aws

Network Load Balancers

Elastic Load Balancing

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Elastic Load Balancing: Network Load Balancers

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

O que é um Network Load Balancer? 1
Componentes do Network Load Balancer 1
Visão geral do Network Load Balancer 2
Benefícios da migração de um Classic Load Balancer 3
Como começar a usar 4
Definição de preço 4
Conceitos básicos 5
Antes de começar 5
Etapa 1: configurar o grupo de destino 5
Etapa 2: escolher um tipo de balanceador de carga 6
Etapa 3: configurar o balanceador de carga e um receptor 7
Etapa 4: testar o balanceador de carga 8
Etapa 5: (opcional) excluir o balanceador de carga 8
Conceitos básicos do uso da AWS CLI 10
Antes de começar 10
Criar um balanceador de carga IPv4 10
Criar o balanceador de carga dualstack 12
Especificar um endereço IP elástico para o load balancer 13
Excluir o load balancer 14
Balanceadores de cargas 15
Estado do load balancer 16
Atributos do load balancer 16
Tipo de endereço IP 17
Mapa de recursos do balanceador de carga 18
Componentes do mapa de recursos 18
Zonas de disponibilidade 19
Balanceamento de carga entre zonas 21
Proteção contra exclusão 21
Tempo limite de inatividade da conexão 22
Nome DNS 23
Afinidade de DNS de zona de disponibilidade 24
Monitoramento 26
Ativar a afinidade de zona de disponibilidade 27
Desativar a afinidade de zona de disponibilidade 27

Criar um balanceador de carga ... 28
Etapa 1: configurar um grupo de destino ... 28
Etapa 2: registrar destinos ... 30
Etapa 3: configurar um balanceador de carga e um receptor ... 30
Etapa 4: testar o balanceador de carga ... 8
Atualizar o tipo de endereço ... 33
Grupos de segurança ... 34
Considerações ... 35
Exemplo: filtro de tráfego de clientes ... 36
Exemplo: aceitar tráfego somente do balanceador de carga ... 36
Atualizar os grupos de segurança associados ... 37
Atualizar as configurações de segurança ... 38
Monitirar grupos de segurança do balanceador de carga ... 38
Atualizar tags ... 39
Excluir um balanceador de carga ... 40
Mudança de zona ... 41
Iniciar uma mudança de zona ... 42
Atualizar uma mudança de zona ... 43
Cancelar uma mudança de zona ... 44
Listeners ... 45
Configuração do receptor ... 45
Regras do listener ... 46
Criar um listener ... 46
Pré-requisitos ... 46
Adicionar um listener ... 47
Configurar os listeners TLS ... 48
Certificados de servidor ... 48
Políticas de segurança ... 51
Políticas ALPN ... 74
Atualizar um listener ... 75
Atualizar um listener TLS ... 76
Substituir o certificado padrão ... 76
Adicionar certificados à lista de certificados ... 77
Remover certificados da lista de certificados ... 78
Atualizar a política de segurança ... 78
Atualizar a política ALPN ... 79

Excluir um listener ... 80
Grupos de destino ... 81
Configuração de roteamento ... 82
Target type ... 83
Roteamento de solicitações e endereços IP ... 84
Recursos on-premises como destinos ... 85
Tipo de endereço IP ... 86
Destinos registrados ... 86
Atributos do grupo de destino ... 87
Preservação do IP do cliente ... 89
Atraso do cancelamento do registro ... 92
Protocolo de proxy ... 93
Conexões de verificação de integridade ... 94
Serviços do VPC endpoint ... 94
Habilitar o Proxy Protocol ... 95
Sessões persistentes ... 95
Criar um grupo de destino ... 96
Configurar verificações de integridade ... 98
Configurações de verificação de integridade ... 100
Status de integridade do destino ... 103
Códigos de motivo de verificação de integridade ... 104
Verificar a integridade de seus destinos ... 105
Modificar as configurações de verificação de integridade de um grupo de destino ... 106
Balanceamento de carga entre zonas ... 107
Modificar o balanceamento de carga entre zonas para um balanceador de carga ... 108
Modificar balanceamento de carga entre zonas para um grupo de destino ... 108
Integridade do grupo de destino ... 109
Ações para estado não íntegro ... 109
Requisitos e considerações ... 109
Exemplo ... 110
Modificar configurações de integridade do grupo de destino ... 112
Encerramento da conexão para destinos não íntegros ... 113
Como usar o failover de DNS do Route 53 para o seu balanceador de carga ... 114
Registrar destinos ... 115
Grupos de segurança de destino ... 116
Network ACLs ... 117

Sub-redes compartilhadas 120
Registrar ou cancelar o registro de destinos 120
Application Load Balancers como destinos 123
Etapa 1:criar o Application Load Balancer 124
Etapa 2: criar o grupo de destino 125
Etapa 3: criar o Network Load Balancer 127
Etapa 4: (opcional) habilitar AWS PrivateLink 128
Atualizar tags 129
Excluir um grupo de destino 130
Monitorar os balanceadores de carga 131
CloudWatch métricas 132
Métricas do Network Load Balancer 133
Dimensões métricas dos Network Load Balancers 145
Estatísticas para métricas do Network Load Balancer 146
Veja CloudWatch as métricas do seu balanceador de carga 147
Logs de acesso 149
Arquivos do log de acesso 149
Entradas do log de acesso 151
Requisitos do bucket 154
Habilitar registro em log de acesso 156
Desabilitar registro em log de acesso 157
Processar arquivos de log de acesso 157
CloudTrail troncos 158
Informações sobre o Elastic Load Balancing em CloudTrail 158
Noções básicas sobre entradas de arquivo de log do Elastic Load Balancing 159
Solução de problemas 162
Um destino registrado não está em serviço 162
As solicitações não são roteadas para os destinos 162
Os destinos recebem mais solicitações de verificação de integridade do que o esperado 163
Os destinos recebem menos solicitações de verificação de integridade do que o esperado 163
Destinos não íntegros recebem solicitações do load balancer 163
As verificações de integridade HTTP ou HTTPS falham no destino devido à incompatibilidade do cabeçalho de host 164
Não é possível associar um grupo de segurança a um balanceador de carga 164
Não é possível remover todos os grupos de segurança 164
Aumento na métrica TCP_ELB_Reset_Count 164

As conexões expiram para solicitações de um destino para o load balancer 165
O desempenho diminui ao mover destinos para um Network Load Balancer 165
Erros de alocação de portas conectando-se por AWS PrivateLink 166
Falha intermitente de conexão quando a preservação do IP do cliente está habilitada 166
Atrasos na conexão TCP 166
Possível falha quando o balanceador de carga está sendo provisionado 167
A resolução de nomes de DNS contém menos endereços IP do que as zonas de disponibilidade habilitadas 167
Solucione problemas de alvos não íntegros usando o mapa de recursos 168
Cotas 170
Histórico do documento 172
..... clxxvii

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 dos Network Load Balancers, são compatíveis com os protocolos TCP, UDP, TCP_UDP e TLS. 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 a um grupo de destino especificado em uma regra de listeners para seu load balancer.

Para obter mais informações, consulte a seguinte documentação do :

- 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 processar milhões de solicitações por segundo. Após o load balancer receber uma solicitação de conexão, ele seleciona um destino no grupo de destino para a regra padrão. Ele tenta abrir uma conexão TCP para o destino selecionado na porta especificada na configuração do listener.

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 ter mais informações, consulte Zonas de disponibilidade.

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.

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 IDs de instância, endereços IP ou um Application Load Balancer. O tipo de destino também afeta se os endereços IP do cliente são preservados. Para ter 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.

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

Como começar a usar

Para criar um Network Load Balancer, tente um dos seguintes tutoriais:

- Conceitos básicos sobre Network Load Balancers
- Tutorial: criar um Network Load Balancer usando a AWS CLI

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

Definição de preço

Para obter mais informações, consulte Preço do Network Load Balancer.

Conceitos básicos sobre Network Load Balancers

Este tutorial fornece uma introdução prática aos balanceadores de carga de rede por meio da AWS Management Console, uma interface baseada na web. Para criar seu primeiro Network Load Balancer, conclua as etapas a seguir.

Tarefas

- Antes de começar
- Etapa 1: configurar o grupo de destino
- Etapa 2: escolher um tipo de balanceador de carga
- Etapa 3: configurar o balanceador de carga e um receptor
- Etapa 4: testar o balanceador de carga
- Etapa 5: (opcional) excluir o balanceador de carga

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

Antes de começar

- Decida quais Zonas de disponibilidade você usará para suas instâncias do EC2. Configure sua nuvem privada virtual (VPC) com, pelo menos, uma sub-rede pública em cada uma destas Zonas de disponibilidade. Essas sub-redes públicas são usadas para configurar o load balancer. Você pode executar suas instâncias do EC2 em outras sub-redes dessas zonas de disponibilidade.
- Execute pelo menos uma instância EC2 em cada Zona de disponibilidade. Certifique-se de que os security groups dessas instâncias permitam acesso ao TCP de clientes na porta do listener e solicitações para verificação de integridade de sua VPC. Para ter mais informações, consulte Grupos de segurança de destino.

Etapa 1: configurar o grupo de destino

Crie um grupo de destino, que é usado no roteamento da solicitação. A regra do seu listener roteia solicitações para os destinos registrados neste grupo de destino. O load balancer verifica a integridade dos destinos desse grupo de destino usando as configurações de verificação de integridade definidas para o grupo de destino.

Para configurar seu grupo-alvo usando o console

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 Criar grupo de destino.
4. Mantenha o tipo de destino como instâncias.
5. Em Nome do grupo de destino, digite um nome para o novo grupo de destino.
6. Em Protocolo, escolha TCP e, em Porta, escolha 80.
7. Em VPC, escolha a VPC que contém suas instâncias.
8. Para Health checks (Verificações de integridade), mantenha as configurações padrão.
9. Escolha Próximo.
10. Na página Registrar destinos, conclua as etapas a seguir. Esta é uma etapa opcional para a criação de um grupo de destino. No entanto, você deve registrar os destinos se quiser testar o balanceador de carga e garantir que ele esteja direcionando o tráfego para os destinos.
    a. Em Instâncias disponíveis, selecione uma ou mais instâncias.
    b. Mantenha a porta 80 padrão e escolha Incluir como pendente abaixo.
11. Selecione Criar grupo de destino.

Etapa 2: escolher um tipo de balanceador de carga

O Elastic Load Balancing oferece suporte para diferentes tipos de balanceadores de carga. Neste tutorial, você criará um Network Load Balancer.

Para criar um Network Load Balancer usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha uma região para seu balanceador de carga. Não deixe de escolher a mesma região usada para as instâncias do EC2.
3. No painel de navegação, em Load Balancing, selecione Load Balancers.
4. Selecione Criar um balanceador de carga.
5. Em Network Load Balancer, escolha Criar.

Etapa 3: configurar o balanceador de carga e um receptor

Para criar um Network Load Balancer, você deve primeiro fornecer informações básicas para o balanceador de carga, como nome, esquema e tipo de endereço IP. Em seguida, forneça informações sobre a rede e sobre um ou mais receptores. Um listener é um processo que verifica se há solicitações de conexão. Ele é configurado com um protocolo e uma porta para as conexões de clientes com o load balancer. Para obter mais informações sobre protocolos e portas suportados, consulte Configuração do receptor.

Para configurar seu load balancer e seu listener

1. Em Load balancer name (Nome do balanceador de carga), insira um nome para o seu balanceador de carga. Por exemplo, `my-nlb`.
2. Para Esquema e Tipo de endereço IP, mantenha os valores padrão.
3. Em Mapeamento de rede, selecione a VPC usada para as instâncias do EC2. Para cada zona de disponibilidade usada para executar as instâncias do EC2, selecione a zona de disponibilidade e selecione uma sub-rede pública para essa zona de disponibilidade.

   Por padrão, AWS atribui um endereço IPv4 a cada nó do balanceador de carga da sub-rede para sua zona de disponibilidade. Como alternativa, ao criar um load balancer voltado para a Internet, será possível selecionar um endereço IP elástico para cada zona de disponibilidade. Isso fornece o balanceador de carga com endereços IP estáticos.
4. Em Grupos de segurança, selecionamos previamente o grupo de segurança padrão para sua VPC. Você pode selecionar outros grupos de segurança, conforme necessário. Se você não tiver um grupo de segurança adequado, escolha Criar um novo grupo de segurança e crie um que atenda às suas necessidades de segurança. Para obter mais informações, consulte Criar um grupo de segurança no Guia do usuário da Amazon VPC.

   > **Warning**
   >
   > Se você não associar grupos de segurança ao balanceador de carga agora, não poderá associá-los posteriormente.
5. Em Receptores e roteamento, mantenha o protocolo e a porta padrão e selecione o grupo de destino na lista. Isso configura um receptor que aceita tráfego TCP na porta 80 e encaminha o tráfego para o grupo de destino selecionado por padrão.

6. (Opcional) Adicione tags para caracterizar o balanceador de carga. As chaves de tag devem ser exclusivas de cada load balancer. Os caracteres permitidos são letras, espaços, números (em UTF-8) e os caracteres especiais a seguir: + - = . _ : / @. Não use espaços no início nem no fim. Os valores de tags diferenciam maiúsculas de minúsculas.
7. Revise sua configuração e escolha Create load balancer (Criar um balanceador de carga). Alguns atributos padrão são aplicados ao balanceador de carga durante a criação. Você pode visualizá-los e editá-los depois de criar o balanceador de carga. Para ter mais informações, consulte Atributos do load balancer.

Etapa 4: testar o balanceador de carga

Depois de criar o load balancer, verifique se está enviando tráfego para suas instâncias EC2.

Para testar seu load balancer

1. Após receber a notificação sobre a criação do load balancer com êxito, selecione Fechar.
2. No painel de navegação, em Balanceamento de carga, selecione Grupos de destino.
3. Selecione o grupo de destino recém-criado.
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 `healthy`, você pode testar seu load balancer.
5. No painel de navegação, em Load Balancing, selecione Load Balancers.
6. Selecione o nome do balanceador de carga recém-criado para abrir a página de detalhes dele.
7. Copie o nome DNS do balanceador de carga (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.

Etapa 5: (opcional) excluir o balanceador de carga

Assim que o load balancer é disponibilizado, você será cobrado por cada hora ou hora parcial em que mantê-lo em execução. Quando não precisar mais do load balancer, pode excluí-lo. Assim que o load balancer for excluído, a cobrança será interrompida. Observe que a exclusão de um load

balancer não afeta os destinos registrados com o load balancer. Por exemplo, as instâncias EC2 continuam a ser executadas.

Para excluir seu 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, em Load Balancing, selecione Load Balancers.
3. Marque a caixa de seleção do balanceador de carga e escolha Ações, Excluir.
4. Quando a confirmação for solicitada, insira **`confirm`** e escolha Excluir.

Tutorial: criar um Network Load Balancer usando a AWS CLI

Este tutorial fornece uma introdução prática a Network Load Balancers por meio da AWS CLI.

Antes de começar

- Instale a AWS CLI ou faça a atualização para a versão atual da AWS CLI caso você esteja usando uma versão que não é compatível com Network Load Balancers. Para obter mais informações, consulte Instalar a AWS Command Line Interface no Guia do usuário da AWS Command Line Interface.
- Decida quais Zonas de disponibilidade você usará para suas instâncias do EC2. Configure sua nuvem privada virtual (VPC) com, pelo menos, uma sub-rede pública em cada uma destas Zonas de disponibilidade.
- Decida se você criará um balanceador de carga IPv4 ou dualstack. Use IPv4 se quiser que seus clientes se comuniquem com o balanceador de carga usando somente endereços IPv4. Use dualstack se você quiser que seus clientes se comuniquem com o balanceador de carga usando endereços IPv4 e IPv6. Você também pode usar dualstack para se comunicar com destinos de back-end, como aplicações IPv6 ou sub-redes dualstack, usando IPv6.
- Execute pelo menos uma instância EC2 em cada Zona de disponibilidade. Certifique-se de que os security groups dessas instâncias permitam acesso ao TCP de clientes na porta do listener e solicitações para verificação de integridade de sua VPC. Para ter mais informações, consulte Grupos de segurança de destino.

Criar um balanceador de carga IPv4

Para criar seu primeiro load balancer, conclua as etapas a seguir.

Criar um balanceador de carga IPv4

1. Use o create-load-balancercomando para criar um balanceador de carga IPv4, especificando uma sub-rede pública para cada zona de disponibilidade na qual você executou instâncias. Você pode especificar somente uma sub-rede por Zona de disponibilidade.

   Por padrão, quando Network Load Balancers são criados por meio da AWS CLI, eles não usam automaticamente o grupo de segurança padrão para a VPC. Se você não associar grupos de

segurança ao balanceador de carga durante a criação, não poderá adicioná-los posteriormente. Recomendamos que você especifique grupos de segurança para o balanceador de carga durante a criação usando a opção `--security-groups`.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --security-groups sg-0123456789EXAMPLE
```

O resultado inclui o Nome de recurso da Amazon (ARN) do load balancer, com o seguinte formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/net/my-load-
balancer/1234567890123456
```

2. Use o create-target-groupcomando para criar um grupo-alvo IPv4, especificando a mesma VPC que você usou para suas instâncias do EC2. Os grupos de destino IPv4 oferecem suporte a destinos de tipo de IP e de instância.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-0598c7d356EXAMPLE
```

A saída inclui o ARN do grupo de destino, com este formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Use o comando register-targets para registrar suas instâncias com o grupo de destino:

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets
 Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

4. Use o comando create-listener para criar um listener para seu load balancer com uma regra padrão que encaminha solicitações ao seu grupo de destino:

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

A saída contém o ARN do listener, com o seguinte formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/net/my-load-
balancer/1234567890123456/1234567890123456
```

5. (Opcional) Você pode verificar a integridade dos alvos registrados para seu grupo-alvo usando este describe-target-healthcomando:

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

Criar o balanceador de carga dualstack

Para criar seu primeiro load balancer, conclua as etapas a seguir.

Criar um balanceador de carga dualstack

1. Use o create-load-balancercomando para criar um balanceador de carga de pilha dupla, especificando uma sub-rede pública para cada zona de disponibilidade na qual você executou instâncias. Você pode especificar somente uma sub-rede por Zona de disponibilidade.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --ip-address-type dualstack
```

   O resultado inclui o Nome de recurso da Amazon (ARN) do load balancer, com o seguinte formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/net/my-load-
balancer/1234567890123456
```

2. Use o create-target-groupcomando para criar um grupo-alvo, especificando a mesma VPC que você usou para suas instâncias do EC2.

   Você deve usar um grupo de destino TCP ou TLS com o balanceador de carga dualstack.

   Você pode criar grupos de destino IPv4 e IPv6 para associá-los a balanceadores de carga dualstack. O tipo de endereço IP do grupo de destino determina a versão do IP que o balanceador de carga usará para se comunicar e verificar a integridade dos destinos de back-end.

Os grupos de destino IPv4 oferecem suporte a destinos de tipo de IP e de instância. Os destinos IPv6 só são compatíveis com destinos IP.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
 vpc-0598c7d356EXAMPLE  --ip-address-type [ipv4 or ipv6]
```

A saída inclui o ARN do grupo de destino, com este formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

3. Use o comando register-targets para registrar suas instâncias com o grupo de destino:

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets
 Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

4. Use o comando create-listener para criar um receptor para o balanceador de carga com uma regra padrão que encaminhe solicitações ao grupo de destino. Os balanceadores de carga dualstack devem ter receptores TCP ou TLS.

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

A saída contém o ARN do listener, com o seguinte formato:

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/net/my-load-
balancer/1234567890123456/1234567890123456
```

5. (Opcional) Você pode verificar a integridade dos alvos registrados para seu grupo-alvo usando este describe-target-healthcomando:

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

Especificar um endereço IP elástico para o load balancer

Quando você cria um Network Load Balancer, pode especificar um endereço IP elástico por sub-rede usando um mapeamento de sub-rede.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \
--subnet-mappings SubnetId=subnet-0e3f5cac72EXAMPLE,AllocationId=eipalloc-12345678
```

Excluir o load balancer

Quando você não precisar mais de seu load balancer e grupo de destino, pode excluí-los da seguinte forma:

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Network Load Balancers

Um load balancer serve como ponto único de contato para os clientes. Os clientes enviam solicitações para o load balancer, e ele as envia para os destinos, como instâncias do EC2, em uma ou mais Zonas de disponibilidade.

Para configurar o load balancer, você cria grupos de destino e, em seguida, registra os destinos nesses grupos. O load balancer é mais eficaz se você garantir que cada Zona de disponibilidade ativada 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 AWS Direct Connect, VPN gerenciada e soluções VPN de terceiros.

Conteúdo

- Estado do load balancer
- Atributos do load balancer
- Tipo de endereço IP
- Mapa de recursos do Network Load Balancer
- Zonas de disponibilidade
- Balanceamento de carga entre zonas
- Proteção contra exclusão
- Tempo limite de inatividade da conexão
- Nome DNS
- Afinidade de DNS de zona de disponibilidade
- Criar um Network Load Balancer
- Tipos de endereço IP para o Network Load Balancer
- Grupos de segurança para o Network Load Balancer
- Tags para o Network Load Balancer
- Excluir um Network Load Balancer
- Mudança de zona

Estado do load balancer

Um balanceador de carga pode estar em um dos seguintes estados:

`provisioning`

O load balancer está sendo configurado.

`active`

O load balancer está totalmente configurado e pronto para rotear o tráfego.

`failed`

O balanceador de carga não pôde ser configurado.

Atributos do load balancer

Um balanceador de carga tem os seguintes atributos:

`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 ter 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 balanceador de carga, impedindo o acesso não intencional ao balanceador de carga interno por meio de um gateway da Internet. Ele está configurado como `false` para balanceadores de carga voltados para a Internet e `true` para balanceadores de carga 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). AWS 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 do balanceador de carga. 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.

Tipo de endereço IP

É possível definir os tipos de endereços IP que os clientes podem usar com o balanceador de carga.

Os balanceadores de carga de rede oferecem suporte aos seguintes tipos de endereço IP:

`ipv4`

Os clientes devem se conectar ao balanceador de carga usando endereços IPv4 (por exemplo, 192.0.2.1). Os balanceadores de carga habilitados para IPv4 (tanto voltados para a Internet quanto internos) são compatíveis com receptores TCP, UDP, TCP_UDP e TLS.

`dualstack`

Os clientes podem se conectar ao load balancer usando endereços IPv4 (por exemplo, 192.0.2.1) e endereços IPv6 (por exemplo, 2001:0db8:85a3:0:0:8a2e:0370:7334). Os balanceadores de carga dualstack (tanto voltados para a Internet quanto internos) são compatíveis com receptores TCP e TLS.

Considerações

- O balanceador de carga se comunica com os destinos com base no tipo de endereço IP do grupo de destino.
- Quando você habilita o modo dualstack para o balanceador de carga, o Elastic Load Balancing fornece um registro DNS AAAA para o balanceador de carga. Os clientes que se comunicam com o load balancer usando endereços IPv4 resolvem o registro DNS A. Os clientes que se comunicam com o load balancer usando endereços IPv6 resolvem o registro DNS AAAA.
- O acesso aos balanceadores de carga dualstack internos por meio do gateway da Internet é bloqueado para impedir o acesso não intencional à Internet. No entanto, isso não impede

outros acessos à Internet (por exemplo, por meio de peering, Transit Gateway ou AWS VPN).
AWS Direct Connect

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

Mapa de recursos do Network Load Balancer

O mapa de recursos do Network Load Balancer fornece uma exibição interativa da arquitetura do seu balanceador de carga, incluindo seus ouvintes, grupos-alvo 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 do seu balanceador de carga.

Para visualizar o mapa de recursos do seu Network Load Balancer usando o console

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. Escolha a guia Mapa de recursos para exibir o mapa de recursos do balanceador de carga.

Componentes do mapa de recursos

Visualizações do mapa

Há duas visualizações disponíveis no mapa de recursos do Network Load Balancer: Overview e Unhealthy Target Map. A opção Visão geral é selecionada por padrão e exibe todos os recursos do seu balanceador de carga. Selecionar a visualização Mapa de Alvos Insalubres exibirá somente os alvos não íntegros e os recursos associados a eles.

A visualização Mapa de alvos não íntegros pode ser usada para solucionar problemas de alvos que estão falhando nas verificações de integridade. Para ter mais informações, consulte Solucione problemas de alvos 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 ouvintes, grupos-alvo e alvos.

Blocos 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.
- Selecionar um bloco de recursos destaca as relações entre ele e outros recursos e exibe detalhes adicionais sobre esse recurso.
  - resumo de saúde do grupo-alvo: o número de alvos registrados para cada estado de saúde.
  - status de saúde do alvo: o status de saúde atual e a descrição do alvo.

> **Note**
>
> Você pode desativar Mostrar detalhes do recurso para ocultar detalhes adicionais no mapa do recurso.

- Cada bloco de recursos contém um link que, quando selecionado, navega até a página de detalhes desse recurso.
  - Ouvintes - Selecione o protocolo de ouvintes: porta. Por exemplo, `TCP:80`.
  - Grupos-alvo - Selecione o nome do grupo-alvo. Por exemplo, `my-target-group`.
  - Alvos - Selecione o ID dos alvos. Por exemplo, `i-1234567890abcdef0`.

Exportar o mapa de recursos

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

Zonas de disponibilidade

Você ativa uma ou mais Zonas de disponibilidade para o seu load balancer quando você o cria. Se você habilitar várias Zonas de disponibilidade para o load balancer, isso aumentará a tolerância a falhas de seus aplicativos. Não é possível desabilitar zonas de disponibilidade para um Network Load Balancer depois de criá-lo, mas é possível habilitar zonas de disponibilidade adicionais.

Quando você habilitar uma Zona de disponibilidade, você especificará uma sub-rede nessa Zona de disponibilidade. O Elastic Load Balancing cria um nó de balanceador de carga na zona de disponibilidade e uma interface de rede para a sub-rede (a descrição começa com “ELB net” e inclui

o nome do balanceador de carga). Cada nó de load balancer na zona de disponibilidade usa essa interface de rede para obter um endereço IPv4. Observe que você pode visualizar essa interface de rede, mas não pode modificá-la.

Ao criar um load balancer voltado para a Internet, se preferir, você poderá especificar um endereço IP elástico por sub-rede. Se você não escolher um dos seus próprios endereços IP elásticos, o Elastic Load Balancing fornecerá um endereço IP elástico por sub-rede para você. Esses endereços IP elásticos fornecem ao load balancer endereços IP estáticos que não serão alterados durante a vida útil do load balancer. Você não pode alterar esses endereços IP elásticos depois de criar o balanceador de carga.

Ao criar um load balancer interno, se preferir, você poderá especificar um endereço IP privado por sub-rede. Se você não especificar um endereço IP da sub-rede, o Elastic Load Balancing escolherá um para você. Esses endereços IP privados fornecem ao load balancer endereços IP estáticos que não serão alterados durante a vida útil do load balancer. Você não pode alterar esses endereços IP privados depois de criar o balanceador de carga.

Considerações

- Para load balancers voltados para a Internet, as sub-redes especificadas devem ter pelo menos 8 endereços IP disponíveis. Para balanceadores de carga internos, isso só é necessário se você permitir AWS selecionar um endereço IPv4 privado da sub-rede.
- Não é possível especificar uma sub-rede em uma zona de disponibilidade restrita. A mensagem de erro é "Load balancers com tipo 'rede' não são compatíveis com a az_name". É possível especificar uma sub-rede em outra zona de disponibilidade que não esteja restrita e usar o balanceamento de carga entre zonas para distribuir o tráfego para destinos na zona de disponibilidade restrita.
- Você pode especificar sub-redes que foram compartilhadas com você.
- Não é possível especificar uma sub-rede em uma Zona local.

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.

Para atualizar zonas de disponibilidade usando o console

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 Mapeamento de rede, escolha Editar sub-redes.
5. Para habilitar uma Zona de disponibilidade, marque a caixa de seleção dessa Zona de disponibilidade. Se houver uma sub-rede para essa Zona de disponibilidade, ela estará selecionada. Se houver mais de uma sub-rede para essa Zona de disponibilidade, selecione uma delas. Observe que você só pode selecionar uma sub-rede por Zona de disponibilidade.

   Para um load balancer voltado para a Internet, você pode selecionar um endereço IP elástico para cada zona de disponibilidade. Para um balanceador de carga interno, você pode atribuir um endereço IP privado do intervalo IPv4 de cada sub-rede, em vez de permitir que o Elastic Load Balancing atribua um.
6. Escolha Salvar alterações.

Para adicionar zonas de disponibilidade usando o AWS CLI

Use o comando set-sub-redes.

Balanceamento de carga entre zonas

Por padrão, cada nó do load balancer distribui tráfego aos destinos registrados somente na sua zona de disponibilidade. Se você ativer o balanceamento de carga entre zonas, cada nó do balanceador de carga 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.

Proteção contra exclusão

Para evitar que seu load balancer seja excluído acidentalmente, é possível ativar a proteção contra exclusão. Por padrão, a proteção contra exclusão está desativada para seu load balancer.

Se você ativar a proteção contra exclusão para o load balancer, deverá desativá-la antes de excluir o load balancer.

Para habilitar a proteção contra exclusão usando o console

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 Atributos, escolha Editar.
5. Em Configuração, ative a Proteção contra exclusão..
6. Escolha Salvar alterações.

Para desabilitar a proteção contra exclusão usando o console

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 Atributos, escolha Editar.
5. Em Configuração, ative a Proteção contra exclusão..
6. Escolha Salvar alterações.

Para ativar ou desativar a proteção contra exclusão usando o AWS CLI

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

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 é fechada. Se um cliente ou um destino envia dados depois do tempo limite de inatividade, ele recebe um pacote TCP RST para indicar que a conexão não é mais válida.

Definimos o valor do tempo limite de inatividade de fluxos TCP como 350 segundos. Não é possível modificar esse valor. Os clientes ou destinos podem usar pacotes de manutenção TCP para redefinir o tempo limite de inatividade. Pacotes Keepalive enviados para manter conexões TLS não podem conter dados ou carga.

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 front-end e back-end 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.

As instâncias do EC2 devem responder a uma nova solicitação dentro de 30 segundos para estabelecer um caminho de retorno.

Nome DNS

Cada Network Load Balancer recebe um nome padrão do Sistema de Nomes de Domínio (DNS) com a seguinte sintaxe: *name*-*id*.elb.*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 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 load balancer.

Primeiro, registre um nome de domínio com um registrador de nomes de domínio credenciado. Em seguida, use o serviço DNS, como o registrador de domínios, para criar um registro DNS para rotear solicitações para o balanceador de carga. 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 balanceador de carga. Para obter mais informações, consulte Rotear tráfego para um balanceador de carga ELB no Guia do desenvolvedor do Amazon Route 53.

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

Linux ou Mac

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

Windows

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

O load balancer tem registros DNS para seus nós de load balancer. É possível usar nomes DNS com a seguinte sintaxe para determinar os endereços IP dos nós do balanceador de carga: *az*.*name-id*.elb.*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
```

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 de balanceadores de carga. Isso leva à distribuição das conexões do cliente entre as zonas de disponibilidade dos balanceadores de carga. Com as políticas de roteamento de afinidade de zona de disponibilidade, as consultas ao DNS do cliente favorecem os endereços IP do balanceador de carga 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.

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 balanceador de carga na sua própria zona de disponibilidade. As consultas poderão ser resolvidas em outras zonas se não houver endereços IP íntegros de balanceadores de carga 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 balanceador de carga na sua própria zona de disponibilidade, enquanto as consultas restantes serão resolvidas em qualquer zona íntegra. As consultas podem ser resolvidas em outras zonas se não houver

endereços IP íntegros na própria zona. Quando não há IPs íntegros em qualquer 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 balanceador de carga em todas as zonas de disponibilidade do balanceador de carga.

> **Note**
>
> 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

A afinidade de zona de disponibilidade ajuda a rotear solicitações do cliente para o balanceador de carga, enquanto o balanceamento de carga entre zonas é usado para ajudar a rotear solicitações do balanceador de carga para os destinos. Ao usar a afinidade de zona de disponibilidade, o balanceamento de carga entre zonas deve ser desativado, isso garante que o tráfego do balanceador de carga dos clientes para os destinos permaneça na mesma 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 seu aplicativo 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 ter 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 balanceadores de carga 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.
- 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

É recomendável rastrear a distribuição das conexões entre as zonas de disponibilidade usando as métricas zonais do balanceador de carga. 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 mais informações, consulte CloudWatch métricas para seu Network Load Balancer.

Ativar a afinidade de zona de disponibilidade

As etapas deste procedimento explicam como ativar a afinidade de zona de disponibilidade usando o console do Amazon EC2.

Ativar a afinidade de zona de disponibilidade usando o console

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 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.

Para ativar a afinidade da Zona de Disponibilidade usando o AWS CLI

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

Desativar a afinidade de zona de disponibilidade

As etapas deste procedimento explicam como desativar a afinidade de zona de disponibilidade usando o console do Amazon EC2.

Desativar a afinidade de zona de disponibilidade usando o console

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 Atributos, escolha Editar.
5. Em Configuração de roteamento da zona de disponibilidade, Política de roteamento do cliente (registro DNS), selecione Qualquer zona de disponibilidade.
6. Escolha Salvar alterações.

Para desativar a afinidade da Zona de Disponibilidade usando o AWS CLI

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

Criar um Network Load Balancer

Um load balancer leva solicitações de clientes e as distribui em destinos em um grupo de destino, como instâncias EC2.

Antes de começar, certifique-se de que a nuvem privada virtual (VPC) do load balancer tenha pelo menos uma sub-rede pública em cada zona de disponibilidade onde você tem destinos. Você também deve configurar um grupo de destino e registrar pelo menos um destino para definir como padrão para rotear tráfego para o grupo de destino.

Para criar um balanceador de carga usando o AWS CLI, consulteTutorial: criar um Network Load Balancer usando a AWS CLI.

Para criar um balanceador de carga usando o AWS Management Console, conclua as tarefas a seguir.

Tarefas

- Etapa 1: configurar um grupo de destino
- Etapa 2: registrar destinos
- Etapa 3: configurar um balanceador de carga e um receptor
- Etapa 4: testar o balanceador de carga

Etapa 1: configurar um grupo de destino

A configuração de um grupo de destino permite que você registre destinos como instâncias do EC2. O grupo de destino que você configura nesta etapa é usado como o grupo de destino na regra do

receptor quando você configura o balanceador de carga. Para ter mais informações, consulte Grupos de destino para Network Load Balancers.

Para configurar seu grupo-alvo usando o console

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 destinos por ID de 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.
   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.
   d. (Opcional) Para Port (Porta), modifique o valor padrão conforme o necessário.
   e. Em Tipo de endereço IP, escolha IPv4 ou IPv6. Essa opção só estará disponível se o tipo de destino for Instâncias ou Endereços IP e o protocolo for TCP ou TLS.

      Você deve associar um grupo de destino IPv6 a um balanceador de carga dualstack. Todos os destinos no grupo de destino devem ter o mesmo tipo de endereço IP. Você não pode alterar o tipo de endereço IP de um grupo de destino depois de criá-lo.
   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 os códigos de sucesso da verificação de integridade. 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 ter mais informações, consulte Verificações de integridade para os grupos de destino.

6. (Opcional) Para adicionar uma tag, expanda Tags, escolha Adicionar tag e digite uma chave de tag e um valor de tag.
7. Selecione Next (Próximo).

Etapa 2: registrar destinos

Você pode registrar instâncias do EC2, endereços IP ou um Application Load Balancer com seu grupo de destino. Esta é uma etapa opcional para criar um balanceador de carga. No entanto, você deve registrar os destinos para garantir que o balanceador de carga possa direcionar tráfego para eles.

1. Na página Registrar destinos, adicione um ou mais destinos da seguinte forma:
   - Se o tipo de destino for Instâncias, selecione uma ou mais instâncias, insira as portas e escolha Incluir como pendente abaixo.
   - Se o tipo de destino for Endereços IP, selecione a rede, insira os endereços IP e as portas e escolha Incluir como pendente abaixo.
   - Se o tipo de destino for Application Load Balancer, selecione um Application Load Balancer.
2. Selecione Criar grupo de destino.

Etapa 3: configurar um balanceador de carga e um receptor

Para criar um Network Load Balancer, você deve primeiro fornecer informações básicas para o balanceador de carga, como nome, esquema e tipo de endereço IP. Em seguida, forneça informações sobre a rede e sobre um ou mais receptores. Um listener é um processo que verifica se há solicitações de conexão. Ele é configurado com um protocolo e uma porta para as conexões de clientes com o load balancer. Para obter mais informações sobre protocolos e portas suportados, consulte Configuração do receptor.

Para configurar seu balanceador de carga e ouvinte usando o console

1. Abra o console do Amazon EC2 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 Load balancer name (Nome do balanceador de carga), insira um nome para o seu balanceador de carga. Por exemplo, **`my-nlb`**. O nome do Network Load Balancer deve ser exclusivo no conjunto de Application Load Balancers e Network Load Balancers para a 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 balanceador de carga voltado para a Internet roteia solicitações de clientes até destinos na Internet. Um load balancer interno roteia solicitações a destinos usando endereços IP privados.

c. Em Tipo de endereço IP, escolha ipv4 se seus clientes usam endereços IPv4 para comunicação com o balanceador de carga ou Dualstack se seus clientes usam endereços IPv4 e IPv6 para comunicação com o balanceador de carga.

6. Mapeamento de rede

a. Em VPC, selecione a VPC usada para as instâncias do EC2.

Se você tiver selecionado Voltado para a Internet para Esquema, somente VPCs com um gateway da Internet estarão disponíveis para seleção.

b. Em Mapeamentos, selecione duas ou mais zonas de disponibilidade e as sub-redes correspondentes. Habilitar várias zonas de disponibilidade aumenta a tolerância a falhas das aplicações. Você pode especificar sub-redes que foram compartilhadas com você.

Para balanceadores de carga voltados 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. Como alternativa, para um balanceador de carga interno, você pode atribuir um endereço IP privado do intervalo IPv4 de cada sub-rede em vez de deixar AWS atribuir um para você.

7. Em Grupos de segurança, selecionamos previamente o grupo de segurança padrão para sua VPC. Você pode selecionar outros grupos de segurança, conforme necessário. Se você não tiver um grupo de segurança adequado, escolha Criar um novo grupo de segurança e crie um que atenda às suas necessidades de segurança. Para obter mais informações, consulte Criar um grupo de segurança no Guia do usuário da Amazon VPC.

> **Warning**
>
> Se você não associar grupos de segurança ao balanceador de carga agora, não poderá associá-los posteriormente.

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. Caso não tenha criado um grupo de destino anteriormente, você deve criar um agora. É possível, opcionalmente, escolher Adicionar receptor para adicionar um receptor (por exemplo, um receptor HTTPS).

   c. (Opcional) Adicione tags para categorizar o receptor.

   d. Em Configurações seguras de receptor (disponíveis somente para receptores TLS), faça o seguinte:

      i. Em Política de segurança, escolha uma política de segurança que atenda aos seus requisitos.

      ii. Em Política ALPN, escolha uma política para habilitar ALPN ou escolha Nenhum para desabilitar ALPN.

      iii. Em Certificado SSL padrão, escolha Do ACM (recomendado) e selecione um certificado. Se você não tiver um certificado disponível, poderá importar um certificado para o ACM ou usar o ACM para obter um. Para obter mais informações, consulte Emitir e gerenciar certificados no Guia do usuário do AWS Certificate Manager .

9. (Opcional) Você pode usar serviços complementares com seu balanceador de carga. Por exemplo, você pode optar por AWS Global Acceleratorcriar um acelerador para você e associar seu balanceador de carga ao acelerador. O nome do acelerador pode ter os seguintes caracteres (até 64 caracteres): a-z, A-Z, 0-9,. (período) e - (hífen). Depois que o acelerador for criado, acesse o AWS Global Acceleratorconsole para concluir a configuração. Para obter mais informações, consulte Adicionar um acelerador ao criar um balanceador de carga

10. Tags

    (Opcional) Adicione tags para caracterizar o balanceador de carga. 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 balanceador de carga durante a criação. Você pode visualizá-los e editá-los depois de criar o balanceador de carga. Para ter mais informações, consulte Atributos do load balancer.

Etapa 4: testar o balanceador de carga

Depois de criar o balanceador de carga, você pode verificar se as instâncias EC2 passaram na verificação de integridade inicial e testar se o balanceador de carga está enviando tráfego para as instâncias do EC2. Para excluir o balanceador de carga, consulte Excluir um Network Load Balancer.

Para testar o balanceador de carga

1. Após a criação do load balancer, selecione Close (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 pode testar seu load balancer. Para ter mais informações, consulte Status de integridade do destino.
5. No painel de navegação, selecione Load Balancers.
6. Selecione o novo balanceador de carga.
7. Copie o nome DNS do balanceador de carga (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.

Tipos de endereço IP para o Network Load Balancer

É possível configurar o Network Load Balancer para que os clientes possam se comunicar com o balanceador de carga usando apenas endereços IPv4 ou endereços IPv4 e IPv6 (dualstack). O balanceador de carga se comunica com os destinos com base no tipo de endereço IP do grupo de destino. Para ter mais informações, consulte Tipo de endereço IP.

Requisitos para dualstack

- É possível definir o tipo de endereço IP ao criar o load balancer e atualizá-lo a qualquer momento.
- A nuvem privada virtual (VPC) e as sub-redes especificadas para o load balancer devem ter blocos CIDR IPv6 associados. Para obter mais informações, consulte Endereços IPv6 no Guia do usuário do Amazon Ec2.
- O balanceador de carga deve ter somente receptores TCP e TLS.
- As tabelas de rota para as sub-redes do load balancer devem rotear o tráfego IPv6.
- As ACLs de rede para as sub-redes do load balancer devem permitir tráfego IPv6.

Como definir o tipo de endereço IP na criação

Defina as configurações conforme descrito em Criar um balanceador de carga.

Para atualizar o tipo de endereço IP usando o console

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 do balanceador de carga.
4. Selecione Ações, Editar tipo de endereço IP.
5. No Tipo de endereço IP, selecione IPv4 para compatibilidade exclusivamente com os endereços IPv4 ou Dualstack para compatibilidade com endereços IPv4 e IPv6.
6. Escolha Salvar alterações.

Para atualizar o tipo de endereço IP usando o AWS CLI

Use o comando set-ip-address-type.

Grupos de segurança para o Network Load Balancer

Você pode associar um grupo de segurança ao Network Load Balancer para controlar o tráfego que tem permissão para acessar e sair do balanceador de carga. 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 balanceador de carga, todo o tráfego do cliente poderá alcançar os receptores do balanceador de carga e todo o tráfego poderá sair do balanceador de carga.

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 balanceador de carga, 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 balanceador de carga, mesmo que você habilite a preservação do IP do cliente para o balanceador de carga.

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

Conteúdo

- Considerações
- Exemplo: filtro de tráfego de clientes
- Exemplo: aceitar tráfego somente do balanceador de carga
- Atualizar os grupos de segurança associados
- Atualizar as configurações de segurança
- Monitirar grupos de segurança do balanceador de carga

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 balanceador de carga posteriormente. Recomendamos que você associe um grupo de segurança ao balanceador de carga quando criá-lo.
- Caso crie um Network Load Balancer com grupos de segurança associados, você poderá mudar os grupos de segurança associados ao balanceador de carga 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 balanceador de carga 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. Se for um balanceador de carga interno, você poderá especificar um intervalo CIDR de VPC como origem para permitir somente tráfego de uma VPC específica. Se for um balanceador de carga 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	Origem	Intervalo de portas	Comentário
protocol	*intervalo de endereços IP do cliente*	*porta do receptor*	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 usuário do Amazon EC2.

Saída

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

Exemplo: aceitar tráfego somente do balanceador de carga

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 balanceador de carga na porta de destino e na porta de verificação de integridade. Para ter mais informações, consulte the section called “Grupos de segurança de destino”.

Entrada

Protocolo	Origem	Intervalo de portas	Comentário
protocol	sg-111112 222233333	*porta de destino*	Permite tráfego de entrada do balanceador de carga na porta de destino
protocol	sg-111112 222233333	*verificação de saúde*	Permite tráfego de entrada do balanceador de carga na porta de verificação de integridade

Saída

Protocolo	Destino	Intervalo de portas	Comentário
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 balanceador de carga ao criá-lo, poderá atualizar os grupos de segurança desse balanceador de carga a qualquer momento.

Para atualizar security groups usando o console

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 o load balancer.
4. Na guia Segurança, escolha Editar.
5. Para associar um security group ao seu load balancer, selecione-o. Para remover um security group do seu load balancer, desmarque-o.
6. Escolha Salvar alterações.

Para atualizar grupos de segurança usando o AWS CLI

Use o comando set-security-groups.

Atualizar as configurações de segurança

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

Atualizar as configurações de segurança usando o console

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 o 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.

Para atualizar as configurações de segurança usando o AWS CLI

Use o comando set-security-groups.

Monitirar grupos de segurança do balanceador de carga

Use as `SecurityGroupBlockedFlowCount_Outbound` CloudWatch métricas `SecurityGroupBlockedFlowCount_Inbound` e para monitorar a contagem de fluxos bloqueados pelos grupos de segurança do balanceador de carga. O tráfego bloqueado não é refletido em outras métricas. Para ter 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 balanceador de carga. Para obter mais informações, consulte Logs de fluxo da VPC no Guia do usuário da Amazon VPC.

Tags para o Network Load Balancer

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

Você pode adicionar várias tags para cada load balancer. Se você adicionar uma tag com uma chave que já esteja associada ao load balancer, o valor dessa tag será atualizado.

Quando você terminar com uma tag, poderá removê-la do seu 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 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.

Para atualizar as tags para um load balancer usando o console

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 Tags (Tags), selecione Manage tags (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 e Valor.
7. Para excluir uma etiqueta, escolha Remove (Remover) ao lado dela.
8. Ao terminar, selecione Salvar alterações.

Para atualizar as tags de um balanceador de carga usando o AWS CLI

Use os comandos add-tags e remove-tags.

Excluir um Network Load Balancer

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

Você não pode excluir um load balancer se a proteção contra exclusão estiver habilitada. Para ter mais informações, consulte Proteção contra exclusão.

Não é possível excluir um load balancer se ele estiver sendo usado por outro serviço. Por exemplo, se o load balancer estiver associado a um serviço de VPC endpoint, será necessário excluir a configuração do serviço de endpoint antes de excluir o load balancer associado.

A exclusão de um load balancer também exclui seus listeners. A exclusão de um load balancer não afeta seus destinos registrados. Por exemplo, as instâncias EC2 continuam a ser executadas e ainda estão registradas em seus grupos de destino. Para excluir seus grupos de destino, consulte Excluir um grupo de destino.

Para excluir um load balancer usando o console

1. Se você tiver um registro DNS para seu domínio que aponte para o balanceador de carga, aponte-o para um novo local e aguarde até que a mudança de DNS entre em vigor antes de excluir o balanceador de carga.

   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 console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, selecione Load Balancers.
4. Marque a caixa de seleção do balanceador de carga.

5. Escolha Ações, Excluir balanceador de carga.
6. Quando a confirmação for solicitada, insira **`confirm`** e escolha Excluir.

Para excluir um balanceador de carga usando o AWS CLI

Use o comando delete-load-balancer.

Mudança de zona

A mudança de zona é um recurso do Controlador de Recuperação de Aplicações do Amazon Route 53 (Route 53 ARC). Com a mudança de zona, você pode retirar um recurso do balanceador de carga 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 balanceador de carga para de enviar o tráfego do recurso para a zona de disponibilidade afetada. O Route 53 ARC cria a mudança de zona imediatamente. No entanto, a efetivação das conexões existentes e em andamento na zona de disponibilidade afetada pode levar algum tempo, normalmente alguns minutos. Para obter mais informações, consulte Funcionamento da mudança de zona: verificações de integridade e endereços IP de zona no Guia do desenvolvedor do Controlador de Recuperação de Aplicações do Amazon Route 53.

As mudanças de zona só são compatíveis com Application Load Balancers e Network Load Balancers com o balanceamento de carga entre zonas desativado. Caso ative o balanceamento de carga entre zonas, você não poderá iniciar uma mudança de zona. Para obter mais informações, consulte Recursos compatíveis com mudanças de zona no Guia do desenvolvedor do Controlador de Recuperação de Aplicações do Amazon Route 53.

Antes de usar uma mudança de zona, analise o seguinte:

- O balanceamento de carga entre zonas não é compatível com mudanças de zona. Você deve desativar o balanceamento de carga entre zonas para usar esse recurso.
- A mudança de zona não é compatível quando você usa um Application Load Balancer como um endpoint do acelerador no AWS Global Accelerator.
- Você pode iniciar uma mudança de zona para um balanceador de carga 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 do balanceador de carga zonal 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 os balanceadores de carga estiverem com o balanceamento de carga entre zonas desativado e você usar uma mudança de zona para remover o endereço IP de um balanceador de carga de zona, a zona de disponibilidade afetada pela mudança de zona também perderá a capacidade de destino.
- Quando um Application Load Balancer for o destino de um Network Load Balancer, sempre inicie a mudança de zona pelo Network Load Balancer. Se você iniciar uma mudança de zona pelo Application Load Balancer, o Network Load Balancer não reconhecerá a mudança e continuará a enviar tráfego para o Application Load Balancer.

Para obter mais orientações e informações, consulte Práticas recomendadas para mudanças de zona com o Route 53 ARC no Guia do desenvolvedor do Controlador de Recuperação de Aplicações do Amazon Route 53.

Iniciar uma mudança de zona

As etapas deste procedimento explicam como ativar uma mudança de zona usando o console do Amazon EC2. Para ver as etapas para iniciar uma mudança de zona usando o console do Route 53 ARC, consulte Como iniciar uma mudança de zona no Guia do desenvolvedor do Controlador de Recuperação de Aplicações do Amazon Route 53.

Para iniciar uma mudança de zona usando o console

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 o nome do balanceador de carga.
4. Na guia Integrações, em Controlador de Recuperação de Aplicações do Amazon Route 53, 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, se quiser.
8. Marque a caixa de seleção para confirmar que iniciar uma mudança de zona reduzirá a capacidade da sua aplicação ao afastar o tráfego da zona de disponibilidade.
9. Escolha Iniciar.

Para iniciar uma mudança zonal usando o AWS CLI

Para trabalhar com mudanças de zona de maneira programática, consulte o Guia de referência da API de mudança de zona.

Atualizar uma mudança de zona

As etapas deste procedimento explicam como atualizar uma mudança de zona usando o console do Amazon EC2. Para ver as etapas para atualizar uma mudança de zona usando o console do Controlador de Recuperação de Aplicações do Amazon Route 53, consulte Atualizar uma mudança de zona no Guia do desenvolvedor do Controlador de Recuperação de Aplicações do Amazon Route 53.

Atualizar uma mudança de zona usando o console

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 o nome de um balanceador de carga que tenha uma mudança de zona ativa.
4. Na guia Integrações, em Controlador de Recuperação de Aplicações do Amazon Route 53, escolha Atualizar mudança de zona.

   Essa ação abrirá o console do Route 53 ARC para continuar a atualização.
5. Em Definir validade da mudança de zona, selecione ou insira uma validade de maneira opcional.
6. Em Comentário, opcionalmente, edite o comentário existente ou insira um novo.
7. Selecione Atualizar.

Para atualizar um deslocamento zonal usando o AWS CLI

Para trabalhar com mudanças de zona de maneira programática, consulte o Guia de referência da API de mudança de zona.

Cancelar uma mudança de zona

As etapas deste procedimento explicam como cancelar uma mudança de zona usando o console do Amazon EC2. Para ver as etapas para cancelar uma mudança de zona usando o console do Controlador de Recuperação de Aplicações do Amazon Route 53, consulte Como cancelar uma mudança de zona no Guia do desenvolvedor do Controlador de Recuperação de Aplicações do Amazon Route 53.

Para cancelar uma mudança de zona usando o console

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 o nome de um balanceador de carga que tenha uma mudança de zona ativa.
4. Na guia Integrações, em Controlador de Recuperação de Aplicações do Amazon Route 53, escolha Cancelar mudança de zona.

   Essa ação abre o console do Route 53 ARC para continuar o cancelamento.
5. Escolha Cancelar mudança de zona.
6. Na caixa de diálogo de confirmação, escolha Confirmar.

Para cancelar uma mudança de zona usando o AWS CLI

Para trabalhar com mudanças de zona de maneira programática, consulte o Guia de referência da API de mudança de zona.

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
- Regras do listener
- Criar um receptor para o Network Load Balancer
- Listeners TLS para o Network Load Balancer
- Atualizar um receptor para o Network Load Balancer
- Atualizar um receptor TLS para o Network Load Balancer
- Excluir um receptor para o Network Load Balancer

Configuração do receptor

Os listeners são compatíveis com os seguintes protocolos e portas:

- Protocols (Protocolos): TCP, TLS, UDP, TCP_UDP
- 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 de listener for TLS, você deverá implantar exatamente um certificado de servidor SSL no listener. Para ter mais informações, consulte Listeners TLS para o Network Load Balancer.

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.

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 Network Load Balancers dualstack, somente os protocolos TCP e TLS são compatíveis.

Você pode usar WebSockets com seus ouvintes.

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.

Regras do listener

Quando você cria um listener, você especifica uma regra para rotear as solicitações. Essa regra encaminha as solicitações para o grupo de destino especificado. Para atualizar essa regra, consulte Atualizar um receptor para o Network Load Balancer.

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 regra do listener. Para ter 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 ter mais informações, consulte Certificados de servidor.

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 ter mais informações, consulte Configuração do receptor.

Para adicionar um listener usando o console

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 ou TLS. Mantenha a porta padrão ou digite uma porta diferente. Para Network Load Balancers dualstack, somente os protocolos TCP e TLS são compatíveis.
6. Em Ação padrão, escolha um grupo de destino disponível.
7. [Listeners TLS] Em Security policy (Política de segurança), é recomendável manter a política de segurança padrão.
8. [Listeners TLS] Em Default SSL certificate (Certificado SSL padrão), siga um destes procedimentos:
   - Se você criou ou importou um certificado usando AWS Certificate Manager, escolha Do ACM e escolha o certificado.
   - Se você tiver carregado um certificado usando o IAM, escolha Do IAM e, em seguida, o certificado.
9. [Listeners TLS] Em Política ALPN, escolha uma política para habilitar ALPN ou escolha Nenhum para desabilitar ALPN. Para ter mais informações, consulte Políticas ALPN.
10. Escolha Adicionar.
11. [Listeners TLS] Para adicionar uma lista de certificados opcional para uso com o protocolo SNI, consulte Adicionar certificados à lista de certificados.

Para adicionar um ouvinte usando o AWS CLI

Use o comando create-listener para criar o listener.

Listeners TLS para o Network Load Balancer

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 front-end 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 passados entre o cliente e o load balancer sejam privados. A cifra é um algoritmo de criptografia que usa chaves de criptografia para criar uma mensagem codificada. Os protocolos usam várias cifras para criptografar dados pela 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 renegociação ou 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.

Para criar um listener TLS, consulte Adicionar um listener. Para demonstrações relacionadas, consulte Suporte TLS no Network Load Balancer e Suporte SNI no Network Load Balancer.

Certificados de servidor

O load balancer requer certificados X.509 (certificado de 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 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.

Conteúdo

- Algoritmos principais suportados
- Certificado padrão
- Lista de certificados
- Renovação de certificado

Algoritmos principais suportados

- RSA de 1024 bits
- RSA de 2048 bits

- RSA 3072 bits
- ECDSA de 256 bits
- ECDSA de 384 bits
- ECDSA de 521 bits

Certificado padrão

Quando você cria um listener TLS, é necessário especificar exatamente um certificado. Esse certificado é conhecido como o certificado padrão. É possível substituir o certificado padrão depois de criar o listener TLS. Para ter 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 ter 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 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 ter 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

Ao criar um listener TLS, é necessário selecionar uma política de segurança. É possível atualizar a política de segurança conforme necessário. Para ter mais informações, consulte Atualizar a política de segurança.

Considerações:

- A `ELBSecurityPolicy-TLS13-1-2-2021-06` política é a política de segurança padrão para ouvintes TLS criados usando o. AWS Management Console
  - Recomendamos a política `ELBSecurityPolicy-TLS13-1-2-2021-06` de segurança, que inclui o TLS 1.3 e é compatível com versões anteriores do TLS 1.2.

- A `ELBSecurityPolicy-2016-08` política é a política de segurança padrão para ouvintes TLS criados usando o. AWS CLI
- Você pode escolher a política de segurança usada para conexões front-end, mas não para conexões back-end.
  - Para conexões de back-end, se seu receptor TLS estiver usando uma política de segurança TLS 1.3, a política de segurança `ELBSecurityPolicy-TLS13-1-0-2021-06` será usada. Caso contrário, a política de segurança `ELBSecurityPolicy-2016-08` será usada para as conexões de back-end.
- Para atender aos padrões de conformidade e segurança que exigem a desativação de determinadas versões do protocolo TLS ou para oferecer suporte a clientes antigos que exigem cifras obsoletas, você pode usar uma das políticas de segurança. `ELBSecurityPolicy-TLS-` Você pode ativar os registros de acesso para obter informações sobre as solicitações de TLS enviadas ao seu Network Load Balancer, analisar padrões de tráfego de TLS, 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 registro de acesso. Para obter mais informações, consulte Logs de acesso e Consultas de exemplo do Network Load Balancer.
- 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 serviços (SCPs), respectivamente. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia do AWS Organizations usuário

Políticas de segurança do TLS 1.3

O Elastic Load Balancing fornece as seguintes políticas de segurança TLS 1.3 para balanceadores de carga de rede:

- `ELBSecurityPolicy-TLS13-1-2-2021-06`(Recomendado)
- `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06`
- `ELBSecurityPolicy-TLS13-1-1-2021-06`
- `ELBSecurityPolicy-TLS13-1-0-2021-06`
- `ELBSecurityPolicy-TLS13-1-3-2021-06`

Políticas de segurança FIPS

O Federal Information Processing Standard (FIPS) é um padrão do governo dos EUA e do Canadá que especifica os requisitos de segurança para módulos criptográficos que protegem informações confidenciais. Para saber mais, consulte Federal Information Processing Standard (FIPS) 140 na página de conformidade de segurança na AWS nuvem.

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

O Elastic Load Balancing fornece as seguintes políticas de segurança FIPS para o Network Load Balancer:

- `ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`(Recomendado)
- `ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`

Políticas compatíveis com FS

O Elastic Load Balancing fornece as seguintes políticas de segurança suportadas por FS (Forward Secrecy) para balanceadores de carga de rede:

- `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`

Políticas de segurança TLS 1.0 - 1.2

O Elastic Load Balancing fornece as seguintes políticas de segurança TLS 1.0 a 1.2 para balanceadores de carga de rede:

- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-2016-08`
- `ELBSecurityPolicy-TLS-1-0-2015-04`
- `ELBSecurityPolicy-2015-05`(idêntico a **`ELBSecurityPolicy-2016-08`**)

Protocolos e cifras TLS

TLS 1.3

A tabela a seguir descreve os protocolos e cifras TLS compatíveis com as políticas de segurança TLS 1.3 disponíveis.

Nota: O `ELBSecurityPolicy-` prefixo foi removido dos nomes das políticas na linha de políticas de segurança.

Exemplo: A política de segurança `ELBSecurityPolicy-TLS13-1-2-2021-06` é exibida como`TLS13-1-2-2021-06`.

Políticas de segurança	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protocolos TLS							
Protocol-TLSv1							✓

Políticas de segurança	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protocol-TLSv1.1						✓	✓
Protocol-TLSv1.2	✓		✓	✓	✓	✓	✓
Protocolo - TLS V1.3	✓	✓	✓	✓	✓	✓	✓
Cifras TLS							
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓

Políticas de segurança	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
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	✓		✓	✓	✓	✓	✓

Políticas de segurança	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-RSA-AES256-GCM-SHA384	✓		✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓
AES128-GCM-SHA256				✓	✓	✓	✓

Políticas de segurança	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
AES128-SHA256				✓	✓	✓	✓
AES128-SHA				✓		✓	✓
AES256-GCM-SHA384				✓	✓	✓	✓
AES256-SHA256				✓	✓	✓	✓
AES256-SHA				✓		✓	✓

Para criar um ouvinte TLS que usa uma política TLS 1.3 usando a CLI

Use o comando create-listener com qualquer política de segurança do TLS 1.3.

O exemplo usa a política `ELBSecurityPolicy-TLS13-1-2-2021-06` de segurança.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Para modificar um ouvinte TLS para usar uma política TLS 1.3 usando a CLI

Use o comando modify-listener com qualquer política de segurança do TLS 1.3.

O exemplo usa a política `ELBSecurityPolicy-TLS13-1-2-2021-06` de segurança.

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

```
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Para visualizar as políticas de segurança usadas por um ouvinte usando a CLI

Use o comando describe-listener com o do `arn` seu ouvinte.

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para visualizar a configuração de uma política de segurança TLS 1.3 usando a CLI

Use o describe-ssl-policiescomando com qualquer política de segurança do TLS 1.3.

O exemplo usa a política `ELBSecurityPolicy-TLS13-1-2-2021-06` de segurança.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-2021-06
```

FIPS

> **Important**
>
> As `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` políticas `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` são fornecidas somente para compatibilidade com versões anteriores. Embora utilizem criptografia FIPS usando o módulo FIPS140, podem não estar em conformidade com as diretrizes mais recentes do NIST para configuração de TLS.

A tabela a seguir descreve os protocolos e cifras TLS compatíveis com as políticas de segurança FIPS disponíveis.

Nota: O `ELBSecurityPolicy-` prefixo foi removido dos nomes das políticas na linha de políticas de segurança.

Exemplo: A política de segurança `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` é exibida como`TLS13-1-2-FIPS-2023-04`.

Políticas de segurança	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
Protocolos TLS								
Protocol-TLSv1								✓
Protocol-TLSv1.1							✓	✓
Protocol-TLSv1.2		✓	✓	✓	✓	✓	✓	✓
Protocolo - TLS V1.3	✓	✓	✓	✓	✓	✓	✓	✓
Cifras TLS								
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-		✓	✓	✓	✓	✓	✓	✓

Políticas de segurança	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
SHA256								
ECDHE-RSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓	✓

Políticas de segurança	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES128-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384			✓	✓	✓	✓	✓	✓

Políticas de segurança	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES256-SHA384			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓	✓
AES128-GCM-SHA256					✓	✓	✓	✓
AES128-SHA256					✓	✓	✓	✓
AES128-SHA						✓	✓	✓

Políticas de segurança	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
AES256-GCM-SHA384					✓	✓	✓	✓
AES256-SHA256					✓	✓	✓	✓
AES256-SHA						✓	✓	✓

Para criar um ouvinte TLS que usa uma política FIPS usando a CLI

Use o comando create-listener com qualquer política de segurança FIPS.

O exemplo usa a política `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` de segurança.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Para modificar um ouvinte TLS para usar uma política FIPS usando a CLI

Use o comando modify-listener com qualquer política de segurança FIPS.

O exemplo usa a política `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` de segurança.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Para visualizar as políticas de segurança usadas por um ouvinte usando a CLI

Use o comando describe-listener com o do `arn` seu ouvinte.

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para visualizar a configuração de uma política de segurança FIPS usando a CLI

Use o describe-ssl-policiescomando com qualquer política de segurança FIPS.

O exemplo usa a política `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` de segurança.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

FS

A tabela a seguir descreve os protocolos e cifras TLS suportados para as políticas de segurança disponíveis suportadas pelo FS.

Nota: O `ELBSecurityPolicy-` prefixo foi removido dos nomes das políticas na linha de políticas de segurança.

Exemplo: A política de segurança `ELBSecurityPolicy-FS-2018-06` é exibida como`FS-2018-06`.

Políticas de segurança	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocolos TLS						
Protocol-TLSv1	✓					✓

Políticas de segurança	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocol-TLSv1.1	✓				✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
Cifras TLS						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓		✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓		✓	✓	✓	✓

Políticas de segurança	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-ECDSA-AES128-SHA	✓			✓	✓	✓
ECDHE-RSA-AES128-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓		✓	✓	✓	✓

Políticas de segurança	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-RSA-AES256-SHA384	✓		✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓			✓	✓	✓
AES128-GCM-SHA256	✓					
AES128-SHA256	✓					
AES128-SHA	✓					
AES256-GCM-SHA384	✓					

Políticas de segurança	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
AES256-SHA256	✓					
AES256-SHA	✓					

Para criar um ouvinte TLS que usa uma política compatível com FS usando a CLI

Use o comando create-listener com qualquer política de segurança compatível com FS.

O exemplo usa a política `ELBSecurityPolicy-FS-2018-06` de segurança.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Para modificar um ouvinte TLS para usar uma política compatível com FS usando a CLI

Use o comando modify-listener com qualquer política de segurança compatível com FS.

O exemplo usa a política `ELBSecurityPolicy-FS-2018-06` de segurança.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Para visualizar as políticas de segurança usadas por um ouvinte usando a CLI

Use o comando describe-listener com o do `arn` seu ouvinte.

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para visualizar a configuração de uma política de segurança compatível com FS usando a CLI

Use o describe-ssl-policiescomando com qualquer política de segurança compatível com FS.

O exemplo usa a política `ELBSecurityPolicy-FS-2018-06` de segurança.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-FS-2018-06
```

TLS 1.0 - 1.2

A tabela a seguir descreve os protocolos e cifras TLS compatíveis com as políticas de segurança TLS 1.0-1.2 disponíveis.

Nota: O `ELBSecurityPolicy-` prefixo foi removido dos nomes das políticas na linha de políticas de segurança.

Exemplo: A política de segurança `ELBSecurityPolicy-TLS-1-2-Ext-2018-06` é exibida como`TLS-1-2-Ext-2018-06`.

Políticas de segurança	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocolos TLS					
Protocol-TLSv1	✓				✓
Protocol-TLSv1.1	✓			✓	✓

Políticas de segurança	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocol-TLSv1.2	✓	✓	✓	✓	✓
Cifras TLS					
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	✓	✓		✓	✓

Políticas de segurança	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
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	✓	✓	✓	✓	✓

Políticas de segurança	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
AES128-SHA	✓	✓		✓	✓
AES256-GCM-SHA384	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓
DES-CBC3-SHA					✓

* Não use essa política a menos que você precise oferecer suporte a um cliente legado que exija a cifra DES-CBC3-SHA, que é uma cifra fraca.

Para criar um ouvinte TLS que usa uma política TLS 1.0-1.2 usando a CLI

Use o comando create-listener com qualquer política de segurança compatível com TLS 1.0-1.2.

O exemplo usa a política `ELBSecurityPolicy-2016-08` de segurança.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Para modificar um ouvinte TLS para usar uma política TLS 1.0-1.2 usando a CLI

Use o comando modify-listener com qualquer política de segurança compatível com TLS 1.0-1.2.

O exemplo usa a política `ELBSecurityPolicy-2016-08` de segurança.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Para visualizar as políticas de segurança usadas por um ouvinte usando a CLI

Use o comando describe-listener com o do `arn` seu ouvinte.

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para visualizar a configuração de uma política de segurança TLS 1.0-1.2 usando a CLI

Use o describe-ssl-policiescomando com qualquer política de segurança compatível com TLS 1.0-1.2.

O exemplo usa a política `ELBSecurityPolicy-2016-08` de segurança.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-2016-08
```

Políticas ALPN

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

Quando o cliente inicia uma conexão ALPN, o 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:

`HTTP10nly`

Negocie somente HTTP/1.*. A lista de preferências de ALPN é http/1.1, http/1.0.

`HTTP20nly`

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

`HTTP20ptional`

Prefira HTTP/1.* em vez de HTTP/2 (que pode ser útil para testes HTTP/2). A lista de preferências de ALPN é http/1.1, http/1.0, h2.

`HTTP2Preferred`

Prefira HTTP/2 em vez de HTTP/1.*. A lista de preferências de ALPN é h2, http/1.1, http/1.0.

`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.

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

Quando o grupo de destino da ação padrão do receptor 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.

Para atualizar o listener usando o console

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 Receptores, escolha o texto na coluna Protocolo:Porta para abrir a página de detalhes do receptor.
5. Selecione a opção Editar.
6. (Opcional) Altere os valores especificados de Protocolo e Porta conforme necessário.
7. (Opcional) Escolha um grupo de destino diferente para a Ação padrão.
8. (Opcional) Adicione, atualize ou remova tags conforme necessário.
9. Escolha Salvar alterações.

Para atualizar seu ouvinte usando o AWS CLI

Use o comando modify-listener.

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

É possível substituir o certificado padrão do listener TLS usando o procedimento a seguir. Para ter mais informações, consulte Certificado padrão.

Como substituir o certificado padrão usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione Balanceador de carga.
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Receptores, escolha o texto na coluna Protocolo:Porta para abrir a página de detalhes do receptor.
5. Em Default SSL certificate (Certificado SSL padrão), execute uma das seguintes ações:
   - Se você criou ou importou um certificado usando AWS Certificate Manager, escolha Do ACM e escolha o certificado.
   - Se você tiver carregado um certificado usando o IAM, escolha Do IAM e, em seguida, o certificado.
6. Escolha Salvar alterações.

Para substituir o certificado padrão usando o AWS CLI

Use o comando modify-listener com a opção --certificates.

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 um ou mais certificados. Você pode adicionar o certificado padrão para garantir que esse certificado seja usado com o protocolo SNI, mesmo que seja substituído como o certificado padrão. Para ter mais informações, consulte Lista de certificados.

Para adicionar certificados à lista de certificados usando o console

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 Receptores, escolha o texto na coluna Protocolo:Porta para abrir a página de detalhes do receptor.
5. Marque a caixa de seleção do receptor e escolha Ações, Adicionar certificados SSL para SNI.

6. 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.
7. Se você tiver um certificado que não seja gerenciado pelo ACM ou pelo IAM, escolha Importar certificado, preencha o formulário e escolha Importar.
8. Escolha Adicionar certificados pendentes.

Para adicionar um certificado à lista de certificados usando o AWS CLI

Use o comando add-listener-certificates.

Remover certificados da lista de certificados

É possível remover certificados da lista de certificados de um listener TLS usando o procedimento a seguir. Para remover o certificado padrão de um listener TLS, consulte Substituir o certificado padrão.

Para remover certificados da lista de certificados usando o console

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 Receptores, escolha o texto na coluna Protocolo:Porta para abrir a página de detalhes do receptor.
5. Marque a caixa de seleção do receptor e escolha Ações, Adicionar certificados SSL para SNI.
6. Marque as caixa de seleção para os certificados e escolha Remove (Remover).
7. Quando a confirmação for solicitada, insira **`confirm`** e escolha Remover.

Para remover um certificado da lista de certificados usando o AWS CLI

Use o comando remove-listener-certificates.

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 ter mais informações, consulte Políticas de segurança.

Para atualizar a política de segurança usando o console

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 Receptores, escolha o texto na coluna Protocolo:Porta para abrir a página de detalhes do receptor.
5. Selecione a opção Editar.
6. Em Security policy (Política de segurança), escolha uma política de segurança.
7. Escolha Salvar alterações.

Para atualizar a política de segurança usando o AWS CLI

Use o comando modify-listener com a opção --ssl-policy.

Atualizar a política ALPN

É possível atualizar a política ALPN para seu listener TLS usando o procedimento a seguir. Para ter mais informações, consulte Políticas ALPN.

Como atualizar a política ALPN usando o console

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 Receptores, escolha o texto na coluna Protocolo:Porta para abrir a página de detalhes do receptor.
5. Selecione a opção Editar.
6. Em Política ALPN, escolha uma política para habilitar ALPN ou escolha Nenhum para desabilitar ALPN.
7. Escolha Salvar alterações.

Para atualizar a política do ALPN usando o AWS CLI

Use o comando modify-listener com a opção --alpn-policy.

Excluir um receptor para o Network Load Balancer

Você pode excluir um listener a qualquer momento.

Para excluir um listener usando o console

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.

Para excluir um ouvinte usando o AWS CLI

Use o comando delete-listener.

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 ter 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 ter mais informações, consulte Verificações de integridade para os grupos de destino.

Conteúdo

- Configuração de roteamento
- Target type
- Tipo de endereço IP
- Destinos registrados
- Atributos do grupo de destino
- Preservação do IP do cliente
- Atraso do cancelamento do registro
- Protocolo de proxy
- Sessões persistentes
- Criar um grupo de destino para o Network Load Balancer
- Verificações de integridade para os grupos de destino
- Balanceamento de carga entre zonas para grupos de destino
- Integridade do grupo de destino
- Registrar destinos com o grupo de destino
- Application Load Balancers como destinos

- Tags para o grupo de destino
- Excluir um grupo de destino

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:

- Protocols (Protocolos): TCP, TLS, UDP, TCP_UDP
- 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, ele 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	Health check protocol (Protocolo da verificação de integridade)
TCP	TCP | TCP_UDP	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

Protocolo do listener	Protocolo do grupo de destino	Tipo de grupo de destino	Health check protocol (Protocolo da verificação de integridade)
TCP_UDP	TCP_UDP	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 para o 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 AWS Direct Connect de uma conexão VPN Site-to-Site.

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 Amazon 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 ter mais informações, consulte Application Load Balancers como destinos.

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 ter 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.

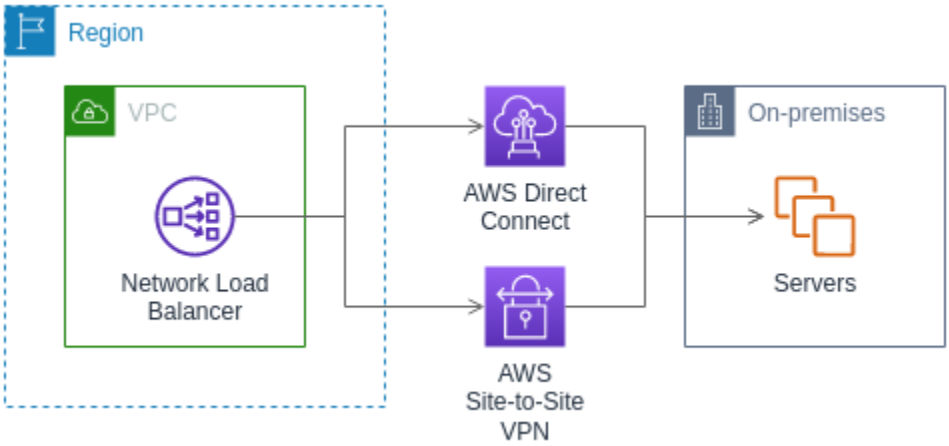
Se você especificar destinos usando endereços IP, você pode rotear o tráfego para uma instância com qualquer endereço IP privado de uma ou mais interfaces de rede. Isso permite que vários

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 AWS Direct Connect de uma conexão VPN Site-to-Site podem servir como destino, 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 AWS Direct Connect, consulte O que é AWS 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.

Network Load Balancers são compatíveis com grupos de destino IPv4 e IPv6. A seleção padrão é IPv4. Os grupos de destino IPv6 só podem ser associados a Network Load Balancers dualstack.

Considerações

- Todos os endereços IP de um grupo de destino devem ter o mesmo tipo de endereço IP. Por exemplo, você não pode registrar um destino IPv4 com um grupo de destino IPv6.
- Os grupos de destino IPv6 só podem ser usados com balanceadores de carga `dualstack` com receptores TCP ou TLS.
- Os grupos de destino IPv6 oferecem suporte a destinos de tipo de IP e de instância.

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 começa a rotear o tráfego para um destino recém-registrado assim que o processo de registro é concluído e o destino passa pela primeira verificação de integridade inicial, 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 for usado um dos seguintes tipos de instância: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1.
- Ao registrar destinos por ID de instância para um grupo de destino IPv6, os destinos devem ter um endereço IPv6 primário atribuído. Para saber mais, consulte endereços IPv6 no Guia do usuário do Amazon EC2
- Ao registrar destinos por ID de instância, as instâncias devem estar na mesma Amazon 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 e TCP_UDP, 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, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1. 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

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.

`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`.

`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 IP do cliente não pode ser desabilitada para grupos de destino UDP e TCP_UDP.

`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.

`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 `off`, a falha de DNS inativo estará desabilitada, o que significa que cada grupo de destino contribuirá de modo independente para o failover de 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 `off`, a falha de DNS é desabilitada, o que significa que cada grupo de destino contribui de forma independente para o failover de DNS. O padrão é um.

`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. O intervalo é 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 esperar antes de alterar o estado de um alvo não íntegro de para. `unhealthy.draining` `unhealthy` O intervalo é de 0 a 360000 segundos. O valor de padrão é 0 segundos.

Nota: Esse atributo só pode ser configurado quando `target_health_state.unhealthy.connection_termination.enabled` é`false`.

Preservação do IP do cliente

Os Network Load Balancers podem preservar o endereço IP de origem dos clientes ao rotear solicitações para destinos de back-end. Quando você desabilita a preservação do IP do cliente, o endereço IP privado do Network Load Balancer torna-se o endereço IP do cliente para todo o tráfego de entrada.

Por padrão, a preservação do IP do cliente é habilitada (e não pode ser desabilitada) para grupos de destino de tipo de instância e de IP com os protocolos UDP e TCP_UDP. 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): habilitados
- Grupos de destino do tipo IP (TCP, TLS): desabilitados

Requisitos e considerações

- Quando a preservação do IP do cliente está habilitada, os destinos devem estar na mesma VPC que o Network Load Balancer e o tráfego deve fluir diretamente do Network Load Balancer para o destino.
- Não há suporte para a preservação de IP quando é usado um endpoint do Gateway Load Balancer para inspecionar o tráfego entre o Network Load Balancer e o destino (instância ou IP), mesmo que o destino esteja na mesma Amazon VPC que o Network Load Balancer.
- Os seguintes tipos de instância não oferecem suporte à preservação do IP do cliente: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, 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 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 ENIs do AWS PrivateLink ou a ENI de outro Network Load Balancer. Isso causará perda de comunicação com esses destinos.
- A preservação do IP do cliente não afeta o tráfego convertido de IPv6 para IPv4. O 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.
- As alterações da preservação do IP do cliente só entram em vigor para novas conexões TCP.

- O loopback NAT, também conhecido como hairpinning, não é compatível quando a preservação do IP do cliente está habilitada. Quando habilitada, você pode encontrar limitações de conexão TCP/IP relacionadas à reutilização observada de soquetes nos destinos. Essas limitações de conexão podem ocorrer quando um cliente ou um dispositivo NAT na frente do cliente usa o mesmo endereço IP de origem e porta de origem ao se conectar a vários nós do balanceador de carga simultaneamente. Se o balanceador de carga rotear essas conexões para o mesmo destino, as conexões aparecerão no destino como se viessem do mesmo soquete de origem, o que resultará em erros de conexão. Se isso acontecer, os clientes poderão tentar novamente (se a conexão falhar) ou se reconectar (se a conexão for interrompida). Você pode reduzir esse tipo de erro de conexão aumentando o número de portas temporárias de origem ou aumentando o número de destinos para o balanceador de carga. Você pode evitar esse tipo de erro de conexão desabilitando a preservação do IP do cliente ou desabilitando o balanceamento de carga entre zonas.
- 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. Os erros na alocação de portas podem ser rastreados por meio da métrica `PortAllocationErrorCount`. Para corrigir erros na alocação de portas, adicione mais destinos ao grupo de destino. Para ter mais informações, consulte CloudWatch métricas para seu Network Load Balancer.

Para configurar a preservação do IP do cliente usando o console

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 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.

Para ativar ou desativar a preservação do IP do cliente usando o AWS CLI

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

Por exemplo, use o comando a seguir para desabilitar a preservação do IP do cliente.

```
aws elbv2 modify-target-group-attributes --attributes
 Key=preserve_client_ip.enabled,Value=false --target-group-arn ARN
```

Sua saída deve ser similar ao exemplo a seguir.

```
{
    "Attributes": [
      {
        "Key": "proxy_protocol_v2.enabled",
        "Value": "false"
      },
      {
        "Key": "preserve_client_ip.enabled",
        "Value": "false"
      },
      {
        "Key": "deregistration_delay.timeout_seconds",
        "Value": "300"
      }
    ]
}
```

Atraso do cancelamento do registro

Quando você cancela o registro de um destino, o balanceador de carga interrompe a criação de novas conexões com 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 que terá o registro cancelado é `draining`. 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.

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.

Para atualizar os atributos de cancelamento de registro usando o console

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.

Para atualizar os atributos de cancelamento de registro usando o AWS CLI

Use o comando modify-target-group-attributes.

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 do seu Network Load Balancer.

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: os endereços IP de origem são os endereços IP privados dos nós do balanceador de carga. Se você precisa dos endereços IP dos clientes, habilite o Proxy Protocol e obtenha os endereços IP dos clientes no cabeçalho do Proxy Protocol.
- UDP e TCP_UDP: os endereços IP de origem são os endereços IP dos clientes.

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.

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

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.

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 TLV (Type-Length-Value) personalizado, conforme mostrado a seguir.

Campo	Comprimento (em octetos)	Descrição
Tipo	1	PP2_TYPE_AWS (0xEA)

Campo	Comprimento (em octetos)	Descrição
Length	2	O comprimento do valor
Valor	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	variável (comprimento do valor menos 1)	O ID do endpoint

Para obter um exemplo que analisa um TLV tipo 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.

Como habilitar o Proxy Protocol v2 usando o console

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.

Para habilitar o protocolo proxy v2 usando o AWS CLI

Use o comando modify-target-group-attributes.

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 aderência é ativado para um grupo-alvo, as verificações passivas de saúde não são suportadas. Para obter mais informações, consulte Verificações de saúde para seus grupos-alvo.
- Sessões persistentes não são compatíveis com receptores TLS.

Para habilitar sticky sessions usando o console

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.

Para ativar sessões fixas usando o AWS CLI

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

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.

Depois de criar um grupo de destino, você pode adicionar tags.

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 ter mais informações, consulte Regras do listener. 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 ter mais informações, consulte Registrar destinos com o grupo de destino. Você também pode modificar as configurações de verificação de integridade para seu grupo de destino. Para ter mais informações, consulte Modificar as configurações de verificação de integridade de um grupo de destino.

Para criar um grupo de destino usando o console

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 destinos por ID de 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.

    d. (Opcional) Para Port (Porta), modifique o valor padrão conforme o necessário.

    e. Em Tipo de endereço IP, escolha IPv4 ou IPv6. Essa opção só estará disponível se o tipo de destino for Instâncias ou Endereços IP e o protocolo for TCP ou TLS.

Você deve associar um grupo de destino IPv6 a um balanceador de carga dualstack. Todos os destinos no grupo de destino devem ter o mesmo tipo de endereço IP. Você não pode alterar o tipo de endereço IP de um grupo de destino depois de criá-lo.

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 ter mais informações, consulte Verificações de integridade para os grupos de destino.
6. (Opcional) Para adicionar uma tag, expanda Tags, escolha Adicionar tag e digite uma chave de tag e um valor de tag.
7. Selecione Next (Próximo).
8. Na página Registrar destinos, adicione um ou mais destinos da seguinte forma:
   - Se o tipo de destino for Instâncias, selecione uma ou mais instâncias, insira as portas e escolha Incluir como pendente abaixo.

     Observação: as instâncias devem ter um endereço IPv6 primário atribuído para serem registradas em um grupo de destino IPv6.
   - Se o tipo de destino for Endereços IP, selecione a rede, insira os endereços IP e as portas e escolha Incluir como pendente abaixo.
9. Selecione Criar grupo de destino.

Para criar um grupo-alvo usando o AWS CLI

Use o comando create-target-group para criar o grupo de destino, o comando add-tags comando para marcar com tag seu grupo de destino e o comando register-targets para adicionar destinos.

Verificações de integridade para os grupos de destino

Você pode registrar os destinos com um ou mais grupos de destino. O load balancer inicia o roteamento de solicitações para um destino recém-registrado assim que o processo de registro é concluído. 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 ter 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. As verificações de saúde passivas não são suportadas para tráfego UDP e grupos-alvo com a aderência ativada. Para obter mais informações, consulte Sessões do Sticky.

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 balanceadores de carga de rede também falharão quando você tiver um grupo-alvo 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, você pode ver as conexões TCP desse teste enviadas do seu balanceador de carga para os destinos registrados

no seu ouvinte TLS. Você pode identificar essas conexões TCP porque elas têm o endereço IP de origem do seu Network Load Balancer e as conexões não contêm pacotes de dados.

Para um serviço de UDP, 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 de um serviço de UDP. Se o serviço que recebe a verificação de integridade falhar, o destino será considerado indisponível. Para melhorar a precisão das verificações de integridade de um serviço de UDP, configure o serviço que ouve a porta de verificação de integridade para acompanhar o status do serviço de UDP e parar a verificação de integridade caso o serviço esteja indisponível.

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 a UnhealthyThresholdcontagem de falhas consecutivas, o balanceador de carga desativará o alvo. Quando as verificações de integridade excedem a HealthyThresholdcontagem de sucessos consecutivos, o balanceador de carga coloca o alvo de volta em serviço.

Configuração	Descrição	Padrão
HealthCheckProtocolo	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
HealthCheckPorto	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.

Configuração	Descrição	Padrão
HealthCheckCaminho	[Verificações de integridade HTTP/HTTPS] O caminho da verificação de saúde que é o destino nos alvos das verificações de saúde. O padrão é /.	/
HealthCheckTimeoutSeconds	O tempo, em segundos, durante o qual ausência de resposta de um destino significa uma falha na verificação de integridade. O intervalo é de 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.	Seis segundos para verificações de integrida de de HTTP e dez segundos para verificações de integrida de de TCP e HTTPS.

Configuração	Descrição	Padrão
HealthCheckIntervalSeconds	A quantia aproximada de tempo, em segundos, entre as verificações de integridade de um destino individual. O intervalo é de 5 a 300 segundos. O padrão é 30 segundos. **Important** 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
HealthyThresholdContagem	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
UnhealthyThresholdContagem	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

Configuração	Descrição	Padrão
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.

Value	Descrição
`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
`unhealthy`	O alvo não respondeu a uma verificação de saúde, falhou na verificação de saúde ou está em estado parado. Código de motivo relacionado: `Target.FailedHealthChecks`

Value	Descrição
`draining`	O destino está cancelando o registro e está acontecendo drenagem da conexão. Código de motivo relacionado: `Target.DeregistrationInProgress`
`unhealthy.draining`	O alvo não respondeu às verificações de saúde ou foi reprovado nas verificações de saúde e entrou em um período de carência. O alvo suporta 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 alvo não está registrado em um grupo-alvo, o grupo-alvo não é usado em uma regra de ouvinte ou o alvo está em uma zona de disponibilidade que não está ativada. 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	Descrição
`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 de seus destinos

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

Para verificar a integridade dos seus destinos usando o console

1. Abra o console 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. O painel 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.

Para verificar a saúde de seus alvos usando o AWS CLI

Use o comando describe-target-health. O resultado desse comando contém o estado de integridade do destino. Ele incluirá um código de motivo se o status for qualquer valor diferente de `Healthy`.

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.

Modificar as configurações de verificação de integridade de um grupo de destino

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

Para modificar as configurações de verificação de integridade de um grupo de destino usando o console

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 e escolha Salvar alterações.

Para modificar as configurações de verificação de saúde de um grupo-alvo usando o AWS CLI

Use o comando modify-target-group.

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 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.

Considerações

- Ao ativar o balanceamento de carga entre zonas para um Network Load Balancer, aplicam-se taxas de transferência de dados do EC2. Para obter mais informações, consulte Entendendo as cobranças de transferência de AWS dados no Guia do usuário de exportações de dados
- 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 desativado, 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 desativado, certifique-se de que todos os grupos de destino participem das mesmas zonas de disponibilidade. Uma zona de disponibilidade vazia é considerada não íntegra.

Modificar o balanceamento de carga entre zonas para um balanceador de carga

Você pode ativar ou desativar o balanceamento de carga entre zonas no balanceador de carga a qualquer momento.

Modificar o balanceamento de carga entre zonas para um 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, 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.

Para modificar o balanceamento de carga entre zonas para seu balanceador de carga usando o AWS CLI

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

Modificar balanceamento de carga entre zonas para um grupo de destino

A configuração de balanceamento de carga entre zonas em nível de grupo de destino substitui a configuração em nível de balanceador de carga.

Você poderá ativar ou desativar 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.

Modificar o balanceamento de carga entre zonas para um grupo de destino usando o console

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.

Para modificar o balanceamento de carga entre zonas para um grupo-alvo usando o AWS CLI

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

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.

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 ter mais informações, consulte Balanceamento de carga entre zonas.
- 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).
- 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, 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.

Modificar configurações de integridade do grupo de destino

Você pode modificar as configurações de integridade do grupo de destino conforme exibido a seguir.

Para modificar as configurações de integridade do grupo de destino usando o console

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. Verifique se o balanceamento de carga entre zonas está ativado ou desativado. Atualize essa configuração conforme necessário para garantir que você tenha capacidade suficiente para processar o tráfego adicional se uma zona falhar.
6. Expanda os requisitos de integridade do grupo de destino.
7. Em Tipo de configuração, recomendamos que você escolha Configuração unificada, que define o mesmo limite para ambas as ações.
8. 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.
9. Escolha Salvar alterações.

Para modificar as configurações de saúde do grupo-alvo usando o AWS CLI

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

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067 \
--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=50
```

Encerramento da conexão para destinos não íntegros

O encerramento da conexão está 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 desativado, o alvo ainda é considerado insalubre e não receberá novas conexões, mas as conexões estabelecidas são mantidas ativas, permitindo que elas se fechem normalmente.

O término da conexão para alvos não íntegros pode ser definido individualmente para cada grupo-alvo.

Modificar a configuração de encerramento da conexão usando o console

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.

Para modificar a configuração de encerramento da conexão usando o AWS CLI

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

Intervalo de drenagem insalubre

> **Important**
>
> O término da conexão deve ser desativado antes de ativar o intervalo de drenagem não íntegro.

Os destinos no `unhealthy.draining` estado são considerados não íntegros, não recebem novas conexões, mas mantêm as conexões estabelecidas durante o intervalo configurado. O intervalo de conexão não íntegra determina a quantidade de tempo que o alvo permanece no

`unhealthy.draining` estado antes que seu estado se torne`unhealthy`. Se o alvo passar pelas verificações de integridade durante o intervalo de conexão não íntegra, seu estado `healthy` voltará a ser. Se um cancelamento de registro for acionado, o estado alvo se torna `draining` e o tempo limite de atraso do cancelamento de registro começa.

O intervalo de drenagem não saudável pode ser definido individualmente para cada grupo-alvo.

Para modificar o intervalo de drenagem insalubre usando o console

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 Target, certifique-se de que a opção Encerrar conexões quando os destinos não estiverem íntegros esteja desativada.
6. Insira um valor para Intervalo de drenagem insalubre.
7. Escolha Salvar alterações.

Para modificar o intervalo de drenagem insalubre usando o AWS CLI

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

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 usar a opção Avaliar a 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`. Para um Network Load Balancer, o Route 53 usa as verificações de integridade do grupo de destino associadas ao balanceador de carga.
- Quando todos os grupos de destino em um Network Load Balancer estiverem íntegros, o Route 53 marcará o registro do alias como íntegro. Se um grupo de destino contiver pelo menos um destino saudável, a verificação de integridade do grupo de destino será aprovada. Em seguida, o Route 53 retornará os registros de acordo com a sua política de roteamento. Se a política de roteamento por failover for usada, o Route 53 retornará o registro primário.
- Se algum dos grupos de destino em um Network Load Balancer não estiver íntegro, o registro do alias apresentará falha na verificação de integridade do Route 53 (falha na abertura). Se for usada a avaliação da integridade do destino, ocorrerá falha na política de roteamento por failover.
- 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 for usada a avaliação da integridade do destino, ocorrerá falha na política de roteamento por failover.

Para obter mais informações, consulte Configurar failover de DNS no Guia do desenvolvedor do Amazon Route 53.

Registrar destinos com o grupo de destino

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 IDs de instância, 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 ter mais informações, consulte Verificações de integridade para os grupos de destino.

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 ter 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.

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, preservamos os endereços IP do cliente ao traduzir endereços IPv4 para IPv6. No entanto, ao traduzir endereços IPv6 para IPv4, o IP de origem é sempre o endereço IP privado do Network Load Balancer.

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 Endereço IPv4 privado).

Para ter mais informações, consulte Grupos de segurança para o Network Load Balancer.

Network ACLs

Quando você registra instâncias do EC2 como destinos, precisa garantir que as ACLs de rede das sub-redes para suas instâncias permitam o tráfego tanto na porta do listener quanto 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 ACLs de rede personalizadas, verifique se elas permitem o tráfego apropriado.

As ACLs da rede associadas às sub-redes das instâncias devem permitir o tráfego a seguir para um balanceador de carga voltado para a Internet.

Regras recomendadas para sub-redes de instância

Inbound

Origem	Protocolo	Intervalo de portas	Comentário
Endereços IP do cliente	*listener*	*listener*	Permitir tráfego do cliente (tipo de destino `instance`)
CIDR DA VPC	*listener*	*listener*	Permitir tráfego do cliente (tipo de destino `ip`)
CIDR DA VPC	*verificação de saúde*	*verificação de saúde*	Permitir tráfego de verificação de integridade do load balancer

Outbound

Destination (Destino)	Protocolo	Intervalo de portas	Comentário
Endereços IP do cliente	*listener*	*listener*	Permitir respostas aos clientes (tipo de destino `instance`)
CIDR DA VPC	*listener*	*listener*	Permitir respostas aos clientes (tipo de destino `ip`)
CIDR DA VPC	*verificação de saúde*	1024-65535	Permitir tráfego de verificação de integridade

As ACLs da rede associadas às sub-redes do balanceador de carga devem permitir o tráfego a seguir para um balanceador de carga voltado para a Internet.

Regras recomendadas para sub-redes do load balancer

Inbound

Origem	Protocolo	Intervalo de portas	Comentário
Endereços IP do cliente	*listener*	*listener*	Permitir tráfego do cliente (tipo de destino `instance`)
CIDR DA VPC	*listener*	*listener*	Permitir tráfego do cliente (tipo de destino `ip`)
CIDR DA VPC	*verificação de saúde*	1024-65535	Permitir tráfego de verificação de integridade

Outbound

Destination (Destino)	Protocolo	Intervalo de portas	Comentário
Endereços IP do cliente	*listener*	*listener*	Permitir respostas aos clientes (tipo de destino `instance`)
CIDR DA VPC	*listener*	*listener*	Permitir respostas aos clientes (tipo de destino `ip`)
CIDR DA VPC	*verificação de saúde*	*verificação de saúde*	Permitir tráfego de verificação de integridade
CIDR DA VPC	*verificação de saúde*	1024-65535	Permitir tráfego de verificação de integridade

Para um balanceador de carga interno, as ACLs da rede das sub-redes das instâncias e os nós do balanceador de carga devem permitir tráfego de entrada e de saída de e para o CIDR da VPC, na porta do receptor e nas portas temporárias.

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 ou cancelar o registro de 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 como você registra os destinos com esse grupo de destino. Para ter mais informações, consulte Target type.

Requisitos e considerações

- Você não pode registrar instâncias por ID de instância se for usado um dos seguintes tipos de instância: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1.
- Ao registrar destinos por ID de instância para um grupo de destino IPv6, os destinos devem ter um endereço IPv6 primário atribuído. Para saber mais, consulte endereços IPv6 no Guia do usuário do Amazon EC2
- Ao registrar destinos por ID de instância, as instâncias devem estar na mesma Amazon 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.
- Para grupos de destino UDP e TCP_UDP, 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, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1. 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.

Conteúdo

- Registrar ou cancelar o registro de destinos por ID de Instância
- Registrar ou cancelar o registro de destinos por endereço IP
- Como registrar ou cancelar o registro de destinos usando a AWS CLI

Registrar ou cancelar o registro de destinos por ID de Instância

Uma instância deve estar no estado `running` quando você registrá-la.

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

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. Para registrar instâncias, escolha Registrar destinos. Selecione uma ou mais instâncias, insira a porta padrão da instância conforme necessário e escolha Incluir como pendente abaixo. Após terminar de adicionar instâncias, escolha Registrar destinos pendentes.

   Observações:

   - para que sejam registradas em um grupo de destino IPv6, as instâncias devem ter um endereço IPv6 primário atribuído.
   - As AWS GovCloud (US) Region s não são compatíveis com a atribuição de um endereço IPv6 primário usando o console. Você deve usar a API para atribuir endereços IPv6 primários em s. AWS GovCloud (US) Region

6. Para cancelar o registro de instâncias, selecione a instância e escolha Cancelar registro.

Registrar ou cancelar o registro de destinos por endereço IP

Destinos IPv4

Um endereço IP que você registra deve ser de um dos seguintes blocos CIDR:

- As sub-redes da VPC para o 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)

O tipo de endereço IP não pode ser alterado após a criação do grupo de destino.

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

Destinos IPv6

- Os endereços IP que você registra devem estar dentro do bloco CIDR da VPC ou dentro de um bloco CIDR da VPC emparelhado.
- O tipo de endereço IP não pode ser alterado após a criação do grupo de destino.
- Você pode associar grupos de destino IPv6 somente a um balanceador de carga dualstack com receptores TCP ou TLS.

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

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. Para registrar endereços IP, escolha Registrar destinos. Para cada endereço IP, selecione a rede, a zona de disponibilidade, o endereço IP (IPv4 ou IPv6) e a porta e, em seguida, escolha

Incluir como pendente abaixo. Quando você concluir a especificação de endereços, escolha Registrar destinos pendentes.

6. Para cancelar o registro de endereços IP, selecione os endereços IP e escolha Cancelar registro. Se você tiver vários endereços IP registrados, poderá ser útil para adicionar um filtro ou alterar a ordem de classificação.

Como registrar ou cancelar o registro de destinos usando a AWS CLI

Use o comando register-targets para adicionar destinos e o comando deregister-targets para remover destinos.

Application Load Balancers como destinos

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

- Para associar um Application Load Balancer como destino de um Network Load Balancer, ele deve estar na mesma Amazon VPC e na mesma conta.
- Você pode associar um Application Load Balancer como destino de vários Network Load Balancers. Para fazer isso, registre o Application Load Balancer em um grupo de destino separado para cada Network Load Balancer individual.

- 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 (se o balanceamento de carga entre zonas estiver desabilitado) ou 100 (se o balanceamento de carga entre zonas estiver habilitado). 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 ter 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.

Etapa 1:criar o Application Load Balancer

Antes de começar, configure os grupos de destino que esse Application Load Balancer usará. Certifique-se de ter uma nuvem privada virtual (VPC) com os destinos que você registrará no grupo de destino. Essa VPC deve ter pelo menos uma sub-rede pública em cada uma das zonas de disponibilidade usadas pelos destinos.

Para criar um Application Load Balancer usando o console

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 Application Load Balancer, escolha Create (Criar).
5. Na página Criar Application Load Balancer, em Configuração básica, especifique o Nome do balanceador de carga, o Esquema e o Tipo de endereço IP.
6. Em Receptores, você pode criar um receptor HTTP ou HTTPS em qualquer porta. No entanto, você deverá garantir que o número da porta desse receptor corresponda à porta do grupo de destino no qual esse Application Load Balancer residirá.
7. Em Zonas de disponibilidade, faça o seguinte:

    a. Em VPC, selecione uma nuvem privada virtual (VPC) com instâncias ou endereços IP que você incluiu como destinos do Application Load Balancer. Você deve usar a mesma VPC que usaria para o Network Load Balancer em Etapa 3: criar um Network Load Balancer e configurar o Application Load Balancer como destino.

b. Selecione duas ou mais zonas de disponibilidade e sub-redes correspondentes. Certifique-se de que essas zonas de disponibilidade correspondam às que estão habilitadas para ou Network Load Balancer para otimizar a disponibilidade, a escalabilidade e o desempenho.

8. Você pode Atribuir um grupo de segurança ao balanceador de carga ao criar um grupo de segurança ou ao selecionar um existente.

   Esse novo grupo de segurança que você seleciona contém uma regra que permite tráfego para a porta do receptor para esse balanceador de carga. Use os blocos CIDR (intervalo de endereços IP) dos computadores do cliente como origem de tráfego nas regras de entrada para grupos de segurança. Isso permite que os clientes enviem tráfego por meio desse Application Load Balancer. Para obter mais informações sobre a configuração de grupos de segurança para um Application Load Balancer como destino de um Network Load Balancer, consulte Grupos de segurança para o Application Load Balancer no Guia do usuário de Application Load Balancers.
9. Em Configurar roteamento, selecione o grupo de destino que você configurou para esse Application Load Balancer. Se você não tiver um grupo de destino disponível e quiser configurar um novo, consulte Create a target group no Guia do usuário de Application Load Balancers.
10. Revise sua configuração e escolha Create load balancer (Criar um balanceador de carga).

Para criar o Application Load Balancer usando o AWS CLI

Use o comando create-load-balancer.

Etapa 2: criar o grupo de destino com o Application Load Balancer como destino

Criar um grupo de destino permite o registro de um Application Load Balancer novo ou existente como destino. Você só pode adicionar um Application Load Balancer por grupo de destino. O mesmo Application Load Balancer também pode ser usado em um grupo de destino separado, como o destino de até dois Network Load Balancers.

Para criar um grupo-alvo e registrar o Application Load Balancer como destino, usando o console

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. Na página Especificar detalhes do grupo, em Configuração básica, escolha Application Load Balancer.
5. Em Nome do grupo de destino, digite um nome para o grupo de destino do Application Load Balancer.
6. Em Protocolo, somente TCP é permitido. Selecione a Porta do grupo de destino. Essa porta do grupo de destino deve corresponder à porta do receptor do Application Load Balancer. Como alternativa, você pode adicionar ou editar a porta do receptor no Application Load Balancer para corresponder a essa porta.
7. Em VPC, selecione a nuvem privada virtual (VPC) com o Application Load Balancer para se registrar no grupo de destino.
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) Adicione uma ou mais tags conforme necessário.
10. Selecione Next (Próximo).
11. Na página Registrar destinos, escolha o Application Load Balancer que você deseja registrar como destino. O Application Load Balancer que você escolher na lista deverá ter um receptor na mesma porta do grupo de destino que você estiver criando. 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 especificada para o grupo de destino. Caso não tenha certeza sobre qual Application Load Balancer adicionar como destino ou não quiser adicioná-lo neste momento, você poderá pode optar por adicionar o Application Load Balancer posteriormente.
12. Selecione Criar grupo de destino.

Criar um grupo de destino e registrar o Application Load Balancer como destino usando a AWS CLI

Use os comandos create-target-group e register-targets.

Etapa 3: criar um Network Load Balancer e configurar o Application Load Balancer como destino

Use as etapas a seguir para criar o Network Load Balancer e, em seguida, configure o Application Load Balancer como destino usando o console.

Para criar seu Network Load Balancer e ouvinte usando o console

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

   No painel Configuração básica, configure o Nome do balanceador de carga, o Esquema e o Tipo de endereço IP.
6. Mapeamento de rede

   a. Em VPC, selecione a mesma VPC que você usou para o destino do Application Load Balancer. Se você tiver selecionado Voltado para a Internet para Esquema, somente VPCs com um gateway da Internet estarão disponíveis para seleção.

   b. Em Mapeamentos, selecione duas ou mais zonas de disponibilidade e as sub-redes correspondentes. Recomendamos que você selecione as mesmas zonas de disponibilidade do destino do Application Load Balancer para otimizar a disponibilidade, a escalabilidade e o desempenho.

      (Opcional) Para usar endereços IP estáticos, escolha Usar um endereço IP elástico nas Configurações de IPv4 para 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. 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 do Application Load Balancer para encaminhar o tráfego. Se você não o vir na lista ou não conseguir selecionar um grupo de destino (porque ele já está sendo usado por outro Network Load Balancer), você poderá criar um grupo de destino do Application Load Balancer, conforme mostrado em Etapa 2: criar o grupo de destino com o Application Load Balancer como destino.

8. Tags

   (Opcional) Adicione tags para caracterizar o balanceador de carga. Para obter mais informações, consulte Etiquetas.

9. Resumo

   Revise sua configuração e escolha Create load balancer (Criar um balanceador de carga).

Para criar o Network Load Balancer usando o AWS CLI

Use o comando create-load-balancer.

Etapa 4: (opcional) criar um serviço de endpoint da 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 .

Tags para o grupo de destino

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.

Para atualizar as tags de um grupo-alvo usando o console

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. Ao concluir a atualização de tags, selecione Salvar alterações.

Para atualizar as tags de um grupo-alvo usando o AWS CLI

Use os comandos add-tags e remove-tags.

Excluir um grupo de destino

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.

Para excluir um grupo-alvo usando o console

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. Quando a confirmação for solicitada, escolha Sim, excluir.

Para excluir um grupo-alvo usando o AWS CLI

Use o comando delete-target-group.

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. Você pode usar essas métricas para verificar se o sistema está executando conforme o esperado. Para ter 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 front-end entre o cliente e o balanceador de carga e outra para a conexão de back-end 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 security group da instância não permitir conexões do cliente, mas as ACLs da rede para a sub-rede do load balancer as permitirem, os logs para a interface de rede do load balancer mostrarão "ACEITAR OK" para as conexões de front-end e back-end, enquanto os logs para a 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.

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 ter 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 ter mais informações, consulte Registro em log de chamadas de API para o Network Load Balancer usando o AWS 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.

Você pode 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
- Dimensões métricas dos Network Load Balancers

- Estatísticas para métricas do Network Load Balancer
- Veja CloudWatch as métricas do seu balanceador de carga

Métricas do Network Load Balancer

O namespace `AWS/NetworkELB` inclui as métricas a seguir.

Métrica	Descrição
`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`
`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 encerradas 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`

Métrica	Descrição
	• `AvailabilityZone` , `LoadBalancer`
`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`
`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`

Métrica	Descrição
`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 de 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 de 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	Descrição
`ConsumedLCUs_TLS`	O número de unidades de capacidade do load balancer (LCU) usadas pelo load balancer para TLS. Você paga pelo número de 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 de 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	Descrição
`HealthyHostCount`	O número de destinos considerados íntegros. Essa métrica não inclui quaisquer Application Load Balancers registrados como destinos. Critérios de relatório: relatado se as verificações de integridade estiverem habilitadas. 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`
`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`

Métrica	Descrição
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
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

Métrica	Descrição
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. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Maximum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
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. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descrição
`ProcessedBytes`	O número total de bytes processados pelo load balancer, incluindo cabeçalhos TCP/IP. 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`
`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`

Métrica	Descrição
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
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. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Estatísticas: a estatística mais útil é Sum. Dimensões • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_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	Descrição
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	Descrição
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	Descrição
`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	Descrição
`UnHealthyHostCount`	O número de destinos considerados sem integridade. Essa métrica não inclui quaisquer Application Load Balancers registrados como destinos. Critérios de relatório: relatado se as verificações de integridade estiverem habilitadas. 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). Reporting criteria (Critérios de relatório): há um valor diferente de zero. 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	Descrição
`AvailabilityZone`	Filtra os dados de métrica por zona de disponibilidade.

Dimensão	Descrição
`LoadBalancer`	Filtra os dados da métrica por load balancer. Especifique o load balancer da seguinte maneira: net/load-balancer-name/1234567890123456 (a parte final do ARN do load balancer).
`TargetGroup`	Filtra os dados da métrica por grupo de destino. Especifique o grupo de destino da seguinte maneira: targetgroup/target-group-name/1234567890123456 (a parte final do ARN do grupo de destino).

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. Dimensão é um par de nome/valor que identifica exclusivamente 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 balanceador de carga usando o CloudWatch console.

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 comando get-metric-statistics 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. Você deve 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 registros de acesso que capturam informações detalhadas sobre as conexões TLS estabelecidas com seu Network Load Balancer. Você pode usar esses logs de acesso para analisar padrões de tráfego e solucionar problemas.

> **Important**
>
> Os registros de acesso são criados somente quando o Network Load Balancer tem um ouvinte TLS e contêm informações somente sobre conexões TLS.

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 acesso 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 por sua vez é criptografada com uma chave KMS que é rotacionada 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.

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.

região

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	Descrição
tipo	O tipo de listener. O valor suportado é `tls`.
versão	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.
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 connection_time.
received_bytes	A contagem de bytes recebidos pelo load balancer do cliente, após a descriptografia.

Campo	Descrição
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, o valor será definido como -.
chosen_cert_arn	O ARN do certificado fornecido ao cliente. Se nenhuma mensagem Hello válida do cliente 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 -.
tls_named_group	Reservado para uso futuro. Esse valor é sempre definido como -.
domain_name	O valor da extensão do cliente server_name na mensagem Hello. Esse valor é codificado em URL. Se nenhuma mensagem Hello válida do cliente for enviada ou a extensão não estiver presente, esse valor será definido como -.
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 listener TLS, nenhum protocolo correspondente será encontrado, ou se nenhuma lista de protocolos válidos 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 listener TLS, nenhum protocolo correspondente será encontrado, ou se nenhuma lista de protocolos válidos for enviada, esse valor será definido como -.

Campo	Descrição
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 listener TLS, nenhuma mensagem Hello válida do cliente será enviada, ou se 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

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
```

Requisitos do bucket

Quando você habilitar o log de acesso, deverá especificar um bucket do S3 para os logs de acesso. O bucket pode pertencer a uma conta diferente daquela que controla o load balancer. O bucket deve atender aos seguintes requisitos:

Requisitos

- O bucket deve estar localizado na mesma região que o load balancer.
- 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. Veja abaixo um exemplo de política .

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::my-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:::my-bucket/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:*"]
                }
            }
        }
    ]
}
```

Na política anterior, em `aws:SourceAccount`, especifique a lista de números de conta para os quais os logs estão sendo entregues a esse bucket. Para `aws:SourceArn`, especifique a lista de ARNs do recurso que gera os logs, no formulário `arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

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 .

```
{
  "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": "*"
    }
  ]
}
```

Habilitar registro em log de acesso

Ao habilitar os registros em log de acesso para o balanceador de carga, você deve especificar o bucket do S3 em que o balanceador de carga armazenará os logs. Certifique-se de que você possui esse bucket e que configurou a política de bucket necessária para este bucket. Para ter mais informações, consulte Requisitos do bucket.

Para habilitar o registro de logs de acesso usando o console

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. Na página Editar atributos do load balancer, faça o seguinte:
   a. Em Monitoramento, ative os Logs de acesso.
   b. Escolha Procurar no S3 e selecione um bucket para ser usado. Como alternativa, insira a localização do bucket do S3, incluindo qualquer prefixo.
   c. Escolha Salvar alterações.

Para habilitar o registro de acesso usando o AWS CLI

Use o comando modify-load-balancer-attributes.

Desabilitar registro em log de acesso

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 Trabalhar com buckets no Guia do usuário do Amazon Simple Storage Service.

Para desabilitar o registro de logs de acesso usando o console

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. Escolha Salvar alterações.

Para desativar o registro de acesso usando o AWS CLI

Use o comando modify-load-balancer-attributes.

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

Registro em log de chamadas de API para o Network Load Balancer usando o AWS CloudTrail

O Elastic Load Balancing é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS service (Serviço da AWS) no Elastic Load Balancing. CloudTrail captura todas as chamadas de API para o Elastic Load Balancing como eventos. As chamadas capturadas incluem chamadas de AWS Management Console e chamadas de código para as operações da API Elastic Load Balancing. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Elastic Load Balancing. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Elastic Load Balancing, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações sobre o Elastic Load Balancing em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Elastic Load Balancing, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do Elastic Load Balancing, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra logs de eventos de todas as Regiões na AWS divisória e entrega os arquivos do log para o bucket Amazon S3 especificado. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão geral da criação de uma trilha

- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Elastic Load Balancing para Network Load Balancers são registradas CloudTrail e documentadas na versão 2015-12-01 de referência da API Elastic Load Balancing. Por exemplo, chamadas para as `DeleteLoadBalancer` ações `CreateLoadBalancer` e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário da raiz ou do .
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte o elemento CloudTrailuserIdentity.

Noções básicas sobre entradas de arquivo de log do Elastic Load Balancing

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Os arquivos de log incluem eventos para todas as chamadas de AWS API para você Conta da AWS, não apenas as chamadas de API do Elastic Load Balancing. Você pode localizar chamadas para a API do Elastic Load Balancing verificando os elementos `eventSource` com o valor `elasticloadbalancing.amazonaws.com`. Para visualizar um registro para uma ação específica, como `CreateLoadBalancer`, verifique os elementos `eventName` com o nome da ação.

A seguir estão exemplos de registros de CloudTrail log do Elastic Load Balancing para um usuário que criou um Network Load Balancer e o excluiu usando o. AWS CLI Você pode identificar a CLI

usando os elementos `userAgent`. Você pode identificar as chamadas de APIs solicitadas usando os elementos `eventName`. Informações sobre o usuário (`Alice`) podem ser encontradas no elemento `userIdentity`.

Example Exemplo: CreateLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing",
        "type": "network"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "network",
            "ipAddressType": "ipv4",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
```

```
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Example Exemplo: DeleteLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

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 ter mais informações, consulte Verificações de integridade para os grupos de destino.

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 ter mais informações, consulte Grupos de segurança de destino.

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 ter mais informações, consulte Network 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 ter mais informações, consulte Grupos de segurança de destino.

Uma lista de controle de acesso (ACL) à rede não permite o tráfego

As ACLs à redes associadas às sub-redes para a VPC devem permitir que o load balancer e os destinos se comuniquem nas duas direções da porta do listener. Para ter mais informações, consulte Network 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.

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.

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.
- 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 portas conectando-se por AWS PrivateLink

Se o Network Load Balancer estiver associado a um serviço de endpoint da VPC, ele oferecerá 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, há uma chance maior de erros de alocação de porta. Os erros na alocação de portas podem ser rastreados por meio da métrica `PortAllocationErrorCount`. Para corrigir erros na alocação de portas, adicione mais destinos ao grupo de destino. Para ter mais informações, consulte CloudWatch métricas para seu Network Load Balancer.

Falha intermitente de conexão quando a preservação do IP do cliente está habilitada

Quando a preservação do IP do cliente está habilitada, você pode encontrar limitações de conexão TCP/IP relacionadas à reutilização observada de soquetes nos destinos. Essas limitações de conexão podem ocorrer quando um cliente ou um dispositivo NAT na frente do cliente usa o mesmo endereço IP de origem e porta de origem ao se conectar a vários nós do balanceador de carga simultaneamente. Se o balanceador de carga rotear essas conexões para o mesmo destino, as conexões aparecerão no destino como se viessem do mesmo soquete de origem, o que resultará em erros de conexão. Se isso acontecer, os clientes poderão tentar novamente (se a conexão falhar) ou se reconectar (se a conexão for interrompida). Você pode reduzir esse tipo de erro de conexão aumentando o número de portas temporárias de origem ou aumentando o número de destinos para o balanceador de carga. Você pode evitar esse tipo de erro de conexão desabilitando a preservação do IP do cliente ou desabilitando o balanceamento de carga entre zonas.

Além disso, quando a preservação do IP do cliente está habilitada, a conectividade poderá falhar se os clientes que estiverem se conectando ao Network Load Balancer também estiverem conectados a destinos atrás do balanceador de carga. Para resolver isso, você pode desabilitar a preservação do IP do cliente nos grupos de destino afetados. Como alternativa, faça com que seus clientes se conectem somente ao Network Load Balancer ou somente aos destinos, mas não a ambos.

Atrasos na conexão TCP

Quando o balanceamento de carga entre zonas e a preservação do IP do cliente estão habilitados, um cliente conectado a diferentes IPs no mesmo balanceador de carga pode ser roteado para o mesmo destino. Se o cliente usar a mesma porta de origem para essas duas conexões, o destino

receberá o que aparentemente é uma conexão duplicada, o que poderá levar a erros de conexão e atrasos de TCP no estabelecimento de novas conexões. Você pode evitar esse tipo de erro de conexão desabilitando o balanceamento de carga entre zonas. Para ter mais informações, consulte Balanceamento de carga entre zonas.

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.

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 instâncias de destino registradas íntegras em todas as zonas de disponibilidade habilitadas, o modo de falha na abertura será habilitado e o DNS fornecerá todos os endereços IP das três AZs habilitadas no resultado.

Solucione problemas de alvos 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 alvos não íntegros e realizar ações com base no código do motivo da falha. Para ter mais informações, consulte Mapa de recursos do Network Load Balancer.

O mapa de recursos fornece duas visualizações: Visão geral e Mapa de alvos insalubres. A opção Visão geral é selecionada por padrão e exibe todos os recursos do seu balanceador de carga. Selecionar a visualização Unhealth Target Map exibirá somente os alvos não íntegros em cada grupo de destino associado ao Network Load Balancer.

> **Note**
>
> A opção Mostrar detalhes do recurso deve estar ativada para visualizar o resumo da verificação de integridade e as mensagens de erro de todos os recursos aplicáveis no mapa de recursos. Quando não ativado, você deve selecionar cada recurso para ver seus detalhes.

A coluna Grupos-alvo exibe um resumo das metas saudáveis e não saudáveis de cada grupo-alvo. Isso pode ajudar a determinar se todos os alvos estão falhando nas verificações de saúde ou se somente alvos específicos estão falhando. Se todos os alvos em um grupo-alvo falharem nas verificações de saúde, verifique as configurações de verificação de saúde do grupo-alvo. Selecione o nome de um grupo-alvo para abrir sua página de detalhes em uma nova guia.

A coluna Metas exibe o TargetID e o status atual da verificação de saúde de cada alvo. Quando um alvo não está íntegro, o código do motivo da falha da verificação de integridade é exibido. Quando um único alvo está falhando em uma verificação de saúde, verifique se o alvo tem recursos suficientes. Selecione o ID de um alvo para abrir sua página de detalhes em uma nova guia.

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

Verifique se sua instância está falhando nas verificações de integridade e, com base no código do motivo da falha, verifique os seguintes problemas:

- Insalubre: a solicitação atingiu o tempo limite

- Verifique se os grupos de segurança e as listas de controle de acesso à rede (ACL) associados aos seus alvos 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 do aplicativo de cada alvo. Para obter mais informações, consulte Códigos de motivo da verificação de saúde.

- Insalubre: FailedHealthChecks
  - Verifique se o alvo está escutando o tráfego na porta de verificação de integridade.

    > Ao usar um ouvinte TLS
    >
    > Você escolhe qual política de segurança é usada para conexões front-end. A política de segurança usada para conexões de back-end é selecionada automaticamente com base na política de segurança de front-end em uso.
    >
    > - Se seu ouvinte TLS estiver usando uma política de segurança TLS 1.3 para conexões front-end, a política de `ELBSecurityPolicy-TLS13-1-0-2021-06` segurança será usada para conexões back-end.
    > - Se seu ouvinte TLS não estiver usando uma política de segurança TLS 1.3 para conexões front-end, a política de `ELBSecurityPolicy-2016-08` segurança será usada para conexões back-end.
    >
    > 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 suporta uma ou mais cifras correspondentes e um protocolo fornecido pelo Network Load Balancer para estabelecer handshakes TLS.

Cotas para seus Network Load Balancers

Sua Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada serviço da AWS. A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar aumentos para algumas cotas e outras cotas 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. Também é possível usar o comando describe-account-limits (AWS CLI) para o Elastic Load Balancing.

Para solicitar o aumento da cota, consulte Requesting a Quota Increase (Solicitar um aumento de cota) no Manual do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o formulário de aumento de limite do Elastic Load Balancing.

Load balancer

Sua Conta da AWS tem as seguintes cotas relacionadas aos Network Load Balancers.

Nome	Padrão	Ajustável
Certificados por Network Load Balancer	25	Yes (Sim)
Receptores por Network Load Balancer	50	Não
ENIs do Network Load Balancer por VPC	1.200 [1]	Yes (Sim)
Network Load Balancers por região	50	Yes (Sim)
Grupos de destino por ação por Network Load Balancer	1	Não
Destinos por zona de disponibilidade por Network Load Balancer	500 [2, 3]	Yes (Sim)
Destinos por Network Load Balancer	3.000 [3]	Yes (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	Yes (Sim)
Destinos por grupo de destino por região (instâncias ou endereços IP)	1.000	Yes (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.

Histórico dos documentos dos Network Load Balancers

A tabela a seguir descreve as versões dos Network Load Balancers.

Alteração	Descrição	Data
Certificados RSA 3072 bits e ECDSA 256/384/521 bits	Esta versão adiciona suporte para certificados RSA de 3072 bits e certificados Elliptic Curve Digital Signature Algorithm (ECDSA) de 256, 384 e 521 bits via (ACM). AWS Certificate Manager	19 de janeiro de 2024
Terminação TLS FIPS 140-3	Esta versão adiciona políticas de segurança que usam módulos criptográficos FIPS 140-3 ao encerrar conexões TLS.	20 de novembro de 2023
Afinidade de DNS zonal	Esta versão adiciona suporte para 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
Desativar o encerramento não íntegro da conexão de destino	Esta versão adiciona suporte para manter conexões ativas com destinos que falham nas verificações de integridade.	12 de outubro de 2023
Encerramento da conexão UDP padrão	Esta versão adiciona suporte para encerrar conexões UDP no final do tempo limite de cancelamento de registro, por padrão.	12 de outubro de 2023

Registre alvos usando IPv6	Esta versão adiciona suporte para registrar instâncias como destinos quando endereçadas pelo 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 no nível do grupo-alvo.	17 de novembro de 2022
Grupos de destino IPv6	Esta versão adiciona suporte para configurar grupos de destino IPv6 para balanceadores de carga de rede.	23 de novembro de 2021
Balanceadores de carga internos IPv6	Esta versão adiciona suporte para configurar grupos de destino IPv6 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 IPv4 e 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	Esta versão permite que você forneça um endereço IP privado do intervalo de endereços IPv4 da sub-rede especificada quando você habilita uma zona de disponibilidade para um load balancer 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	Esta versão adiciona suporte para três políticas de segurança adicionais predefinidas de sigilo direto.	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 na nova região	Esta versão adiciona suporte para balanceadores de carga de rede 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.