-type dualstack \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para adicionar um listener

Use o comando create-listener. Para obter exemplos, consulte Criar um listener.

CloudFormation

Para criar um Network Load Balancer

Defina um recurso do tipo AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'department'
          Value: '123'
```

Para adicionar um listener

Defina um recurso do tipo AWS::ElasticLoadBalancingV2::Listener. Para obter exemplos, consulte Criar um listener.

Teste o balanceador de carga

Depois de criar seu Network Load Balancer, você pode verificar se suas EC2 instâncias passaram na verificação de integridade inicial e, em seguida, testar se o Network Load Balancer está enviando tráfego para suas instâncias. EC2 Para excluir o Network Load Balancer, consulte Excluir um Network Load Balancer.

Para testar o Network Load Balancer

1. Após a criação do Network Load Balancer, selecione Fechar.
2. No painel de navegação esquerdo, selecione Grupos de destino.
3. Selecione o novo grupo de destino.
4. Escolha Destinos e verifique se a sua instância está pronta. Se o status de uma instância for `initial`, talvez seja porque a instância ainda está no processo de ser registrada ou ainda não passou pelo número mínimo de verificações de integridade para ser considerada íntegra. Após o status de pelo menos uma instância ser íntegro, você poderá testar seu Network Load Balancer. Para obter mais informações, consulte Status de integridade do destino.
5. No painel de navegação, selecione Load Balancers.
6. Selecione o novo Network Load Balancer.
7. Copie o nome DNS do Network Load Balancer (por exemplo, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com). Cole o nome DNS no campo de endereço de um navegador da web conectado à Internet. Se tudo estiver funcionando, o navegador exibirá a página padrão do seu servidor.

Próximas etapas

Após criar seu balanceador de carga, siga os seguintes passos:

- Configure os atributos do balanceador de carga.
- Configure os atributos do grupo de destino.

- [Receptores TLS] Adicione certificados à lista de certificados opcionais.
- Configure os atributos de monitoramento.

Atualizar as zonas de disponibilidade do Network Load Balancer

Você pode habilitar ou desabilitar as zonas de disponibilidade do seu Network Load Balancer a qualquer momento. Quando você habilita uma zona de disponibilidade, você precisa especificar uma sub-rede nessa zona de disponibilidade. Depois de habilitar uma Zona de disponibilidade, o load balancer começa a rotear as solicitações para os destinos registrados nessa Zona de disponibilidade. O load balancer é mais eficaz se você garantir que cada Zona de disponibilidade ativada tenha pelo menos um destino registrado. Habilitar várias zonas de disponibilidade ajuda a melhorar a tolerância a falhas das suas aplicações.

O balanceamento de carga elástico cria um nó do Network Load Balancer na zona de disponibilidade que você escolher e uma interface de rede para a sub-rede selecionada nessa zona de disponibilidade. Cada nó do Network Load Balancer na Zona de Disponibilidade usa a interface de rede para obter um IPv4 endereço. Você pode visualizar essas interfaces de rede, mas elas não podem ser modificadas.

Considerações

- Para Network Load Balancers voltados para a Internet, as sub-redes especificadas devem ter pelo menos 8 endereços IP disponíveis. Para balanceadores de carga de rede internos, isso só é necessário se você permitir AWS selecionar um IPv4 endereço privado na sub-rede.
- Não é possível especificar uma sub-rede em uma zona de disponibilidade restrita. No entanto, é possível especificar uma sub-rede em uma zona de disponibilidade não restrita e usar o balanceamento de carga entre zonas para distribuir o tráfego para destinos na zona de disponibilidade restrita.
- Não é possível especificar uma sub-rede em uma Zona local.
- Você não pode remover uma sub-rede se o Network Load Balancer tiver associações ativas de endpoint da VPC da Amazon.
- Ao adicionar outra vez uma sub-rede removida anteriormente, uma nova interface de rede será criada com uma ID diferente.
- As alterações de sub-rede na mesma zona de disponibilidade devem ser ações independentes. Primeiro, você conclui a remoção da sub-rede existente e, em seguida, pode adicionar a nova sub-rede.

- A remoção da sub-rede pode levar até 3 minutos para ser concluída.

Ao criar um Network Load Balancer voltado para a internet, é possível especificar um endereço IP elástico para cada zona de disponibilidade. Os endereços IP elásticos fornecem seu Network Load Balancer com endereços IP estáticos. Se você optar por não especificar um endereço IP elástico, AWS atribuirá um endereço IP elástico para cada zona de disponibilidade.

Ao criar um Network Load Balancer interno, você pode especificar um endereço IP privado de cada sub-rede. Os endereços IP privados fornecem seu Network Load Balancer com endereços IP estáticos. Se você optar por não especificar um endereço IP privado, AWS atribuirá um para você.

Antes de atualizar as zonas de disponibilidade do Network Load Balancer, recomendamos avaliar quaisquer possíveis impactos nas conexões, nos fluxos de tráfego ou nas workloads de produção existentes.

⚠ A atualização de uma zona de disponibilidade pode causar interrupções

- Quando uma sub-rede é removida, a Interface de Rede Elástica (ENI) associada é excluída. Isso faz com que todas as conexões ativas na Zona de Disponibilidade sejam encerradas.
- Depois que uma sub-rede é removida, todos os destinos na zona de disponibilidade à qual ela estava associada são marcados como `unused`. Isso resulta na remoção desses destinos do grupo de destinos disponíveis e no encerramento de todas as conexões ativas com esses destinos. Isso inclui todas as conexões originadas de outras zonas de disponibilidade ao utilizar o balanceamento de carga entre zonas.
- Os Network Load Balancers têm um tempo de vida útil (TTL) de 60 segundos para seu nome de domínio totalmente qualificado (FQDN). Quando uma zona de disponibilidade que contém destinos ativos é removida, quaisquer conexões existentes de cliente podem passar por tempos limite até que a resolução do DNS ocorra novamente e o tráfego seja transferido para qualquer zona de disponibilidade restante.

Console

Para modificar as zonas de disponibilidade

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.

2. No painel de navegação, selecione Balanceador de carga.
3. Selecione o load balancer.
4. Na guia Mapeamento de rede, escolha Editar sub-redes.
5. Para habilitar uma zona de disponibilidade, marque a caixa de seleção e selecione uma sub-rede. Se houver apenas uma sub-rede disponível, ela será selecionada para você.
6. Para alterar a sub-rede de uma zona de disponibilidade habilitada, escolha uma das outras sub-redes na lista.
7. Para desabilitar uma zona de disponibilidade, desmarque a caixa de seleção.
8. Escolha Salvar alterações.

AWS CLI

Para modificar as zonas de disponibilidade

Use o comando set-sub-redes.

```
aws elbv2 set-subnets \
    --load-balancer-arn load-balancer-arn \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890
```

CloudFormation

Para modificar as zonas de disponibilidade

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref new-subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Atualizar os tipos de endereço IP para o Network Load Balancer

Você pode configurar seu Network Load Balancer para que os clientes possam se comunicar com o Network Load Balancer IPv4 usando somente endereços ou usando endereços IPv6 e endereços (IPv4 pilha dupla). O Network Load Balancer se comunica com os destinos com base no tipo de endereço IP do grupo de destino. Para obter mais informações, consulte Tipo de endereço IP.

Requisitos para dualstack

- É possível definir o tipo de endereço IP ao criar o Network Load Balancer e atualizá-lo a qualquer momento.
- A nuvem privada virtual (VPC) e as sub-redes que você especifica para o Network Load Balancer devem ter blocos CIDR associados. IPv6 Para obter mais informações, consulte IPv6os endereços no Guia EC2 do usuário da Amazon.
- As tabelas de rotas das sub-redes do Network Load Balancer devem rotear o tráfego. IPv6
- A rede ACLs das sub-redes do Network Load Balancer deve permitir tráfego. IPv6
- Não há receptores QUIC ou TCP_QUIC conectados ao Network Load Balancer.

Console

Para atualizar o tipo de endereço IP

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Marque a caixa de seleção para o Network Load Balancer.
4. Selecione Ações, Editar tipo de endereço IP.
5. Para o tipo de endereço IP, escolha oferecer suporte somente IPv4para IPv4 endereços ou Dualstack para oferecer suporte a ambos IPv4 e endereços. IPv6
6. Escolha Salvar alterações.

AWS CLI

Para atualizar o tipo de endereço IP

Use o comando set-ip-address-type.

```
aws elbv2 set-ip-address-type \
```

```
    --load-balancer-arn load-balancer-arn \
    --ip-address-type dualstack
```

CloudFormation

Para atualizar o tipo de endereço IP

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Editar atributos para o Network Load Balancer

Após criar um Network Load Balancer, você poderá editar seus atributos.

Atributos do load balancer

- Deletion protection (Proteção contra exclusão)
- Balanceamento de carga entre zonas
- Afinidade de DNS de zona de disponibilidade
- Endereços IP secundários

Deletion protection (Proteção contra exclusão)

Para evitar que seu Network Load Balancer seja excluído acidentalmente, é possível ativar a proteção contra exclusão. Por padrão, a proteção contra exclusão é desabilitada para seu Network Load Balancer.

Se você habilitar a proteção contra exclusão para o Network Load Balancer, deverá desabilitá-la antes de excluir o Network Load Balancer.

Console

Para habilitar ou desabilitar a proteção contra exclusão

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Selecione o nome do Network Load Balancer para abrir a página de detalhes dele.
4. Na guia Atributos, escolha Editar.
5. Em Proteção, ative ou desative a Proteção contra exclusão.
6. Escolha Salvar alterações.

AWS CLI

Para habilitar ou desabilitar a proteção contra exclusão

Use o comando modify-load-balancer-attributes com o atributo `deletion_protection.enabled`.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=deletion_protection.enabled,Value=true"
```

CloudFormation

Para habilitar ou desabilitar a proteção contra exclusão

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso para incluir o `deletion_protection.enabled` atributo.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
```

```
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "deletion_protection.enabled"
          Value: "true"
```

Balanceamento de carga entre zonas

Com Network Load Balancers, o balanceamento de carga entre zonas é desativado por padrão no nível do balanceador de carga, mas você pode ativá-lo a qualquer momento. Para grupos de destino, o padrão é usar a configuração do balanceador de carga, mas você pode substituir o padrão ativando ou desativando explicitamente o balanceamento de carga entre zonas em nível de grupo de destino. Para obter mais informações, consulte the section called “Balanceamento de carga entre zonas”.

Console

Para habilitar ou desabilitar o balanceamento de carga entre zonas para o balanceador de carga.

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing, selecione Load Balancers.
3. Selecione o nome do balanceador de carga para abrir a página de detalhes dele.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, ative ou desative Balanceamento de carga entre zonas.
6. Escolha Salvar alterações.

AWS CLI

Para habilitar ou desabilitar o balanceamento de carga entre zonas para o balanceador de carga.

Use o comando modify-load-balancer-attributes com o atributo `load_balancing.cross_zone.enabled`.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Para habilitar ou desabilitar o balanceamento de carga entre zonas para o balanceador de carga.

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancer recurso para incluir o `load_balancing.cross_zone.enabled` atributo.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Afinidade de DNS de zona de disponibilidade

Ao usar a política padrão de roteamento de cliente, as solicitações enviadas para o nome de DNS do Network Load Balancer receberão todos os endereços IP íntegros do Network Load Balancer. Isso leva à distribuição das conexões de clientes entre as zonas de disponibilidade do Network Load Balancer. Com as políticas de roteamento de afinidade de zona de disponibilidade, as consultas ao DNS do cliente favorecem os endereços IP do Network Load Balancer na sua própria zona de disponibilidade. Isso ajuda a melhorar a latência e a resiliência, pois os clientes não precisam cruzar os limites de zona de disponibilidade ao se conectarem aos destinos.

As políticas de roteamento de afinidade de zona de disponibilidade se aplicam somente aos clientes que resolvem o nome de DNS de Network Load Balancers usando o Route 53 Resolver. Para obter

mais informações, consulte O que é Amazon Route 53 Resolver? no Guia do desenvolvedor do Amazon Route 53

Políticas de roteamento de clientes disponíveis para Network Load Balancers usando o Route 53 Resolver:

- Afinidade de zona de disponibilidade: 100% de afinidade zonal

  As consultas ao DNS do cliente favorecerão o endereço IP do Network Load Balancer na sua própria zona de disponibilidade. As consultas poderão ser resolvidas para outras zonas se não houver endereços IP de Network Load Balancer íntegros na sua própria zona.
- Afinidade de zona de disponibilidade parcial: 85% de afinidade zonal

  85% das consultas ao DNS do cliente favorecerão os endereços IP do Network Load Balancer na sua própria zona de disponibilidade, enquanto as consultas restantes serão resolvidas para qualquer zona íntegra. As consultas podem ser resolvidas em outras zonas íntegras se não houver endereços IP íntegros na própria zona. Quando não há endereços IP íntegros em nenhuma zona, as consultas são resolvidas em qualquer zona.
- Qualquer zona de disponibilidade (padrão):0% de afinidade zonal

  As consultas ao DNS do cliente são resolvidas entre endereços IP íntegros do Network Load Balancer em todas as zonas de disponibilidade do Network Load Balancer.

A afinidade de zona de disponibilidade ajuda a rotear solicitações do cliente para o Network Load Balancer, enquanto o balanceamento de carga entre zonas é usado para ajudar a rotear solicitações do Network Load Balancer para os destinos. Ao usar a afinidade de zona de disponibilidade, o balanceamento de carga entre zonas deve ser desativado para que o Network Load Balancer direcione o tráfego do cliente somente para destinos dentro da sua própria zona de disponibilidade. Com essa configuração, o tráfego do cliente é enviado para a mesma zona de disponibilidade do Network Load Balancer. Portanto, é recomendável configurar a aplicação para escalar de forma independente em cada zona de disponibilidade. Essa é uma consideração importante quando o número de clientes por zona de disponibilidade ou o tráfego por zona de disponibilidade não são os mesmos. Para obter mais informações, consulte Balanceamento de carga entre zonas para grupos de destino.

Quando uma zona de disponibilidade for considerada não íntegra ou quando uma mudança de zona for iniciada, o endereço IP zonal será considerado não íntegro e não será retornado aos clientes, a menos que uma falha na abertura esteja efetiva. A afinidade de zona de disponibilidade

é mantida quando o registro de DNS apresenta falha na abertura. Isso ajuda a manter as zonas de disponibilidade independentes e evitar possíveis falhas entre zonas.

Ao usar a afinidade de zona de disponibilidade, são esperados tempos de desequilíbrio entre as zonas de disponibilidade. É recomendável garantir que os destinos sejam escalados em nível zonal para suportar a workload de cada zona de disponibilidade. Nos casos em que esses desequilíbrios são significativos, é recomendável desativar a afinidade de zona de disponibilidade. Isso permite uma distribuição uniforme das conexões do cliente entre todas as zonas de disponibilidade dos Network Load Balancers em 60 segundos ou o TTL do DNS.

Antes de usar afinidade de zona de disponibilidade, considere o seguinte:

- A afinidade de zona de disponibilidade causa alterações em todos os clientes dos Network Load Balancers que estão usando o Route 53 Resolver.
  - Os clientes não conseguem decidir entre as resoluções de DNS da zona local e de várias zonas. A afinidade de zona de disponibilidade decide por eles.
  - Os clientes não têm um método confiável para determinar quando estão sendo afetados pela afinidade de zona de disponibilidade ou para saber qual endereço IP está em qual zona de disponibilidade.
- Ao usar a afinidade da zona de disponibilidade com Network Load Balancers e o Resolvedor do Route 53, recomendamos que os clientes usem o endpoint de entrada do Resolvedor do Route 53 em sua própria zona de disponibilidade.
- Os clientes permanecerão atribuídos ao endereço IP da zona local até que ele seja considerado totalmente não íntegro, de acordo com as verificações de integridade do DNS, e seja removido do DNS.
- Usar a afinidade de zona de disponibilidade com o balanceamento de carga entre zonas ativado pode levar a uma distribuição desequilibrada das conexões do cliente entre as zonas de disponibilidade. É recomendável configurar sua pilha de aplicações para escalar de forma independente em cada zona de disponibilidade, garantindo que ela possa suportar o tráfego de clientes zonais.
- Se o balanceamento de carga entre zonas estiver ativado, o Network Load Balancer estará sujeito ao impacto entre zonas.
- A carga em cada uma das zonas de disponibilidade do Network Load Balancer será proporcional às localizações zonais das solicitações dos clientes. Se você não configurar quantos clientes estão em execução em cada zona de disponibilidade, terá que escalar de forma independente cada zona de disponibilidade, reativamente.

Monitoramento

Recomenda-se rastrear a distribuição das conexões entre as zonas de disponibilidade usando as métricas zonais do Network Load Balancer. Você pode usar métricas para visualizar o número de conexões novas e ativas por zona.

Recomendamos rastrear o seguinte:

- **`ActiveFlowCount`**: o número total de fluxos (ou conexões) simultâneos dos clientes para os destinos.
- **`NewFlowCount`**: o número total de novos fluxos (ou conexões) estabelecidos dos clientes para os destinos no período.
- **`HealthyHostCount`**: o número de destinos considerados íntegros.
- **`UnHealthyHostCount`**: o número de destinos considerados não íntegros.

Para obter mais informações, consulte CloudWatch métricas para seu Network Load Balancer.

Habilitar a afinidade da zona de disponibilidade

Console

Para habilitar a afinidade da zona de disponibilidade

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Selecione o nome do Network Load Balancer para abrir a página de detalhes dele.
4. Na guia Atributos, escolha Editar.
5. Em Configuração de roteamento da zona de disponibilidade, Política de roteamento do cliente (registro de DNS), selecione Afinidade de zona de disponibilidade ou Afinidade de zona de disponibilidade parcial.
6. Escolha Salvar alterações.

AWS CLI

Para habilitar a afinidade da zona de disponibilidade

Use o comando modify-load-balancer-attributes com o atributo `dns_record.client_routing_policy`.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes
 "Key=dns_record.client_routing_policy,Value=partial_availability_zone_affinity"
```

CloudFormation

Para habilitar a afinidade da zona de disponibilidade

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso para incluir o `dns_record.client_routing_policy` atributo.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "dns_record.client_routing_policy"
          Value: "partial_availability_zone_affinity"
```

Endereços IP secundários

Se ocorrerem erros de alocação de porta e você não puder adicionar destinos ao grupo de destino para solucioná-los, você pode adicionar endereços IP secundários às interfaces de rede do balanceador de carga. Para cada zona em que o balanceador de carga está ativado, selecionamos IPv4 endereços da sub-rede do balanceador de carga e os atribuímos à interface de rede correspondente. Esses endereços IP secundários são usados para estabelecer conexões com os destinos. Eles também são usados para o tráfego de verificação de integridade. Recomendamos que você adicione um endereço IP secundário para começar, monitore a métrica

de `PortAllocationErrors` e adicione outro endereço IP secundário somente se os erros de alocação de porta não forem resolvidos.

> **Warning**
>
> Após adicionar endereços IP secundários, você não poderá removê-los. A única maneira de liberar os endereços IP secundários é excluir o balanceador de carga. Antes de adicionar endereços IP secundários, verifique se há IPv4 endereços disponíveis suficientes nas sub-redes do balanceador de carga.

Console

Para adicionar um endereço IP secundário

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Selecione o nome do Network Load Balancer para abrir a página de detalhes dele.
4. Na guia Atributos, escolha Editar.
5. Expanda Atributos de casos especiais, desbloqueie o atributo Endereços IP secundários atribuídos automaticamente por sub-rede e escolha o número dos endereços IP secundários.
6. Escolha Salvar alterações.

AWS CLI

Para adicionar um endereço IP secundário

Use o comando modify-load-balancer-attributes com o atributo `secondary_ips.auto_assigned.per_subnet`.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=secondary_ips.auto_assigned.per_subnet,Value=1"
```

Você pode usar o describe-network-interfacescomando para obter os IPv4 endereços das interfaces de rede do balanceador de carga. O parâmetro `--filters` direciona os resultados das interfaces de rede para os Network Load Balancers de rede e o parâmetro `--query` direciona ainda mais os resultados para o balanceador de carga com o nome especificado

e exibe somente os campos especificados. É possível incluir campos adicionais conforme necessário.

```
aws elbv2 describe-network-interfaces \
    --filters "Name=interface-type,Values=network_load_balancer" \
    --query "NetworkInterfaces[?contains(Description,'my-nlb')].
{ID:NetworkInterfaceId,AZ:AvailabilityZone,Addresses:PrivateIpAddresses[*]}"
```

CloudFormation

Para adicionar um endereço IP secundário

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso para incluir o `secondary_ips.auto_assigned.per_subnet` atributo.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "secondary_ips.auto_assigned.per_subnet"
          Value: "1"
```

Atualizar os grupos de segurança para o Network Load Balancer

É possível associar um grupo de segurança ao Network Load Balancer para controlar o tráfego que tem permissão para acessar e sair do Network Load Balancer. Você especifica as portas, os protocolos e as fontes para permitir o tráfego de entrada, e as portas, os protocolos e os destinos para permitir o tráfego de saída. Se você não atribuir um grupo de segurança ao Network Load Balancer, todo o tráfego do cliente poderá alcançar os receptores do balanceador de carga e todo o tráfego poderá sair do Network Load Balancer.

Você pode adicionar uma regra aos grupos de segurança associados aos seus destinos que faça referência ao grupo de segurança associado ao Network Load Balancer. Isso permite que os clientes enviem tráfego para seus destinos por meio do Network Load Balancer, mas impede que eles enviem tráfego diretamente para seus destinos. Fazer referência ao grupo de segurança associado ao Network Load Balancer nos grupos de segurança associados aos destinos garante que os destinos aceitem o tráfego do Network Load Balancer, mesmo que você habilite a preservação do IP do cliente para o Network Load Balancer.

Você não é cobrado pelo tráfego que é bloqueado pelas regras de entrada do grupo de segurança.

Conteúdo

Considerações

- Você pode associar grupos de segurança a um Network Load Balancer quando criá-lo. Se você criar um Network Load Balancer sem associar grupos de segurança, não poderá associá-los ao Network Load Balancer posteriormente. Recomendamos associar um grupo de segurança ao Network Load Balancer ao criá-lo.
- Caso crie um Network Load Balancer com grupos de segurança associados, você poderá mudar os grupos de segurança associados ao Network Load Balancer a qualquer momento.
- As verificações de integridade estão sujeitas às regras de saída, mas não às regras de entrada. Você deve garantir que as regras de saída não bloqueiem o tráfego da verificação de integridade. Caso contrário, o Network Load Balancer considerará os destinos não íntegros.
- Você pode controlar se o PrivateLink tráfego está sujeito às regras de entrada. Se você habilitar regras de entrada no PrivateLink tráfego, a origem do tráfego será o endereço IP privado do cliente, não a interface do endpoint.

Exemplo: filtro de tráfego de clientes

As regras de entrada a seguir no grupo de segurança associado ao Network Load Balancer só permitem tráfego proveniente do intervalo de endereços especificado. Para um Network Load Balancer interno, você poderá especificar um intervalo CIDR de VPC como origem para permitir somente tráfego de uma VPC específica. Para um Network Load Balancer voltado para a Internet que precise aceitar tráfego de qualquer lugar na Internet, você poderá especificar 0.0.0.0/0 como origem.

Entrada

Protocolo	Fonte	Intervalo de portas	Comment
protocol	*client IP address range*	*listener port*	Permite tráfego de entrada do CIDR de origem na porta do receptor
ICMP	0.0.0.0/0	Todos	Permite que o tráfego ICMP de entrada dê suporte a MTU ou a Path MTU Discovery †

† Para obter mais informações, consulte Path MTU Discovery no Guia do EC2 usuário da Amazon.

Saída

Protocolo	Destino	Intervalo de portas	Comment
Todos	Qualquer lugar	Todos	Permite todo o tráfego de saída

Exemplo: aceitar tráfego somente do Network Load Balancer

Suponha que o Network Load Balancer tenha um grupo de segurança sg-111112222233333. Use as regras a seguir nos grupos de segurança associados às instâncias de destino para garantir que elas aceitem tráfego somente do Network Load Balancer. Você deve garantir que os destinos aceitem o tráfego do Network Load Balancer na porta de destino e na porta de verificação de integridade. Para obter mais informações, consulte the section called “Grupos de segurança de destino”.

Entrada

Protocolo	Fonte	Intervalo de portas	Comment
protocol	sg-111112 222233333	*target port*	Permite tráfego de entrada do Network Load Balancer na porta de destino
protocol	sg-111112 222233333	*health check*	Permite tráfego de entrada do Network Load Balancer na porta de verificação de integridade

Saída

Protocolo	Destino	Intervalo de portas	Comment
Todos	Qualquer lugar	Any	Permite todo o tráfego de saída

Atualizar os grupos de segurança associados

Se você tiver associado pelo menos um grupo de segurança a um Network Load Balancer ao criá-lo, poderá atualizar os grupos de segurança desse Network Load Balancer a qualquer momento.

Console

Para atualizar os grupos de segurança

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione o Network Load Balancer.
4. Na guia Segurança, escolha Editar.
5. Para associar um grupo de segurança ao seu Network Load Balancer, selecione-o. Para remover um grupo de segurança do seu Network Load Balancer, desmarque-o.
6. Escolha Salvar alterações.

AWS CLI

Para atualizar os grupos de segurança

Use o comando set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --security-groups sg-1234567890abcdef0 sg-0abcdef0123456789
```

CloudFormation

Para atualizar os grupos de segurança

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
        - !Ref myNewSecurityGroup
```

Atualizar as configurações de segurança

Por padrão, aplicamos as regras do grupo de segurança de entrada a todo o tráfego enviado ao Network Load Balancer. No entanto, talvez você não queira aplicar essas regras ao tráfego enviado ao Network Load Balancer por meio do Network Load Balancer AWS PrivateLink, que pode ser originado da sobreposição de endereços IP. Nesse caso, você pode configurar o Network Load Balancer para que não apliquemos as regras de entrada para o tráfego enviado ao Network Load Balancer por meio de. AWS PrivateLink

Console

Para atualizar as configurações de segurança

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione o Network Load Balancer.
4. Na guia Segurança, escolha Editar.
5. Em Configuração de segurança, desmarque Aplicar regras de entrada no tráfego. PrivateLink
6. Escolha Salvar alterações.

AWS CLI

Para atualizar as configurações de segurança

Use o comando set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --enforce-security-group-inbound-rules-on-private-link-traffic off
```

CloudFormation

Para atualizar as configurações de segurança

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      EnforceSecurityGroupInboundRulesOnPrivateLinkTraffic: off
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
```

```
    SecurityGroups:
      - !Ref mySecurityGroup
```

Monitorar grupos de segurança do Network Load Balancer

Use as `SecurityGroupBlockedFlowCount_Outbound` CloudWatch métricas `SecurityGroupBlockedFlowCount_Inbound` e para monitorar a contagem de fluxos bloqueados pelos grupos de segurança do Network Load Balancer. O tráfego bloqueado não é refletido em outras métricas. Para obter mais informações, consulte the section called “CloudWatch métricas”.

Use os logs de fluxo da VPC para monitorar o tráfego aceito ou rejeitado pelos grupos de segurança do Network Load Balancer. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário da Amazon VPC.

Marcar um Network Load Balancer.

As tags ajudam você a categorizar os Network Load Balancers de maneiras diferentes. Por exemplo, você pode marcar um recurso por finalidade, proprietário ou ambiente.

Você pode adicionar várias tags para cada Network Load Balancer. Se você adicionar uma tag com uma chave que já está associada ao Network Load Balancer, o valor dessa tag será atualizado.

Após terminar de usar uma tag, você poderá removê-la do seu Network Load Balancer.

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 os valores de marcas 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 nos nomes ou valores de suas tags porque ele está reservado para AWS uso. 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.

Console

Para atualizar as tags para um balanceador de carga

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Marque a caixa de seleção para o Network Load Balancer.
4. Na guia Tags, selecione Gerenciar tags.
5. Para adicionar uma tag, escolha Adicionar tag, e insira a chave e o valor da tag. Os caracteres permitidos são letras, espaços, números (em UTF-8) e os seguintes caracteres especiais: + - = . _ : / @. Não use espaços no início nem no fim. Os valores de tags diferenciam maiúsculas de minúsculas.
6. Para atualizar uma tag, insira novos valores em Chave ou Valor.
7. Para excluir uma tag, escolha Remover ao lado da tag.
8. Escolha Salvar alterações.

AWS CLI

Como adicionar tags do

Use o comando add-tags. O exemplo a seguir adiciona duas tags.

```
aws elbv2 add-tags \
    --resource-arns load-balancer-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Como remover tags

Use o comando remove-tags. O exemplo a seguir remove as tags com as chaves especificadas.

```
aws elbv2 remove-tags \
    --resource-arns load-balancer-arn \
    --tag-keys project department
```

CloudFormation

Como adicionar tags do

Defina um recurso do tipo AWS::ElasticLoadBalancingV2::LoadBalancerrecurso para incluir a `Tags` propriedade.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Excluir um Network Load Balancer

Assim que o Network Load Balancer é disponibilizado, é será cobrado por cada hora ou hora parcial em que mantê-lo em execução. Quando não precisar mais do Network Load Balancer, você poderá excluí-lo. Assim que o Network Load Balancer for excluído, a cobrança será interrompida.

Não será possível excluir um Network Load Balancer se a proteção contra exclusão estiver habilitada. Para obter mais informações, consulte Deletion protection (Proteção contra exclusão).

Não será possível excluir um Network Load Balancer se ele estiver sendo usado por outro serviço. Por exemplo, se o Network Load Balancer estiver associado a um serviço de endpoint da VPC, será necessário excluir a configuração do serviço de endpoint antes de excluir o Network Load Balancer associado.

A exclusão de um Network Load Balancer também exclui seus receptores. A exclusão de um Network Load Balancer não afeta seus destinos registrados. Por exemplo, suas EC2 instâncias continuam em execução e ainda estão registradas em seus grupos-alvo. Para excluir seus grupos de destino, consulte Excluir um grupo de destino para o Network Load Balancer.

Console

Para excluir um Network Load Balancer

1. Se você tiver um registro DNS para seu domínio que aponte para o Network Load Balancer, aponte-o para um novo local e aguarde até que a mudança de DNS entre em vigor antes de excluir o Network Load Balancer. Por exemplo:
   - Se o registro for um registro CNAME com Time-To-Live (TTL) de 300 segundos, aguarde pelo menos 300 segundos antes de seguir para a próxima etapa.
   - Se o registro for um registro de alias (A) do Route 53, aguarde pelo menos 60 segundos.
   - Se você estiver usando o Route 53, a alteração do registro levará 60 segundos para se propagar para todos os servidores globais de nome do Route 53. Adicione esse tempo ao valor do TTL do registro que está sendo atualizado.
2. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, selecione Load Balancers.
4. Marque a caixa de seleção para o Network Load Balancer.
5. Escolha Ações, Excluir balanceador de carga.
6. Quando a confirmação for solicitada, insira **`confirm`** e escolha Excluir.

AWS CLI

Para excluir um Network Load Balancer

Use o comando delete-load-balancer.

```
aws elbv2 delete-load-balancer \
    --load-balancer-arn load-balancer-arn
```

Visualizar o mapa de recursos do Network Load Balancer

O mapa de recursos do Network Load Balancer fornece uma exibição interativa da arquitetura dos Network Load Balancers, incluindo seus receptores, grupos de destino e destinos associados. O mapa de recursos também destaca os relacionamentos e os caminhos de roteamento entre todos os recursos, produzindo uma representação visual da configuração dos Network Load Balancers.

Para exibir o mapa de recursos para o balanceador de carga

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Balanceador de carga.
3. Selecione o Network Load Balancer.
4. Escolha a guia Mapa de recursos.

Componentes do mapa de recursos

Visualizações do mapa

Há duas visualizações disponíveis no mapa de recursos do Network Load Balancer: Visão geral e Mapa de destinos não íntegros. A opção Visão geral é selecionada por padrão e exibe todos os recursos do seu Network Load Balancer. Selecionar a visualização Mapa de destinos não íntegros exibirá somente os destinos não íntegros e os recursos associados a eles.

A exibição Mapa de destino não íntegro pode ser usada para solucionar problemas de destinos que estão falhando nas verificações de integridade. Para obter mais informações, consulte Solucionar problemas de destinos não íntegros usando o mapa de recursos.

Colunas de recursos

O mapa de recursos do Network Load Balancer contém três colunas de recursos, uma para cada tipo de recurso. Os grupos de recursos são Receptores, Grupos de destino e Destinos.

Títulos de recursos

Cada recurso em uma coluna tem seu próprio bloco, que exibe detalhes sobre esse recurso específico.

- Passar o mouse sobre um bloco de recursos destaca as relações entre ele e outros recursos.
- A seleção de um bloco de recursos destaca as relações entre ele e outros recursos e exibe detalhes adicionais sobre esse recurso.
  - Resumo de integridade do grupo de destino: o número de destinos registrados para cada estado de integridade.
  - Status de integridade do destino: o status de integridade atual e a descrição do destino.

> **Note**
>
> É possível desativar Mostrar detalhes do recurso para ocultar detalhes adicionais no mapa de recursos.

- Cada bloco de recursos contém um link que, quando selecionado, navega até a página de detalhes desse recurso.
  - Receptores: selecione protocol:port dos receptores. Por exemplo, `TCP:80`.
  - Grupos de destino: selecione o nome do grupo de destino. Por exemplo, `my-target-group`.
  - Destinos: selecione o ID dos destinos. Por exemplo, `i-1234567890abcdef0`.

Exportar o mapa de recursos

Selecionar Exportar oferece a você a opção de exportar a visualização atual do mapa de recursos do seu Network Load Balancer como PDF.

CloudWatch registros para seu Network Load Balancer

O Amazon CloudWatch Logs oferece suporte aos logs de acesso do Network Load Balancer como registros vendidos, melhorando a observabilidade e simplificando a depuração de padrões de tráfego de rede. Você pode analisar os registros de acesso do Network Load Balancer diretamente CloudWatch para obter informações sobre as conexões dos clientes, a distribuição do tráfego e o status da conexão, ajudando você a identificar e solucionar problemas de rede com mais rapidez.

Você pode configurar a entrega de logs de acesso do Network Load Balancer para Amazon CloudWatch Logs, Amazon Data Firehose e Amazon Simple Storage Service (Amazon S3) com suporte para o formato Apache Parquet.

> **Important**
>
> Os logs de acesso serão criados somente se o load balancer tiver um receptor TLS e os logs contiverem somente informações sobre solicitações TLS. Os logs de acesso registram as solicitações com base no melhor esforço. Recomendamos que você use logs de acesso para compreender a natureza das solicitações, não como uma contabilidade completa de todas as solicitações.

> **Important**
>
> Os logs de acesso “legados” tradicionais permanecem disponíveis para o Network Load Balancer. Para gerenciar as configurações dos logs de acesso legados, acesse a guia Atributos do balanceador de carga. Para obter mais informações sobre os logs de acesso “legados”, consulte Logs de acesso do Network Load Balancer.

Com essa integração do CloudWatch Logs, você pode rastrear padrões de acesso detalhados usando consultas do CloudWatch Logs Insights, criar filtros métricos para monitoramento e revisar padrões de tráfego em tempo real usando o Live Tail.

Você pode ativar CloudWatch os registros para registros de acesso ao Network Load Balancer na guia Integrações do balanceador de carga no console. Para habilitar o registro em log, você deve estar registrado como usuário com certas permissões. Além disso, você deve conceder permissões AWS para permitir que os registros sejam enviados.

Para obter as permissões necessárias para cada destino de registro, consulte Habilitar o registro a partir de AWS serviços.

Para obter mais informações, consulte O que é o Amazon CloudWatch Logs? .

Para obter informações sobre preços, consulte Amazon CloudWatch Pricing.

Mudança de zona para o Network Load Balancer

A mudança de zona é um recurso do Controlador de Recuperação de Aplicações (ARC) da Amazon. Com a mudança de zona, você pode retirar um recurso de Network Load Balancer de uma zona de disponibilidade prejudicada com uma única ação. Dessa forma, é possível continuar a operar em outras zonas de disponibilidade íntegras em uma Região da AWS.

Quando você inicia uma mudança de zona, o Network Load Balancer para de rotear tráfego para os destinos na zona de disponibilidade afetada. As conexões existentes com os destinos na zona de disponibilidade afetada não são encerradas pela mudança de zona. Pode levar vários minutos para que essas conexões sejam concluídas normalmente.

Conteúdo

- Substituição administrativa de mudança de zona
- Habilitar mudança de zona para o Network Load Balancer
- Iniciar uma mudança de zona para o Network Load Balancer
- Atualizar uma mudança de zona para o Network Load Balancer
- Cancelar uma mudança de zona para o Network Load Balancer

Antes de começar uma mudança de zona

- A mudança de zona é desabilitada por padrão e deve ser habilitada em cada Network Load Balancer. Para obter mais informações, consulte Habilitar mudança de zona para o Network Load Balancer.
- Você pode iniciar uma mudança de zona para um Network Load Balancer específico somente para uma única zona de disponibilidade. Você não pode iniciar uma mudança de zona para várias zonas de disponibilidade.
- AWS remove proativamente os endereços IP zonais do Network Load Balancer do DNS quando vários problemas de infraestrutura afetam os serviços. Antes de iniciar uma mudança de zona, sempre verifique a capacidade atual da zona de disponibilidade. Se você usar uma mudança de zona no Network Load Balancer, a zona de disponibilidade afetada pela mudança de zona também perderá a capacidade de destino.
- Durante a mudança de zona nos Network Load Balancers com o balanceamento de carga entre zonas habilitado, os endereços IP do balanceador de carga de zona são removidos do DNS. As conexões existentes com destinos na zona de disponibilidade comprometida persistem até serem fechadas organicamente, enquanto as novas conexões não são mais roteadas para alvos na zona de disponibilidade comprometida.

Para obter mais informações, consulte Práticas recomendadas para mudanças de zona no ARC no Guia do desenvolvedor do Amazon Application Recovery Controller (ARC).

Substituição administrativa de mudança de zona

Os destinos que pertencem a um Network Load Balancer incluirão um novo status `AdministrativeOverride`, que é independente do estado `TargetHealth`.

Quando uma mudança de zona é iniciada para um Network Load Balancer, todos os destinos dentro da zona da qual os recursos estão sendo deslocados são considerados administrativamente

substituídos. O Network Load Balancer interrompe o roteamento de novos tráfegos para destinos substituídos administrativamente. As conexões existentes permanecem intactas até serem fechadas organicamente.

Os estados `AdministrativeOverride` possíveis são:

unknown

O estado não pode ser propagado devido a um erro interno

no_override

Nenhuma substituição está ativa no momento no destino

zonal_shift_active

A mudança de zona está ativa na zona de disponibilidade de destino

zonal_shift_delegated_para_dns

O estado de mudança zonal desse alvo não está disponível, `DescribeTargetHealth` mas pode ser visualizado diretamente por meio da AWS ARC - Zonal Shift API ou do console.

Habilitar mudança de zona para o Network Load Balancer

A mudança de zona é desabilitada por padrão e deve ser habilitada em cada Network Load Balancer. Isso garante que você possa iniciar uma mudança de zona usando somente os Network Load Balancers específicos que você deseja. Para obter mais informações, consulte the section called “Mudança de zona”.

Pré-requisitos

Se você habilitar o balanceamento de carga entre zonas para o balanceador de carga, cada grupo de destino vinculado ao balanceador de carga deverá atender aos seguintes requisitos antes de você habilitar a mudança de zona.

- O protocolo do grupo de destino deve ser `TCP` ou `TLS`.
- O tipo de grupo de destino não deve ser `alb`.
- Encerramento da conexão para destinos não íntegros deve ser desabilitado.
- O atributo do grupo de destino `load_balancing.cross_zone.enabled` deve ser `true` ou `use_load_balancer_configuration` (padrão).

Console

Para habilitar a mudança de zona

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione o Network Load Balancer.
4. Na guia Atributos, escolha Editar.
5. Em Configuração de roteamento da zona de disponibilidade, para Integração de mudança de zona do ARC selecione Habilitar.
6. Escolha Salvar alterações.

AWS CLI

Para habilitar a mudança de zona

Use o comando modify-load-balancer-attributes com o atributo `zonal_shift.config.enabled`.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=zonal_shift.config.enabled,Value=true"
```

CloudFormation

Para habilitar a mudança de zona

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso para incluir o `zonal_shift.config.enabled` atributo.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
```

```
      - !Ref subnet-AZ2
    SecurityGroups:
      - !Ref mySecurityGroup
    LoadBalancerAttributes:
      -Key: "zonal_shift.config.enabled"
       Value: "true"
```

Iniciar uma mudança de zona para o Network Load Balancer

A mudança zonal no ARC permite que você mova temporariamente o tráfego dos recursos suportados para fora de uma zona de disponibilidade, para que seu aplicativo possa continuar operando normalmente com outras zonas de disponibilidade em uma AWS região.

Pré-requisito

Antes de começar, verifique se você ativou a mudança de zona para o balanceador de carga.

Console

Este procedimento explica como iniciar uma mudança de zona usando o EC2 console da Amazon. Para verificar as etapas de como iniciar uma mudança de zona usando o console do ARC, consulte Starting a zonal shift no Guia do desenvolvedor do Amazon Application Recovery Controller (ARC).

Como iniciar uma mudança de zona

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione o Network Load Balancer.
4. Na guia Integrações, expanda Amazon Application Recovery Controller (ARC) e escolha Iniciar mudança de zona.
5. Selecione a zona de disponibilidade da qual você deseja remover o tráfego.
6. Escolha ou insira uma data de validade para a mudança de zona. Inicialmente, uma mudança de zona pode ser definida entre 1 minuto e 3 dias (72 horas).

   Todas as mudanças de zona são temporárias. Você deve definir uma validade, mas pode atualizar mudanças ativas posteriormente para definir uma nova validade.

7. Insira um comentário. Você pode atualizar a mudança de zona posteriormente para editar o comentário.
8. Marque a caixa de seleção para confirmar que iniciar uma mudança de zona reduz a capacidade da sua aplicação ao afastar o tráfego da zona de disponibilidade.
9. Escolha Confirmar.

AWS CLI

Como iniciar uma mudança de zona

Use o start-zonal-shiftcomando Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift start-zonal-shift \
    --resource-identifier load-balancer-arn \
    --away-from use2-az2 \
    --expires-in 2h \
    --comment "zonal shift due to scheduled maintenance"
```

Atualizar uma mudança de zona para o Network Load Balancer

Você pode atualizar uma mudança de zona para definir uma nova expiração, editar ou substituir o comentário pela mudança de zona.

Console

Este procedimento explica como atualizar uma mudança de zona usando o EC2 console da Amazon. Para verificar as etapas de como atualizar uma mudança de zona usando o console do Amazon Application Recovery Controller (ARC), consulte Updating a zonal shift no Guia do desenvolvedor do Amazon Application Recovery Controller (ARC).

Como atualizar uma mudança de zona

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione um Application Load Balancer com uma mudança de zona ativa.
4. Na guia Integrações, expanda Amazon Application Recovery Controller (ARC) e escolha Atualizar mudança de zona.

Essa ação abre o console do ARC para continuar o processo de atualização.

5. (Opcional) Em Definir expiração da mudança de zona selecione ou insira uma expiração.
6. (Opcional) Em Comentário, opcionalmente, edite o comentário existente ou insira um novo.
7. Selecione Atualizar.

AWS CLI

Como atualizar uma mudança de zona

Use o update-zonal-shiftcomando Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift update-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE \
    --expires-in 1h \
    --comment "extending zonal shift for scheduled maintenance"
```

Cancelar uma mudança de zona para o Network Load Balancer

Você pode cancelar uma mudança de zona a qualquer momento antes que ela expire. Você pode cancelar os turnos zonais que você inicia ou os turnos zonais que AWS começam para um recurso para uma execução prática de mudança automática zonal.

Console

Esse procedimento explica como cancelar uma mudança de zona usando o EC2 console da Amazon. Para verificar as etapas de como cancelar uma mudança de zona usando o console do Amazon Application Recovery Controller (ARC), consulte Canceling a zonal shift no Guia do desenvolvedor do Amazon Application Recovery Controller (ARC).

Como cancelar uma mudança de zona

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione um Network Load Balancer que tenha uma mudança de zona ativa.
4. Na guia Integrações, em Amazon Application Recovery Controller (ARC), escolha Cancelar mudança de zona.

Essa ação abre o console do ARC para continuar o processo de cancelamento.

5. Escolha Cancelar mudança de zona.
6. Quando a confirmação for solicitada, escolha Confirmar.

AWS CLI

Como cancelar uma mudança de zona

Use o cancel-zonal-shiftcomando Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift cancel-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE
```

Reservas de capacidade para seu Network Load Balancer

As reservas da Unidade de Capacidade do Balanceador de Carga (LCU) permitem que você reserve uma capacidade estática mínima para seu balanceador de carga. Os Network Load Balancers escalam automaticamente para oferecer suporte às workloads detectadas e atender às necessidades de capacidade. Quando a capacidade mínima é configurada, seu balanceador de carga continua aumentando ou diminuindo a escala com base no tráfego recebido, mas também evita que a capacidade fique abaixo da capacidade mínima configurada.

Considere usar a reserva da LCU nas seguintes situações:

- Você tem um evento próximo com um tráfego repentino e incomum e deseja garantir que seu balanceador de carga ofereça suporte ao aumento repentino de tráfego durante o evento.
- Você tem picos de tráfego imprevisíveis devido à natureza da sua workload por um curto período.
- Você está configurando seu balanceador de carga para integrar ou migrar seus serviços em um horário de início específico e precisa começar com uma alta capacidade em vez de esperar que o ajuste de escala automático entre em funcionamento.
- Você está migrando workloads entre balanceadores de carga e deseja configurar o destino de acordo com a escala da origem.

Estime a capacidade de que você precisa

Quando estiver determinando a quantidade de capacidade que você deve reservar para seu balanceador de carga, recomendamos que você realize testes de carga ou revise dados históricos da workload que representem o tráfego futuro que você espera. Você pode estimar quanta capacidade precisa reservar com base no tráfego analisado usando o console do Elastic Load Balancing.

Como alternativa, você pode consultar a CloudWatch métrica ProcessedBytespara determinar o nível correto de capacidade. A capacidade do seu balanceador de carga é reservada em LCUs, com cada LCU sendo igual a 2,2 Mbps. Você pode usar a métrica Max (ProcessedBytes) para ver o tráfego máximo de taxa de transferência por minuto no balanceador de carga e, em seguida, converter essa taxa de transferência em uma taxa de conversão de 2,2 LCUs Mbps igual a 1 LCU.

Caso você não tenha dados históricos da workload para referenciar e não possa realizar o teste de carga, você pode estimar a capacidade necessária usando a calculadora de reservas da LCU. A calculadora de reservas da LCU usa dados com base nas cargas de trabalho históricas AWS observadas e pode não representar sua carga de trabalho específica. Para obter mais informações, consulte Calculadora de reserva de unidades de capacidade do balanceador de carga.

Regiões aceitas

Este atributo está disponível apenas nas seguintes regiões:

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (Oregon)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)
- Ásia-Pacífico (Tóquio)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Estocolmo)

Valores mínimos e máximos para uma reserva de LCU

O total da solicitação de reserva deve ser de pelo menos 2.750 LCU por zona de disponibilidade. O valor máximo é determinado pelas cotas da sua conta. Para obter mais informações, consulte the section called “Unidades de capacidade do balanceador de carga”.

Solicitar reserva de unidades de capacidade do balanceador de carga para o Network Load Balancer

Antes de usar a reserva de LCU, analise o seguinte:

- A reserva de LCU não é compatível em Network Load Balancers que usam receptores TLS.
- A reserva de LCU é compatível somente com a reserva de capacidade de throughput para Network Load Balancers. Ao solicitar uma reserva de LCU, converta suas necessidades de capacidade de Mbps para LCUs usar a taxa de conversão de 1 LCU para 2,2 Mbps.
- A capacidade é reservada em nível regional e distribuída de forma igualitária nas zonas de disponibilidade. Confirme se você tem metas distribuídas uniformemente suficientes em cada zona de disponibilidade antes de ativar a reserva de LCU.
- As solicitações de reserva de LCU são atendidas por ordem de chegada e dependem da capacidade disponível para uma zona naquele momento. A maioria das solicitações geralmente é atendida em uma hora, mas também pode levar algumas horas.
- Para atualizar uma reserva existente, a solicitação anterior deve ser provisionada ou falhar. Você pode aumentar a capacidade reservada quantas vezes precisar, mas só pode diminuir a capacidade reservada duas vezes por dia.
- Você continuará incorrendo em cobranças por qualquer capacidade reservada ou provisionada até que ela seja encerrada ou cancelada.

Console

Para solicitar uma reserva de LCU

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Balanceador de carga.
3. Selecione o nome do balanceador de carga.
4. Na guia Capacidade, selecione Editar reserva de LCU.
5. Selecione Estimativa baseada em referência histórica.
6. Selecione o período de referência para ver o nível recomendado de LCU reservada.

7. Se você não tiver uma carga de trabalho de referência histórica, poderá escolher Estimativa manual e inserir o número de LCUs a serem reservadas.
8. Escolha Salvar.

AWS CLI

Para solicitar uma reserva de LCU

Use o comando modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --minimum-load-balancer-capacity CapacityUnits=3000
```

CloudFormation

Para solicitar uma reserva de LCU

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-alb
      Type: application
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      MinimumLoadBalancerCapacity:
        CapacityUnits: 3000
```

Atualizar ou cancelar reservas de unidades de capacidade do balanceador de carga para seu Network Load Balancer

Se os padrões de tráfego do seu balanceador de carga mudarem, você poderá atualizar ou cancelar a reserva de LCU para seu balanceador de carga.

Console

Para atualizar ou cancelar uma reserva da LCU

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Balanceador de carga.
3. Selecione o nome do balanceador de carga.
4. Na guia Capacidade, faça o seguinte:
   a. Para atualizar a reserva da LCU, selecione Editar reserva da LCU.
   b. Para cancelar a reserva da LCU, selecione Cancelar capacidade.

AWS CLI

Para cancelar uma reserva da LCU

Use o comando modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --reset-capacity-reservation
```

Monitorar a reserva de unidades de capacidade do balanceador de carga para o Network Load Balancer

Status de reserva

Os seguintes são os valores de status possíveis para uma reserva da LCU:

- `pending`: indica a reserva que está em processo de provisionamento.
- `provisioned`: indica que a capacidade reservada está pronta e disponível para uso.
- `failed`: indica que a solicitação não pode ser concluída no momento.
- `rebalancing`: indica que uma zona de disponibilidade foi adicionada ou removida e que o balanceador de carga está reequilibrando a capacidade.

Utilização da LCU

Para definir a utilização reservada da LCU, você pode comparar a métrica `ProcessedBytes` por minuto com `Sum(ReservedLCUs)` por hora. Para converter bytes por minuto em LCU por hora, use (bytes por minuto) *8/60/(10^6)/2,2.

Console

Para visualizar o status de uma reserva de LCU

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Balanceador de carga.
3. Selecione o nome do balanceador de carga.
4. Na guia Capacidade, é possível visualizar o Status da reserva e o valor da LCU reservada.

AWS CLI

Para monitorar o status de uma reserva de LCU

Use o comando describe-capacity-reservation.

```
aws elbv2 describe-capacity-reservation \
    --load-balancer-arn load-balancer-arn
```

Receptores para Network Load Balancers

Um receptor é um processo que verifica solicitações de conexão, usando o protocolo e a porta que você configura. Antes de começar a usar o Network Load Balancer, você deve adicionar ao menos um receptor. Se o balanceador de carga não tiver receptores, não poderá receber tráfego de clientes. As regras que você define para um receptor determinam como o balanceador de carga roteia solicitações para os destinos registrados, como instâncias do EC2.

Conteúdo

Configuração do receptor

Os listeners são compatíveis com os seguintes protocolos e portas:

- Protocolos: TCP, TLS, UDP, TCP_UDP, QUIC, TCP_QUIC
- Ports (Portas): 1-65535

Você pode usar um listener TLS para transferir o trabalho de criptografia e descriptografia para seu load balancer, de forma que os aplicativos possam se concentrar na respectiva lógica de negócios. Se o protocolo do receptor for TLS, você deverá implantar pelo menos um certificado de servidor SSL no receptor. Para obter mais informações, consulte Certificados de servidor.

Se você precisar garantir que os destinos descriptografem o tráfego TLS em vez do balanceador de carga, será possível criar um receptor TCP na porta 443 em vez de criar um receptor TLS. Com um receptor TCP, o balanceador de carga transmite o tráfego criptografado para os destinos sem descriptografá-lo.

Você pode usar um receptor QUIC para aceitar o tráfego QUIC. O Network Load Balancer atua como um balanceador de carga de passagem de acordo com a RFC9000. Use um receptor QUIC e backends habilitados para QUIC para permitir uma migração de conexão perfeita para dispositivos móveis.

Para oferecer suporte a TCP e UDP na mesma porta, crie um listener TCP_UDP. Os grupos de destino de um listener TCP_UDP devem usar o protocolo TCP_UDP.

Para oferecer suporte a TCP e QUIC na mesma porta, crie um receptor TCP_QUIC. Os grupos de destino de um receptor TCP_QUIC devem usar o protocolo TCP_QUIC.

Um receptor UDP para um balanceador de carga de pilha dupla requer grupos de destino IPv6.

WebSockets é suportado somente em ouvintes TCP, TLS, TCP_UDP e TCP_QUIC.

O tráfego QUIC não oferece suporte à negociação de versões. QUIC v1 é a única versão compatível com o QUIC.

Todo o tráfego de rede enviado para um listener configurado é classificado como tráfego intencional. O tráfego de rede que não corresponde a um listener configurado é classificado como tráfego não intencional. Solicitações ICMP diferentes do Tipo 3 também são consideradas tráfego não intencional. Os Network Load Balancers eliminam o tráfego não intencional sem encaminhá-lo para quaisquer destinos. Os pacotes de dados TCP enviados para a porta de um configurado que não são novas conexões ou parte de uma conexão TCP ativa são rejeitados com uma redefinição de TCP (RST).

Para obter mais informações, consulte Roteamento de solicitação no Guia do usuário do Elastic Load Balancing.

Ações padrão

Quando você cria um receptor, você especifica uma ação padrão para rotear as solicitações. A ação padrão encaminha as solicitações para os grupos de destino que você especificar.

Distribuir tráfego para vários grupos de destino

Se você especificar vários grupos de destino para uma ação padrão, as solicitações serão distribuídas para esses grupos de destino com base nos respectivos pesos relativos. Você deve especificar um peso de 0 a 999 para cada grupo de destino. Um grupo de destino com peso 0 não recebe tráfego. Após adicionar um grupo de destino ou atualizar os pesos do grupo de destino, as novas conexões são roteadas com base nos novos pesos do grupo de destino. As conexões atuais não são afetadas e continuam até serem encerradas normalmente.

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 com peso de 10.

Um caso de uso comum é migrar o tráfego de um grupo de destino para outro. Isso significa que você aumenta gradualmente o peso do novo grupo de destino enquanto diminui o peso do grupo de destino original até que seja 0. Se você atualizar o peso de um grupo de destino como 0, após um curto período ele não receberá novas conexões e as conexões existentes serão encerradas.

Sessões persistentes e grupos de destino ponderados

As ações de encaminhamento executadas nos receptores podem especificar se a persistência do grupo de destino deve ser habilitada. Quando habilitada, a persistência do grupo de destino faz com que as conexões subsequentes do mesmo endereço IP de origem prefiram o grupo de destino escolhido anteriormente.

Considerações

- No caso de receptores TLS, não é possível adicionar grupos de destino TCP e grupos de destino TLS à regra do receptor. Todos os grupos de destino devem usar o mesmo protocolo.
- No caso de receptores TLS, a persistência do grupo de destino não é compatível.
- Quanto a balanceadores de carga de pilha dupla, não é possível adicionar grupos de destino IPv4 e grupos de destino IPv6 à mesma ação padrão. Todos os grupos de destino na ação padrão devem usar o mesmo tipo de endereço IP.
- No caso de receptores, se uma ação de encaminhamento contiver vários grupos de destino e qualquer um deles tiver a persistência habilitada, a ação de encaminhamento também deverá ter a persistência do grupo de destino habilitada.

Atributos do receptor

Os atributos de receptor para Network Load Balancers são:

`tcp.idle_timeout.seconds`

O valor de tempo limite de inatividade de TCP, em segundos. O intervalo válido é de 60-6.000 segundos. O padrão é 350 segundos.

Para obter mais informações, consulte Atualizar o tempo limite de inatividade.

Receptores seguros

Para usar um listener TLS, é necessário implantar pelo menos um certificado de servidor no load balancer. O load balancer usa um certificado de servidor para encerrar a conexão de frontend e para descriptografar solicitações dos clientes antes de enviá-las aos destinos. Observe que, se você precisar transmitir tráfego criptografado para os destinos sem que o balanceador de carga o descriptografe, crie um receptor TCP na porta 443 em vez de criar um receptor TLS. O balanceador de carga transmite a solicitação para o destino no estado em que ela se encontra, sem descriptografá-la.

O Elastic Load Balancing usa uma configuração de negociação TLS, conhecida como política de segurança, para negociar conexões TLS entre um cliente e o balanceador de carga. Uma política de segurança é uma combinação de cifras e protocolos. O protocolo estabelece uma conexão segura entre um cliente e um servidor, além de garantir que todos os dados transmitidos entre o cliente e o balanceador de carga sejam privados. A cifra é um algoritmo criptográfico que usa chaves de criptografia para criar uma mensagem codificada. Os protocolos usam várias cifras para criptografar dados na internet. Durante o processo de negociação de conexão, o cliente e o load balancer apresentam uma lista de cifras e protocolos que cada um suporta, em ordem de preferência. A primeira cifra na lista do servidor que corresponder a qualquer uma das cifras do cliente será selecionada para a conexão segura.

Os Network Load Balancers não são compatíveis com autenticação TLS mútua (mTLS). Para compatibilidade com mTLS, crie um receptor TCP em vez de um receptor TLS. O balanceador de carga transmite a solicitação no estado em que ela se encontra para que você possa implementar a mTLS no destino.

Os Network Load Balancers são compatíveis com a retomada de TLS usando PSK para TLS 1.3 e tíquetes de sessão para TLS 1.2 e anteriores. Não há suporte para retomadas com ID de sessão ou quando vários certificados são configurados no receptor usando SNI. O atributo de dados 0-RTT e a extensão early_data não estão implementados.

Para demonstrações relacionadas, consulte Suporte TLS no Network Load Balancer e Suporte SNI no Network Load Balancer.

Políticas ALPN

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

Quando o cliente inicia uma conexão ALPN, o load balancer compara a lista de preferências de ALPN do cliente com a política ALPN. Se o cliente oferecer suporte a um protocolo da política ALPN, o load balancer estabelecerá a conexão com base na lista de preferências da política ALPN. Caso contrário, o load balancer não usará ALPN.

Políticas ALPN com suporte

Veja a seguir as políticas ALPN com suporte:

`HTTP1Only`

Negocie somente HTTP/1 .*. A lista de preferências do ALPN é http/1 0,1, http/1 0,0.

`HTTP2Only`

Negocie apenas HTTP/2. A lista de preferências de ALPN é h2.

`HTTP2Optional`

Prefira HTTP/1 .* em vez de HTTP/2 (o que pode ser útil para HTTP/2 testes). A lista de preferências do ALPN é http/1 .1, http/1 .0, h2.

`HTTP2Preferred`

Prefiro HTTP/2 em vez de HTTP/1 .*. A lista de preferências do ALPN é h2, http/1 .1, .0. http/1

`None`

Não negocie ALPN. Esse é o padrão.

Habilitar conexões ALPN

É possível habilitar conexões ALPN ao criar ou modificar um listener TLS. Para obter mais informações, consulte Adicionar um listener e Atualizar a política ALPN.

Criar um receptor para o Network Load Balancer

Um listener é um processo que verifica se há solicitações de conexão. Você define um listener ao criar seu load balancer e você pode adicionar listeners ao seu load balancer a qualquer momento.

Pré-requisitos

- Você deve especificar um grupo de destino para a ação padrão. Para obter mais informações, consulte Criar um grupo de destino para o Network Load Balancer.
- É necessário especificar um certificado SSL para um listener TLS. O load balancer usará o certificado para encerrar a conexão e descriptografar solicitações dos clientes antes de roteá-las aos destinos. Para obter mais informações, consulte Certificados de servidor para seu Network Load Balancer.
- Você não pode usar um grupo de destino IPv4 com um receptor UDP para um balanceador de carga `dualstack`.
- Os receptores QUIC e TCP_QUIC não são permitidos em balanceadores de carga `dualstack` ou balanceadores de carga com grupos de segurança associados.
- Os receptores QUIC e TCP_QUIC não são permitidos em balanceadores de carga com grupos de segurança associados.
- Somente um receptor QUIC ou TCP_QUIC é permitido em um Network Load Balancer a qualquer momento.
- Os receptores QUIC e TCP_QUIC não são permitidos em um Network Load Balancer que tenha os receptores UDP ou TCP_UDP.

Adicionar um listener

Você configura um listener com um protocolo e uma porta para as conexões de clientes com o load balancer, e um grupo de destino para a regra do listener padrão. Para obter mais informações, consulte Configuração do receptor.

Console

Para adicionar um listener

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Selecione o nome do balanceador de carga para abrir a página de detalhes dele.
4. Na guia Receptores, escolha Adicionar receptor.
5. Em Protocolo, selecione TCP, UDP, TCP_UDP, TLS, QUIC ou TCP_QUIC. Mantenha a porta padrão ou digite uma porta diferente.
6. Em Ação padrão, selecione um grupo de destino para encaminhar o tráfego.

   Para adicionar outro grupo de destino, selecione Adicionar grupo de destino e atualize os pesos conforme necessário.

   Caso você não tenha um grupo de destino que responda às suas necessidades, escolha Criar grupo de destino para criar um agora. Para obter mais informações, consulte Criar um grupo de destino.
7. [Listeners TLS] Em Security policy (Política de segurança), é recomendável manter a política de segurança padrão.
8. [Ouvintes TLS] Em Certificado de SSL/TLS servidor padrão, escolha o certificado padrão. Você pode selecionar o certificado de uma das seguintes origens:

   - Se você criou ou importou um certificado usando AWS Certificate Manager, escolha Do ACM e escolha o certificado em Certificado (do ACM).
   - Se você tiver importado um certificado usando o IAM, selecione Do IAM e, em seguida, selecione o certificado em Certificado (do IAM).
   - Se você tiver um certificado, selecione Importar certificado. Selecione Importar para o ACM ou Importar para o IAM. Para a chave privada do certificado, copie e cole o conteúdo do arquivo de chave privada (PEM-encoded). Para Corpo do certificado, copie e cole o conteúdo do arquivo de certificado de chave pública (PEM-encoded). Para a cadeia de certificados, copie e cole o conteúdo do arquivo da cadeia de certificados (PEM-encoded), a menos que você esteja usando um certificado autoassinado e não seja importante que os navegadores aceitem implicitamente o certificado.
9. [Listeners TLS] Em Política ALPN, escolha uma política para habilitar ALPN ou escolha Nenhum para desabilitar ALPN. Para obter mais informações, consulte Políticas ALPN.

10. Para adicionar tags, expanda Tags de receptor (Opcional). Escolha Adicionar nova tag e insira a chave de tag e um valor para a tag.
11. Escolha Adicionar.
12. [Receptores TLS] Para adicionar certificados à lista de certificados opcionais, consulte Adicionar certificados à lista de certificados.

AWS CLI

Para criar um grupo de destino

Se você não tiver um grupo de destino para usar a ação padrão, use o comando create-target-group para criar um agora. Para obter exemplos, consulte Criar um grupo de destino.

Para adicionar um receptor TCP

Use o comando create-listener, especificando o protocolo TCP.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Para adicionar um receptor TCP com vários grupos de destino

Use o comando create-listener, especificando o protocolo TCP, os grupos de destino e os pesos.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
            ]
        }
    }]'
```

Para adicionar um receptor TLS

Use o comando create-listener, especificando o protocolo TLS.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TLS \
    --port 443 \
    --certificates CertificateArn=certificate-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Para adicionar um receptor UDP

Use o comando create-listener, especificando o protocolo UDP.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol UDP \
    --port 53 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Para adicionar um receptor QUIC

Use o comando create-listener, especificando o protocolo QUIC.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol QUIC \
    --port 443 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Para adicionar um receptor TCP

Defina um recurso do tipo AWS::ElasticLoadBalancingV2: :Listener usando o protocolo TCP.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
```

```
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Para adicionar um receptor TCP com vários grupos de destino

Defina um recurso do tipo AWS::ElasticLoadBalancingV2: :Listener usando o protocolo TCP.

```
Resources:
    myTCPListener:
        Type: 'AWS::ElasticLoadBalancingV2::Listener'
        Properties:
        LoadBalancerArn: !Ref myLoadBalancer
        Protocol: TCP
        Port: 80
        DefaultActions:
            - Type: forward
            ForwardConfig:
                TargetGroups:
                - TargetGroupArn: !Ref myTargetGroup1,
                    Weight: 10
                - TargetGroupArn: !Ref myTargetGroup2,
                    Weight: 30
            TargetGroupStickinessConfig:
                Enabled: true
```

Para adicionar um receptor TLS

Defina um recurso do tipo AWS::ElasticLoadBalancingV2: :Listener usando o protocolo TLS.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
```

```
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Para adicionar um receptor UDP

Defina um recurso do tipo AWS::ElasticLoadBalancingV2: :Listener usando o protocolo UDP.

```
Resources:
  myUDPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: UDP
      Port: 53
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Para adicionar um receptor QUIC

Defina um recurso do tipo AWS::ElasticLoadBalancingV2: :Listener usando o protocolo QUIC.

```
Resources:
  myQUICListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: QUIC
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Certificados de servidor para seu Network Load Balancer

Ao criar um receptor seguro para o Network Load Balancer, você deve implantar pelo menos um certificado no balanceador de carga. O balanceador de carga exige X.509 certificados (certificado

do servidor). Os certificados são uma forma digital de identificação emitida por uma autoridade certificadora (CA). Um certificado contém informações de identificação, período de validade, chave pública, número de série e a assinatura digital do emissor.

Quando você cria um certificado para uso com seu load balancer, é necessário especificar um nome de domínio. O nome de domínio no certificado deve corresponder ao registro de nome de domínio personalizado para que possamos verificar a conexão TLS. Se eles não coincidirem, o tráfego não será criptografado.

Você precisa especificar um nome de domínio totalmente qualificado (FQDN) para seu certificado, como `www.example.com` ou um nome de domínio de apex como `example.com`. Você também pode usar um asterisco (*) como um caractere curinga para proteger vários nomes de site no mesmo domínio. Quando você solicita um certificado-curinga, o asterisco (*) deve estar na posição mais à esquerda do nome do domínio e só pode proteger um nível de subdomínio. Por exemplo,`*.example.com` protege `corp.example.com` e `images.example.com`, mas não pode proteger `test.login.example.com`. Note também que `*.example.com` protege apenas os subdomínios de `example.com`, mas não protege o domínio vazio ou apex (`example.com`). O nome-curinga será exibido no campo Assunto e na extensão Nome alternativo do assunto do certificado. Para obter mais informações sobre certificados públicos, consulte Solicitação de um certificado público no Manual do usuário do AWS Certificate Manager .

Recomendamos que você crie certificados para seus balanceadores de carga usando o AWS Certificate Manager (ACM). O ACM se integra ao Elastic Load Balancing para que você possa implantar o certificado em seu balanceador de carga. Para obter mais informações, consulte o Guia do usuário do AWS Certificate Manager.

Como alternativa, você pode usar as ferramentas TLS para criar uma solicitação de assinatura de certificado (CSR) e, em seguida, obter a CSR assinada por uma CA para produzir um certificado e, em seguida, importar o certificado para o ACM ou fazer o upload do certificado no (IAM). AWS Identity and Access Management Para obter mais informações, consulte Importar certificados no Guia do usuário do AWS Certificate Manager ou Trabalhar com certificados de servidor no Guia do usuário do IAM.

Algoritmos de chave com suporte

- RSA de 1024 bits
- RSA de 2048 bits
- RSA de 3072 bits

- ECDSA de 256 bits
- ECDSA de 384 bits
- ECDSA de 521 bits

Importante — Comportamento ao usar IAM-imported certificados

Se você importar um certificado para o AWS Identity and Access Management (IAM) e anexá-lo a um ouvinte NLB TLS, o tamanho e o algoritmo da chave do certificado não serão validados no momento da anexação. A validação ocorre de forma assíncrona depois que o certificado é associado ao ouvinte. Se o certificado usar um tamanho de chave não suportado (por exemplo, RSA 4096 bits), o ouvinte entrará em um estado não funcional e você receberá uma notificação por meio do Personal Health Dashboard AWS (PHD).

Observe que, se seu ouvinte tiver um certificado em funcionamento anteriormente configurado, o tráfego poderá continuar sendo atendido por esse certificado enquanto o certificado não suportado for rejeitado. A notificação PHD indicará que o ouvinte está configurado com um certificado não suportado, mas não confirma se o tráfego ainda está sendo atendido por um certificado anterior.

Para evitar isso, verifique o tamanho da chave do seu certificado antes de importá-lo para o IAM. Para certificados RSA, o tamanho máximo de chave suportado para ouvintes NLB TLS é de 3072 bits.

Se você usar o AWS Certificate Manager (ACM) para provisionar ou importar certificados, tamanhos de chave não suportados serão rejeitados no momento da anexação, fornecendo feedback imediato.

Certificado padrão

Quando você cria um receptor TLS, é necessário especificar pelo menos um certificado. Esse certificado é conhecido como o certificado padrão. É possível substituir o certificado padrão depois de criar o listener TLS. Para obter mais informações, consulte Substituir o certificado padrão.

Se você especificar certificados adicionais em uma lista de certificados, o certificado padrão será usado somente se um cliente se conectar sem usar o protocolo Server Name Indication (SNI) para especificar um nome de host ou se não houver certificados correspondentes na lista de certificados.

Se você não especificar certificados adicionais, mas precisar hospedar vários aplicativos seguros por meio de um único load balancer, poderá usar um certificado curinga ou adicionar um Subject Alternative Name (SAN) para cada domínio adicional ao seu certificado.

Lista de certificados

Após criar um listener TLS, ele terá um certificado padrão e uma lista de certificados vazia. Você pode adicionar certificados à lista de certificados para o listener. O uso de uma lista de certificados permite que um load balancer ofereça suporte a vários domínios na mesma porta e forneça um certificado diferente para cada domínio. Para obter mais informações, consulte Adicionar certificados à lista de certificados.

O load balancer usa um algoritmo inteligente de seleção de certificado com suporte para SNI. Se o nome de host fornecido por um cliente corresponder a um único certificado na lista, o load balancer selecionará esse certificado. Se um nome de host fornecido por um cliente corresponder a vários certificados na lista, o load balancer selecionará o melhor certificado que o cliente puder comportar. A seleção do certificado se baseia nos critérios a seguir, na seguinte ordem:

- Algoritmo de chave pública (prefira ECDSA em relação a RSA)
- Algoritmo hashing (prefira SHA em relação a MD5)
- Comprimento da chave (prefira o maior)
- Período de validade

As entradas no log de acesso do load balancer indicam o hostname especificado pelo cliente e o certificado apresentado ao cliente. Para obter mais informações, consulte Entradas do log de acesso.

Renovação de certificado

Cada certificado vem com um período de validade. Você deve garantir que renovou ou substituiu os certificados do load balancer antes do fim do período de validade. Isso inclui o certificado padrão e os certificados em uma lista de certificados. Renovar ou substituir um certificado não afeta as solicitações em andamento recebidas por um nó do load balancer e são pendentes de roteamento para um destino íntegro. Depois de um certificado ser renovado, as novas solicitações usarão o certificado renovado. Depois de o certificado ser substituído, as novas solicitações usarão o novo certificado.

Você pode gerenciar a renovação e a substituição do certificado da seguinte forma:

- Os certificados fornecidos AWS Certificate Manager e implantados em seu balanceador de carga podem ser renovados automaticamente. O ACM tenta renovar os certificados antes que eles expirem. Para obter mais informações, consulte Renovação gerenciada no Guia do usuário do AWS Certificate Manager .

- Se você tiver importado um certificado no ACM, deverá monitorar a data de validade do certificado e renová-lo antes que expire. Para obter mais informações, consulte Importar certificados no Manual do usuário do AWS Certificate Manager .
- Se você tiver importado um certificado para o IAM, precisará criar um novo certificado, importá-lo para o ACM ou IAM, adicionar o novo certificado ao balanceador de carga e remover o certificado expirado do seu balanceador de carga.

Políticas de segurança para o Network Load Balancer

Ao criar um listener TLS, é necessário selecionar uma política de segurança. Uma política de segurança determina quais cifras e protocolos são aceitos nas negociações SSL entre seu balanceador de carga e um cliente. A política de segurança do seu balanceador de carga poderá ser atualizada se seus requisitos mudarem ou quando lançarmos uma nova política de segurança. Para obter mais informações, consulte Atualizar a política de segurança.

Considerações

- Um receptor TLS exige uma política de segurança. Caso você não especifique uma política de segurança ao criar o receptor, usaremos a política de segurança padrão. A política de segurança padrão depende de como você criou o receptor TLS:
  - Console: A política de segurança padrão é `ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09`.
  - Outros métodos (por exemplo, o AWS CLI AWS CloudFormation, e o AWS CDK) — A política de segurança padrão é`ELBSecurityPolicy-2016-08`.
- Políticas de segurança com PQ em seus nomes oferecem troca híbrida de chaves pós-quânticas. Para fins de compatibilidade, eles oferecem suporte a algoritmos de troca de ML-KEM chaves clássicos e pós-quânticos. Os clientes devem oferecer suporte à troca de ML-KEM chaves para usar o TLS pós-quântico híbrido para troca de chaves. As políticas híbridas pós-quânticas oferecem suporte aos algoritmos SECP256R1MLKEM768, SEcp384R1MLKEM1024 e X25519MLKEM768. Para obter mais informações, consulte Post-quantum Criptografia.
- A AWS recomenda implementar a nova política `ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09` de segurança pós-quântica baseada em TLS (PQ-TLS) ou. `ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09` Essa política garante compatibilidade com versões anteriores ao oferecer suporte a clientes capazes de negociar híbridos PQ-TLS, somente TLS 1.3 ou somente TLS 1.2, minimizando assim a interrupção do serviço durante a transição para a criptografia pós-quântica. Você pode migrar progressivamente para políticas de segurança mais restritivas à

medida que seus aplicativos cliente desenvolvem a capacidade de negociar operações de PQ-TLS troca de chaves.

- Você pode habilitar logs de acesso para obter informações sobre as solicitações de TLS enviadas ao Network Load Balancer, analisar padrões de tráfego TLS para gerenciar atualizações de políticas de segurança e solucionar problemas. Ative o registro de acesso para seu balanceador de carga e examine as entradas correspondentes do log de acesso. Para obter mais informações, consulte Logs de acesso e Consultas de exemplo do Network Load Balancer.
- Para visualizar a versão do protocolo TLS (posição 5 do campo de registro) e a troca de chaves (posição 13 do campo de registro) para solicitações de acesso ao seu balanceador de carga, ative o registro de acesso e examine as entradas de registro correspondentes. Para obter mais informações, consulte Logs de acesso.
- Você pode restringir quais políticas de segurança estão disponíveis para os usuários em todo o seu Contas da AWS e AWS Organizations usando as chaves de condição do Elastic Load Balancing em suas políticas de IAM e controle de serviço (SCPs), respectivamente. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia do usuário do AWS Organizations .
- As políticas que oferecem suporte somente ao TLS 1.3 oferecem suporte ao Forward Secrecy (FS). As políticas que oferecem suporte a TLS 1.3 e TLS 1.2 que têm somente cifras no formato TLS_* e ECDHE_* também fornecem FS.
- Os Network Load Balancers oferecem suporte à extensão Extended Master Secret (EMS) para TLS 1.2.

Conexões de back-end

Você pode escolher a política de segurança usada para conexões front-end, mas não para conexões backend. A política de segurança para conexões de back-end depende da política de segurança do ouvinte. Se algum de seus ouvintes estiver usando:

- Política de TLS pós-quântico FIPS - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09`
- Política FIPS - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`
- Post-quantum Política TLS - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-PQ-2025-09`
- Política TLS 1.3 - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-2021-06`

- Todas as outras políticas TLS que as conexões de back-end usam `ELBSecurityPolicy-2016-08`

Você pode descrever os protocolos e as cifras usando o comando da AWS CLI describe-ssl-policies ou consultar as tabelas a seguir.

Políticas de segurança

- Políticas de segurança de TLS
  - Protocolos por política
  - Cifras por política
  - Políticas por cifra
- Políticas de segurança FIPS
  - Protocolos por política
  - Cifras por política
  - Políticas por cifra
- Políticas de segurança compatíveis com FS
  - Protocolos por política
  - Cifras por política
  - Políticas por cifra

Políticas de segurança de TLS

Você pode usar as políticas de segurança do TLS para atender aos requisitos de conformidade e padrões de segurança que exigem a desativação de determinadas versões do protocolo TLS ou para oferecer suporte a clientes legados que exigem cifras descontinuadas.

As políticas que oferecem suporte somente ao TLS 1.3 oferecem suporte ao Forward Secrecy (FS). As políticas que oferecem suporte a TLS 1.3 e TLS 1.2 que têm somente cifras no formato TLS_* e ECDHE_* também fornecem FS.

Conteúdo

Protocolos por política

A tabela a seguir descreve os protocolos compatíveis com cada política de segurança do TLS.

Políticas de segurança	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-3-2021-06	Sim	Não	Nº	Não
ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	Sim	Não	Nº	Não
ELBSecurityPolicy-TLS13-1-2-2021-06	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Res-2021-06	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-1-2021-06	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
ELBSecurityPolicy-TLS13-1-0-2021-06	Yes (Sim)	Yes (Sim)	Yes (Sim)	Yes (Sim)

Políticas de segurança	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	Yes (Sim)	Yes (Sim)	Yes (Sim)	Yes (Sim)
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	Não	Sim	Não	Nº
ELBSecurityPolicy-TLS-1-2-2017-01	Não	Sim	Não	Nº
ELBSecurityPolicy-TLS-1-1-2017-01	Não	Yes (Sim)	Yes (Sim)	Não
ELBSecurityPolicy-2016-08	Não	Yes (Sim)	Yes (Sim)	Yes (Sim)
ELBSecurityPolicy-2015-05	Não	Yes (Sim)	Yes (Sim)	Yes (Sim)

Cifras por política

A tabela a seguir descreve as cifras compatíveis com cada política de segurança do TLS.

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-3-2021-06 ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256
ELBSecurityPolicy-TLS13-1-2-2021-06 ELBSecurityPolicy-TLS13-1-2-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256

Política de segurança	Cifras
	• ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-Res-2021-06 ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-1-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-0-2021-06 ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-TLS-1-2-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256

Política de segurança	Cifras
ELBSecurityPolicy-TLS-1-1-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-2016-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-2015-05	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Políticas por cifra

A tabela a seguir descreve as políticas de segurança do TLS compatíveis com cada cifra.

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL: TLS_AES_128_GCM_SHA256 IANA: TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09	1301

Nome da cifra	Políticas de segurança	Pacote de cifras
	• ELBSecurityPolicy-TLS13-1-2 -2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1 -2021-06 • ELBSecurityPolicy-TLS13-1-0 -2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL: TLS_AES_256_GCM_SHA384 IANA: TLS_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	1302

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL: TLS_CHACHA20_POLY1305_SHA256 IANA: TLS_CHACHA20_POLY1305_SHA256	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-3-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09	1303

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02b

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02f

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c023

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c027

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c009
OpenSSL — ECDHE-RSA-AES128-SHA IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c013

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02c

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c030

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c024

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c028

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c014

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES128-GCM-SHA256 IANA: TLS_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	9c

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES128-SHA256 IANA: TLS_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	3c

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES128-SHA IANA: TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	2f

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES256-GCM-SHA384 IANA: TLS_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	9d

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES256-SHA256 IANA: TLS_RSA_WITH_AES_256_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	3d

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES256-SHA IANA: TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS13-1-0-PQ-2025-09 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	35

Políticas de segurança FIPS

O Federal Information Processing Standard (FIPS, Padrão de processamento de informações federal) é um padrão de segurança dos governos dos Estados Unidos e do Canadá que especifica os requisitos de segurança para módulos de criptografia que protegem informações confidenciais. Para saber mais, consulte Federal Information Processing Standard (FIPS) 140 na página AWS Cloud Security Compliance.

Todas as políticas FIPS utilizam o módulo criptográfico validado pelo AWS-LC FIPS. Para saber mais, consulte a página do Módulo AWS-LC Criptográfico no site do Programa de Validação do Módulo Criptográfico do NIST.

> **Important**
>
> As políticas `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` e `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` são fornecidas somente para compatibilidade legada. Embora

utilizem criptografia do FIPS com o módulo FIPS140, podem não estar em conformidade com as diretrizes mais recentes do NIST para configuração de TLS.

Conteúdo

Protocolos por política

A tabela a seguir descreve os protocolos compatíveis com cada política de segurança do FIPS.

Políticas de segurança	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	Sim	Não	Nº	Não
ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09	Sim	Não	Nº	Não
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não

Políticas de segurança	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09	Yes (Sim)	Yes (Sim)	Não	Não
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	Yes (Sim)	Yes (Sim)	Yes (Sim)	Yes (Sim)
ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	Yes (Sim)	Yes (Sim)	Yes (Sim)	Yes (Sim)

Cifras por política

A tabela a seguir descreve as cifras compatíveis com cada política de segurança do FIPS.

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256

Política de segurança	Cifras
	• ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de segurança	Cifras
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Políticas por cifra

A tabela a seguir descreve as políticas de segurança do FIPS compatíveis com cada cifra.

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL: TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	1301

Nome da cifra	Políticas de segurança	Pacote de cifras
IANA: TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL: TLS_AES_256_GCM_SHA384 IANA: TLS_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	1302

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c02b

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c02f

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c023

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c027

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES128-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c009
OpenSSL — ECDHE-RSA-AES128-SHA IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c013

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c02c

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c030

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c024

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c028

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c014

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES128-GCM-SHA256 IANA: TLS_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	9c
OpenSSL — AES128-SHA256 IANA: TLS_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	3c

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES128-SHA IANA: TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	2f
OpenSSL — AES256-GCM-SHA384 IANA: TLS_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	9d

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — AES256-SHA256 IANA: TLS_RSA_WITH_AES_256_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	3d
OpenSSL — AES256-SHA IANA: TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-PQ-2025-09 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09	35

Políticas de segurança compatíveis com FS

As políticas de segurança compatíveis com FS (Forward Secrecy) fornecem proteções adicionais contra a espionagem de dados criptografados por meio do uso de uma chave de sessão aleatória

exclusiva. Isso evita a decodificação dos dados capturados, mesmo que a chave secreta de longo prazo seja comprometida.

As políticas nesta seção oferecem suporte ao FS, e “FS” está incluído em seus nomes. Entretanto, essas não são as únicas políticas que oferecem suporte ao FS. As políticas que oferecem suporte somente ao TLS 1.3 oferecem suporte ao FS. As políticas que oferecem suporte a TLS 1.3 e TLS 1.2 que têm somente cifras no formato TLS_* e ECDHE_* também fornecem FS.

Conteúdo

Protocolos por política

A tabela a seguir descreve os protocolos compatíveis com cada política de segurança com suporte do FS.

Políticas de segurança	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-FS-1-2-Res-2020-10	Não	Sim	Não	Nº
ELBSecurityPolicy-FS-1-2-Res-2019-08	Não	Sim	Não	Nº
ELBSecurityPolicy-FS-1-2-2019-08	Não	Sim	Não	Nº
ELBSecurityPolicy-FS-1-1-2019-08	Não	Yes (Sim)	Yes (Sim)	Não
ELBSecurityPolicy-FS-2018-06	Não	Yes (Sim)	Yes (Sim)	Yes (Sim)

Cifras por política

A tabela a seguir descreve as cifras para as quais cada política de segurança compatível com FS oferece suporte.

Política de segurança	Cifras
ELBSecurityPolicy-FS-1-2-Res-2020-10	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-FS-1-2-Res-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-FS-1-2-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA
ELBSecurityPolicy-FS-1-1-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256

Política de segurança	Cifras
	• ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA
ELBSecurityPolicy-FS-2018-06	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

Políticas por cifra

A tabela a seguir descreve as políticas de segurança com suporte do FS, compatíveis com cada cifra.

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-ECDSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c02b
OpenSSL — ECDHE-RSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c02f
OpenSSL — ECDHE-ECDSA-AES128-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c023
OpenSSL — ECDHE-RSA-AES128-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c027
OpenSSL — ECDHE-ECDSA-AES128-SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c009

Nome da cifra	Políticas de segurança	Pacote de cifras
IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		
OpenSSL — ECDHE-RSA-AES128-SHA IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c013
OpenSSL — ECDHE-ECDSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c02c
OpenSSL — ECDHE-RSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2020-10 • ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c030
OpenSSL — ECDHE-ECDSA-AES256-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c024

Nome da cifra	Políticas de segurança	Pacote de cifras
OpenSSL — ECDHE-RSA-AES256-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c028
OpenSSL — ECDHE-ECDSA-AES256-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c00a
OpenSSL — ECDHE-RSA-AES256-SHA IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c014

Atualizar um receptor para o Network Load Balancer

Você pode atualizar o protocolo do receptor, a porta do receptor ou o grupo de destino que recebe tráfego da ação de encaminhamento. A ação padrão, também conhecida como regra padrão, encaminha as solicitações para o grupo de destino selecionado.

Se você alterar o protocolo de TCP, UDP ou QUIC para TLS, será necessário especificar uma política de segurança e um certificado do servidor. Se você alterar o protocolo de TLS para TCP, UDP ou QUIC, a política de segurança e o certificado do servidor serão removidos.

Quando o grupo de destino da ação padrão de um receptor TCP, TLS ou QUIC é atualizado, novas conexões são roteadas para o grupo de destino recém-configurado. No entanto, isso não afeta qualquer conexão ativa criada antes dessa alteração. Essas conexões ativas permanecem associadas ao destino no grupo de destino original por até uma hora se estiver sendo enviado tráfego, ou até o tempo limite de inatividade se nenhum tráfego for enviado, o que ocorrer primeiro.

O parâmetro `Connection termination on deregistration` não é aplicado na atualização do receptor, pois ele é aplicado no cancelamento do registro dos destinos.

Não são permitidas atualizações de portas para receptores QUIC ou TCP_QUIC. Para atualizar a porta para receptores que processam tráfego QUIC, o receptor deve ser excluído e recriado com a nova porta.

Console

Atualizar um receptor

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Ouvintes, escolha o texto na Protocol:Portcoluna para abrir a página de detalhes do ouvinte.
5. Selecione Ações, Editar receptor.
6. Atualize os valores conforme necessário.
   - (Opcional) Altere o Protocolo.
   - (Opcional) Altere a Porta.
   - (Opcional) Selecione grupos de destino diferentes para a Ação padrão.
   - (Opcional) Para adicionar outro grupo de destino, selecione Adicionar grupo de destino e atualize os pesos conforme necessário.
   - (Opcional) Para remover um grupo de destino, selecione Remover.
7. (Opcional) Adicione, atualize ou remova tags conforme necessário.
8. Escolha Salvar alterações.

AWS CLI

Para atualizar a ação padrão

Use o comando modify-listener a seguir para alterar o grupo de destino.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
```

```
    --default-actions Type=forward,TargetGroupArn=new-target-group-arn
```

O exemplo a seguir atualiza um receptor com vários grupos de destino.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
            ]
        }
    }]'
```

Como adicionar tags do

Use o comando add-tags. O exemplo a seguir adiciona duas tags.

```
aws elbv2 add-tags \
    --resource-arns listener-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Como remover tags

Use o comando remove-tags. O exemplo a seguir remove as tags com as chaves especificadas.

```
aws elbv2 remove-tags \
    --resource-arns listener-arn \
    --tag-keys project department
```

CloudFormation

Para atualizar a ação padrão

Atualize o recurso AWS::ElasticLoadBalancingV2: :Listener para incluir o novo grupo-alvo.

```
Resources:
  myTCPListener:
```

```
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref newTargetGroup
```

Como alternativa, para distribuir o tráfego entre vários grupos de destino, defina as `DefaultActions` como mostrado a seguir.

```
DefaultActions:
    - Type: forward
    ForwardConfig:
        TargetGroups:
        - TargetGroupArn: !Ref TargetGroup1
            Weight: 10
        - TargetGroupArn: !Ref TargetGroup2
            Weight: 30
```

Como adicionar tags do

Atualize o recurso AWS::ElasticLoadBalancingV2: :Listener para incluir a propriedade Tags.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Atualizar o tempo limite de inatividade de TCP para o receptor do Network Load Balancer

Para cada solicitação de TCP feita por meio de um Network Load Balancer, o estado da conexão é rastreado. Se não há dados enviados do cliente nem do destino por um período que ultrapasse o tempo limite de inatividade, a conexão é fechada.

Considerações

- Para fluxos TCP, o valor do tempo limite padrão de inatividade é de 350 segundos.
- O tempo limite de inatividade da conexão para receptores TLS é de 350 segundos e não pode ser modificado.

Console

Para atualizar o tempo limite de inatividade do TCP

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing, selecione Load Balancers.
3. Marque a caixa de seleção para o Network Load Balancer.
4. Na guia de receptores, marque a caixa de seleção do receptor TCP e escolha Ações, Visualizar detalhes do receptor.
5. Na página de detalhes do receptor, na guia Atributos, selecione Editar. Se o receptor usar um protocolo diferente do TCP, essa guia não estará presente.
6. Insira um valor para o tempo limite de inatividade do TCP de 60 a 6.000 segundos.
7. Escolha Salvar alterações.

AWS CLI

Para atualizar o tempo limite de inatividade do TCP

Use o comando modify-listener-attributes com o atributo `tcp.idle_timeout.seconds`.

```
aws elbv2 modify-listener-attributes \
    --listener-arn listener-arn \
    --attributes Key=tcp.idle_timeout.seconds,Value=500
```

O seguinte é um exemplo de saída.

```
{
    "Attributes": [
        {
            "Key": "tcp.idle_timeout.seconds",
            "Value": "500"
        }
    ]
}
```

CloudFormation

Para atualizar o tempo limite de inatividade do TCP

Atualize o recurso AWS::ElasticLoadBalancingV2: :Listener para incluir o atributo listener. `tcp.idle_timeout.seconds`

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      ListenerAttributes:
        - Key: "tcp.idle_timeout.seconds"
          Value: "500"
```

Atualizar um receptor TLS para o Network Load Balancer

Depois de criar um listener TLS, você poderá substituir o certificado padrão, adicionar ou remover certificados da lista de certificados, atualizar a política de segurança ou atualizar a política ALPN.

Tarefas

- Substituir o certificado padrão
- Adicionar certificados à lista de certificados

- Remover certificados da lista de certificados
- Atualizar a política de segurança
- Atualizar a política ALPN

Substituir o certificado padrão

Você pode substituir o certificado padrão do seu receptor TLS conforme necessário. Para obter mais informações, consulte Certificado padrão.

Console

Para substituir o certificado padrão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Balanceador de carga.
3. Selecione o load balancer.
4. Na guia Ouvintes, escolha o texto na Protocol:Portcoluna para abrir a página de detalhes do ouvinte.
5. Na guia Certificados, escolha Alterar padrão.
6. Na tabela Certificados do ACM e do IAM, selecione um novo certificado padrão.
7. (Opcional) Por padrão, selecionamos Adicionar certificado padrão anterior à lista de certificados de receptor. Recomendamos que você mantenha essa opção selecionada, a menos que você não tenha certificados de receptor para SNI atualmente e confie na retomada da sessão TLS.
8. Escolha Salvar como padrão.

AWS CLI

Para substituir o certificado padrão

Use o comando modify-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --certificates CertificateArn=new-default-certificate-arn
```

CloudFormation

Para substituir o certificado padrão

Atualize o recurso AWS::ElasticLoadBalancingV2: :Listener com o novo certificado padrão.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "new-default-certificate-arn"
```

Adicionar certificados à lista de certificados

Você pode adicionar certificados à lista de certificados do listener usando o procedimento a seguir. Ao criar um listener TLS pela primeira vez, a lista de certificados estará vazia. Você pode adicionar o certificado padrão à lista de certificados para garantir que esse certificado seja usado com o protocolo SNI, mesmo que ele seja substituído como certificado padrão. Para obter mais informações, consulte Lista de certificados.

Console

Para adicionar certificados à lista de certificados

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Ouvintes, escolha o texto na Protocol:Portcoluna para abrir a página de detalhes do ouvinte.
5. Escolha a guia Certificados.
6. Para adicionar o certificado padrão à lista, selecione Adicionar padrão à lista.

7. Para adicionar certificados não padrão à lista, siga os passos a seguir:

   a. Escolha Adicionar certificado.

   b. Para adicionar certificados que já sejam gerenciados pelo ACM ou pelo IAM, marque as caixas de seleção dos certificados e escolha Incluir como pendente abaixo.

   c. Para adicionar um certificado que não seja gerenciado pelo ACM ou pelo IAM, escolha Importar certificado, preencha o formulário e escolha Importar.

   d. Escolha Adicionar certificados pendentes.

AWS CLI

Para adicionar certificados à lista de certificados

Use o comando add-listener-certificates.

```
aws elbv2 add-listener-certificates \
    --listener-arn listener-arn \
    --certificates \
        CertificateArn=certificate-arn-1 \
        CertificateArn=certificate-arn-2 \
        CertificateArn=certificate-arn-3
```

CloudFormation

Para adicionar certificados à lista de certificados

Defina um recurso do tipo AWS::ElasticLoadBalancingV2:: ListenerCertificate.

```
Resources:
  myCertificateList:
    Type: 'AWS::ElasticLoadBalancingV2::ListenerCertificate'
    Properties:
      ListenerArn: !Ref myTLSListener
      Certificates:
        - CertificateArn: "certificate-arn-1"
        - CertificateArn: "certificate-arn-2"
        - CertificateArn: "certificate-arn-3"

  myTLSListener:
    Type: AWS::ElasticLoadBalancingV2::Listener
    Properties:
```

```
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLSS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn-1"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Remover certificados da lista de certificados

É possível remover certificados da lista de certificados de um listener TLS usando o procedimento a seguir. Após a remoção de um certificado, o receptor não poderá mais criar conexões usando esse certificado. Para ter certeza de que os clientes não serão afetados, adicione um novo certificado à lista e confirme se as conexões estão funcionando antes de remover um certificado da lista.

Para remover o certificado padrão de um listener TLS, consulte Substituir o certificado padrão.

Console

Para remover certificados da lista de certificados

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Ouvintes, escolha o texto na Protocol:Portcoluna para abrir a página de detalhes do ouvinte.
5. Na guia Certificados, marque as caixas de seleção para os certificados e escolha Remover.
6. Quando a confirmação for solicitada, insira **`confirm`** e escolha Rejeitar.

AWS CLI

Para remover certificados da lista de certificados

Use o comando remove-listener-certificates.

```
aws elbv2 remove-listener-certificates \
    --listener-arn listener-arn \
```

```
    --certificates CertificateArn=certificate-arn
```

Atualizar a política de segurança

Ao criar um listener TLS, você poderá selecionar a política de segurança que atenda às suas necessidades. Quando uma nova política de segurança é adicionada, você pode atualizar seu receptor HTTPS para usar a nova política de segurança. Os Network Load Balancers não são compatíveis com políticas de segurança personalizadas. Para obter mais informações, consulte Políticas de segurança para o Network Load Balancer.

A atualização da política de segurança pode resultar em interrupções se o balanceador de carga estiver lidando com um alto volume de tráfego. Para diminuir a possibilidade de interrupções quando seu balanceador de carga está lidando com um grande volume de tráfego, crie um balanceador de carga adicional para ajudar a lidar com o tráfego ou solicite uma reserva de LCU.

Console

Para atualizar a política de segurança

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Ouvintes, escolha o texto na Protocol:Portcoluna para abrir a página de detalhes do ouvinte.
5. Selecione Ações, Editar receptor.
6. Na seção Configurações de receptor seguro, em Política de segurança, escolha uma nova política de segurança.
7. Escolha Salvar alterações.

AWS CLI

Para atualizar a política de segurança

Use o comando modify-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
```

```
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06
```

CloudFormation

Para atualizar a política de segurança

Atualize o recurso AWS::ElasticLoadBalancingV2: :Listener com a nova política de segurança.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "default-certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Atualizar a política ALPN

Você pode atualizar a política ALPN para seu receptor TLS conforme necessário. Para obter mais informações, consulte Políticas ALPN.

Console

Para atualizar a política ALPN

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Ouvintes, escolha o texto na Protocol:Portcoluna para abrir a página de detalhes do ouvinte.
5. Selecione Ações, Editar receptor.
6. Na seção Configurações de receptor seguro, em Política ALPN, escolha uma política para habilitar ALPN ou escolha Nenhuma para desabilitar ALPN.

7. Escolha Salvar alterações.

AWS CLI

Para atualizar a política ALPN

Use o comando modify-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --alpn-policy HTTP2Preferred
```

CloudFormation

Para atualizar a política ALPN

Atualize o recurso AWS::ElasticLoadBalancingV2: :Listener para incluir a política ALPN.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      AlpnPolicy:
        - HTTP2Preferred
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Excluir um receptor para o Network Load Balancer

Antes de excluir um receptor, considere o impacto em seu aplicativo:

- [Receptores TCP e TLS] O balanceador de carga para imediatamente de aceitar novas conexões no receptor. Qualquer handshake TLS em andamento pode falhar. As conexões existentes

permanecem abertas até que se fechem naturalmente ou expirem. In-flightsolicitações em conexões existentes foram concluídas com êxito.

- [Receptores UDP e QUIC] Qualquer pacote em trânsito pode não chegar ao destino.

Console

Excluir um receptor

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Marque a caixa de seleção para balanceador de carga.
4. Na guia Receptores, marque a caixa de seleção do receptor e escolha Ações, Excluir receptor.
5. Quando a confirmação for solicitada, insira **`confirm`** e escolha Excluir.

AWS CLI

Excluir um receptor

Use o comando delete-listener.

```
aws elbv2 delete-listener \
    --listener-arn listener-arn
```

Grupos de destino para Network Load Balancers

Cada grupo de destino é usado para rotear solicitações para um ou mais destinos registrados. Ao criar um listener, especifique um grupo de destino para a ação padrão dele. O tráfego é encaminhado para o grupo de destino especificado na regra do listener. Você pode criar grupos de destino diferentes para tipos de solicitações diferentes. Por exemplo, você pode criar um grupo de destino para solicitações gerais e outros grupos de destino para solicitações para os microsserviços do aplicativo. Para obter mais informações, consulte Componentes do Network Load Balancer.

Você define as configurações de verificação de integridade para seu load balancer 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 listener, o load balancer monitora continuamente a integridade de todos os destinos registrados com o grupo de destino que estiverem em uma Zona de disponibilidade habilitada para o load balancer. O load balancer roteia solicitações para os destinos registrados que são íntegros. Para obter mais informações, consulte Verificações de integridade para grupos de destino do Network Load Balancer.

Conteúdo

Configuração de roteamento

Por padrão, um load balancer 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 para Network Load Balancers são compatíveis com os seguintes protocolos e portas:

- Protocolos: TCP, TLS, UDP, TCP_UDP, QUIC, TCP_QUIC
- Ports (Portas): 1-65535

Se um grupo de destino estiver configurado com o protocolo TLS, o load balancer estabelecerá conexões TLS com os destinos usando certificados instalados nos destinos. O load balancer não valida esses certificados. Portanto, é possível usar certificados autoassinados ou certificados que tenham expirado. Como o balanceador de carga está em uma nuvem privada virtual (VPC), o tráfego entre o balanceador de carga e os destinos é autenticado no nível do pacote, portanto, não corre o risco man-in-the-middle de ataques ou falsificação, mesmo que os certificados nos destinos não sejam válidos.

A tabela a seguir resume as combinações compatíveis das configurações do protocolo do listener e do grupo de destino.

Protocolo do listener	Protocolo do grupo de destino	Tipo de grupo de destino	Protocolo da verificação de integridade
TCP	TCP | TCP_UDP | TCP_QUIC	instância | ip	HTTP | HTTPS | TCP
TCP	TCP	alb	HTTP | HTTPS
TLS	TCP | TLS	instância | ip	HTTP | HTTPS | TCP
UDP	UDP | TCP_UDP	instância | ip	HTTP | HTTPS | TCP
TCP_UDP	TCP_UDP	instância | ip	HTTP | HTTPS | TCP
QUIC	QUIC | TCP_QUIC	instância | ip	HTTP | HTTPS | TCP

Protocolo do listener	Protocolo do grupo de destino	Tipo de grupo de destino	Protocolo da verificação de integridade
TCP_QUIC	TCP_QUIC	instância | ip	HTTP | HTTPS | TCP

Target type

Quando você cria um grupo de destino, você especifica o tipo de destino, que determina como você especifica seus destinos. 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 especificados por endereço IP.

`alb`

O destino é um Application Load Balancer.

Quando o tipo de destino é `ip`, você pode especificar os endereços IP de um dos seguintes blocos CIDR:

- As sub-redes da VPC do grupo de destino
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

> **Important**
>
> Você não pode especificar publicamente endereços IP roteáveis.

Todos os blocos CIDR compatíveis permitem que você registre os seguintes destinos em um grupo de destino:

- AWS recursos que são endereçáveis por endereço IP e porta (por exemplo, bancos de dados).
- Recursos locais vinculados AWS por meio Direct Connect de uma conexão Site-to-Site VPN.

Quando a preservação do IP do cliente está desabilitada para seus grupos de destino, o balanceador de carga pode suportar aproximadamente 55 mil conexões por minuto para cada combinação de endereço IP do Network Load Balancer e destino exclusivo (endereço IP e porta). Se você exceder essas conexões, há uma chance maior de erros de alocação de porta. Se você receber erros de alocação de porta, adicione mais destinos ao grupo de destino.

Ao iniciar um Network Load Balancer em uma VPC compartilhada (como participante), você só pode registrar destinos em sub-redes que foram compartilhadas com você.

Quando o tipo de destino é `alb`, você pode registrar um único Application Load Balancer como destino. Para obter mais informações, consulte Usar um Application Load Balancer como destino de um Network Load Balancer.

Os Network Load Balancers não são compatíveis com o tipo de destino `lambda`. Os Application Load Balancers são os únicos balanceadores de carga compatíveis com o tipo de destino `lambda`. Para obter mais informações, consulte Lambda functions as targets no Guia do usuário de Application Load Balancers.

Se você tiver microsserviços em instâncias registradas em um Network Load Balancer, não poderá usar o balanceador de carga para possibilitar a comunicação entre eles, a menos que o balanceador de carga esteja voltado para a Internet ou as instâncias estejam registradas por endereço IP. Para obter mais informações, consulte As conexões expiram para solicitações de um destino para o load balancer.

Roteamento de solicitações e endereços IP

Se você especificar destinos usando um ID de instância, o tráfego será roteado para instâncias usando o endereço IP primário privado especificado na interface de rede primária para a instância. O load balancer grava novamente o endereço IP de destino do pacote de dados antes de encaminhá-lo para a instância de destino.

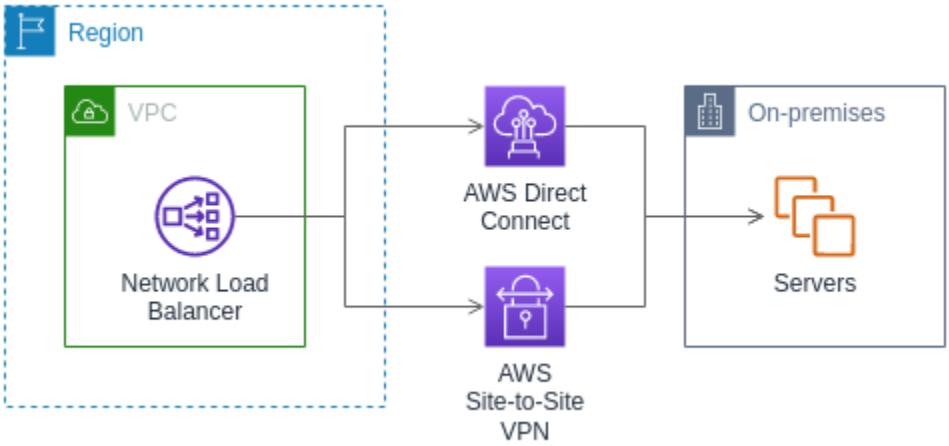
Se você especificar destinos usando endereços IP, você pode rotear o tráfego para uma instância com qualquer endereço IP privado de uma ou mais interfaces de rede. Isso permite que vários

aplicativos em uma instância usem a mesma porta. Observe que cada interface de rede pode ter seu próprio security group. O load balancer grava novamente o endereço IP de destino antes de encaminhá-lo para o destino.

Para obter mais informações sobre permissão de tráfego para suas instâncias, consulte Grupos de segurança de destino.

Recursos on-premises como destinos

Recursos locais vinculados por meio Direct Connect de uma conexão Site-to-Site VPN podem servir como alvo, quando o tipo de destino for `ip`.



Ao usar recursos on-premises, os endereços IP desses destinos ainda devem vir de um dos seguintes blocos CIDR:

- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Para obter mais informações sobre Direct Connect, consulte O que é Direct Connect?

Para obter mais informações sobre AWS Site-to-Site VPN, consulte O que é AWS Site-to-Site VPN?

Tipo de endereço IP

Ao criar um novo grupo de destino, você pode selecionar o tipo de endereço IP dele. Isso controla a versão do IP usada para comunicação com os destinos e para a verificação do status de integridade deles.

Os grupos de destino de seus Network Load Balancers são compatíveis com os seguintes tipos de endereço IP:

`ipv4`

O balanceador de carga se comunica com os destinos usando. IPv4

`ipv6`

O balanceador de carga se comunica com os destinos usando. IPv6

Considerações

- O balanceador de carga se comunica com os destinos com base no tipo de endereço IP do grupo de destino. Os destinos de um IPv4 grupo-alvo devem aceitar o IPv4 tráfego do balanceador de carga e os destinos de um IPv6 grupo-alvo devem aceitar o IPv6 tráfego do balanceador de carga.
- Você não pode usar um IPv6 grupo-alvo com um balanceador de `ipv4` carga.
- Você não pode usar um IPv4 grupo-alvo com um ouvinte UDP para um balanceador de `dualstack` carga.
- Você não pode registrar um Application Load Balancer com um IPv6 grupo-alvo.
- Você não pode usar um IPv6 grupo-alvo com os protocolos QUIC ou TCP_QUIC.

Destinos registrados

O seu load balancer serve como um ponto único de contato para clientes e distribui o tráfego de entrada nos destinos íntegros registrados. Cada grupo de destino deve ter pelo menos um destino registrado em cada zona de disponibilidade que é habilitada para o load balancer. Você pode registrar cada destino com um ou mais grupos de destino.

Se a demanda da seu aplicativo aumentar, você pode registrar destinos adicionais com um ou mais grupos de destino, a fim de dar conta da demanda. O balanceador de carga inicia o roteamento do

tráfego para um destino recém-registrado assim que o processo de registro é concluído e o destino passa pelas verificações de integridade iniciais, independentemente do limite configurado.

Se a demanda na aplicação diminuir ou se você precisar fazer manutenção nos destinos, poderá cancelar o registro dos destinos nos 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 load balancer interrompe o roteamento do tráfego para um destino assim que o registro dele é 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 do tráfego.

Se você estiver registrando destinos por ID de instância, poderá usar o balanceador de carga com um grupo do Auto Scaling. Depois que você anexar um grupo de destino a um grupo do Auto Scaling, o Auto Scaling registrará os destinos no grupo de destino para você quando ele os iniciar. Para obter mais informações, consulte Anexar um balanceador de carga ao seu grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

Requisitos e considerações

- Você não pode registrar instâncias por ID de instância se elas usarem um dos seguintes tipos de instância: C1,, CC1,, CC2, CG1, CG2, CR1, G1,,, M1 HI1, M2 HS1, M3 ou T1.
- Ao registrar destinos por ID de instância para um grupo de IPv6 destino, os destinos devem ter um IPv6 endereço principal atribuído. Para saber mais, consulte os IPv6 endereços no Guia do usuário do Amazon EC2
- Ao registrar destinos por ID da instância, as instâncias devem estar na mesma VPC que o Network Load Balancer. Não será possível registrar instâncias por ID de instância se elas estiverem em uma VPC emparelhada com a VPC do balanceador de carga (mesma região ou região diferente). Você poderá registrar essas instâncias pelo endereço IP.
- Se você registrar um destino por endereço IP e o endereço IP estiver na mesma VPC que o load balancer, o load balancer verificará se ele é de uma sub-rede que ele possa acessar.
- O balanceador de carga direciona o tráfego para destinos localizados somente em zonas de disponibilidade habilitadas. Destinos em zonas não habilitadas não são usados.
- Para grupos de destino UDP, TCP_UDP, QUIC e TCP_QUIC, não registre instâncias por endereço IP se elas residirem fora da VPC do balanceador de carga ou se usarem um dos seguintes tipos de instância: C1,,,,,,, G1,,,, M1, M2 CC1 CC2 CG1 CG2 CR1, M3 ou T1. HI1 HS1 Destinos que residem fora da VPC do balanceador de carga ou que usam um tipo de instância incompatível podem receber tráfego do balanceador de carga, mas não conseguem responder.

Atributos do grupo de destino

Você pode configurar um grupo de destino editando os atributos. Para obter mais informações, consulte Editar atributos do grupo de destino.

Os seguintes atributos de grupo de destino são compatíveis. Você só pode modificar esses atributos quando o tipo de grupo de destino é `instance` ou `ip`. Se o tipo de grupo de destino for `alb`, esses atributos sempre usarão os valores padrão.

`deregistration_delay.timeout_seconds`

A quantidade de tempo que o Elastic Load Balancing deve aguardar antes de alterar o estado de um destino que terá o registro cancelado de `draining` para `unused`. O intervalo é 0-3600 segundos. O valor de padrão é de 300 segundos. Para tráfego QUIC, o valor é sempre 300 segundos.

`deregistration_delay.connection_termination.enabled`

Indica se o balanceador de carga encerra as conexões no final do tempo limite de cancelamento do registro. O valor é `true` ou `false`. Para novos grupos de destino UDP/TCP_UDP, o padrão é `true`. Caso contrário, o padrão é `false`. Esse atributo não se aplica ao tráfego QUIC.

`load_balancing.cross_zone.enabled`

Indica se o balanceamento de carga entre zonas está habilitado. O valor é `true`, `false` ou `use_load_balancer_configuration`. O padrão é `use_load_balancer_configuration`.

`preserve_client_ip.enabled`

Indica se a preservação do IP do cliente está habilitada. O valor é `true` ou `false`. O padrão é desativado se o tipo de grupo de destino for endereço IP e o protocolo do grupo de destino for TCP ou TLS. Caso contrário, o padrão é habilitado. A preservação do cliente não pode ser desabilitada para grupos de destino UDP e TCP_UDP, QUIC e TCP_QUIC.

`proxy_protocol_v2.enabled`

Indica se o Proxy Protocol versão 2 está habilitado. Por padrão, o Proxy Protocol está desabilitado.

`stickiness.enabled`

Indica se sticky sessions estão habilitadas. O valor é `true` ou `false`. O padrão é `false`. Esse atributo não se aplica ao tráfego QUIC.

`stickiness.type`

O tipo de perdurabilidade. O valor possível é `source_ip`.

`target_group_health.dns_failover.minimum_healthy_targets.count`

O número mínimo de destinos que devem ser íntegros. Se o número de destinos íntegros for menor do que esse valor, marque a zona como não íntegra no DNS, para que o tráfego seja roteado somente para zonas íntegras. Os valores possíveis são `off` ou um número inteiro de 1 até o número máximo de destinos. Quando estiver `off`, a falha de DNS é desabilitada, ou seja, mesmo que todos os destinos no grupo de destino não estejam íntegros, a zona não será removida do DNS. O padrão é um.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

A porcentagem mínima de destinos que devem ser íntegros. Se a porcentagem de destinos íntegros for menor do que esse valor, marque a zona como não íntegra no DNS, para que o tráfego seja roteado somente para zonas íntegras. Os valores possíveis são `off` ou um número inteiro de 1 a 100. Quando estiver `off`, a falha de DNS é desabilitada, ou seja, mesmo que todos os destinos no grupo de destino não estejam íntegros, a zona não será removida do DNS. O padrão é `off`.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

O número mínimo de destinos que devem estar íntegros. Se o número de destinos íntegros for menor do que desse valor, envie tráfego para todos os alvos, incluindo alvos não íntegros. Os valores possíveis são de 1 ao número máximo de destinos. O padrão é um.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

O percentual mínimo de destinos que devem estar íntegros. Se a porcentagem de destinos íntegros for menor do que valor, envie tráfego para todos os destinos, incluindo destinos não íntegros. Os valores possíveis são `off` ou um número inteiro de 1 a 100. O padrão é `off`.

`target_health_state.unhealthy.connection_termination.enabled`

Indica se o balanceador de carga encerra as conexões com destinos não íntegros. O valor é `true` ou `false`. O padrão é `true`.

`target_health_state.unhealthy.draining_interval_seconds`

A quantidade de tempo que o Elastic Load Balancing deve aguardar antes de alterar o estado de um destino não íntegro de `unhealthy.draining` para `unhealthy`. O intervalo é 0 – 360.000 segundos. O valor de padrão é 0 segundos.

Observação: esse atributo só pode ser configurado quando `target_health_state.unhealthy.connection_termination.enabled` é `false`.

Integridade do grupo de destino

Por padrão, um grupo de destino é considerado íntegro desde que tenha pelo menos um destino íntegro. Se você tiver uma frota grande, não é suficiente ter apenas um destino íntegro distribuindo o tráfego. Em vez disso, você pode especificar uma contagem ou percentual mínimo de destinos que devem estar íntegros e quais ações o balanceador de carga executa quando os destinos íntegros ficarem abaixo do limite especificado. Isso melhora a disponibilidade do seu aplicativo.

Conteúdo

Ações para estado não íntegro

Você pode configurar os limites íntegros para as seguintes ações:

- Failover de DNS: quando os destinos íntegros em uma zona ficam abaixo do limite, marcamos os endereços IP do nó do balanceador de carga da zona como não íntegros em DNS. Portanto, quando os clientes resolvem o nome DNS do balanceador de carga, o tráfego é roteado somente para zonas íntegras.
- Failover de roteamento: quando os destinos íntegros em uma zona ficam abaixo do limite, o balanceador de carga envia tráfego para todos os destinos que estão disponíveis para o nó do balanceador de carga, incluindo destinos não íntegros. Isso aumenta a probabilidade de sucesso da conexão de um cliente, especialmente quando os destinos temporariamente são reprovados nas verificações de integridade, e reduz o risco de sobrecarga dos destinos íntegros.

Requisitos e considerações

- Se você especificar os dois tipos de limites para uma ação (contagem e porcentagem), o balanceador de carga executará a ação quando um dos limites for violado.

- Se você especificar limites para ambas as ações, o limite para failover de DNS deverá ser maior ou igual ao limite para failover de roteamento, de modo que o failover de DNS ocorra com o failover de roteamento ou antes dele.
- Se você especificar o limite como um percentual, calcularemos o valor dinamicamente com base no número total de destinos registrados nos grupos de destino.
- O número total de destinos depende do balanceamento de carga entre zonas estar ativado ou desativado. Se o balanceamento de carga entre zonas estiver desativado, cada nó enviará tráfego somente para os destinos na sua própria zona, o que significa que os limites se aplicarão ao número de destinos em cada zona habilitada separadamente. Se o balanceamento de carga entre zonas estiver ativado, cada nó enviará tráfego a todos os destinos em todas as zonas habilitadas, o que significa que os limites especificados se aplicarão ao número total de destinos em todas as zonas habilitadas. Para obter mais informações, consulte Balanceamento de carga entre zonas.
- Quando houver um failover de DNS, todos os grupos de destino associados ao balanceador de carga serão afetados. Verifique se você tem capacidade suficiente nas zonas restantes para processar esse tráfego adicional, especialmente se o balanceamento de carga entre zonas estiver desativado.
- Com o failover de DNS, removemos os endereços IP das zonas não íntegras do nome de host DNS do balanceador de carga. No entanto, o cache DNS do cliente local pode conter esses endereços IP até que o time-to-live (TTL) no registro DNS expire (60 segundos).
- Com o failover de DNS, se houver vários grupos de destino vinculados a um Network Load Balancer e um grupo de destino não estiver íntegro em uma zona, o failover de DNS ocorre, mesmo que outro grupo de destino esteja íntegro nessa zona.
- Com o failover de DNS, se todas as zonas do balanceador de carga forem consideradas não íntegras, o balanceador de carga enviará tráfego para todas as zonas, incluindo as zonas não íntegras.
- Além da existência de destinos íntegros em número suficiente, há outros fatores que podem levar ao failover de DNS, como a integridade da zona.

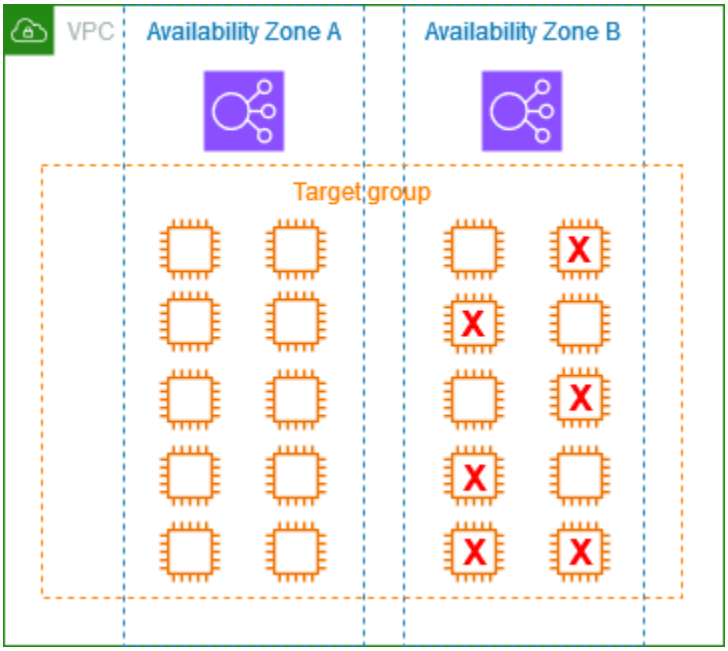
Exemplo

O exemplo a seguir demonstra como as configurações de integridade do grupo de destino são aplicadas.

Cenário

- Um balanceador de carga compatível com duas zonas de disponibilidade, A e B

- Cada zona de disponibilidade contém 10 destinos registrados
- O grupo de destino tem as seguintes configurações de integridade:
  - Failover de DNS: 50%
  - Failover de roteamento: 50%
- Seis destinos apresentam falha na zona de disponibilidade B



Se o balanceamento de carga entre zonas estiver desativado

- O nó do balanceador de carga em cada zona de disponibilidade só pode enviar tráfego para os 10 destinos em sua zona de disponibilidade.
- Há 10 destinos íntegros na zona de disponibilidade A, o que atende ao percentual necessário de destinos íntegros. O balanceador de carga continua distribuindo o tráfego entre os 10 destinos íntegros.
- Há apenas 4 destinos íntegros na zona de disponibilidade B, o que representa 40% dos destinos do nó do balanceador de carga na zona de disponibilidade B. Como isso é inferior ao percentual necessário de destinos íntegros, o balanceador de carga executará as seguintes ações:
  - Failover de DNS: a zona de disponibilidade B será marcada como não íntegra no DNS. Como os clientes não conseguem resolver o nome do balanceador de carga para o nó do balanceador de carga na zona de disponibilidade B e a zona de disponibilidade A está íntegra, os clientes enviam novas conexões para a zona de disponibilidade A.

- Failover de roteamento: quando novas conexões são enviadas explicitamente para a zona de disponibilidade B, o balanceador de carga distribui o tráfego para todos os destinos na zona de disponibilidade B, incluindo os destinos não íntegros. Isso evita interrupções entre os destinos íntegros restantes.

Se o balanceamento de carga entre zonas estiver ativado

- Cada nó do balanceador de carga pode enviar tráfego para todos os 20 destinos registrados em ambas as zonas de disponibilidade.
- Há 10 destinos íntegros na zona de disponibilidade A e 4 destinos íntegros na zona de disponibilidade B, totalizando 14 destinos íntegros. Isso representa 70% dos destinos para os nós do balanceador de carga em ambas as zonas de disponibilidade, o que atende ao percentual necessário de destinos íntegros.
- O balanceador de carga distribui tráfego entre os 14 destinos íntegros nas duas zonas de disponibilidade.

Como usar o failover de DNS do Route 53 para o seu balanceador de carga

Se você usa o Route 53 para rotear consultas de DNS para seu balanceador de carga, também poderá configurar o failover de DNS para o seu balanceador de carga usando o Route 53. Em uma configuração de failover, o Route 53 verifica a integridade dos destinos dos grupos de destino do balanceador de carga para determinar se eles estão disponíveis. Se não houver destinos íntegros registrados no balanceador de carga ou se o próprio balanceador de carga não estiver íntegro, o Route 53 roteará o tráfego para outro recurso disponível, como um balanceador de carga íntegro ou um site estático no Amazon S3.

Por exemplo, vamos supor que você tenha uma aplicação Web para `www.example.com` e deseja instâncias redundantes em execução por trás de dois balanceadores de carga que residam em diferentes regiões. Você deseja que o tráfego seja roteado primariamente para o balanceador de carga em uma região e quer usar o balanceador de carga na outra região como backup durante falhas. Se você configurar o failover de DNS, poderá especificar os balanceadores de carga primário e secundário (backup). O Route 53 direcionará o tráfego para o balanceador de carga primário, se estiver disponível, ou para o balanceador de carga secundário, em caso contrário.

Como funciona a avaliação da integridade do destino

- Quando a opção de avaliar a integridade do destino está definida como `Yes` em um registro de alias para um Network Load Balancer, o Route 53 avalia a integridade do recurso especificado pelo valor do `alias target`. O Route 53 usa as verificações de integridade do grupo de destino.
- Se todos os grupos de destino vinculados a um Network Load Balancer estiverem íntegros, o Route 53 marcará o registro do alias como íntegro. Se você configurou um limite para um grupo de destino e ele atinge esse limite, ele passa nas verificações de integridade. Do contrário, se um grupo de destino contiver pelo menos um destino íntegro, sua verificação de integridade será aprovada. Se a verificação de integridade tiver êxito, o Route 53 retornará os registros de acordo com a sua política de roteamento. Se uma política de roteamento por failover for usada, o Route 53 retornará o registro primário.
- Se todos os grupos de destino em um Network Load Balancer não estiverem íntegros, o registro do alias apresentará falha na verificação de integridade do Route 53 (falha na abertura). Se a avaliação da integridade do destino for usada, a política de roteamento por failover redirecionará o tráfego para o recurso secundário.
- Se todos os grupos de destino em um Network Load Balancer estiverem vazios (sem destinos), o Route 53 considerará o registro não íntegro (falha na abertura). Se a avaliação da integridade do destino for usada, a política de roteamento por failover redirecionará o tráfego para o recurso secundário.

Para obter mais informações, consulte Uso dos limites de integridade do grupo-alvo do balanceador de carga para melhorar a disponibilidade no AWS blog e Configuração do failover de DNS no Guia do desenvolvedor do Amazon Route 53.

Criar um grupo de destino para o Network Load Balancer

Você registra destinos para seu Network Load Balancer com um grupo de destino. Por padrão, o load balancer 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 destinos em um grupo de destino, crie um listener e especifique o grupo de destino em uma ação padrão para o listener. Para obter mais informações, consulte Ações padrão. Você pode especificar o mesmo grupo de destino em vários receptores, mas esses receptores devem pertencer ao mesmo Network Load Balancer. Para usar um grupo de destino com um

balanceador de carga, você deve verificar se o grupo de destino não está sendo usado por um receptor para qualquer outro balanceador de carga.

Você pode adicionar ou remover destinos do seu grupo de destino a qualquer momento. Para obter mais informações, consulte Registrar destinos para o Network Load Balancer. Você também pode modificar as configurações de verificação de integridade para seu grupo de destino. Para obter mais informações, consulte Atualizar as configurações da verificação de integridade de um grupo de destino do Network Load Balancer.

Requisitos

- Depois de criar um grupo de destino, você não pode mudar o tipo de destino ou o tipo de endereço IP desse grupo.
- Todos os destinos em um grupo-alvo devem ter o mesmo tipo de endereço IP do grupo-alvo: IPv4 ou IPv6.
- Você deve usar um IPv6 grupo-alvo com um balanceador de carga de pilha dupla.
- Você não pode usar um IPv4 grupo-alvo com um ouvinte UDP para um balanceador de `dualstack` carga.
- Você não pode usar um IPv6 grupo-alvo com os protocolos QUIC ou TCP_QUIC.

Console

Para criar um grupo de destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Grupos de destino.
3. Selecione Criar grupo de destino.
4. No painel Configuração básica, faça o seguinte:

    a. Em Escolher um tipo de destino, selecione Instâncias para registrar os destinos por ID da instância, Endereços IP para registrar destinos por endereço IP ou Application Load Balancer para registrar um Application Load Balancer como destino.

    b. Em Nome do grupo de destino, insira um nome para o grupo de destino. Esse nome deve ser exclusivo por região e por conta, pode ter o máximo de 32 caracteres, deve conter apenas caracteres alfanuméricos ou hifens, e não deve iniciar nem terminar com hífen.

    c. Em Protocol (Protocolo), escolha um protocolo da seguinte maneira:

- Se o protocolo do listener for TCP, escolha TCP ou TCP_UDP.
- Se o protocolo do listener for TLS, escolha TCP ou TLS.
- Se o protocolo do listener for UDP, escolha UDP ou TCP_UDP.
- Se o protocolo do listener for TCP_UDP, escolha TCP_UDP.
- Se o protocolo do receptor for QUIC, selecione QUIC.
- Se o protocolo do receptor for TCP_QUIC, selecione TCP_QUIC.
- Se o tipo de destino for Application Load Balancer, o protocolo precisa ser TCP.

d. Para Porta, modifique o valor padrão conforme necessário.

   Se o tipo de destino for Application Load Balancer, a porta precisa corresponder à porta do receptor do Application Load Balancer.

e. Para o tipo de endereço IP, escolha IPv4ou IPv6. Essa opção só estará disponível se o tipo de destino for Instâncias ou Endereços IP.

f. Em VPC, selecione a nuvem privada virtual (VPC) com os destinos a serem registrados.

5. No painel Verificações de integridade, modifique as configurações padrão, conforme necessário. Em Configurações avançadas de verificação de integridade, escolha a porta, a contagem, o tempo limite, o intervalo e especifique os códigos de sucesso. Se as verificações de integridade excederem o número de Limite não íntegro, o balanceador de carga tornará o destino inoperante. Quando as verificações de integridade excederem o número de Limite íntegro, o balanceador de carga tornará o destino operacional novamente. Para obter mais informações, consulte ???.
6. (Opcional) Para adicionar uma tag, expanda Tags, escolha Adicionar tag e digite uma chave de tag e um valor de tag.
7. Escolha Próximo.
8. (Opcional) Registrar os destinos. O tipo de destino do grupo de destino define as informações que você fornece. Se você não estiver pronto para registrar os destinos agora, poderá fazê-lo posteriormente.
   - Instâncias: selecione as instâncias EC2, insira as portas e selecione Incluir como pendente abaixo.
   - Endereços IP: selecione a VPC que contém os endereços IP ou Outros endereços IP privados, insira os endereços IP e as portas e selecione Incluir como pendente abaixo.
   - Application Load Balancer: selecione o Application Load Balancer. Para obter mais informações, consulte Usar Application Load Balancers como destinos.

9. Selecione Criar grupo de destino.

AWS CLI

Para criar um grupo de destino

Use o comando create-target-group. O exemplo mostrado a seguir cria um grupo de destino com o protocolo TCP, os destinos registrados por endereço IP, uma tag e as configurações padrão de verificação de integridade.

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type ip \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

Para registrar destinos

Use o comando register-targets para registrar destinos com o grupo de destino. Para obter exemplos, consulte the section called “Registrar destinos”.

CloudFormation

Para criar um grupo de destino

Defina um recurso do tipo AWS::ElasticLoadBalancingV2::TargetGroup. O exemplo a seguir cria um grupo de destino com o protocolo TCP, os destinos registrados por endereço IP, uma tag, as configurações padrão de verificação de integridade e dois destinos registrados.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
```

```
        Value: '123'
    Targets:
      - Id: 10.0.50.10
        Port: 80
      - Id: 10.0.50.20
        Port: 80
```

Atualizar as configurações de integridade do grupo de destino para o Network Load Balancer

Por padrão, os Network Load Balancer monitoram a integridade dos destinos e roteiam as solicitações para destinos íntegros. No entanto, se o balanceador de carga não tiver destinos íntegros suficientes, ele enviará tráfego automaticamente para todos os destinos registrados (falha na abertura). É possível modificar as configurações de integridade do grupo de destino para definir os limites de failover de DNS e failover de roteamento. Para obter mais informações, consulte the section called “Integridade do grupo de destino”.

Console

Para atualizar as configurações de integridade do grupo de destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Balanceamento de carga, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Expanda os requisitos de integridade do grupo de destino.
6. Em Tipo de configuração, recomendamos que você escolha Configuração unificada, que define o mesmo limite para failover de DNS e failover de roteamento.
7. Em Requisitos de estado íntegro, execute uma das seguintes ações:
   - Escolha Contagem mínima de destinos íntegros e, em seguida, insira um número de 1 até o número máximo de destinos para seu grupo de destino.
   - Escolha Porcentagem mínima de destinos íntegros e, em seguida, insira um número de 1 a 100.
8. O texto informativo indica se o balanceamento de carga entre zonas está habilitado para o grupo de destino. Se o balanceamento de carga entre zonas estiver desabilitado, você

poderá habilitá-lo para garantir capacidade suficiente. Em Configuração de seleção de destino, atualize o Balanceamento de carga entre zonas.

O texto a seguir indica que o balanceamento de carga entre zonas está desabilitado:

```
Healthy state requirements apply to each zone independently.
```

O texto a seguir indica que o balanceamento de carga entre zonas está habilitado:

```
Healthy state requirements apply to the total targets across all applicable
 zones.
```

9. Escolha Salvar alterações.

AWS CLI

Para atualizar as configurações de integridade do grupo de destino

Use o comando modify-target-group-attributes. O exemplo a seguir define como 50% o limite de integridade de ambas as ações de estado não íntegro.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \

 "Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50"
 \

 "Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=5
```

CloudFormation

Para modificar configurações de integridade do grupo de destino

Atualize o AWS::ElasticLoadBalancingV2::TargetGrouprecurso. O exemplo a seguir define como 50% o limite de integridade de ambas as ações de estado não íntegro.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
```

```
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_group_health.dns_failover.minimum_healthy_targets.percentage"
          Value: "50"
        - Key:
"target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage"
          Value: "50"
```

Verificações de integridade para grupos de destino do Network Load Balancer

Você pode registrar os destinos com um ou mais grupos de destino. O balanceador de carga inicia as solicitações de roteamento para um destino recém-registrado assim que o processo de registro é concluído e o destino é aprovado nas verificações de integridade iniciais. Pode levar alguns minutos para que o processo de registro seja concluído e as verificações de integridade sejam iniciadas.

Os Network Load Balancers usam verificações de integridade ativas e passivas para determinar se um destino está disponível para lidar com solicitações. Por padrão, cada nó do load balancer roteia solicitações somente para destinos íntegros na sua zona de disponibilidade. Se você habilitar o balanceamento de carga entre zonas, cada nó do load balancer roteará solicitações para destinos íntegros em todas as zonas de disponibilidade habilitadas. Para obter mais informações, consulte Balanceamento de carga entre zonas.

Com as verificações de integridade passivas, o load balancer observa como os destinos respondem às conexões. As verificações de integridade passivas permitem que o load balancer detecte um destino não íntegro antes que ele seja relatado como não íntegro pelas verificações de integridade ativas. Você não pode desabilitar, configurar nem monitorar as verificações de integridade passivas. Não há suporte a verificações de integridade passivas para tráfego UDP e grupos de destino com a persistência ativada. Para obter mais informações, consulte Sessões persistentes.

Se um destino se tornar não íntegro, o balanceador de carga enviará um TCP RST para pacotes recebidos nas conexões de cliente associadas ao destino, a menos que o destino não íntegro acione o balanceador de carga para apresentar falha na abertura.

Se um ou mais grupos de destino não têm um destino íntegro em uma zona de disponibilidade habilitada, removemos o endereço IP da sub-rede correspondente do DNS para que a solicitações não sejam roteadas para destinos nesta zona de disponibilidade. Se todos os destinos falharem nas verificações de integridade ao mesmo tempo em todas as zonas de disponibilidade habilitadas, o balanceador de carga apresentará falha ao abrir. Os Network Load Balancers também falharão quando você tiver um grupo de destino vazio. O efeito da falha na abertura é permitir o tráfego para todos os destinos em todas as zonas de disponibilidade habilitadas, independentemente do seu estado de integridade.

Se um grupo de destino estiver configurado com verificações de integridade de HTTPS, seus destinos registrados falharão nas verificações de integridade se forem compatíveis somente com TLS 1.3. Esses destinos devem ser compatíveis com uma versão anterior do TLS, como o TLS 1.2.

Para solicitações de verificação de integridade HTTP ou HTTPS, o cabeçalho de host contém o endereço IP do nó do load balancer e a porta do listener, não o endereço IP do destino e a porta de verificação de integridade.

Se você adicionar um receptor de TLS ao Network Load Balancer, executaremos um teste de conectividade do receptor. Como o encerramento do TLS também encerra uma conexão TCP, uma nova conexão TCP será estabelecida entre o load balancer e seus destinos. Portanto, talvez você veja as conexões TCP para este teste enviadas do seu balanceador de carga para os destinos registrados com o receptor TLS. É possível identificar essas conexões TCP porque elas têm o endereço IP de origem do seu Network Load Balancer e não contêm pacotes de dados.

Para serviços UDP e QUIC, a disponibilidade do destino pode ser testada usando verificações de integridade não UDP no grupo de destino. Você pode usar qualquer verificação de integridade disponível (TCP, HTTP ou HTTPS) e qualquer porta no destino para verificar a disponibilidade do seu serviço. Se o serviço que recebe a verificação de integridade falhar, o destino será considerado indisponível. Para melhorar a precisão das verificações de integridade do seu serviço, configure a recepção do serviço para a porta de verificação de integridade para acompanhar o status do serviço UDP ou QUIC e parar a verificação de integridade caso o serviço esteja indisponível.

Para obter mais informações, consulte the section called “Integridade do grupo de destino”.

Conteúdo

- Verificar a integridade dos destinos do Network Load Balancer
- Atualizar as configurações da verificação de integridade de um grupo de destino do Network Load Balancer

Configurações de verificação de integridade

Você pode configurar as verificações de integridade ativas para os destinos em um grupo de destino usando as configurações a seguir. Se as verificações de integridade excederem as falhas UnhealthyThresholdCountconsecutivas, o balanceador de carga colocará o alvo fora de serviço. Quando as verificações de integridade excedem os sucessos HealthyThresholdCountconsecutivos, o balanceador de carga coloca o alvo de volta em serviço.

Configuração	Description	Padrão
HealthCheckProtocol	O protocolo que o load balancer usa ao executar verificações de integridade nos destinos. Os protocolos possíveis são HTTP, HTTPS e TCP. O padrão é o protocolo TCP. Se o tipo de destino for `alb`, os protocolo s compatíveis de verificação de integridade serão HTTP e HTTPS.	TCP
HealthCheckPort	A porta que o load balancer usa ao executar verificações de integridade nos destinos. O padrão é usar a porta em que cada destino recebe o tráfego do load balancer.	Porta em que cada destino recebe o tráfego do balanceador de carga.
HealthCheckPath	[Verificações de integridade de HTTP/HTTPS] O caminho da verificação de integridade que é o destino para verificações de integridade. O padrão é /.	/
HealthCheckTimeoutSeconds	O tempo, em segundos, durante o qual ausência de resposta de um destino significa	Seis segundos

Configuração	Description	Padrão
	uma falha na verificação de integridade. O intervalo é de 2 a 120 segundos. Os valores padrão são seis segundos para verificações de integridade de HTTP e dez segundos para verificações de integridade de TCP e HTTPS.	para verificações de integrida de de HTTP e dez segundos para verificações de integrida de de TCP e HTTPS.
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. O padrão é 30 segundos. As verificações de integridade de um Network Load Balancer são distribuídas e usam um mecanismo de consenso para determinar a integridade do destino. Portanto, os destinos recebem mais do que o número configurado de verificações de integridade. Para reduzir o impacto em seus destinos se você estiver usando verificações de integridade HTTP, use um destino mais simples, como um arquivo HTML estático, ou alterne para verificações de integridade TCP.	30 segundos
HealthyThresholdCount	O número de verificações de integridade bem-sucedidas consecutivas necessárias antes de considerar íntegro um destino não íntegro. O intervalo é de 2 a 10. O padrão é 5.	5

Configuração	Description	Padrão
UnhealthyThresholdCount	O número de verificações de integridade consecutivas exigido antes considerar um destino não íntegro. O intervalo é de 2 a 10. O padrão é 2.	2
Matcher	[Verificações de integridade de HTTP/HTTPS] Os códigos HTTP a serem usados ao verificar uma resposta bem-sucedida de um destino. O intervalo é de 200 a 599. O padrão é 200 a 399.	200 – 399

Status de integridade do destino

Antes que o load balancer envie uma solicitação de verificação de integridade para um destino, você deverá registrá-lo com um grupo de destino, especificar o grupo de destino em uma regra do listener e garantir que a Zona de disponibilidade do destino esteja habilitado para o load balancer.

A tabela a seguir descreve os valores possíveis para o status de integridade de um destino registrado.

Valor	Description
`initial`	O load balancer está no processo de registro do destino ou executando as verificações de integridade iniciais no destino. Códigos de motivo relacionados: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	O destino é íntegro. Códigos de motivo relacionados: nenhum

Valor	Description
`unhealthy`	O destino não respondeu a uma verificação de integrida de, falhou em uma verificação de integridade ou está parado. Código de motivo relacionado: `Target.FailedHealthChecks`
`draining`	O destino está cancelando o registro e está acontecendo drenagem da conexão. Código de motivo relacionado: `Target.DeregistrationInProgress`
`unhealthy.draining`	O destino não respondeu a verificações de integridade ou falhou em verificações de integridade e entrou em um período de carência. O destino oferece suporte a conexões existentes e não aceitará novas conexões durante esse período de carência. Código de motivo relacionado: `Target.FailedHealthChecks`
`unavailable`	A integridade do destino não está disponível. Código de motivo relacionado: `Elb.InternalError`
`unused`	O destino não está registrado com um grupo de destino, o grupo de destino não é usado em uma regra de receptor ou o destino está em uma Zona de disponibi lidade que não está habilitada. Códigos de motivo relacionados: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`

Códigos de motivo de verificação de integridade

Se o status de um destino for qualquer valor diferente de `Healthy`, a API retornará um código de motivo e uma descrição do problema; o console exibirá a mesma descrição em uma dica de ferramenta. Observe que os códigos de motivo que começarem com `Elb` são originados no load balancer, e os códigos de motivo que começarem com `Target` são originados no destino.

Código do motivo	Description
`Elb.InitialHealthChecking`	Verificações de integridade iniciais em andamento
`Elb.InternalError`	As verificações de integridade falharam devido a um erro interno
`Elb.RegistrationInProgress`	O registro do destino está em andamento
`Target.DeregistrationInProgress`	O cancelamento do registro do destino está em andamento
`Target.FailedHealthChecks`	Verificações de integridade com falha
`Target.InvalidState`	O destino está no estado interrompido O destino está no estado encerrado O destino está no estado encerrado ou interrompido O destino está em um estado inválido
`Target.IpUnusable`	O endereço IP não pode ser usado como um destino, uma vez que está sendo usado por um load balancer.
`Target.NotInUse`	O grupo de destino não está configurado para receber tráfego do load balancer O destino está em uma Zona de disponibilidade que não está habilitada para o load balancer
`Target.NotRegistered`	O destino não está registrado no grupo de destino

Verificar a integridade dos destinos do Network Load Balancer

Você pode verificar a integridade dos destinos registrados com seus grupos de destino. Para obter ajuda com falhas na verificação de integridade, consulte Solução de problemas: um destino registrado não está em serviço.

Console

Para verificar a integridade de seus destinos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Balanceamento de carga, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. A guia Detalhes exibe o número total de destinos, mais o número de destinos para cada status de integridade.
5. Na guia Destinos, a coluna Status da integridade indica o status de cada destino.
6. Se o status de um destino for qualquer valor diferente de `Healthy`, a coluna Detalhes do status da integridade conterá mais informações.

Como receber notificações por e-mail sobre destinos não íntegros

Use CloudWatch alarmes para acionar uma função Lambda para enviar detalhes sobre alvos não íntegros. Para step-by-step obter instruções, consulte a seguinte postagem no blog: Identificação de alvos não íntegros do seu balanceador de carga.

AWS CLI

Para verificar a integridade de seus destinos

Use o comando describe-target-health. Este exemplo filtra a saída para incluir somente destinos que não estejam íntegros. Para destinos que não estão íntegros, a saída inclui um código do motivo.

```
aws elbv2 describe-target-health \
    --target-group-arn target-group-arn \
    --query "TargetHealthDescriptions[?TargetHealth.State!='healthy'].
[Target.Id,TargetHealth.State,TargetHealth.Reason]" \
    --output table
```

O seguinte é um exemplo de saída.

```
-----------------------------------------------
|            DescribeTargetHealth             |
+--------------+---------+-------------------+
|  172.31.0.57 |  unused |  Target.NotInUse  |
|  172.31.0.50 |  unused |  Target.NotInUse  |
+--------------+---------+-------------------+
```

Estados destino e códigos do motivo

A lista mostrada a seguir apresenta os códigos do motivo possíveis para cada estado de destino.

O estado de destino é healthy

Um código do motivo não é fornecido.

O estado de destino é initial

- `Elb.RegistrationInProgress`: o destino está em processo de registro no balanceador de carga.
- `Elb.InitialHealthChecking`: O balanceador de carga ainda está enviando ao destino o número mínimo de verificações de integridade necessárias para determinar seu status de integridade.

O estado de destino é unhealthy

- `Target.FailedHealthChecks`: O balanceador de carga recebeu um erro ao estabelecer uma conexão com o destino ou a resposta do destino foi malformada.

O estado de destino é unused

- `Target.NotRegistered`: O destino não está registrado no grupo de destino
- `Target.NotInUse`: O grupo de destino não é usado por nenhum balanceador de carga ou o destino está em uma zona de disponibilidade que não está habilitada para seu balanceador de carga.
- `Target.InvalidState`: O destino está no estado encerrado ou interrompido.
- `Target.IpUnusable`: O endereço IP de destino é reservado para uso por um balanceador de carga.

O estado de destino é draining

- `Target.DeregistrationInProgress`: O destino está em processo de cancelamento de registro e o período de atraso do cancelamento do registro não expirou.

O estado de destino é unavailable

- `Elb.InternalError`: a integridade do destino não está disponível devido a um erro interno.

Atualizar as configurações da verificação de integridade de um grupo de destino do Network Load Balancer

Você pode atualizar as configurações de verificação de integridade do grupo de destino a qualquer momento. Para visualizar a lista de configurações de verificação de integridade, consulte the section called “Configurações de verificação de integridade”.

Console

Para atualizar as configurações de verificação de integridade

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Balanceamento de carga, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Verificações de integridade, selecione Editar.
5. Na página Editar configurações da verificação de integridade, modifique as configurações conforme necessário.
6. Escolha Salvar alterações.

AWS CLI

Para atualizar as configurações de verificação de integridade

Use o comando modify-target-group. O exemplo a seguir atualiza HealthyThresholdCountas HealthCheckTimeoutSecondsconfigurações e.

```
aws elbv2 modify-target-group \
    --target-group-arn target-group-arn \
    --healthy-threshold-count 3 \
```

```
    --health-check-timeout-seconds 20
```

CloudFormation

Para atualizar as configurações de verificação de integridade

Atualize o AWS::ElasticLoadBalancingV2::TargetGrouprecurso para incluir as configurações atualizadas da verificação de saúde. O exemplo a seguir atualiza HealthyThresholdCountas HealthCheckTimeoutSecondsconfigurações e.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      HealthyThresholdCount: 3
      HealthCheckTimeoutSeconds: 20
```

Editar os atributos do grupo de destino para o Network Load Balancer

Após criar um grupo de destino para o Network Load Balancer, você poderá editar os atributos do grupo de destino.

Atributos do grupo de destino

- Preservação do IP do cliente
- Atraso do cancelamento do registro
- Protocolo de proxy
- Sessões persistentes
- Balanceamento de carga entre zonas para grupos de destino
- Encerramento da conexão para destinos não íntegros
- Intervalo de drenagem de não íntegros

Preservação do IP do cliente

Os Network Load Balancers podem preservar os endereços IP de origem dos clientes ao rotear solicitações para destinos de backend. Quando você desabilita a preservação do IP do cliente, o endereço IP de origem é o endereço IP privado do Network Load Balancer.

Por padrão, a preservação do IP do cliente está habilitada (e não pode ser desabilitada) para grupos de destino de tipo de instância e de IP com os protocolos UDP, TCP_UDP, QUIC e TCP_QUIC. No entanto, você pode habilitar ou desabilitar a preservação do IP do cliente para grupos de destino TCP e TLS usando o atributo do grupo de destino `preserve_client_ip.enabled`.

Configurações padrão

- Grupos de destino de tipo de instância: habilitados
- Grupos de destino de tipo IP (UDP, TCP_UDP, QUIC, TCP_QUIC): habilitados
- Grupos de destino do tipo IP (TCP, TLS): desabilitados

Quando a preservação do IP do cliente está habilitada

A tabela a seguir descreve os endereços IP que os destinos recebem quando a preservação do IP do cliente está habilitada.

Destinos	IPv4 solicitações de clientes	IPv6 solicitações de clientes
Tipo de instância (IPv4)	IPv4 Endereço do cliente	Endereço do balanceador IPv4 de carga
Tipo de IP (IPv4)	IPv4 Endereço do cliente	Endereço do balanceador IPv4 de carga
Tipo de IP (IPv6)	Endereço do balanceador IPv6 de carga	IPv6 Endereço do cliente

Quando a preservação do IP do cliente está desabilitada

A tabela a seguir descreve os endereços IP que os destinos recebem quando a preservação do IP do cliente está desabilitada.

Destinos	IPv4 solicitações de clientes	IPv6 solicitações de clientes
Tipo de instância (IPv4)	Endereço do balanceador IPv4 de carga	Endereço do balanceador IPv4 de carga
Tipo de IP (IPv4)	Endereço do balanceador IPv4 de carga	Endereço do balanceador IPv4 de carga
Tipo de IP (IPv6)	Endereço do balanceador IPv6 de carga	Endereço do balanceador IPv6 de carga

Requisitos e considerações

- As alterações da preservação do IP do cliente só entram em vigor para novas conexões TCP.
- Quando a preservação do IP do cliente está habilitada, o tráfego deve fluir diretamente do Network Load Balancer para o destino. O destino deve estar localizado na mesma VPC do balanceador de carga ou em uma VPC emparelhada na mesma região.
- Não há suporte à preservação de IP do cliente quando os destinos são acessados por meio de um gateway de trânsito.
- Não há suporte para a preservação de IP do cliente quando é usado um endpoint do balanceador de carga do gateway para inspecionar o tráfego entre o Network Load Balancer e o destino (instância ou endereço IP), mesmo que o destino esteja na mesma VPC que o Network Load Balancer.
- Os tipos de instância a seguir não oferecem suporte à preservação do IP do cliente: C1 CC1 CC2, CG1, CG2, CR1,,,,, C1, HI1, M2 HS1, M3 e T1. Recomendamos que você registre esses tipos de instância como endereços IP, com a preservação do IP do cliente desabilitada.
- A preservação do IP do cliente não afeta o tráfego de entrada de AWS PrivateLink. O endereço IP de origem do AWS PrivateLink tráfego é sempre o endereço IP privado do Network Load Balancer.
- A preservação do IP do cliente não é compatível quando um grupo de destino contém interfaces de rede do AWS PrivateLink ou a interface de rede de outro Network Load Balancer. Isso causa perda de comunicação com esses destinos.
- A preservação do IP do cliente não afeta o tráfego convertido de IPv6 para IPv4. O endereço IP de origem desse tipo de tráfego é sempre o endereço IP privado do Network Load Balancer.
- Quando você especifica destinos por tipo de Application Load Balancer, o IP do cliente de todo o tráfego de entrada é preservado pelo Network Load Balancer e enviado ao Application Load

Balancer. Em seguida, o Application Load Balancer anexa o IP do cliente ao cabeçalho de solicitação `X-Forwarded-For` antes de enviá-lo ao destino.

- O loopback NAT, também conhecido como hairpinning, não é compatível quando a preservação do IP do cliente está habilitada. Isso ocorre ao usar Network Load Balancers internos e o destino registrado atrás de um Network Load Balancer cria conexões com o mesmo Network Load Balancer. A conexão pode ser roteada para o destino que está tentando criar a conexão, levando a erros de conexão. Recomendamos não conectar a um Network Load Balancer a partir de destinos por trás do mesmo Network Load Balancer. Como opção, você também pode evitar esse tipo de erro de conexão ao desabilitar a preservação do IP do cliente. Se precisar do endereço IP do cliente, você poderá recuperá-lo usando o Proxy Protocol v2. Para obter mais informações, consulte Protocolo de proxy.
- Quando a preservação do IP do cliente está desabilitada, o Network Load Balancer pode oferecer suporte a 55 mil conexões simultâneas ou a cerca de 55 mil conexões por minuto para cada destino exclusivo (endereço IP e porta). Se você exceder essas conexões, existirá uma probabilidade maior de erros de alocação de porta, resultando em falhas para o estabelecimento de novas conexões. Para obter mais informações, consulte Erros de alocação de porta para fluxos de backend.

Console

Para modificar a preservação do IP do cliente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Atributos, selecione Editar e localize o painel Configuração de tráfego.
5. Para habilitar a preservação do IP do cliente, ative Preservar endereços IP do cliente. Para desabilitar a preservação do IP do cliente, desative Preservar endereços IP do cliente.
6. Escolha Salvar alterações.

AWS CLI

Para habilitar a preservação do IP do cliente

Use o comando modify-target-group-attributes com o atributo `preserve_client_ip.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=preserve_client_ip.enabled,Value=true"
```

CloudFormation

Para habilitar a preservação do IP do cliente

Atualize o AWS::ElasticLoadBalancingV2::TargetGroup recurso para incluir o `preserve_client_ip.enabled` atributo.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "preserve_client_ip.enabled"
          Value: "true"
```

Atraso do cancelamento do registro

Quando você cancela o registro de um destino, o balanceador de carga interrompe a criação de novas conexões para o destino. O load balancer usa a diminuição de conexão para garantir que o tráfego em trânsito seja concluído nas conexões existentes. Se o destino com o registro cancelado permanecer íntegro e uma conexão existente não estiver ociosa, o balanceador de carga poderá continuar enviando tráfego para o destino. Para garantir que essas conexões existentes sejam fechadas, você pode executar uma das ações a seguir: habilitar o atributo do grupo de destino para encerramento de conexões, garantir que a instância não esteja íntegra antes de cancelar o registro dela ou fechar periodicamente conexões de clientes.

O estado inicial de um destino em cancelamento de registro é `draining`, período durante o qual o destino deixará de receber novas conexões. No entanto, o destino ainda poderá receber conexões devido ao atraso na propagação da configuração. Por padrão, o load balancer altera o estado de um destino que terá o registro cancelado para `unused` após 300 segundos. Para alterar a quantidade

de tempo que o load balancer aguarda antes de alterar o estado de um destino que terá o registro cancelado para `unused`, atualize o valor de atraso do cancelamento do registro. Recomendamos que você especifique um valor de, pelo menos, 120 segundos para garantir que as solicitações sejam concluídas. Para tráfego QUIC, o valor é sempre 300 segundos e não pode ser ajustado.

Se você habilitar o atributo do grupo de destino para encerramento de conexões, as conexões com destinos com registros cancelados serão fechadas logo após o final do tempo limite de cancelamento do registro.

Console

Para modificar os atributos de atraso do cancelamento de registro

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Para alterar o tempo limite de cancelamento do registro, insira um novo valor para Atraso do cancelamento de registro. Para garantir que as conexões existentes sejam fechadas após o cancelamento do registro dos destinos, selecione Encerrar conexões no cancelamento do registro.
6. Escolha Salvar alterações.

AWS CLI

Para modificar os atributos de atraso do cancelamento de registro

Use o modify-target-group-attributescomando com `deregistration_delay.timeout_seconds` os `deregistration_delay.connection_termination.enabled` atributos e.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \
      "Key=deregistration_delay.timeout_seconds,Value=60" \
      "Key=deregistration_delay.connection_termination.enabled,Value=true"
```

CloudFormation

Para modificar os atributos de atraso do cancelamento de registro

Atualize o AWS::ElasticLoadBalancingV2::TargetGrouprecurso para incluir `deregistration_delay.timeout_seconds` os `deregistration_delay.connection_termination.enabled` atributos e.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "deregistration_delay.timeout_seconds"
          Value: "60"
        - Key: "deregistration_delay.connection_termination.enabled"
          Value: "true"
```

Protocolo de proxy

Os Network Load Balancers usam o protocolo de proxy versão 2 para enviar informações de conexão adicionais, como a origem e o destino. O Proxy Protocol versão 2 oferece uma codificação binária do cabeçalho do Proxy Protocol.

Com receptores de TCP, o balanceador de carga acrescenta um cabeçalho do protocolo de proxy aos dados de TCP. Ele não descarta nem substitui os dados existentes, inclusive cabeçalhos do protocolo de proxy enviados pelo cliente ou quaisquer outros proxies, balanceadores de carga ou servidores no caminho da rede. Portanto, é possível receber mais de um cabeçalho do Proxy Protocol. Além disso, se houver outro caminho de rede para os destinos fora do Network Load Balancer, o primeiro cabeçalho do protocolo de proxy pode não ser o do balanceador de carga.

Os receptores TLS não oferecem suporte a conexões de entrada com cabeçalhos de protocolo de proxy enviados pelo cliente ou por quaisquer outros proxies.

O tráfego QUIC não é compatível com a versão 2 do protocolo proxy.

Se você especificar destinos por endereço IP, os endereços IP de origem fornecidos às suas aplicações dependerão do protocolo do grupo de destino, da seguinte forma:

- TCP e TLS: por padrão, a preservação do IP do cliente é desabilitada e os endereços IP de origem fornecidos para suas aplicações são os endereços IP privados dos nós do balanceador de carga. Para preservar o endereço IP do cliente, certifique-se de que o destino esteja localizado na mesma VPC ou em uma VPC pareada e habilite a preservação do IP do cliente. Se o endereço IP do cliente for necessário e essas condições ainda não foram atendias, habilite o protocolo de proxy e obtenha o endereço IP dos clientes no cabeçalho do protocolo de proxy.
- UDP e TCP_UDP: os endereços IP de origem são os endereços IP dos clientes, pois a preservação do IP do cliente é habilitada por padrão para esses protocolos e não pode ser desabilitada. Se você especificar destinos por ID de instância, os endereços IP de origem fornecidos aos aplicativos serão os endereços IP dos clientes. No entanto, se preferir, você poderá ativar o Proxy Protocol e obter os endereços IP dos clientes que se encontram no cabeçalho do Proxy Protocol.

Conexões de verificação de integridade

Depois que habilitar o Proxy Protocol, o cabeçalho do Proxy Protocol também será incluído nas conexões de verificação de integridade do load balancer. No entanto, com conexões de verificação de integridade, as informações de conexão do cliente não serão enviadas no cabeçalho do Proxy Protocol.

Os destinos podem falhar nas verificações de integridade se não conseguirem analisar o cabeçalho do protocolo proxy. Por exemplo, eles podem apresentar o seguinte erro: HTTP 400: Solicitação inválida.

Serviços do VPC endpoint

Para o tráfego oriundo dos consumidores de serviço por meio de um serviço do VPC endpoint, os endereços IP de origem fornecidos aos seus aplicativos são os endereços IP privados dos nós do load balancer. Se os seus aplicativos precisam dos endereços IP dos consumidores de serviço, habilite o Proxy Protocol e obtenha os endereços IP no cabeçalho do Proxy Protocol.

O cabeçalho do Proxy Protocol também inclui o ID do endpoint. Essas informações são codificadas usando um vetor personalizado Type-Length-Value (TLV) da seguinte forma.

Campo	Comprimento (em octetos)	Description
Tipo	1	PP2_TYPE_AWS (0xEA)
Length	2	O comprimento do valor
Valor	1	PP2_SUBTIPO_ (0x01AWS_VPCE_ID)
	variável (comprimento do valor menos 1)	O ID do endpoint

Para obter um exemplo que analisa o tipo TLV 0xEA, consulte/. https://github.com/aws/ elastic-load-balancing-tools tree/master/proprot

Habilitar o Proxy Protocol

Antes de habilitar o Proxy Protocol em um grupo de destino, certifique-se de que os aplicativos esperem e possam analisar o cabeçalho do Proxy Protocol v2. Caso contrário, poderá haver falha neles. Para obter mais informações, consulte o Proxy Protocol versões 1 e 2.

Console

Para habilitar a versão 2 do protocolo proxy

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir a página de detalhes dele.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos, selecione Protocolo de proxy v2.
6. Escolha Salvar alterações.

AWS CLI

Para habilitar a versão 2 do protocolo proxy

Use o comando modify-target-group-attributes com o atributo `proxy_protocol_v2.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=proxy_protocol_v2.enabled,Value=true"
```

CloudFormation

Para habilitar a versão 2 do protocolo proxy

Atualize o AWS::ElasticLoadBalancingV2::TargetGroup recurso para incluir o `proxy_protocol_v2.enabled` atributo.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "proxy_protocol_v2.enabled"
          Value: "true"
```

Sessões persistentes

As sticky sessions são um mecanismo para rotear tráfego de clientes para o mesmo destino em um grupo de destino. Isso é útil para servidores que mantêm as informações de estado em ordem para fornecer uma experiência contínua aos clientes.

Considerações

- O uso de sticky sessions pode levar a uma distribuição desigual de conexões e de fluxos, o que pode afetar a disponibilidade dos destinos. Por exemplo, todos os clientes atrás do mesmo dispositivo NAT têm o mesmo endereço IP de origem. Portanto, todo o tráfego desses clientes é roteado para o mesmo destino.
- O load balancer poderá redefinir as sticky sessions de um grupo de destino se o estado de integridade de qualquer um de seus destinos mudar ou se você registrar ou cancelar o registro de destinos com o grupo de destino.

- Quando o atributo de persistência é ativado para um grupo de destino, as verificações de integridade passivas não são aceitas. Para obter mais informações, consulte Verificações de integridade para seus grupos de destino.
- Sessões persistentes não são compatíveis com receptores TLS ou QUIC.

Console

Para habilitar a sessão persistente

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Em Configuração da seleção do destino, ative Perdurabilidade.
6. Escolha Salvar alterações.

AWS CLI

Para habilitar a sessão persistente

Use o comando modify-target-group-attributes com o atributo `stickiness.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=stickiness.enabled,Value=true"
```

CloudFormation

Para habilitar a sessão persistente

Atualize o AWS::ElasticLoadBalancingV2::TargetGroup recurso para incluir o `stickiness.enabled` atributo.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
```

```
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "stickiness.enabled"
          Value: "true"
```

Balanceamento de carga entre zonas para grupos de destino

Os nós do load balancer distribuem solicitações de clientes para destinos registrados. Quando o balanceamento de carga entre zonas estiver ativado, cada nó do balanceador de carga distribuirá o tráfego aos destinos registrados em todas as zonas de disponibilidade registradas. Quando o balanceamento de carga entre zonas estiver desativado, cada nó do balanceador de carga distribuirá o tráfego somente para os destinos registrados na respectiva zona de disponibilidade. Isso poderá ser usado se os domínios de falha zonais forem preferidos com relação aos regionais, garantindo que uma zona íntegra não seja afetada por uma zona não íntegra ou para melhorias gerais na latência.

Com Network Load Balancers, o balanceamento de carga entre zonas fica desabilitado por padrão no nível do balanceador de carga, mas você pode habilitá-lo a qualquer momento. Para grupos de destino, o padrão é usar a configuração do balanceador de carga, mas você pode substituir o padrão habilitando ou desabilitando explicitamente o balanceamento de carga entre zonas em nível de grupo de destino.

Considerações

- Ao habilitar o balanceamento de carga entre zonas para um Network Load Balancer, as tarifas de transferência de dados do EC2 são aplicáveis. Para obter mais informações, consulte Como entender as cobranças de transferência dados no Guia do usuário de exportações de dados da AWS .
- A configuração do grupo de destino determina o comportamento de balanceamento de carga do grupo de destino. Por exemplo, se o balanceamento de carga entre zonas estiver habilitado em nível de balanceador de carga e desabilitado em nível de grupo de destino, o tráfego enviado ao grupo de destino não será roteado entre as zonas de disponibilidade.
- Quando o balanceamento de carga entre zonas estiver desabilitado, verifique se você tem capacidade de destino suficiente em cada uma das zonas de disponibilidade do balanceador de carga para que cada zona possa fornecer a workload associada.

- Quando o balanceamento de carga entre zonas estiver desabilitado, certifique-se de que todos os grupos de destino participem das mesmas zonas de disponibilidade. Uma zona de disponibilidade vazia é considerada não íntegra.
- Você poderá habilitar ou desabilitar o balanceamento de carga entre zonas em nível de grupo de destino se o tipo do grupo de destino for `instance` ou `ip`. Se o tipo de grupo de destino for `alb`, o grupo de destino sempre herdará do balanceador de carga a configuração de balanceamento de carga entre zonas.

Para saber mais sobre como habilitar o balanceamento de carga entre zonas no balanceador de carga, consulte the section called “Balanceamento de carga entre zonas”.

Console

Para modificar o balanceamento de carga entre zonas para um grupo de destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Balanceamento de carga, escolha Grupos de destino.
3. Selecione o nome do grupo de destino para abrir a página de detalhes dele.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do grupo de destino, selecione Ativado para Balanceamento de carga entre zonas.
6. Escolha Salvar alterações.

AWS CLI

Para modificar o balanceamento de carga entre zonas para um grupo de destino

Use o comando modify-target-group-attributes com o atributo `load_balancing.cross_zone.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Para modificar o balanceamento de carga entre zonas para um grupo de destino

Atualize o AWS::ElasticLoadBalancingV2::TargetGroup recurso para incluir o `load_balancing.cross_zone.enabled` atributo.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Encerramento da conexão para destinos não íntegros

O encerramento da conexão é habilitado por padrão. Quando o destino de um Network Load Balancer falha nas verificações de integridade configuradas e é considerado não íntegro, o balanceador de carga encerra as conexões estabelecidas e interrompe o roteamento de novas conexões para o destino. Com o encerramento da conexão desabilitado, o destino ainda é considerado não íntegro e não aceita novas conexões, mas as conexões estabelecidas são mantidas ativas, permitindo que elas sejam fechadas suavemente.

O encerramento da conexão para destinos não íntegros é configurado por grupo de destino.

Console

Para modificar o atributo de encerramento da conexão

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Balanceamento de carga, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Em Gerenciamento de estado não íntegro do destino, escolha se a opção Encerrar conexões quando os destinos se tornarem não íntegros está habilitada ou desabilitada.
6. Escolha Salvar alterações.

AWS CLI

Para desabilitar o atributo de encerramento da conexão

Use o comando modify-target-group-attributes com o atributo `target_health_state.unhealthy.connection_termination.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.connection_termination.enabled,Value=false"
```

CloudFormation

Para desabilitar o atributo de encerramento da conexão

Atualize o AWS::ElasticLoadBalancingV2::TargetGroup recurso para incluir o `target_health_state.unhealthy.connection_termination.enabled` atributo.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.connection_termination.enabled"
          Value: "false"
```

Intervalo de drenagem de não íntegros

Os destinos no estado `unhealthy.draining` são considerados não íntegros, não recebem novas conexões, mas mantêm as conexões estabelecidas ao longo do intervalo configurado. O intervalo de conexão não íntegra determina a quantidade de tempo que o destino permanece no estado `unhealthy.draining` antes de passar a `unhealthy`. Se o destino passar nas verificações de integridade durante o intervalo de conexão não íntegra, seu estado voltará a ser `healthy`. Se um cancelamento de registro for acionado, o estado de destino se tornará `draining` e o tempo limite de atraso do cancelamento de registro começará.

Requisito

O encerramento da conexão deve ser desabilitado antes da habilitação do intervalo de drenagem de não íntegros.

Console

Para modificar o intervalo de drenagem não íntegra

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Balanceamento de carga, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Em Gerenciamento de estado não íntegro dos destinos, certifique-se de que a opção Encerrar conexões quando os destinos se tornarem não íntegros esteja desativada.
6. Insira um valor para Intervalo de drenagem de não íntegros.
7. Escolha Salvar alterações.

AWS CLI

Para modificar o intervalo de drenagem não íntegra

Use o comando modify-target-group-attributes com o atributo `target_health_state.unhealthy.draining_interval_seconds`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.draining_interval_seconds,Value=60"
```

CloudFormation

Para modificar o intervalo de drenagem não íntegra

Atualize o AWS::ElasticLoadBalancingV2::TargetGroup recurso para incluir o `target_health_state.unhealthy.draining_interval_seconds` atributo.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
```

```
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.draining_interval_seconds"
          Value: "60"
```

Registrar destinos para o Network Load Balancer

Quando o destino estiver pronto para processar solicitações, registre-o em um ou mais grupos de destino. O tipo de destino do grupo de destino determina como você registra os destinos. Por exemplo, você pode registrar uma instância IDs, endereços IP ou um Application Load Balancer. O Network Load Balancer inicia as solicitações de roteamento para os destinos assim que o processo de registro é concluído e o destino é aprovado nas verificações de integridade iniciais. Pode levar alguns minutos para que o processo de registro seja concluído e as verificações de integridade sejam iniciadas. Para obter mais informações, consulte Verificações de integridade para grupos de destino do Network Load Balancer.

Se a demanda em seus destinos atualmente registrados aumentar, você pode registrar destinos adicionais para lidar com a demanda. Se a demanda nos alvos registrados diminuir, será possível cancelar o registro de alvos do grupo de destino. Pode levar alguns minutos para que o processo de cancelamento do registro seja concluído e para que o load balancer interrompa as solicitações de roteamento para o destino. Se a demanda aumentar posteriormente, será possível registrar novamente os alvos que cancelaram o registro no grupo de destino. Se você precisar atender um destino, poderá cancelar o registro e registrá-lo novamente quando a manutenção estiver concluída.

Quando você cancelar o registro de um destino, o Elastic Load Balancing esperará até que as solicitações em andamento sejam concluídas. Isso é conhecido como drenagem de conexão. O status de um destino é `draining` enquanto a drenagem de conexão estiver em andamento. Depois que o cancelamento do registro for concluído, o status do destino será alterado para `unused`. Para obter mais informações, consulte Atraso do cancelamento do registro.

Se você estiver registrando destinos por ID de instância, poderá usar o balanceador de carga com um grupo do Auto Scaling. Depois de 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 automaticamente registradas no grupo de destino. Se você desvincular o balanceador de carga

do grupo do Auto Scaling, as instâncias terão o registro automaticamente cancelado do grupo de destino. Para obter mais informações, consulte Anexar um balanceador de carga ao seu grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

Conteúdo

Grupos de segurança de destino

Antes de adicionar destinos ao seu grupo de destino, configure os grupos de segurança associados aos destinos para aceitar o tráfego do Network Load Balancer.

Recomendações para grupos de segurança de destino se o balanceador de carga tiver um grupo de segurança associado

- Para permitir tráfego do cliente: adicione uma regra que faça referência ao grupo de segurança associado ao balanceador de carga.
- Para permitir PrivateLink tráfego: se você configurou o balanceador de carga para avaliar as regras de entrada para o tráfego enviado AWS PrivateLink, adicione uma regra que aceite o tráfego do grupo de segurança do balanceador de carga na porta de tráfego. Caso contrário, adicione uma regra que aceite tráfego dos endereços IP privados do balanceador de carga na porta de tráfego.
- Para aceitar verificações de integridade do balanceador de carga: adicione uma regra que aceite tráfego de verificação de integridade dos grupos de segurança do balanceador de carga na porta de verificação de integridade.

Recomendações para grupos de segurança de destino se o balanceador de carga não estiver associado a um grupo de segurança

- Para permitir tráfego do cliente: se o balanceador de carga preservar os endereços IP do cliente, adicione uma regra que aceite o tráfego dos endereços IP dos clientes aprovados na porta de tráfego. Caso contrário, adicione uma regra que aceite tráfego dos endereços IP privados do balanceador de carga na porta de tráfego.

- Para permitir PrivateLink tráfego: adicione uma regra que aceite tráfego dos endereços IP privados do balanceador de carga na porta de tráfego.
- Para aceitar verificações de integridade do balanceador de carga: adicione uma regra que aceite tráfego de verificação de integridade dos endereços IP privados do balanceador de carga na porta de verificação de integridade.

Como a preservação do IP do cliente funciona

Os Network Load Balancers não preservam os endereços IP do cliente, a menos que você defina o atributo `preserve_client_ip.enabled` como `true`. Além disso, com balanceadores de carga de rede de pilha dupla, a preservação do endereço IP do cliente não funciona ao traduzir IPv4 endereços para ou para IPv6 endereços. IPv6 IPv4 A preservação do endereço IP do cliente só funciona quando os endereços IP do cliente e do destino são ambos IPv4 ou ambos IPv6.

Para encontrar os endereços IP privados do balanceador de carga usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Network Interfaces.
3. No campo de pesquisa, insira o nome do Network Load Balancer. Há uma interface de rede por sub-rede do load balancer.
4. Na guia Detalhes de cada interface de rede, copie o endereço de IPv4 Endereço privado.

Para obter mais informações, consulte Atualizar os grupos de segurança para o Network Load Balancer.

Rede ACLs

Ao registrar instâncias do EC2 como destinos, você deve garantir que a rede das sub-redes ACLs de suas instâncias permita tráfego na porta do ouvinte e na porta de verificação de integridade. A lista de controle de acesso (ACL) à rede padrão para uma VPC permite todo o tráfego de entrada e saída. Se você criar uma rede personalizada ACLs, verifique se ela permite o tráfego adequado.

A rede ACLs associada às sub-redes das suas instâncias deve permitir o seguinte tráfego para um balanceador de carga voltado para a Internet.

Regras recomendadas para sub-redes de instância

Inbound

Origem	Protocolo	Intervalo de portas	Comentário
Client IP addresses	*listener*	*target port*	Permitir tráfego de clientes (preservação de IP:0N)
VPC CIDR	*listener*	*target port*	Permitir tráfego de clientes (preservação de IP:0FF)
VPC CIDR	*health check*	*health check*	Permitir tráfego de verificação de integridade

Outbound

Destination (Destino)	Protocolo	Intervalo de portas	Comentário
Client IP addresses	*listener*	1024-65535	Permitir tráfego de retorno ao cliente (preservação de IP:0N)
VPC CIDR	*listener*	1024-65535	Permitir tráfego de retorno ao cliente (preservação de IP:0FF)
VPC CIDR	*health check*	1024-65535	Permitir tráfego de verificação de integridade

A rede ACLs associada às sub-redes do seu balanceador de carga deve permitir o seguinte tráfego para um balanceador de carga voltado para a Internet.

Regras recomendadas para sub-redes do load balancer

Inbound

Origem	Protocolo	Intervalo de portas	Comentário
Client IP addresses	*listener*	*listener*	Permitir tráfego de clientes
VPC CIDR	*listener*	1024-65535	Permitir resposta do alvo
VPC CIDR	*health check*	1024-65535	Permitir tráfego de verificação de integridade

Outbound

Destination (Destino)	Protocolo	Intervalo de portas	Comentário
Client IP addresses	*listener*	1024-65535	Permitir respostas aos clientes
VPC CIDR	*listener*	*target port*	Permitir solicitações aos alvos
VPC CIDR	*health check*	*health check*	Permitir a verificação de integridade dos alvos

Para um balanceador de carga interno, a rede ACLs das sub-redes de suas instâncias e nós do balanceador de carga deve permitir tráfego de entrada e saída de e para o CIDR da VPC, na porta do ouvinte e nas portas efêmeras.

Sub-redes compartilhadas

Os participantes podem criar um Network Load Balancer em uma VPC compartilhada. Os participantes não podem registrar um destino executado em uma sub-rede que não seja compartilhada com eles.

Sub-redes compartilhadas para balanceadores de carga de rede são suportadas em todas as AWS regiões, exceto:

- Ásia-Pacífico (Osaka) `ap-northeast-3`
- Ásia-Pacífico (Hong Kong) `ap-east-1`
- Oriente Médio (Bahrein) `me-south-1`
- AWS China (Pequim) `cn-north-1`
- AWS China (Ningxia) `cn-northwest-1`

Registrar destinos

Cada grupo de destino deve ter pelo menos um destino registrado em cada zona de disponibilidade que é habilitada para o load balancer.

O tipo de destino do seu grupo de destino determina quais destinos você pode registrar. Para obter mais informações, consulte Target type. Use as informações abaixo para registrar os destinos com um grupo de destino do tipo `instance` ou `ip`. Se o tipo de destino for `alb`, consulte Usar Application Load Balancers como destinos.

Requisitos e considerações

- Uma instância deve estar no estado `running` quando você registrá-la.
- Você não pode registrar instâncias por ID de instância se elas usarem um dos seguintes tipos de instância: C1,, CC1,, CC2, CG1, CG2, CR1, G1,,, M1 HI1, M2 HS1, M3 ou T1.
- Ao registrar destinos por ID da instância, as instâncias devem estar na mesma VPC que o Network Load Balancer. Não será possível registrar instâncias por ID de instância se elas estiverem em uma VPC emparelhada com a VPC do balanceador de carga (mesma região ou região diferente). Você poderá registrar essas instâncias pelo endereço IP.
- Ao registrar destinos por ID de instância para um grupo de IPv6 destino, os destinos devem ter um IPv6 endereço principal atribuído. Para saber mais, consulte os IPv6 endereços no Guia do usuário do Amazon EC2
- Ao registrar destinos por endereço IP para um grupo de IPv4 destino, os endereços IP que você registra devem ser de um dos seguintes blocos CIDR:
  - As sub-redes da VPC do grupo de destino
  - 10.0.0.0/8 (RFC 1918)
  - 100.64.0.0/10 (RFC 6598)
  - 172.16.0.0/12 (RFC 1918)

  - 192.168.0.0/16 (RFC 1918)
- Ao registrar destinos por endereço IP para um grupo de IPv6 destino, os endereços IP que você registra devem estar dentro do bloco CIDR da IPv6 VPC ou dentro do bloco CIDR de uma VPC IPv6 emparelhada.
- Se você registrar um destino por endereço IP e o endereço IP estiver na mesma VPC que o load balancer, o load balancer verificará se ele é de uma sub-rede que ele possa acessar.
- Para grupos de destino UDP, TCP_UDP, QUIC e TCP_QUIC, não registre instâncias por endereço IP se elas residirem fora da VPC do balanceador de carga ou se usarem um dos seguintes tipos de instância: C1,,,,,,, G1,,,, M1, M2 CC1 CC2 CG1 CG2 CR1, M3 ou T1. HI1 HS1 Destinos que residem fora da VPC do balanceador de carga ou que usam um tipo de instância incompatível podem receber tráfego do balanceador de carga, mas não conseguem responder.

Requisitos e considerações específicos do QUIC

- Todos os destinos registrados em um grupo de destino QUIC ou TCP_QUIC precisam ter uma ID de servidor especificada.
- O servidor IDs deve ser exclusivo para todos os destinos existentes em um ouvinte do Network Load Balancer.
- O servidor QUIC IDs tem sempre 8 bytes. Ao registrar o destino, a ID do servidor tem de estar no formato `0x`, seguido por 16 caracteres hexadecimais.
- Depois que um destino é registrado com uma ID de servidor, essa ID é imutável. Para alterar a ID do servidor de destino, o registro dessa ID tem de ser cancelado primeiro para depois registrar a nova ID de servidor.
- Uma combinação de identificador de destino e porta precisa ter uma ID de servidor. Não há suporte para o uso de uma ID de servidor diferente para a mesma combinação de IP ou ID de instância e porta na mesma VPC.
- Evite reutilizar a mesma ID de servidor para um destino diferente dentro de 6 horas.

Console

Para registrar destinos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.

3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Escolha a guia Destinos.
5. Escolha Register targets (Registrar destinos).
6. Se o tipo de destino do grupo de destino for `instance`, selecione as instâncias disponíveis, substitua a porta padrão caso seja necessário e escolha Incluir como pendente abaixo.
7. Se o tipo de destino do grupo de destino for `ip`, para cada endereço IP, selecione a rede, insira o endereço IP e as portas e escolha Incluir como pendente abaixo.
8. Se o tipo de destino do grupo de destino for `alb`, substitua a porta padrão, se necessário, e selecione o Application Load Balancer. Para obter mais informações, consulte Usar Application Load Balancers como destinos.
9. Se o protocolo do grupo de destino for QUIC ou TCP_QUIC, certifique-se de que uma ID do servidor esteja especificada.
10. Escolha Registrar destinos pendentes.

AWS CLI

Para registrar destinos

Use o comando register-targets. O exemplo a seguir registra destinos por ID de instância. Como a porta não está especificada, o balanceador de carga usa a porta do grupo de destino.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

O exemplo a seguir registra destinos por endereço IP. Como a porta não está especificada, o balanceador de carga usa a porta do grupo de destino.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10 Id=10.0.50.20
```

O exemplo a seguir registra um Application Load Balancer como destino.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
```

```
    --targets Id=application-load-balancer-arn
```

O exemplo a seguir registra destinos em um grupo de destino QUIC ou TCP_QUIC.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10,QuicServerId=0xa1b2c3d4e5f65890
 Id=10.0.50.20,QuicServerId=0xa1b2c3d4e5f65999
```

CloudFormation

Para registrar destinos

Atualize o AWS::ElasticLoadBalancingV2::TargetGrouprecurso para incluir os novos alvos. O exemplo a seguir registra dois destinos por ID de instância.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
```

O exemplo a seguir registra dois destinos por ID de instância em um grupo de destino com protocolo QUIC ou TCP_QUIC.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
```

```
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65999
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65000
```

Cancelar o registro de destinos

Se a demanda na aplicação diminuir ou se você precisar fazer manutenção nos destinos, poderá cancelar o registro dos destinos nos 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 load balancer interrompe o roteamento do tráfego para um destino assim que o registro dele é cancelado. O destino entra no estado `draining` até que as solicitações em andamento tenham sido concluídas.

Console

Para cancelar o registro de destinos

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Destinos, selecione os destinos a serem removidos.
5. Escolha Cancelar registro.

AWS CLI

Para cancelar o registro de destinos

Use o comando deregister-targets. O exemplo mostrado a seguir cancela o registro de dois destinos que foram registrados por ID de instância.

```
aws elbv2 deregister-targets \
```

```
    --target-group-arn target-group-arn \
    --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

Usar um Application Load Balancer como destino de um Network Load Balancer

Você pode criar um grupo de destino com um único Application Load Balancer como destino e configurar o Network Load Balancer para encaminhar tráfego para ele. Nesse cenário, o Application Load Balancer assume a decisão de balanceamento de carga assim que o tráfego chega até ele. Essa configuração combina os recursos dos dois balanceadores de carga e oferece as seguintes vantagens:

- Você pode usar o recurso de roteamento baseado em solicitações da camada 7 do Application Load Balancer em combinação com recursos compatíveis com o Network Load Balancer, como serviços de endpoint (AWS PrivateLink) e endereços IP estáticos.
- Você pode usar essa configuração para aplicações que precisam de um único endpoint para vários protocolos, como serviços de mídia usando HTTP para sinalização e RTP para transmitir conteúdo.

Você pode usar esse recurso com um Application Load Balancer interno ou voltado para a Internet como destino de um Network Load Balancer interno ou voltado para a Internet.

Considerações

- Você só pode registrar um Application Load Balancer por grupo de destino.
- Para associar um Application Load Balancer como destino de um Network Load Balancer, os balanceadores de carga precisam estar na mesma VPC dentro da mesma conta.
- Você pode associar um Application Load Balancer como destino de até dois Network Load Balancers. Para fazer isso, registre o Application Load Balancer em um grupo de destino separado para cada Network Load Balancer.
- Cada Application Load Balancer que você registra em um Network Load Balancer diminui o número máximo de destinos por zona de disponibilidade por Network Load Balancer em 50. Você pode desabilitar o balanceamento de carga entre zonas em ambos os balanceadores de carga para minimizar a latência e evitar cobranças de transferência de dados regionais. Para obter mais informações, consulte Cotas para seus Network Load Balancers.

- Quando o tipo de grupo de destino é `alb`, você não pode modificar os atributos do grupo de destino. Esses atributos sempre usam seus valores padrão.
- Depois de registrar um Application Load Balancer como destino, você não pode excluir o Application Load Balancer até cancelar o registro dele de todos os grupos de destino.
- A comunicação entre um Network Load Balancer e um Application Load Balancer sempre usa. IPv4

Tarefas

Pré-requisito

Se você ainda não tiver um Application Load Balancer para usar como destino, crie o balanceador de carga, os receptores e seus grupos de destino. 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

Crie um grupo de destino do tipo `alb`. Você pode registrar seu Application Load Balancer como destino ao criar o grupo de destino ou posteriormente.

Console

Para criar um grupo de destino para o Application Load Balancer como destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.
3. Selecione Criar grupo de destino.
4. No painel Configuração básica, em Escolher um tipo de destino, selecione Application Load Balancer.
5. Em Nome do grupo de destino, insira um nome para o grupo de destino.

6. Em Protocolo, somente TCP é permitido. Selecione a Porta do grupo de destino. A porta do grupo de destino deve corresponder à porta do receptor do Application Load Balancer. Se você escolher outra porta para esse grupo de destino, poderá atualizar a porta do receptor no Application Load Balancer para que seja correspondente.
7. Em VPC, selecione a nuvem privada virtual (VPC) para o grupo de destino. Ela deve ser a mesma VPC usada pelo Application Load Balancer.
8. Em Verificações de integridade, escolha HTTP ou HTTPS como o Protocolo de verificação de integridade. As verificações de saúde são enviadas ao Application Load Balancer e encaminhadas para seus destinos usando a porta, o protocolo e o caminho de ping especificados. Certifique-se de que o Application Load Balancer possa receber essas verificações de saúde ao ter um receptor com uma porta e um protocolo que correspondam à porta e ao protocolo da verificação de integridade.
9. (Opcional) Expanda as Tags. Para cada etiqueta, escolha Adicionar nova etiqueta e insira a chave da etiqueta e o valor da etiqueta.
10. Escolha Próximo.
11. Se estiver tudo pronto para registrar o Application Load Balancer, selecione Registrar agora. Em seguida, substitua a porta padrão, se necessário, e selecione o Application Load Balancer. O Application Load Balancer precisa ter um receptor na mesma porta do grupo de destino. Você pode adicionar ou editar um receptor nesse balanceador de carga para corresponder à porta do grupo de destino ou retornar à etapa anterior e alterar a porta do grupo de destino.

    Se não for possível registrar o Application Load Balancer como destino, selecione Registrar mais tarde e registre o destino posteriormente. Para obter mais informações, consulte the section called “Registrar destinos”.
12. Selecione Criar grupo de destino.

AWS CLI

Para criar um grupo de destino do tipo alb

Use o comando create-target-group. O protocolo deve ser TCP e a porta precisa corresponder à porta do receptor do Application Load Balancer.

```
aws elbv2 create-target-group \
    --name my-target-group \
```

```
    --protocol TCP \
    --port 80 \
    --target-type alb \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

CloudFormation

Para criar um grupo de destino do tipo alb

Defina um recurso do tipo AWS::ElasticLoadBalancingV2::TargetGroup. O protocolo deve ser TCP e a porta precisa corresponder à porta do receptor do Application Load Balancer.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: alb
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: !Ref myApplicationLoadBalancer
          Port: 80
```

Etapa 2: criar um Network Load Balancer e configurar o roteamento.

Ao criar o Network Load Balancer, é possível configurar a ação padrão para encaminhar o tráfego para o Application Load Balancer.

Console

Para criar o Network Load Balancer

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).

3. Selecione Criar um balanceador de carga.
4. Em Network Load Balancer, escolha Criar.
5. Configuração básica

   a. Em Nome do balanceador de carga, insira um nome para o seu Network Load Balancer.

   b. Em Scheme (Esquema), escolha Internet-facing (Voltado para a Internet) ou Internal (Interno). Um Network Load Balancer voltado para a Internet roteia solicitações de clientes até destinos na Internet. Um Network Load Balancer interno roteia solicitações para destinos usando endereços IP privados.

   c. Para o tipo de endereço IP do balanceador de carga, escolha IPv4se seus clientes usam IPv4 endereços para se comunicar com o Network Load Balancer ou Dualstack se seus clientes usam IPv4 ambos IPv6 e endereços para se comunicar com o Network Load Balancer.

6. Mapeamento de rede

   a. Em VPC, selecione a mesma VPC que você usou para o Application Load Balancer. Com um balanceador de carga voltado para a Internet, somente VPCs com um gateway de Internet estão disponíveis para seleção.

   b. Para Zonas de disponibilidade e sub-redes, selecione pelo menos uma zona de disponibilidade e selecione uma sub-rede por zona. Recomendamos que você selecione as mesmas zonas de disponibilidade habilitadas para seu Application Load Balancer. Isso otimiza a disponibilidade, o dimensionamento e o desempenho.

      (Opcional) Para usar endereços IP estáticos, escolha Usar um endereço IP elástico nas IPv4configurações de cada zona de disponibilidade. Com endereços IP estáticos, você pode adicionar determinados endereços IP a uma lista de permissões para firewalls ou codificar endereços IP com clientes.

7. Grupos de segurança

   Nós selecionamos previamente o grupo de segurança padrão para a VPC do balanceador de carga. Você pode selecionar grupos de segurança adicionais, conforme necessário. Se você não tiver um grupo de segurança que atenda a suas necessidades, escolha criar um novo grupo de segurança para criar um. Para saber mais, consulte Criar um grupo de segurança no Guia do usuário da Amazon VPC.

> **Warning**
>
> Se você não associar grupos de segurança ao Network Load Balancer agora, não poderá associá-los posteriormente.

> **Warning**
>
> Para utilizar receptores QUIC ou TCP_QUIC, seu Network Load Balancer não deve ter grupos de segurança.

8. Receptores e roteamento

   a. O padrão é um receptor que aceite tráfego TCP na porta 80. Somente receptores de TCP podem encaminhar tráfego para um grupo de destino do Application Load Balancer. Você deve manter o Protocolo como TCP, mas pode modificar a Porta, conforme necessário.

      Com essa configuração, você pode usar receptores HTTPS no Application Load Balancer para encerrar o tráfego TLS.

   b. Em Ação padrão, selecione o grupo de destino que você criou na etapa anterior.

   c. (Opcional) Escolha Adicionar tag de receptor e digite uma chave de tag e um valor de tag.

9. Tags do balanceador de carga

   (Opcional) Expanda as Tags do balanceador de carga. Escolha Adicionar nova tag e digite uma chave de tag e um valor de tag. Para obter mais informações, consulte Etiquetas.

10. Resumo

    Revise sua configuração e escolha Criar um balanceador de carga.

AWS CLI

Para criar o Network Load Balancer

Use o comando create-load-balancer. Recomendamos que você use as mesmas zonas de disponibilidade habilitadas para seu Application Load Balancer.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para adicionar um receptor TCP

Use o comando create-listener para adicionar um receptor TCP. Somente receptores TCP podem encaminhar tráfego para um Application Load Balancer. Para a ação padrão, use o grupo de destino que você criou na etapa anterior.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Para criar o Network Load Balancer

Defina um recurso do tipo AWS::ElasticLoadBalancingV2::LoadBalancere um recurso do tipo AWS::ElasticLoadBalancingV2::Listener. Somente receptores TCP podem encaminhar tráfego para um Application Load Balancer. Para a ação padrão, use o grupo de destino que você criou na etapa anterior.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-load-balancer
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

```
myTCPListener:
  Type: 'AWS::ElasticLoadBalancingV2::Listener'
  Properties:
    LoadBalancerArn: !Ref myLoadBalancer
    Protocol: TCP
    Port: 80
    DefaultActions:
      - Type: forward
        TargetGroupArn: !Ref myTargetGroup
```

Etapa 3: (opcional) criar um serviço de endpoint de VPC

Para usar o Network Load Balancer que você configurou na etapa anterior como um endpoint para conectividade privada, você pode habilitar o AWS PrivateLink. Isso estabelece uma conexão privada com o balanceador de carga como um serviço de endpoint.

Criar um serviço de endpoint da VPC usando o Network Load Balancer

1. No painel de navegação, selecione Balanceador de carga.
2. Selecione o nome do Network Load Balancer para abrir a página de detalhes dele.
3. Na guia Integrações, expanda Serviços de endpoint da VPC (AWS PrivateLink).
4. Selecione Criar serviços de endpoint para abrir a página Serviços de endpoint. Ver as etapas restantes, consulte Criar um serviço de endpoint no Guia do AWS PrivateLink .

Marcar um grupo de destino para o Network Load Balancer

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 nos nomes ou valores das tags porque ele está reservado para AWS uso. 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.

Console

Para gerenciar as tags de um grupo de destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Tags, selecione Gerenciar tags e execute uma ou mais das ações a seguir:
   a. Para atualizar uma tag, insira novos valores para Chave e Valor.
   b. Para adicionar uma nova tag, escolha Adicionar tag e insira uma Chave e um Valor.
   c. Para excluir uma tag, escolha Remover ao lado da tag.
5. Escolha Salvar alterações.

AWS CLI

Como adicionar tags do

Use o comando add-tags. O exemplo a seguir adiciona duas tags.

```
aws elbv2 add-tags \
    --resource-arns target-group-arn \
    --tags "Key=project,value=lima" "Key=department,Value=digital-media"
```

Como remover tags

Use o comando remove-tags. O exemplo a seguir remove as tags com as chaves especificadas.

```
aws elbv2 remove-tags \
    --resource-arns target-group-arn \
    --tag-keys project department
```

CloudFormation

Como adicionar tags do

Atualize o AWS::ElasticLoadBalancingV2::TargetGrouprecurso para incluir a `Tags` propriedade.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Excluir um grupo de destino para o Network Load Balancer

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. Se você não precisar mais de uma instância do EC2 registrada, poderá interrompê-la ou encerrá-la.

Console

Como excluir um grupo de destino

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Balanceamento de carga, selecione Grupos de destino.
3. Selecione o grupo de destino e escolha Actions (Ações), Delete (Excluir).

4. Escolha Excluir.

AWS CLI

Como excluir um grupo de destino

Use o comando delete-target-group.

```
aws elbv2 delete-target-group \
    --target-group-arn target-group-arn
```

Monitorar os Network Load Balancers

Você pode usar os recursos a seguir para monitorar seus load balancers, analisar os padrões de tráfego e solucionar problemas com seu load balancers e destinos.

CloudWatch métricas

Você pode usar CloudWatch a Amazon para recuperar estatísticas sobre pontos de dados para seus balanceadores de carga e destinos como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Essas métricas podem ser usadas para verificar se o sistema está executando conforme o esperado. Para obter mais informações, consulte CloudWatch métricas para seu Network Load Balancer.

Logs de fluxo da VPC

Você pode usar logs de fluxo da VPC para capturar informações detalhadas sobre o tráfego de entrada e saída do Network Load Balancer. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário da Amazon VPC.

Crie um log de fluxo para cada interface de rede para o seu load balancer. Há uma interface de rede por sub-rede do load balancer. Para identificar as interfaces de rede para um Network Load Balancer, procure o nome do balanceador de carga no campo de descrição da interface de rede.

Há duas entradas para cada conexão por meio do Network Load Balancer: uma para a conexão de frontend entre o cliente e o balanceador de carga e outra para a conexão de backend entre o balanceador de carga e o destino. Se o atributo de preservação do IP do cliente do grupo de destino estiver habilitado, a conexão aparecerá para a instância como uma conexão do cliente. Caso contrário, o IP de origem da conexão será o endereço IP privado do balanceador de carga. Se o grupo de segurança da instância não permitir conexões do cliente, mas a rede da sub-rede ACLs do balanceador de carga permitir, os registros da interface de rede do balanceador de carga mostrarão “ACEITAR OK” para as conexões de front-end e back-end, enquanto os registros da interface de rede da instância mostrarão “REJEITAR OK” para a conexão.

Se um Network Load Balancer tiver grupos de segurança associados, os logs de fluxo conterão entradas para o tráfego permitido ou rejeitado pelos grupos de segurança. Para Network Load Balancers com receptores TLS, as entradas de logs de fluxo só refletem as entradas rejeitadas.

Monitor de CloudWatch Internet da Amazon

Você pode usar o Internet Monitor para ver como os problemas da Internet afetam o desempenho e a disponibilidade entre seus aplicativos hospedados AWS e seus usuários finais. Você também

pode explorar, quase em tempo real, como melhorar a latência projetada de seu aplicativo migrando para outros serviços ou redirecionando o tráfego para sua carga de trabalho por meio de diferentes. Regiões da AWS Para obter mais informações, consulte Usando o Amazon CloudWatch Internet Monitor.

Logs de acesso

Você pode usar logs de acesso para capturar informações detalhadas sobre as solicitações TLS feitas ao seu load balancer. Os arquivos de log são armazenados no Amazon S3. Você pode usar esses logs de acesso para analisar padrões de tráfego e solucionar problemas com seus destinos. Para obter mais informações, consulte Logs de acesso do Network Load Balancer.

CloudTrail troncos

Você pode usar AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para a API do Elastic Load Balancing e armazená-las como arquivos de log no Amazon S3. Você pode usar esses CloudTrail registros para determinar quais chamadas foram feitas, o endereço IP de origem da chamada, quem fez a chamada, quando a chamada foi feita e assim por diante. Para obter mais informações, consulte Registrar chamadas de API para uso do Elastic Load Balancing. CloudTrail

CloudWatch métricas para seu Network Load Balancer

O Elastic Load Balancing publica pontos de dados na Amazon CloudWatch para seus balanceadores de carga e seus alvos. CloudWatchpermite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Por exemplo, você pode monitorar o número total de destinos íntegros de um load balancer ao longo de um período especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

É possível usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um CloudWatch alarme para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica estiver fora do que você considera um intervalo aceitável.

O Elastic Load Balancing reporta métricas CloudWatch somente quando as solicitações estão fluindo pelo balanceador de carga. Se houver solicitações passando pelo balanceador de carga, o Elastic Load Balancing vai medir e enviar suas métricas em intervalos de 60 segundos. Se não há solicitações passando pelo load balancer ou não há dados para uma métrica, a métrica não é

reportada. Para balanceadores de carga de rede com grupos de segurança, o tráfego rejeitado pelos grupos de segurança não é capturado nas CloudWatch métricas.

Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Conteúdo

Métricas do Network Load Balancer

O namespace `AWS/NetworkELB` inclui as métricas a seguir.

Métrica	Description
`ActiveFlowCount`	O número total de fluxos simultâneos (ou conexões) dos clientes para os destinos. Esta métrica inclui somente as conexões nos estados SYN_SENT e ESTABLISHED. As conexões TCP não são encerradas no load balancer; portanto, um cliente que abre uma conexão TCP com um destino conta como um único fluxo. Critérios de relatório: sempre relatado. Estatísticas: as estatísticas mais úteis são `Average`, `Maximum` e `Minimum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`
`ActiveFlowCount_TCP`	O número total de fluxos (conexões) TCP simultâneos dos clientes para os destinos. Esta métrica inclui as conexões nos estados SYN_SENT e ESTABLISHED. As conexões TCP não são encerrada

Métrica	Description
	s no load balancer; portanto, um cliente que abre uma conexão TCP com um destino conta como um único fluxo. Critérios de relatório: há um valor diferente de zero Estatísticas: as estatísticas mais úteis são `Average`, `Maximum` e `Minimum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`
`ActiveFlowCount_TLS`	O número total de fluxos (conexões) TLS simultâneos dos clientes para os destinos. Esta métrica inclui as conexões nos estados SYN_SENT e ESTABLISHED. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: as estatísticas mais úteis são `Average`, `Maximum` e `Minimum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`

Métrica	Description
`ActiveFlowCount_UDP`	O número total de fluxos (conexões) UDP simultâneos dos clientes para os destinos. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: as estatísticas mais úteis são `Average`, `Maximum` e `Minimum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`
`ActiveZonalShiftHostCount`	O número de destinos que estão participando ativamente da mudança de zona no momento. Critérios de relatórios: relatados quando o balanceador de carga aceita a mudança de zona. Estatísticas: as estatísticas mais úteis são `Maximum` e `Minimum`. Dimensões • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

Métrica	Description
`ClientTLSNegotiationErrorCount`	O número total de handshakes TLS com falha durante a negociação entre um cliente e um listener TLS. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer`
`ConsumedLCUs`	O número de unidades de capacidade do balanceador de carga (LCU) usadas pelo balanceador de carga. Você paga pelo número LCUs que usa por hora. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing. Critérios de relatório: sempre relatado. Estatísticas: todas Dimensões • `LoadBalancer`
`ConsumedLCUs_TCP`	O número de unidades de capacidade do load balancer (LCU) usadas pelo load balancer para TCP. Você paga pelo número LCUs que usa por hora. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: todas Dimensões • `LoadBalancer`

Métrica	Description
`ConsumedLCUs_TLS`	O número de unidades de capacidade do load balancer (LCU) usadas pelo load balancer para TLS. Você paga pelo número LCUs que usa por hora. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: todas Dimensões • `LoadBalancer`
`ConsumedLCUs_UDP`	O número de unidades de capacidade do load balancer (LCU) usadas pelo load balancer para UDP. Você paga pelo número LCUs que usa por hora. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: todas Dimensões • `LoadBalancer`

Métrica	Description
HealthyHostCount	O número de destinos considerados íntegros. Essa métrica não inclui quaisquer Application Load Balancers registrados como destinos. Critérios de relatórios: relatados se houver destinos registrados. Estatísticas: as estatísticas mais úteis são Maximum e Minimum. Dimensões • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
NewFlowCount	O número total de novos fluxos (ou conexões) estabelecidos dos clientes para os destinos no período. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup
NewFlowCount_TCP	O número total de novos fluxos (ou conexões) TCP estabelecidos dos clientes para os destinos no período. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup

Métrica	Description
NewFlowCount_TLS	O número total de novos fluxos (ou conexões) TLS estabelecidos dos clientes para os destinos no período. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup
NewFlowCount_UDP	O número total de novos fluxos (ou conexões) UDP estabelecidos dos clientes para os destinos no período. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup

Métrica	Description
NewFlowCount_QUIC	O número total de datagramas UDP que exigiram uma decisão de roteamento no período. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
PeakBytesPerSecond	A média mais alta de bytes processados por segundo, calculada a cada 10 segundos durante a janela de amostragem. Essa métrica não inclui o tráfego de verificação de integridade. Critérios de relatório: sempre relatado Estatísticas: a estatística mais útil é Maximum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
PeakPacketsPerSecond	Maior taxa média de pacotes (pacotes processados por segundo), calculada a cada dez segundos durante a janela de amostragem. Essa métrica inclui o tráfego de verificação de integridade. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é Maximum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Description
`PortAllocationErrorCount`	O número total de erros temporários de alocação de portas durante uma operação de conversão do IP do cliente. Um valor diferente de zero indica conexões de clientes descartadas. Observação: os Network Load Balancers podem oferecer suporte a 55 mil conexões simultâneas ou a cerca de 55 mil conexões por minuto para cada destino exclusivo (endereço IP e porta) quando executar a conversão do endereço do cliente. Para corrigir erros na alocação de portas, adicione mais destinos ao grupo de destino. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes`	O número total de bytes processados pelo balanceador de carga, incluindo TCP/IP cabeçalhos. Essa contagem inclui o tráfego de e para destinos, menos o tráfego de verificação de integridade. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Description
`ProcessedBytes_TCP`	O número total de bytes processados pelos listeners TCP. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes_TLS`	O número total de bytes processados pelos listeners TLS. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes_UDP`	O número total de bytes processados pelos listeners UDP. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Description
`ProcessedBytes_QUIC`	O número total de bytes processados pelos receptores QUIC. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedPackets`	O número total de pacotes processados pelo balanceador de carga. Essa contagem inclui o tráfego de e para destinos, inclusive o tráfego de verificação de integridade. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedFlowCount`	O número total de fluxos (ou conexões) rejeitados pelo balanceador de carga. Critérios de relatório: sempre relatado. Estatísticas: as estatísticas mais úteis são `Average`, `Maximum` e `Minimum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Description
`RejectedFlowCount_TCP`	O número de fluxos de TCP (ou conexões) rejeitados pelo balancead or de carga. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ReservedLCUs`	O número de unidades de capacidade do balanceador de carga (LCUs) reservadas para seu balanceador de carga usando a reserva da LCU. Critérios de relatório: há um valor diferente de zero Estatísticas: todas Dimensões • `LoadBalancer`
`SecurityGroupBlock edFlowCou nt_Inbound_ICMP`	O número de novas mensagens ICMP rejeitadas pelas regras de entrada dos grupos de segurança do balanceador de carga. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Description
SecurityGroupBlockedFlowCount_Inbound_TCP	O número de novos fluxos TCP rejeitados pelas regras de entrada dos grupos de segurança do balanceador de carga. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_UDP	O número de novos fluxos UDP rejeitados pelas regras de entrada dos grupos de segurança do balanceador de carga. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_ICMP	O número de novas mensagens ICMP rejeitadas pelas regras de saída dos grupos de segurança do balanceador de carga. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Description
SecurityGroupBlockedFlowCount_Outbound_TCP	O número de novos fluxos TCP rejeitados pelas regras de saída dos grupos de segurança do balanceador de carga. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_UDP	O número de novos fluxos UDP rejeitados pelas regras de saída dos grupos de segurança do balanceador de carga. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
TargetTLSNegotiationErrorCount	O número total de handshakes TLS com falha durante a negociação entre um listener TLS e um destino. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer

Métrica	Description
`TCP_Client_Reset_Count`	O número total de pacotes de redefinição (RST) enviados de um cliente para um destino. Essas redefinições são geradas pelo cliente e encaminhadas pelo load balancer. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`TCP_ELB_Reset_Count`	O número total de pacotes de redefinição (RST) gerados pelo load balancer. Para obter mais informações, consulte Solução de problemas. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`TCP_Target_Reset_Count`	O número total de pacotes de redefinição (RST) enviados de um destino para um cliente. Essas redefinições são geradas pelo destino e encaminhadas pelo load balancer. Critérios de relatório: sempre relatado. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Description
UnHealthyHostCount	O número de destinos considerados sem integridade. Essa métrica não inclui quaisquer Application Load Balancers registrados como destinos. Critérios de relatórios: relatados se houver destinos registrados. Estatísticas: as estatísticas mais úteis são Maximum e Minimum. Dimensões • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
UnhealthyRoutingFlowCount	O número de fluxos (ou conexões) que são roteados usando a ação de failover de roteamento (falha na abertura). Essa métrica não é compatível com receptores TLS. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum.
ZonalHealthStatus	O número de zonas de disponibilidade que o balanceador de carga considera íntegras. O balanceador de carga emite um 1 para cada zona de disponibilidade íntegra e um 0 para cada zona de disponibilidade não íntegra. Critérios de relatório: relatado se as verificações de integridade estiverem habilitadas. Estatísticas: as estatísticas mais úteis são Maximum e Minimum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Description
`QUIC_Unknown_Server_ID_Packet_Drop_Count`	O número de datagramas UDP descartados que contêm uma ID de servidor não associada a um destino no Network Load Balancer. Critérios de emissão de relatórios: reportados somente para receptores QUIC. Estatísticas: a estatística mais útil é `Sum`. Dimensões • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Dimensões métricas dos Network Load Balancers

Para filtrar as métricas do load balancer, use as dimensões a seguir.

Dimensão	Description
`AvailabilityZone`	Filtra os dados de métrica por zona de disponibilidade.
`LoadBalancer`	Filtra os dados da métrica por load balancer. Especifique o balanceador de carga da seguinte forma: net/ load-balancer-name/1234567890123456 (a parte final do ARN do balanceador de carga).
`TargetGroup`	Filtra os dados da métrica por grupo de destino. Especifique o grupo-alvo da seguinte forma: targetgroup/ target-group-name/1234567890123456 (a parte final do ARN do grupo-alvo).

Estatísticas para métricas do Network Load Balancer

CloudWatch fornece estatísticas com base nos pontos de dados métricos publicados pelo Elastic Load Balancing. As estatísticas são agregações de dados de métrica ao longo de um período especificado. Quando você solicita estatísticas, o fluxo de dados apresentado é identificado pelo

nome da métrica e pela dimensão. Uma dimensão é um name/value par que identifica de forma exclusiva uma métrica. Por exemplo, você pode solicitar estatísticas de todas as instâncias EC2 íntegras por atrás de um load balancer iniciado em uma Zona de disponibilidade específica.

As estatísticas `Minimum` e `Maximum` refletem os valores mínimos e máximos dos pontos de dados relatados por cada um dos nós do load balancer em cada janela de amostragem. Aumentos no máximo de `HealthyHostCount` correspondem a diminuições no mínimo de `UnHealthyHostCount`. É recomendável monitorar o `HealthyHostCount` máximo invocando o alarme quando o `HealthyHostCount` máximo estiver abaixo do mínimo exigido ou for `0`. Isso pode ajudar a identificar quando os destinos se tornaram não íntegros. Também é recomendável monitorar o `UnHealthyHostCount` mínimo invocando o alarme quando o `UnHealthyHostCount` mínimo ultrapassar `0`. Isso permite que você fique ciente de quando não há mais destinos registrados.

A estatística `Sum` é o valor agregado entre todos os nós do load balancer. Como as métricas incluem vários relatórios por período, `Sum` só será aplicável às métricas agregadas em todos os nós do load balancer.

A estatística `SampleCount` é o número de amostras medidas. Como as métricas são obtidas com base em intervalos de amostragem e eventos, essa estatística normalmente não é útil. Por exemplo, com `HealthyHostCount`, `SampleCount` se baseia no número de amostras que cada nó do load balancer relata, não no número de hosts íntegros.

Veja CloudWatch as métricas do seu balanceador de carga

Você pode visualizar as CloudWatch métricas dos seus balanceadores de carga usando o console do Amazon EC2. Essas métricas são exibidas como gráficos de monitoramento. O monitoramento de gráficos mostrará pontos de dados se o load balancer estiver ativo e recebendo solicitações.

Como alternativa, você pode visualizar as métricas do seu load balancer usando o console do CloudWatch.

Para visualizar as métricas usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Para visualizar métricas filtradas por grupo de destino, faça o seguinte:
   a. No painel de navegação, selecione Grupos de destino.
   b. Selecione o seu grupo de destino e escolha Monitoramento.

c. (Opcional) Para filtrar os resultados de acordo com o horário, selecione um período na opção Exibindo os dados de.

d. Para obter uma visualização maior de uma única métrica, selecione seu gráfico.

3. Para visualizar métricas filtradas por load balancer, faça o seguinte:

a. No painel de navegação, selecione Load Balancers.

b. Selecione o load balancer e escolha Monitoramento.

c. (Opcional) Para filtrar os resultados de acordo com o horário, selecione um período na opção Exibindo os dados de.

d. Para obter uma visualização maior de uma única métrica, selecione seu gráfico.

Para visualizar métricas usando o CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Selecione o namespace NetworkELB.
4. (Opcional) Para visualizar uma métrica em todas as dimensões, digite o nome no campo de pesquisa.

Para visualizar métricas usando o AWS CLI

Use o comando list-metrics para listar as métricas disponíveis:

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

Para obter as estatísticas de uma métrica usando o AWS CLI

Use o get-metric-statisticscomando a seguir para obter estatísticas para a métrica e a dimensão especificadas. Observe que CloudWatch trata cada combinação exclusiva de dimensões como uma métrica separada. Você não consegue recuperar estatísticas usando combinações de dimensões que não tenham sido especialmente publicadas. É necessário especificar as mesmas dimensões usadas ao criar as métricas.

```
aws cloudwatch get-metric-statistics --namespace AWS/NetworkELB \
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \
```

```
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

A seguir está um exemplo de saída:

```
{
    "Datapoints": [
        {
            "Timestamp": "2017-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2017-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Logs de acesso do Network Load Balancer

O Elastic Load Balancing fornece logs de acesso que capturam informações detalhadas sobre as conexões TLS estabelecidas com o Network Load Balancer. Você pode usar esses logs de acesso para analisar padrões de tráfego e solucionar problemas.

> **Important**
>
> Embora os registros de acesso “legados” tradicionais (descritos nesta seção) permaneçam disponíveis, o Network Load Balancer agora oferece opções aprimoradas de registro por meio CloudWatch de registros. CloudWatch Os registros oferecem opções de entrega mais flexíveis, inclusive para Amazon CloudWatch Logs, Amazon Data Firehose e Amazon Simple Storage Service. Para configurar essas opções aprimoradas de registro em log, acesse a guia Integrações do balanceador de carga. Para obter mais informações sobre CloudWatch registros, consulteCloudWatch registros para seu Network Load Balancer.

> **Important**
>
> Os logs de acesso serão criados somente se o load balancer tiver um receptor TLS e os logs contiverem somente informações sobre solicitações TLS. Os logs de acesso registram as solicitações com base no melhor esforço. Recomendamos que você use logs de acesso para compreender a natureza das solicitações, não como uma contabilidade completa de todas as solicitações.

O registro de logs de acesso é um recurso opcional do Elastic Load Balancing e é desabilitado por padrão. Depois de habilitar o registro de logs de acesso para o balanceador de carga, o Elastic Load Balancing captura os logs como arquivos compactados e os armazena no bucket do Amazon S3 que você especificar. Você pode desativar o registro de acessos em log a qualquer momento.

É possível habilitar a criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) ou usando o Key Management Service com chaves gerenciadas pelo cliente (SSE-KMS CMK) para o bucket do S3. Cada arquivo de log de acesso é automaticamente criptografado antes de ser armazenado no seu bucket do S3 e descriptografado quando você o acessar. Você não precisa tomar nenhuma ação, pois não há diferença na forma como você acessa arquivos de log criptografados ou não criptografados. Cada arquivo de log é criptografado com uma chave exclusiva, que é em si criptografada com uma chave do KMS alternada regularmente. Para obter mais informações, consulte Especificação da criptografia do Amazon S3 (SSE-S3) e Especificação da criptografia do lado do servidor com (SSE-KMS) no Guia do usuário do Amazon AWS KMS S3.

Não há cobrança adicional pelos logs de acesso. Os custos de armazenamento do Amazon S3 são cobrados de você, mas não é cobrada a largura de banda usada pelo Elastic Load Balancing para enviar arquivos de log para o Amazon S3. Para obter mais informações sobre os custos de armazenamento, consulte Definição de preço do Amazon S3.

Conteúdo

Arquivos do log de acesso

O Elastic Load Balancing publica um arquivo de log para cada nó do balanceador de carga a cada 5 minutos. A entrega de logs, no final das contas, é consistente. O load balancer pode distribuir vários logs para o mesmo período. Isso normalmente acontece se o site tiver alto tráfego.

Os nomes dos arquivos dos logs de acesso usa o seguinte formato:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_net.load-balancer-id_end-time_random-string.log.gz
```

bucket

O nome do bucket do S3.

prefix

O prefixo (hierarquia lógica) no bucket. Se você não especificar um prefixo, os logs serão colocados no nível raiz do bucket.

aws-account-id

O Conta da AWS ID do proprietário.

region

A Região para seu load balancer e o bucket do S3.

aaaa/mm/dd

A data em que o log foi entregue.

load-balancer-id

O ID de recursos do load balancer. Se o ID de recursos contiver barras (/), elas são substituídos por pontos (.).

end-time

A data e a hora em que o intervalo de registro terminou. Por exemplo, um horário de término de 20181220T2340Z contém entradas para solicitações feitas entre 23:35 e 23:40.

random-string

Uma string aleatória gerada pelo sistema.

A seguir está um exemplo de nome de arquivo de log:

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-
loadbalancer.1234567890abcdef_20200501T0000Z_20sg8hgm.log.gz
```

Você pode armazenar os arquivos de log no bucket pelo tempo que desejar, mas também pode definir regras do ciclo de vida do Amazon S3 para arquivar ou excluir os arquivos de log automaticamente. Para obter mais informações, consulte Gerenciar o ciclo de vida de armazenamento no Guia do usuário do Amazon S3.

Entradas do log de acesso

A tabela a seguir descreve os campos de uma entrada no log de acesso, em ordem. Todos os campos são delimitados por espaços. Quando novos campos são introduzidos, eles são adicionados no final da entrada de log. Ao processar os arquivos de log, você deverá ignorar quaisquer campos no final da entrada de log que não sejam esperados.

Campo	Description
type	O tipo de listener. O valor suportado é `tls`.
version	A versão da entrada de log. A versão atual é 2.0.
horário	A hora registrada ao final da conexão TLS, no formato ISO 8601.
elb	O ID de recursos do load balancer.
listener	O ID do recurso do listener TLS para a conexão.
client_port	O endereço IP e a porta do cliente.
destination_port	O endereço IP e a porta do destino. Se o cliente se conectar diretamente ao load balancer, o destino será o listener. Se o cliente se conectar usando um serviço de VPC endpoint, o destino será o VPC endpoint.
connection_time	O tempo total para a conexão ser concluída, do início ao encerramento, em milissegundos.

Campo	Description
tls_handshake_time	O tempo total para o handshake TLS ser concluído depois que a conexão TCP for estabelecida, incluindo atrasos no lado do cliente, em milissegundos. Esse tempo está incluído no campo `connectio n_time` . Se não houver nenhum handshake TLS ou uma falha no handshake TLS, esse valor será definido como `-`.
received_bytes	A contagem de bytes recebidos pelo load balancer do cliente, após a descriptografia.
sent_bytes	A contagem de bytes enviados pelo load balancer para o cliente, antes da criptografia.
incoming_tls_alert	O valor inteiro de alertas TLS recebidos pelo load balancer do cliente, se estiver presente. Caso contrário, esse valor será definido como`-`.
chosen_cert_arn	O ARN do certificado fornecido ao cliente. Se nenhuma mensagem de saudação do cliente válida for enviada, esse valor será definido como`-`.
chosen_cert_serial	Reservado para uso futuro. Esse valor é sempre definido como`-`.
tls_cipher	O pacote de criptografia negociado com o cliente, no formato OpenSSL. Se a negociação de TLS não for concluída, esse valor será definido como. `-`
tls_protocol_version	O protocolo TLS negociado com o cliente, no formato de string. Os valores possíveis são `tlsv10`, `tlsv11`, `tlsv12` e `tlsv13`. Se a negociação de TLS não for concluída, esse valor será definido como. `-`
troca de chaves tls_	A troca de chaves usada durante apertos de mão para TLS ou PQ-TLS. Se a negociação de TLS ou PQ-TLS não for concluída, esse valor será definido como. `-`
domain_name	O valor da extensão do cliente server_name na mensagem Hello. Esse valor é codificado em URL. Se nenhuma mensagem de saudação do cliente válida for enviada ou a extensão não estiver presente, esse valor será definido como`-`.

Campo	Description
alpn_fe_protocol	O protocolo de aplicativo negociado com o cliente, no formato de string. Os valores possíveis são h2, `http/1.1` e `http/1.0`. Se nenhuma política ALPN estiver configurada no ouvinte TLS, nenhum protocolo correspondente for encontrado ou nenhuma lista de protocolos válida for enviada, esse valor será definido como. -
alpn_be_protocol	O protocolo de aplicativo negociado com o destino, no formato de string. Os valores possíveis são h2, `http/1.1` e `http/1.0`. Se nenhuma política ALPN estiver configurada no ouvinte TLS, nenhum protocolo correspondente for encontrado ou nenhuma lista de protocolos válida for enviada, esse valor será definido como. -
alpn_client_preference_list	O valor da extensão application_layer_protocol_negotiation na mensagem Hello do cliente. Esse valor é codificado em URL. Cada protocolo está entre aspas duplas, e os protocolos são separados por uma vírgula. Se nenhuma política ALPN estiver configurada no ouvinte TLS, nenhuma mensagem de saudação de cliente válida for enviada ou a extensão não estiver presente, esse valor será definido como. - A string será truncada se for maior do que 256 bytes.
tls_connection_creation_time	A hora registrada no início da conexão TLS, no formato ISO 8601.

Exemplo de entradas de log do

A seguir estão exemplo de entradas de log. Observe que o texto aparece em várias linhas somente para facilitar a leitura.

Veja a seguir um exemplo de um listener TLS sem uma política ALPN.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
```

```
- - - 2018-12-20T02:59:30
```

Veja a seguir um exemplo de um listener TLS com uma política ALPN.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1" 2020-04-01T08:51:20
```

Processar arquivos de log de acesso

Os arquivos de log de acesso são compactados. Se você abrir os arquivos usando o console do Amazon S3, eles serão descompactados e as informações serão exibidas. Se você baixar os arquivos, deverá descompactá-los para visualizar as informações.

Se houver uma grande demanda no seu site, o load balancer poderá gerar arquivos de log com gigabytes de dados. Talvez você não consiga processar uma quantidade tão grande de dados usando o line-by-line processamento. Assim, pode ter de usar ferramentas analíticas que forneçam soluções de processamento paralelo. Por exemplo, você pode usar as ferramentas analíticas a seguir para analisar e processar logs de acesso:

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão. Para obter mais informações, consulte Consultar logs do Network Load Balancer no Guia do usuário do Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

Habilitar logs de acesso do Network Load Balancer

Ao habilitar os registro de acesso em logs para o load balancer, você deve especificar o nome do bucket do S3 onde o load balancer armazenará os logs. O bucket deve ter uma política de bucket que conceda permissão para o Elastic Load Balancing gravar no bucket.

> **Important**
>
> Os logs de acesso serão criados somente se o load balancer tiver um receptor TLS e os logs contiverem somente informações sobre solicitações TLS.

Requisitos do bucket

É possível usar um bucket existente ou criar um bucket especificamente para logs de acesso. O bucket deve atender aos seguintes requisitos:

Requisitos

- O bucket deve estar localizado na mesma região que o load balancer. O bucket e o balanceador de carga podem pertencer a contas diferentes.
- O prefixo especificado não deve incluir `AWSLogs`. Adicionamos a parte do nome do arquivo que começa com `AWSLogs` após o nome do bucket e o prefixo que você especificar.
- O bucket deve ter uma política de bucket que conceda permissão para gravar os logs de acesso em seu bucket. As políticas de bucket são um conjunto de instruções JSON gravadas na linguagem de políticas de acesso para definir permissões de acesso para o seu bucket.

Exemplo de política de bucket

Veja abaixo um exemplo de política . Para os `Resource` elementos, *`amzn-s3-demo-destination-bucket`* substitua pelo nome do bucket do S3 para seus registros de acesso. Certifique-se de omitir o *`Prefix/`* se você não estiver usando um prefixo de bucket. Para`aws:SourceAccount`, especifique o ID da AWS conta com o balanceador de carga. Para`aws:SourceArn`, substitua *`region`* e *`012345678912`* com a região e o ID da conta do balanceador de carga, respectivamente.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-
bucket/Prefix/AWSLogs/account-ID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        }
    ]
```

```
}
```

Criptografia

Você pode habilitar a criptografia do lado do servidor para o bucket do log de acesso do Amazon S3 de uma das seguintes formas:

- Chaves gerenciadas pelo Amazon S3 (SSE-S3)
- AWS KMS chaves armazenadas em AWS Key Management Service (SSE-KMS) †

† Com os registros de acesso do Network Load Balancer, você não pode usar chaves AWS gerenciadas, você deve usar chaves gerenciadas pelo cliente.

Para obter mais informações, consulte Especificação da criptografia do Amazon S3 (SSE-S3) e Especificação da criptografia do lado do servidor com (SSE-KMS) no Guia do usuário do Amazon AWS KMS S3.

A política de chave deve permitir que o serviço criptografe e descriptografe os logs. Veja abaixo um exemplo de política .

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

Configurar logs de acesso

Use o procedimento a seguir para configurar logs de acesso para capturar informações da solicitação e entregar arquivos de log ao seu bucket do S3.

Console

Habilitar logs de acesso

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Selecione o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Em Monitoramento, ative os Logs de acesso.
6. Para URI do S3, insira o URI do S3 para seus arquivos de log. O URI especificado dependerá de você estar ou não usando um prefixo.
   - URI com um prefixo: s3:///*amzn-s3-demo-logging-bucketlogging-prefix*
   - URI sem prefixo: s3://*amzn-s3-demo-logging-bucket*
7. Escolha Salvar alterações.

AWS CLI

Habilitar logs de acesso

Use o modify-load-balancer-attributescomando com os atributos relacionados.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes \
        Key=access_logs.s3.enabled,Value=true \
        Key=access_logs.s3.bucket,Value=amzn-s3-demo-logging-bucket \
        Key=access_logs.s3.prefix,Value=logging-prefix
```

CloudFormation

Habilitar logs de acesso

Atualize o AWS::ElasticLoadBalancingV2::LoadBalancerrecurso para incluir os atributos relacionados.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "access_logs.s3.enabled"
          Value: "true"
        - Key: "access_logs.s3.bucket"
          Value: "amzn-s3-demo-logging-bucket"
        - Key: "access_logs.s3.prefix"
          Value: "logging-prefix"
```

Desabilitar logs de acesso do Network Load Balancer

Você pode desabilitar o registro de acesso em logs para seu load balancer a qualquer momento. Depois de desabilitar o registro de log de acesso, seus logs permanecerão no seu bucket do S3 até que você os exclua. Para obter mais informações, consulte Criação, configuração e trabalho com buckets do S3 no Guia do usuário do Amazon S3.

Console

Para desabilitar logs de acesso

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Load Balancers.
3. Selecione o nome do balanceador de carga para abrir sua página de detalhes.

4. Na guia Atributos, escolha Editar.
5. Em Monitoramento, desative os Logs de acesso.
6. Selecione Salvar alterações.

AWS CLI

Para desabilitar logs de acesso

Use o comando modify-load-balancer-attributes.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes Key=access_logs.s3.enabled,Value=false
```

Solucionar problemas do Network Load Balancer

As informações a seguir podem ajudar na solução de problemas com o Network Load Balancer.

Um destino registrado não está em serviço

Se um destino estiver levando mais tempo que o esperado para entrar no estado `InService`, ele pode estar falhando nas verificações de integridade. O destino não entrará em serviço até ser aprovado em uma verificação de integridade. Para obter mais informações, consulte Verificações de integridade para grupos de destino do Network Load Balancer.

Verifique se a sua instância está falhando nas verificações de integridade e verifique o seguinte:

Um security group não permite o tráfego

Os security groups associados a uma instância devem permitir tráfego do load balancer usando a porta de verificação de integridade e o protocolo de verificação de integridade. Para obter mais informações, consulte Grupos de segurança de destino. Além disso, o security group para seu load balancer deve permitir o tráfego para as instâncias. Para obter mais informações, consulte Atualizar os grupos de segurança para o Network Load Balancer.

Uma lista de controle de acesso (ACL) à rede não permite o tráfego

A ACL da rede associada às sub-redes das instâncias e as sub-redes do balanceador de carga devem permitir tráfego e verificações de integridade do balanceador de carga. Para obter mais informações, consulte Rede ACLs.

As solicitações não são roteadas para os destinos

Verifique o seguinte:

Um security group não permite o tráfego

Os security groups associados às instâncias devem permitir tráfego na porta do listener de endereços IP do cliente (se os destinos são especificados por ID de instância) ou nós do load balancer (se os destinos são especificados por endereço IP). Para obter mais informações, consulte Grupos de segurança de destino. Além disso, o security group para seu load balancer

deve permitir o tráfego para as instâncias. Para obter mais informações, consulte Atualizar os grupos de segurança para o Network Load Balancer.

Uma lista de controle de acesso (ACL) à rede não permite o tráfego

A rede ACLs associada às sub-redes da sua VPC deve permitir que o balanceador de carga e os destinos se comuniquem em ambas as direções na porta do ouvinte. Para obter mais informações, consulte Rede ACLs.

Os destinos estão em uma zona de disponibilidade que não está habilitada

Se você registrar destinos em uma zona de disponibilidade, mas não habilitá-la, esses destinos registrados não receberão tráfego do load balancer.

A instância está em uma VPC emparelhada

Se você tiver instâncias em uma VPC emparelhada com a VPC do load balancer, será necessário registrá-las no load balancer por endereço IP, não por ID de instância.

A ID do servidor configurada não corresponde à ID configurada no destino

Se você estiver usando receptores QUIC, a ID configurada no destino precisa corresponder à ID configurada com o grupo de destino do Network Load Balancer.

Os destinos recebem mais solicitações de verificação de integridade do que o esperado

As verificações de integridade de um Network Load Balancer são distribuídas e usam um mecanismo de consenso para determinar a integridade do destino. Portanto, os destinos recebem mais do que o número configurado de verificações de integridade por meio da configuração `HealthCheckIntervalSeconds`.

Os destinos recebem menos solicitações de verificação de integridade do que o esperado

Verifique se `net.ipv4.tcp_tw_recycle` está habilitado. Essa configuração é conhecida por causar problemas com load balancers. A configuração `net.ipv4.tcp_tw_reuse` é considerada uma alternativa mais segura.

Destinos não íntegros recebem solicitações do load balancer

Isso ocorre quando todos os destinos registrados não são íntegros. Se houver pelo menos um destino registrado íntegro, o Network Load Balancer roteará solicitações somente aos destinos registrados íntegros.

Quando houver apenas destinos registrados não íntegros, o Network Load Balancer roteará solicitações para todos os destinos registrados, o que é conhecido como modo de falha na abertura. O Network Load Balancer faz isso em vez de remover todos os endereços IP do DNS quando nenhum destino está íntegro e as respectivas zonas de disponibilidade não têm um destino íntegro para o qual enviar a solicitação.

As verificações de integridade HTTP ou HTTPS falham no destino devido à incompatibilidade do cabeçalho de host

O cabeçalho de host HTTP na solicitação de verificação de integridade contém o endereço IP do nó do load balancer e a porta do listener, não o endereço IP do destino e a porta de verificação de integridade. Se você estiver mapeando solicitações de entrada por cabeçalho de host, deverá garantir que as verificações de integridade correspondam a qualquer cabeçalho de host HTTP. Outra opção é adicionar um serviço HTTP separado em uma porta diferente e configurar o grupo de destino para usar essa porta para verificações de integridade. Como alternativa, considere usar verificações de integridade TCP.

Não é possível associar um grupo de segurança a um balanceador de carga

Se o Network Load Balancer foi criado sem grupos de segurança, ele não é compatível com grupos de segurança após a criação. Você só pode associar um grupo de segurança a um balanceador de carga durante a criação ou a um balanceador de carga existente que foi originalmente criado com grupos de segurança.

Não é possível remover todos os grupos de segurança

Se o Network Load Balancer foi criado com grupos de segurança, deve haver pelo menos um grupo de segurança associado a ele o tempo todo. Você não pode remover todos os grupos de segurança do balanceador de carga ao mesmo tempo.

Aumento na métrica TCP_ELB_Reset_Count

Para cada solicitação de TCP que um cliente faz por meio de um Network Load Balancer, o estado da conexão é rastreado. Se nenhum dado é enviado por meio da conexão pelo cliente ou pelo destino por um período que ultrapasse o tempo limite de inatividade, a conexão é fechada. Se um cliente envia dados depois do tempo limite de inatividade, ele recebe um pacote TCP RST para indicar que a conexão não é mais válida. Além disso. se um destino se tornar não íntegro, o balanceador de carga enviará um TCP RST para pacotes recebidos nas conexões de cliente associadas ao destino, a menos que o destino não íntegro acione o balanceador de carga para apresentar falha na abertura.

Se você observar um pico na métrica `TCP_ELB_Reset_Count` pouco antes ou logo após o aumento da métrica `UnhealthyHostCount`, provavelmente os pacotes TCP RST foram enviados porque o destino estava começando a falhar, mas não estava marcado como não íntegro. Se você observar aumentos persistentes em `TCP_ELB_Reset_Count` sem que as metas sejam marcadas como não íntegras, verifique os logs de fluxo da VPC para clientes que enviam dados em fluxos expirados.

As conexões expiram para solicitações de um destino para o load balancer

Verifique se a preservação de IP do cliente está habilitada no grupo de destino. O loopback NAT, também conhecido como hairpinning, não é compatível quando a preservação do IP do cliente está habilitada.

Se uma instância é um cliente de um balanceador de carga no qual está registrada e ela tem a preservação do IP do cliente habilitada, a conexão só é bem-sucedida se a solicitação é roteada para uma instância diferente. Se a solicitação for roteada para a mesma instância da qual foi enviada, a conexão expirará porque os endereços IP de origem e destino são os mesmos. Observe que isso se aplica aos pods do Amazon EKS executados na mesma instância de nó de processamento do EC2, mesmo que tenham endereços IP diferentes.

Se uma instância deve enviar solicitações para um load balancer com o qual está registrada, siga um destes procedimentos:

- Desabilite a preservação do IP do cliente. Em vez disso, use o Proxy Protocol v2 para obter o endereço IP do cliente.
- Certifique-se de que os contêineres que devem se comunicar estão em diferentes instâncias de contêiner.

O desempenho diminui ao mover destinos para um Network Load Balancer

Tanto os Classic Load Balancers quanto os Application Load Balancers usam multiplexação de conexão, mas os Network Load Balancers, não. Portanto, os destinos podem receber mais conexões TCP atrás de um Network Load Balancer. Certifique-se de que os destinos estejam preparados para lidar com o volume de solicitações de conexão que possam receber.

Erros de alocação de porta para fluxos de backend

Com o PrivateLink tráfego ou quando a preservação do IP do cliente está desativada, um Network Load Balancer suporta 55.000 conexões simultâneas ou cerca de 55.000 conexões por minuto para cada destino exclusivo (endereço IP e porta). Se você exceder esses limites, há uma chance maior de erros de alocação de porta. É possível rastrear os erros na alocação de portas por meio da métrica `PortAllocationErrorCount`. Você pode rastrear as conexões ativas usando a métrica `ActiveFlowCount`. Para obter mais informações, consulte CloudWatch métricas para seu Network Load Balancer.

Para corrigir erros na alocação de portas, é recomendável adicionar destinos ao grupo de destino.

Como opção, se não puder adicionar destinos ao grupo de destino, você poderá adicionar até 7 endereços IP secundários às interfaces de rede do balanceador de carga. Os endereços IP secundários são alocados automaticamente a partir dos blocos IPv4 CIDR das sub-redes correspondentes. Cada endereço IP secundário consome 6 unidades de endereçamento de rede. Após adicionar um endereço IP secundário, você não poderá removê-lo. A única maneira de liberar os endereços IP secundários é excluir o balanceador de carga.

Falha intermitente no estabelecimento da conexão TCP ou atrasos no estabelecimento da conexão TCP

Quando a preservação do endereço IP do cliente estiver habilitada, ele poderá se conectar a um endereço IP de destino diferente usando a mesma porta de origem temporária. Esses endereços IP de destino podem ser do mesmo balanceador de carga (em diferentes zonas de disponibilidade) quando o balanceamento de carga entre zonas estiver habilitado ou balanceadores de carga de rede diferentes, que usem o mesmo endereço IP de destino e porta, estiverem registrados. Nesse caso, se essas conexões forem roteadas para o mesmo endereço IP e porta de destino, haverá

uma conexão duplicada no destino, pois as conexões tiveram como origem o mesmo endereço IP e porta do cliente. Isso leva a erros de conexão e atrasos ao estabelecer uma dessas conexões. Isso ocorre com frequência quando um dispositivo NAT à frente do cliente e o mesmo endereço IP e porta de origem são alocados para a conexão a vários endereços IP do Network Load Balancer simultaneamente.

Você pode reduzir esse tipo de erro de conexão aumentando o número de portas de origem temporárias alocadas pelo cliente ou dispositivo NAT ou aumentando o número de destinos para o balanceador de carga. Recomendamos que os clientes alterem a porta de origem usada ao se reconectar após essas falhas de conexão. Para evitar esse tipo de erro de conexão, se você estiver usando um único Network Load Balancer, considere desabilitar o balanceamento de carga entre zonas ou, se estiver usando vários Network Load Balancers, considere não usar o mesmo endereço IP e porta de destino registrados em vários grupos de destino. Como alternativa, você pode desabilitar a preservação do IP do cliente. Se precisar do IP do cliente, você poderá recuperá-lo usando o Proxy Protocol v2. Para saber mais sobre o Proxy Protocol v2, consulte Protocolo de proxy.

Possível falha quando o balanceador de carga está sendo provisionado

Um dos motivos pelos quais um Network Load Balancer poderá falhar quando estiver sendo provisionado é se você usar um endereço IP que já está atribuído ou alocado em outro lugar (por exemplo, atribuído como endereço IP secundário para uma instância do EC2). Esse endereço IP impede que o balanceador de carga seja configurado e seu estado é `failed`. Você pode resolver isso ao remover a alocação do endereço IP associado e tentando novamente o processo de criação.

O tráfego é distribuído de forma desigual entre os destinos

Os receptores TCP e TLS fazem o roteamento de conexões TCP, enquanto que os receptores UDP fazem o roteamento de fluxos UDP. O balanceador de carga seleciona os destinos usando um algoritmo de hash de fluxo. Uma única conexão de um cliente é inerentemente fixa.

Se você perceber que alguns destinos parecem receber mais tráfego do que outros, recomendamos analisar os logs de fluxo da VPC. Compare o número de conexões exclusivas para cada endereço IP de destino. Mantenha o período de tempo o mais curto possível, pois o registro, o cancelamento do registro e os destinos não íntegros influenciam esses números de conexão.

A seguir, possíveis cenários em que as conexões podem ser distribuídas de forma desigual:

- Se você começar com um pequeno número de destinos e registrar destinos adicionais posteriormente, os destinos originais ainda terão conexões com os clientes. Com uma workload HTTP, os keepalives garantem que os clientes reutilizem as conexões. Se você diminuir o número máximo de keepalives em sua aplicação da Web, os clientes abrirão novas conexões com mais frequência.
- Se a aderência do grupo de destino estiver habilitada, se houver um pequeno número de clientes, e os clientes se comunicarem por meio de um dispositivo NAT com um único endereço IP de origem, as conexões desses clientes serão roteadas para o mesmo destino.
- Se o balanceamento de carga entre zonas estiver desabilitado e os clientes preferirem o endereço IP do balanceador de carga de uma das zonas do balanceador de carga, as conexões serão distribuídas de forma desigual entre as zonas do balanceador de carga.

A resolução de nomes de DNS contém menos endereços IP do que as zonas de disponibilidade habilitadas

Idealmente, seu Network Load Balancer fornece um endereço IP por zona de disponibilidade habilitada quando ele têm pelo menos um host íntegro na zona de disponibilidade. Quando não houver um host íntegro em uma zona de disponibilidade específica e o balanceamento de carga entre zonas estiver desativado, o endereço IP do Network Load Balancer respectivo a essa AZ será removido do DNS.

Por exemplo, suponha que o Network Load Balancer tenha três zonas de disponibilidade habilitadas, todas com pelo menos uma instância de destino registrada íntegra.

- Se as instâncias de destino registradas na zona de disponibilidade A se tornarem não íntegras, o endereço IP correspondente da zona de disponibilidade A para o Network Load Balancer será removido do DNS.
- Se duas das zonas de disponibilidade habilitadas não tiverem instâncias de destino registradas íntegras, os respectivos dois endereços IP do Network Load Balancer serão removidos do DNS.
- Se não houver nenhuma instância de destino registrada íntegra em todas as zonas de disponibilidade habilitadas, o modo de abertura de falha será ativado e o DNS fornecerá todos os endereços IP das três habilitadas AZs no resultado.

Pacotes IP fragmentados não são roteados para os destinos

Os Network Load Balancers não são compatíveis com pacotes IP fragmentados para tráfego não UDP.

Solucionar problemas de destinos não íntegros usando o mapa de recursos

Se suas metas do Network Load Balancer estiverem falhando nas verificações de integridade, você poderá usar o mapa de recursos para encontrar destinos não íntegros e realizar ações com base no código do motivo da falha. Para obter mais informações, consulte Visualizar o mapa de recursos do Network Load Balancer.

O mapa de recursos fornece duas exibições: Visão geral e Mapa de destino não íntegro. A opção Visão geral é selecionada por padrão e exibe todos os recursos do seu balanceador de carga. Selecionar a visualização Mapa de destinos não íntegros exibirá somente os destinos não íntegros em cada grupo de destino associado ao Network Load Balancer.

> **Note**
>
> A opção Mostrar detalhes do recurso deverá estar ativada para que seja possível visualizar o resumo da verificação de integridade e as mensagens de erro de todos os recursos aplicáveis no mapa de recursos. Se não estiver habilitada, será necessário selecionar cada recurso para visualizar seus detalhes.

A coluna Grupos de destino exibe um resumo dos destinos íntegros e não íntegros de cada grupo de destino. Isso pode ajudar a determinar se todos os destinos estão falhando nas verificações de integridade ou se somente destinos específicos estão falhando. Se todos os destinos em um grupo de destino falharem nas verificações de integridade, verifique as configurações da verificação de integridade do grupo de destino. Selecione o nome de um grupo de destino para abrir sua página de detalhes em uma nova guia.

A coluna Destinos exibe o TargetID e o status atual da verificação de integridade de cada destino. Quando um destino não está íntegro, o código do motivo da falha da verificação de integridade é exibido. Quando um único destino está falhando em uma verificação de integridade, verifique se o destino tem recursos suficientes. Selecione um ID de destino para abrir sua página de detalhes em uma nova guia.

Selecionar Exportar oferece a você a opção de exportar a visualização atual do mapa de recursos do seu Network Load Balancer como PDF.

Verifique se a sua instância está falhando nas verificações de integridade e, com base no código de motivo da falha, verifique os seguintes problemas:

- Não íntegro: a solicitação excedeu o tempo limite
  - Verifique se os grupos de segurança e as listas de controle de acesso (ACL) à rede associados aos seus destinos e ao Network Load Balancer não estão bloqueando a conectividade.
  - Verifique se o destino tem capacidade suficiente disponível para aceitar conexões do Network Load Balancer.
  - As respostas da verificação de integridade do Network Load Balancer podem ser visualizadas nos registros de aplicações de cada destino. Para obter mais informações, consulte Códigos de motivo da verificação de integridade.
- Insalubre: FailedHealthChecks
  - Verifique se o destino está escutando tráfego na porta de verificação de integridade.

    Ao usar um receptor TLS

    Você escolhe qual política de segurança é usada para conexões de frontend. A política de segurança usada em conexões de backend é selecionada automaticamente com base na política de segurança de frontend em uso. Se algum de seus ouvintes tiver:

    - Política de TLS pós-quântico FIPS - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-FIPS-PQ-2025-09`
    - Política FIPS - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`
    - Política de TLS pós-quântico - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-PQ-2025-09`
    - Política TLS 1.3 - Uso de conexões de back-end `ELBSecurityPolicy-TLS13-1-0-2021-06`
    - Todas as outras políticas TLS que as conexões de back-end usam `ELBSecurityPolicy-2016-08`

    Para obter mais informações, consulte Políticas de segurança.
  - Verifique se o destino está fornecendo um certificado e uma chave de servidor no formato correto especificado pela política de segurança.

- Verifique se o destino oferece suporte uma ou mais cifras correspondentes e a um protocolo fornecido pelo Network Load Balancer para estabelecer handshakes TLS.

Cotas para seus Network Load Balancers

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas.

Para visualizar as cotas para Network Load Balancers, abra o Console do Service Quotas. No painel de navegação, escolha Serviços da AWS e selecione Elastic Load Balancing. Você também pode usar o comando describe-account-limits(AWS CLI) para o Elastic Load Balancing.

Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, envie uma solicitação para um aumento de cotas de serviço.

Cotas

- Balanceador de carga
- Grupos de destino
- Unidades de capacidade do balanceador de carga

Balanceador de carga

Você Conta da AWS tem as seguintes cotas relacionadas aos balanceadores de carga de rede.

Nome	Padrão	Ajustável
Certificados por Network Load Balancer	25	Sim
Ouvintes por Network Load Balancer	50	Não
Network Load Balancer ENIs por VPC	1.200 [1]	Sim
Network Load Balancers por região	50	Sim
Destinos por zona de disponibilidade por Network Load Balancer	500 [2, 3]	Sim
Destinos por Network Load Balancer	3.000 [3]	Sim

¹ Cada Network Load Balancer usa uma interface de rede por zona. A cota é definida no nível da VPC. Ao compartilhar sub-redes ou VPCs, o uso é calculado em todos os locatários.

² Se um destino for registrado com N grupos de destino, ele contará como N destinos com relação a esse limite. Cada Application Load Balancer que é um destino do Network Load Balancer conta como 50 destinos quando o balanceamento de carga entre zonas está desabilitado, ou como cem destinos quando o balanceamento de carga entre zonas está habilitado.

³ Se o balanceamento de carga entre zonas estiver habilitado, o máximo será de 500 destinos por balanceador de carga, independentemente do número de zonas de disponibilidade.

Grupos de destino

As cotas a seguir são para grupos de destino.

Nome	Padrão	Ajustável
Grupos de destino por região	3.000 ₁	Sim
Destinos por grupo de destino por região (instâncias ou endereços IP)	1.000	Sim
Destinos por grupo de destino por região (Application Load Balancers)	1	Não

* Essa cota é compartilhada por Application Load Balancers e Network Load Balancers.

Unidades de capacidade do balanceador de carga

As cotas a seguir são para Load Balancer Capacity Units LCUs ().

Nome	Padrão	Ajustável
Unidades de capacidade de balanceador de carga de rede reservadas (LCUs) por balanceador de carga de rede, por zona de disponibilidade	45000	Sim

Nome	Padrão	Ajustável
Unidades de capacidade reservadas do Network Load Balancer (LCU) por região	0	Sim

Histórico dos documentos dos Network Load Balancers

A tabela a seguir descreve as versões dos Network Load Balancers.

Alteração	Descrição	Data
Grupos de destino ponderados	Esta versão adiciona suporte para ações padrão com grupos-alvo ponderados.	19 de novembro de 2025
Suporte aos protocolos QUIC e TCP_QUIC	Esta versão adiciona suporte aos protocolos QUIC e TCP_QUIC.	13 de novembro de 2025
IPv4 Endereços secundários	Esta versão adiciona suporte para adicionar IPv4 endereços secundários às interfaces de rede do balanceador de carga.	29 de julho de 2025
Desabilitar zonas de disponibilidade	Esta versão adiciona suporte para desabilitar uma zona de disponibilidade de um balanceador de carga existente.	13 de fevereiro de 2025
Reservas de unidade de capacidade	Esta versão inclui suporte para definir uma capacidade mínima para seu balanceador de carga.	20 de novembro de 2024
O suporte UDP acabou IPv6 para balanceadores de carga de pilha dupla	Esta versão permite que os clientes acessem aplicativos baseados em UDP usando. IPv6	31 de outubro de 2024
Certificados RSA de 3072 bits e ECDSA de 256/384/521 bits	Esta versão adiciona suporte para certificados RSA de 3072 bits e certificados Elliptic	19 de janeiro de 2024

	Curve Digital Signature Algorithm (ECDSA) de 256, 384 e 521 bits via (ACM). AWS Certificate Manager	
Encerramento de TLS com FIPS 140-3	Esta versão adiciona políticas de segurança que usam módulos criptográficos do FIPS 140-3 ao encerrar conexões TLS.	20 de novembro de 2023
Afinidade de DNS de zona	Esta versão adiciona suporte a clientes que resolvem o DNS do balanceador de carga para receber um endereço IP na mesma Zona de Disponibi lidade (AZ) em que estão.	12 de outubro de 2023
Desabilitar encerramento de conexão de destino não íntegra	Esta versão adiciona suporte para manter conexões ativas com destinos que falham nas verificações de integridade.	12 de outubro de 2023
Encerramento de conexão UDP padrão	Esta versão adiciona suporte ao encerramento de conexões UDP no final do tempo limite de cancelamento do registro por padrão.	12 de outubro de 2023
Registre alvos usando IPv6	Esta versão adiciona suporte para registrar instâncias como destinos quando abordadas por IPv6.	2 de outubro de 2023
Grupos de segurança para o Network Load Balancer	Esta versão adiciona suporte para associar grupos de segurança aos Network Load Balancers na criação.	10 de agosto de 2023

Integridade do grupo de destino	Esta versão adiciona suporte para configurar a contagem ou a porcentagem mínima de destinos que devem estar íntegros e quais ações o balanceador de carga executará quando o limite não for atingido.	17 de novembro de 2022
Configuração de verificação de integridade	Esta versão fornece melhorias para a configuração da verificação de integridade.	17 de novembro de 2022
Balanceamento de carga entre zonas	Esta versão adiciona suporte para configurar o balanceamento de carga entre zonas em nível de grupo de destino.	17 de novembro de 2022
IPv6 grupos-alvo	Esta versão adiciona suporte para configurar IPv6 grupos-alvo para balanceadores de carga de rede.	23 de novembro de 2021
IPv6 balanceadores de carga internos	Esta versão adiciona suporte para configurar IPv6 grupos-alvo para balanceadores de carga de rede.	23 de novembro de 2021
TLS 1.3	Esta versão adiciona políticas de segurança compatíveis com TLS versão 1.3.	14 de outubro de 2021
Application Load Balancers como destinos	Esta versão adiciona suporte para configurar um Application Load Balancer como destino de um Network Load Balancer.	27 de setembro de 2021

Preservação do IP do cliente	Esta versão adiciona suporte para configurar a preservação do IP do cliente.	4 de fevereiro de 2021
Política de segurança para FS compatível com TLS versão 1.2	Esta versão adiciona uma política de segurança para Forward Secrecy (FS – Sigilo de encaminhamento) compatível com TLS versão 1.2.	24 de novembro de 2020
Modo de pilha dupla	Esta versão adiciona suporte ao modo de pilha dupla, que permite que os clientes se conectem ao balanceador de carga usando endereços e IPv4 endereços. IPv6	13 de novembro de 2020
Encerramento da conexão no cancelamento do registro	Esta versão adiciona suporte para encerrar conexões com destinos cujo registro foi cancelado no final do tempo limite de cancelamento do registro.	13 de novembro de 2020
Políticas ALPN	Esta versão adiciona suporte para listas de preferências de ALPN (Application-Layer Protocol Negotiation).	27 de maio de 2020
Sessões persistentes	Esta versão adiciona suporte para sticky sessions com base no protocolo e no endereço IP de origem.	28 de fevereiro de 2020

Sub-redes compartilhadas	Esta versão adiciona suporte para especificar sub-redes que foram compartilhadas com você por outra Conta da AWS.	26 de novembro de 2019
Endereços IP privados	Essa versão permite que você forneça um endereço IP privado do intervalo de IPv4 endereços da sub-rede que você especifica ao ativar uma zona de disponibilidade para um balanceador de carga interno.	25 de novembro de 2019
Adicionar sub-redes	Esta versão adiciona suporte para habilitar zonas de disponibilidade adicionais após a criação do seu load balancer.	25 de novembro de 2019
Políticas de segurança para FS	Essa versão adiciona suporte para três políticas adicionais de segurança de sigilo de encaminhamento predefinidas.	8 de outubro de 2019
Suporte a SNI	Esta versão acrescenta suporte a SNI (Server Name Indication, indicação de nome de servidor).	12 de setembro de 2019
Protocolo UDP	Esta versão adiciona suporte ao protocolo UDP.	24 de junho de 2019
Disponível em nova região	Esta versão adiciona suporte a Network Load Balancers na região Ásia-Pacífico (Osaka).	12 de junho de 2019

Protocolo TLS	Esta versão inclui suporte ao protocolo TLS.	24 de janeiro de 2019
Balanceamento de carga entre zonas	Esta versão adiciona suporte o balanceamento de carga entre zonas.	22 de fevereiro de 2018
Protocolo de proxy	Esta versão inclui o suporte para habilitar o Proxy Protocol.	17 de novembro de 2017
Endereços IP como destinos	Esta versão inclui o suporte para registrar endereços IP como destinos.	21 de setembro de 2017
Novo tipo de balanceador de carga	Esta versão do Elastic Load Balancing apresenta Network Load Balancers.	7 de setembro de 2017

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.