



Balancedores de carga de gateway

Elastic Load Balancing



Elastic Load Balancing: Balanceadores de carga de gateway

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 clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, conectados ou patrocinados pela Amazon.

Table of Contents

O que é um balanceador de carga de gateway?	1
Visão geral do Gateway Load Balancer	1
Fornecedores de dispositivos	2
Conceitos básicos	2
Preços	2
Conceitos básicos	3
Visão geral	3
Roteamento	5
Pré-requisitos	6
Etapa 1: Crie um Gateway Load Balancer	6
Etapa 2: Criar um serviço de endpoint do Gateway Load Balancer	7
Etapa 3: Criar um endpoint do Gateway Load Balancer	8
Etapa 4: Configurar o roteamento	10
Conceitos básicos do uso da CLI	12
Visão geral	12
Roteamento	5
Pré-requisitos	15
Etapa 1: Criar um Gateway Load Balancer e registrar destinos	15
Etapa 2: Criar um endpoint do Gateway Load Balancer	17
Etapa 3: configurar o roteamento	18
Balanceadores de cargas	20
Estado do load balancer	20
Tipo de endereço IP	21
Atributos do load balancer	22
Zonas de disponibilidade	22
A unidade de transmissão máxima (MTU) da rede	22
Proteção contra exclusão	23
Balanceamento de carga entre zonas	24
Fluxos assimétricos	24
Intervalo ocioso	24
Criar um balanceador de carga	25
Pré-requisitos	25
Criar o balanceador de carga	25
Próximas etapas importantes	26

Atualizar tags	26
Excluir um balanceador de carga	28
Listeners	29
Grupos de destino	30
Configuração de roteamento	30
Target type	31
Destinos registrados	31
Atributos do grupo de destino	32
Atraso do cancelamento do registro	33
Failover de destino	34
Aderência do fluxo	35
Criar um grupo de destino	36
Configurar verificações de integridade	39
Configurações de verificação de integridade	39
Status de integridade do destino	41
Códigos de motivo de verificação de integridade	42
Cenários de falha do destino	43
Verificar a integridade de seus destinos	44
Modificar configurações de verificação de integridade	45
Registrar destinos	46
Grupos de segurança de destino	46
Network ACLs	47
Registrar ou cancelar o registro de destinos	47
Atualizar tags	50
Excluir um grupo de destino	51
Monitorar os load balancers	53
Métricas do CloudWatch	54
Métricas do Gateway Load Balancer	55
Dimensões métricas dos Gateway Load Balancers	57
Visualizar métricas do CloudWatch para seu Gateway Load Balancer	57
Logs do CloudTrail	59
Informações do Elastic Load Balancing no CloudTrail	60
Noções básicas sobre entradas de arquivo de log do Elastic Load Balancing	61
Cotas	64
Histórico do documento	66
.....	lxvii

O que é um balanceador de carga de gateway?

O Elastic Load Balancing distribui automaticamente seu tráfego de entrada entre vários destinos 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 Gateway Load Balancers. Para obter mais informações sobre os outros balanceadores de carga, consulte o [Manual do usuário para Application Load Balancers](#), o [Manual do usuário para Network Load Balancers](#) e o [Manual do usuário para Classic Load Balancers](#).

Visão geral do Gateway Load Balancer

Os balanceadores de carga de gateway permitem que você implante, escale e gerencie dispositivos virtuais, como firewalls, sistemas de detecção e prevenção de intrusões e sistemas de inspeção profunda de pacotes. Eles combinam um gateway de rede transparente (ou seja, um único ponto de entrada e saída para todo o tráfego) e distribui o tráfego enquanto escala os dispositivos virtuais segundo a demanda.

Um balanceador de carga de gateway opera na terceira camada do modelo Open Systems Interconnection (OSI), a camada de rede. Ele escuta todos os pacotes IP em todas as portas e encaminha o tráfego para o grupo de destino especificado na regra do listener. Ele mantém a perdurabilidade dos fluxos para um dispositivo de destino específico usando 5 tuplas (para fluxos TCP/UDP) ou 3 tuplas (para fluxos não TCP/UDP). O Gateway Load Balancer e suas instâncias de dispositivos virtuais registradas trocam tráfego de aplicações usando o protocolo [GENEVE](#) na porta 6081.

Os balanceadores de carga de gateway usam endpoints do balanceador de carga de gateway para trocar tráfego com segurança através dos limites da VPC. Um endpoint do balanceador de carga de gateway é um endpoint da VPC que fornece conectividade privada entre dispositivos virtuais na VPC do provedor de serviços e servidores de aplicações na VPC do consumidor de serviços. Implante o

balanceador de carga de gateway na mesma VPC dos dispositivos virtuais. Registre os dispositivos virtuais em um grupo de destino para o balanceador de carga de gateway.

O tráfego de e para um endpoint do Gateway Load Balancer é configurado usando tabelas de rotas. O tráfego flui da VPC do consumidor de serviços pelo endpoint do Gateway Load Balancer para o Gateway Load Balancer na VPC do provedor de serviços e, em seguida, retorna à VPC do consumidor do serviço. Você deve criar o endpoint do Gateway Load Balancer e os servidores de aplicações em sub-redes diferentes. Isso permite configurar o endpoint do Gateway Load Balancer como o próximo salto na tabela de rotas para a sub-rede da aplicação.

Para obter mais informações, consulte [Acessar dispositivos virtuais pelo AWS PrivateLink](#) no Guia do AWS PrivateLink.

Fornecedores de dispositivos

Você é responsável por escolher e qualificar o software dos fornecedores de dispositivos. O software do dispositivo é o responsável pela tarefa de inspecionar ou modificar o tráfego do balanceador de carga. Os fornecedores de dispositivos listados como [Parceiros do Elastic Load Balancing](#) integraram e qualificaram seu software de dispositivos com a AWS. Você pode confiar mais no software dos dispositivos dos fornecedores desta lista. No entanto, a AWS não garante a segurança ou a confiabilidade do software desses fornecedores.

Conceitos básicos

Para criar um Gateway Load Balancer usando o AWS Management Console, consulte [Conceitos básicos](#). Para criar um Gateway Load Balancer usando o AWS Command Line Interface, consulte [Conceitos básicos do uso da CLI](#).

Preços

Com o load balancer, você paga somente pelo que utilizar. Para obter mais informações, consulte [Preço do Elastic Load Balancing](#).

Como começar a usar Gateway Load Balancers

Os Gateway Load Balancers facilitam a implementação, a escala e o gerenciamento de dispositivos virtuais de terceiros, como dispositivos de segurança.

Neste tutorial, implementaremos um sistema de inspeção usando um Gateway Load Balancer e um endpoint de Gateway Load Balancer.

Índice

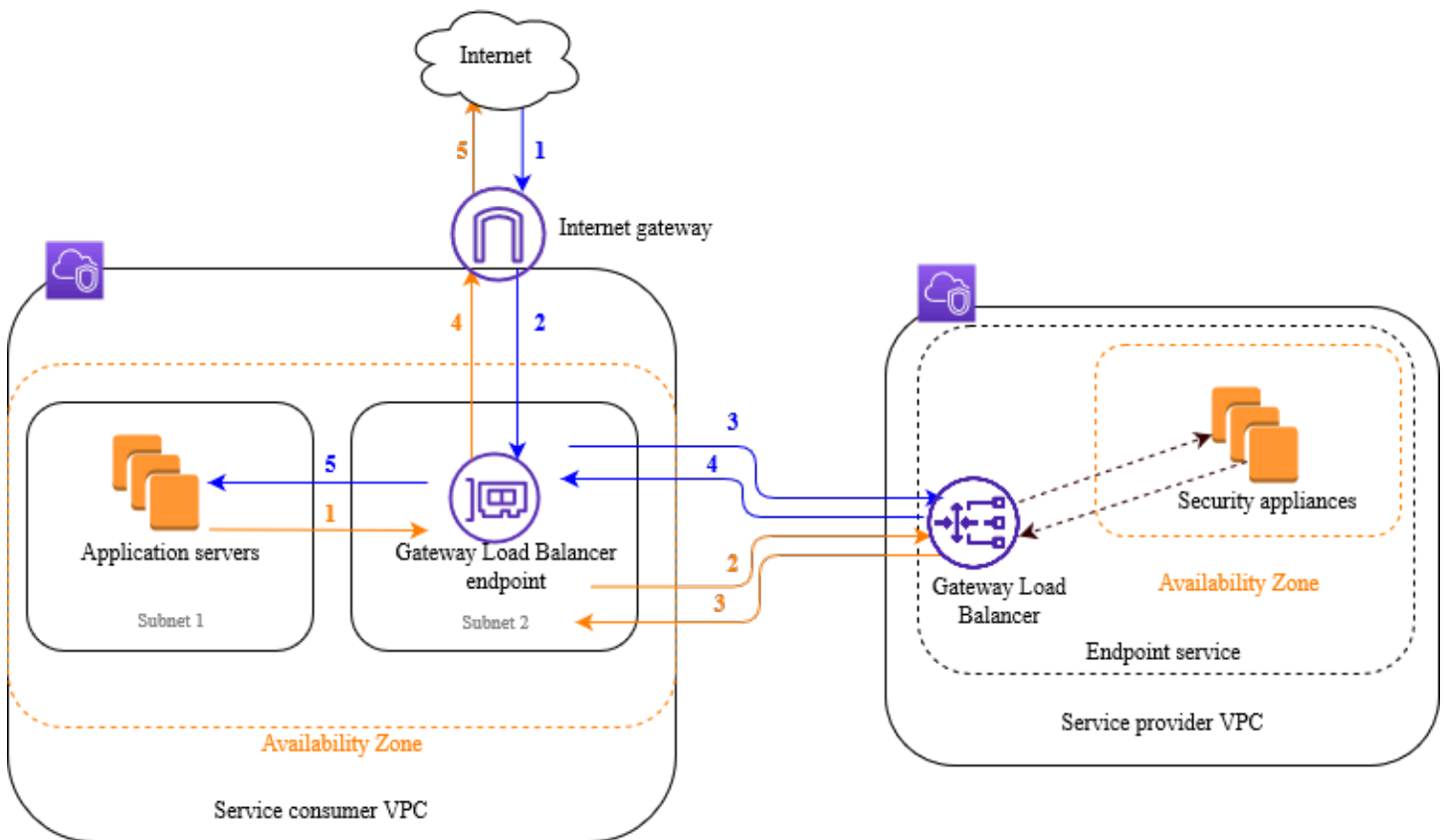
- [Visão geral](#)
- [Pré-requisitos](#)
- [Etapa 1: Crie um Gateway Load Balancer](#)
- [Etapa 2: Criar um serviço de endpoint do Gateway Load Balancer](#)
- [Etapa 3: Criar um endpoint do Gateway Load Balancer](#)
- [Etapa 4: Configurar o roteamento](#)

Visão geral

Um endpoint do Gateway Load Balancer é um endpoint da VPC que fornece conectividade privada entre dispositivos virtuais na VPC do provedor de serviços e servidores de aplicações na VPC do consumidor de serviços. O Gateway Load Balancer é implementado na mesma VPC dos dispositivos virtuais. Esses dispositivos são registrados como um grupo de destino para o Gateway Load Balancer.

Os servidores de aplicações são executados em uma sub-rede (sub-rede de destino) na VPC do consumidor de serviços, enquanto o endpoint do Gateway Load Balancer está em outra sub-rede da mesma VPC. Todo o tráfego que entra na VPC do consumidor do serviço pelo gateway da Internet é encaminhado primeiro ao endpoint do Gateway Load Balancer antes de ser encaminhado à sub-rede de destino.

Da mesma forma, todo o tráfego que sai dos servidores da aplicação (sub-rede de destino) é encaminhado primeiro ao endpoint do Gateway Load Balancer antes de ser encaminhado à Internet. O diagrama de rede a seguir é uma representação visual de como um endpoint do Gateway Load Balancer é usado para acessar um serviço de endpoint.



Os itens numerados a seguir destacam e explicam os elementos mostrados na imagem anterior.

Tráfego da Internet para a aplicação (setas azuis):

1. O tráfego entra na VPC do consumidor do serviço pelo gateway da Internet.
2. O tráfego é enviado ao endpoint do Gateway Load Balancer, como resultado de um roteamento de entrada.
3. O tráfego é enviado ao Gateway Load Balancer, que distribui o tráfego para um dos dispositivos de segurança.
4. O tráfego é reencaminhado ao endpoint do Gateway Load Balancer após a inspeção pelo dispositivo de segurança.
5. O tráfego é enviado aos servidores de aplicação (sub-rede de destino).

Tráfego da aplicação para a Internet (setas laranjas):

1. O tráfego é enviado ao endpoint do Gateway Load Balancer como resultado da rota padrão configurada na sub-rede do servidor de aplicação.

2. O tráfego é enviado ao Gateway Load Balancer, que distribui o tráfego para um dos dispositivos de segurança.
3. O tráfego é reencaminhado ao endpoint do Gateway Load Balancer após a inspeção pelo dispositivo de segurança.
4. O tráfego é enviado ao gateway da Internet com base na configuração da tabela de rotas.
5. O tráfego é reencaminhado à Internet.

Roteamento

A tabela de rotas do gateway da Internet deve conter entrada que roteia o tráfego destinado aos servidores de aplicações ao endpoint do Gateway Load Balancer. Para especificar o endpoint do Gateway Load Balancer, use o ID do endpoint da VPC. O exemplo a seguir mostra as rotas de uma configuração dualstack.

Destination (Destino)	Destino
<i>CIDR IPv4 da VPC</i>	Local
<i>CIDR IPv6 da VPC</i>	Local
<i>CIDR IPv4 da sub-rede 1</i>	<i>vpc-endpoint-id</i>
<i>CIDR IPv6 da sub-rede 1</i>	<i>vpc-endpoint-id</i>

A tabela de rotas para a sub-rede com os servidores de aplicações deve conter entradas que roteiem todo o tráfego dos servidores de aplicações ao endpoint do Gateway Load Balancer.

Destination (Destino)	Destino
<i>CIDR IPv4 da VPC</i>	Local
<i>CIDR IPv6 da VPC</i>	Local
0.0.0.0/0	<i>vpc-endpoint-id</i>
::/0	<i>vpc-endpoint-id</i>

A tabela de rotas para a sub-rede com o endpoint do Gateway Load Balancer deve rotear o tráfego que retorna da inspeção ao destino final. Para o tráfego proveniente da Internet, a rota local garante que o tráfego chegará aos servidores de aplicações. Para o tráfego proveniente dos servidores de aplicações, adicione entradas que roteiam todo o tráfego ao gateway da Internet.

Destination (Destino)	Destino
<i>CIDR IPv4 da VPC</i>	Local
<i>CIDR IPv6 da VPC</i>	Local
0.0.0.0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

Pré-requisitos

- Certifique-se de que a VPC consumidora de serviços tenha pelo menos duas sub-redes para cada zona de disponibilidade que contém servidores de aplicativos. Uma sub-rede é destinada aos servidores da aplicação, e a outra é destinada ao endpoint do Gateway Load Balancer.
- O Gateway Load Balancer e os destinos podem estar na mesma sub-rede.
- Você não pode usar uma sub-rede compartilhada de outra conta para implantar o Gateway Load Balancer.
- Inicie pelo menos uma instância do dispositivo de segurança em cada sub-rede do dispositivo de segurança na VPC do provedor de serviços. Os grupos de segurança para essas instâncias devem permitir tráfego UDP na porta 6081.

Etapa 1: Crie um Gateway Load Balancer

Use o procedimento a seguir para criar seu balanceador de carga, receptor e grupo de destino.

Para criar seu balanceador de carga, receptor e grupo de destino

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em Load Balancing, selecione Load Balancers.
3. Selecione Criar um balanceador de carga.

4. Em Gateway 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.
 - b. No Tipo de endereço IP, selecione IPv4 para oferecer suporte somente aos endereços IPv4 ou Dualstack para oferecer suporte aos endereços IPv4 e IPv6.
6. Mapeamento de rede
 - a. Para VPC, selecione a VPC provedora de serviços.
 - b. Para Mapeamentos, selecione todas as zonas de disponibilidade nas quais você iniciou as instâncias do dispositivo de segurança e uma sub-rede por zona de disponibilidade.
7. Roteamento de receptores de IP
 - a. Em Ação padrão, selecione um grupo de destino existente para receber tráfego. Esse grupo de destino deve usar o protocolo GENEVE.

Se você não tiver um grupo de destino, escolha Criar grupo de destino, que abre uma nova guia no seu navegador. Escolha um tipo de destino, insira um nome para o grupo de destino e mantenha o protocolo GENEVE. Selecione a VPC com suas instâncias do dispositivo de segurança. Modifique as configurações da verificação de integridade conforme necessário e adicione as tags necessárias. Escolha Next (Próximo). Você pode registrar suas instâncias do dispositivo de segurança com o grupo de destino agora ou depois de concluir este procedimento. Escolha Criar grupo de destino e, em seguida, retorne à guia anterior do navegador.
 - b. (Opcional) Expanda as Tags do receptor e adicione as tags necessárias.
8. (Opcional) Expanda as Tags do balanceador de carga e adicione as tags necessárias.
9. Selecione Criar um balanceador de carga.

Etapa 2: Criar um serviço de endpoint do Gateway Load Balancer

Use o seguinte procedimento para criar um serviço de endpoint usando um Gateway Load Balancer.

Para criar um serviço de endpoint do Gateway Load Balancer

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.

2. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
3. Escolha Criar serviço de endpoint e proceda da seguinte maneira:
 - a. Em Load balancer type (Tipo de load balancer), escolha Gateway.
 - b. Em Available load balancers (Balanceadores de carga disponíveis), selecione seu Gateway Load Balancer.
 - c. Em Exigir aceitação para o endpoint, selecione Aceitação obrigatória para aceitar as solicitações de conexão ao serviço manualmente. Caso contrário, elas serão aceitas automaticamente.
 - d. Em Supported IP address types (Tipos de endereço IP compatíveis), siga um destes procedimentos:
 - Selecionar IPv4: habilite o serviço de endpoint para aceitar solicitações IPv4.
 - Selecionar IPv6: habilite o serviço de endpoint para aceitar solicitações IPv6.
 - Selecionar IPv4 e IPv6: habilite o serviço de endpoint para aceitar solicitações IPv4 e IPv6.
 - e. (Opcional) Para adicionar uma etiqueta, escolha Add new tag (Adicionar nova etiqueta) e insira a chave e o valor da etiqueta.
 - f. Escolha Create (Criar). Você precisará do nome do serviço para criar o endpoint.
4. Selecione o novo serviço de endpoint e escolha Ações, Permitir entidades principais. Insira os ARNs dos consumidores de serviço que são permitidos para criar um endpoint para seu serviço. Um consumidor de serviço pode ser um usuário, perfil do IAM ou Conta da AWS. Escolha Allow principals (Permitir principais).

Etapa 3: Criar um endpoint do Gateway Load Balancer

Use o seguinte procedimento para criar um endpoint do Gateway Load Balancer que se conecte ao serviço de endpoint do Gateway Load Balancer. Endpoints do Gateway Load Balancer são zonais. Recomendamos que você crie um endpoint do Gateway Load Balancer por zona. Para obter mais informações, consulte [Acessar dispositivos virtuais pelo AWS PrivateLink](#) no Guia do AWS PrivateLink.

Para criar um endpoint do Gateway Load Balancer

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.

2. No painel de navegação, escolha Endpoints.
3. Escolha Criar endpoint e proceda da seguinte maneira:
 - a. Em Service category (Categoria de serviço), escolha Other endpoint services (Outros serviços de endpoint).
 - b. Em Nome do serviço, insira o nome do serviço e escolha Verificar serviço.
 - c. Para VPC, selecione a VPC consumidora de serviços.
 - d. Para Sub-redes, selecione uma sub-rede para o endpoint do Gateway Load Balancer.
 - e. Em IP address type (Tipo de endereço IP), escolha uma das seguintes opções:
 - IPv4: atribua endereços IPv4 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4.
 - IPv6: atribua endereços IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas forem sub-redes IPv6 apenas.
 - Dualstack: atribua endereços IPv4 e IPv6 às interfaces de rede de endpoint. Só haverá suporte para esta opção se todas as sub-redes selecionadas tiverem intervalos de endereços IPv4 e IPv6.
 - f. (Opcional) Para adicionar uma etiqueta, escolha Add new tag (Adicionar nova etiqueta) e insira a chave e o valor da etiqueta.
 - g. Escolha Criar endpoint. O status inicial é `pending acceptance`.

Para aceitar a solicitação de conexão do endpoint, use este procedimento.

1. No painel de navegação, escolha Endpoint Services (Serviços do endpoint).
2. Selecione o serviço de endpoint.
3. Na guia Endpoint connections (Conexões de endpoint), selecione a conexão de endpoint.
4. Para aceitar a solicitação de conexão, escolha Actions (Ações), Accept endpoint connection request (Aceitar solicitação de conexão de endpoint). Quando a confirmação for solicitada, insira **accept** e escolha Accept (Aceitar).

Etapa 4: Configurar o roteamento

Configure as tabelas de rotas para a VPC do consumidor de serviço conforme a seguir. Isso permite que os dispositivos de segurança realizem a inspeção de segurança do tráfego de entrada destinado aos servidores de aplicações.

Para configurar o roteamento

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Route tables (Tabelas de rotas).
3. Selecione a tabela de rotas do gateway da Internet e faça o seguinte:
 - a. Selecione Actions (Ações), Edit routes (Editar rotas).
 - b. Escolha Add route (Adicionar rota). Em Destination (Destino), insira o bloco CIDR IPv4 da sub-rede para os servidores de aplicações. Em Target (Destino), selecione o endpoint da VPC.
 - c. Se você oferece suporte a IPv6, escolha Add route (Adicionar rota). Em Destination (Destino), insira o bloco CIDR IPv6 da sub-rede para os servidores de aplicações. Em Target (Destino), selecione o endpoint da VPC.
 - d. Escolha Save changes (Salvar alterações).
4. Selecione a tabela de rotas para a sub-rede com os servidores de aplicações e faça o seguinte:
 - a. Selecione Actions (Ações), Edit routes (Editar rotas).
 - b. Escolha Add route (Adicionar rota). Em Destination, insira **0.0.0.0/0**. Em Target (Destino), selecione o endpoint da VPC.
 - c. Se você oferece suporte a IPv6, escolha Add route (Adicionar rota). Em Destination, insira **::/0**. Em Target (Destino), selecione o endpoint da VPC.
 - d. Escolha Save changes (Salvar alterações).
5. Selecione a tabela de rotas para a sub-rede com o endpoint do Gateway Load Balancer e faça o seguinte:
 - a. Selecione Actions (Ações), Edit routes (Editar rotas).
 - b. Escolha Add route (Adicionar rota). Em Destination, insira **0.0.0.0/0**. Em Target (Destino), selecione o gateway da Internet.
 - c. Se você oferece suporte a IPv6, escolha Add route (Adicionar rota). Em Destination, insira **::/0**. Em Target (Destino), selecione o gateway da Internet.

- d. Escolha Save changes (Salvar alterações).

Saiba como começar a usar Gateway Load Balancers com a AWS CLI

Os Gateway Load Balancers facilitam a implementação, a escala e o gerenciamento de dispositivos virtuais de terceiros, como dispositivos de segurança.

Neste tutorial, implementaremos um sistema de inspeção usando um Gateway Load Balancer e um endpoint de Gateway Load Balancer.

Índice

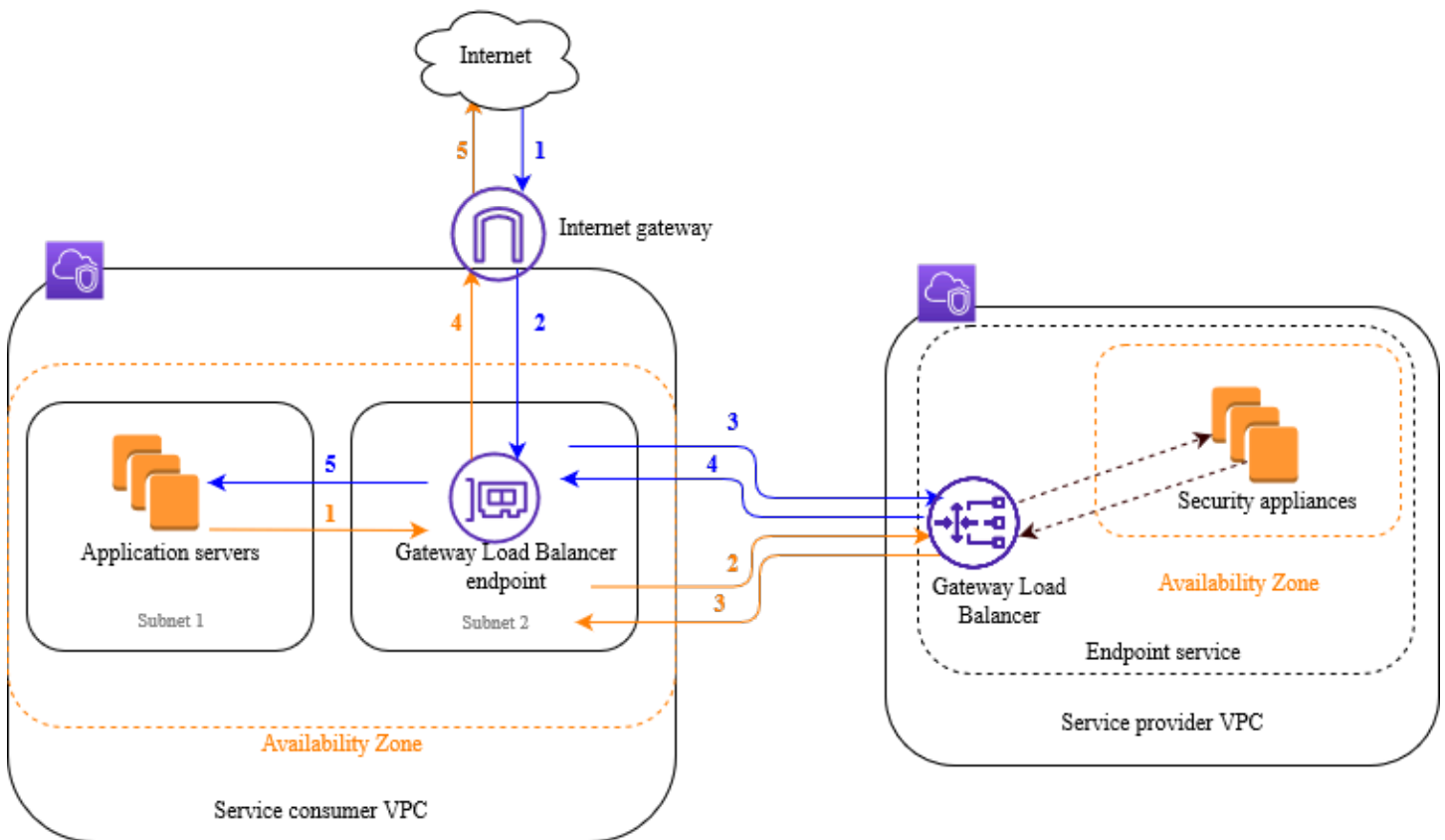
- [Visão geral](#)
- [Pré-requisitos](#)
- [Etapa 1: Criar um Gateway Load Balancer e registrar destinos](#)
- [Etapa 2: Criar um endpoint do Gateway Load Balancer](#)
- [Etapa 3: configurar o roteamento](#)

Visão geral

Um endpoint do Gateway Load Balancer é um endpoint da VPC que fornece conectividade privada entre dispositivos virtuais na VPC do provedor de serviços e servidores de aplicações na VPC do consumidor de serviços. O Gateway Load Balancer é implementado na mesma VPC dos dispositivos virtuais. Esses dispositivos são registrados como um grupo de destino para o Gateway Load Balancer.

Os servidores de aplicações são executados em uma sub-rede (sub-rede de destino) na VPC do consumidor de serviços, enquanto o endpoint do Gateway Load Balancer está em outra sub-rede da mesma VPC. Todo o tráfego que entra na VPC do consumidor do serviço pelo gateway da Internet é encaminhado primeiro ao endpoint do Gateway Load Balancer antes de ser encaminhado à sub-rede de destino.

Da mesma forma, todo o tráfego que sai dos servidores da aplicação (sub-rede de destino) é encaminhado primeiro ao endpoint do Gateway Load Balancer antes de ser encaminhado à Internet. O diagrama de rede a seguir é uma representação visual de como um endpoint do Gateway Load Balancer é usado para acessar um serviço de endpoint.



Os itens numerados a seguir destacam e explicam os elementos mostrados na imagem anterior.

Tráfego da Internet para a aplicação (setas azuis):

1. O tráfego entra na VPC do consumidor do serviço pelo gateway da Internet.
2. O tráfego é enviado ao endpoint do Gateway Load Balancer, como resultado de um roteamento de entrada.
3. O tráfego é enviado ao Gateway Load Balancer, que distribui o tráfego para um dos dispositivos de segurança.
4. O tráfego é reencaminhado ao endpoint do Gateway Load Balancer após a inspeção pelo dispositivo de segurança.
5. O tráfego é enviado aos servidores de aplicação (sub-rede de destino).

Tráfego da aplicação para a Internet (setas laranjas):

1. O tráfego é enviado ao endpoint do Gateway Load Balancer como resultado da rota padrão configurada na sub-rede do servidor de aplicação.

2. O tráfego é enviado ao Gateway Load Balancer, que distribui o tráfego para um dos dispositivos de segurança.
3. O tráfego é reencaminhado ao endpoint do Gateway Load Balancer após a inspeção pelo dispositivo de segurança.
4. O tráfego é enviado ao gateway da Internet com base na configuração da tabela de rotas.
5. O tráfego é reencaminhado à Internet.

Roteamento

A tabela de rotas do gateway da Internet deve conter entrada que roteia o tráfego destinado aos servidores de aplicações ao endpoint do Gateway Load Balancer. Para especificar o endpoint do Gateway Load Balancer, use o ID do endpoint da VPC. O exemplo a seguir mostra as rotas de uma configuração dualstack.

Destination (Destino)	Destino
<i>CIDR IPv4 da VPC</i>	Local
<i>CIDR IPv6 da VPC</i>	Local
<i>CIDR IPv4 da sub-rede 1</i>	<i>vpc-endpoint-id</i>
<i>CIDR IPv6 da sub-rede 1</i>	<i>vpc-endpoint-id</i>

A tabela de rotas para a sub-rede com os servidores de aplicações deve conter entradas que roteiem todo o tráfego dos servidores de aplicações ao endpoint do Gateway Load Balancer.

Destination (Destino)	Destino
<i>CIDR IPv4 da VPC</i>	Local
<i>CIDR IPv6 da VPC</i>	Local
0.0.0.0/0	<i>vpc-endpoint-id</i>
::/0	<i>vpc-endpoint-id</i>

A tabela de rotas para a sub-rede com o endpoint do Gateway Load Balancer deve rotear o tráfego que retorna da inspeção ao destino final. Para o tráfego proveniente da Internet, a rota local garante que o tráfego chegará aos servidores de aplicações. Para o tráfego proveniente dos servidores de aplicações, adicione entradas que roteiam todo o tráfego ao gateway da Internet.

Destination (Destino)	Destino
<i>CIDR IPv4 da VPC</i>	Local
<i>CIDR IPv6 da VPC</i>	Local
0.0.0.0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

Pré-requisitos

- Instale a AWS CLI ou atualize para a versão atual da AWS CLI se você está usando uma versão que não é compatível com Gateway Load Balancers. Para obter mais informações, consulte [Instalar a AWS Command Line Interface](#) no Guia do usuário da AWS Command Line Interface.
- Certifique-se de que a VPC consumidora de serviços tenha pelo menos duas sub-redes para cada zona de disponibilidade que contém servidores de aplicativos. Uma sub-rede é destinada aos servidores da aplicação, e a outra é destinada ao endpoint do Gateway Load Balancer.
- Certifique-se de que a VPC provedora de serviços tenha pelo menos duas sub-redes para cada zona de disponibilidade que contém instâncias de dispositivos de segurança. Uma sub-rede é destinada às instâncias, e a outra é destinada ao Gateway Load Balancer.
- Inicie pelo menos uma instância do dispositivo de segurança em cada sub-rede do dispositivo de segurança na VPC do provedor de serviços. Os grupos de segurança para essas instâncias devem permitir tráfego UDP na porta 6081.

Etapa 1: Criar um Gateway Load Balancer e registrar destinos

Use o procedimento a seguir para criar seu balanceador de carga, receptor e grupos de destino e para registrar suas instâncias do dispositivo de segurança como destinos.

Para criar um Gateway Load Balancer e registrar destinos

1. Use o comando [create-load-balancer](#) para criar um load balancer do tipo gateway. Você pode especificar uma sub-rede para cada zona de disponibilidade na qual lançou instâncias do dispositivo de segurança.

```
aws elbv2 create-load-balancer --name my-load-balancer --type gateway --  
subnets provider-subnet-id
```

O padrão é oferecer suporte somente a endereços IPv4. Adicione a opção `--ip-address-type dualstack` para oferecer suporte tanto para endereços IPv4 como IPv6.

O resultado inclui o nome do recurso da Amazon (ARN) do load balancer, com o seguinte formato.

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

2. Use o comando [create-target-group](#) para criar um grupo de destino, especificando a VPC provedora de serviços na qual você executou suas instâncias.

```
aws elbv2 create-target-group --name my-targets --protocol GENEVE --port 6081 --  
vpc-id provider-vpc-id
```

A saída inclui o ARN do grupo de destino, com o seguinte formato.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-  
targets/0123456789012345
```

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 seu balanceador de carga com uma regra padrão que encaminha solicitações ao seu grupo de destino.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --default-actions  
Type=forward,TargetGroupArn=targetgroup-arn
```

A saída contém o ARN do receptor, com o seguinte formato.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/gwy/my-load-balancer/1234567890123456/abc1234567890123
```

5. (Opcional) Você pode verificar a integridade do destinos registrados para o seu grupo de destino usando este comando [describe-target-health](#).

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

Etapa 2: Criar um endpoint do Gateway Load Balancer

Use o seguinte procedimento para criar um endpoint do Gateway Load Balancer. Endpoints do Gateway Load Balancer são zonais. Recomendamos que você crie um endpoint do Gateway Load Balancer por zona. Para obter mais informações, consulte [Acessar dispositivos virtuais por meio de AWS PrivateLink](#).

Para criar um endpoint do Gateway Load Balancer

1. Use o comando [create-vpc-endpoint-service-configuration](#) para criar uma configuração de serviço de endpoint usando seu Gateway Load Balancer.

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-arns loadbalancer-arn --no-acceptance-required
```

Adicione a opção `--supported-ip-address-types ipv4 ipv6` para oferecer suporte tanto para endereços IPv4 como IPv6.

A saída contém o ID do serviço (por exemplo, `vpce-svc-12345678901234567`) e o nome do serviço (por exemplo, `com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567`).

2. Use o comando [modify-vpc-endpoint-service-permissions](#) para permitir que consumidores de serviço criem um endpoint para seu serviço. Um consumidor de serviço pode ser um usuário, perfil do IAM ou Conta da AWS. O exemplo a seguir adiciona permissão para a Conta da AWS especificada.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-12345678901234567 --add-allowed-principals arn:aws:iam::123456789012:root
```

- Use o comando [create-vpc-endpoint](#) para criar um endpoint do Gateway Load Balancer para seu serviço.

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --service-name com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567 --vpc-id consumer-vpc-id --subnet-ids consumer-subnet-id
```

Adicione a opção `--ip-address-type dualstack` para oferecer suporte tanto para endereços IPv4 como IPv6.

A saída contém o ID do endpoint do Gateway Load Balancer (por exemplo, `vpce-01234567890abcdef`).

Etapa 3: configurar o roteamento

Configure as tabelas de rotas para a VPC do consumidor de serviço conforme a seguir. Isso permite que os dispositivos de segurança realizem a inspeção de segurança do tráfego de entrada destinado aos servidores de aplicações.

Para configurar o roteamento

- Use o comando [create-route](#) para adicionar entradas à tabela de rotas do gateway da Internet que roteia o tráfego destinado aos servidores de aplicações ao endpoint do Gateway Load Balancer.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv4 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

Adicione a seguinte rota se você oferece suporte à IPv6.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv6 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

- Use o comando [create-route](#) para adicionar uma entrada à tabela de rotas para a sub-rede com os servidores de aplicações que roteiem todo o tráfego dos servidores de aplicações ao endpoint do Gateway Load Balancer.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block  
0.0.0.0/0 --vpc-endpoint-id vpce-01234567890abcdef
```

Adicione a seguinte rota se você oferece suporte à IPv6.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block ::/0  
--vpc-endpoint-id vpce-01234567890abcdef
```

3. Use o comando [create-route](#) para adicionar uma entrada à tabela de rotas da sub-rede com o endpoint do Gateway Load Balancer que roteia todo o tráfego originado dos servidores de aplicações para o gateway da Internet.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block  
0.0.0.0/0 --gateway-id igw-01234567890abcdef
```

Adicione a seguinte rota se você oferece suporte à IPv6.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block ::/0 --  
gateway-id igw-01234567890abcdef
```

4. Repita o procedimento para cada tabela de rotas de sub-rede da aplicação em cada zona.

Balanceadores de carga de gateway

Use um Gateway Load Balancer para implantar e gerenciar uma frota de dispositivos virtuais compatíveis com o protocolo GENEVE.

Um Gateway Load Balancer opera na terceira camada do modelo Open Systems Interconnection (OSI). Ele escuta todos os pacotes de IP em todas as portas e encaminha o tráfego para o grupo de destino especificado na regra do receptor, usando o protocolo GENEVE na porta 6081.

Você pode adicionar ou remover destinos do seu load balancer conforme mudarem suas necessidades, sem perturbar o fluxo geral de solicitações. 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.

Conteúdos

- [Estado do load balancer](#)
- [Tipo de endereço IP](#)
- [Atributos do load balancer](#)
- [Zonas de disponibilidade](#)
- [A unidade de transmissão máxima \(MTU\) da rede](#)
- [Proteção contra exclusão](#)
- [Balanceamento de carga entre zonas](#)
- [Fluxos assimétricos](#)
- [Intervalo ocioso](#)
- [Criar um Gateway Load Balancer](#)
- [Tags para o Gateway Load Balancer](#)
- [Excluir um Gateway Load Balancer](#)

Estado do load balancer

O Gateway Load Balancer pode estar em um dos seguintes estados:

provisioning

O Gateway Load Balancer está sendo configurado.

active

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

failed

O Gateway Load Balancer não pôde ser configurado.

Tipo de endereço IP

Você pode definir os tipos de endereços IP que os servidores de aplicações podem usar para acessar seus Gateway Load Balancers. Veja a seguir os tipos de endereço IP compatíveis:

- `ipv4` — Somente o IPv4 é compatível.
- `dualstack` — IPv4 e IPv6 são compatíveis.

Considerações sobre o balanceador de carga dualstack

- A nuvem privada virtual (VPC) e as sub-redes especificadas para o load balancer devem ter blocos CIDR IPv6 associados.
- As tabelas de rotas para as sub-redes na VPC do consumidor de serviços devem rotear o tráfego IPv6 e as ACLs de rede para essas sub-redes devem permitir tráfego IPv6.
- Um Gateway Load Balancer encapsula o tráfego de clientes IPv4 e IPv6 com um cabeçalho IPv4 GENEVE e o envia para o dispositivo. O dispositivo encapsula o tráfego de clientes IPv4 e IPv6 com um cabeçalho IPv4 GENEVE e o envia de volta para o Gateway Load Balancer.

É possível definir o tipo de endereço IP ao criar o load balancer. É possível atualizá-lo a qualquer momento.

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, em LOAD BALANCING (BALANCEAMENTO DE CARGA), escolha Load balancers (Balanceadores de carga).
3. Selecione o load balancer.
4. Selecione Ações, Editar tipo de endereço IP.

5. No Tipo de endereço IP, selecione ipv4 para oferecer suporte somente aos endereços IPv4 ou dualstack para oferecer suporte aos endereços IPv4 e IPv6.
6. Escolha Salvar.

Para atualizar o tipo de endereço IP usando a AWS CLI

Use o comando [set-ip-address-type](#).

Atributos do load balancer

A seguir, veja os atributos do balanceador de carga para Gateway Load Balancers:

`deletion_protection.enabled`

Indica se a [proteção contra exclusão](#) está habilitada. O padrão é false.

`load_balancing.cross_zone.enabled`

Indica se o [balanceamento de carga entre zonas](#) está habilitado. O padrão é false.

Zonas de disponibilidade

Ao criar um Gateway Load Balancer, você habilita uma ou mais zonas de disponibilidade e especifica a sub-rede que corresponde a cada zona. Quando você habilita várias zonas de disponibilidade, isso garante que o balanceador de carga possa continuar roteando o tráfego mesmo que uma zona de disponibilidade fique indisponível. As sub-redes especificadas devem ter pelo menos 8 endereços IP disponíveis cada. As sub-redes não podem ser removidas após a criação do balanceador de carga. Para remover uma sub-rede, você deve criar um novo balanceador de carga.

A unidade de transmissão máxima (MTU) da rede

A unidade de transmissão máxima (MTU) é o tamanho do maior pacote de dados que pode ser transmitido pela rede. A interface MTU do Gateway Load Balancer oferece suporte a pacotes de até 8.500 bytes. Pacotes com tamanho superior a 8.500 bytes que chegam ao Gateway Load Balancer são descartados.

Um Gateway Load Balancer encapsula o tráfego IP com um cabeçalho GENEVE e o envia para o dispositivo. O processo de encapsulamento do GENEVE adiciona 64 bytes ao pacote original.

Portanto, para oferecer suporte a pacotes de até 8.500 bytes, a configuração de MTU do seu dispositivo deve oferecer suporte a pacotes de pelo menos 8.564 bytes.

Os Gateway Load Balancers não são compatíveis com fragmentação de IP. Além disso, os Gateway Load Balancers não geram a mensagem ICMP “Destino inacessível: fragmentação necessária e conjunto de DF”. Por isso, não há suporte ao Path MTU Discovery (PMTUD).

Proteção contra exclusão

Para evitar que seu Gateway Load Balancer seja excluído acidentalmente, você pode ativar a proteção contra exclusão. Por padrão, a proteção contra exclusão fica desabilitada.

Se você ativar a proteção contra exclusão para o Gateway Load Balancer, deverá desativá-la antes de excluí-lo.

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, em LOAD BALANCING, escolha Load balancers.
3. Selecione o Gateway Load Balancer.
4. Escolha Ações, Editar atributos.
5. Na página Edit load balancer attributes (Editar atributos do load balancer), selecione Enable (Habilitar) em Delete Protection (Proteção contra a exclusão) e escolha Save (Salvar).

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, em LOAD BALANCING, escolha Load balancers.
3. Selecione o Gateway Load Balancer.
4. Escolha Ações, Editar atributos.
5. Na página Editar atributos do balanceador de carga, desmarque Habilitar em Proteção contra a exclusão e escolha Salvar.

Para habilitar ou desabilitar a proteção contra exclusão usando a AWS CLI

Use o [modify-load-balancer-attributes](#) comando com o `deletion_protection.enabled` atributo.

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 habilitar o balanceamento de carga entre zonas, cada nó do Gateway Load Balancer distribuirá o tráfego aos destinos registrados em todas as zonas de disponibilidade habilitadas. Para mais informações, consulte [Balanceamento de carga entre zonas](#) no Manual do usuário do Elastic Load Balancing.

Para ativar o balanceamento de carga entre zonas 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, escolha Load balancers.
3. Selecione o Gateway Load Balancer.
4. Escolha Ações, Editar atributos.
5. Na página Editar atributos do balanceador de carga, selecione Habilitar em Balanceamento de carga entre zonas e selecione Salvar.

Para ativar o balanceamento de carga entre zonas usando a AWS CLI

Use o [modify-load-balancer-attributes](#) comando com o `load_balancing.cross_zone.enabled` atributo.

Fluxos assimétricos

Os Gateway Load Balancers oferecem suporte a fluxos assimétricos quando o balanceador de carga processa o pacote de fluxo inicial e o pacote de fluxo de resposta não é roteado pelo balanceador de carga. O roteamento assimétrico não é recomendado, pois pode resultar na redução do desempenho da rede. Os Gateway Load Balancers não oferecem suporte a fluxos assimétricos quando o balanceador de carga não processa o pacote de fluxo inicial, mas o pacote de fluxo de resposta é roteado pelo balanceador de carga.

Intervalo ocioso

Os Gateway Load Balancers oferecem suporte ao tempo limite de inatividade para fluxos TCP e não TCP.

- Para fluxos TCP, o valor do tempo limite ocioso é 350 segundos.

- Para fluxos não TCP, o valor do tempo limite ocioso é 120 segundos.

Observação: os valores de tempo limite ocioso dos Gateway Load Balancers são estáticos e não podem ser alterados.

Criar um Gateway Load Balancer

Um Gateway Load Balancer leva solicitações de clientes e as distribui em destinos em um grupo de destino, como instâncias EC2.

Para criar um Gateway Load Balancer usando o AWS Management Console, execute as tarefas a seguir.

Tarefas

- [Pré-requisitos](#)
- [Criar o balanceador de carga](#)
- [Próximas etapas importantes](#)

Como alternativa, para criar um Gateway Load Balancer usando o AWS CLI, consulte [Conceitos básicos do uso da CLI](#).

Pré-requisitos

Antes de começar, certifique-se de que a nuvem privada virtual (VPC) do Gateway Load Balancer tenha pelo menos uma sub-rede pública em cada zona de disponibilidade onde você tem destinos.

Criar o balanceador de carga

Use o procedimento a seguir para criar seu Gateway Load Balancer. Forneça algumas informações básicas de configuração do seu balanceador de carga, como nome e tipo de endereço IP. Em seguida, forneça informações sobre sua rede e o receptor que roteia o tráfego para seus grupos de destino. Os Gateway Load Balancers exigem grupos de destino que usem o protocolo GENEVE.

Para criar o balanceador de carga e o receptor

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 Criar um balanceador de carga.

4. Em Gateway 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-g1b** O nome do Gateway Load Balancer deve ser exclusivo no conjunto de balanceadores de carga da região. Os nomes podem ter no máximo 32 caracteres, podem conter somente caracteres alfanuméricos e hifens e não devem começar ou terminar com um hífen.
 - b. No Tipo de endereço IP, selecione IPv4 para oferecer suporte somente aos endereços IPv4 ou Dualstack para oferecer suporte aos endereços IPv4 e IPv6.
6. Mapeamento de rede
 - a. Para VPC, selecione a VPC provedora de serviços.
 - b. Para Mapeamentos, selecione todas as zonas de disponibilidade nas quais você iniciou as instâncias do dispositivo de segurança e as sub-redes públicas correspondentes.
7. Roteamento de receptores de IP
 - a. Em Ação padrão, selecione um grupo de destino para receber tráfego. Se você não tiver um grupo de destino, escolha Criar grupo de destino. Para obter mais informações, consulte [Criar um grupo de destino](#).
 - b. (Opcional) Expanda as Tags do receptor e adicione as tags necessárias.
8. (Opcional) Expanda as Tags do balanceador de carga e adicione as tags necessárias.
9. Revise sua configuração e escolha Criar um balanceador de carga.

Próximas etapas importantes

Depois de criar seu balanceador de carga, verifique se suas instâncias do EC2 passaram pela verificação de integridade inicial. Para testar o balanceador de carga, é necessário criar um endpoint do Gateway Load Balancer e atualizar a tabela de rotas para tornar o endpoint do Gateway Load Balancer o próximo salto. Essas configurações são definidas no console do Amazon VPC. Para mais informações, consulte o tutorial [Conceitos básicos](#).

Tags para o Gateway Load Balancer

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

Você pode adicionar várias tags para cada load balancer. As chaves de tag devem ser exclusivas de cada Gateway 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 Gateway 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 prefixo `aws:` no nome nem no valor de suas tags, pois ele é reservado para uso da AWS. 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 Gateway 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, escolha Load balancers.
3. Selecione o Gateway Load Balancer.
4. Escolha Tags, Adicionar/Editar tags e, em seguida, execute uma ou mais das ações a seguir:
 - a. Para atualizar uma tag, edite os valores de Chave e Valor.
 - b. Para adicionar uma nova tag, escolha Criar tag. Digite um valor para Chave de tag e Valor.
 - c. Para excluir uma tag, escolha o ícone de exclusão (X) ao lado da tag.
5. Ao concluir a atualização de tags, selecione Salvar.

Para atualizar as tags para um Gateway Load Balancer usando a AWS CLI

Use os comandos [add-tags](#) e [remove-tags](#).

Excluir um Gateway Load Balancer

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

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

A exclusão de um Gateway Load Balancer também exclui seus receptores. A exclusão de um Gateway 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 Gateway 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, escolha Load balancers.
3. Selecione o Gateway Load Balancer.
4. Escolha Ações, Excluir.
5. Quando a confirmação for solicitada, escolha Sim, excluir.

Para excluir um Gateway Load Balancer usando a AWS CLI

Use o comando [delete-load-balancer](#).

Receptores para seus Gateway Load Balancers

Quando você criar seu Gateway Load Balancer, você adiciona um receptor. Um listener é um processo que verifica se há solicitações de conexão.

Os receptores dos Gateway Load Balancers escutam todos os pacotes de IP em todas as portas. Não é possível especificar um protocolo ou uma porta ao criar um receptor para um Gateway Load Balancer.

Quando você cria um listener, você especifica uma regra para rotear as solicitações. Essa regra encaminha as solicitações para o grupo de destino especificado. Você pode atualizar a regra do receptor para encaminhar solicitações para um grupo de destino diferente.

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, em LOAD BALANCING, escolha Load balancers.
3. Selecione o load balancer e escolha Listeners.
4. Escolha Editar receptor.
5. Em Encaminhando para um grupo de destino, selecione um grupo de destino.
6. Escolha Save (Salvar).

Para atualizar o listener usando a AWS CLI

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

Grupos de destino para seus Gateway 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 receptor. Você pode criar grupos de destino diferentes para tipos de solicitações diferentes.

Você define as configurações de verificação de integridade para seu Gateway 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 receptor, o Gateway 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 Gateway Load Balancer. O Gateway Load Balancer roteia solicitações para os destinos registrados que são íntegros. Para obter mais informações, consulte [Verificações de integridade para os grupos de destino](#).

Índice

- [Configuração de roteamento](#)
- [Target type](#)
- [Destinos registrados](#)
- [Atributos do grupo de destino](#)
- [Atraso do cancelamento do registro](#)
- [Failover de destino](#)
- [Aderência do fluxo](#)
- [Criar um grupo de destino para seu Gateway Load Balancer](#)
- [Verificações de integridade para os grupos de destino](#)
- [Registrar destinos com o grupo de destino](#)
- [Tags para o grupo de destino](#)
- [Excluir um grupo de destino](#)

Configuração de roteamento

Os grupos de destino para Gateway Load Balancers são compatíveis com os seguintes protocolos e portas:

- Protocolo: GENEVE
- Porta: 6081

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 seu tipo de destino.

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.

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.

Destinos registrados

O seu Gateway 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 Gateway Load Balancer. Você pode registrar cada destino com um ou mais grupos de destino.

Se a demanda aumentar, você pode registrar destinos adicionais com um ou mais grupos de destino, a fim de dar conta da demanda. O Gateway Load Balancer inicia o roteamento do tráfego para um destino recém-registrado assim que o processo de registro é concluído.

Se a demanda diminuir, ou se você precisar fazer manutenção nos seus destinos, você pode cancelar o registro dos destinos dos seus grupos de destino. Cancelar o registro de um destino o remove do seu grupo de destino, mas não afeta o destino de outra forma. O Gateway 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.

Atributos do grupo de destino

É possível usar os seguintes atributos com grupos de destino:

`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.

`stickiness.enabled`

Indica se a aderência de fluxo configurável está habilitada para o grupo de destino. Os valores possíveis são `true` ou `false`. O padrão é `false`. Quando o atributo é definido como `false`, `5_tuple` é usado.

`stickiness.type`

Indica o tipo de aderência de fluxo. Os valores possíveis para grupos de destino associados aos Gateway Load Balancers são:

- `source_ip_dest_ip`
- `source_ip_dest_ip_proto`

`target_failover.on_deregistration`

Indica como o Gateway Load Balancer trata os fluxos existentes quando um destino tem o registro cancelado. Os valores possíveis são `rebalance` e `no_rebalance`. O padrão é `no_rebalance`. Os dois atributos (`target_failover.on_deregistration` e `target_failover.on_unhealthy`) não podem ser definidos de forma independente. O valor definido para ambos os atributos deve ser o mesmo.

`target_failover.on_unhealthy`

Indica como o Gateway Load Balancer trata os fluxos existentes quando um destino não está íntegro. Os valores possíveis são `rebalance` e `no_rebalance`. O padrão é `no_rebalance`. Os dois atributos (`target_failover.on_deregistration` e `target_failover.on_unhealthy`) não podem ser definidos de forma independente. O valor definido para ambos os atributos deve ser o mesmo.

Atraso do cancelamento do registro

Quando você cancela o registro de um destino, o Gateway Load Balancer gerencia os fluxos para esse destino da seguinte forma:

Novos fluxos

O Gateway Load Balancer para de enviar novos fluxos.

Fluxos existentes

O Gateway Load Balancer manipula os fluxos existentes com base no protocolo:

- TCP: os fluxos existentes são fechados se ficarem ociosos por mais de 350 segundos.
- Outros protocolos: os fluxos existentes são fechados se ficarem ociosos por mais de 120 segundos.

Para ajudar a drenar os fluxos existentes, você pode habilitar o rebalanceamento de fluxo para seu grupo de destino. Para obter mais informações, consulte [the section called “Failover de destino”](#).

Um destino cancelado mostra que está `draining` até que o tempo limite expire. Depois que o tempo limite do cancelamento de registro expirar, o destino passa para um estado `unused`.

Para atualizar o valor de retardo de cancelamento do 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 página Detalhes do grupo, na seção Atributos, escolha Editar.
5. Na página Editar atributos, altere o valor do Atraso do cancelamento do registro conforme o necessário.
6. Escolha Save changes (Salvar alterações).

Para atualizar o valor de atraso de cancelamento do registro usando a AWS CLI

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

Failover de destino

Com o failover de destino, você especifica como o Gateway Load Balancer trata os fluxos de tráfego existentes após um destino tornar-se não íntegro ou quando o registro do destino é cancelado. Por padrão, o Gateway Load Balancer continua enviando fluxos existentes para o mesmo destino, mesmo que o destino tenha falhado ou tenha seu registro cancelado. Você pode gerenciar esses fluxos reformulando-os (`rebalance`) ou deixando-os no estado padrão (`no_rebalance`).

Sem rebalancear:

O Gateway Load Balancer continua enviando fluxos existentes para destinos com falha ou esgotados. No entanto, novos fluxos são enviados para destinos íntegros. Esse é o comportamento padrão.

Rebalancear:

O Gateway Load Balancer reformula os fluxos existentes e os envia para destinos íntegros após o tempo limite do atraso no cancelamento do registro.

Para destinos com registro cancelado, o tempo mínimo de failover dependerá do atraso no cancelamento do registro. O destino não é marcado como cancelado até que o atraso no cancelamento do registro seja concluído.

Para destinos não íntegros, o tempo mínimo de failover dependerá da configuração da verificação de integridade do grupo de destino (limite de tempos de intervalo). Esse é o tempo mínimo antes do qual um destino é sinalizado como não íntegro. Após esse período, o Gateway Load Balancer pode levar vários minutos devido ao tempo adicional de propagação e ao atraso na retransmissão de TCP antes de redirecionar novos fluxos para destinos íntegros.

Para atualizar o valor de destino de failover usando a nova experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na página Detalhes do grupo, na seção Atributos, escolha Editar.
5. Na página Editar atributos, altere o valor do Failover de destino conforme necessário.
6. Escolha Save changes (Salvar alterações).

Para atualizar o valor de destino de failover usando a AWS CLI

Use o comando [modify-target-group-attributes](#), com os seguintes pares de valores-chave:

- Key= `target_failover.on_deregistration` e Value= `no_rebalance` (padrão) ou `rebalance`
- Key= `target_failover.on_unhealthy` e Value= `no_rebalance` (padrão) ou `rebalance`

Note

Ambos os atributos (`target_failover.on_deregistration` e `target_failover.on_unhealthy`) devem ter o mesmo valor.

Aderência do fluxo

Por padrão, o Gateway Load Balancer mantém a aderência dos fluxos para um dispositivo de destino específico usando 5 tuplas (para fluxos TCP/UDP). Cinco tuplas incluem IP de origem, porta de origem, IP de destino, porta de destino e protocolo de transporte. Você pode usar o atributo de tipo

de aderência para modificar o padrão (5 tuplas) e escolher 3 tuplas (IP de origem, IP de destino e protocolo de transporte) ou 2 tuplas (IP de origem e IP de destino).

Considerações sobre a aderência do fluxo

- A aderência do fluxo é configurada e aplicada no nível do grupo de destino e se aplica a todo o tráfego que vai para o grupo de destino.
- A aderência de fluxo de 2 e 3 tuplas não é suportada quando o modo de dispositivo AWS Transit Gateway está ativado. Para usar o modo de dispositivo em seu AWS Transit Gateway, use a aderência de fluxo de 5 tuplas em seu Gateway Load Balancer
- A aderência de fluxo pode levar a uma distribuição desigual de conexões e de fluxos, o que pode afetar a disponibilidade dos destinos. É recomendável que você encerre ou drene todos os fluxos existentes antes de modificar o tipo de aderência do grupo de destino.

Para atualizar a aderência do fluxo 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 página Detalhes do grupo, na seção Atributos, escolha Editar.
5. Na página Editar atributos, altere o valor da Aderência do fluxo conforme necessário.
6. Escolha Save changes (Salvar alterações).

Para habilitar ou modificar a aderência do fluxo usando a AWS CLI

Use o comando [modify-target-group-attributes](#) com os atributos de grupo de destino `stickiness.enabled` e `stickiness.type`.

Criar um grupo de destino para seu Gateway Load Balancer

Você registra destinos para seu Gateway Load Balancer usando um grupo de destino.

Para rotear o tráfego aos destinos em um grupo de destino, crie um listener e especifique o grupo de destino em uma ação padrão para o listener. Para obter mais informações, consulte [Listeners](#).

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

New EC2 experience

Para criar um grupo de destino usando a nova experiência do EC2

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. Configuração básica
 - a. Para Escolher um tipo de destino, selecione Instâncias para especificar destinos por ID de instância ou selecione Endereços IP para especificar destinos por endereço IP.
 - b. Em Nome do grupo de destino, digite 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 hífens, e não deve iniciar nem terminar com hífen.
 - c. Verifique se o Protocolo é GENEVE e a porta é 6081. Nenhum outro protocolo ou porta é compatível.
 - d. Para VPC, selecione a nuvem privada virtual (VPC) com as instâncias do dispositivo de segurança para incluir em seu grupo de destino.
5. (Opcional) Nas Verificações de integridade, modifique as configurações padrão e avançadas conforme o necessário. Se as verificações de integridade excederem o número de Limite não íntegro, o balanceador de carga tirará o destino de serviço. Quando as verificações de integridade excederem o número de Limite íntegro, o balanceador de carga colocará o destino de volta em serviço. Para obter mais informações, consulte [Verificações de integridade para os grupos de destino](#).
6. (Opcional) Expanda Tags e adicione as tags de que você precisa.
7. Escolha Next (Próximo).
8. Para Registrar destinos, adicione um ou mais destinos da seguinte forma:
 - Se o tipo de destino for Instâncias, selecione uma ou mais instâncias, insira uma ou mais portas e escolha Incluir como pendente abaixo.

- Se o tipo de destino for Endereços IP, selecione a rede, insira o endereço IP e as portas e escolha Incluir como pendente abaixo.
9. Selecione Criar grupo de destino.

Old EC2 experience

Para criar um grupo de destino usando a antiga experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Selecione Criar grupo de destino.
4. Em Nome do grupo de destino, digite 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 hífens, e não deve iniciar nem terminar com hífen.
5. Para Protocolo, use GENEVE. Com o protocolo GENEVE, a porta deve ser 6081.
6. Para Target type (Tipo de destino), selecione instance para especificar destinos por ID de instância ou ip para especificar destinos por endereço IP.
7. Em VPC, selecione uma nuvem privada virtual (VPC).
8. (Opcional) Nas Health check settings (Configurações da verificação de integridade) e nas Advanced health check settings (Configurações avançadas da verificação de integridade), modifique as configurações padrão conforme o necessário. Escolha Create (Criar).
9. (Opcional) Adicione uma ou mais tags, da seguinte forma:
 - a. Selecione o grupo de destino recém-criado.
 - b. Selecione Tags, Add/Edit Tags (Adicionar/Editar tags).
 - c. Na página Add/Edit Tags (Adicionar/Editar tags), para cada tag que você adicionar, selecione Create Tag (Criar tag) e especifique a chave e o valor da tag. Ao concluir a inclusão de tags, selecione Save (Salvar).
10. (Opcional) Para adicionar destinos ao grupo de destino, consulte [Registrar destinos com o grupo de destino](#).

Para criar um grupo de destino usando a 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 Gateway 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.

O Gateway Load Balancer envia periodicamente uma solicitação para cada destino registrado para verificar seu status. Após cada verificação de integridade ser concluída, o Gateway Load Balancer fechará a conexão estabelecida para a verificação de integridade.

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 o número especificado de falhas `UnhealthyThresholdCountconsecutivas`, o Gateway Load Balancer desativará o alvo. Quando as verificações de integridade excedem o número especificado de sucessos `HealthyThresholdCountconsecutivos`, o Gateway Load Balancer coloca o alvo novamente em serviço.

Configuração	Descrição
<code>HealthCheckProtocol</code>	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 TCP.
<code>HealthCheckPort</code>	A porta que o Gateway Load Balancer usa ao executar verificações de integridade nos destinos. O intervalo é de 1 a 65535. O padrão é 80.
<code>HealthCheckPath</code>	[Verificações de integridade HTTP/HTTPS] O caminho da verificação de saúde que é o destino nos alvos das verificações de saúde. O padrão é /.
<code>HealthCheckTimeoutSeconds</code>	O tempo, em segundos, durante o qual ausência de resposta de um destino significa

Configuração	Descrição
	uma falha na verificação de integridade. O intervalo é de 2 a 120. O padrão é 5.
HealthCheckIntervalSeconds	<p>A quantia aproximada de tempo, em segundos, entre as verificações de integridade de um destino individual. O intervalo é de 5 a 300. O padrão é 10 segundos. Esse valor deve ser maior ou igual HealthCheckTimeoutSeconds.</p> <div data-bbox="829 611 1507 1157" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>As verificações de integridade para Gateway Load Balancers são distribuídas e usam um mecanismo de consenso para determinar a integridade do destino. Portanto, você deve esperar que os dispositivos de destino recebam várias verificações de integridade dentro do intervalo de tempo configurado.</p></div>
HealthyThresholdCount	O número de verificações de integridade bem-sucedidas consecutivas necessárias antes de considerar íntegro um destino não íntegro. O intervalo é de 2 a 10. O padrão é 5.
UnhealthyThresholdCount	O número de verificações de integridade consecutivas exigido antes considerar um destino não íntegro. O intervalo é de 2 a 10. O padrão é 2.
Matcher	[Verificações de integridade de HTTP/HTTPS] Os códigos HTTP a serem usados ao verificar uma resposta bem-sucedida de um destino. Esse valor deve ser entre 200–399.

Status de integridade do destino

Antes que o Gateway 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 receptor e garantir que a zona de disponibilidade do destino esteja habilitada para o Gateway Load Balancer.

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

Value	Descrição
<code>initial</code>	<p>O Gateway Load Balancer está no processo de registro do destino ou executando as verificações de integridade iniciais no destino.</p> <p>Códigos de motivo relacionados: <code>Elb.RegistrationInProgress</code> <code>Elb.InitialHealthChecking</code></p>
<code>healthy</code>	<p>O destino é íntegro.</p> <p>Códigos de motivo relacionados: nenhum</p>
<code>unhealthy</code>	<p>O destino não respondeu a uma verificação de integridade ou falhou em uma verificação de integridade.</p> <p>Código de motivo relacionado: <code>Target.FailedHealthChecks</code></p>
<code>unused</code>	<p>O destino não está registrado em um grupo de destino, o grupo de destino não é usado em uma regra do listener, o destino está em uma zona de disponibilidade desativada ou o destino está no estado parado ou encerrado.</p> <p>Códigos de motivo relacionados: <code>Target.NotRegistered</code> <code>Target.NotInUse</code> <code>Target.InvalidState</code> <code>Target.IpUnusable</code></p>

Value	Descrição
draining	O destino está cancelando o registro e está acontecendo drenagem da conexão. Código de motivo relacionado: <code>Target.DeregistrationInProgress</code>
unavailable	A integridade do destino não está disponível. Código de motivo relacionado: <code>Elb.InternalError</code>

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. Os códigos de motivo que comecem com `Elb` são originados no Gateway Load Balancer, e os códigos de motivo que comecem com `Target` são originados no destino.

Código do motivo	Descrição
<code>Elb.InitialHealthChecking</code>	Verificações de integridade iniciais em andamento
<code>Elb.InternalError</code>	As verificações de integridade falharam devido a um erro interno
<code>Elb.RegistrationInProgress</code>	O registro do destino está em andamento
<code>Target.DeregistrationInProgress</code>	O cancelamento do registro do destino está em andamento
<code>Target.FailedHealthChecks</code>	Verificações de integridade com falha
<code>Target.InvalidState</code>	O destino está no estado interrompido O destino está no estado encerrado O destino está no estado encerrado ou interrompido

Código do motivo	Descrição
	O destino está em um estado inválido
<code>Target.IpUnusable</code>	O endereço IP não pode ser usado como um destino, uma vez que está sendo usado por um load balancer.
<code>Target.NotInUse</code>	O grupo de destino não está configurado para receber tráfego do Gateway Load Balancer O destino está em uma zona de disponibilidade que não está habilitada para o Gateway Load Balancer
<code>Target.NotRegistered</code>	O destino não está registrado no grupo de destino

Cenários de falha do destino do Gateway Load Balancer

Fluxos existentes: por padrão, os fluxos existentes vão para o mesmo destino, a menos que o fluxo expire ou seja redefinido, independentemente da integridade e do status de registro do destino. Essa abordagem facilita a drenagem da conexão e acomoda firewalls de terceiros que às vezes não conseguem responder às verificações de integridade devido ao alto uso da CPU. Para obter mais informações, consulte [Target failover](#).

Novos fluxos: novos fluxos são enviados para um destino íntegro. Quando uma decisão de balanceamento de carga para um fluxo for tomada, o Gateway Load Balancer enviará o fluxo para o mesmo destino, mesmo que esse destino não seja mais íntegro ou que outros destinos fiquem íntegros.

Quando todos os destinos não estão íntegros, o Gateway Load Balancer escolhe um destino aleatoriamente e encaminha o tráfego para ele durante toda a vida útil do fluxo, até que ele seja reiniciado ou tenha atingido o tempo limite. Como o tráfego está sendo encaminhado para um destino não íntegro, o tráfego é descartado até que o destino volte a ser íntegro.

TLS 1.3: se um grupo de destino estiver configurado com verificações de integridade de HTTPS, seus destinos registrados falharão nas verificações de integridade se oferecerem suporte somente a TLS 1.3. Esses destinos devem oferecer suporte a uma versão anterior do TLS, como o TLS 1.2.

Balanceamento de carga entre zonas: por padrão, o balanceamento de carga entre zonas de disponibilidade está desativado. Se o balanceamento de carga entre zonas estiver ativado, cada

Gateway Load Balancer poderá ver todos os destinos em todas as zonas de disponibilidade, e todos serão tratados da mesma forma, independentemente da zona.

As decisões de balanceamento de carga e verificação de integridade são sempre independentes entre as zonas. Mesmo quando o balanceamento de carga entre zonas está ativado, o comportamento dos fluxos existentes e dos novos fluxos é o mesmo descrito acima. Para mais informações, consulte [Balanceamento de carga entre zonas](#) no Manual do usuário do Elastic Load Balancing.

Verificar a integridade de seus destinos

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

New EC2 experience

Para verificar a integridade dos seus destinos usando a nova experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Destinos, a coluna Status indica o status de cada destino.
5. Se o status de destino for qualquer valor diferente de `Healthy`, a coluna Detalhes do status conterá mais informações.

Old EC2 experience

Para verificar a integridade dos seus destinos usando a antiga experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Selecione o grupo de destino.
4. Escolha Destinos e visualize o status de cada destino na coluna Status. Se o status for qualquer valor diferente de `Healthy`, o console exibirá mais informações.

Para verificar a integridade dos seus destinos usando a 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 configurações de verificação de integridade

Você pode modificar algumas das configurações de verificação de integridade de seu grupo de destino.

New EC2 experience

Para modificar as configurações de verificação de integridade de um grupo de destino usando a nova experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Escolha o nome do grupo de destino para abrir sua página de detalhes.
4. Na guia Detalhes do grupo, na seção Configurações da verificação de integridade, escolha Editar.
5. Na página Editar configurações da verificação de integridade, modifique as configurações conforme necessário e escolha Salvar alterações.

Old EC2 experience

Para modificar as configurações de verificação de integridade de um grupo de destino usando a antiga experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Selecione o grupo de destino.
4. Escolha Verificações de integridade, Editar.
5. Na página Editar grupo de destino, modifique as configurações conforme o necessário e, em seguida, selecione Salvar.

Para modificar as configurações de verificação de integridade de um grupo de destino usando a AWS CLI

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

Registrar destinos com o grupo de destino

Quando o destino estiver pronto para processar solicitações, registre-o em um ou mais grupos de destino. É possível registrar destinos por ID de instância ou por endereço IP. O Gateway Load Balancer inicia as solicitações de roteamento ao destino assim que o processo de registro for concluído e o destino passar nas verificações de integridade iniciais. Pode levar alguns minutos para que o processo de registro seja concluído e as verificações de integridade sejam iniciadas. Para obter mais informações, consulte [Verificações de integridade para 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 Gateway Load Balancer interrompa as solicitações de roteamento para o destino. Se a demanda aumentar posteriormente, será possível registrar novamente os alvos que cancelaram o registro no grupo de destino. Se você precisar atender um destino, poderá cancelar o registro e registrá-lo novamente quando a manutenção estiver concluída.

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

Grupos de segurança de destino

Quando você registra instâncias do EC2 como destinos, precisa garantir que os grupos de segurança dessas instâncias permitam tráfego interno como externo na porta 6081.

Os Gateway Load Balancers não têm grupos de segurança associados. Portanto, os `security groups` para seus destinos devem usar endereços IP para permitir o tráfego do load balancer.

Network ACLs

Quando você registra instâncias do EC2 como destinos, precisa garantir que a lista de controle de acesso (ACL) de rede das sub-redes para suas instâncias permitam o tráfego na porta 6081. A ACL de rede padrão para um VPC permite todo o tráfego de entrada e saída. Se você criar ACLs de rede personalizadas, verifique se elas permitem o tráfego apropriado.

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 Gateway Load Balancer.

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

Requisitos

- 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.

Índice

- [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.

New EC2 experience

Para registrar ou cancelar o registro de destinos por ID de instância usando a nova experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione 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 e escolha Incluir como pendente abaixo. Após terminar de adicionar instâncias, escolha Registrar destinos pendentes.
6. Para cancelar o registro de instâncias, selecione a instância e escolha Cancelar registro.

Old EC2 experience

Para registrar ou cancelar o registro de destinos por ID de instância usando a antiga experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Selecione o grupo de destino.
4. Escolha Targets (Destinos), Edit (Editar).
5. (Opcional) Em Registered instances (Instâncias registradas), selecione as instâncias que terão o registro cancelado e selecione Remove (Remover).
6. (Opcional) Em Instâncias, selecione as instâncias em execução que serão registradas e, em seguida, selecione Adicionar às registradas.
7. Escolha Save (Salvar).

Registrar ou cancelar o registro de destinos por endereço IP

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)

New EC2 experience

Para registrar ou cancelar o registro de destinos por endereço IP usando a nova experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione 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, especifique a rede, a zona de disponibilidade, o endereço IP 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.

Old EC2 experience

Para registrar ou cancelar o registro de destinos por endereço IP usando a antiga experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Selecione o grupo de destino e selecione Targets (Destinos), Edit (Editar).
4. Para registrar endereços IP, escolha o ícone Register targets (Registrar destinos) (o sinal de mais) na barra de menus. Para cada endereço IP, especifique a rede, a zona de disponibilidade, o endereço IP e a porta e, em seguida, escolha Add to list (Adicionar à lista). Quando você concluir a especificação de endereços, escolha Register (Registrar).
5. Para cancelar o registro de endereços IP, escolha o ícone Deregister targets (Cancelar o registro de destinos) (o sinal de menos) na barra de menus. Se você tiver vários endereços IP registrados, poderá ser útil para adicionar um filtro ou alterar a ordem de classificação. Selecione os endereços IP e escolha Deregister (Cancelar o registro).
6. Para sair desta tela, escolha o ícone Back to target group (Voltar para o grupo de destino) (o botão Voltar) na barra de menus.

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.

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 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 prefixo `aws:` no nome nem no valor de suas tags, pois ele é reservado para uso da AWS. 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.

New EC2 experience

Para atualizar as tags de um grupo de destino usando a nova experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione 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 Remove ao lado da tag.
5. Ao concluir a atualização de tags, selecione Salvar alterações.

Old EC2 experience

Para atualizar as tags de um grupo de destino usando a antiga experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Selecione o grupo de destino.
4. Na guia Tags, selecione Add/Edit Tags (Adicionar/Editar tags) e execute uma ou mais das ações a seguir:
 - a. Para atualizar uma tag, edite os valores de Chave e Valor.
 - b. Para adicionar uma nova tag, selecione Criar tag e, em seguida, insira os valores para Chave e Valor.
 - c. Para excluir uma tag, escolha o ícone de exclusão (X) ao lado da tag.
5. Ao concluir a atualização de tags, selecione Salvar.

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

Use os comandos [add-tags](#) e [remove-tags](#).

Excluir um grupo de destino

Você pode excluir um grupo de destino se não houve ações de encaminhamento de regras 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.

New EC2 experience

Para excluir um grupo de destino usando a nova experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, 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.

Old EC2 experience

Para excluir um grupo de destino usando a antiga experiência do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em LOAD BALANCING, selecione Grupos de destino.
3. Selecione o grupo de destino e escolha Actions (Ações), Delete (Excluir).
4. Quando a confirmação for solicitada, selecione Yes (Sim).

Para excluir um grupo de destino usando a AWS CLI

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

Monitorar os Gateway Load Balancers

Você pode usar os recursos a seguir para monitorar seu Gateway Load Balancers, analisar padrões de tráfego e solucionar problemas. No entanto, o Gateway Load Balancer não gera logs de acesso, pois é um balanceador de carga transparente de camada 3 que não encerra fluxos. Para receber logs de acesso, você deve habilitar o registro em log de acesso nos dispositivos de destino do Gateway Load Balancer, como firewalls, IDS/IPS e dispositivos de segurança. Além disso, você também pode optar por habilitar os logs de fluxo da VPC nos Gateway Load Balancers.

Métricas do CloudWatch

Você pode usar o Amazon CloudWatch para recuperar estatísticas sobre os pontos de dados para os seus Gateway Load Balancers e destinos como um conjunto ordenado de dados de séries temporais, conhecidos como métricas. Você pode usar essas métricas para verificar se o sistema está executando conforme o esperado. Para obter mais informações, consulte [Métricas do CloudWatch para seu Gateway Load Balancer](#).

Logs de fluxo da VPC

Você pode usar os logs de fluxo da VPC para capturar informações detalhadas sobre o tráfego de entrada e saída do seu Gateway 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 Gateway Load Balancer. Há uma interface de rede por sub-rede. Para identificar as interfaces de rede para um Gateway Load Balancer, procure o nome do Gateway Load Balancer no campo de descrição da interface de rede.

Há duas entradas para cada conexão por meio de seu Gateway Load Balancer: uma para a conexão de front-end entre o cliente e o Gateway Load Balancer e outra para a conexão de back-end entre o Gateway Load Balancer e o destino. Se o destino for registrado por ID de instância, a conexão será exibida para a instância como uma conexão do cliente. Se o grupo de segurança da instância não permitir conexões do cliente, mas as ACLs da rede para a sub-rede as permitirem, os logs para a interface de rede do Gateway 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.

Logs do CloudTrail

É possível usar o AWS CloudTrail para capturar informações detalhadas sobre as chamadas feitas para a API Elastic Load Balancing e armazená-las como arquivos de log no Amazon S3. Você pode usar esses logs do CloudTrail para determinar quais chamadas foram feitas, o endereço IP de origem da chamada, quem fez a chamada, quando ela foi feita, etc. Para obter mais informações, consulte [Registro de chamadas de API para seu Gateway Load Balancer usando o AWS CloudTrail](#).

Métricas do CloudWatch para seu Gateway Load Balancer

O Elastic Load Balancing publica pontos de dados no Amazon CloudWatch para seus Gateway Load Balancers e destinos. O CloudWatch permite recuperar estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos 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 Gateway 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 alarme do CloudWatch para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica sair do que você considera um intervalo aceitável.

O Elastic Load Balancing relata métricas para o CloudWatch somente quando as solicitações são enviadas pelo Gateway Load Balancer. Se houver solicitações em fluxo, o Elastic Load Balancing vai medir e enviar suas métricas em intervalos de 60 segundos. Se não há solicitações em fluxo ou não há dados para uma métrica, a métrica não é reportada.

Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

Índice

- [Métricas do Gateway Load Balancer](#)
- [Dimensões métricas dos Gateway Load Balancers](#)
- [Visualizar métricas do CloudWatch para seu Gateway Load Balancer](#)

Métricas do Gateway Load Balancer

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

Métrica	Descrição
ActiveFlowCount	<p>O número total de fluxos simultâneos (ou conexões) dos clientes para os destinos.</p> <p>Critérios de relatório: há um valor diferente de zero</p> <p>Estatísticas: as estatísticas mais úteis são Average, Maximum e Minimum.</p> <p>Dimensões</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
ConsumedLCUs	<p>O número de unidades de Load Balancer Capacity (LCU – Capacidade de load balancer) usadas pelo load balancer. Você paga pelo número de LCUs que usa por hora. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing.</p> <p>Critérios de relatório: sempre relatado</p> <p>Estatísticas: todas</p> <p>Dimensões</p> <ul style="list-style-type: none"> • LoadBalancer
HealthyHostCount	<p>O número de destinos considerados íntegros.</p> <p>Critérios de relatório: relatado se as verificações de integridade estiverem habilitadas</p> <p>Estatísticas: as estatísticas mais úteis são Maximum e Minimum.</p>

Métrica	Descrição
	<p>Dimensões</p> <ul style="list-style-type: none"> • <code>LoadBalancer</code> , <code>TargetGroup</code> • <code>AvailabilityZone</code> , <code>LoadBalancer</code> , <code>TargetGroup</code>
<code>NewFlowCount</code>	<p>O número total de novos fluxos (ou conexões) estabelecidos dos clientes para os destinos no período.</p> <p>Critérios de relatório: há um valor diferente de zero</p> <p>Estatísticas: a estatística mais útil é <code>Sum</code>.</p> <p>Dimensões</p> <ul style="list-style-type: none"> • <code>LoadBalancer</code> • <code>AvailabilityZone</code> , <code>LoadBalancer</code>
<code>ProcessedBytes</code>	<p>O número total de bytes processados pelo load balancer. Essa contagem inclui o tráfego de e para destinos, mas não o tráfego de verificação de integridade.</p> <p>Critérios de relatório: há um valor diferente de zero</p> <p>Estatísticas: a estatística mais útil é <code>Sum</code>.</p> <p>Dimensões</p> <ul style="list-style-type: none"> • <code>LoadBalancer</code> • <code>AvailabilityZone</code> , <code>LoadBalancer</code>

Métrica	Descrição
UnHealthyHostCount	<p>O número de destinos considerados não íntegros.</p> <p>Critérios de relatório: relatado se as verificações de integridade estiverem habilitadas</p> <p>Estatísticas: as estatísticas mais úteis são Maximum e Minimum.</p> <p>Dimensões</p> <ul style="list-style-type: none"> • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup

Dimensões métricas dos Gateway Load Balancers

Para filtrar as métricas do Gateway Load Balancer, use as dimensões a seguir.

Dimensão	Descrição
AvailabilityZone	Filtra os dados de métrica por zona de disponibilidade.
LoadBalancer	Filtra os dados da métrica por Gateway Load Balancer. Especifique o Gateway Load Balancer da seguinte maneira: gateway/load-balancer-name/1234567890123456 (a parte final do ARN).
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).

Visualizar métricas do CloudWatch para seu Gateway Load Balancer

Você pode visualizar as métricas do CloudWatch para seus Gateway Load Balancers usando o console do Amazon EC2. Essas métricas são exibidas como gráficos de monitoramento. O monitoramento de gráficos mostrará pontos de dados se o Gateway Load Balancer estiver ativo e recebendo solicitações.

Como alternativa, você pode visualizar as métricas do seu Gateway Load Balancer usando o console do CloudWatch.

Para visualizar as métricas usando o console do Amazon EC2

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 Gateway Load Balancer, faça o seguinte:
 - a. No painel de navegação, selecione Load Balancers.
 - b. Selecione o Gateway 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.

Como exibir métricas usando o console do CloudWatch

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Selecione o namespace GatewayELB.
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/GatewayELB
```

Para obter as estatísticas de uma métrica usando a AWS CLI

Use o comando [get-metric-statistics](#) para obter estatísticas para a métrica e a dimensão especificadas. Observe que o CloudWatch trata cada combinação única de dimensões como uma métrica distinta. 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/GatewayELB \  
--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": "2020-12-18T22:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    {  
      "Timestamp": "2020-12-18T04:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    ...  
  ],  
  "Label": "UnHealthyHostCount"  
}
```

Registro de chamadas de API para seu Gateway Load Balancer usando o AWS CloudTrail

O Elastic Load Balancing é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um produto da AWS no Elastic Load Balancing. O CloudTrail captura todas as chamadas de API para o Elastic Load Balancing como eventos. As chamadas capturadas incluem chamadas do AWS Management Console e chamadas de código para as operações de API do Elastic Load Balancing. Se você criar uma trilha, poderá habilitar a

entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Elastic Load Balancing. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Elastic Load Balancing, o endereço IP no qual a solicitação foi feita, quem fez a solicitação e quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o [Guia do usuário do AWS CloudTrail](#).

Informações do Elastic Load Balancing no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre atividade no Elastic Load Balancing, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de produtos da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte [Visualizar eventos com o histórico de eventos do CloudTrail](#).

Para obter um registro de eventos em andamento na sua conta da AWS, incluindo eventos do Elastic Load Balancing, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configurar notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões](#) e [Receber arquivos de log do CloudTrail de várias contas](#)

Todas as ações do Elastic Load Balancing para Gateway Load Balancers são registradas pelo CloudTrail e documentadas na [Referência da API do Elastic Load Balancing versão 2015-12-01](#). Por exemplo, as chamadas para as ações `CreateLoadBalancer` e `DeleteLoadBalancer` geram entradas nos arquivos de log do CloudTrail.

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 uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

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 a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Os arquivos de log incluem eventos para as chamadas da API da AWS para a sua conta da AWS, não apenas chamadas da 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 log do CloudTrail para o Elastic Load Balancing para um usuário que criou um Gateway Load Balancer e o excluiu em seguida usando a 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": "2020-12-11T15:31:48Z",
    "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 boto-core/1.4.1",
    "requestParameters": {
      "subnets": ["subnet-8360a9e7", "subnet-b7d581c0"],
      "name": "my-load-balancer",
      "type": "gateway"
    },
  },
  "responseElements": {
    "loadBalancers": [{
      "type": "gateway",
      "loadBalancerName": "my-load-balancer",
      "vpcId": "vpc-3ac0fb5f",
      "state": {"code": "provisioning"},
      "availabilityZones": [
        {"subnetId": "subnet-8360a9e7", "zoneName": "us-west-2a"},
        {"subnetId": "subnet-b7d581c0", "zoneName": "us-west-2b"}
      ],
      "createdTime": "Dec 11, 2020 5:23:50 PM",
      "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0",
    }
  ]
},
"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": "2020-12-12T15:31:48Z",
  "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/gateway/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"
}
```

Cotas para o Gateway Load Balancers

Sua conta da AWS possui cotas padrão, anteriormente chamadas de limites, para cada produto 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 solicitar um aumento de cota, use o [formulário de aumento de limite](#)

balanceador de cargas

A conta da AWS tem as seguintes cotas relacionadas aos Gateway Load Balancers.

Nome	Padrão	Ajustável
Gateway Load Balancers por região	100	Sim
Gateway Load Balancers por VPC	100	Sim
ENIs de Gateway Load Balancers por VPC	300 *	Sim
Receptores por Gateway Load Balancer	1	Não

* Cada Gateway Load Balancer usa uma interface de rede por zona.

Grupos de destino

As cotas a seguir são para grupos de destino.

Nome	Padrão	Ajustável
Grupos de destino GENEVE por região	100	Sim
Destinos por grupo de destino	1.000	Sim
Destinos por zona de disponibilidade por grupo de destino GENEVE	300	Não
Destinos por zona de disponibilidade por Gateway Load Balancer	300	Não

Nome	Padrão	Ajustável
Destinos por Gateway Load Balancer	300	Não

Largura de banda

Por padrão, cada endpoint da VPC é compatível com uma largura de banda de até 10 Gbps por zona de disponibilidade e pode aumentar a escala verticalmente para até 100 Gbps de modo automático.

Se a sua aplicação precisar de throughput mais alta, entre em contato com o suporte da AWS.

Histórico documental de Gateway Load Balancers

A tabela a seguir descreve todos os lançamentos dos Gateway Load Balancers.

Alteração	Descrição	Data
Suporte a IPv6	Você pode configurar seu Gateway Load Balancer para aceitar tanto endereços IPv4 como IPv6.	12 de dezembro de 2022
Aderência de fluxo configurável	Você pode configurar o hashing que mantém a aderência de fluxo a um dispositivo de destino específico.	25 de agosto de 2022
Versão inicial	Este lançamento do Elastic Load Balancing apresenta os Gateway Load Balancers.	10 de novembro de 2020

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.