Elastic Load Balancing

Classic Load Balancers

Table of Contents

O que é um balanceador de carga clássico? ... 1
- Visão geral do balanceador de carga clássico ... 1
- Benefits ... 2
- Como começar a usar ... 2
- Pricing ... 2

Tutorial: Crie um Classic Load Balancer ... 3
- Antes de começar ... 3
- Etapa 1: Selecione um tipo de balanceador de carga ... 3
- Etapa 2: Defina seu balanceador de carga ... 4
- Etapa 3: Atribua grupos de segurança ao balanceador de carga em uma VPC ... 5
- Etapa 4: Configure as verificações de integridade para as instâncias do EC2 ... 5
- Etapa 5: Registre instâncias do EC2 com seu balanceador de carga ... 6
- Etapa 6: Coloque uma marcação em seu balanceador de carga (opcional) ... 6
- Etapa 7: Crie e verifique seu balanceador de carga ... 7
- Etapa 8: Excluir o balanceador de carga (opcional) ... 7

Balanceadores de carga voltados para a Internet ... 8
- Nomes DNS públicos para seu balanceador de carga ... 8
- Criar um balanceador de carga voltado para a Internet ... 9

Balanceadores de carga internos ... 10
- Nome DNS público para seu balanceador de carga ... 10
- Criar um balanceador de carga interno ... 11
  - Prerequisites ... 11
  - Criar um balanceador de carga interno usando o console ... 11
  - Criar um balanceador de carga interno usando a AWS CLI ... 13

Instâncias registradas ... 15
- Práticas recomendadas para as suas instâncias ... 15
- Preparar sua VPC e instâncias do EC2 ... 15
- Configurar verificações de integridade ... 16
  - Configuração de verificação de integridade ... 17
  - Atualizar a configuração de verificação de integridade ... 18
  - Verificar a integridade das suas instâncias ... 19
  - Solucionar problemas das verificações de integridade ... 19
- Configurar grupos de segurança ... 19
  - Grupos de segurança para balanceadores de carga em uma VPC ... 20
  - Grupos de segurança para instâncias em uma VPC ... 22
  - ACLs da rede dos balanceadores de carga de uma VPC ... 22
  - Grupos de segurança para instâncias do EC2-Classic ... 24
- Adicionar ou remover zonas de disponibilidade ... 26
  - Adicione uma Zona de disponibilidade ... 27
  - Remover uma Zona de disponibilidade ... 28
- Adicionar ou remover sub-redes ... 28
  - Requirements ... 29
  - Adicionar uma sub-rede ... 29
  - Remover uma sub-rede ... 30
- Registrar ou cancelar o registro de instâncias ... 31
  - Prerequisites ... 31
  - Registrar uma instância ... 32
  - Visualize as instâncias registradas em um balanceador de carga ... 32
  - Determine o balanceador de carga para uma instância registrada ... 33
  - Cancelar o registro de uma instância ... 33

Listeners ... 34
- Protocols ... 34
  - Protocolo TCP/SSL ... 35
  - Protocolo HTTP/HTTPS ... 35

Listeners HTTPS/SSL ... 35
Certificados do servidor SSL ... 35
Negociação SSL ... 36
Autenticação do servidor backend ... 36
Configurações do listener ... 36
Cabeçalhos X-Forwarded ... 38
X-Forwarded-For ... 38
X-Forwarded-Proto ... 39
X-Forwarded-Port ... 39
Listeners HTTPS ... 40
Certificados SSL/TLS ... 40
Criar ou importar um certificado SSL/TLS usando o AWS Certificate Manager ... 41
Importar um certificado SSL/TLS usando o IAM ... 41
Configurações de negociação SSL ... 41
Políticas de segurança ... 41
Protocolos SSL ... 42
Preferência ditada pelo servidor ... 42
Codificações SSL ... 43
Políticas de segurança SSL predefinidas ... 45
Criar um balanceador de carga HTTPS ... 48
Prerequisites ... 49
Criar um balanceador de carga HTTPS/SSL usando o console ... 49
Criar um balanceador de carga HTTPS/SSL usando a AWS CLI ... 54
Configurar um listener HTTPS ... 62
Prerequisites ... 63
Adicionar um listener HTTPS usando o console ... 63
Adicionar um listener HTTPS usando a AWS CLI ... 64
Substituir o certificado SSL ... 65
Substituir o certificado SSL usando o console ... 66
Substituir o certificado SSL usando a AWS CLI ... 66
Atualizar a configuração de negociação SSL ... 67
Atualizar a configuração da negociação SSL usando o console ... 67
Atualizar a configuração de negociação SSL usando a AWS CLI ... 68
Configurar o balanceador de carga ... 72
Configurar o tempo limite de inatividade ... 72
Configurar o tempo limite de inatividade usando o console ... 72
Configurar o tempo limite de inatividade usando a AWS CLI ... 73
Configurar o balanceamento de carga entre zonas ... 73
Habilitar o balanceamento de carga entre zonas ... 74
Desabilitar o balanceamento de carga entre zonas ... 75
Configurar a descarga da conexão ... 76
Habilitar a descarga da conexão ... 77
Desabilitar a descarga da conexão ... 77
Configurar o protocolo de proxy ... 78
Cabeçalho do protocolo de proxy ... 78
Pré-requisitos para habilitar o protocolo de proxy ... 79
Habilitar o protocolo de proxy usando a AWS CLI ... 79
Desabilitar o protocolo de proxy usando a AWS CLI ... 80
Configurar sessões persistentes ... 81
Persistência da sessão com base na duração ... 82
Persistência da sessão controlada pela aplicação ... 84
Configurar o modo de mitigação de dessincronização ... 86
Classifications ... 86
Modes ... 87
Modificar o modo de mitigação de dessincronização ... 88
Colocar uma marcação em seu balanceador de carga ... 88
Restrições de tags ... 89

Adicione um tag 89
Remover uma marcação 89
Configure o nome de domínio 90
Como associar seu nome de domínio personalizado com o nome do seu balanceador de carga 91
Configure o failover de DNS para o seu balanceador de carga 91
Dissociar seu nome de domínio personalizado do seu balanceador de carga 92
Monitore seu balanceador de carga 93
Métricas do CloudWatch 93
Métricas do Classic Load Balancer 94
Dimensões métricas dos Classic Load Balancers 99
Estatísticas para métricas do Classic Load Balancer 99
Visualizar métricas do CloudWatch para o balanceador de carga 100
Logs de acesso 101
Arquivos do log de acesso 101
Entradas do log de acesso 102
Processando logs de acesso 105
Habilitar logs de acesso 105
Desabilitar logs de acesso 110
Logs do CloudTrail 111
Informações do Elastic Load Balancing no CloudTrail 111
Noções básicas sobre entradas de arquivo de log do Elastic Load Balancing 112
Solução dos problemas do seu balanceador de carga 114
Erros de API 115
CertificateNotFound: Undefined (certificado não encontrado: indefinido) 115
OutofService: A transient error occurred (Fora de serviço: ocorreu um erro temporário) 116
Erros de HTTP 116
HTTP 400: BAD_REQUEST 117
HTTP 405: METHOD_NOT_ALLOWED 117
HTTP 408: Request Timeout (HTTP 408: limite de tempo de solicitação) 117
HTTP 502: Bad Gateway (HTTP 502: gateway incorreto) 117
HTTP 503: Service Unavailable (HTTP 503: serviço indisponível) 117
HTTP 504: Gateway Timeout (HTTP 504: limite de tempo do gateway) 118
Métricas do código de resposta 118
HTTPCode_ELB_4XX 119
HTTPCode_ELB_5XX 119
HTTPCode_Backend_2XX 119
HTTPCode_Backend_3XX 119
HTTPCode_Backend_4XX 119
HTTPCode_Backend_5XX 120
Verificações de integridade 120
Erro na página de destino da verificação de integridade 120
A conexão com as instâncias expirou 121
A autenticação de chave pública não está funcionando 122
A instância não está recebendo tráfego do load balancer 122
As portas da instância não estão abertas 122
As instâncias em um grupo do Auto Scaling estão falhando na verificação de integridade do ELB . 123
Conectividade do cliente 123
Registro de instância 123
O registro de uma instância EC2 está demorando muito 124
Não é possível registrar uma instância iniciada a partir de uma AMI paga 124
Cotas 125
Histórico do documento 126

O que é um balanceador de carga clássico?

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

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

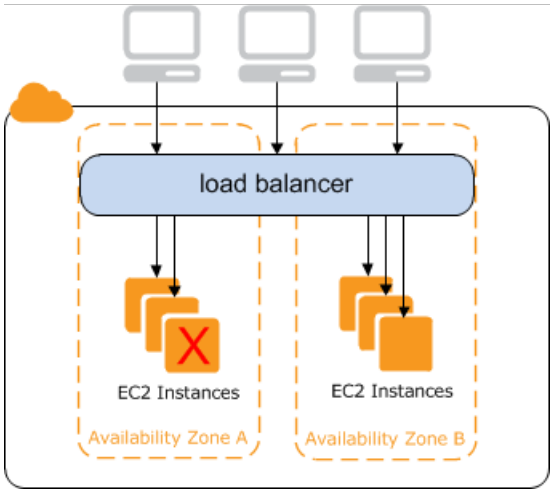
Visão geral do balanceador de carga clássico

O load balancer distribui o tráfego de entrada do aplicativo por várias instâncias EC2 em diversas Zonas de disponibilidade. Isso aumenta a tolerância a falhas dos seus aplicativos. O Elastic Load Balancing detecta instâncias com problemas de integridade e roteia o tráfego somente para instâncias íntegras.

Seu load balancer serve como ponto único de contato para os clientes. Isso aumenta a disponibilidade do seu aplicativo. Você pode adicionar e remover instâncias do load balancer do conforme mudarem suas necessidades, sem perturbar o fluxo geral de solicitações para seu aplicativo. 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.

Um listener verifica a solicitações de conexão de clientes, usando o protocolo e a porta que você configurar, e encaminha solicitações para uma ou mais instâncias registrados usando o protocolo e o número da porta que você configurar. Você adiciona um ou mais listeners ao seu load balancer.

Você pode configurar as verificações de integridade, as quais são usadas para monitorar a integridade das instâncias registradas para que o load balancer envie solicitações somente às instâncias íntegras.



Para garantir que suas instâncias registradas sejam capazes de lidar com a carga de solicitações em cada Zona de disponibilidade, é importante manter aproximadamente o mesmo número de instâncias em cada Zona de disponibilidade registrada no load balancer. Por exemplo, se você tiver dez instâncias na Zona de disponibilidade us-west-2a e duas instâncias em us-west-2b, as solicitações serão distribuídas uniformemente entre as duas Zonas de disponibilidade. Como resultado, a duas instâncias em us-west-2b servirão a mesma quantidade de tráfego que as dez instâncias em us-west-2a. Em vez disso, você deve ter seis instâncias em cada Zona de disponibilidade.

Por padrão, o load balancer distribui tráfego uniformemente entre as Zonas de disponibilidade que você habilitar para o load balancer. Para distribuir o tráfego uniformemente em todas as instâncias registradas em todas as Zonas de disponibilidade habilitadas, habilite o balanceamento de carga entre zonas no seu load balancer. No entanto, recomendamos ainda que você mantenha números aproximadamente equivalentes de instâncias em cada Zona de disponibilidade, para melhor tolerância a falhas.

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

Benefits

O uso de um balanceador de carga clássico em vez de um balanceador de carga da aplicação tem os seguintes benefícios:

- Suporte para EC2-Classic
- Suporte para listeners TCP e SSL
- Suporte a sticky sessions usando cookies gerado pelo aplicativo

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

Como começar a usar

- Para aprender a criar um balanceador de carga clássico e registrar instâncias do EC2 com ele, consulte Tutorial: Crie um Classic Load Balancer (p. 3).
- Para aprender a criar um load balancer HTTPS e registrar instâncias EC2 com ele, consulte Criar um balanceador de carga clássico com um listener HTTPS (p. 48).
- Para aprender a usar os diversos recursos compatíveis com o Elastic Load Balancing, consulte Configurar o balanceador de carga clássico (p. 72).

Pricing

Com o load balancer, você paga somente pelo que utilizar. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing.

Tutorial: Crie um Classic Load Balancer

Este tutorial fornece uma introdução prática a balanceadores de carga clássicos por meio do AWS Management Console, uma interface baseada na Web. Você criará um load balancer que recebe tráfego HTTP público e o envia para suas instâncias EC2.

Observe que você pode criar seu load balancer para uso com EC2-Classic ou VPC. Algumas das tarefas descritas neste tutorial aplicam-se somente a load balancers em uma VPC.

Tarefas

- Antes de começar (p. 3)
- Etapa 1: Selecione um tipo de balanceador de carga (p. 3)
- Etapa 2: Defina seu balanceador de carga (p. 4)
- Etapa 3: Atribua grupos de segurança ao balanceador de carga em uma VPC (p. 5)
- Etapa 4: Configure as verificações de integridade para as instâncias do EC2 (p. 5)
- Etapa 5: Registre instâncias do EC2 com seu balanceador de carga (p. 6)
- Etapa 6: Coloque uma marcação em seu balanceador de carga (opcional) (p. 6)
- Etapa 7: Crie e verifique seu balanceador de carga (p. 7)
- Etapa 8: Excluir o balanceador de carga (opcional) (p. 7)

Antes de começar

- Siga as etapas em Preparar sua VPC e instâncias do EC2 (p. 15).
- Execute as instâncias EC2 que você planeja registrar com seu load balancer. Verifique se os security groups dessas instâncias permitem acesso HTTP na porta 80.
- Instale um servidor Web, como o Apache ou Internet Information Services (IIS), em cada instância, insira o nome DNS no campo de endereço de um navegador da Web conectado à Internet e verifique se o navegador exibe a página padrão do servidor.

Etapa 1: Selecione um tipo de balanceador de carga

O Elastic Load Balancing é compatível com diferentes tipos de balanceador de carga. Neste tutorial, você criará um balanceador de carga clássico.

Para criar um balanceador de carga clássico

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, escolha uma região para seu balanceador de carga. Certifique-se de selecionar a mesma região selecionada para suas instâncias do EC2.
3. No painel de navegação, em LOAD BALANCING, escolha Load balancers.
4. Selecione Criar load balancer.
5. Em Classic Load Balancer, selecione Criar.

Etapa 2: Defina seu balanceador de carga

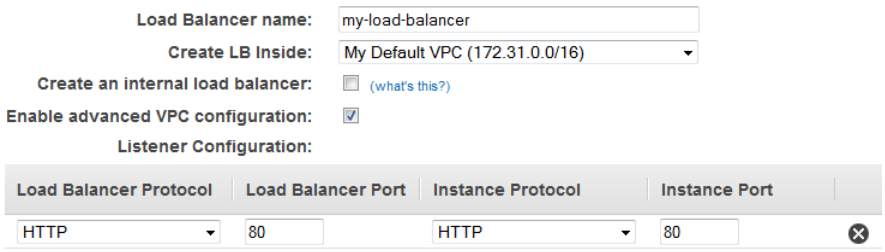
Você deve fornecer algumas configurações básicas sobre seu load balancer, como nome, rede e listener.

Escuta é um processo que verifica se há solicitações de conexão. Ele é pré-configurado com um protocolo e uma porta para conexões front-end (cliente para load balancer) e um protocolo e uma porta para conexões back-end (load balancer para instância). Neste tutorial, você configura um listener que aceita solicitações HTTP na porta 80 e as envia para suas instâncias na porta 80 usando HTTP.

Para definir seu load balancer e seu listener

1. Em Load Balancer name (Nome do balanceador de carga), digite um nome para o balanceador de carga.

   O nome de seu balanceador de carga clássico deve ser exclusivo dentro de seu conjunto de balanceadores de carga clássicos e para a região. Ele pode ter no máximo 32 caracteres, pode conter apenas caracteres alfanuméricos e hifens e não deve iniciar nem terminar com hífen.
2. Em Create LB inside (Criar LB interno), selecione a mesma rede que você selecionou para suas instâncias: EC2-Classic ou uma VPC específica.
3. [VPC padrão] Se você selecionou uma VPC padrão e gostaria de escolher as sub-redes para o balanceador de carga, selecione Enable advanced VPC configuration (Habilitar configuração avançada de VPC).
4. Deixe a configuração padrão do listener.

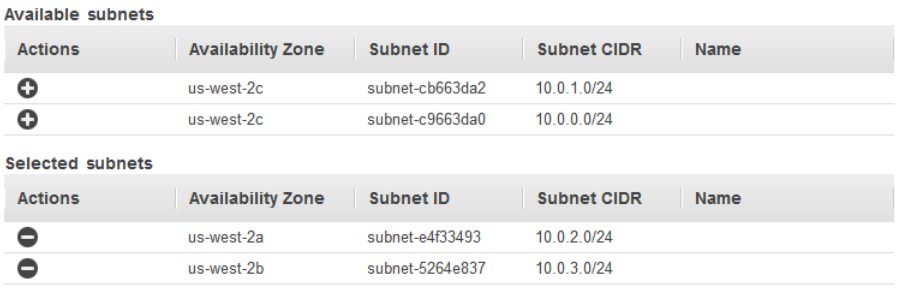


5. [EC2-VPC] Em Sub-redes disponíveis, selecione pelo menos uma sub-rede pública usando o ícone de adição. A sub-rede é movida sob Sub-redes selecionadas. Para melhorar a disponibilidade do seu load balancer, selecione mais de uma sub-rede pública.

   Note

   Se você selecionou o EC2-Classic como rede ou tem uma VPC padrão, mas não selecionou Ativar configuração avançada de VPC, você não vê a interface do usuário para selecionar sub-redes.

   Você pode adicionar no máximo uma sub-rede por Zona de disponibilidade. Se você selecionar uma sub-rede de uma Zona de disponibilidade onde já houver uma sub-rede selecionada, essa sub-rede substituirá a sub-rede atualmente selecionada por essa Zona de disponibilidade.



6. Selecione Próximo: atribuir security groups.

Etapa 3: Atribua grupos de segurança ao balanceador de carga em uma VPC

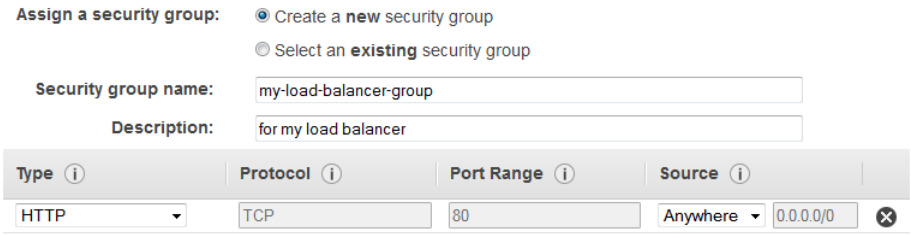
Caso tenha selecionado VPC como sua rede, será preciso atribuir o load balancer como security group que permita tráfego às portas especificadas para seu load balancer e as verificações de integridade para seu load balancer.

Note

Se você tiver selecionado EC2-Classic como sua rede, pode continuar para a próxima etapa. Por padrão, o Elastic Load Balancing fornecerá um grupo de segurança para balanceadores de carga no EC2-Classic.

Para atribuir security group ao seu load balancer

1. Na página Atribuir security groups, selecione Criar novo security group.
2. Digite um nome e uma descrição para seu security group ou mantenha o nome e a descrição padrão. Esse novo security group contém uma regra que permite o tráfego para a porta que você configurou que o load balancer usasse.



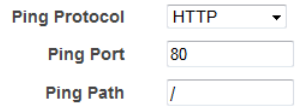
3. Selecione Next: Configure Security Settings (Próximo: Definir configurações de segurança).
4. Para este tutorial, você não está usando um listener seguro. Selecione Próximo: configurar verificação de integridade para avançar para a próxima etapa.

Etapa 4: Configure as verificações de integridade para as instâncias do EC2

O Elastic Load Balancing verifica automaticamente a integridade das instâncias do EC2 para seu balanceador de carga. Caso o Elastic Load Balancing encontre uma instância não íntegra, ele interromperá o envio de tráfego para a instância e roteará novamente o tráfego para instâncias íntegras. Nesta etapa, você personaliza as verificações de integridade para o load balancer.

Para configurar verificações de integridade para suas instâncias

1. Na página Configurar verificação de integridade, deixe o Protocolo de ping definido como HTTP e a Porta de ping definida como 80.
2. Em Ping Path, substitua o valor padrão pela barra única ("/"). Isso diz ao Elastic Load Balancing para enviar consultas de verificação de integridade para a página inicial padrão do seu servidor Web, como `index.html`.



3. Em Detalhes avançados, deixe os valores padrão.
4. Selecione Próximo: adicionar instâncias do EC2.

Etapa 5: Registre instâncias do EC2 com seu balanceador de carga

O load balancer distribui o tráfego entre as instâncias registradas nele.

> **Note**
>
> Quando você registrar uma instância com uma interface de rede elástica (ENI) anexada, o load balancer roteará o tráfego para o endereço IP principal da interface primária (eth0) da instância.

Para registrar instâncias EC2 com seu load balancer

1. Na página Adicionar instâncias do EC2, selecione as instâncias para registrar com o load balancer.
2. Habilite o balanceamento de carga entre zonas e a drenagem de conexão.
3. Selecione Próximo: adicionar tags.

Como alternativa, você pode registrar instâncias com seu load balancer mais tarde usando as seguintes opções:

- Selecione as instâncias em execução após criar o load balancer. Para obter mais informações, consulte Registrar instâncias com seu load balancer (p. 31).
- Configure o Auto Scaling para registrar as instâncias automaticamente quando ele as lançar. Para obter mais informações, consulte Configure uma aplicação dimensionada e com balanceamento de carga no Manual do usuário do Amazon EC2 Auto Scaling.

Etapa 6: Coloque uma marcação em seu balanceador de carga (opcional)

Você pode marcar o load balancer ou avançar à próxima etapa. Observe que você pode atribuir uma tag aos load balancer mais tarde; para obter mais informações, consulte Colocar uma marcação em seu balanceador de carga clássico (p. 88).

Para adicionar tags ao load balancer

1. Na página Adicionar tags, especifique uma chave e um valor para a tag.
2. Para adicionar outra tag, escolha Criar tag e especifique uma chave e um valor para a tag.
3. Depois de concluir a adição de tags, escolha Revisar e criar.

Etapa 7: Crie e verifique seu balanceador de carga

Antes de criar o load balancer, revise as configurações selecionadas por você. Depois de criar o load balancer, você pode verificar se está enviando tráfego para suas instâncias EC2.

Para criar e testar seu load balancer

1. Na página Review (Revisar), selecione Create (Criar).
2. Depois de receber a notificação sobre a criação do load balancer, selecione Fechar.
3. Selecione o novo load balancer.
4. Na guia Descrição, verifique a linha Status. Se ele indica que algumas de suas instâncias não estão em serviço, provavelmente é porque elas ainda estão no processo de registro. Para obter mais informações, consulte Solução dos problemas de um balanceador de carga clássico: registro de instância (p. 123).
5. Depois de pelo menos uma de suas instâncias EC2 entrar em serviço, você pode testar seu load balancer. Copie a string de DNS name (Nome DNS) (por exemplo, my-load-balancer-1234567890.us-west-2.elb.amazonaws.com) e cole-a no campo de endereço de um navegador da Web conectado à Internet. Se o load balancer estiver trabalhando, consulte a página padrão do seu servidor.

Etapa 8: Excluir o balanceador de carga (opcional)

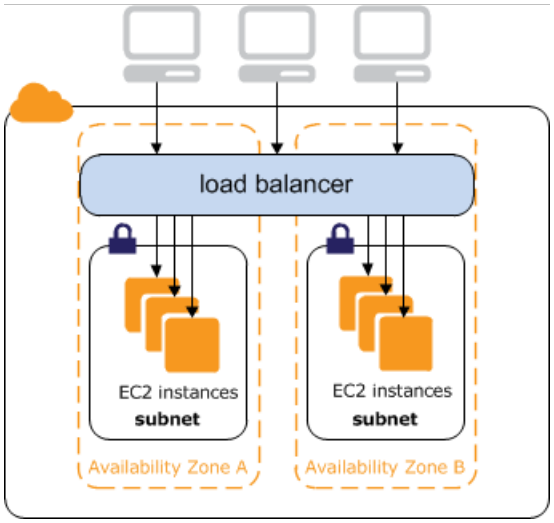
Assim que o load balancer é disponibilizado, você será cobrado por cada hora ou hora parcial em que mantê-lo em execução. Quando não precisar mais do load balancer, pode excluí-lo. Assim que o load balancer for excluído, a cobrança será interrompida. Observe que a exclusão de um load balancer não afeta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

Para excluir o load balancer

1. Se você tiver um registro CNAME para seu domínio que aponta para o load balancer, aponte-o para um novo local e aguarde até que a mudança de DNS surta efeito antes de excluir seu load balancer.
2. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
3. No painel de navegação, em LOAD BALANCING, escolha Load balancers.
4. Selecione o load balancer.
5. Escolha Actions, Delete.
6. Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).
7. (Opcional) Depois de excluir um load balancer, as instâncias EC2 associadas ao load balancer continuam a ser executadas, e você será cobrado por cada hora cheia ou hora parcial em que mantive-los em execução. Para obter mais informações sobre como interromper ou terminar suas instâncias, consulte Parar e iniciar sua instância ou Encerrar sua instância no Manual do usuário do Amazon EC2 para instâncias do Linux.

Balanceadores de carga clássicos voltados para a Internet

Um balanceador de carga voltado para a Internet tem um nome DNS que pode ser resolvido publicamente, para que ele possa rotear solicitações de clientes pela Internet para as instâncias do EC2 registradas com o balanceador de carga.



Se um load balancer estiver em uma VPC com o ClassicLink ativado, suas instâncias poderão ser instâncias EC2-Classic vinculadas. Se um load balancer estiver no EC2-Classic, suas instâncias deverão estar no EC2-Classic.

Tópicos

- Nomes DNS públicos para seu balanceador de carga (p. 8)
- Criar um balanceador de carga voltado para a Internet (p. 9)

Nomes DNS públicos para seu balanceador de carga

Quando o load balancer é criado, ele recebe um nome DNS público que os clientes podem usar para enviar solicitações. Os servidores DNS resolvem o nome DNS do seu load balancer para os endereços IP públicos dos nós do load balancer para seu load balancer. Cada nó do load balancer está conectado às instâncias back-end usando endereços IP privados.

EC2-VPC

Os load balancers de uma VPC oferecem suporte somente a endereços IPv4. O console exibe um nome DNS público da seguinte forma:

```
name-1234567890.region.elb.amazonaws.com
```

EC2-Classic

Os load balancers no EC2-Classic oferecem suporte a endereços IPv4 e IPv6. O console exibe os seguintes nomes DNS públicos:

```
name-123456789.region.elb.amazonaws.com
ipv6.name-123456789.region.elb.amazonaws.com
dualstack.name-123456789.region.elb.amazonaws.com
```

A base do nome DNS público retorna somente registros do IPv4. O nome DNS público com o prefixo `ipv6` retorna somente registros do IPv6. O nome DNS público com o prefixo `dualstack` retorna os registros do IPv4 e do IPv6. Recomendamos que você ative o suporte a IPv6 usando o nome DNS com o prefixo `dualstack` para garantir que os clientes possam acessar o load balancer usando IPv4 ou IPv6.

Os clientes podem se conectar ao seu load balancer no EC2-Classic usando IPv4 ou IPv6. No entanto, a comunicação entre o load balancer e suas instâncias back-end usa apenas IPv4, independentemente de como o cliente se comunica com o seu load balancer.

Criar um balanceador de carga voltado para a Internet

Quando você cria um balanceador de carga em uma VPC, pode torná-lo um balanceador de carga interno ou voltado para a Internet. Você cria um balanceador de carga voltado para a Internet em uma sub-rede pública. Os balanceadores de carga do EC2-Classic são sempre voltados para a Internet.

Quando você cria o load balancer, configura listeners, configura verificações de integridade e registra instâncias back-end. Você configura um listener ao especificar um protocolo e uma porta para conexões front-end (cliente para load balancer), além de protocolo e uma porta para conexões back-end (load balancer para instâncias back-end). Você pode configurar vários listeners para o load balancer.

Para criar um balanceador de carga básico voltado para a Internet, consulte Tutorial: Crie um Classic Load Balancer (p. 3).

Para criar um load balancer com um listener HTTPS, consulte Criar um balanceador de carga clássico com um listener HTTPS (p. 48).

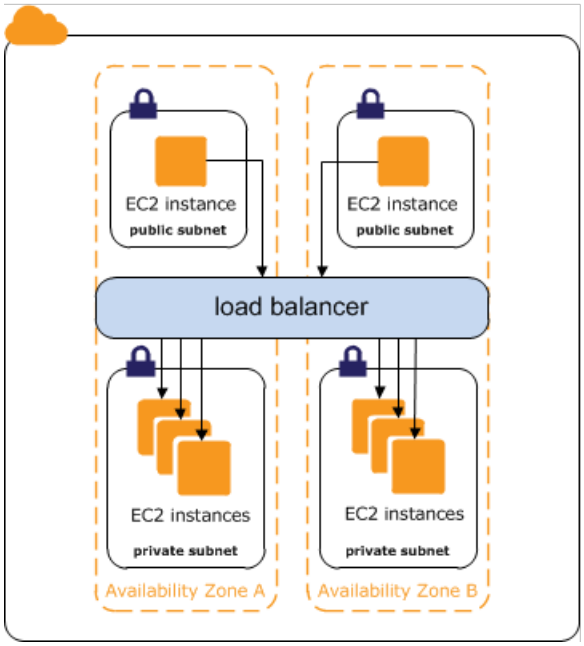
Classic Load Balancers internos

Quando você criar um balanceador de carga em uma VPC, deverá escolher se deve fazer dele um balanceador de carga interno ou voltado para a Internet.

Os nós de um load balancer voltado para a Internet têm endereços IP públicos. O nome DNS de um load balancer voltado para a Internet é resolvível publicamente para os endereços IP públicos dos nós. Portanto, os load balancers voltados para a Internet podem rotear solicitações de clientes pela Internet. Para obter mais informações, consulte Balanceadores de carga clássicos voltados para a Internet (p. 8).

Os nós de um load balancer interno têm somente endereços IP privados. O nome DNS de um load balancer interno é resolvido publicamente para os endereços IP privados dos nós. Portanto, load balancers internos só podem rotear solicitações de clientes com acesso à VPC para o load balancer.

Se sua aplicação tiver vários níveis, como servidores Web que devem ser conectados à Internet e servidores de banco de dados que só são conectados a servidores Web, você poderá criar uma arquitetura que use tanto balanceadores de carga internos quanto voltados para a Internet. Crie um load balancer voltado para a Internet e registre os servidores da web nele. Crie um load balancer interno e registre os servidores de banco de dados nele. Os servidores da web recebem solicitações do load balancer voltado para a Internet e enviam solicitações dos servidores de banco de dados para o load balancer interno. Os servidores de banco de dados recebem solicitações do load balancer interno.



Tópicos

- Nome DNS público para seu balanceador de carga (p. 10)
- Criar um balanceador de carga clássico interno (p. 11)

Nome DNS público para seu balanceador de carga

Quando um load balancer interno é criado, ele recebe um nome DNS público da seguinte forma:

```
internal-name-123456789.region.elb.amazonaws.com
```

Os servidores DNS resolvem o nome DNS do seu load balancer para os endereços IP privados dos nós do load balancer para seu load balancer interno. Cada nó do load balancer está conectado a endereços IP privados das instâncias back-end usando interfaces de rede elástica. Se o balanceamento de carga entre zonas estiver habilitado, cada nó será conectado a cada instância back-end, independentemente da Zona de disponibilidade. Caso contrário, cada nó será conectado apenas às instâncias que estiverem em sua Zona de disponibilidade.

Criar um balanceador de carga clássico interno

Você pode criar um load balancer interno para distribuir o tráfego para suas instâncias EC2 a partir de clientes com acesso à VPC para o load balancer.

Tópicos

- Prerequisites (p. 11)
- Criar um balanceador de carga interno usando o console (p. 11)
- Criar um balanceador de carga interno usando a AWS CLI (p. 13)

Prerequisites

- Se você ainda não tiver criado uma VPC para seu load balancer, deverá criá-la antes de começar. Para obter mais informações, consulte Preparar sua VPC e instâncias do EC2 (p. 15).
- Execute as instâncias EC2 que você planeja registrar com seu load balancer interno. Execute-as em sub-redes privadas na VPC destinada ao load balancer.

Criar um balanceador de carga interno usando o console

Por padrão, o Elastic Load Balancing cria um balanceador de carga voltado para a Internet. Use o procedimento a seguir para criar um load balancer interno e registrar suas instâncias EC2 com o load balancer interno recém-criado.

Para criar um load balancer interno

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 Criar load balancer.
4. Em Select load balancer type (Selecionar tipo de balanceador de carga), escolha Classic Load Balancer (Balanceador de carga clássico).
5. Na página Definir load balancer, faça o seguinte:

   a. Em Load Balancer name (Nome do balanceador de carga), digite um nome para o balanceador de carga.

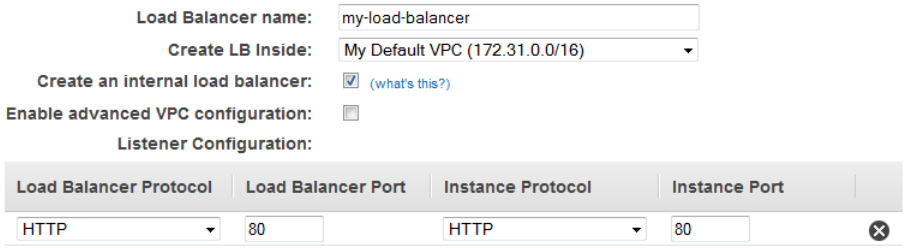
      O nome de seu balanceador de carga clássico deve ser exclusivo dentro de seu conjunto de balanceadores de carga clássicos e para a região. Ele pode ter no máximo 32 caracteres, pode conter apenas caracteres alfanuméricos e hifens e não deve iniciar nem terminar com hífen.

b. Em Create LB inside (Criar LB dentro), selecione uma VPC para seu balanceador de carga.

c. Escolha Create an internal load balancer (Criar um balanceador de carga interno).

d. [VPC padrão] Se você selecionou uma VPC padrão e gostaria de selecionar as sub-redes para o balanceador de carga, escolha Enable advanced VPC configuration (Habilitar configuração avançada de VPC).

e. Deixe a configuração padrão do listener.



f. Em Sub-redes disponíveis, selecione pelo menos uma sub-rede usando o ícone de adição. A sub-rede é movida sob Sub-redes selecionadas. Para melhorar a disponibilidade do seu load balancer, selecione mais de uma sub-rede.

> **Note**
>
> Se você selecionou uma VPC padrão como rede, mas não selecionou Ativar configuração de VPC avançada, você não tem a opção de selecionar sub-redes.

Você pode anexar no máximo uma sub-rede por Zona de disponibilidade. Se selecionar uma segunda sub-rede de uma Zona de disponibilidade onde já houver uma sub-rede anexada, essa sub-rede substituirá a sub-rede atualmente anexada pela Zona de disponibilidade.

g. Selecione Próximo: atribuir security groups.

6. Na página Atribuir security groups, selecione Criar novo security group. Digite um nome e uma descrição para seu security group ou mantenha o nome e a descrição padrão. Esse novo security group contém uma regra que permite o tráfego para a porta que você configurou que o load balancer usasse. Se você usará uma porta diferente para as verificações de integridade, deve selecionar Adicionar regra para adicionar uma regra que permita o tráfego de entrada para essa porta também. Selecione Next: Configure Security Settings (Próximo: Definir configurações de segurança).
7. Na página Definir configurações de segurança, selecione Próximo: configurar verificação de integridade para avançar para a próxima etapa. Se você preferir criar um load balancer do HTTPS, consulte Listeners HTTPS para seu balanceador de carga clássico (p. 40).
8. Na página Configurar verificação de integridade, ajuste as configurações de verificação de integridade que o aplicativo exige e, em seguida, selecione Próximo: adicionar instâncias do EC2.
9. Na página Adicionar instâncias do EC2, selecione as instâncias para registrar com o load balancer e, em seguida, selecione Próximo: adicionar tags.

> **Note**
>
> Quando você registrar uma instância com uma interface de rede elástica (ENI) anexada, o load balancer roteará o tráfego para o endereço IP principal da interface primária (eth0) da instância.

10. (Opcional) Você pode adicionar tags ao seu load balancer. Ao concluir a adição de tags, selecione Revisar e criar.
11. Na página Revisar, verifique suas configurações. Se você precisar fazer alterações, escolha o link correspondente para editá-las. Quando terminar, escolha Create (Criar imagem).
12. Depois de receber a notificação sobre a criação do load balancer, selecione Fechar.
13. Selecione o novo load balancer.
14. Na guia Descrição, observe que o Nome do DNS e o Esquema indicam que o load balancer é interno.

Verifique a linha Status. Se ele indica que algumas de suas instâncias não estão em serviço, provavelmente é porque elas ainda estão no processo de registro. Para obter mais informações, consulte Solução dos problemas de um balanceador de carga clássico: registro de instância (p. 123).

Criar um balanceador de carga interno usando a AWS CLI

Por padrão, o Elastic Load Balancing cria um balanceador de carga voltado para a Internet. Use o procedimento a seguir para criar um load balancer interno e registrar suas instâncias EC2 com o load balancer interno recém-criado.

Para criar um load balancer interno

1. Use o comando create-load-balancer com a opção `--scheme` definida como `internal`, da seguinte forma:

```
aws elb create-load-balancer --load-balancer-name my-internal-loadbalancer --listeners
 Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80
 --subnets subnet-4e05f721 --scheme internal --security-groups sg-b9ffedd5
```

   Esta é uma resposta de exemplo. Observe que o nome indica que esse é um load balancer interno.

```
{
    "DNSName": "internal-my-internal-loadbalancer-786501203.us-
west-2.elb.amazonaws.com"
}
```

2. Use o comando register-instances-with-load-balancer para adicionar instâncias:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-internal-
loadbalancer --instances i-4f8cf126 i-0bb7ca62
```

   Esta é uma resposta de exemplo:

```
{
    "Instances": [
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

3. (Opcional) Use o seguinte comando describe-load-balancers para verificar o load balancer interno:

```
aws elb describe-load-balancers --load-balancer-name my-internal-loadbalancer
```

   A resposta inclui os campos `DNSName` e `Scheme`, que indicam que esse é um load balancer interno.

```
{
    "LoadBalancerDescriptions": [
        {
```

```
            ...
            "DNSName": "internal-my-internal-loadbalancer-1234567890.us-
west-2.elb.amazonaws.com",
            "SecurityGroups": [
                "sg-b9ffedd5"
            ],
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": []
            },
            "LoadBalancerName": "my-internal-loadbalancer",
            "CreatedTime": "2014-05-22T20:32:19.920Z",
            "AvailabilityZones": [
                "us-west-2a"
            ],
            "Scheme": "internal",
            ...
        }
    ]
}
```

Instâncias registradas para seu balanceador de carga clássico

Depois de criar seu balanceador de carga clássico, você deve registrar suas instâncias do EC2 no balanceador de carga. Você pode selecionar as instâncias do EC2 de uma única zona de disponibilidade ou de várias zonas de disponibilidade dentro da mesma região do balanceador de carga. O Elastic Load Balancing realiza rotineiramente verificações de integridade nas instâncias do EC2 registradas e distribui automaticamente as solicitações de entrada para o nome DNS do seu balanceador de carga entre todas as instâncias do EC2 íntegras registradas.

Tópicos

- Práticas recomendadas para as suas instâncias (p. 15)
- Preparar sua VPC e instâncias do EC2 (p. 15)
- Configurar as verificações de integridade do seu balanceador de carga clássico (p. 16)
- Configurar grupos de segurança para seu balanceador de carga clássico (p. 19)
- Adicionar ou remover zonas de disponibilidade para o seu balanceador de carga no EC2-Classic (p. 26)
- Adicionar ou remover sub-redes para seu balanceador de carga clássico em uma VPC (p. 28)
- Registrar ou cancelar o registro de instâncias do EC2 do seu balanceador de carga clássico (p. 31)

Práticas recomendadas para as suas instâncias

- Instale um servidor web, como Apache ou Internet Information Services (IIS), em todas as instâncias que você planeja registrar com seu load balancer.
- Para listeners HTTP e HTTPS, recomendamos que você ative a opção de keep-alive nas suas instâncias EC2, que permite que o load balancer reutilize as conexões com suas instâncias para várias solicitações de clientes. Isso reduz a carga no seu servidor web e melhora a taxa de transferência do load balancer. O tempo limite do keep-alive deve ser pelo menos 60 segundos, para garantir que o load balancer seja responsável para fechar a conexão para sua instância.
- O Elastic Load Balancing é compatível com descoberta de caminho de Maximum Transmission Unit (MTU). Para garantir que o Path MTU Discovery funcione corretamente, você deve garantir que o security group da sua instância permita as mensagens necessárias de fragmentação ICMP (tipo 3, código 4). Para obter mais informações, consulte Descoberta de caminho MTU no Manual do usuário do Amazon EC2 para instâncias do Linux.

Preparar sua VPC e instâncias do EC2

Recomendamos que você inicie suas instâncias e crie seu load balancer em uma Virtual Private Cloud (VPC). Se você tiver uma nova conta da AWS ou planeja usar uma região que não usou antes, terá uma VPC padrão. Você pode usar uma VPC padrão se a tiver, ou criar a sua própria VPC.

Balanceadores de carga em uma VPC

A Amazon Virtual Private Cloud (Amazon VPC) permite que você defina um ambiente de redes virtuais em uma seção privada e isolada na Nuvem AWS. Dentro dessa nuvem privada virtual (VPC), você pode iniciar recursos da AWS, como balanceadores de carga e instâncias do EC2. Para obter mais informações, consulte o Manual do usuário da Amazon VPC.

Sub-redes para seu balanceador de carga

Para garantir que o load balancer possa ser dimensionado corretamente, verifique se cada sub-rede do load balancer tem um bloco CIDR com pelo menos uma bitmask `/27` (por exemplo, `10.0.0.0/27`) e pelo menos 8 endereços de IP gratuitos. Seu load balancer usa esses endereços IP para estabelecer conexões com as instâncias.

Crie uma sub-rede em cada Zona de disponibilidade na qual você deseja iniciar instâncias. Dependendo da seu aplicativo, você pode executar suas instâncias em sub-redes públicas, sub-redes privadas ou uma combinação de sub-redes públicas e privadas. Uma sub-rede pública tem uma rota para um gateway da Internet. Observe que as VPCs padrão têm uma sub-rede pública por Zona de disponibilidade, por padrão.

Quando você criar um load balancer, deverá adicionar uma ou mais sub-redes públicas ao load balancer. Se suas instâncias estiverem em sub-redes privadas, crie sub-redes públicas nas mesmas Zonas de disponibilidade que as sub-redes com suas instâncias; você adicionará essas sub-redes públicas ao load balancer.

Grupos de segurança

Você deve garantir que o load balancer consiga se comunicar com suas instâncias tanto na porta do listener quanto na porta de verificação de integridade. Para obter mais informações, consulte Grupos de segurança para balanceadores de carga em uma VPC (p. 20). O security group das suas instâncias deve permitir tráfego em ambas as direções em ambas as portas de cada sub-rede para seu load balancer. Para obter mais informações, consulte Grupos de segurança para instâncias em uma VPC (p. 22).

Network ACLs

Os Network ACLs da sua VPC devem permitir o tráfego nas duas direções na porta do listener e na porta de verificação de integridade. Para obter mais informações, consulte ACLs da rede dos balanceadores de carga de uma VPC (p. 22).

ClassicLink

O ClassicLink permite que suas instâncias do EC2-Classic se comuniquem com instâncias da VPC usando endereços IP privados, desde que os security groups da VPC permitam. Se você planeja registrar instâncias do EC2-Classic vinculadas no load balancer, precisa habilitar o ClassicLink para sua VPC e, em seguida, criar o load balancer no VPC habilitado para o ClassicLink. Para obter mais informações, consulte Noções básicas do ClassicLink e Trabalhar com o ClassicLink no Manual do usuário do Amazon EC2 para instâncias do Linux.

Configurar as verificações de integridade do seu balanceador de carga clássico

Seu balanceador de carga clássico envia periodicamente solicitações às instâncias registradas dele mesmo, para testar os seus status. Esses testes se chamam verificações de integridade. O status das instâncias que estão íntegras no momento da verificação de integridade é `InService`. O status de quaisquer instâncias que não estejam íntegras no momento da verificação de integridade é `OutOfService`. O load balancer executa verificações de integridade em todas as instâncias registradas, quer ela esteja em estado íntegro ou em um estado não íntegro.

O load balancer roteia solicitações somente para as instâncias íntegras. Quando o load balancer determina que uma instância está com problemas de integridade, ele interromperá o roteamento de solicitações para essa instância. O load balancer voltará a rotear as solicitações para a instância quando ela voltar ao estado de integridade.

O balanceador de carga verifica a integridade das instâncias registradas usando a configuração padrão de verificação de integridade fornecida pelo Elastic Load Balancing ou uma configuração de verificação de integridade que você configurar.

Se você tiver associado o seu grupo do Auto Scaling a um balanceador de carga clássico, poderá usar a verificação de integridade do balanceador de carga para determinar o estado de integridade das instâncias no seu grupo do Auto Scaling. Por padrão, um grupo do Auto Scaling periodicamente determina o estado de integridade de cada instância. Para obter mais informações, consulte Adicionar verificações de integridade do Elastic Load Balancing ao grupo do Auto Scaling no Manual do usuário do Amazon EC2 Auto Scaling.

Tópicos

- Configuração de verificação de integridade (p. 17)
- Atualizar a configuração de verificação de integridade (p. 18)
- Verificar a integridade das suas instâncias (p. 19)
- Solucionar problemas das verificações de integridade (p. 19)

Configuração de verificação de integridade

A configuração de integridade contém as informações que um load balancer usa para determinar a integridade das instâncias registradas. A tabela a seguir descreve os campos de configuração de verificação de integridade.

Campo	Descrição
Protocolo	O protocolo a ser usado para se conectar com a instância. Valores válidos: `TCP`, `HTTP`, `HTTPS` e `SSL` Padrão do console: `HTTP` Padrão da CLI/API: `TCP`
Porta	A porta a ser usada para se conectar com a instância, como um par `protocol:port`. Se o load balancer não conseguir se conectar com a instância na porta especificada dentro do período de tempo limite de resposta configurado, a instância será considerada não íntegra. Protocolos: `TCP`, `HTTP`, `HTTPS` e `SSL` Intervalo de portas: 1 a 65535 Padrão do console: `HTTP:80` Padrão da CLI/API: `TCP:80`
Caminho	O destino para a solicitação HTTP ou HTTPS. Uma solicitação HTTP ou HTTPS GET é emitida para a instância na porta e no caminho. Se o load balancer receber qualquer resposta diferente de "200 OK" dentro do período de tempo limite de resposta, a instância será considerada não íntegra. Se a resposta incluir um corpo, seu aplicativo deverá definir o cabeçalho Content-Length para um valor maior que ou igual a zero ou especificar Transfer-Encoding com um valor definido como 'chunked' (em partes). Padrão: `/index.html`

Campo	Descrição
Tempo limite de resposta	A quantidade de tempo de espera ao receber uma resposta da verificação de integridade, em segundos. Valores válidos: 2 a 60 Padrão: 5
HealthCheck Interval	A quantidade de tempo entre as verificações de integridade de uma instância individual, em segundos. Valores válidos: 5 a 300 Padrão: 30
Limite não íntegro	O número de verificações de integridade consecutivas com falha que deve ocorrer antes de declarar uma instância do EC2 não íntegra. Valores válidos: 2 a 10 Padrão: 2
Healthy Threshold	O número de verificações de integridade consecutivas bem-sucedidas que deve ocorrer antes de declarar uma instância do EC2 íntegra. Valores válidos: 2 a 10 Padrão: 10

O balanceador de carga envia uma solicitação de verificação de integridade para cada instância registrada a cada `Interval` segundos, usando a porta, o protocolo e o caminho especificados. Cada solicitação de verificação de integridade é independente e demora durante todo o intervalo. O tempo necessário para a instância responder não afeta o intervalo para a próxima verificação de integridade. Se a verificação de integridade exceder as falhas consecutivas de UnhealthyThresholdCount, o load balancer tirará a instância de serviço. Quando as verificações de integridade excederem os sucessos consecutivos de HealthyThresholdCount, o load balancer colocará a instância de volta em serviço.

Uma verificação de integridade HTTP/HTTPS será bem-sucedida se a instância retornar um código de resposta 200 dentro do intervalo de verificação de integridade. Uma verificação de integridade TCP será bem-sucedida se a conexão TCP for bem-sucedida. Uma verificação de integridade SSL será bem-sucedida se um handshake for bem-sucedido.

Atualizar a configuração de verificação de integridade

Você pode atualizar a configuração de verificação de integridade para o load balancer a qualquer momento.

Para atualizar a configuração de verificação de integridade do seu 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 seu load balancer.
4. Na guia Verificação de integridade, selecione Editar verificação de integridade.
5. Na página Configurar verificação de integridade, atualize a configuração conforme necessário.

6. Escolha Save (Salvar).

Para atualizar a configuração de verificação de integridade do seu load balancer usando a AWS CLI

Use o comando configure-health-check:

```
aws elb configure-health-check --load-balancer-name my-load-balancer --health-check
 Target=HTTP:80/path,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Verificar a integridade das suas instâncias

Você pode verificar o status de integridade das suas instâncias registradas.

Para verificar o status da integridade das suas instâncias 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 seu load balancer.
4. Na guia Descrição, o Status indica quantas instâncias estão em serviço.
5. Na guia Instâncias, a coluna Status indica o status de cada instância.

Para verificar o status da integridade das suas instâncias usando a AWS CLI

Use o comando describe-instance-health:

```
aws elb describe-instance-health --load-balancer-name my-load-balancer
```

Solucionar problemas das verificações de integridade

Suas instâncias registradas podem apresentar falha na verificação de integridade do load balancer por vários motivos. Os motivos mais comuns para ocorrer falha em uma verificação de integridade são quando as instâncias EC2 fecham conexões para o load balancer ou quando o tempo limite da resposta das instâncias EC2 é atingido. Para obter informações sobre possíveis causas e etapas que você possa tomar para resolver problemas de verificação de integridade com falha, consulte Solução dos problemas de um balanceador de carga clássico: verificações de integridade (p. 120).

Configurar grupos de segurança para seu balanceador de carga clássico

Um security group atua como um firewall que controla o tráfego permitido de e para uma ou mais instâncias. Quando você executa uma instância EC2, pode associar um ou mais security groups com ela. Para cada security group, você adiciona uma ou mais regras para permitir o tráfego. Você pode modificar as regras para um security group a qualquer momento; as novas regras são aplicadas automaticamente a todas as instâncias associadas ao security group. Para obter mais informações, consulte Grupos de segurança do Amazon EC2 no Manual do usuário do Amazon EC2 para instâncias do Linux.

Há uma diferença significativa entre a maneira como balanceadores de carga clássicos oferecem suporte a grupos de segurança no EC2-Classic e em uma VPC. No EC2-Classic, o load balancer fornece um grupo de segurança de origem especial que você pode usar para garantir que as instâncias recebam tráfego somente do seu load balancer. Você não pode modificar esse security group de origem. Em uma VPC, você fornece o security group para seu load balancer, que permite que você escolha as portas e

protocolos a serem permitidos. Por exemplo, você pode abrir conexões ICMP (Internet Control Message Protocol) para o load balancer responder às solicitações de ping (no entanto, as solicitações de ping não são encaminhadas a nenhuma instância).

No EC2-Classic e em uma VPC, você deve garantir que os security groups das suas instâncias permitam que o load balancer se comunique com suas instâncias na porta de listener e na porta de verificação de integridade. Em uma VPC, os security groups e as listas de controle de acesso (ACL) à rede devem permitir tráfego em ambas as direções sobre essas portas.

Tópicos

- Grupos de segurança para balanceadores de carga em uma VPC (p. 20)
- Grupos de segurança para instâncias em uma VPC (p. 22)
- ACLs da rede dos balanceadores de carga de uma VPC (p. 22)
- Grupos de segurança para instâncias do EC2-Classic (p. 24)

Grupos de segurança para balanceadores de carga em uma VPC

Ao usar o AWS Management Console para criar um load balancer em uma VPC, você pode escolher um security group existente para a VPC ou criar um novo security group para a VPC. Se você escolher um security group existente, ele deverá permitir tráfego em ambas as direções ao listener e às portas de verificação de integridade para o load balancer. Se você optar por criar um security group, o console adicionará automaticamente regras para permitir todo o tráfego para essas portas.

[VPC não padrão] Se você usar a AWS CLI ou a API para criar um load balancer em uma VPC não padrão, mas não especificar um security group, o load balancer será automaticamente associado ao security group padrão da VPC.

[VPC padrão] Se você usar a AWS CLI ou a API para criar um load balancer na sua VPC padrão, não poderá escolher um security group existente para seu load balancer. Em vez disso, o Elastic Load Balancing fornecerá um grupo de segurança com regras para permitir todo o tráfego nas portas especificadas para o balanceador de carga. O Elastic Load Balancing cria apenas um grupo de segurança por conta da AWS, com um nome do formulário default_elb_*id* (por exemplo, `default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE`). Load balancers subsequentes que você criar no VPC padrão também usarão esse security group. Leia as regras do security group para garantir que eles permitem tráfego no listener e nas portas de verificação de integridade do novo load balancer. Ao excluir seu load balancer, esse security group não será excluído automaticamente.

Se você adicionar um listener a um load balancer existente, deverá analisar seus security groups para garantir que eles permitam tráfego na porta do novo listener em ambas as direções.

Tópicos

- Regras recomendadas para os grupos de segurança do balanceador de carga (p. 20)
- Gerenciar grupos de segurança usando o console (p. 21)
- Gerenciar grupos de segurança usando a AWS CLI (p. 22)

Regras recomendadas para os grupos de segurança do balanceador de carga

Os security groups dos seus load balancers devem permitir que eles se comuniquem com suas instâncias. As regras recomendadas dependem do tipo de balanceador de carga (voltado para a Internet ou interno).

A tabela a seguir mostra as regras recomendadas para um balanceador de carga voltado para a Internet.

Inbound			
Origem	Protocolo	Intervalo de portas	Comentário
0.0.0.0/0	TCP	*listener*	Permite todo o tráfego de entrada na porta do listener do load balancer
Outbound			
Destino	Protocolo	Intervalo de portas	Comentário
security group da instância	TCP	*listener da instância*	Permitir tráfego de saída para instâncias na porta do ouvinte da instância
security group da instância	TCP	*verificação de saúde*	Permitir tráfego de saída para instâncias na porta de verificação de integridade

A tabela a seguir mostra as regras recomendadas para um balanceador de carga interno.

Inbound			
Origem	Protocolo	Intervalo de portas	Comentário
CIDR DA VPC	TCP	*listener*	Permite tráfego de entrada do CIDR da VPC na porta do listener do load balancer
Outbound			
Destino	Protocolo	Intervalo de portas	Comentário
security group da instância	TCP	*listener da instância*	Permitir tráfego de saída para instâncias na porta do ouvinte da instância
security group da instância	TCP	*verificação de saúde*	Permitir tráfego de saída para instâncias na porta de verificação de integridade

Gerenciar grupos de segurança usando o console

Use o procedimento a seguir para alterar os security groups associados com seu load balancer em uma VPC.

Para atualizar um security group atribuído ao seu load balancer

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 seu load balancer.
4. Na guia Descrição, selecione Editar security groups.

5. Na página Editar security groups, selecione ou desmarque os security groups conforme necessário.
6. Quando terminar, escolha Salvar.

Gerenciar grupos de segurança usando a AWS CLI

Use o comando apply-security-groups-to-load-balancer para associar um security group a um load balancer em uma VPC. Os security groups especificados substituem os que foram associados anteriormente.

```
aws elb apply-security-groups-to-load-balancer --load-balancer-name my-loadbalancer --
security-groups sg-53fae93f
```

Esta é uma resposta de exemplo:

```
{
  "SecurityGroups": [
     "sg-53fae93f"
  ]
}
```

Grupos de segurança para instâncias em uma VPC

Os security groups para suas instâncias devem permitir que eles se comuniquem com o load balancer. A tabela a seguir mostra as regras recomendadas.

Inbound			
Origem	Protocolo	Intervalo de portas	Comentário
security group do load balancer	TCP	*listener da instância*	Permitir tráfego do load balancer na porta do ouvinte da instância
security group do load balancer	TCP	*verificação de saúde*	Permitir tráfego do load balancer na porta de verificação de integridade

Recomendamos também que você permita a entrada de tráfego ICMP para oferecer suporte ao Path MTU Discovery. Para obter mais informações, consulte Descoberta de caminho MTU no Manual do usuário do Amazon EC2 para instâncias do Linux.

ACLs da rede dos balanceadores de carga de uma VPC

A lista de controle de acesso (ACL) da rede padrão para a VPC permite todo o tráfego de entrada e saída. Se você criar Network ACLs personalizadas, deverá adicionar regras que permitam que o load balancer e as instâncias se comuniquem.

As regras recomendadas para a sub-rede do seu balanceador de carga dependem do tipo de balanceador (voltado para a Internet ou interno).

Veja a seguir as regras recomendadas para um balanceador de carga voltado para a Internet.

Inbound			
Origem	Protocolo	Porta	Comentário
0.0.0.0/0	TCP	*listener*	Permite todo o tráfego de entrada na porta do listener do load balancer
CIDR DA VPC	TCP	1024-65535	Permitir tráfego de entrada de CIDR da VPC em portas efêmeras
Outbound			
Destino	Protocolo	Porta	Comentário
CIDR DA VPC	TCP	*listener da instância*	Permitir todo o tráfego de saída na porta do listener da instância
CIDR DA VPC	TCP	*verificação de saúde*	Permitir todo o tráfego de saída na porta de verificação de integridade
0.0.0.0/0	TCP	1024-65535	Permitir todo o tráfego de saída nas portas efêmeras

Veja a seguir as regras recomendadas para um balanceador de carga interno.

Inbound			
Origem	Protocolo	Porta	Comentário
CIDR DA VPC	TCP	*listener*	Permite tráfego de entrada do CIDR da VPC na porta do listener do load balancer
CIDR DA VPC	TCP	1024-65535	Permitir tráfego de entrada de CIDR da VPC em portas efêmeras
Outbound			
Destino	Protocolo	Porta	Comentário
CIDR DA VPC	TCP	*listener da instância*	Permitir tráfego de saída para a CIDR da VPC na porta do listener da instância
CIDR DA VPC	TCP	*verificação de saúde*	Permitir tráfego de saída para a CIDR da VPC na

			porta de verificação de integridade
CIDR DA VPC	TCP	1024-65535	Permitir tráfego de saída para a CIDR da VPC nas portas efêmeras

As regras recomendados para a sub-rede das suas instâncias dependem de se a sub-rede é pública ou privada. As regras a seguir são para uma sub-rede privada. Se suas instâncias estiverem em uma sub-rede pública, altere a origem e o destino da CIDR da VPC para `0.0.0.0/0`.

Inbound			
Origem	Protocolo	Porta	Comentário
CIDR DA VPC	TCP	*listener da instância*	Permitir tráfego de entrada da CIDR da VPC na porta do listener da instância
CIDR DA VPC	TCP	*verificação de saúde*	Permitir tráfego de entrada da CIDR da VPC na porta de verificação de integridade
Outbound			
Destino	Protocolo	Porta	Comentário
CIDR DA VPC	TCP	1024-65535	Permitir tráfego de saída para a CIDR da VPC nas portas efêmeras

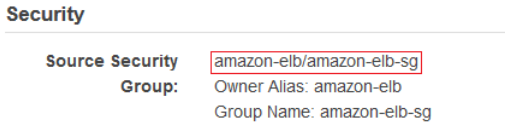
Grupos de segurança para instâncias do EC2-Classic

Para permitir a comunicação entre seu balanceador e suas instâncias iniciadas no EC2-Classic, crie uma regra de entrada para o grupo de segurança de suas instâncias que permita o tráfego de entrada de todos os endereços IP (usando o bloco CIDR `0.0.0.0/0`) ou apenas do balanceador de carga (usando o grupo de segurança de origem fornecido pelo Elastic Load Balancing).

Use o procedimento a seguir para bloquear o tráfego entre o seu load balancer e suas instâncias do EC2-Classic.

Para bloquear o tráfego entre o seu load balancer e as instâncias 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 seu load balancer.
4. Na guia Descrição, copie o nome do security group de origem.



5. Na guia Instâncias, selecione o ID de instância de uma das instâncias registradas no load balancer.
6. Na guia Descrição, em Security groups, selecione o nome do security group.
7. Na guia Entrada, selecione Editar, Adicionar regra.
8. Na coluna Tipo, selecione o tipo de protocolo. As colunas Protocolo e Intervalo de porta são preenchidas. Na coluna Fonte, selecione `Custom IP` e, em seguida, cole o nome do security group de origem que você copiou anteriormente (por exemplo, `amazon-elb/amazon-elb-sg`).
9. (Opcional) Se o seu security group tiver regras menos restritivas que a regra que você acabou de adicionar, remova a regra menos restritiva usando o ícone de exclusão.

Para bloquear o tráfego entre o seu load balancer e as instâncias usando a AWS CLI

1. Use o comando describe-load-balancer para exibir o nome e o proprietário do security group de origem para o load balancer:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

   A resposta inclui o nome e o proprietário no campo `SourceSecurityGroup`. Por exemplo:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "SourceSecurityGroup": {
                "OwnerAlias": "amazon-elb",
                "GroupName": "amazon-elb-sg"
            }
        }
    ]
}
```

2. Adicione uma regra ao security group para suas instâncias da seguinte forma:

   a. Se você não souber o nome do security group para suas instâncias, use o comando describe-instances para obter o nome e a ID do security group para a instância especificada:

```
aws ec2 describe-instances --instance-ids i-315b7e51
```

      A resposta inclui o nome e a ID do security group no campo `SecurityGroups`. Anote o nome do security group; você o usará na próxima etapa.

   b. Use o comando authorize-security-group-ingress para adicionar uma regra ao security group da sua instância para permitir tráfego do seu load balancer:

```
aws ec2 authorize-security-group-ingress --group-name my-security-group --source-
security-group-name amazon-elb-sg  --source-security-group-owner-id amazon-elb
```

3. (Opcional) Use o comando describe-security-groups para verificar se o security group tem a nova regra:

```
aws ec2 describe-security-groups --group-names my-security-group
```

   A resposta inclui uma estrutura de dados `UserIdGroupPairs` que relaciona os security groups que recebem permissões para acessar a instância.

```
{
    "SecurityGroups": [
```

```
        {
            ...
            "IpPermissions": [
                {
                    "IpRanges": [],
                    "FromPort": -1,
                    "IpProtocol": "icmp",
                    "ToPort": -1,
                    "UserIdGroupPairs": [
                        {
                            "GroupName": "amazon-elb-sg",
                            "GroupId": "sg-5a9c116a",
                            "UserId": "amazon-elb"
                        }
                    ]
                },
                {
                    "IpRanges": [],
                    "FromPort": 1,
                    "IpProtocol": "tcp",
                    "ToPort": 65535,
                    "UserIdGroupPairs": [
                        {
                            "GroupName": "amazon-elb-sg",
                            "GroupId": "sg-5a9c116a",
                            "UserId": "amazon-elb"
                        }
                    ]
                },
                {
                    "IpRanges": [],
                    "FromPort": 1,
                    "IpProtocol": "udp",
                    "ToPort": 65535,
                    "UserIdGroupPairs": [
                        {
                            "GroupName": "amazon-elb-sg",
                            "GroupId": "sg-5a9c116a",
                            "UserId": "amazon-elb"
                        }
                    ]
                },
                . . .
}
```

4. (Opcional) Se o seu security group tiver regras menos restritivas que a regra que você acabou de adicionar, use o comando revoke-security-group-ingress para remover as regras menos restritivas. Por exemplo, o comando a seguir remove uma regra que permite que o tráfego TCP de todos (intervalo CIDR `0.0.0.0/0`):

```
aws ec2 revoke-security-group-ingress --group-name my-security-group --protocol tcp --
port 80 --cidr 0.0.0.0/0
```

Adicionar ou remover zonas de disponibilidade para o seu balanceador de carga no EC2-Classic

Quando você adicionar uma zona de disponibilidade ao seu balanceador de carga, o Elastic Load Balancing criará um nó de balanceador de carga na zona de disponibilidade. Os nós do load balancer

aceitam o tráfego dos clientes e encaminham as solicitações para suas instâncias registradas íntegras em uma ou mais Zonas de disponibilidade.

Você pode configurar o load balancer no EC2-Classic para distribuir as solicitações de entrada em instâncias EC2 em uma única Zona de disponibilidade ou em várias Zonas de disponibilidade. Primeiro, execute instâncias EC2 em todas as Zonas de disponibilidade que você planeja usar. Em seguida, registre essas instâncias com o load balancer. Por fim, adicione as Zonas de disponibilidade do load balancer. Depois de adicionar uma Zona de disponibilidade, o load balancer começa a rotear as solicitações para as instâncias registradas nessa Zona de disponibilidade. Observe que você pode modificar as Zonas de disponibilidade do seu load balancer a qualquer momento.

Por padrão, o load balancer roteia solicitações uniformemente em suas Zonas de disponibilidade. Para rotear as solicitações uniformemente entre as instâncias registradas nas Zonas de disponibilidade, habilite o balanceamento de carga entre zonas. Para obter mais informações, consulte Configurar o balanceamento de carga entre zonas para seu balanceador de carga clássico (p. 73).

Você pode remover uma Zona de disponibilidade do seu load balancer temporariamente quando ela não tiver instâncias íntegras registradas ou quando você deseja solucionar problemas ou atualizar as instâncias registradas. Depois que você remover uma Zona de disponibilidade, o load balancer interromperá o roteamento das solicitações para as instâncias registradas nessa Zona de disponibilidade, mas continuará a rotear as solicitações para as instâncias registradas das Zonas de disponibilidade restantes.

Se o load balancer estiver em uma VPC, consulte Adicionar ou remover sub-redes para seu balanceador de carga clássico em uma VPC (p. 28).

Tópicos

- Adicione uma Zona de disponibilidade (p. 27)
- Remover uma Zona de disponibilidade (p. 28)

Adicione uma Zona de disponibilidade

Você pode expandir a disponibilidade da seu aplicativo para uma Zona de disponibilidade adicional. Registre as instâncias nessa Zona de disponibilidade com o load balancer e adicione a Zona de disponibilidade. Para obter mais informações, consulte Registrar ou cancelar o registro de instâncias do EC2 do seu balanceador de carga clássico (p. 31).

Para adicionar uma Zona de disponibilidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em LOAD BALANCING, escolha Load balancers.
3. Selecione seu load balancer.
4. Na guia Instâncias, selecione Editar zonas de disponibilidade.
5. Na página Adicionar e remover zonas de disponibilidade, selecione a zona de disponibilidade.
6. Escolha Save (Salvar).

Para adicionar uma Zona de disponibilidade usando a AWS CLI

Use o comando enable-availability-zones-for-load-balancer para adicionar uma Zona de disponibilidade:

```
aws elb enable-availability-zones-for-load-balancer --load-balancer-name my-loadbalancer --
availability-zones us-west-2b
```

A resposta lista todas as Zonas de disponibilidade para o load balancer. Por exemplo:

```
{
  "AvailabilityZones": [
    "us-west-2a",
    "us-west-2b"
  ]
}
```

Remover uma Zona de disponibilidade

Você pode remover uma Zona de disponibilidade do seu load balancer. Observe que depois de remover uma Zona de disponibilidade, as instâncias nessa Zona de disponibilidade serão registradas no load balancer. Para obter mais informações, consulte Registrar ou cancelar o registro de instâncias do EC2 do seu balanceador de carga clássico (p. 31).

Para remover uma Zona de disponibilidade usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em LOAD BALANCING, escolha Load balancers.
3. Selecione seu load balancer.
4. Na guia Instâncias, selecione Editar zonas de disponibilidade.
5. Na página Adicionar e remover zonas de disponibilidade, desmarque a zona de disponibilidade.
6. Escolha Save (Salvar).

Para remover uma Zona de disponibilidade usando a AWS CLI

Use o comando disable-availability-zones-for-load-balancer:

```
aws elb disable-availability-zones-for-load-balancer --load-balancer-name my-loadbalancer
 --availability-zones us-west-2a
```

A resposta lista as demais Zonas de disponibilidade para o load balancer. Por exemplo:

```
{
    "AvailabilityZones": [
        "us-west-2b"
    ]
}
```

Adicionar ou remover sub-redes para seu balanceador de carga clássico em uma VPC

Quando você adiciona uma sub-rede ao balanceador de carga, o Elastic Load Balancing cria um nó de balanceador de carga na zona de disponibilidade. Os nós do load balancer aceitam o tráfego dos clientes e encaminham as solicitações para suas instâncias registradas íntegras em uma ou mais Zonas de disponibilidade. Para load balancers em uma VPC, recomendamos que você adicione uma sub-rede por Zona de disponibilidade para pelo menos duas Zonas de disponibilidade. Isso aprimora a disponibilidade do seu load balancer. Observe que você pode modificar as sub-redes para seu load balancer a qualquer momento.

Selecione sub-redes nas mesmas Zonas de disponibilidade como suas instâncias. Se o balanceador de carga for um balanceador voltado para a Internet, você deverá selecionar sub-redes públicas para que suas instâncias backend recebam tráfego do balanceador de carga (mesmo se as instâncias backend

estiverem em sub-redes privadas). Se o load balancer for interno, recomendamos que você selecione sub-redes privadas. Para obter mais informações sobre sub-redes para seu load balancer, consulte Preparar sua VPC e instâncias do EC2 (p. 15).

Depois de adicionar uma sub-rede, o load balancer iniciará rotear solicitações às instâncias registradas na Zona de disponibilidade correspondente. Por padrão, o load balancer roteia solicitações uniformemente entre as Zonas de disponibilidade para suas sub-redes. Para rotear as solicitações uniformemente entre as instâncias registradas nas Zonas de disponibilidade para suas sub-redes, habilite o balanceamento de carga entre zonas. Para obter mais informações, consulte Configurar o balanceamento de carga entre zonas para seu balanceador de carga clássico (p. 73).

Você pode remover uma sub-rede do seu load balancer temporariamente quando sua Zona de disponibilidade não tiver instâncias íntegras registradas ou quando você deseja solucionar problemas ou atualizar as instâncias registradas. Depois que você remover uma sub-rede, o load balancer interromperá o roteamento das solicitações para as instâncias registradas nessa Zona de disponibilidade, mas continuará a rotear as solicitações para as instâncias registradas das Zonas de disponibilidade das sub-redes restantes.

Se o load balancer estiver no EC2-Classic, consulte Adicionar ou remover zonas de disponibilidade para o seu balanceador de carga no EC2-Classic (p. 26).

Tópicos

- Requirements (p. 29)
- Adicionar uma sub-rede (p. 29)
- Remover uma sub-rede (p. 30)

Requirements

Quando você atualizar as sub-redes para seu load balancer, deverá cumprir os seguintes requisitos:

- O load balancer deve ter no mínimo uma sub-rede em todos os momentos.
- Você pode adicionar no máximo uma sub-rede por Zona de disponibilidade.
- Não é possível adicionar uma sub-rede da Zona local.

Como não existem APIs separadas para adicionar e remover sub-redes de um load balancer, considere a ordem de operações cuidadosamente ao trocar a sub-redes atuais para novas sub-redes, a fim de atender a esses requisitos. Além disso, você deve adicionar temporariamente uma sub-rede da outra Zona de disponibilidade se precisar trocar todas as sub-redes para o load balancer. Por exemplo, se o load balancer tiver uma única Zona de disponibilidade e você precisar trocar sua sub-rede por outra sub-rede, você deverá primeiro adicionar uma sub-rede de uma segunda Zona de disponibilidade. Em seguida, você pode remover a sub-rede na Zona de disponibilidade original (sem precisar descer para uma sub-rede), adicionar uma nova sub-rede na Zona de disponibilidade original (sem exceder uma sub-rede por Zona de disponibilidade) e, em seguida, remover a sub-rede da segunda Zona de disponibilidade (se ela só for necessária para realizar a troca).

Adicionar uma sub-rede

Você pode expandir a disponibilidade do seu load balancer para uma sub-rede adicional. Registre-se a instâncias nessa sub-rede com o load balancer e, em seguida, anexe uma sub-rede para o load balancer que está na mesma Zona de disponibilidade que as instâncias. Para obter mais informações, consulte Registrar ou cancelar o registro de instâncias do EC2 do seu balanceador de carga clássico (p. 31).

Para adicionar uma sub-rede ao seu 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 seu load balancer.
4. No painel inferior, selecione a guia Instâncias.
5. Selecione Adicionar zonas de disponibilidade.
6. Em Sub-redes disponíveis, selecione a sub-rede usando o ícone de adição (+). A sub-rede é movida sob Sub-redes selecionadas.

   Observe que você só pode selecionar no máximo uma subnet por Zona de disponibilidade. Se você selecionar uma sub-rede de uma Zona de disponibilidade onde já houver uma sub-rede selecionada, essa sub-rede substituirá a sub-rede atualmente selecionada por essa Zona de disponibilidade.
7. Escolha Save (Salvar).

Para adicionar uma sub-rede ao seu load balancer usando a CLI

Use o comando attach-load-balancer-to-subnets para adicionar duas sub-redes ao load balancer:

```
aws elb attach-load-balancer-to-subnets --load-balancer-name my-load-balancer --
subnets subnet-dea770a9 subnet-fb14f6a2
```

A resposta lista todas as sub-redes para o load balancer. Por exemplo:

```
{
    "Subnets": [
        "subnet-5c11033e",
        "subnet-dea770a9",
        "subnet-fb14f6a2"
    ]
}
```

Remover uma sub-rede

Você pode remover uma sub-rede do seu load balancer. Observe que, depois de remover uma sub-rede, as instâncias da sub-rede permanecerão registradas no load balancer. Para obter mais informações, consulte Registrar ou cancelar o registro de instâncias do EC2 do seu balanceador de carga clássico (p. 31).

Para remover uma sub-rede 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 seu load balancer.
4. No painel inferior, selecione a guia Instâncias.
5. Selecione Adicionar zonas de disponibilidade.
6. Em Sub-redes selecionadas, remova a sub-rede usando o ícone de exclusão (-). A sub-rede é movida para Sub-redes disponíveis.
7. Escolha Save (Salvar).

Para remover uma sub-rede usando a AWS CLI

Use o comando detach-load-balancer-from-subnets para remover as sub-redes especificadas do load balancer especificado:

```
aws elb detach-load-balancer-from-subnets --load-balancer-name my-loadbalancer --
subnets subnet-450f5127
```

A resposta lista as sub-redes restantes do load balancer. Por exemplo:

```
{
    "Subnets": [
        "subnet-15aaab61"
    ]
}
```

Registrar ou cancelar o registro de instâncias do EC2 do seu balanceador de carga clássico

Registrando uma instância EC2 a adiciona ao seu load balancer. O load balancer monitora continuamente a integridade das instâncias registradas em suas Zonas de disponibilidade habilitadas e roteia solicitações para as instâncias que estão íntegras. Se a demanda nas suas instâncias aumentar, você poderá registrar instâncias adicionais com o load balancer para lidar com a demanda.

Cancelar o registro de uma instância EC2 a remove do seu load balancer. O load balancer interrompe as solicitações para a instância assim que o registro for cancelado. Se a demanda diminuir, ou se você precisar fazer manutenção nas suas instâncias, é possível cancelar o registro delas pelo load balancer. Uma instância cujo registro é cancelado permanece em execução, mas deixa de receber tráfego do load balancer, e você pode registrá-la com o load balancer novamente quando estiver pronto.

Quando você cancelar o registro de uma instância, o Elastic Load Balancing esperará até que as solicitações em andamento tenham sido concluídas, se a descarga da conexão estiver habilitada. Para obter mais informações, consulte Configurar a descarga da conexão para seu balanceador de carga clássico (p. 76).

Se o balanceador de carga estiver anexado a um grupo do Auto Scaling, as instâncias do grupo serão registradas automaticamente no balanceador de carga. Se você desvincular um balanceador de carga de seu grupo do Auto Scaling, as instâncias do grupo terão o registro cancelado.

O Elastic Load Balancing registra a instância do EC2 em seu balanceador de carga usando seu endereço IP.

[EC2-VPC] Quando você registrar uma instância com uma interface de rede elástica (ENI) anexada, o load balancer roteará solicitações para o endereço IP principal da interface primária (eth0) da instância.

Tópicos

- Prerequisites (p. 31)
- Registrar uma instância (p. 32)
- Visualize as instâncias registradas em um balanceador de carga (p. 32)
- Determine o balanceador de carga para uma instância registrada (p. 33)
- Cancelar o registro de uma instância (p. 33)

Prerequisites

A instância deve estar em execução na mesma rede que o load balancer (EC2-Classic ou a mesma VPC). Se você tiver instâncias do EC2-Classic e um load balancer em uma VPC com o ClassicLink ativado,

poderá vincular as instâncias do EC2-Classic a essa VPC e, em seguida, registrá-las no load balancer da VPC.

Registrar uma instância

Quando estiver pronto, registre sua instância com o load balancer. Se a instância estiver em uma Zona de disponibilidade habilitada para o load balancer, ela estará pronta para receber tráfego do load balancer assim que ele passar pelo número necessário de verificações de integridade.

Para registrar suas instâncias 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 seu load balancer.
4. No painel inferior, selecione a guia Instâncias.
5. Selecione Editar instâncias.
6. Selecione a instância a ser registrada com seu load balancer.
7. Escolha Save (Salvar).

Para registrar suas instâncias usando a AWS CLI

Use o comando register-instances-with-load-balancer:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --
instances i-4e05f721
```

Veja a seguir um exemplo de resposta que lista as instâncias registradas no load balancer:

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        },
        {
            "InstanceId": "i-4e05f721"
        }
    ]
}
```

Visualize as instâncias registradas em um balanceador de carga

Use o seguinte comando describe-load-balancers para listar as instâncias registradas no balanceador de carga especificado:

```
aws elb describe-load-balancers --load-balancer-names my-load-balancer --output text --
query "LoadBalancerDescriptions[*].Instances[*].InstanceId"
```

A seguir está um exemplo de saída:

```
i-e905622e
i-315b7e51
```

```
i-4e05f721
```

Determine o balanceador de carga para uma instância registrada

Use o seguinte comando describe-load-balancers para obter o nome do balanceador de carga no qual a instância especificada está registrada:

```
aws elb describe-load-balancers --output text --query "LoadBalancerDescriptions[?
Instances[?InstanceId=='i-e905622e']].[LoadBalancerName]"
```

A seguir está um exemplo de saída:

```
my-load-balancer
```

Cancelar o registro de uma instância

Você pode cancelar uma instância do seu load balancer se não precisar mais da capacidade ou se precisar fazer manutenção na instância.

Se o balanceador de carga estiver anexado a um grupo do Auto Scaling, desanexar a instância do grupo também cancelará o seu registro no balanceador de carga. Para obter mais informações, consulte Desvincular instâncias do EC2 do grupo do Auto Scaling no Manual do usuário do Amazon EC2 Auto Scaling.

Para cancelar o registro das suas instâncias 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 seu load balancer.
4. No painel inferior, selecione a guia Instâncias.
5. Na coluna da instância Ações, selecione Remover do load balancer.
6. Quando a confirmação for solicitada, selecione Sim, remover.

Para cancelar o registro das suas instâncias usando a AWS CLI

Use o comando deregister-instances-from-load-balancer:

```
aws elb deregister-instances-from-load-balancer --load-balancer-name my-loadbalancer --
instances i-4e05f721
```

Veja a seguir um exemplo de resposta que lista as instâncias restantes registradas no load balancer:

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        }
    ]
}
```

Listeners para seu balanceador de carga clássico

Antes de começar a usar o Elastic Load Balancing, é preciso configurar um ou mais listeners para seu balanceador de carga clássico. Um listener é um processo que verifica se há solicitações de conexão. Ele é pré-configurado com um protocolo e uma porta para conexões front-end (cliente para load balancer), além de protocolo e uma porta para conexões back-end (load balancer para instância back-end).

O Elastic Load Balancing suporta os seguintes protocolos:

- HTTP
- HTTPS (HTTP seguro)
- TCP
- SSL (TCP seguro)

O protocolo HTTPS utiliza o protocolo SSL para estabelecer conexões seguras sobre a layer HTTP. Você também pode usar o protocolo SSL para estabelecer conexões seguras sobre a layer TCP.

Se a conexão front-end usar TCP ou SSL, as conexões back-end poderão usar TCP ou SSL. Se a conexão front-end usar HTTP ou HTTPS, suas conexões back-end poderão usar HTTP ou HTTPS.

As instâncias back-end podem ouvir nas portas 1-65535.

Os load balancers podem ouvir nas seguintes portas:

- [EC2-VPC] 1-65535
- [EC2-Classic] 25, 80, 443, 465, 587, 1024-65535

Tópicos

- Protocols (p. 34)
- Listeners HTTPS/SSL (p. 35)
- Configurações do listener para balanceadores de carga clássicos (p. 36)
- Cabeçalhos HTTP e balanceadores de carga clássicos (p. 38)

Protocols

A comunicação para um aplicativo web típico passa por layers de hardware e software. Cada layer fornece uma função de comunicação específica. O controle sobre a função de comunicação é transmitido de uma layer para a seguinte, em sequência. O Open System Interconnection (OSI) define uma estrutura modelo para a implementação de um formato padrão para comunicação, chamado de protocolo, nessas layers. Para obter mais informações, consulte modelo OSI na Wikipédia.

Quando você usa o Elastic Load Balancing, precisa de uma compreensão básica da camada 4 e da camada 7. Layer 4 é a layer de transporte que descreve a conexão do Transmission Control Protocol (TCP) entre o cliente e a instância back-end, por meio do load balancer. Layer 4 é o nível mais baixo configurável para seu load balancer. Layer 7 é a layer do aplicativo que descreve o uso de conexões de Hypertext Transfer Protocol (HTTP) e HTTPS (HTTP seguro) de clientes para o load balancer e do load balancer para a instância back-end.

O protocolo Secure Sockets Layer (SSL) é usado principalmente para criptografar dados confidenciais em redes não seguras, como a Internet. O protocolo SSL estabelece uma conexão segura entre um cliente e o servidor de back-end e garante que todos os dados passados entre seu cliente e seu servidor sejam privados e íntegros.

Protocolo TCP/SSL

Quando você usa TCP (layer 4) para conexões front-end e back-end, o load balancer encaminhará a solicitação para as instâncias back-end sem modificar os cabeçalhos. Após o load balancer receber a solicitação, ele tentará abrir uma conexão TCP para a instância back-end na porta especificada na configuração do listener.

Como os load balancers interceptam tráfego entre clientes e suas instâncias back-end, os logs de acesso para a sua instância back-end contêm o endereço IP do load balancer em vez do cliente de origem. Você pode habilitar o protocolo de proxy, que adiciona um cabeçalho com as informações de conexão do cliente, como o endereço IP de origem, endereço IP de destino e números de porta. O cabeçalho é, então, enviado para a instância back-end como parte da solicitação. Você pode analisar a primeira linha na solicitação para recuperar as informações de conexão. Para obter mais informações, consulte . Configurar o suporte ao protocolo de proxy para o balanceador de carga clássico (p. 78).

Usando essa configuração, você não recebe cookies para perdurabilidade da sessão nem cabeçalhos X-Forwarded.

Protocolo HTTP/HTTPS

Quando você usa HTTP (layer 7) para conexões front-end e back-end, o load balancer analisará os cabeçalhos da solicitação e encerrará a conexão antes de enviar a solicitação para as instâncias back-end.

Para cada instância registrada e íntegra por trás de um balanceador de carga HTTP/HTTPS, o Elastic Load Balancing abrirá e manterá uma ou mais conexões TCP. Essas conexões garantem que exista sempre uma conexão estabelecida e pronta para receber solicitações HTTP/HTTPS.

As solicitações HTTP e as respostas HTTP usam campos de cabeçalho para enviar informações sobre as mensagens HTTP. O Elastic Load Balancing suporta cabeçalhos `X-Forwarded-For`. Como os load balancers interceptam o tráfego entre clientes e servidores, os logs de acesso do seu servidor contêm apenas o endereço IP do load balancer. Para ver o endereço IP do cliente, use o cabeçalho da solicitação `X-Forwarded-For`. Para obter mais informações, consulte . X-Forwarded-For (p. 38).

Quando você usa HTTP/HTTPS, pode ativar as sticky sessions no seu load balancer. Uma sticky session vincula a sessão de um usuário a uma determinada instância back-end. Isso garante que todas as solicitações vindas do usuário durante a sessão sejam enviadas para a mesma instância back-end. Para obter mais informações, consulte . Configurar sessões persistentes para seu balanceador de carga clássico (p. 81).

Nem todas os extensões de HTTP são suportadas pelo load balancer. Pode ser necessário usar um listener TCP se o load balancer não for capaz de encerrar a solicitação em decorrência de métodos, códigos de resposta ou outras implementações inesperadas de HTTP 1.0/1.1 não padrão.

Listeners HTTPS/SSL

Você pode criar um load balancer com os recursos de segurança a seguir.

Certificados do servidor SSL

Se você usar HTTPS ou SSL para suas conexões front-end, deverá implantar um certificado X.509 (certificado de servidor SSL) no seu load balancer. O load balancer descriptografa solicitações de clientes

antes de enviá-las para as instâncias back-end (conhecidas como terminação SSL). Para obter mais informações, consulte . Certificados SSL/TLS para balanceadores de carga clássicos (p. 40).

Se você não quiser que o load balancer lide com a terminação SSL (conhecida como SSL Offloading), pode usar o TCP para as conexões front-end e back-end e implantar certificados nas instâncias registradas que lidam com as solicitações.

Negociação SSL

O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez chamados cifras. No entanto, alguns casos de uso podem exigir que todos os dados da rede sejam criptografados e permitam apenas cifras específicas. Alguns padrões de conformidade de segurança (como PCI, SOX, etc.) podem exigir um conjunto específico de protocolos e cifras dos clientes para garantir que os padrões de segurança sejam atendidos. Em tais casos, você pode criar uma configuração de negociação SSL personalizada, com base em suas necessidades específicas. Sua cifras e seus protocolos devem entrar em vigor dentro de 30 segundos. Para obter mais informações, consulte . Configurações de negociação SSL para balanceadores de carga clássicos (p. 41).

Autenticação do servidor backend

Se você usar HTTPS ou SSL para suas conexões back-end, poderá habilitar a autenticação das suas instâncias registradas. Então, você poderá usar o processo de autenticação para garantir que as instâncias aceitem apenas comunicação criptografada, e para garantir que cada instância registrada tenha a chave pública correta.

Para obter mais informações, consulte Configurar autenticação do servidor back-end (p. 59).

Configurações do listener para balanceadores de carga clássicos

As tabelas a seguir resumem as configurações do listener que podem ser usadas para configurar os balanceadores de carga clássicos.

Balanceador de carga HTTP/HTTPS

Caso de uso	Protocolo de front-end	Opções de front-end	Protocolo de backend	Opções de backend	Observações
Load balancer HTTP básico	HTTP	NA	HTTP	NA	• Oferece suporte para X-Forwarded headers (Cabeçalhos X-Forwarded) (p. 38)
Proteja o site ou a aplicação usando o Elastic Load Balancing para descarregar a	HTTPS	Negociação SSL (p. 41)	HTTP	NA	• Oferece suporte para X-Forwarded headers (Cabeçalhos X-Forwarded) (p. 38)

Caso de uso	Protocolo de front-end	Opções de front-end	Protocolo de backend	Opções de backend	Observações
descriptografia SSL					• Exige um certificado SSL (p. 40) implantado no load balancer
Proteja o site ou o aplicativo usando criptografia de ponta a ponta	HTTPS	Negociação SSL (p. 41)	HTTPS	Autenticação de back-end	• Oferece suporte para X-Forwarded headers (Cabeçalhos X-Forwarded) (p. 38) • Exige certificados SSL (p. 40) implantados no load balancer e instâncias registradas

Balanceador de carga TCP/SSL

Caso de uso	Protocolo de front-end	Opções de front-end	Protocolo de backend	Opções de backend	Observações
Load balancer TCP básico	TCP	NA	TCP	NA	• Compatível com cabeçalho de protocolo de proxy (p. 78)
Proteja o site ou a aplicação usando o Elastic Load Balancing para descarregar a descriptografia SSL	SSL	Negociação SSL (p. 41)	TCP	NA	• Exige um certificado SSL (p. 40) implantado no load balancer • Compatível com cabeçalho de protocolo de proxy (p. 78)
Proteja o site ou a aplicação usando criptografia de ponta a ponta com o Elastic Load Balancing	SSL	Negociação SSL (p. 41)	SSL	Autenticação de back-end	• Exige certificados SSL (p. 40) implantados no load balancer e instâncias registradas

Caso de uso	Protocolo de front-end	Opções de front-end	Protocolo de backend	Opções de backend	Observações
					• Não insira cabeçalhos SNI nas conexões SSL do back-end • Não é compatível com cabeçalho de protocolo de proxy

Cabeçalhos HTTP e balanceadores de carga clássicos

As solicitações HTTP e as respostas HTTP usam campos de cabeçalho para enviar informações sobre as mensagens HTTP. Os campos de cabeçalho são pares de nome-valor separados por dois pontos e separados por um retorno de carro (CR) e um avanço de linha (LF). Um conjunto padrão de campos de cabeçalho HTTP está definido na RFC 2616, Cabeçalhos de mensagem. Há também cabeçalhos HTTP não padrão disponíveis (e adicionados automaticamente), que são amplamente usados pelas aplicações. Alguns dos cabeçalhos HTTP não padrão possuem um prefixo `X-Forwarded`. Os balanceadores de carga clássicos são compatíveis com os seguintes cabeçalhos `X-Forwarded`.

Para obter mais informações sobre conexões HTTP, consulte Roteamento de solicitação no Manual do usuário do Elastic Load Balancing.

Prerequisites

- Confirme se as configurações do seu listener são compatíveis com cabeçalhos X-Forwarded. Para obter mais informações, consulte . Configurações do listener para balanceadores de carga clássicos (p. 36).
- Configure o servidor web para registrar em log os endereços IP do cliente.

Cabeçalhos X-Forwarded

- X-Forwarded-For (p. 38)
- X-Forwarded-Proto (p. 39)
- X-Forwarded-Port (p. 39)

X-Forwarded-For

O cabeçalho de solicitação `X-Forwarded-For` é adicionado automaticamente e ajuda você a identificar o endereço IP de um cliente quando usar um balanceador de carga HTTP ou HTTPS. Como os load balancers interceptam o tráfego entre clientes e servidores, os logs de acesso do seu servidor contêm apenas o endereço IP do load balancer. Para ver o endereço IP do cliente, use o cabeçalho da solicitação `X-Forwarded-For`. O Elastic Load Balancing armazena o endereço IP do cliente no cabeçalho de solicitação `X-Forwarded-For` e encaminha o cabeçalho para o seu servidor. Se o cabeçalho de solicitação `X-Forwarded-For` não estiver incluído na solicitação, o balanceador de carga criará um com

o endereço IP do cliente como o valor da solicitação. Caso contrário, o balanceador de carga anexará o endereço IP do cliente ao cabeçalho existente e encaminhará o cabeçalho para o seu servidor. O cabeçalho de solicitação `X-Forwarded-For` pode conter vários endereços IP separados por vírgula. O endereço mais à esquerda é o IP do cliente, onde a solicitação foi feita pela primeira vez. Ele é seguido por quaisquer identificadores de proxy subsequentes em cadeia.

O cabeçalho de solicitação `X-Forwarded-For` leva a seguinte forma:

```
X-Forwarded-For: client-ip-address
```

Veja a seguir um exemplo de cabeçalho de solicitação `X-Forwarded-For` para um cliente com o endereço IP `203.0.113.7`.

```
X-Forwarded-For: 203.0.113.7
```

Veja a seguir um exemplo de cabeçalho de solicitação `X-Forwarded-For` para um cliente com o endereço IPv6 `2001:DB8::21f:5bff:febf:ce22:8a2e`.

```
X-Forwarded-For: 2001:DB8::21f:5bff:febf:ce22:8a2e
```

X-Forwarded-Proto

O cabeçalho da solicitação `X-Forwarded-Proto` ajuda você a identificar o protocolo (HTTP ou HTTPS) que um cliente usou para se conectar ao seu load balancer. Os logs de acesso do servidor contêm apenas o protocolo usado entre o servidor e o load balancer; eles não contêm informações sobre o protocolo usado entre o cliente e o load balancer. Para determinar o protocolo usado entre o cliente e o balanceador de carga, use o cabeçalho de solicitação `X-Forwarded-Proto`. O Elastic Load Balancing armazena o protocolo usado entre o cliente e o balanceador de carga no cabeçalho da solicitação `X-Forwarded-Proto` e encaminha o cabeçalho para seu servidor.

O aplicativo ou o site podem usar o protocolo armazenado no cabeçalho da solicitação `X-Forwarded-Proto` para renderizar uma resposta que redireciona para o URL apropriado.

O cabeçalho de solicitação `X-Forwarded-Proto` leva a seguinte forma:

```
X-Forwarded-Proto: originatingProtocol
```

O exemplo a seguir contém um cabeçalho de solicitação `X-Forwarded-Proto` para uma solicitação originada do cliente como solicitação de HTTPS:

```
X-Forwarded-Proto: https
```

X-Forwarded-Port

O cabeçalho de solicitação `X-Forwarded-Port` ajuda a identificar a porta de destino que o cliente usou para se conectar ao load balancer.

Listeners HTTPS para seu balanceador de carga clássico

Você pode criar um load balancer que use o protocolo SSL/TLS para conexões criptografadas (também conhecido como SSL offload). Esse recurso permite a criptografia de tráfego entre o load balancer e os clientes que iniciam sessões HTTPS e para conexões entre seu load balancer e suas instâncias EC2.

O Elastic Load Balancing usa configurações de negociação de Secure Sockets Layer (SSL), conhecidas como políticas de segurança, para negociar conexões entre os clientes e o balanceador de carga. Quando você usa HTTPS/SSL para suas conexões front-end, pode usar uma política de segurança predefinida ou personalizada. É preciso implantar um certificado SSL no seu load balancer. O load balancer usa esse certificado para encerrar a conexão e, em seguida, descriptografa solicitações dos clientes antes de enviá-las às instâncias. O load balancer usa um pacote de criptografia estático para conexões back-end. Você também pode optar por habilitar a autenticação em suas instâncias.

O Elastic Load Balancing não oferece suporte a Server Name Indication (SNI) no seu balanceador de carga. Você pode usar uma das duas alternativas:

- Implantar um certificado no load balancer e adicionar um Subject Alternative Name (SAN, Nome alternativo) para cada website adicional. Os SANs permitem que você proteja vários nomes de host usando um único certificado. Fale com seu provedor de certificados para obter mais informações sobre o número de SANs suportados por certificado e como adicionar e remover SANs.
- Use listeners de TCP na porta 443 para conexões front-end e back-end. O load balancer passa a solicitação como está, para que você possa lidar com o encerramento HTTPS da instância do EC2.

Tópicos

- Certificados SSL/TLS para balanceadores de carga clássicos (p. 40)
- Configurações de negociação SSL para balanceadores de carga clássicos (p. 41)
- Criar um balanceador de carga clássico com um listener HTTPS (p. 48)
- Configurar um listener HTTPS para seu balanceador de carga clássico (p. 62)
- Substituir o certificado SSL do seu balanceador de carga clássico (p. 65)
- Atualizar a configuração de negociação SSL do seu balanceador de carga clássico (p. 67)

Certificados SSL/TLS para balanceadores de carga clássicos

Se você usar HTTPS (SSL ou TLS) para o listener front-end, deverá implantar um certificado SSL/TLS no seu load balancer. O load balancer usa o certificado para encerrar a conexão e, em seguida, descriptografa solicitações dos clientes antes de enviá-las às instâncias.

Os protocolos SSL e TLS usam um certificado X.509 (certificado de servidor SSL/TLS) para autenticar tanto o cliente quanto o aplicativo back-end. Um certificado X.509 é uma forma digital de identificação emitida por uma autoridade certificadora (CA) e contém informações de identificação, período de validade, chave pública, número de série e assinatura digital do emissor.

Você pode criar um certificado usando o AWS Certificate Manager ou uma ferramenta que ofereça suporte aos protocolos SSL e TLS, como OpenSSL. Você especificará esse certificado ao criar ou atualizar um listener HTTPS para seu load balancer. Quando você cria um certificado para uso com seu load balancer, é necessário especificar um nome de domínio.

Criar ou importar um certificado SSL/TLS usando o AWS Certificate Manager

Recomendamos que você use o AWS Certificate Manager (ACM) para criar ou importar certificados para o balanceador de carga. O ACM se integra ao Elastic Load Balancing para que você possa implantar o certificado em seu balanceador de carga. Para implantar um certificado em seu balanceador de carga, o certificado deverá estar na mesma região que o balanceador de carga. Para obter mais informações, consulte Solicitar um certificado público ou Importar certificados no Manual do usuário do AWS Certificate Manager.

Para permitir que um usuário do IAM implante o certificado em seu balanceador de carga usando o AWS Management Console, você deve permitir o acesso à ação da API `ListCertificates` do ACM. Para obter mais informações, consulte Listar certificados no Manual do usuário do AWS Certificate Manager.

> Important
>
> Não é possível instalar certificados com chaves RSA de 4.096 bits ou chaves EC no balanceador de carga por meio de integração com o ACM. É necessário fazer upload dos certificados com chaves RSA de 4.096 bits ou chaves EC no IAM para usá-los com o balanceador de carga.

Importar um certificado SSL/TLS usando o IAM

Se não estiver usando o ACM, você pode usar ferramentas SSL/TLS, como OpenSSL, para criar uma solicitação de assinatura de certificado (CSR), obter a assinatura de um CA no CSR para produzir um certificado e fazer upload do certificado no AWS Identity and Access Management (IAM). Para obter mais informações sobre a upload de certificados no IAM, consulte Trabalhar com certificados de servidor no Manual do usuário do IAM.

Configurações de negociação SSL para balanceadores de carga clássicos

O Elastic Load Balancing usa uma configuração de negociação com Secure Sockets Layer (SSL), conhecida como política de segurança, para negociar conexões SSL entre um cliente e o balanceador de carga. A política de segurança é uma combinação de protocolos SSL, cifras SSL e a opção Preferência ditada pelo servidor. Para obter mais informações sobre como configurar uma conexão SSL para seu load balancer, consulte Listeners para seu balanceador de carga clássico (p. 34).

Tópicos

- Políticas de segurança (p. 41)
- Protocolos SSL (p. 42)
- Preferência ditada pelo servidor (p. 42)
- Codificações SSL (p. 43)
- Políticas de segurança SSL predefinidas para balanceadores de carga clássicos (p. 45)

Políticas de segurança

Uma política de segurança determina quais cifras e protocolos são suportados nas negociações SSL entre um cliente e um load balancer. Você pode configurar os balanceadores de carga clássicos para usar políticas de segurança predefinidas ou personalizadas.

Observe que um certificado fornecido pelo AWS Certificate Manager (ACM) contém uma chave pública RSA. Portanto, você deve incluir um pacote de criptografia que use RSA na sua política de segurança, caso use um certificado fornecido pelo ACM. Caso contrário, a conexão TLS falhará.

Políticas de segurança predefinidas

Os nomes das políticas de segurança predefinidas mais recentes incluem informações da versão com base no ano e no mês em que foram lançadas. Por exemplo, a política de segurança padrão predefinida é `ELBSecurityPolicy-2016-08`. Sempre que uma nova política de segurança predefinido for liberado, você pode atualizar sua configuração para usá-la.

Para obter informações sobre os protocolos e cifras habilitados para as políticas de segurança predefinidas, consulte Políticas de segurança SSL predefinidas (p. 45).

Políticas de segurança personalizadas

Você pode criar uma configuração de negociação personalizada com as cifras e os protocolos de que você precisa. Por exemplo: alguns padrões de conformidade de segurança (como PCI e SOC) podem exigir um conjunto específico de protocolos e cifras para garantir que os padrões de segurança sejam atendidos. Nesses casos, você pode criar uma política de segurança personalizada para atender a esses padrões.

Para obter informações sobre a criação de uma política de segurança personalizada, consulte Atualizar a configuração de negociação SSL do seu balanceador de carga clássico (p. 67).

Protocolos SSL

O protocolo SSL estabelece uma conexão segura entre um cliente e um servidor, além de garantir que todos os dados passados entre o cliente e o load balancer sejam privados.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS) são protocolos de criptografia usados para criptografar dados confidenciais em redes não seguras, como a Internet. O protocolo TLS é uma versão mais recente do protocolo SSL. Na documentação do Elastic Load Balancing, nós nos referimos à documentação dos protocolos SSL e TLS como protocolo SSL.

Protocolos SSL

As versões a seguir do protocolo SSL são suportadas:

- TLS 1.2
- TLS 1.1
- TLS 1.0
- SSL 3.0

Protocolo SSL defasado

Se você tiver habilitado o protocolo SSL 2.0 em uma política personalizada, recomendamos atualizar sua política de segurança para a política de segurança predefinida padrão.

Preferência ditada pelo servidor

O Elastic Load Balancing é compatível com a opção Server Order Preference (Preferência de ordem de servidor) para negociar conexões entre um cliente e um balanceador de carga. Durante o processo de negociação de conexão SSL, o cliente e o load balancer apresentam uma lista de cifras e protocolos que cada um suporta, em ordem de preferência. Por padrão, a primeira lista de cifras no cliente que corresponde a qualquer uma das cifras do load balancer é selecionada para a conexão SSL. Se o load

balancer estiver configurado para oferecer suporte à Preferência ditada pelo servidor, o load balancer selecionará a primeira cifra de sua lista que estiver na lista de cifras do cliente. Isso garante que o load balancer determine qual cifra é usada para conexão SSL. Se você não ativar a Preferência ditada pelo servidor, a ordem das cifras apresentada pelo cliente será usada para negociar conexões entre o cliente e o load balancer.

Codificações SSL

Um cifra SSL é um algoritmo de criptografia que usa chaves de criptografia para criar uma mensagem codificada. Os protocolos SSL usam várias codificações SSL para criptografar dados pela Internet.

Observe que um certificado fornecido pelo AWS Certificate Manager (ACM) contém uma chave pública RSA. Portanto, você deve incluir um pacote de criptografia que use RSA na sua política de segurança, caso use um certificado fornecido pelo ACM. Caso contrário, a conexão TLS falhará.

O Elastic Load Balancing oferece suporte às seguintes codificações para uso com balanceadores de carga clássicos. Um subconjunto dessas cifras é usado pelas políticas SSL predefinidas. Todas essas cifras estão disponíveis para uso em uma política personalizada. Recomendamos que você use somente as cifras incluídas na política de segurança padrão (aquelas com um asterisco). Muitas das outras cifras não são seguras e devem ser usadas por sua conta e risco.

Ciphers

- ECDHE-ECDSA-AES128-GCM-SHA256 *
- ECDHE-RSA-AES128-GCM-SHA256 *
- ECDHE-ECDSA-AES128-SHA256 *
- ECDHE-RSA-AES128-SHA256 *
- ECDHE-ECDSA-AES128-SHA *
- ECDHE-RSA-AES128-SHA *
- DHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES256-GCM-SHA384 *
- ECDHE-RSA-AES256-GCM-SHA384 *
- ECDHE-ECDSA-AES256-SHA384 *
- ECDHE-RSA-AES256-SHA384 *
- ECDHE-RSA-AES256-SHA *
- ECDHE-ECDSA-AES256-SHA *
- AES128-GCM-SHA256 *
- AES128-SHA256 *
- AES128-SHA *
- AES256-GCM-SHA384 *
- AES256-SHA256 *
- AES256-SHA *
- DHE-DSS-AES128-SHA
- CAMELLIA128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- ECDHE-RSA-RC4-SHA
- RC4-SHA
- ECDHE-ECDSA-RC4-SHA

- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-DSS-CAMELLIA256-SHA
- CAMELLIA256-SHA
- EDH-DSS-DES-CBC3-SHA
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- DHE-RSA-CAMELLIA128-SHA
- DHE-DSS-CAMELLIA128-SHA
- ADH-AES128-GCM-SHA256
- ADH-AES128-SHA
- ADH-AES128-SHA256
- ADH-AES256-GCM-SHA384
- ADH-AES256-SHA
- ADH-AES256-SHA256
- ADH-CAMELLIA128-SHA
- ADH-CAMELLIA256-SHA
- ADH-DES-CBC3-SHA
- ADH-DES-CBC-SHA
- ADH-RC4-MD5
- ADH-SEED-SHA
- DES-CBC-SHA
- DHE-DSS-SEED-SHA
- DHE-RSA-SEED-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- IDEA-CBC-SHA
- RC4-MD5
- SEED-SHA
- DES-CBC3-MD5
- DES-CBC-MD5
- RC2-CBC-MD5
- PSK-AES256-CBC-SHA
- PSK-3DES-EDE-CBC-SHA
- KRB5-DES-CBC3-SHA
- KRB5-DES-CBC3-MD5

- PSK-AES128-CBC-SHA
- PSK-RC4-SHA
- KRB5-RC4-SHA
- KRB5-RC4-MD5
- KRB5-DES-CBC-SHA
- KRB5-DES-CBC-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-ADH-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-KRB5-RC2-CBC-SHA
- EXP-KRB5-DES-CBC-SHA
- EXP-KRB5-RC2-CBC-MD5
- EXP-KRB5-DES-CBC-MD5
- EXP-ADH-RC4-MD5
- EXP-RC4-MD5
- EXP-KRB5-RC4-SHA
- EXP-KRB5-RC4-MD5

* Essas são as cifras recomendadas e incluídas na política de segurança padrão.

Políticas de segurança SSL predefinidas para balanceadores de carga clássicos

Você pode escolher uma das políticas de segurança predefinidas para os seus ouvintes de HTTPS/SSL. Recomendamos a política de segurança predefinida padrão, `ELBSecurityPolicy-2016-08`, para fins de compatibilidade. Você pode usar uma das políticas `ELBSecurityPolicy-TLS` para atender aos requisitos de conformidade e padrões de segurança que exigem a desativação de determinadas versões do protocolo TLS. Como alternativa, você pode criar uma política de segurança personalizada. Para obter mais informações, consulte . Atualizar a configuração de negociação SSL (p. 67).

Cifras baseadas em RSA e DSA são específicas do algoritmo de assinatura usado para criar o certificado SSL. Crie um certificado SSL usando o algoritmo de assinatura baseado na cifras habilitadas para a sua política de segurança.

Se você selecionar uma política habilitada para Preferência de ordem de servidor, o balanceador de carga usará as codificações na ordem em que forem especificadas aqui para negociar conexões entre o cliente e o balanceador de carga. Caso contrário, o load balancer usará as cifras na ordem em que forem apresentadas pelo cliente.

A tabela a seguir descreve as políticas de segurança predefinidas mais recentes para balanceadores de carga clássicos, incluindo as codificações SSL e os protocolos SSL habilitados, além da política padrão, `ELBSecurityPolicy-2016-08`. O `ELBSecurityPolicy-` foi removido dos nomes de política na linha de cabeçalho para que se ajustem ao espaço.

> **Tip**
>
> Esta tabela se aplica somente aos balanceadores de carga clássicos. Para obter informações que se apliquem aos outros balanceadores de carga, consulte Políticas de segurança para

balanceadores de carga da aplicação e Políticas de segurança para balanceadores de carga da rede.

Política de segurança	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
Protocolos SSL						
Protocol-TLSv1	✓			✓	✓	✓
Protocol-TLSv1.1	✓	✓		✓	✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
Opções SSL						
Preferência ditada pelo servidor	✓	✓	✓	✓	✓	✓
Cifras SSL						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	✓		✓	✓	✓
ECDHE-RSA-AES128-SHA	✓	✓		✓	✓	✓
DHE-RSA-AES128-SHA					✓	✓

Política de segurança	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓	✓		✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓	✓		✓	✓	✓
AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
AES128-SHA256	✓	✓	✓	✓	✓	✓
AES128-SHA	✓	✓		✓	✓	✓
AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓	✓
DHE-DSS-AES128-SHA					✓	✓

Política de segurança	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
DES-CBC3-SHA				✓	✓	

Políticas de segurança predefinidas

A seguir, estão as políticas de segurança predefinidas para balanceadores de carga clássicos. Para descrever uma política predefinida, use o comando describe-load-balancer-policies.

- ELBSecurityPolicy-2016-08
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2015-05
- ELBSecurityPolicy-2015-03
- ELBSecurityPolicy-2015-02
- ELBSecurityPolicy-2014-10
- ELBSecurityPolicy-2014-01
- ELBSecurityPolicy-2011-08
- ELBSample-ELBDefaultNegotiationPolicy ou ELBSample-ELBDefaultCipherPolicy
- ELBSample-OpenSSLDefaultNegotiationPolicy ou ELBSample-OpenSSLDefaultCipherPolicy

Criar um balanceador de carga clássico com um listener HTTPS

Um load balancer leva solicitações de clientes e as distribui entre as instâncias EC2 registradas com o load balancer.

Você pode criar um load balancer que ouça tanto a porta HTTP (80) quanto a HTTPS (443). Se você especificar que o listener HTTPS envia solicitações para as instâncias na porta 80, o load balancer encerrará as solicitações e a comunicação para as instâncias não criptografadas. Se o listener HTTPS enviar solicitações para as instâncias na porta 443, a comunicação do load balancer para as instâncias será criptografada.

Se o load balancer usar uma conexão criptografada para se comunicar com as instâncias, você poderá também habilitar a autenticação das instâncias. Isso garante que o load balancer se comunique com uma instância somente se sua chave pública corresponder à chave especificada para o load balancer para essa finalidade.

Para obter informações sobre a adição de um listener HTTPS a um load balancer existente, consulte Configurar um listener HTTPS para seu balanceador de carga clássico (p. 62).

Tópicos

- Prerequisites (p. 49)
- Criar um balanceador de carga HTTPS/SSL usando o console (p. 49)
- Criar um balanceador de carga HTTPS/SSL usando a AWS CLI (p. 54)

Prerequisites

Antes de começar, certifique-se de que você atendeu aos seguintes pré-requisitos:

- Siga as etapas em Preparar sua VPC e instâncias do EC2 (p. 15).
- Execute as instâncias EC2 que você planeja registrar com seu load balancer. Os security groups dessas instâncias devem permitir tráfego do load balancer.
- As instâncias EC2 devem responder ao destino da verificação de integridade com um código de status HTTP 200. Para obter mais informações, consulte . Configurar as verificações de integridade do seu balanceador de carga clássico (p. 16).
- Se você pretende ativar a opção de keep-alive em suas instâncias EC2, recomendamos que você defina as configurações de keep-alive para, pelo menos, as configurações do tempo limite de inatividade do seu load balancer. Se você quiser garantir que o load balancer é responsável por fechar a conexões para sua instância, certifique-se de que o valor definido na sua instância para o tempo de keep-alive é maior do que a configuração de tempo limite de inatividade no load balancer. Para obter mais informações, consulte . Configurar o tempo limite de inatividade da conexão para seu balanceador de carga clássico (p. 72).
- Se você criar um listener seguro, deverá implantar um certificado de servidor SSL no load balancer. O load balancer usa o certificado para encerrar e, em seguida, descriptografar as solicitações antes de enviá-las para as instâncias. Se você não tiver um certificado SSL, pode criar um. Para obter mais informações, consulte . Certificados SSL/TLS para balanceadores de carga clássicos (p. 40).

Criar um balanceador de carga HTTPS/SSL usando o console

Para criar um load balancer HTTPS/SSL, execute as tarefas a seguir.

Tarefas

- Etapa 1: Defina seu balanceador de carga (p. 49)
- Etapa 2: Atribua grupos de segurança ao balanceador de carga em uma VPC (p. 51)
- Etapa 3: Defina as configurações de segurança (p. 51)
- Etapa 4: Configure as verificações de integridade (p. 53)
- Etapa 5: Registre instâncias do EC2 com seu balanceador de carga (p. 53)
- Etapa 6: Coloque uma marcação em seu balanceador de carga (opcional) (p. 53)
- Etapa 7: Crie e verifique seu balanceador de carga (p. 54)
- Etapa 8: Excluir o balanceador de carga (opcional) (p. 54)

Etapa 1: Defina seu balanceador de carga

Primeiro, forneça algumas informações sobre a configuração básica do load balancer, como nome, rede e um ou mais listeners.

Escuta é um processo que verifica se há solicitações de conexão. Ele é pré-configurado com um protocolo e uma porta para conexões front-end (cliente para load balancer) e um protocolo e uma porta para conexões back-end (load balancer para instância). Para obter informações sobre configuração de portas, protocolos e listeners suportados pelo Elastic Load Balancing, consulte Listeners para seu balanceador de carga clássico (p. 34).

Neste exemplo, você configura dois listeners para o load balancer. O primeiro listener aceita solicitações HTTP na porta 80 e as envia para as instâncias na porta 80 usando HTTP. O segundo listener aceita

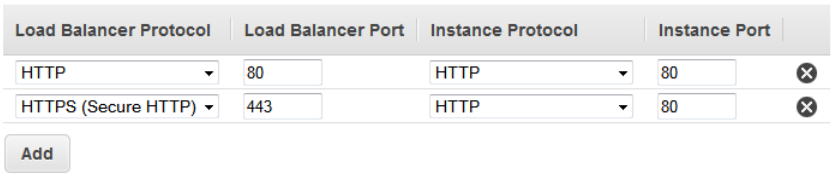
solicitações HTTPS na porta 443 e as envia para as instâncias usando HTTP na porta 80 (ou usando HTTPS na porta 443, se você deseja configurar a autenticação da instância back-end).

Para definir o load balancer

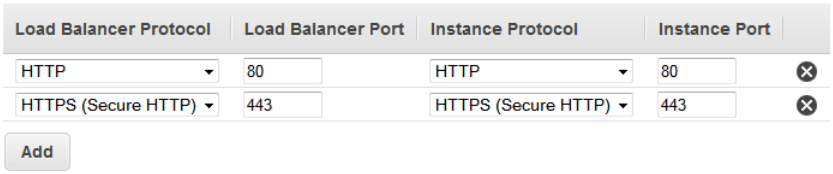
1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em LOAD BALANCING, escolha Load balancers.
3. Selecione Criar load balancer.
4. Em Select load balancer type (Selecionar tipo de balanceador de carga), escolha Classic Load Balancer (Balanceador de carga clássico).
5. Em Load Balancer name (Nome do balanceador de carga), digite um nome para o balanceador de carga.

   O nome de seu balanceador de carga clássico deve ser exclusivo dentro de seu conjunto de balanceadores de carga clássicos e para a região. Ele pode ter no máximo 32 caracteres, pode conter apenas caracteres alfanuméricos e hifens e não deve iniciar nem terminar com hífen.
6. Em Create LB inside (Criar LB interno), selecione a mesma rede que você selecionou para suas instâncias: EC2-Classic ou uma VPC específica.
7. [VPC padrão] Se você selecionou uma VPC padrão e gostaria de escolher as sub-redes para o balanceador de carga, selecione Enable advanced VPC configuration (Habilitar configuração avançada de VPC).
8. Em Configuração do listener, deixe o listener padrão e selecione Adicionar para inserir outro listener. Em Protocolo do load balancer para o novo listener, selecione HTTPS (HTTP seguro). Isso atualiza a Porta do load balancer, o Protocolo da instância e a Porta da instância.

   Por padrão, o Protocolo da instância é HTTP e a Porta da instância é 80.

   Se você deseja configurar a autenticação de back-end das instâncias (posteriormente em Etapa 3: Defina as configurações de segurança (p. 51)), altere o protocolo da instância para HTTPS (HTTP seguro). Isso também atualiza a Porta da instância.

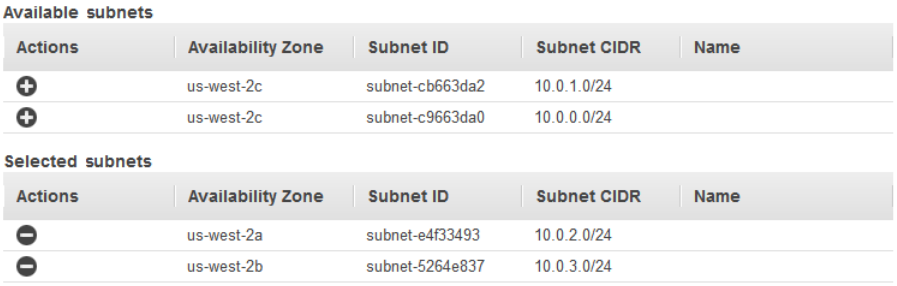
   

9. [EC2-VPC] Em Sub-redes disponíveis, selecione pelo menos uma sub-rede usando o ícone de adição. As sub-redes são movidas para Sub-redes selecionadas. Para melhorar a disponibilidade do seu load balancer, selecione sub-redes a partir de mais de uma Zona de disponibilidade.

   Note

   Se você selecionou o EC2-Classic como rede ou tem uma VPC padrão, mas não selecionou Ativar configuração avançada de VPC, você não vê a interface do usuário para selecionar sub-redes.

   Você pode adicionar no máximo uma sub-rede por Zona de disponibilidade. Se você selecionar uma segunda sub-rede de uma Zona de disponibilidade onde já houver uma sub-rede selecionada, essa sub-rede substituirá a sub-rede atualmente selecionada por essa Zona de disponibilidade.



10. Selecione Próximo: atribuir security groups.

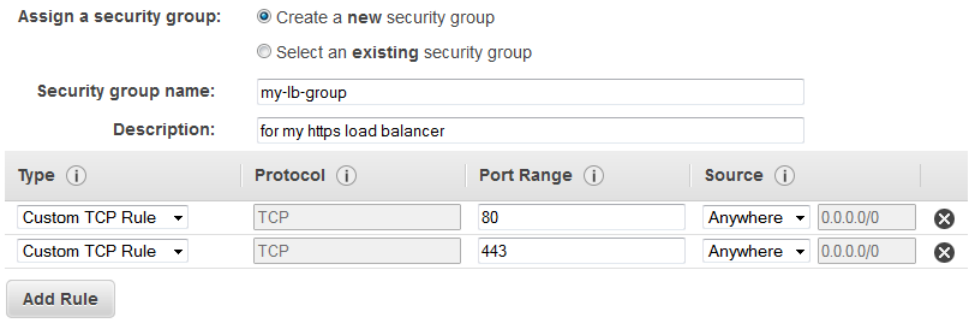
Etapa 2: Atribua grupos de segurança ao balanceador de carga em uma VPC

Caso tenha selecionado VPC como sua rede, será preciso atribuir o load balancer como security group que permita tráfego às portas especificadas para seu load balancer e as verificações de integridade para seu load balancer.

> **Note**
>
> Se você tiver selecionado EC2-Classic como sua rede, pode continuar para a próxima etapa. Por padrão, o Elastic Load Balancing fornecerá um grupo de segurança para balanceadores de carga no EC2-Classic.

Para atribuir security group ao seu load balancer

1. Na página Atribuir security groups, selecione Criar novo security group.
2. Digite um nome e uma descrição para seu security group ou mantenha o nome e a descrição padrão. Esse novo security group contém uma regra que permite o tráfego para as portas que você configurou que o load balancer usasse.



3. Selecione Next: Configure Security Settings (Próximo: Definir configurações de segurança).

Etapa 3: Defina as configurações de segurança

Ao usar HTTPS ou SSL para o listener front-end, você deverá implantar um certificado SSL no seu load balancer. O load balancer usa o certificado para encerrar a conexão e, em seguida, descriptografa solicitações dos clientes antes de enviá-las às instâncias.

Você também deve especificar uma política de segurança. O Elastic Load Balancing fornece políticas de segurança que têm configurações de negociação SSL predefinidas, ou você pode criar a sua própria política de segurança personalizada.

Se você tiver configurado HTTPS/SSL na conexão back-end, pode habilitar a autenticação das suas instâncias.

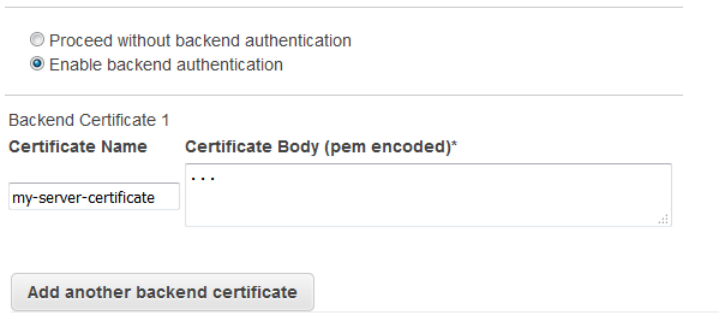
Para definir as configurações de segurança

1. Em Selecionar certificado, execute uma das seguintes ações:
   - Se você tiver criado ou importado um certificado usando o AWS Certificate Manager, selecione Choose an existing certificate from AWS Certificate Manager (ACM) (Escolher um certificado existente do AWS Certificate Manager (ACM)), em seguida, selecione o certificado no item Certificate (Certificado).
   - Se você importou um certificado usando o IAM, selecione Choose an existing certificate from AWS Identity and Access Management (IAM) (Escolher um certificado existente do AWS Identity and Access Management (IAM)), em seguida, selecione o certificado no item Certificate (Certificado).
   - Caso você precise importar um certificado, mas o ACM não esteja disponível na sua região, selecione Upload a new SSL Certificate to AWS Identity and Access Management (IAM) (Fazer upload de um novo certificado SSL no AWS Identity and Access Management (IAM)). Digite o nome do certificado. Em Chave privada, copie e cole o conteúdo do arquivo de chave privada (codificado por PEM). No Certificado de chave pública, copie e cole o conteúdo do arquivo do certificado de chave pública (codificado por PEM). Na Cadeia de certificados, copie e cole o conteúdo do arquivo da cadeia do certificado (codificado por PEM), exceto se estiver usando um certificado autoatribuído e se não for importante que os navegadores aceitem implicitamente o certificado.
2. Em Select a Cipher (Selecionar uma codificação), verifique se Predefined Security Policy (Política de segurança predefinida) está selecionada e definida como ELBSecurityPolicy-2016-08. Recomendamos que você sempre use a política de segurança predefinida mais recente. Se você precisar usar uma outra política de segurança predefinida ou criar uma política personalizada, consulte Atualizar a configuração de negociação SSL (p. 67).
3. (Opcional) Se você tiver configurado o listener HTTPS para se comunicar com instâncias usando uma conexão criptografada, pode opcionalmente configurar a autenticação das instâncias.
   a. Em Certificado back-end, selecione Ativar autenticação back-end.

      Note

      Se você não visualizar a seção Certificado back-end, volte para Configuração do listener e selecione HTTPS (HTTP seguro) em Protocolo da instância.

   b. Em Nome de certificado, digite o nome do certificado de chave pública.
   c. Em Corpo do certificado (codificado por PEM), copie e cole o conteúdo do certificado. O load balancer se comunica com uma instância somente se sua chave pública corresponder a essa chave.
   d. Para adicionar outro certificado, selecione Adicionar outro certificado back-end.



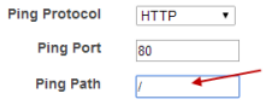
4. Selecione Próximo: configurar verificação de integridade.

Etapa 4: Configure as verificações de integridade

O Elastic Load Balancing verifica automaticamente a integridade das instâncias do EC2 registradas para seu balanceador de carga. Caso o Elastic Load Balancing encontre uma instância não íntegra, ele interromperá o envio de tráfego para a instância e roteará novamente o tráfego para instâncias íntegras. Para obter mais informações sobre como configurar verificações de integridade, consulte Configurar as verificações de integridade do seu balanceador de carga clássico (p. 16).

Para configurar verificações de integridade para suas instâncias

1. Na página Configurar verificação de integridade, selecione um protocolo e uma porta de ping. Suas instâncias EC2 devem aceitar o tráfego especificado na porta de ping especificada.
2. Em Ping Path, substitua o valor padrão pela barra única ("/"). Isso diz ao Elastic Load Balancing para enviar solicitações de verificação de integridade para a página inicial padrão do seu servidor Web, como `index.html`.



3. Deixe as outras configurações em seus valores padrão.
4. Selecione Próximo: adicionar instâncias do EC2.

Etapa 5: Registre instâncias do EC2 com seu balanceador de carga

O load balancer distribui o tráfego entre as instâncias registradas nele. Você pode selecionar as instâncias do EC2 em uma única zona de disponibilidade ou em várias zonas de disponibilidade dentro da mesma região do balanceador de carga. Para obter mais informações, consulte . Instâncias registradas para seu balanceador de carga clássico (p. 15).

> Note
>
> Quando você registrar uma instância com uma interface de rede elástica (ENI) anexada, o load balancer roteará o tráfego para o endereço IP principal da interface primária (eth0) da instância.

Para registrar instâncias EC2 com seu load balancer

1. Na página Adicionar instâncias do EC2, selecione as instâncias para registrar com o load balancer.
2. Habilite o balanceamento de carga entre zonas e a drenagem de conexão.
3. Selecione Próximo: adicionar tags.

Etapa 6: Coloque uma marcação em seu balanceador de carga (opcional)

Você pode marcar o load balancer ou avançar à próxima etapa.

Para adicionar tags ao load balancer

1. Na página Adicionar tags, especifique uma chave e um valor para a tag.
2. Para adicionar outra tag, escolha Criar tag e especifique uma chave e um valor para a tag.
3. Depois de concluir a adição de tags, escolha Revisar e criar.

Etapa 7: Crie e verifique seu balanceador de carga

Antes de criar o load balancer, revise as configurações selecionadas por você. Depois de criar o load balancer, você pode verificar se está enviando tráfego para suas instâncias EC2.

Para criar e testar seu load balancer

1. Na página Revisar, verifique suas configurações. Se você precisar fazer alterações, escolha o link correspondente para editá-las.
2. Escolha Create (Criar).
3. Depois de receber a notificação sobre a criação do load balancer, selecione Fechar.
4. Selecione o novo load balancer.
5. Na guia Descrição, verifique a linha Status. Se ele indica que algumas de suas instâncias não estão em serviço, provavelmente é porque elas ainda estão no processo de registro. Para obter mais informações, consulte . Solução dos problemas de um balanceador de carga clássico: registro de instância (p. 123).
6. (Opcional) Depois de pelo menos uma de suas instâncias EC2 entrar em serviço, você pode testar seu load balancer. Copie a string de DNS name (Nome DNS) (por exemplo, `my-load-balancer-1234567890.us-west-2.elb.amazonaws.com`) e cole-a no campo de endereço de um navegador da Web conectado à Internet. Se o load balancer estiver trabalhando, consulte a página padrão do seu servidor.

Etapa 8: Excluir o balanceador de carga (opcional)

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

Para excluir o load balancer

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.
4. Escolha Actions, Delete.
5. Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).
6. (Opcional) Depois de excluir um load balancer, as instâncias EC2 associadas ao load balancer continuam a ser executadas, e você será cobrado por cada hora cheia ou hora parcial em que mantive-los em execução. Para obter mais informações sobre como interromper ou terminar suas instâncias, consulte Parar e iniciar sua instância ou Encerrar sua instância no Manual do usuário do Amazon EC2 para instâncias do Linux.

Criar um balanceador de carga HTTPS/SSL usando a AWS CLI

Use as instruções a seguir para criar um load balancer HTTPS/SSL usando a AWS CLI.

Tarefas

- Etapa 1: Configure os listeners (p. 55)
- Etapa 2: Configure a política de segurança SSL (p. 55)
- Etapa 3: Configure a autenticação de instância backend (opcional) (p. 59)
- Etapa 4: Configure as verificações de integridade (opcional) (p. 60)

- Etapa 5: Registre as instâncias do EC2 (p. 61)
- Etapa 6: Verifique as instâncias (p. 61)
- Etapa 7: Excluir o balanceador de carga (opcional) (p. 62)

Etapa 1: Configure os listeners

Escuta é um processo que verifica se há solicitações de conexão. Ele é pré-configurado com um protocolo e uma porta para conexões front-end (cliente para load balancer) e um protocolo e uma porta para conexões back-end (load balancer para instância). Para obter informações sobre configuração de portas, protocolos e listeners suportados pelo Elastic Load Balancing, consulte Listeners para seu balanceador de carga clássico (p. 34).

Neste exemplo, você configura dois listeners para seu load balancer especificando as portas e os protocolos a serem usados para conexões front-end e back-end. O primeiro listener aceita solicitações HTTP na porta 80 e as envia para as instâncias na porta 80 usando HTTP. O segundo listener solicitações HTTPS na porta 443 e envia solicitações para instâncias usando HTTP na porta 80.

Como o segundo listener usa HTTPS para a conexão front-end, você deve implantar um certificado de servidor SSL no seu load balancer. O load balancer usa o certificado para encerrar e, em seguida, descriptografar as solicitações antes de enviá-las para as instâncias.

Para configurar listeners para o seu load balancer

1. Obtenha o Nome de recurso da Amazon (ARN) do certificado SSL. Por exemplo:

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

   ```
   arn:aws:iam::123456789012:server-certificate/my-server-certificate
   ```

2. Use o comando create-load-balancer para configurar o load balancer com os dois listeners:

   ```
   aws elb create-load-balancer --load-balancer-name my-load-balancer --listeners
    "Protocol=http,LoadBalancerPort=80,InstanceProtocol=http,InstancePort=80"
    "Protocol=https,LoadBalancerPort=443,InstanceProtocol=http,InstancePort=80,SSLCertificateId="ARN"
    --availability-zones us-west-2a
   ```

   Esta é uma resposta de exemplo:

   ```
   {
     "DNSName": "my-loadbalancer-012345678.us-west-2.elb.amazonaws.com"
   }
   ```

3. (Opcional) Use o comando describe-load-balancers para ver detalhes do seu load balancer:

   ```
   aws elb describe-load-balancers --load-balancer-name my-load-balancer
   ```

Etapa 2: Configure a política de segurança SSL

Você pode selecionar uma das políticas de segurança predefinidas ou criar a sua própria política de segurança personalizada. Caso contrário, o Elastic Load Balancing configurará o balanceador de carga

com a política de segurança predefinida padrão, `ELBSecurityPolicy-2016-08`. Recomendamos que você use a política de segurança padrão. Para obter mais informações sobre as políticas de segurança, consulte Configurações de negociação SSL para balanceadores de carga clássicos (p. 41).

Para verificar se o seu load balancer está associado à política de segurança padrão

Use o comando describe-load-balancers:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Esta é uma resposta de exemplo. Observe que `ELBSecurityPolicy-2016-08` está associado ao load balancer na porta 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Se você preferir, você pode configurar a política de segurança de SSL para seu load balancer, em vez de usar a política de segurança padrão.

(Opcional) para usar uma política de segurança SSL predefinida

1. Use o comando describe-load-balancer-policies para listar os nomes das políticas de segurança predefinidas:

   ```
   aws elb describe-load-balancer-policies
   ```

   Para obter informações sobre a configuração das políticas de segurança predefinidas, consulte Políticas de segurança SSL predefinidas (p. 45).
2. Use o comando create-load-balancer-policy para criar uma política de negociação SSL usando uma das políticas de segurança predefinidas descritas na etapa anterior:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType
--policy-attributes AttributeName=Reference-Security-Policy,AttributeValue=predefined-
policy
```

3. (Opcional) Use o comando describe-load-balancer-policies para verificar se a política foi criada:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-
name my-SSLNegotiation-policy
```

A resposta inclui a descrição da política.

4. Use o comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --
load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> O comando `set-load-balancer-policies-of-listener` substitui o conjunto atual de políticas para a porta especificada do load balancer pelo conjunto de políticas especificado. A lista `--policy-names` deve incluir todas as políticas para ser habilitada. Se você pular uma política que atualmente está ativada, ela será desativada.

5. (Opcional) Use o comando describe-load-balancers para verificar se a política foi habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Veja a seguir um exemplo de resposta mostrando que a política está habilitada na porta 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "my-SSLNegotiation-policy"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
```

```
    ]
}
```

Quando você cria uma política de segurança personalizada, deve habilitar pelo menos um protocolo e uma cifra. Cifras DSA e RSA são específicas do algoritmo de assinatura e são usadas para criar o certificado SSL. Se você já tiver seu certificado SSL, ative a cifra que foi usada para criar seu certificado. O nome da sua política personalizada não deve começar com `ELBSecurityPolicy-` ou `ELBSample-`, pois esses prefixos são reservados para os nomes das políticas de segurança predefinidas.

(Opcional) para usar uma política de segurança SSL personalizada

1. Use o comando create-load-balancer-policy para criar uma política de negociação SSL usando uma política de segurança personalizada. Por exemplo:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
 --policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType
 --policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
 AttributeName=Protocol-TLSv1.1,AttributeValue=true
 AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
 AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

2. (Opcional) Use o comando describe-load-balancer-policies para verificar se a política foi criada:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-
name my-SSLNegotiation-policy
```

   A resposta inclui a descrição da política.

3. Use o comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --
load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

   > **Note**
   >
   > O comando `set-load-balancer-policies-of-listener` substitui o conjunto atual de políticas para a porta especificada do load balancer pelo conjunto de políticas especificado. A lista `--policy-names` deve incluir todas as políticas para ser habilitada. Se você pular uma política que atualmente está ativada, ela será desativada.

4. (Opcional) Use o comando describe-load-balancers para verificar se a política foi habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

   Veja a seguir um exemplo de resposta mostrando que a política está habilitada na porta 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
```

```
                    "InstanceProtocol": "HTTP"
                },
                "PolicyNames": [
                    "my-SSLNegotiation-policy"
                ]
            },
            {
                "Listener": {
                    "InstancePort": 80,
                    "LoadBalancerPort": 80,
                    "Protocol": "HTTP",
                    "InstanceProtocol": "HTTP"
                },
                "PolicyNames": []
            }
        ],
        ...
    }
  ]
}
```

Etapa 3: Configure a autenticação de instância backend (opcional)

Se você configurar HTTPS/SSL na conexão back-end, terá a opção de configurar a autenticação das suas instâncias.

Quando você configura a autenticação de instância back-end, cria uma política de chave pública. Em seguida, você usa essa política de chave pública para criar uma política de autenticação de instância back-end. Por fim, você define a política de autenticação de instância back-end com a porta da instância para o protocolo HTTPS.

O load balancer se comunica com uma instância somente se a chave pública que a instância apresenta ao load balancer corresponder a uma chave pública na política de autenticação do seu load balancer.

Para configurar a autenticação da instância back-end

1. Use o comando a seguir para recuperar a chave pública:

```
openssl x509 -in your X509 certificate PublicKey -pubkey -noout
```

2. Use o comando create-load-balancer-policy para criar uma política de chave pública:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
name my-PublicKey-policy \
--policy-type-name PublicKeyPolicyType --policy-attributes
 AttributeName=PublicKey,AttributeValue=MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
```

```
3rrszlaEXAMPLE=
```

Note

Para especificar um valor de chave pública para `--policy-attributes`, remova a primeira e a última linha da chave pública (a linha que contém "`-----BEGIN PUBLIC KEY-----`" e a linha que contém "`-----END PUBLIC KEY-----`"). A AWS CLI não aceita caracteres de espaço em branco em `--policy-attributes`.

3. Use o comando create-load-balancer-policy para criar uma política de autenticação de instância back-end usando `my-PublicKey-policy`.

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
name my-authentication-policy --policy-type-name BackendServerAuthenticationPolicyType
 --policy-attributes AttributeName=PublicKeyPolicyName,AttributeValue=my-PublicKey-
policy
```

Você também pode usar várias políticas de chave pública. O load balancer tenta todas as chaves, uma de cada vez. Se a chave pública apresentada por uma instância corresponder a uma dessas chaves públicas, a instância será autenticada.

4. Use o comando set-load-balancer-policies-for-backend-server para definir `my-authentication-policy` para a porta da instância para HTTPS. Neste exemplo, a porta da instância é 443.

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-
loadbalancer --instance-port 443 --policy-names my-authentication-policy
```

5. (Opcional) Use o comando describe-load-balancer-policies para listar as políticas para seu load balancer:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer
```

6. (Opcional) Use o comando describe-load-balancer-policies para visualizar detalhes da política:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-
names my-authentication-policy
```

Etapa 4: Configure as verificações de integridade (opcional)

O Elastic Load Balancing verifica regularmente a integridade de cada instância do EC2 registrada com base nas verificações de integridade que você configurou. Caso o Elastic Load Balancing encontre uma instância não íntegra, ele interromperá o envio de tráfego para a instância e roteará o tráfego para instâncias íntegras. Para obter mais informações, consulte . Configurar as verificações de integridade do seu balanceador de carga clássico (p. 16).

Quando você cria seu balanceador de carga, o Elastic Load Balancing usa as configurações padrão para as verificações de integridade. Se preferir, você pode alterar a configuração da verificação de integridade do seu load balancer em vez de usar as configurações padrão.

Para configurar as verificações de integridade das suas instâncias

Use o comando configure-health-check:

```
aws elb configure-health-check --load-balancer-name my-loadbalancer --health-check
 Target=HTTP:80/ping,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Esta é uma resposta de exemplo:

```
{
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/ping",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    }
}
```

Etapa 5: Registre as instâncias do EC2

Depois de criar seu load balancer, você deve registrar suas instâncias EC2 no load balancer. Você pode selecionar as instâncias do EC2 de uma única zona de disponibilidade ou de várias zonas de disponibilidade dentro da mesma região do balanceador de carga. Para obter mais informações, consulte . Instâncias registradas para seu balanceador de carga clássico (p. 15).

Use o comando register-instances-with-load-balancer da seguinte forma:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --
instances i-4f8cf126 i-0bb7ca62
```

Esta é uma resposta de exemplo:

```
{
    "Instances": [
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

Etapa 6: Verifique as instâncias

O load balancer é utilizável assim que qualquer uma de suas instâncias registradas estiver no estado `InService`.

Para verificar o estado de suas instâncias EC2 recém-registradas, use o comando describe-instance-health a seguir:

```
aws elb describe-instance-health  --load-balancer-name my-loadbalancer --
instances i-4f8cf126 i-0bb7ca62
```

Esta é uma resposta de exemplo:

```
{
    "InstanceStates": [
        {
            "InstanceId": "i-4f8cf126",
            "ReasonCode": "N/A",
            "State": "InService",
            "Description": "N/A"
        },
        {
            "InstanceId": "i-0bb7ca62",
            "ReasonCode": "Instance",
```

```
            "State": "OutOfService",
            "Description": "Instance registration is still in progress"
        }
    ]
}
```

Se o campo `State` de uma instância for `OutOfService`, talvez seja porque suas instâncias ainda estão sendo registradas. Para obter mais informações, consulte . Solução dos problemas de um balanceador de carga clássico: registro de instância (p. 123).

Após o estado de pelo menos uma de suas instâncias ser `InService`, você poderá testar seu load balancer. Para testar seu balanceador de carga, copie o nome DNS do balanceador de carga e cole-o no campo de endereço de um navegador da Web conectado à Internet. Se o load balancer estiver trabalhando, consulte a página padrão do seu servidor HTTP.

Etapa 7: Excluir o balanceador de carga (opcional)

A exclusão de um load balancer cancela automaticamente o registro das instâncias EC2 associadas. Assim que o load balancer for excluído, as cobranças desse load balancer será interrompida. No entanto, as instâncias EC2 continuam a rodar e você continuará a ser cobrado.

Para excluir seu load balancer, use o comando delete-load-balancer a seguir:

```
aws elb delete-load-balancer --load-balancer-name my-loadbalancer
```

Para interromper suas instâncias EC2, use o comando stop-instances. Para encerrar suas instâncias EC2, use o comando terminate-instances.

Configurar um listener HTTPS para seu balanceador de carga clássico

Escuta é um processo que verifica se há solicitações de conexão. Ele é pré-configurado com um protocolo e uma porta para conexões front-end (cliente para load balancer) e um protocolo e uma porta para conexões back-end (load balancer para instância). Para obter informações sobre configuração de portas, protocolos e listeners suportados pelo Elastic Load Balancing, consulte Listeners para seu balanceador de carga clássico (p. 34).

Se você tiver um load balancer com um listener que aceita solicitações HTTP na porta 80, pode adicionar um listener que aceite solicitações HTTPS na porta 443. Se você especificar que o listener HTTPS envia solicitações para as instâncias na porta 80, o load balancer encerrará as solicitações SSL e a comunicação para as instâncias não criptografadas. Se o listener HTTPS enviar solicitações para as instâncias na porta 443, a comunicação do load balancer para as instâncias será criptografada.

Se o load balancer usar uma conexão criptografada para se comunicar com as instâncias, você poderá também habilitar a autenticação das instâncias. Isso garante que o load balancer se comunique com uma instância somente se sua chave pública corresponder à chave especificada para o load balancer para essa finalidade.

Para obter informações sobre a criação do novo listener HTTPS, consulte Criar um balanceador de carga clássico com um listener HTTPS (p. 48).

Tópicos

- Prerequisites (p. 63)
- Adicionar um listener HTTPS usando o console (p. 63)
- Adicionar um listener HTTPS usando a AWS CLI (p. 64)

Prerequisites

Para ativar o suporte HTTPS para um listener HTTPS, você deve implantar um certificado de servidor SSL no seu load balancer. O load balancer usa o certificado para encerrar e, em seguida, descriptografar as solicitações antes de enviá-las para as instâncias. Se você não tiver um certificado SSL, pode criar um. Para obter mais informações, consulte . Certificados SSL/TLS para balanceadores de carga clássicos (p. 40).

Adicionar um listener HTTPS usando o console

Você pode adicionar um listener HTTPS a um load balancer existente.

Para adicionar um listener HTTPS ao seu load balancer

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 seu load balancer.
4. Na guia Listeners, selecione Editar.
5. Na página Editar listeners, selecione Adicionar.
6. Em Protocolo do load balancer, selecione HTTPS (HTTP seguro). Isso atualiza a Porta do load balancer, o Protocolo da instância e a Porta da instância.

   Important

   Por padrão, o protocolo da instância é HTTP. Se você quiser configurar a autenticação da instâncias back-end, altere o protocolo da instância para HTTPS (HTTP seguro). Isso também atualiza a porta da instância.
7. Em Cifra, selecione Alterar. Verifique se Predefined Security Policy (Política de segurança predefinida) está selecionada e definida como ELBSecurityPolicy-2016-08. Recomendamos que você sempre use a política de segurança predefinida mais recente. Se você precisar usar uma outra política de segurança predefinida ou criar uma política personalizada, consulte Atualizar a configuração de negociação SSL (p. 67).
8. Se você já tiver um certificado implantado no seu load balancer e quiser continuar a usá-lo, pode ignorar esta etapa.

   Em Certificado SSL, selecione Alterar e, em seguida, execute uma das seguintes ações:

   - Se você criou ou importou um certificado usando o AWS Certificate Manager, selecione Choose an existing certificate from AWS Certificate Manager (ACM) (Escolher um certificado existente do AWS Certificate Manager (ACM)), selecione o certificado em Certificate (Certificado) e, em seguida, selecione Save (Salvar).

     Note

     Essa opção estará disponível apenas em regiões que suportam o AWS Certificate Manager.
   - Se você importou um certificado usando o IAM, selecione Choose an existing certificate from AWS Identity and Access Management (IAM) (Escolher um certificado existente do AWS Identity and Access Management (IAM)), selecione o certificado em Certificate (Certificado) e, em seguida, selecione Save (Salvar).
   - Caso você precise importar um certificado SSL, mas o ACM não seja suportado pela sua região, selecione Upload a new SSL Certificate to AWS Identity and Access Management (IAM) (Fazer upload de um novo certificado SSL no AWS Identity and Access Management (IAM)). Digite o nome do certificado. Em Chave privada, copie e cole o conteúdo do arquivo de chave privada (codificado por PEM). No Certificado de chave pública, copie e cole o conteúdo do arquivo do certificado de chave pública (codificado por PEM). Na Cadeia de certificados, copie e cole o conteúdo do arquivo

da cadeia do certificado (codificado por PEM), exceto se estiver usando um certificado autoatribuído e se não for importante que os navegadores aceitem implicitamente o certificado.

9. (Opcional) Selecione Adicionar para adicionar mais listeners.
10. Selecione Salvar para adicionar os listeners que você acabou de configurar.
11. (Opcional) Para configurar a autenticação de instância back-end para um load balancer existente, é preciso usar a AWS CLI ou uma API, pois essa tarefa não é suportada pelo console. Para obter mais informações, consulte Configurar autenticação de instância back-end (p. 59).

Adicionar um listener HTTPS usando a AWS CLI

Você pode adicionar um listener HTTPS a um load balancer existente.

Para adicionar um listener HTTPS ao seu load balancer usando a AWS CLI

1. Obtenha o Nome de recurso da Amazon (ARN) do certificado SSL. Por exemplo:

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

   ```
   arn:aws:iam::123456789012:server-certificate/my-server-certificate
   ```

2. Use o seguinte comando create-load balancer-listeners para adicionar um listener ao seu load balancer que aceite solicitações HTTPS na porta 443 e envie solicitações para as instâncias na porta 80 usando HTTP:

   ```
   aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
   listeners
    Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTP,InstancePort=80,SSLCertificateId=ARN
   ```

   Se você deseja configurar a autenticação de instâncias back-end, use o comando a seguir para adicionar um listener que aceite solicitações HTTPS na porta 443 e envie as solicitações para as instâncias na porta 443 usando HTTPS:

   ```
   aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
   listeners
    Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTPS,InstancePort=443,SSLCertificateId=ARN
   ```

3. (Opcional) Você pode usar o comando describe-load-balancers para exibir os detalhes atualizados do seu load balancer:

   ```
   aws elb describe-load-balancers --load-balancer-name my-load-balancer
   ```

   Esta é uma resposta de exemplo:

   ```
   {
       "LoadBalancerDescriptions": [
           {
               ...
               "ListenerDescriptions": [
                   {
                       "Listener": {
                           "InstancePort": 80,
   ```

```
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

4. (Opcional) Seu listener HTTPS foi criado usando a política de segurança padrão. Se você quiser especificar uma política de segurança predefinida diferente ou uma política de segurança personalizada, use os comandos create-load balancer-policy e set-load-balancer-policies-of-listener. Para obter mais informações, consulte . Atualizar a configuração de negociação SSL usando a AWS CLI (p. 68).
5. (Opcional) Para configurar a autenticação de instâncias back-end, use o comando set-load-balancer-policies-for-backend-server. Para obter mais informações, consulte Configurar autenticação de instância back-end (p. 59).

Substituir o certificado SSL do seu balanceador de carga clássico

Se você tiver um listener HTTPS, significa que implantou um certificado de servidor SSL no load balancer quando criou o listener. Cada certificado vem com um período de validade. Você deve garantir que renovou ou substituiu o certificado antes do fim do período de validade.

Certificados fornecidos pelo AWS Certificate Manager e implantados no seu load balancer podem ser renovados automaticamente. O ACM tenta renovar os certificados antes que eles expirem. Para obter mais informações, consulte Renovação gerenciada no Manual do usuário do AWS Certificate Manager. Se você tiver importado um certificado no ACM, deverá monitorar a data de validade do certificado e renová-lo antes que expire. Para obter mais informações, consulte Importar certificados no Manual do usuário do AWS Certificate Manager. Depois que um certificado implantado no load balancer for renovado, as novas solicitações usarão o certificado renovado.

Para substituir um certificado, você deve primeiro criar um novo certificado seguindo as mesmas etapas usadas ao criar o certificado atual. Depois você pode substituir o certificado. Depois que um certificado implantado no load balancer ser substituído, as novas solicitações usarão o novo certificado.

Observe que renovar ou substituir um certificado não afeta as solicitações já recebidas por um nó do load balancer e são pendentes de roteamento para um destino íntegro.

Tópicos

- Substituir o certificado SSL usando o console (p. 66)
- Substituir o certificado SSL usando a AWS CLI (p. 66)

Substituir o certificado SSL usando o console

Você pode substituir o certificado implantado no seu balanceador de carga por um certificado fornecido pelo ACM ou por um certificado carregado no IAM.

Para substituir o certificado SSL para um load balancer HTTPS

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 seu load balancer.
4. Na guia Listeners, em Certificado SSL, selecione Alterar.
5. Na página Selecionar certificado, execute uma das seguintes ações:
   - Se você criou ou importou um certificado usando o AWS Certificate Manager, selecione Choose an existing certificate from AWS Certificate Manager (ACM) (Escolher um certificado existente do AWS Certificate Manager (ACM)), selecione o certificado em Certificate (Certificado) e, em seguida, selecione Save (Salvar).
   - Se você importou um certificado usando o IAM, selecione Choose an existing certificate from AWS Identity and Access Management (IAM) (Escolher um certificado existente do AWS Identity and Access Management (IAM)), selecione o certificado em Certificate (Certificado) e, em seguida, selecione Save (Salvar).
   - Caso você precise importar um certificado, mas o ACM não seja suportado pela sua região, selecione Upload a new SSL Certificate to AWS Identity and Access Management (IAM) (Fazer upload de um novo certificado SSL no AWS Identity and Access Management (IAM)). Digite um nome para o certificado, copie as informações necessárias para o formulário e, em seguida, selecione Salvar. Observe que a cadeia do certificado não será necessária se o certificado for autoatribuído.

Substituir o certificado SSL usando a AWS CLI

Você pode substituir o certificado implantado no seu balanceador de carga por um certificado fornecido pelo ACM ou por um certificado carregado no IAM.

Para substituir um certificado SSL por um certificado fornecido pelo ACM

1. Use o comando request-certificate para solicitar um novo certificado:

```
aws acm request-certificate --domain-name www.example.com
```

2. Use o comando set-load-balancer-listener-ssl-certificate para definir o certificado:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Para substituir um certificado SSL por um certificado carregado no IAM

1. Se você tiver um certificado SSL, mas não o carregou, consulte Carregar um certificado do servidor no Manual do usuário do IAM.
2. Use o comando get-server-certificate para obter o ARN do certificado:

```
aws iam get-server-certificate --server-certificate-name my-new-certificate
```

3. Use o comando set-load-balancer-listener-ssl-certificate para definir o certificado:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:iam::123456789012:server-certificate/my-new-certificate
```

Atualizar a configuração de negociação SSL do seu balanceador de carga clássico

O Elastic Load Balancing fornece políticas de segurança que têm configurações de negociação SSL predefinidas para serem usadas na negociação de conexões SSL entre os clientes e o seu balanceador de carga. Se você estiver usando o protocolo HTTPS/SSL para seu listener, pode usar uma das políticas de segurança predefinidas ou usar a sua própria política de segurança personalizada.

Para obter mais informações sobre as políticas de segurança, consulte Configurações de negociação SSL para balanceadores de carga clássicos (p. 41). Para obter informações sobre as configurações das políticas de segurança fornecidas pelo Elastic Load Balancing, consulte Políticas de segurança SSL predefinidas (p. 45).

Se você criar um listener HTTPS/SSL sem associar uma política de segurança, o Elastic Load Balancing associará a política de segurança predefinida padrão, `ELBSecurityPolicy-2016-08`, a seu balanceador de carga.

Se você tiver um balanceador de carga existente com uma configuração de negociação SSL que não use os protocolos e codificações mais recentes, recomendamos que atualize o balanceador de carga para usar o ELBSecurityPolicy-2016-08. Se você preferir, pode criar uma configuração personalizada. Recomendamos enfaticamente que você teste as novas políticas de segurança antes de atualizar a configuração do seu load balancer.

Os exemplos a seguir mostram como atualizar a configuração de negociação SSL para um listener HTTPS/SSL. Observe que a alteração não afeta as solicitações recebidas por um nó do load balancer e são pendentes de roteamento para uma instância íntegra, mas a configuração atualizada será usada com as novas solicitações recebidas.

Tópicos

- Atualizar a configuração da negociação SSL usando o console (p. 67)
- Atualizar a configuração de negociação SSL usando a AWS CLI (p. 68)

Atualizar a configuração da negociação SSL usando o console

Por padrão, o Elastic Load Balancing associa a política predefinida mais recente a seu balanceador de carga. Quando uma nova política predefinida é adicionada, recomendamos que você atualize o load balancer para usar a nova política predefinida. Você também pode selecionar uma política de segurança predefinida diferente ou criar uma política personalizada.

Para atualizar a configuração de negociação SSL para um load balancer HTTPS/SSL

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 seu load balancer.

4. Na guia Listeners, em Cifra, selecione Alterar.
5. Na página Selecionar uma cifra, selecione uma política de segurança usando uma das seguintes opções:
   - (Recomendado) Selecione Predefined Security Policy (Política de segurança predefinida), mantenha a política padrão ELBSecurityPolicy-2016-08 e, em seguida, selecione Save (Salvar).
   - Selecione Política de segurança predefinida, selecione uma política predefinida diferente do padrão e, em seguida, selecione Salvar.
   - Selecione Política de segurança personalizada e habilite pelo menos um protocolo e uma cifra, da seguinte forma:

     a. Em Protocolos SSL, selecione um ou mais protocolos para habilitar.
     b. Em Opções SSL, selecione Preferência de ordem de servidor para usar a ordem listada na Políticas de segurança SSL predefinidas (p. 45) para negociação SSL.
     c. Em Cifras SSL, selecione uma ou mais cifras para habilitar. Se você já tiver um certificado SSL, deverá habilitar a cifra usada para criar o certificado, pois as cifras DSA e RSA são específicas do algoritmo de assinatura.
     d. Escolha Save (Salvar).

Atualizar a configuração de negociação SSL usando a AWS CLI

Você pode usar a política de segurança predefinida padrão, `ELBSecurityPolicy-2016-08`, uma política de segurança predefinida diferente ou uma política de segurança personalizada.

Para usar uma política de segurança SSL predefinida

1. Use o seguinte comando describe-load-balancer-policies para listar as políticas de segurança predefinidas fornecidas pelo Elastic Load Balancing. A sintaxe a ser usada dependerá do sistema operacional e do shell em uso.

   Linux

   ```
   aws elb describe-load-balancer-policies --query 'PolicyDescriptions[?
   PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}' --output table
   ```

   Windows

   ```
   aws elb describe-load-balancer-policies --query "PolicyDescriptions[?
   PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}" --output table
   ```

   A seguir está um exemplo de saída:

   ```
   ------------------------------------------
   |      DescribeLoadBalancerPolicies      |
   +----------------------------------------+
   |               PolicyName               |
   +----------------------------------------+
   |  ELBSecurityPolicy-2016-08             |
   |  ELBSecurityPolicy-TLS-1-2-2017-01     |
   |  ELBSecurityPolicy-TLS-1-1-2017-01     |
   |  ELBSecurityPolicy-2015-05             |
   |  ELBSecurityPolicy-2015-03             |
   |  ELBSecurityPolicy-2015-02             |
   |  ELBSecurityPolicy-2014-10             |
   ```

```
|  ELBSecurityPolicy-2014-01              |
|  ELBSecurityPolicy-2011-08              |
|  ELBSample-ELBDefaultCipherPolicy       |
|  ELBSample-OpenSSLDefaultCipherPolicy   |
+-----------------------------------------+
```

Para determinar quais cifras estão habilitadas para uma política, use o seguinte comando:

```
aws elb describe-load-balancer-policies --policy-names ELBSecurityPolicy-2016-08 --
output table
```

Para obter informações sobre a configuração das políticas de segurança predefinidas, consulte Políticas de segurança SSL predefinidas (p. 45).

2. Use o comando create-load-balancer-policy para criar uma política de negociação SSL usando uma das políticas de segurança predefinidas descritas na etapa anterior. Por exemplo, o comando a seguir usa a política de segurança predefinida padrão:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy  --policy-type-name SSLNegotiationPolicyType
--policy-attributes AttributeName=Reference-Security-
Policy,AttributeValue=ELBSecurityPolicy-2016-08
```

Se você excedeu o limite do número de políticas para o load balancer, use o comando delete-load-balancer-policy para excluir qualquer política não utilizada.

3. (Opcional) Use o comando describe-load-balancer-policies para verificar se a política foi criada:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-
name my-SSLNegotiation-policy
```

A resposta inclui a descrição da política.

4. Use o comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --
load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> O comando `set-load-balancer-policies-of-listener` substitui o conjunto atual de políticas para a porta especificada do load balancer pelo conjunto de políticas especificado. A lista `--policy-names` deve incluir todas as políticas para ser habilitada. Se você pular uma política que atualmente está ativada, ela será desativada.

5. (Opcional) Use o comando describe-load-balancers para verificar se a nova política é habilitada para a porta do load balancer:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

A resposta mostra que a política está habilitada na porta 443.

```
...
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
```

```
            "LoadBalancerPort": 443,
            "Protocol": "HTTPS",
            "InstanceProtocol": "HTTPS"
        },
        "PolicyNames": [
            "my-SSLNegotiation-policy"
        ]
    }
...
```

Quando você cria uma política de segurança personalizada, deve habilitar pelo menos um protocolo e uma cifra. Cifras DSA e RSA são específicas do algoritmo de assinatura e são usadas para criar o certificado SSL. Se você já tiver um certificado SSL, ative a cifra que foi usada para criar o certificado. O nome da sua política personalizada não deve começar com `ELBSecurityPolicy-` ou `ELBSample-`, pois esses prefixos são reservados para os nomes das políticas de segurança predefinidas.

Para usar uma política de segurança SSL personalizada

1. Use o comando create-load-balancer-policy para criar uma política de negociação SSL usando uma política de segurança personalizada. Por exemplo:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
 --policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType
 --policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
 AttributeName=Protocol-TLSv1.1,AttributeValue=true
 AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
 AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

   Se você excedeu o limite do número de políticas para o load balancer, use o comando delete-load-balancer-policy para excluir qualquer política não utilizada.

2. (Opcional) Use o comando describe-load-balancer-policies para verificar se a política foi criada:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-
name my-SSLNegotiation-policy
```

   A resposta inclui a descrição da política.

3. Use o comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --
load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

   Note

   O comando `set-load-balancer-policies-of-listener` substitui o conjunto atual de políticas para a porta especificada do load balancer pelo conjunto de políticas especificado. A lista `--policy-names` deve incluir todas as políticas para ser habilitada. Se você pular uma política que atualmente está ativada, ela será desativada.

4. (Opcional) Use o comando describe-load-balancers para verificar se a nova política é habilitada para a porta do load balancer:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

   A resposta mostra que a política está habilitada na porta 443.

```
...
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
          "LoadBalancerPort": 443,
          "Protocol": "HTTPS",
          "InstanceProtocol": "HTTPS"
      },
      "PolicyNames": [
          "my-SSLNegotiation-policy"
      ]
  }
...
```

Configurar o balanceador de carga clássico

Tópicos

- Configurar o tempo limite de inatividade da conexão para seu balanceador de carga clássico (p. 72)
- Configurar o balanceamento de carga entre zonas para seu balanceador de carga clássico (p. 73)
- Configurar a descarga da conexão para seu balanceador de carga clássico (p. 76)
- Configurar o suporte ao protocolo de proxy para o balanceador de carga clássico (p. 78)
- Configurar sessões persistentes para seu balanceador de carga clássico (p. 81)
- Configurar o modo de mitigação de dessincronização para o balanceador de carga clássico (p. 86)
- Colocar uma marcação em seu balanceador de carga clássico (p. 88)
- Configure um nome de domínio personalizado para seu balanceador de carga clássico (p. 90)

Configurar o tempo limite de inatividade da conexão para seu balanceador de carga clássico

Para cada solicitação que um cliente faz por meio de um balanceador de carga clássico, o balanceador de carga mantém duas conexões. A conexão front-end é entre o cliente e o load balancer. A conexão back-end é entre o load balancer e uma instância do EC2 registrada. O load balancer tem um período de tempo limite ocioso configurado que se aplica às suas conexões. Se nenhum dado tiver sido enviado ou recebido até o período que o tempo limite de inatividade terminar, o load balancer fechará a conexão. Para garantir que operações demoradas, como uploads de arquivo, tenham tempo para serem concluídas, envie pelo menos 1 byte de dados antes de decorrer cada período de tempo limite de inatividade e aumente a duração do período do tempo limite de inatividade conforme o necessário.

Se você usar listeners HTTP e HTTPS, recomendamos que ative a opção de keep-alive do HTTP para suas instâncias. Você pode habilitar a opção de keep-alive do nas configurações do servidor web para suas instâncias do O keep-alive, quando habilitado, permite que o load balancer reutilize conexões back-end até que o tempo limite de keep-alive expire. Para garantir que o load balancer é responsável por fechar as conexões com a instância, certifique-se de que o valor que você definiu no keep-alive do HTTP é maior do que a configuração de tempo limite de inatividade configurado para o load balancer.

Observe que os testes de keep-alive do TCP não impedem que o load balancer encerre a conexão, pois não enviam dados na payload.

Tópicos

- Configurar o tempo limite de inatividade usando o console (p. 72)
- Configurar o tempo limite de inatividade usando a AWS CLI (p. 73)

Configurar o tempo limite de inatividade usando o console

Por padrão, o Elastic Load Balancing define o tempo limite de inatividade para o balanceador de carga como 60 segundos. Use o procedimento a seguir para definir um valor diferente para o tempo limite ocioso.

Para ajustar a configuração de tempo limite de inatividade para seu load balancer

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 seu load balancer.
4. Na guia Descrição, selecione Editar tempo limite de inatividade.
5. Na página Definir configurações de conexão, digite um valor para o Tempo limite de inatividade. O intervalo para o tempo limite de inatividade é de 1 a 4,000 segundos.
6. Escolha Save (Salvar).

Configurar o tempo limite de inatividade usando a AWS CLI

Use o comando modify-load-balancer-attributes para definir o tempo limite de inatividade para seu load balancer:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"ConnectionSettings\":{\"IdleTimeout\":30}}"
```

Esta é uma resposta de exemplo:

```
{
    "LoadBalancerAttributes": {
        "ConnectionSettings": {
            "IdleTimeout": 30
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Configurar o balanceamento de carga entre zonas para seu balanceador de carga clássico

Com o balanceamento de carga entre zonas, cada nó do balanceador de carga do seu Classic Load Balancer distribui solicitações uniformemente a todas as instâncias registradas em todas as zonas de disponibilidade habilitadas. Se o balanceamento de carga entre zonas estiver desabilitado, cada nó do load balancer distribuirá solicitações uniformemente às instâncias registradas somente em sua zona de disponibilidade. Para mais informações, consulte Balanceamento de carga entre zonas no Manual do usuário do Elastic Load Balancing.

O balanceamento de carga entre zonas reduz a necessidade de manter o número equivalente de instâncias em cada Zona de disponibilidade habilitada e melhora a capacidade de seu aplicativo de lidar com a perda de uma ou mais instâncias. No entanto, recomendamos ainda que você mantenha números aproximadamente equivalentes de instâncias em cada Zona de disponibilidade habilitada, para maior tolerância a falhas.

Para ambientes em que os clientes colocam pesquisas de DNS no cache, as solicitações de entrada podem favorecer uma das Zonas de disponibilidade. Usando o balanceamento de carga entre zonas, esse desequilíbrio na carga da solicitação será distribuído entre todas as instâncias disponíveis na região, reduzindo o impacto do mau comportamento de clientes.

Quando você cria um balanceador de carga clássico, o padrão para balanceamento de carga entre zonas depende de como você cria o balanceador de carga. Com a API ou a CLI, o balanceamento de carga entre zonas é desativado por padrão. Com o AWS Management Console, a opção de ativar o balanceamento de carga entre zonas é selecionado por padrão. Depois de criar um balanceador de carga clássico, você pode habilitar ou desabilitar o balanceamento de carga entre zonas a qualquer momento.

Tópicos

- Habilitar o balanceamento de carga entre zonas (p. 74)
- Desabilitar o balanceamento de carga entre zonas (p. 75)

Habilitar o balanceamento de carga entre zonas

Você pode habilitar o balanceamento de carga entre zonas para seu balanceador de carga clássico a qualquer momento.

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 seu load balancer.
4. Na guia Descrição, selecione Alterar configuração de balanceamento de carga entre zonas.
5. Na página Alterar configuração de balanceamento de carga entre zonas, selecione Habilitar.
6. Escolha Save (Salvar).

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

1. Use o comando modify-load-balancer-attributes para definir o atributo `CrossZoneLoadBalancing` do load balancer para `true`:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":true}}"
```

   Esta é uma resposta de exemplo:

```
{
   "LoadBalancerAttributes": {
     "CrossZoneLoadBalancing": {
         "Enabled": true
       }
   },
   "LoadBalancerName": "my-loadbalancer"
 }
```

2. (Opcional) Use o comando describe-load-balancer-attributes para verificar se o balanceamento de carga entre zonas está habilitado para o load balancer:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

   Esta é uma resposta de exemplo:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
```

```
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
            "Enabled": false
        }
    }
}
```

Desabilitar o balanceamento de carga entre zonas

Você pode desativar a opção de balanceamento de carga entre zonas para seu load balancer a qualquer momento.

Para desativar 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 seu load balancer.
4. Na guia Descrição, selecione Alterar balanceamento de carga entre zonas.
5. Na página Configurar balanceamento de carga entre zonas, selecione Desabilitar.
6. Escolha Save (Salvar).

Para desabilitar o balanceamento de carga entre zonas, defina o atributo `CrossZoneLoadBalancing` do seu load balancer como `false`.

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

1. Use o comando modify-load-balancer-attributes:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":false}}"
```

   Esta é uma resposta de exemplo:

```
{
   "LoadBalancerAttributes": {
     "CrossZoneLoadBalancing": {
         "Enabled": false
       }
   },
   "LoadBalancerName": "my-loadbalancer"
 }
```

2. (Opcional) Use o comando describe-load-balancer-attributes para verificar se o balanceamento de carga entre zonas está desabilitado para o load balancer:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

   Esta é uma resposta de exemplo:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": false
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
            "Enabled": false
        }
    }
}
```

Configurar a descarga da conexão para seu balanceador de carga clássico

Para garantir que o balanceador de carga clássico interromperá o envio de solicitações para instâncias cujo registro está sendo cancelado ou que não sejam íntegras, mantendo as conexões existentes abertas, use a descarga da conexão. Isso permite que o load balancer conclua as solicitações em trânsito feitas para instâncias cujo registro está sendo cancelado ou que não estejam íntegras.

Quando você habilitar a drenagem de conexão, poderá especificar um tempo máximo para o load balancer manter as conexões ativas antes de relatar a instância como registro cancelado. O valor de tempo limite máximo pode ser definido entre 1 e 3.600 segundos (o padrão é 300 segundos). Quando o tempo limite máximo for atingido, o load balancer forçosamente fechará as conexões para a instância de cancelamento do registro.

Embora as solicitações em andamento estejam sendo atendidas, o load balancer relata o estado de uma instância de cancelamento de registro como `InService: Instance deregistration currently in progress`. Quando o cancelamento do registro da instância terminar de atender a todas as solicitações em andamento, ou quando o tempo limite máximo for atingido, o load balancer informará o estado da instância como `OutOfService: Instance is not currently registered with the LoadBalancer`.

Se uma instância deixar de ser íntegra, o load balancer reportará o estado da instância como `OutOfService`. Se houver solicitações em andamento feitas à instância não íntegra, elas serão concluídas. O tempo limite máximo não se aplica a conexões para instâncias com problemas de integridade.

Se suas instâncias fizerem parte de um grupo do Auto Scaling e a descarga da conexão estiver habilitada para o seu balanceador de carga, o Auto Scaling aguardará as solicitações em andamento serem concluídas ou o tempo limite máximo expirar antes de terminar as instâncias por causa de um evento de escalabilidade ou uma substituição de verificação de integridade.

Você pode desativar a drenagem da conexão se quiser que seu load balancer feche imediatamente as conexões para as instâncias que estiverem cancelando ou registro ou que ficaram não íntegras. Quando a drenagem da conexão estiver desativada, quaisquer solicitações em andamento feitas às instâncias que estiverem cancelando o registro ou não ficaram íntegras não serão concluídas.

Tópicos

- Habilitar a descarga da conexão (p. 77)
- Desabilitar a descarga da conexão (p. 77)

Habilitar a descarga da conexão

Você pode ativar a drenagem de conexão para seu load balancer a qualquer momento.

Para habilitar a drenagem de conexão 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 seu load balancer.
4. Na guia Instâncias, em Drenagem de conexão, selecione (Editar).
5. Na página Configurar drenagem de conexão, selecione Ativar drenagem de conexão.
6. (Opcional) Em Tempo limite, digite um valor entre 1 e 3.600 segundos.
7. Escolha Save (Salvar).

Para habilitar a drenagem da conexão usando a AWS CLI

Use o comando modify-load-balancer-attributes:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":true,\"Timeout\":300}}"
```

Esta é uma resposta de exemplo:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": true,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Desabilitar a descarga da conexão

Você pode desabilitar a drenagem de conexão para seu load balancer a qualquer momento.

Para desabilitar a drenagem de conexão 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 seu load balancer.
4. Na guia Instâncias, em Drenagem de conexão, selecione (Editar).
5. Na página Configurar drenagem de conexão, desmarque Ativar drenagem de conexão.
6. Escolha Save (Salvar).

Para desabilitar a drenagem de conexão usando a AWS CLI

Use o comando modify-load-balancer-attributes:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":false}}"
```

Esta é uma resposta de exemplo:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Configurar o suporte ao protocolo de proxy para o balanceador de carga clássico

O protocolo de proxy é um protocolo de Internet usado para transportar informações de conexão da origem que solicita a conexão ao destino ao qual a conexão foi solicitada. O Elastic Load Balancing usa o protocolo de proxy versão 1, que usa um formato de cabeçalho legível por humanos.

Por padrão, quando você usa o Transmission Control Protocol (TCP) para conexões front-end e backend, o balanceador de carga clássico encaminha solicitações para as instâncias sem modificar os cabeçalhos de solicitação. Se você habilitar o protocolo de proxy, um cabeçalho legível por humanos será adicionado ao cabeçalho de solicitação com informações de conexão, como o endereço IP de origem, endereço IP de destino e números de portas. O cabeçalho, então, será enviado à instância como parte da solicitação.

> **Note**
>
> O AWS Management Console não é compatível com a habilitação do protocolo de proxy.

Tópicos

- Cabeçalho do protocolo de proxy (p. 78)
- Pré-requisitos para habilitar o protocolo de proxy (p. 79)
- Habilitar o protocolo de proxy usando a AWS CLI (p. 79)
- Desabilitar o protocolo de proxy usando a AWS CLI (p. 80)

Cabeçalho do protocolo de proxy

O cabeçalho do protocolo de proxy ajuda você a identificar o endereço IP de um cliente quando você tiver um balanceador de carga que usa TCP para conexões backend. Como os load balancers interceptam tráfego entre clientes e suas instâncias, os logs de acesso da sua instância contêm o endereço IP do load balancer em vez do cliente de origem. Você pode analisar a primeira linha da solicitação para recuperar o endereço IP do cliente e o número da porta.

O endereço do proxy no cabeçalho para IPv6 é o endereço IPv6 público do seu load balancer. Este endereço IPv6 corresponde ao endereço IP resolvido de nome DNS do load balancer, que começa com `ipv6` ou `dualstack`. Se o cliente se conectar com IPv4, o endereço do proxy no cabeçalho será o endereço privado IPv4 do load balancer, que não é resolvível por uma busca de DNS fora da rede do EC2-Classic.

A linha do protocolo de proxy é uma única linha que termina com um retorno de carro e feed de linha ("\r\n") e tem o seguinte formato:

```
PROXY_STRING + single space + INET_PROTOCOL + single space + CLIENT_IP + single space +
 PROXY_IP + single space + CLIENT_PORT + single space + PROXY_PORT + "\r\n"
```

Exemplo: IPv4

Veja a seguir um exemplo da linha de protocolo de proxy para IPv4.

```
PROXY TCP4 198.51.100.22 203.0.113.7 35646 80\r\n
```

Exemplo: IPv6 (somente EC2-Classic)

Veja a seguir um exemplo da linha de protocolo de proxy para IPv6.

```
PROXY TCP6 2001:DB8::21f:5bff:febf:ce22:8a2e 2001:DB8::12f:8baa:eafc:ce29:6b2e 35646 80\r\n
```

Pré-requisitos para habilitar o protocolo de proxy

Antes de começar, faça o seguinte:

- Confirme se o balanceador de carga não está por trás de um servidor de proxy com o protocolo de proxy habilitado. Se o protocolo de proxy estiver habilitado tanto no servidor de proxy quanto no balanceador de carga, este adicionará outro cabeçalho à solicitação, que já tem um cabeçalho do servidor de proxy. Dependendo de como sua instância estiver configurada, essa duplicação poderá resultar em erros.
- Confirme se suas instâncias podem processar as informações do protocolo de proxy.
- Confirme se as configurações do seu listener são compatíveis com o protocolo de proxy. Para obter mais informações, consulte . Configurações do listener para balanceadores de carga clássicos (p. 36).

Habilitar o protocolo de proxy usando a AWS CLI

Para habilitar o protocolo de proxy, você precisa criar uma política do tipo `ProxyProtocolPolicyType` e, em seguida, habilitar a política na porta da instância.

Use o procedimento a seguir para criar uma nova política para o load balancer do tipo `ProxyProtocolPolicyType`, definir a política recém-criada para a instância na porta `80` e verificar se a política está ativada.

Para habilitar o Proxy Protocol para o load balancer

1. (Opcional) Use o seguinte comando describe-load-balancer-policy-types para listar as políticas compatíveis com o Elastic Load Balancing:

   ```
   aws elb describe-load-balancer-policy-types
   ```

   A resposta inclui os nomes e as descrições dos tipos de política suportados. A tabela a seguir mostra a saída para o tipo `ProxyProtocolPolicyType`:

   ```
   {
       "PolicyTypeDescriptions": [
           ...
           {
               "PolicyAttributeTypeDescriptions": [
                   {
   ```

```
                    "Cardinality": "ONE",
                    "AttributeName": "ProxyProtocol",
                    "AttributeType": "Boolean"
                }
            ],
            "PolicyTypeName": "ProxyProtocolPolicyType",
            "Description": "Policy that controls whether to include the IP address and
 port of the originating
request for TCP messages. This policy operates on TCP/SSL listeners only"
        },
        ...
    ]
}
```

2. Use o seguinte comando create-load-balancer-policy para criar uma política que habilita o protocolo de proxy:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
name my-ProxyProtocol-policy --policy-type-name ProxyProtocolPolicyType --policy-
attributes AttributeName=ProxyProtocol,AttributeValue=true
```

3. Use o comando set-load-balancer-policies-for-backend-server para habilitar a política recém-criada na porta especificada. Observe que esse comando substitui o conjunto atual de políticas habilitadas. Portanto, a opção `--policy-names` deve especificar tanto a política que você está adicionando à lista (por exemplo, `my-ProxyProtocol-policy`) quanto quaisquer políticas que estejam atualmente habilitadas (por exemplo, `my-existing-policy`).

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-
loadbalancer --instance-port 80 --policy-names my-ProxyProtocol-policy my-existing-
policy
```

4. (Opcional) Use o seguinte comando describe-load-balancers para verificar se o protocolo de proxy está habilitado:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

A resposta inclui as informações a seguir, que mostra que a política `my-ProxyProtocol-policy` está associada com a porta `80`.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "BackendServerDescriptions": [
                {
                    "InstancePort": 80,
                    "PolicyNames": [
                        "my-ProxyProtocol-policy"
                    ]
                }
            ],
            ...
        }
    ]
}
```

Desabilitar o protocolo de proxy usando a AWS CLI

Você pode desativar as políticas associadas à sua instância e, em seguida, habilitá-las posteriormente.

Para desabilitar a política do protocolo de proxy

1. Use o seguinte comando set-load-balancer-policies-for-backend-server para desabilitar a política do protocolo de proxy omitindo-a da opção `--policy-names`, mas incluindo as outras políticas que deveriam permanecer habilitadas (como `my-existing-policy`).

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-existing-policy
```

   Se não houver outras políticas para habilitar, especifique uma string vazia com a opção `--policy-names`, da seguinte forma:

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names "[]"
```

2. (Opcional) Use o comando describe-load-balancers para verificar se a política foi desabilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

   A resposta inclui as informações a seguir, que mostram que nenhuma porta está associada com uma política.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "BackendServerDescriptions": [],
            ...
        }
    ]
}
```

Configurar sessões persistentes para seu balanceador de carga clássico

Por padrão, um balanceador de carga clássico roteia cada solicitação de forma independente para a instância registrada com a menor carga. No entanto, você pode usar o recurso sticky session (também conhecida como afinidade de sessão), que permite que o load balancer vincule a sessão de um usuário a uma instância específica. Isso garante que todas as solicitações do usuário durante a sessão sejam enviadas para a mesma instância.

O segredo para o gerenciamento de sticky sessions é determinar por quanto tempo o load balancer deve rotear consistentemente a solicitação do usuário para a mesma instância. Se sua aplicação tiver seu próprio cookie de sessão, você pode configurar o Elastic Load Balancing de forma que o cookie da sessão acompanhe a duração especificada pelo cookie de sessão da aplicação. Se sua aplicação não tiver seu próprio cookie de sessão, você pode configurar o Elastic Load Balancing para criar um cookie de sessão ao especificar sua própria duração de persistência.

O Elastic Load Balancing cria um cookie, chamado AWSELB, que é usado para mapear a sessão para a instância.

Requirements

- Um load balancer HTTP/HTTPS.

- Pelo menos uma instância íntegra em cada Zona de disponibilidade.

Compatibility

- A RFC para a propriedade do caminho de um cookie permite sublinhados. No entanto, o URI do Elastic Load Balancing codifica caracteres sublinhados como `%5F`, pois alguns navegadores, como o Internet Explorer 7, esperam que os sublinhados sejam codificados no URI como `%5F`. Por causa do possível impacto a navegadores que estejam funcionando no momento, o Elastic Load Balancing continuará a codificar em URI os caracteres sublinhados. Por exemplo, se o cookie tiver a propriedade `path=/my_path`, o Elastic Load Balancing mudará essa propriedade na solicitação encaminhada para `path=/my%5Fpath`.
- Você não pode definir o sinalizador `secure` ou o sinalizador `HttpOnly` nos cookies de perdurabilidade da sessão baseado na duração. No entanto, esses cookies não contêm dados confidenciais. Observe que, se você definir o sinalizador `secure` ou o sinalizador `HttpOnly` em um cookie de perdurabilidade da sessão controlada pelo aplicativo, ele também será configurado no cookie AWSELB.
- Se você tiver um ponto-e-vírgula no final no campo `Set-Cookie` de um cookie do aplicativo, o load balancer ignorará o cookie.

Tópicos

- Persistência da sessão com base na duração (p. 82)
- Persistência da sessão controlada pela aplicação (p. 84)

Persistência da sessão com base na duração

O load balancer usa um cookie especial, AWSELB, para rastrear a instância para cada solicitação a cada listener. Quando o load balancer receber uma solicitação, ele primeiro verificará se esse cookie está presente na solicitação. Se estiver, a solicitação será enviada para a instância especificada no cookie. Se não houver um cookie, o load balancer selecionará uma instância com base no algoritmo de balanceamento de carga existente. Um cookie é inserido na resposta para vincular solicitações subsequentes do mesmo usuário para essa instância. A configuração da política de perdurabilidade define a expiração de um cookie, que estabelece a validade de cada cookie. O load balancer não atualiza o tempo de expiração do cookie e não verifica se o cookie expirou antes de usá-lo. Após um cookie expirar, a sessão não será mais sticky. O cliente deve remover o cookie do armazenamento de cookies após a expiração.

Com solicitações de CORS (cross-origin resource sharing, compartilhamento de recursos de origem cruzada), alguns navegadores exigem `SameSite=None; Secure` para habilitar a perdurabilidade. Nesse caso, o Elastic Load Balancing cria um segundo cookie de persistência, o AWSELBCORS, que inclui as mesmas informações que o cookie de persistência original, além deste atributo `SameSite`. Os clientes recebem ambos os cookies.

Se uma instância falhar ou ficar não deixar de ser íntegra, o load balancer interromperá as solicitações de roteamento para essa instância e escolherá uma nova instância íntegra com base no algoritmo de balanceamento de carga existente. A solicitação é roteada para a nova instância como se não houvesse cookie e a sessão não for mais perdurável.

Se um cliente mudar para um listener com uma porta de back-end diferente, a perdurabilidade será perdida.

Para habilitar sticky sessions com base na duração para um load balancer usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em LOAD BALANCING, escolha Load balancers.
3. Selecione seu load balancer.

4. Na guia Descrição, selecione Editar perdurabilidade.
5. Na página Editar perdurabilidade, selecione Habilitar perdurabilidade de cookies gerada pelo load balancer.
6. (Opcional) Em Período de expiração, digite o período de expiração do cookie, em segundos. Se você não especificar um período de expiração, a sticky session durará por toda a sessão do navegador.
7. Escolha Save (Salvar).

Para habilitar sticky sessions com base na duração para um load balancer usando a AWS CLI

1. Use o comando create-lb-cookie-perdurabilidade-policy para criar uma política de perdurabilidade de cookies gerada pelo load balancer com um período de expiração do cookie de 60 segundos:

```
aws elb create-lb-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-duration-cookie-policy --cookie-expiration-period 60
```

2. Use o comando set-load-balancer-policies-of-listener para habilitar a perdurabilidade da sessão para o load balancer especificado:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --
load-balancer-port 443 --policy-names my-duration-cookie-policy
```

> **Note**
>
> O comando `set-load-balancer-policies-of-listener` substitui o conjunto atual de políticas associado à porta especificada do load balancer. Sempre que você usar esse comando, especifique a opção `--policy-names` para listar todas as políticas a serem habilitadas.

3. (Opcional) Use o comando describe-load-balancers para verificar se a política foi habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

A resposta inclui as informações a seguir, que mostram que a política está ativada para o listener na porta especificada:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-duration-cookie-policy",
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                ...
            ],
            ...
            "Policies": {
```

```
                "LBCookieStickinessPolicies": [
                 {
                        "PolicyName": "my-duration-cookie-policy",
                        "CookieExpirationPeriod": 60
                    }

                ],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": [
                    "ELBSecurityPolicy-2016-08"
                ]
            },
            ...
        }
    ]
}
```

Persistência da sessão controlada pela aplicação

O load balancer usa um cookie especial para associar a sessão com a instância que lidou com a solicitação inicial, mas segue a vida do cookie do aplicativo especificado na configuração da política. O load balancer só inserirá um novo cookie de perdurabilidade se a resposta do aplicativo incluir um novo cookie do aplicativo. O cookie de perdurabilidade do load balancer não será atualizado com cada solicitação. Se o cookie for explicitamente removido ou expirar, a sessão deixará de ser perdurável até ser emitido um novo cookie do aplicativo.

Os seguintes atributos definidos por instâncias back-end são enviados para clientes no cookie: `path`, `port`, `domain`, `secure`, `httponly`, `discard`, `max-age`, `expires`, `version`, `comment`, `commenturl` e `samesite`.

Se uma instância falhar ou ficar não deixar de ser íntegra, o load balancer interromperá as solicitações de roteamento para essa instância e escolherá uma nova instância íntegra com base no algoritmo de balanceamento de carga existente. O load balancer trata a sessão agora como "grudada" à nova instância íntegra e continua a rotear solicitações para essa instância, mesmo se a instância falha retornar.

Para habilitar a perdurabilidade da sessão controlada por aplicativo 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 seu load balancer.
4. Na guia Descrição, selecione Editar perdurabilidade.
5. Na página Editar perdurabilidade, selecione Habilitar perdurabilidade de cookies gerada pelo aplicativo.
6. Em Nome de cookie, digite o nome do cookie do aplicativo.
7. Escolha Save (Salvar).

Para habilitar a perdurabilidade da sessão controlada por aplicativo usando a AWS CLI

1. Use o comando create-app-cookie-stickiness-policy para criar uma política de perdurabilidade de cookie gerada pelo aplicativo:

```
aws elb create-app-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-app-cookie-policy --cookie-name my-app-cookie
```

2. Use o comando set-load-balancer-policies-of-listener para habilitar a perdurabilidade da sessão para um load balancer:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --
load-balancer-port 443 --policy-names my-app-cookie-policy
```

Note

O comando `set-load-balancer-policies-of-listener` substitui o conjunto atual de políticas associado à porta especificada do load balancer. Sempre que você usar esse comando, especifique a opção `--policy-names` para listar todas as políticas a serem habilitadas.

3. (Opcional) Use o comando describe-load-balancers para verificar se a política de perdurabilidade está habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

4. A resposta inclui as informações a seguir, que mostram que a política está ativada para o listener na porta especificada:

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-app-cookie-policy",
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "TCP",
                        "InstanceProtocol": "TCP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [
                {
                        "PolicyName": "my-app-cookie-policy",
                        "CookieName": "my-app-cookie"
                    }

                ],
                "OtherPolicies": [
                    "ELBSecurityPolicy-2016-08"
                ]
            },
            ...
```

```
        }
    ]
}
```

Configurar o modo de mitigação de dessincronização para o balanceador de carga clássico

O modo de mitigação de dessincronização protege sua aplicação contra problemas causados por HTTP Desync. O balanceador de carga classifica cada solicitação com base em seu nível de ameaça, permite solicitações seguras e, em seguida, reduz o risco, conforme instruído pelo modo de mitigação especificado. Os modos de mitigação de dessincronização são: monitor (monitorado), defensive (defensivo) e strictest (mais rigoroso). O padrão é o modo defensivo, que fornece mitigação durável contra HTTP Desync, mantendo a disponibilidade da sua aplicação. Você pode alternar para o modo mais restrito para garantir que sua aplicação receba somente solicitações que estejam em conformidade com o RFC 7230.

A biblioteca http_desync_guardian analisa solicitações HTTP para evitar ataques de HTTP Desync. Para obter mais informações, consulte HTTP Desync Guardian no github.

Tópicos

- Classifications (p. 86)
- Modes (p. 87)
- Modificar o modo de mitigação de dessincronização (p. 88)

> **Tip**
>
> Essa configuração se aplica somente aos balanceadores de carga clássicos. Para obter informações que se aplicam aos balanceadores de carga da aplicação, consulte Modo de mitigação de dessincronização para balanceadores de carga da aplicação.

Classifications

As classificações são as seguintes:

- Compatível: a solicitação está em conformidade com o RFC 7230 e não representa ameaças de segurança conhecidas.
- Aceitável: a solicitação não está em conformidade com o RFC 7230, mas não representa ameaças de segurança conhecidas.
- Ambígua: a solicitação não está em conformidade com o RFC 7230, mas representa um risco, pois vários servidores Web e proxies podem lidar com ela de formas diferentes.
- Grave: a solicitação representa um alto risco de segurança. O balanceador de carga bloqueia a solicitação, atende uma resposta 400 ao cliente e fecha a conexão do cliente.

As listas a seguir descrevem os problemas para cada classificação.

Acceptable

- Um cabeçalho contém um caractere não ASCII ou de controle.

- A versão de solicitação contém um valor incorreto.
- Há um cabeçalho Content-Length (Comprimento de conteúdo) com um valor de 0 para uma solicitação GET ou HEAD.
- O URI de solicitação contém um espaço que não é codificado por URL.

Ambiguous

- O URI de solicitação contém caracteres de controle.
- A solicitação contém um cabeçalho Transfer-Coding (Codificação de transferência) e um cabeçalho Content-Length (Comprimento de conteúdo).
- Há vários cabeçalhos Content-Length (Comprimento de conteúdo) com o mesmo valor.
- Um cabeçalho está vazio ou há uma linha com apenas espaços.
- Há um cabeçalho que pode ser normalizado para Transfer-Enconding (Codificação de transferência) ou Content-Length (Comprimento de conteúdo) usando técnicas comuns de normalização de texto.
- Há um cabeçalho Content-Length (Comprimento de conteúdo) para uma solicitação GET ou HEAD.
- Há um cabeçalho Transfer-Encoding (Codificação de transferência) para uma solicitação GET ou HEAD.

Severe

- O URI de solicitação contém um caractere nulo ou retorno de carro.
- O cabeçalho Content-Length (Comprimento de conteúdo) contém um valor que não pode ser analisado ou não é um número válido.
- Um cabeçalho contém um caractere nulo ou retorno de carro.
- O cabeçalho Transfer-Encoding (Codificação de transferência) contém um valor inválido.
- O método de solicitação está malformado.
- A versão da solicitação está malformada.
- Há vários cabeçalhos Content-Length (Comprimento de conteúdo) com valores diferentes.
- Há vários cabeçalhos Transfer-Coding (Codificação de transferência): cabeçalhos em bloco.

Se uma solicitação não estiver em conformidade com o RFC 7230, o balanceador de carga incrementará a métrica `DesyncMitigationMode_NonCompliant_Request_Count`. Para obter mais informações, consulte . Métricas do Classic Load Balancer (p. 94).

Modes

A tabela a seguir descreve como os balanceadores de carga clássicos tratam solicitações com base no modo e na classificação.

Classificação	Modo monitorado	Modo defensivo	Modo mais restrito
Compatível	Permitido	Permitido	Permitido
Aceitável	Permitido	Permitido	Bloqueado
Ambíguo	Permitido	Permitido[1]	Bloqueado
Grave	Permitido	Bloqueado	Bloqueado

[1] Encaminha as solicitações, mas fecha as conexões entre cliente e destino.

Modificar o modo de mitigação de dessincronização

Para atualizar o modo de mitigação de dessincronização 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.
4. Na aba Description (Descrição), escolha Configure desync mitigation mode (Configurar o modo de mitigação de dessincronização).
5. Na página Configure desync mitigation mode (Configurar o modo de mitigação de dessincronização), escolha Monitor (Monitorado), Denfensive (Defensivo) ou Strictest (Mais rigoroso).
6. Escolha Save (Salvar).

Para atualizar o modo de mitigação de dessincronização usando a AWS CLI

Use o comando modify-load-balancer-attributes com o atributo `elb.http.desyncmitigationmode` configurado como `monitor`, `defensive` ou `strictest`.

```
aws elb modify-load-balancer-attributes --load-balancer-name my-load-balancer --load-
balancer-attributes file://attribute.json
```

Veja a seguir o conteúdo de `attribute.json`.

```
{
    "AdditionalAttributes": [
        {
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }
    ]
}
```

Colocar uma marcação em seu balanceador de carga clássico

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

Você pode adicionar várias marcações a cada balanceador de carga clássico. As chaves de tag devem ser exclusivas de cada load balancer. Se você adicionar uma tag com uma chave que já esteja associada ao load balancer, o valor dessa tag será atualizado.

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

Tópicos

- Restrições de tags (p. 89)
- Adicione um tag (p. 89)
- Remover uma marcação (p. 89)

Restrições de tags

As restrições básicas a seguir se aplicam às tags:

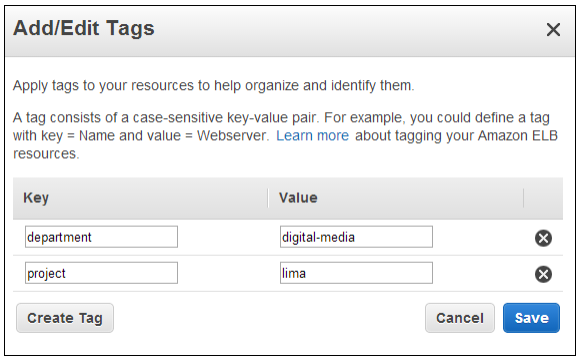
- Número máximo de tags por recurso: 50
- Comprimento máximo da chave: 127 caracteres Unicode
- Comprimento máximo de valor: 255 caracteres Unicode
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas. Os caracteres permitidos são letras, espaços e números representáveis em UTF-8, além 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.

Adicione um tag

Você pode adicionar tags ao seu load balancer a qualquer momento.

Para adicionar uma tag 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 seu load balancer.
4. Na guia Tags, selecione Adicionar/editar tags.
5. Na página Adicionar/editar tags, em cada tag, selecione Criar tag e especifique uma chave e um valor.



6. Ao terminar de adicionar tags, selecione Salvar.

Para adicionar uma tag usando a AWS CLI

Use o comando add-tags para adicionar a tag especificada:

```
aws elb add-tags --load-balancer-name my-loadbalancer --tag "Key=project,Value=lima"
```

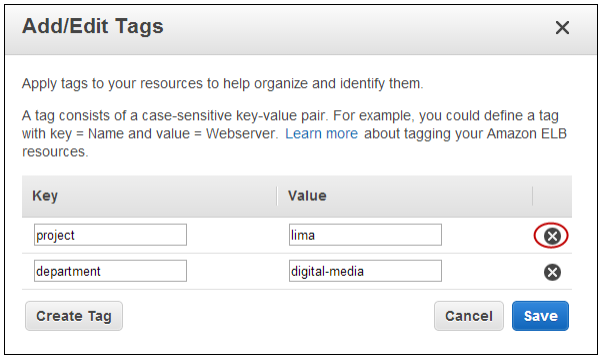
Remover uma marcação

Você pode remover as tags do seu load balancer sempre que terminar de usá-lo.

Para remover uma tag 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 seu load balancer.
4. Na guia Tags, selecione Adicionar/editar tags.
5. Na página Adicionar/editar tags, selecione o ícone de exclusão da tag,



6. Ao terminar de remover as tags, selecione Salvar.

Para remover uma tag usando a AWS CLI

Use o comando remove-tags para remover a tag com a chave especificada:

```
aws elb remove-tags --load-balancer-name my-loadbalancer --tag project
```

Configure um nome de domínio personalizado para seu balanceador de carga clássico

Cada balanceador de carga clássico recebe um nome de Sistema de Nomes de Domínio (DNS) padrão. Esse nome DNS inclui o nome da região da AWS em que o balanceador de carga é criado. Por exemplo, se você criar um balanceador de carga denominado `my-loadbalancer` na região Oeste dos EUA (Oregon), seu balanceador de carga receberá um nome DNS como `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com`. Para acessar o site nas suas instâncias, cole esse nome DNS no campo de endereço de um navegador da web. No entanto, esse nome DNS não é fácil para os clientes se lembrarem de usar.

Se você preferir usar um nome DNS amigável para seu load balancer, como `www.example.com`, em vez do nome DNS padrão, pode criar um nome de domínio personalizado e associá-lo com o nome DNS do seu load balancer. Quando um cliente faz uma solicitação usando esse nome de domínio personalizado, o servidor DNS o resolverá para o nome DNS para seu load balancer.

Tópicos

- Como associar seu nome de domínio personalizado com o nome do seu balanceador de carga (p. 91)
- Configure o failover de DNS para o seu balanceador de carga (p. 91)
- Dissociar seu nome de domínio personalizado do seu balanceador de carga (p. 92)

Como associar seu nome de domínio personalizado com o nome do seu balanceador de carga

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

- Para usar o Amazon Route 53 para registrar um nome de domínio, consulte Registrar nomes de domínio com o Route 53 no Guia do desenvolvedor do Amazon Route 53.
- Para obter uma lista de registradores chancelados, consulte Diretório de registradores chancelados.

Em seguida, use o serviço DNS, como o registrador de domínios, para criar um registro CNAME a fim de rotear consultas para o load balancer. Para obter mais informações, consulte a documentação do serviço DNS.

Também é possível usar o Route 53 como seu serviço DNS. Você cria uma zona hospedada, que contém informações sobre como rotear o tráfego na Internet para seu domínio, e um conjunto de registro do recurso do alias, que roteia as consultas de seu nome de domínio para o balanceador de carga. O Route 53 não cobra por consultas de DNS de conjuntos de registros de alias, e você pode usar esses conjuntos para rotear consultas de DNS para o balanceador de carga para o apex de zona do seu domínio (por exemplo, `example.com`). Para obter informações sobre a transferência de serviços DNS para os domínios existentes ao Route 53, consulte Configurar o Amazon Route 53 como serviço DNS no Guia do desenvolvedor do Amazon Route 53.

Por fim, crie uma zona hospedada e um conjunto de registros de alias para seu domínio usando o Route 53. Para obter mais informações, consulte Rotear tráfego para um balanceador de carga no Guia do desenvolvedor do Amazon Route 53.

Configure o failover de DNS para o seu balanceador de carga

Se você usa o Route 53 para rotear consultas de DNS para seu balanceador de carga, também poderá configurar o failover de DNS para o seu balanceador de carga usando o Route 53. Em uma configuração de failover, o Route 53 verifica a integridade das instâncias do EC2 registradas para o balanceador de carga, para determinar se elas estão disponíveis. Se não houver instâncias do EC2 íntegras registradas no balanceador de carga, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 roteará o tráfego para outro recurso disponível, como um balanceador de carga íntegro ou um site estático no Amazon S3.

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

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

Dissociar seu nome de domínio personalizado do seu balanceador de carga

Você pode dissociar seu nome de domínio personalizado de uma instância do load balancer ao primeiro excluir os conjuntos de registro de recurso na sua hosted zone e, em seguida, excluir a hosted zone. Para obter mais informações, consulte Editar registros e Excluir uma zona hospedada pública no Guia do desenvolvedor do Amazon Route 53.

Monitore seu Classic Load Balancer

Você pode usar os recursos a seguir para monitorar seus load balancers, analisar os padrões de tráfego e solucionar problemas com seu load balancers e instâncias back-end.

Métricas do CloudWatch

O Elastic Load Balancing publica pontos de dados no Amazon CloudWatch sobre seus balanceadores de carga e instâncias backend. O CloudWatch permite recuperar estatísticas sobre esses pontos de dados 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 mais informações, consulte Métricas do CloudWatch para seu Classic Load Balancer (p. 93).

Logs de acesso do Elastic Load Balancing

Os logs de acesso do Elastic Load Balancing capturam informações detalhadas para solicitações feitas para o seu balanceador de carga e as armazena como arquivos de log no bucket do Amazon S3 que você especificar. Cada log contém detalhes, como a hora em que uma solicitação foi recebida, o endereço IP do cliente, latências, caminho da solicitação e respostas do servidor. Você pode usar esses logs de acesso para analisar padrões de tráfego e para solucionar problemas em seus aplicativos de back-end. Para mais informações, consulte Logs de acesso do seu Classic Load Balancer (p. 101).

Logs do CloudTrail

O AWS CloudTrail permite controlar as chamadas feitas para a API do Elastic Load Balancing por sua conta da AWS ou em nome dela. O CloudTrail armazena as informações em arquivos de log no bucket do Amazon S3 que você especificar. Você pode usar esses arquivos de log para monitorar a atividade dos seus load balancers ao determinar quais solicitações foram feitas, os endereços IP de onde as solicitações vieram, quem fez a solicitação, quando a solicitação foi feita e assim por diante. Para mais informações, consulte Registro de chamadas de API para seu Classic Load Balancer usando o AWS CloudTrail (p. 111).

Métricas do CloudWatch para seu Classic Load Balancer

O Elastic Load Balancing publica pontos de dados no Amazon CloudWatch para seus balanceadores de carga e instâncias backend. 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 instâncias EC2 íntegras para um load balancer ao longo de um período especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um 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 balanceador de carga. Se houver solicitações passando pelo balanceador de carga, o Elastic Load Balancing vai medir e enviar suas métricas em intervalos de 60 segundos. Se não há solicitações passando pelo load balancer ou não há dados para uma métrica, a métrica não é reportada.

Para obter mais informações sobre o Amazon CloudWatch, consulte o Manual do usuário do Amazon CloudWatch.

Índice

- Métricas do Classic Load Balancer (p. 94)
- Dimensões métricas dos Classic Load Balancers (p. 99)
- Estatísticas para métricas do Classic Load Balancer (p. 99)
- Visualizar métricas do CloudWatch para o balanceador de carga (p. 100)

Métricas do Classic Load Balancer

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

Métrica	Descrição
`BackendConnectionErrors`	O número de conexões que não foram estabelecidas com êxito entre o load balancer e as instâncias registradas. Como o load balancer tenta executar a conexão novamente quando há erros, essa contagem pode exceder a taxa de solicitações. Observe que essa contagem também inclui erros de conexão relacionados a verificações de saúde. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Observe que `Average`, `Minimum` e `Maximum` são reportadas por nó do load balancer e geralmente não são úteis. No entanto, a diferença entre o mínimo e o máximo (ou o pico e a média ou a média e o mais baixo) pode ser útil para determinar se um nó de load balancer é uma exceção. Example: suponhamos que o load balancer tenha 2 instâncias em us-west-2a e 2 instâncias em us-west-2b e que tentativas de se conectar a 1 instância em us-west-2a resultem em erros de conexão do back-end. A soma para us-west-2a inclui esses erros de conexão, enquanto a soma para us-west-2b não os inclui. Portanto, a soma para o load balancer é igual à soma para us-west-2a.
`DesyncMitigationMode_NonCompliant_request_count`	[HTTP listener] O número de solicitações que não estão em conformidade com a RFC 7230. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`.
`HealthyHostCount`	O número de instâncias íntegras registradas com o load balancer. A instância recém-registrada é considerada saudável após passar pela primeira verificação de saúde. Se o balanceamento de carga entre zonas estiver ativado, o número de instâncias saudáveis para a dimensão `LoadBalancerName` é calculado em todas as zonas de disponibilidade. Do contrário, ele é calculado por zona de disponibilidade. Reporting criteria: há instâncias registradas Estatísticas: as estatísticas mais úteis são `Average` e `Maximum`. Essas estatísticas são determinadas pelos nós do load balancer. Observe que alguns nós do load balancer podem determinar que uma instância não é saudável por um breve período, enquanto outros nós determinam que ela é saudável.

Métrica	Descrição
	Example: suponhamos que o load balancer tenha 2 Instâncias em us-west-2a e 2 instâncias em us-west-2b e us-west-2a tem 1 instância não íntegra e us-west-2b não tem nenhuma instância não íntegra. Com a dimensão `AvailabilityZone`, há uma média de 1 instância saudável e 1 não saudável em us-west-2a e uma média de 2 instâncias saudáveis e 0 instâncias não saudáveis em us-west-2b.
`HTTPCode_Backend_2XX`, `HTTPCode_Backend_3XX`, `HTTPCode_Backend_4XX`, `HTTPCode_Backend_5XX`	[HTTP listener] O número de códigos de resposta HTTP gerados por instâncias registradas. Essa contagem não inclui códigos de resposta gerados pelo load balancer. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` são todos 1. Example: suponhamos que o load balancer tenha 2 instâncias em us-west-2a e 2 instâncias em us-west-2b e que tentativas enviadas para 1 instância em us-west-2a resultem em respostas HTTP 500 A soma para us-west-2a inclui essas respostas de erro, enquanto a soma para us-west-2b não as inclui. Portanto, a soma para o load balancer é igual à soma para us-west-2a.
`HTTPCode_ELB_4XX`	[HTTP listener] O número de códigos de erro do cliente HTTP 4XX gerados pelo load balancer. Erros de cliente são gerados quando uma solicitação é defeituosa ou incompleta. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` são todos 1. Example: suponhamos que o load balancer tenha us-west-2a e us-west-2b habilitados e que ente as solicitações de clientes está um URL de solicitação malformado. Como resultado, os erros do cliente provavelmente vão aumentar em todas as zonas de disponibilidade. A soma para o load balancer é a soma dos valores para as zonas de disponibilidade.

Métrica	Descrição
`HTTPCode_ELB_5XX`	[HTTP listener] O número de códigos de erro do servidor HTTP 5XX gerados pelo load balancer. Essa contagem não inclui códigos de resposta gerados por instâncias registradas. A métrica é reportada se não houver instâncias saudáveis registradas no load balancer, ou se a taxa de solicitações excede a capacidade das instâncias (spillover) ou do load balancer. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` são todos 1. Example: suponhamos que o load balancer tenha us-west-2a e us-west-2b habilitados e que as instâncias em us-west-2a estejam enfrentando latência alta e demorando para responder a solicitações. Como resultado, a fila de pico para os nós do load balancer em us-west-2a é preenchida, e os clientes recebem um erro 503. Se us-west-2b continuar a responder normalmente, a soma para o load balancer será igual à soma para us-west-2a.
`Latency`	[Listener do HTTP] O tempo total, em segundos, decorrido desde momento em que o load balancer envia a solicitação até uma instância registrada, até que a instância comece a enviar os cabeçalhos de resposta. [Listener do TCP] O tempo total, em segundos, decorrido para o load balancer estabelecer uma conexão com êxito com uma instância registrada. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Average`. Use `Maximum` para determinar se algumas solicitações estão levando muito mais tempo do que a média. Observe que `Minimum` normalmente não é útil. Example: suponhamos que o load balancer tenha 2 instâncias em us-west-2a e 2 instâncias em us-west-2b e que tentativas enviadas para 1 instância em us-west-2a tenham uma latência maior A média para us-west-2a tem um valor mais alto do que a média para us-west-2b.

Métrica	Descrição
`RequestCount`	O número de solicitações concluídas ou conexões feitas durante o intervalo especificado (1 ou 5 minutos). [HTTP listener] O número de solicitações recebidas e roteadas, incluindo respostas de erro de HTTP das instâncias registradas. [TCP listener] O número de conexões feitas com as instâncias registradas. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam 1. Example: suponhamos que o load balancer tenha 2 instâncias em us-west-2a e 2 instâncias em us-west-2b e que 100 solicitações sejam enviadas para o load balancer. Sessenta solicitações são enviadas para us-west-2a, e cada instância recebe 30 solicitações, e 40 solicitações são enviadas para us-west-2b, e cada instância recebe 20 solicitações. Com a dimensão `AvailabilityZone`, há uma soma de 60 solicitações em us-west-2a e 40 solicitações em us-west-2b. Com a dimensão `LoadBalancerName`, há uma soma de 100 solicitações.
`SpilloverCount`	O número total de solicitações que foram rejeitadas porque a fila de pico está cheia. [HTTP listener] O load balancer retorna um código de erro HTTP 503. [TCP listener] O load balancer fecha a conexão. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`. Observe que `Average`, `Minimum` e `Maximum` são reportadas por nó do load balancer e geralmente não são úteis. Example: suponhamos que o load balancer tenha us-west-2a e us-west-2b habilitados e que as instâncias em us-west-2a estejam enfrentando latência alta e demorando para responder a solicitações. Como resultado, a fila de pico para o nó do load balancer em us-west-2a é preenchida, resultando em spillover. Se us-west-2b continuar a responder normalmente, a soma para o load balancer será a mesma que a soma para us-west-2a.

Métrica	Descrição
`SurgeQueueLength`	O número total de solicitações (listener HTTP) ou de conexões (listener TCP) com encaminhamento pendente a uma instância íntegra. O tamanho máximo da fila é 1.024. As solicitações ou conexões adicionais são rejeitadas quando a fila está cheia. Para mais informações, consulte `SpilloverCount`. Reporting criteria (Critérios de relatório): há um valor diferente de zero. Statistics: a estatística mais útil é `Maximum`, porque representa o pico de solicitações em fila. A estatística `Average` pode ser útil em combinação com `Minimum` e `Maximum` para determinar o intervalo de solicitações enfileiradas. Observe que `Sum` não é útil. Example: suponhamos que o load balancer tenha us-west-2a e us-west-2b habilitados e que as instâncias em us-west-2a estejam enfrentando latência alta e demorando para responder a solicitações. Como resultado, a fila de pico para os nós do load balancer em us-west-2a é preenchida, gerando maior probabilidade de aumento nos tempos de resposta para os clientes. Se isso continuar, o load balancer provavelmente terá spillovers (consulte a métrica `SpilloverCount`). Se us-west-2b continuar a responder normalmente, `max` para o load balancer será o mesmo que `max` para us-west-2a.
`UnHealthyHostCount`	O número de instâncias não íntegras registradas com o load balancer. Uma instância é considerada não saudável depois de exceder o limite de saúde configurado para verificações de saúde. Uma instância não saudável é considerada saudável novamente depois de atender ao limite de saúde configurado para verificações de saúde. Reporting criteria: há instâncias registradas Estatísticas: as estatísticas mais úteis são `Average` e `Minimum`. Essas estatísticas são determinadas pelos nós do load balancer. Observe que alguns nós do load balancer podem determinar que uma instância não é saudável por um breve período, enquanto outros nós determinam que ela é saudável. Exemplo: consulte `HealthyHostCount`.

As métricas a seguir permitem estimar os custos caso você migre um Classic Load Balancer para um Application Load Balancer. Essas métricas devem ser usadas apenas para fins informativos, e não com alarmes do CloudWatch. Observe que, se o Classic Load Balancer tiver vários listeners, essas métricas serão agregadas entre eles.

Essas estimativas se baseiam em um load balancer com uma regra padrão e um certificado com 2K. Se você usa um certificado de 4K ou mais, recomendamos estimar os custos da seguinte maneira: crie um Application Load Balancer com base no Classic Load Balancer usando a ferramenta de migração e monitore a métrica `ConsumedLCUs` para o Application Load Balancer. Para obter mais informações, consulte Migrar um Classic Load Balancer para um Application Load Balancer no Manual do usuário do Elastic Load Balancing.

Métrica	Descrição
`EstimatedALBActiveConnectionCount`	O número estimado de conexões TCP simultâneas ativas de clientes com o load balancer e do load balancer com destinos.

Métrica	Descrição
`EstimatedALBConsumedLCUs`	O número estimado de unidades de capacidade do balanceador de carga (LCU) usadas por um Application Load Balancer. Você paga pelo número de LCUs que usa por hora. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing.
`EstimatedALBNewConnectionCount`	O número estimado de novas conexões TCP estabelecidas de clientes com o load balancer e do load balancer com destinos.
`EstimatedProcessedBytes`	O número estimado de bytes processados por um Application Load Balancer.

Dimensões métricas dos Classic Load Balancers

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

Dimensão	Descrição
`AvailabilityZone`	Filtra os dados da métrica pela zona de disponibilidade especificada.
`LoadBalancerName`	Filtra os dados da métrica pelo load balancer especificado.

Estatísticas para métricas do Classic Load Balancer

O CloudWatch fornece estatísticas com base nos pontos de dados da métrica publicados pelo Elastic Load Balancing. As estatísticas são agregações de dados de métrica ao longo de um período especificado. Quando você solicita estatísticas, o fluxo de dados apresentado é identificado pelo nome da métrica e pela dimensão. Dimensão é um par de nome/valor que identifica exclusivamente uma métrica. Por exemplo, você pode solicitar estatísticas de todas as instâncias EC2 íntegras por atrás de um load balancer iniciado em uma Zona de disponibilidade específica.

As estatísticas `Minimum` e `Maximum` refletem o mínimo e o máximo relatados por cada um dos nós do load balancer. Por exemplo, vamos supor que existam 2 nós no load balancer. Um nó tem `HealthyHostCount` com `Minimum` de 2, `Maximum` de 10 e `Average` de 6, enquanto o outro nó tem `HealthyHostCount` com `Minimum` de 1, `Maximum` de 5 e `Average` de 3. Assim, o load balancer tem `Minimum` de 1, `Maximum` de 10 e `Average` de cerca de 4.

A estatística `Sum` é o valor agregado entre todos os nós do load balancer. Como as métricas incluem vários relatórios por período, `Sum` só será aplicável às métricas agregadas em todos os nós do load balancer, como `RequestCount`, `HTTPCode_ELB_XXX`, `HTTPCode_Backend_XXX`, `BackendConnectionErrors` e `SpilloverCount`.

A estatística `SampleCount` é o número de amostras medidas. Como as métricas são obtidas com base em intervalos de amostragem e eventos, essa estatística normalmente não é útil. Por exemplo, com `HealthyHostCount`, `SampleCount` se baseia no número de amostras que cada nó do load balancer relata, não no número de hosts íntegros.

Um percentil indica a posição relativa de um valor no dataset. Você pode especificar qualquer percentil usando até duas casas decimais (por exemplo, p95.45). Por exemplo, 95º percentil significa que 95% dos dados está abaixo desse valor e 5% está acima. Percentis geralmente são usados para isolar anomalias. Por exemplo, vamos supor que um aplicativo atende à maioria das solicitações de um cache em 1-2 ms, mas em 100-200 ms se o cache estiver vazio. O máximo reflete o caso mais lento, cerca de 200 ms. A média não indica a distribuição dos dados. Percentis fornecem uma visão mais significativa da performance do aplicativo. eAo usar o 99.º percentil como acionador do Auto Scaling ou alarme do

CloudWatch, você pode determinar que não mais de 1% das solicitações demore mais do que 2 ms para serem processadas.

Visualizar métricas do CloudWatch para o balanceador de carga

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

Como alternativa, você pode visualizar as métricas do seu balanceador de carga usando o 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. No painel de navegação, em LOAD BALANCING (BALANCEAMENTO DE CARGA), escolha Load balancers (Balanceadores de carga).
3. Selecione seu load balancer.
4. Escolha a guia Monitoring (Monitoramento).
5. (Opcional) Para filtrar os resultados de acordo com o horário, selecione um período na opção Exibindo os dados de.
6. Para obter uma visualização maior de uma única métrica, selecione seu gráfico. As seguintes métricas estão disponíveis:

   - Hosts íntegros – `HealthyHostCount`
   - Hosts não íntegros – `UnHealthyHostCount`
   - Latência média – `Latency`
   - Solicitações de soma – `RequestCount`
   - Erros de conexão do back-end – `BackendConnectionErrors`
   - Comprimento da fila de sobretensão – `SurgeQueueLength`
   - Contagem de transmissão – `SpilloverCount`
   - Soma HTTP 2XXs – `HTTPCode_Backend_2XX`
   - Soma HTTP 4XXs – `HTTPCode_Backend_4XX`
   - Soma HTTP 5XXs – `HTTPCode_Backend_5XX`
   - Soma ELB HTTP 4XXs – `HTTPCode_ELB_4XX`
   - Soma ELB HTTP 5XXs – `HTTPCode_ELB_5XX`

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 ELB.
4. Execute um destes procedimentos:
   - Selecione uma dimensão métrica para visualizar as métricas por load balancer, por Zona de disponibilidade ou em todos os load balancers.
   - Para visualizar uma métrica em todas as dimensões, digite o nome no campo de pesquisa.
   - Para visualizar uma métrica de um único load balancer, digite o nome no campo de pesquisa.
   - Para visualizar uma métrica de uma única Zona de disponibilidade, digite o nome no campo de pesquisa.

Logs de acesso do seu Classic Load Balancer

O Elastic Load Balancing fornece logs de acesso que capturam informações detalhadas sobre as solicitações enviadas ao seu balanceador de carga. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor. Você pode usar esses logs de acesso para analisar padrões de tráfego e solucionar problemas.

O registro de logs de acesso é um recurso opcional do Elastic Load Balancing e é desabilitado por padrão. Depois de habilitar o registro de logs de acesso para seu balanceador de carga, o Elastic Load Balancing capturará os logs e os armazenará no bucket do Amazon S3 que você especificar. Você pode desativar o registro de acesso a qualquer momento.

Cada arquivo de log de acesso é automaticamente criptografado usando SSE-S3 antes de ser armazenado no bucket do S3 e descriptografado quando você o acessar. Não é necessário realizar nenhuma ação. A criptografia e a descriptografia são realizadas de forma transparente. Cada arquivo de log é criptografado com uma chave exclusiva, que é em si criptografada com uma chave mestra alternada regularmente. Para obter mais informações, consulte Proteção de dados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) no Manual do usuário do Amazon Simple Storage Service.

Não há cobrança adicional pelos logs de acesso. Os custos de armazenamento do Amazon S3 serão cobrados de você, mas não será cobrada a largura de banda usada pelo Elastic Load Balancing para enviar arquivos de log para o Amazon S3. Para obter mais informações sobre os custos de armazenamento, consulte Definição de preço do Amazon S3.

Índice

- Arquivos do log de acesso (p. 101)
- Entradas do log de acesso (p. 102)
- Processando logs de acesso (p. 105)
- Habilitar os logs de acesso do seu Classic Load Balancer (p. 105)
- Desabilitar os logs de acesso do seu Classic Load Balancer (p. 110)

Arquivos do log de acesso

O Elastic Load Balancing publica um arquivo de log para cada nó do balanceador de carga no intervalo especificado por você. Você pode especificar um intervalo de publicação de 5 minutos ou 60 minutos quando habilitar o log de acesso para seu load balancer. Por padrão, o Elastic Load Balancing publica logs em um intervalo de 60 minutos. Se o intervalo for definido para 5 minutos, os logs serão publicados às 1:05, 1:10, 1:15 e assim por diante. O início da entrega do log é atrasado em até 5 minutos se o intervalo for definido para 5 minutos, e em até 15 minutos se o intervalo for definido como 60 minutos. Você pode modificar o intervalo de publicação a qualquer momento.

O load balancer pode distribuir vários logs para o mesmo período. Isso normalmente acontece se o site tiver alto tráfego, vários nós do load balancer e um curto intervalo de publicação de log.

Os nomes dos arquivos dos logs de acesso usa o seguinte formato:

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-balancer-name_end-time_ip-address_random-string.log
```

bucket

O nome do bucket do S3.

prefixo

O prefixo (hierarquia lógica) no bucket. Se você não especificar um prefixo, os logs serão colocados no nível raiz do bucket.

aws-account-id

O ID da conta da AWS do proprietário.

região

A Região para seu load balancer e o bucket do S3.

aaaa/mm/dd

A data em que o log foi entregue.

load-balancer-name

O nome do load balancer.

end-time

A data e a hora em que o intervalo de registro terminou. Por exemplo, a hora de fim de 20140215T2340Z contém entradas para solicitações feitas entre 23:35 e 23:40, se o intervalo de publicação for de 5 minutos.

ip-address

O endereço IP do nó do load balancer que processou a solicitação. Para um load balancer interno, esse é um endereço IP privado.

random-string

Uma string aleatória gerada pelo sistema.

A seguir está um exemplo de nome de arquivo de log:

```
s3://my-loadbalancer-logs/my-app/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2014/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20140215T2340Z_172.160.001.192_20sg8hgm.log
```

Você pode armazenar os arquivos de log no bucket pelo tempo que desejar, mas também pode definir regras do ciclo de vida do Amazon S3 para arquivar ou excluir os arquivos de log automaticamente. Para obter mais informações, consulte Gerenciamento do ciclo de vida de objetos no Manual do usuário do Amazon Simple Storage Service.

Entradas do log de acesso

O Elastic Load Balancing registra as solicitações enviadas ao balanceador de carga, inclusive aquelas que nunca chegaram às instâncias backend. Por exemplo: se um cliente enviar uma solicitação mal formada ou se não houver instâncias íntegras para responder, as solicitações ainda assim são registradas.

Important

O Elastic Load Balancing registra as solicitações na base do melhor esforço. Recomendamos que você use logs de acesso para compreender a natureza das solicitações, não como uma contabilidade completa de todas as solicitações.

Sintaxe

Cada entrada de log contém os detalhes de uma única solicitação feita para o load balancer. Todos os campos na entrada de log são delimitados por espaços. Cada entrada no arquivo de log tem o seguinte formato:

```
timestamp elb client:port backend:port request_processing_time backend_processing_time
 response_processing_time elb_status_code backend_status_code received_bytes sent_bytes
 "request" "user_agent" ssl_cipher ssl_protocol
```

A tabela a seguir descreve os campos de uma entrada no log de acesso.

Campo	Descrição
hora	A hora em que o load balancer recebeu a solicitação do cliente, no formato ISO 8601.
elb	O nome do load balancer
client:port	O endereço IP e porta do cliente solicitante.
backend:port	O endereço IP e porta da instância registrada que processou essa solicitação. Se o load balancer não puder enviar a solicitação a uma instância registrada, ou se a instância fechar a conexão antes de uma resposta ser enviada, esse valor será definido como `-`. Esse valor também pode ser configurado como `-` se a instância registrada não responder antes do tempo limite de inatividade.
request_processing_time	[Listener do HTTP] O tempo total, em segundos, decorrido do momento em que o load balancer recebeu a solicitação até que foi enviado a uma instância registrada. [Listener do TCP] O tempo total, em segundos, decorrido do momento em que o load balancer aceitou uma conexão TCP/SSL de um cliente até o momento em que o load balancer envia o primeiro byte de dados a uma instância. Esse valor será configurado como `-1` se o load balancer não conseguir despachar a solicitação a uma instância registrada. Isso pode acontecer se a instância registrada fechar a conexão antes do tempo limite de inatividade ou se o cliente enviar uma solicitação malformada. Além disso, para listeners de TCP, isso pode acontecer se o cliente estabelecer uma conexão com o load balancer, mas não envia dado algum. Esse valor também pode ser configurado como `-1` se a instância registrada não responder antes do tempo limite de inatividade.
backend_processing_time	[Listener do HTTP] O tempo total, em segundos, decorrido desde momento em que o load balancer envia a solicitação até uma instância registrada, até que a instância comece a enviar os cabeçalhos de resposta. [Listener do TCP] O tempo total, em segundos, decorrido para o load balancer estabelecer uma conexão com êxito com uma instância registrada. Esse valor será configurado como `-1` se o load balancer não conseguir despachar a solicitação a uma instância registrada. Isso pode acontecer se a instância registrada fechar a conexão antes do tempo limite de inatividade ou se o cliente enviar uma solicitação malformada. Esse valor também pode ser configurado como `-1` se a instância registrada não responder antes do tempo limite de inatividade.
response_processing_time	[Listener do HTTP] O tempo total decorrido (em segundos) desde o momento em que o load balancer recebeu o cabeçalho de resposta da instância

Campo	Descrição
	registrada até que ele começou a enviar a resposta ao cliente. Isso inclui o tempo de fila no load balancer e o tempo de aquisição de conexão do load balancer ao cliente. [Listener do TCP] O tempo total decorrido (em segundos) desde o momento em que o load balancer recebeu o primeiro byte da instância registrada até que ele começou a enviar a resposta ao cliente. Esse valor será configurado como `-1` se o load balancer não conseguir despachar a solicitação a uma instância registrada. Isso pode acontecer se a instância registrada fechar a conexão antes do tempo limite de inatividade ou se o cliente enviar uma solicitação malformada. Esse valor também pode ser configurado como `-1` se a instância registrada não responder antes do tempo limite de inatividade.
elb_status_code	[Listener do HTTP] O código de status da resposta do load balancer.
backend_status_code	[Listener do HTTP] O código de status de resposta da instância registrada.
received_bytes	O tamanho da solicitação, em bytes, recebida do cliente (solicitante). [Listener do HTTP] O valor inclui o corpo da solicitação, mas não os cabeçalhos. [Listener do TCP] O valor inclui o corpo da solicitação e os cabeçalhos.
sent_bytes	O tamanho da resposta, em bytes, enviada ao cliente (solicitante). [Listener do HTTP] O valor inclui o corpo da resposta, mas não os cabeçalhos. [Listener do TCP] O valor inclui o corpo da solicitação e os cabeçalhos.
request	A linha de solicitação do cliente entre aspas duplas e registradas no seguinte formato: método HTTP + Protocolo://Cabeçalho do host:porta + Caminho + versão HTTP. O load balancer preserva o URL enviado pelo cliente, da forma como se encontra, ao gravar o URI da solicitação. Ele não define o tipo de conteúdo para o arquivo do log de acesso. Ao processar esse campo, considere como o cliente enviou o URL. [Listener do TCP] O URL é três traços, cada um separado por um espaço, terminando com um espaço ("- - - ").
user_agent	[Listener do HTTP/HTTPS] Uma string usuário-agente que identifica o cliente que originou a solicitação. A string consiste em um ou mais identificadores de produto, produto[/versão]. Se a string tiver mais de 8 KB, ela ficará truncada.
ssl_cipher	[Listener HTTPS/SSL] A cifra do SSL. Esse valor só será registrado se a conexão SSL/TLS de entrada tiver sido estabelecida após uma negociação bem-sucedida. Caso contrário, o valor será configurado como `-`.
ssl_protocol	[Listener HTTPS/SSL] O protocolo SSL. Esse valor só será registrado se a conexão SSL/TLS de entrada tiver sido estabelecida após uma negociação bem-sucedida. Caso contrário, o valor será configurado como `-`.

Exemplos

Entrada HTTP de exemplo

A seguir está uma entrada no log de exemplo para um listener do HTTP (porta 80 para porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.000073
 0.001048 0.000057 200 200 0 29 "GET http://www.example.com:80/ HTTP/1.1" "curl/7.38.0" - -
```

Entrada HTTPS de exemplo

A seguir está uma entrada no log de exemplo para um listener HTTPS (porta 443 para porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.000086
 0.001048 0.001337 200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1" "curl/7.38.0"
 DHE-RSA-AES128-SHA TLSv1.2
```

Entrada TCP de exemplo

A seguir está uma entrada no log de exemplo para um listener do TCP (porta 8080 para porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001069
 0.000028 0.000041 - - 82 305 "- - - " "-" - -
```

Entrada SSL de exemplo

A seguir está uma entrada no log de exemplo para um listener do SSL (porta 8443 para porta 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001065
 0.000015 0.000023 - - 57 502 "- - - " "-" ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2
```

Processando logs de acesso

Se houver uma grande demanda no seu site, o load balancer poderá gerar arquivos de log com gigabytes de dados. Você pode não conseguir processar uma quantidade tão grande de dados usando o processamento linha por linha. Assim, pode ter de usar ferramentas analíticas que forneçam soluções de processamento paralelo. Por exemplo, você pode usar as ferramentas analíticas a seguir para analisar e processar logs de acesso:

- O Amazon Athena é um serviço de consultas interativas que facilita a análise de dados no Amazon S3 usando SQL padrão. Para obter mais informações, consulte Consultar logs do Classic Load Balancer no Manual do usuário do Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

Habilitar os logs de acesso do seu Classic Load Balancer

Para habilitar os logs de acesso do seu balanceador de carga, você deve especificar o nome do bucket do amazon S3 em que o balanceador de carga armazenará os logs. Você também deve anexar uma política de buckets para esse bucket que conceda permissão ao Elastic Load Balancing para gravar no bucket.

Important

O bucket e o load balancer devem estar na mesma Região. O bucket pode pertencer a uma conta diferente daquela que controla o load balancer.

Tarefas

- Etapa 1: Crie um bucket do S3 (p. 106)
- Etapa 2: Anexe uma política ao seu bucket do S3 (p. 106)
- Etapa 3: Habilite os logs de acesso (p. 108)
- Etapa 4: Verifique se o balanceador de carga criou um arquivo de teste no bucket do S3 (p. 109)

Etapa 1: Crie um bucket do S3

Você pode criar um bucket do S3 usando o console do Amazon S3. Se você já tiver um bucket e quiser usá-lo para armazenar os logs de acesso, ignore esta etapa e vá para Etapa 2: Anexe uma política ao seu bucket do S3 (p. 106) para conceder permissão ao Elastic Load Balancing para gravar logs no seu bucket.

Tip

Se você usar o console para habilitar os logs de acesso, poderá ignorar esta etapa e deixar o Elastic Load Balancing criar para você um bucket com as permissões necessárias. Se você usar a AWS CLI para habilitar os logs de acesso, deverá criar o bucket e conceder as permissões necessárias.

Requisitos

- O bucket deve estar localizado na mesma região que o load balancer.
- São necessárias chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Nenhuma outra opção de criptografia é compatível.

Para criar um bucket do S3 usando o console do Amazon S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Create bucket (Criar bucket).
3. Na página Criar bucket (Criar bucket), faça o seguinte:
   a. Para Bucket Name (Nome do bucket), digite um nome para o seu bucket. Esse nome deve ser exclusivo entre todos os nomes de buckets existentes no Amazon S3. Em algumas regiões, talvez haja restrições adicionais quanto a nomes de buckets. Para obter mais informações, consulte Restrições e limitações de bucket no Manual do usuário do Amazon Simple Storage Service.
   b. Em Region (Região), selecione a Região em que você criou seu load balancer.
   c. Escolha Create (Criar OpsItem).

Etapa 2: Anexe uma política ao seu bucket do S3

Depois de criar ou identificar seu bucket do S3, anexe uma política ao bucket. As políticas de bucket são um conjunto de instruções JSON gravadas na linguagem de políticas de acesso para definir permissões de acesso para o seu bucket. Cada instrução inclui informações sobre uma única permissão e contém uma série de elementos.

Se o seu bucket já tiver uma política anexada, você poderá adicionar as instruções para o log de acesso do Elastic Load Balancing à política. Se você fizer isso, recomendamos que avalie o conjunto resultante

de permissões para garantir que eles são apropriadas para os usuários que precisam de acesso ao bucket para logs de acesso.

> **Tip**
>
> Se você usar o console para habilitar os logs de acesso, poderá ignorar esta etapa e deixar o Elastic Load Balancing criar para você um bucket com as permissões necessárias.

Para anexar uma instrução de política ao seu bucket

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione o bucket. Escolha Permissions (Permissões) e escolha Bucket Policy (Política de bucket).
3. Se você estiver criando uma nova política de bucket, copie todo esse documento de política para o editor de políticas e substitua os espaços reservados pelo nome e pelo prefixo do bucket, pelo ID da conta da AWS do Elastic Load Balancing (com base na região do balanceador de carga) e pelo ID da sua própria conta da AWS. Se você estiver editando uma política de bucket existente, copie apenas a nova instrução do documento de política (o texto entre [e] do elemento `Statement`).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/your-aws-account-id/*"
    }
  ]
}
```

A tabela a seguir contém os IDs de conta a serem usados em sua política de bucket.

Região	Nome da região	ID da conta do Elastic Load Balancing
`us-east-1`	Leste dos EUA (Norte da Virgínia)	127311923021
`us-east-2`	Leste dos EUA (Ohio)	033677994240
`us-west-1`	US West (N. California)	027434742980
`us-west-2`	Oeste dos EUA (Oregon)	797873946194
`af-south-1`	Africa (Cape Town)	098369216593
`ca-central-1`	Canada (Central)	985666609251
`eu-central-1`	Europa (Frankfurt)	054676820928
`eu-west-1`	Europa (Irlanda)	156460612806
`eu-west-2`	Europa (Londres)	652711504416
`eu-south-1`	Europe (Milan)	635631232127
`eu-west-3`	Europa (Paris)	009996457667

Região	Nome da região	ID da conta do Elastic Load Balancing
eu-north-1	Europe (Stockholm)	897822967062
ap-east-1	Asia Pacific (Hong Kong)	754344448648
ap-northeast-1	Ásia-Pacífico (Tóquio)	582318560864
ap-northeast-2	Ásia-Pacífico (Seul)	600734575887
ap-northeast-3	Asia Pacific (Osaka)	383597477331
ap-southeast-1	Ásia-Pacífico (Cingapura)	114774131450
ap-southeast-2	Ásia-Pacífico (Sydney)	783225319266
ap-south-1	Asia Pacific (Mumbai)	718504428378
me-south-1	Middle East (Bahrain)	076674570225
sa-east-1	América do Sul (São Paulo)	507241528517
us-gov-west-1*	AWS GovCloud (EUA-Oeste)	048591011584
us-gov-east-1*	AWS GovCloud (EUA-Leste)	190560391635
cn-north-1*	China (Beijing)	638102146993
cn-northwest-1*	China (Ningxia)	037604701340

* Essas Regiões requerem uma conta separada. Para obter mais informações, consulte AWS GovCloud (EUA-Oeste) e China (Pequim).

4. Escolha Save (Salvar).

Etapa 3: Habilite os logs de acesso

Você pode habilitar os logs de acesso usando o AWS Management Console ou a AWS CLI. Observe que, quando você habilitar os logs de acesso usando o console, poderá fazer com que o Elastic Load Balancing crie o bucket para você com as permissões necessárias para que o balanceador de carga grave no seu bucket.

Use o exemplo a seguir para capturar e entregar logs ao seu bucket do S3 a cada 60 minutos (o intervalo padrão).

Para habilitar os logs de acesso ao seu load balancer usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em LOAD BALANCING (BALANCEAMENTO DE CARGA), escolha Load balancers (Balanceadores de carga).
3. Selecione seu load balancer.
4. Na guia Descrição, selecione Configurar logs de acesso.
5. Na página Configurar logs de acesso, faça o seguinte:

a. Selecione Habilitar logs de acesso.
b. Deixe Intervalo como a seleção padrão, `60 minutes`.
c. Em Local do S3, digite o nome do bucket do S3, incluindo o prefixo (por exemplo, `my-loadbalancer-logs/my-app`). Você pode especificar o nome de um bucket existente ou um nome para um novo bucket.
d. (Opcional) Se o bucket não existir, selecione Criar este local para mim. Você deve especificar um nome exclusivo entre todos os nomes de buckets existentes no Amazon S3 e seguir as convenções de nomeação do DNS. Para obter mais informações, consulte as Regras para nomear buckets no Manual do usuário do Amazon Simple Storage Service.
e. Escolha Save (Salvar).

Para habilitar os logs de acesso ao seu load balancer usando a AWS CLI

Primeiro, crie um arquivo .json que permita ao Elastic Load Balancing capturar e entregar logs a cada 60 minutos ao bucket do S3 que você criou para os logs:

```
{
  "AccessLog": {
    "Enabled": true,
    "S3BucketName": "my-loadbalancer-logs",
    "EmitInterval": 60,
    "S3BucketPrefix": "my-app"
  }
}
```

Para habilitar os logs de acesso, especifique o arquivo .json no comando modify-load balancer-atributos da seguinte forma:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes file://my-json-file.json
```

Esta é uma resposta de exemplo:

```
{
    "LoadBalancerAttributes": {
        "AccessLog": {
            "Enabled": true,
            "EmitInterval": 60,
            "S3BucketName": "my-loadbalancer-logs",
            "S3BucketPrefix": "my-app"
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Etapa 4: Verifique se o balanceador de carga criou um arquivo de teste no bucket do S3

Após o log de acesso ser habilitado para o seu balanceador de carga, o Elastic Load Balancing validará o bucket do S3 e criará um arquivo de teste. Você pode usar o console do S3 para verificar se o arquivo de teste foi criado.

Para verificar se o Elastic Load Balancing criou um arquivo de teste no seu bucket do S3

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

2. Selecione seu bucket do S3.
3. Navegue até o bucket que você especificou para o registro de acesso e procure `ELBAccessLogTestFile`. Por exemplo, se você tiver usado o console para criar o bucket e a política de bucket, o caminho será o seguinte:

```
my-bucket/prefix/AWSLogs/123456789012/ELBAccessLogTestFile
```

Gerenciar o bucket do S3 para os logs de acesso

Após habilitar o registro de acesso em logs, lembre-se de desabilitá-lo antes de excluir o bucket com os logs de acesso. Caso contrário, se houver um novo bucket com o mesmo nome e a política de bucket necessária criada em uma conta da AWS que não seja a sua, o Elastic Load Balancing poderá gravar os logs de acesso do seu balanceador de carga nesse novo bucket.

Desabilitar os logs de acesso do seu Classic Load Balancer

Você pode desabilitar os logs de acesso para seu load balancer a qualquer momento. Depois de desabilitar o registro de logs de acesso, seus logs permanecerão no seu Amazon S3 até que você os exclua. Para obter mais informações sobre como gerenciar o bucket do S3, consulte Como trabalhar com buckets no Manual do usuário do Amazon Simple Storage Service.

Para desabilitar o registro de logs de acesso usando o console

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em LOAD BALANCING (BALANCEAMENTO DE CARGA), escolha Load balancers (Balanceadores de carga).
3. Selecione seu load balancer.
4. Na guia Descrição, selecione Configurar logs de acesso.
5. Na página Configurar logs de acesso, desmarque a opção Habilitar logs de acesso.
6. Escolha Save (Salvar).

Para desabilitar o registro de logs de acesso usando a AWS CLI

Use o comando modify-load-balancer-attributes para desabilitar o log de acesso:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"AccessLog\":{\"Enabled\":false}}"
```

Esta é uma resposta de exemplo:

```
{
    "LoadBalancerName": "my-loadbalancer",
    "LoadBalancerAttributes": {
        "AccessLog": {
            "S3BucketName": "my-loadbalancer-logs",
            "EmitInterval": 60,
            "Enabled": false,
            "S3BucketPrefix": "my-app"
        }
    }
}
```

Registro de chamadas de API para seu Classic 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.

Para monitorar outras ações para o load balancer, como quando um cliente faz uma solicitação para seu load balancer, use os logs de acesso. Para mais informações, consulte Logs de acesso do seu Classic Load Balancer (p. 101).

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 os 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, você pode configurar outros produtos da AWS para analisar mais profundamente e agir sobre os 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
- Recebimento de arquivos de log do CloudTrail de várias regiões
- Recebimento de arquivos de log do CloudTrail de várias contas

Todas as ações do Elastic Load Balancing para Classic Load Balancers são registradas pelo CloudTrail e documentadas na Referência da API do Elastic Load Balancing versão 2012-06-01. 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 raiz ou do AWS Identity and Access Management (IAM).
- 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 Classic 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": "AIDAJDPLRKLG7UEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-12345678","subnet-76543210"],
        "loadBalancerName": "my-load-balancer",
        "listeners": [{
           "protocol": "HTTP",
           "loadBalancerPort": 80,
           "instanceProtocol": "HTTP",
           "instancePort": 80
        }]
    },
    "responseElements": {
        "dNSName": "my-loadbalancer-1234567890.elb.amazonaws.com"
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
```

```
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
    "recipientAccountId": "123456789012"
}
```

Example Exemplo: DeleteLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJDPLRKLG7UEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-08T12:39:25Z",
    "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": {
        "loadBalancerName": "my-load-balancer"
    },
    "responseElements": null,
    "requestID": "f0f17bb6-b9ba-11e3-9b20-999fdEXAMPLE",
    "eventID": "4f99f0e8-5cf8-4c30-b6da-3b69fEXAMPLE"
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
    "recipientAccountId": "123456789012"
}
```

Solução dos problemas do seu balanceador de carga clássico

As tabelas a seguir listam os recursos para soluções de problemas que você achará úteis à medida que trabalhar com um balanceador de carga clássico.

Erros de API

Erro
CertificateNotFound: Undefined (certificado não encontrado: indefinido) (p. 115)
OutofService: A transient error occurred (Fora de serviço: ocorreu um erro temporário) (p. 116)

Erros de HTTP

Erro
HTTP 400: BAD_REQUEST (p. 117)
HTTP 405: METHOD_NOT_ALLOWED (p. 117)
HTTP 408: Request Timeout (HTTP 408: limite de tempo de solicitação) (p. 117)
HTTP 502: Bad Gateway (HTTP 502: gateway incorreto) (p. 117)
HTTP 503: Service Unavailable (HTTP 503: serviço indisponível) (p. 117)
HTTP 504: Gateway Timeout (HTTP 504: limite de tempo do gateway) (p. 118)

Métricas do código de resposta

Métrica do código de resposta
HTTPCode_ELB_4XX (p. 119)
HTTPCode_ELB_5XX (p. 119)
HTTPCode_Backend_2XX (p. 119)
HTTPCode_Backend_3XX (p. 119)
HTTPCode_Backend_4XX (p. 119)
HTTPCode_Backend_5XX (p. 120)

Problemas de verificação de integridade

Problema
Erro na página de destino da verificação de integridade (p. 120)

Problema
A conexão com as instâncias expirou (p. 121)
A autenticação de chave pública não está funcionando (p. 122)
A instância não está recebendo tráfego do load balancer (p. 122)
As portas da instância não estão abertas (p. 122)
As instâncias em um grupo do Auto Scaling estão falhando na verificação de integridade do ELB (p. 123)

Problemas de conectividade

Problema
Os clientes não conseguem se conectar ao load balancer (p. 123)

Problemas de registro de instância

Problema
O registro de uma instância EC2 está demorando muito (p. 124)
Não é possível registrar uma instância iniciada a partir de uma AMI paga (p. 124)

Solução dos problemas de um balanceador de carga clássico: erros da API

A seguir, estão mensagens de erro apresentadas pela API do Elastic Load Balancing, as possíveis causas e as etapas que você pode seguir para resolver os problemas.

Mensagens de erro

- CertificateNotFound: Undefined (certificado não encontrado: indefinido) (p. 115)
- OutofService: A transient error occurred (Fora de serviço: ocorreu um erro temporário) (p. 116)

CertificateNotFound: Undefined (certificado não encontrado: indefinido)

Causa 1: há um atraso na propagação do certificado para todas as regiões quando ele é criado usando o AWS Management Console. Quando esse atraso ocorre, a mensagem de erro é mostrada na última etapa do processo de criação do load balancer.

Solução 1: aguarde aproximadamente 15 minutos e tente novamente. Se o problema persistir, vá para o AWS Support Center para obter assistência.

Cause 2 (Causa 2): se você está usando a AWS CLI ou a API diretamente, pode receber esse erro se fornecer um nome de recurso da Amazon (ARN) para um certificado que não existe.

Solução 2: use a ação do Identity and Access Management (IAM) GetServerCertificate para obter o ARN do certificado e verificar se você forneceu o valor correto para o ARN.

OutofService: A transient error occurred (Fora de serviço: ocorreu um erro temporário)

Causa: há um problema interno temporário dentro do serviço do Elastic Load Balancing ou da rede subjacente. Esse problema temporário também poderá ocorrer quando o Elastic Load Balancing consultar a integridade do balanceador de carga e de suas instâncias registradas.

Solução: tentar a chamada de API novamente. Se o problema persistir, vá para o AWS Support Center para obter assistência.

Solução dos problemas de um balanceador de carga clássico: erros de HTTP

O método HTTP (também chamado verbo) especifica a ação a ser executada no recurso que recebe uma solicitação HTTP. Os métodos padrão para solicitações HTTP são definidos na RFC 2616, Definições do método. Entre os métodos padrão estão GET, POST, PUT, HEAD e OPTIONS. Alguns aplicativos Web exigem (e, às vezes, introduzem) métodos que são extensões de métodos HTTP/1.1. Exemplos comuns de métodos estendidos de HTTP incluem PATCH, REPORT, MKCOL, PROPFIND, MOVE e LOCK. O Elastic Load Balancing aceita todos os métodos HTTP padrão e não padrão.

As solicitações de HTTP e as respostas usam campos de cabeçalho para enviar informações sobre as mensagens HTTP. Os campos de cabeçalho são pares de nome-valor separados por dois pontos separados por um retorno de carro (CR) e um avanço de linha (LF). Um conjunto padrão de campos de cabeçalho HTTP está definido na RFC 2616, Cabeçalhos de mensagem. Para obter mais informações, consulte Cabeçalhos HTTP e balanceadores de carga clássicos (p. 38).

Quando um load balancer receber uma solicitação HTTP, ele verificará solicitações malformadas e tamanho do método. O tamanho total do método em uma solicitação HTTP para um load balancer não deve ultrapassar 127 caracteres. Se a solicitação HTTP for aprovada nas duas verificações, o load balancer enviará a solicitação à instância EC2. Se o campo do método na solicitação estiver malformada, o load balancer responderá com um erro HTTP 400: BAD_REQUEST (p. 117). Se a duração do método na solicitação exceder 127 caracteres, o load balancer responderá com um erro HTTP 405: METHOD_NOT_ALLOWED (p. 117).

A instância EC2 processa uma solicitação válida ao implementar o método na solicitação e enviar uma resposta de volta para o cliente. Suas instâncias deverão ser configuradas para lidar com métodos suportados e não suportados.

A seguir estão mensagens de erro apresentadas pelo seu load balancer, as possíveis causas e as etapas que você pode tomar para resolver o problema.

Mensagens de erro

- HTTP 400: BAD_REQUEST (p. 117)
- HTTP 405: METHOD_NOT_ALLOWED (p. 117)
- HTTP 408: Request Timeout (HTTP 408: limite de tempo de solicitação) (p. 117)
- HTTP 502: Bad Gateway (HTTP 502: gateway incorreto) (p. 117)
- HTTP 503: Service Unavailable (HTTP 503: serviço indisponível) (p. 117)
- HTTP 504: Gateway Timeout (HTTP 504: limite de tempo do gateway) (p. 118)

HTTP 400: BAD_REQUEST

Descrição: indica que o cliente enviou uma solicitação incorreta.

Cause 1 (Causa 1): o cliente enviou uma solicitação malformada que não atende às especificações de HTTP. Por exemplo, uma solicitação não pode ter espaços no URL.

Causa 2: o cliente usou o método HTTP CONNECT, que não é compatível com o Elastic Load Balancing.

Solução: conecte-se diretamente à instância e capture os detalhes da solicitação do cliente. Analise os cabeçalhos e o URL quanto a solicitações malformadas. Verifique se a solicitação atende às especificações de HTTP. Verifique se o HTTP CONNECT não foi usado.

HTTP 405: METHOD_NOT_ALLOWED

Descrição: indica que o tamanho do método não é válido.

Causa: o tamanho do método no cabeçalho da solicitação excede 127 caracteres.

Solução: verifique o tamanho do método.

HTTP 408: Request Timeout (HTTP 408: limite de tempo de solicitação)

Descrição: indica que o cliente cancelou a solicitação ou não enviou uma solicitação completa.

Causa 1: uma interrupção da rede ou uma construção de solicitação incorreta, como cabeçalhos parcialmente formados, o tamanho do conteúdo especificado não corresponder ao tamanho real do conteúdo transmitido, etc.

Solução 1: inspecione o código que está fazendo a solicitação e tente enviá-lo diretamente às instâncias registradas (ou um ambiente de desenvolvimento/teste) onde você tem mais controle sobre a inspeção da solicitação em si.

Causa 2: a conexão com o cliente está fechada (o load balancer não pôde enviar uma resposta).

Solução 2: verifique se o cliente não está fechando a conexão antes de uma resposta ser enviada usando um packet sniffer (analisador de pacotes) na máquina fazendo a solicitação.

HTTP 502: Bad Gateway (HTTP 502: gateway incorreto)

Descrição: indica que o load balancer não conseguiu analisar a resposta enviada de uma instância registrada.

Causa: uma resposta malformada da instância ou, possivelmente, um problema com o load balancer.

Solução: verifique se a resposta sendo enviada da instância está em conformidade com as especificações de HTTP. Vá para o AWS Support Center para obter assistência.

HTTP 503: Service Unavailable (HTTP 503: serviço indisponível)

Descrição: indica que o load balancer ou as instâncias registradas estão causando o erro.

Causa 1: capacidade insuficiente no load balancer para lidar com a solicitação.

Solução 1: deve ser um problema temporário que deve durar apenas alguns minutos. Se o problema persistir, vá para o AWS Support Center para obter assistência.

Cause 2 (Causa 2): não há nenhuma instância registrada.

Solução 2: registre pelo menos uma instância em cada zona de disponibilidade em que seu load balancer foi configurado para responder. Verifique observando as métricas de `HealthyHostCount` no CloudWatch. Se você não puder garantir que uma instância é registrada em cada Zona de disponibilidade, recomendamos ativar o balanceamento de carga entre zonas. Para obter mais informações, consulte Configurar o balanceamento de carga entre zonas para seu balanceador de carga clássico (p. 73).

Cause 3 (Causa 3): não há nenhuma instância íntegra.

Solução 3: verifique se você tem instâncias íntegras em cada zona de disponibilidade em que seu load balancer foi configurado para responder. Verifique isso analisando a métrica `HealthyHostCount`.

Cause 4 (Causa 4): a fila de pico está cheia.

Solution 4 (Solução 4): garanta que suas instâncias tenham capacidade suficiente para lidar com a taxa de solicitações. Verifique isso analisando a métrica `SpilloverCount`.

HTTP 504: Gateway Timeout (HTTP 504: limite de tempo do gateway)

Descrição: indica que o load balancer fechou uma conexão, pois uma solicitação não foi concluída dentro do tempo limite de inatividade.

Causa 1: o aplicativo leva mais tempo para responder do que o tempo limite de inatividade configurado.

Solução 1: monitore as métricas `HTTPCode_ELB_5XX` e `Latency`. Se houver um aumento nessas métricas, pode ser porque o aplicativo não respondeu dentro do período de tempo limite de inatividade. Para obter detalhes sobre as solicitações que ultrapassam esse limite, habilite os logs de acesso no balanceador de carga e analise os códigos de resposta 504 nos logs gerados pelo Elastic Load Balancing. Se necessário, você pode aumentar a capacidade ou aumentar o tempo limite de inatividade configurado de forma que as operações demoradas (como o upload de um arquivo grande) possam ser concluídas. Para obter mais informações, consulte Configurar o tempo limite de inatividade da conexão para seu balanceador de carga clássico (p. 72) e Como solucionar problemas de alta latência do Elastic Load Balancing.

Causa 2: as instâncias registradas estão fechando a conexão ao Elastic Load Balancing.

Solução 2: habilite as configurações do keep-alive nas instâncias do EC2 e verifique se o tempo limite do keep-alive é maior do que as configurações de tempo limite de inatividade do load balancer.

Solução dos problemas de um balanceador de carga clássico: métricas do código de resposta

Seu balanceador de carga envia métricas ao Amazon CloudWatch para os códigos de resposta HTTP enviados para clientes, identificando a origem de erros como o balanceador de carga ou como as instâncias registradas. Você pode usar as métricas apresentadas pelo CloudWatch a seu balanceador de carga para solucionar problemas. Para obter mais informações, consulte Métricas do CloudWatch para seu Classic Load Balancer (p. 93).

A seguir, estão as métricas do código de resposta apresentadas pelo CloudWatch a seu balanceador de carga, as possíveis causas e as etapas que você pode seguir para resolver os problemas.

Métricas do código de resposta

- HTTPCode_ELB_4XX (p. 119)
- HTTPCode_ELB_5XX (p. 119)
- HTTPCode_Backend_2XX (p. 119)
- HTTPCode_Backend_3XX (p. 119)
- HTTPCode_Backend_4XX (p. 119)
- HTTPCode_Backend_5XX (p. 120)

HTTPCode_ELB_4XX

Causa: uma solicitação malformada ou cancelada do cliente.

Solutions

- Consulte HTTP 400: BAD_REQUEST (p. 117).
- Consulte HTTP 405: METHOD_NOT_ALLOWED (p. 117).
- Consulte HTTP 408: Request Timeout (HTTP 408: limite de tempo de solicitação) (p. 117).

HTTPCode_ELB_5XX

Causa: o load balancer ou a instância registrada está causando o erro ou o load balancer não está conseguindo analisar a resposta.

Solutions

- Consulte HTTP 502: Bad Gateway (HTTP 502: gateway incorreto) (p. 117).
- Consulte HTTP 503: Service Unavailable (HTTP 503: serviço indisponível) (p. 117).
- Consulte HTTP 504: Gateway Timeout (HTTP 504: limite de tempo do gateway) (p. 118).

HTTPCode_Backend_2XX

Causa: uma resposta normal e bem-sucedida das instâncias registradas.

Solução: nenhuma.

HTTPCode_Backend_3XX

Causa: uma resposta de redirecionamento enviada das instâncias registradas.

Solução: visualize os logs de acesso ou os logs de erro na instância para determinar a causa. Envie solicitações diretamente para a instância (ignorando o load balancer) para exibir as respostas.

HTTPCode_Backend_4XX

Causa: uma resposta de erro do cliente enviada pelas instâncias registradas.

Solução: visualize os logs de acesso ou de erro nas instâncias para determinar a causa. Envie solicitações diretamente para a instância (ignore o load balancer) para exibir as respostas.

Note

Se o cliente cancelar uma solicitação HTTP iniciada com um cabeçalho `Transfer-Encoding: chunked`, há um problema conhecido no qual o load balancer encaminha a solicitação para a instância, ainda que o cliente tenha cancelado a solicitação. Isso pode causar erros de back-end.

HTTPCode_Backend_5XX

Causa: uma resposta de erro do servidor enviada das instâncias registradas.

Solução: visualize os logs de acesso ou os logs de erro nas instâncias para determinar a causa. Envie solicitações diretamente para a instância (ignore o load balancer) para exibir as respostas.

Note

Se o cliente cancelar uma solicitação HTTP iniciada com um cabeçalho `Transfer-Encoding: chunked`, há um problema conhecido no qual o load balancer encaminha a solicitação para a instância, ainda que o cliente tenha cancelado a solicitação. Isso pode causar erros de back-end.

Solução dos problemas de um balanceador de carga clássico: verificações de integridade

Seu balanceador de carga verifica a integridade das instâncias registradas usando a configuração padrão de verificação de integridade fornecida pelo Elastic Load Balancing ou uma configuração de verificação de integridade personalizada que você especificar. A configuração de verificação de integridade contém informações como protocolo, porta de ping, caminho de ping, tempo limite de resposta e intervalo de verificação de integridade. Uma instância é considerada íntegra se retornar um código de resposta 200 dentro do intervalo de verificação de integridade. Para obter mais informações, consulte Configurar as verificações de integridade do seu balanceador de carga clássico (p. 16).

Se o estado atual de algumas ou todas as suas instâncias for `OutOfService` e o campo de descrição exibir a mensagem `Instance has failed at least the Unhealthy Threshold number of health checks consecutively`, as instâncias terão falhado na verificação de integridade do load balancer. A seguir estão os problemas a serem procurados, as possíveis causas e as etapas que você pode tomar para resolver os problemas.

Problemas

- Erro na página de destino da verificação de integridade (p. 120)
- A conexão com as instâncias expirou (p. 121)
- A autenticação de chave pública não está funcionando (p. 122)
- A instância não está recebendo tráfego do load balancer (p. 122)
- As portas da instância não estão abertas (p. 122)
- As instâncias em um grupo do Auto Scaling estão falhando na verificação de integridade do ELB (p. 123)

Erro na página de destino da verificação de integridade

Problema: uma solicitação HTTP GET emitida para a instância na porta e no caminho de ping especificados (por exemplo, HTTP:80/index.html) recebe um código de resposta diferente de 200.

Causa 1: nenhuma página de destino foi configurada na instância.

Solução 1: crie uma página de destino (por exemplo, `index.html`) em cada instância registrada e especifique seu caminho como o caminho de ping.

Causa 2: o valor do cabeçalho Content-Length na resposta não está definido.

Solução 2: se a resposta inclui um corpo, defina o cabeçalho Content-Length para um valor maior ou igual a zero ou defina o valor de Transfer-Encoding para "chunked" (em partes).

Causa 3: o aplicativo não foi configurado para receber solicitações do load balancer nem para retornar um código de resposta 200.

Solução 3: verifique o aplicativo na instância para investigar a causa.

A conexão com as instâncias expirou

Problema: as solicitações de verificação de integridade do load balancer para as instâncias do EC2 estão expirando ou apresentando falhas intermitentemente.

Primeiro, verifique o problema conectando-se diretamente com a instância. Recomendamos que você se conecte à sua instância de dentro da rede usando o endereço IP privado da instância.

Use o comando a seguir para uma conexão TCP:

```
telnet private-IP-address-of-the-instance port
```

Use o comando a seguir para uma conexão HTTP ou HTTPS:

```
curl -I private-IP-address-of-the-instance:port/health-check-target-page
```

Se você estiver usando uma conexão HTTP/HTTPS e recebendo uma resposta não 200, consulte Erro na página de destino da verificação de integridade (p. 120). Se você for capaz de se conectar diretamente com a instância, verifique o seguinte:

Causa 1: a instância está falhando ao responder dentro do tempo limite de resposta configurado.

Solução 1: ajuste as configurações de tempo limite de resposta na configuração de verificação de integridade do load balancer.

Causa 2: a instância está sob uma carga significativa e está demorando mais do que o tempo limite de resposta configurado para responder.

Solução 2:

- Verifique o gráfico de monitoramento quanto à superutilização de CPU. Para obter mais informações, consulte Obter estatísticas para uma instância do EC2 específica no Manual do usuário do Amazon EC2 para instâncias do Linux.
- Verifique a utilização de recursos de outros aplicativos, como memória ou limites, conectando-se às suas instâncias EC2.
- Se necessário, adicione mais instâncias ou habilite o Auto Scaling. Para mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

Causa 3: se você está usando uma conexão HTTP ou HTTPS e a verificação de integridade está sendo executada em uma página de destino especificada no campo de caminho de ping (por exemplo, `HTTP:80/index.html`), pode ser que a página de destino precise de mais tempo para responder do que o tempo limite configurado.

Solução 3: use uma página de destino de verificação de integridade mais simples ou ajuste as configurações do intervalo de verificação de integridade.

A autenticação de chave pública não está funcionando

Problema: um load balancer configurado para usar o protocolo HTTPS ou SSL com a autenticação de back-end habilitada falha ao autenticar a chave pública.

Causa: a chave pública no certificado SSL não corresponde à chave pública configurada no load balancer. Use o comando `s_client` para ver a lista de certificados no servidor na cadeia de certificação. Para obter mais informações, consulte s_client na documentação do OpenSSL.

Solução: talvez você precise atualizar seu certificado SSL. Se o seu certificado SSL estiver atualizado, tente reinstalá-lo no seu load balancer. Para obter mais informações, consulte Substituir o certificado SSL do seu balanceador de carga clássico (p. 65).

A instância não está recebendo tráfego do load balancer

Problema: o security group da instância está bloqueando o tráfego do load balancer.

Faça uma captura de pacotes na instância para verificar o problema. Use o seguinte comando :

```
# tcpdump port health-check-port
```

Causa 1: o security group associado à instância não permite tráfego do load balancer.

Solução 1: edite o security group da instância para permitir o tráfego do load balancer. Adicione uma regra para permitir todo o tráfego do security group do load balancer.

Causa 2: o security group do load balancer em uma VPC não permite tráfego para instâncias do EC2.

Solução 2: edite o security group do load balancer para permitir o tráfego para as sub-redes e instâncias do EC2.

Para obter mais informações sobre o gerenciamento de security groups para EC2-Classic, consulte Grupos de segurança para instâncias do EC2-Classic (p. 24).

Para obter mais informações sobre o gerenciamento de security groups para uma VPC, consulte Grupos de segurança para balanceadores de carga em uma VPC (p. 20).

As portas da instância não estão abertas

Problema: a verificação de integridade enviada à instância do EC2 pelo load balancer está bloqueada pela porta ou por um firewall.

Verifique o problema usando o seguinte comando:

```
netstat -ant
```

Causa: a porta de integridade ou a porta do listener especificada (se configurada de outra maneira) não está aberta. Tanto a porta especificada para a verificação de integridade quanto a porta do listener devem estar abertas e ouvindo.

Solução: abra a porta do listener e a porta especificadas na configuração de verificação de integridade (se configurada de outra maneira) nas instâncias para receber tráfego do load balancer.

As instâncias em um grupo do Auto Scaling estão falhando na verificação de integridade do ELB

Problema: as instâncias no grupo do Auto Scaling são aprovadas na verificação de integridade padrão do Auto Scaling, mas não na verificação de integridade do ELB.

Causa: o Auto Scaling usa as verificações de status do EC2 para detectar problemas de hardware e software com as instâncias, mas o balanceador executa verificações de integridade enviando uma solicitação à instância e aguardando um código de resposta 200 ou estabelecendo uma conexão TCP (para uma verificação de integridade baseada em TCP) com a instância.

Uma instância pode falhar na verificação de integridade do ELB porque um aplicativo em execução na instância tem problemas que fazem com que o load balancer a considere fora de serviço. Essa instância pode ser aprovada na verificação de integridade do Auto Scaling. Ela não seria substituída pela política do Auto Scaling, porque é considerada íntegra com base na verificação de status do EC2.

Solução: use a verificação de integridade do ELB para o grupo do Auto Scaling. Quando você usa a verificação de integridade do ELB, o Auto Scaling determina o status da integridade de suas instâncias ao verificar os resultados tanto da verificação de status da instância quanto da verificação de integridade do ELB. Para obter mais informações, consulte Adicionar verificações de integridade ao grupo do Auto Scaling no Manual do usuário do Amazon EC2 Auto Scaling.

Solução dos problemas de um balanceador de carga clássico: conectividade do cliente

Se o balanceador de carga voltado para a Internet em uma VPC não estiver respondendo às solicitações, verifique o seguinte:

Seu balanceador de carga voltado para a Internet está anexado a uma sub-rede privada

Verifique se você especificou sub-redes públicas para seu load balancer. Uma sub-rede pública tem uma rota para o gateway da Internet para sua Virtual Private Cloud (VPC).

Um security group ou Network ACL não permite o tráfego

O security group para o load balancer e quaisquer Network ACLs para as sub-redes do load balancer devem permitir tráfego de entrada dos clientes e de saída para os clientes nas portas do listener. Para obter mais informações, consulte Grupos de segurança para balanceadores de carga em uma VPC (p. 20).

Solução dos problemas de um balanceador de carga clássico: registro de instância

Quando você registra uma instância com seu load balancer, há uma série de etapas executadas antes de o load balancer começar a enviar solicitações para sua instância.

A seguir estão problemas que seu load balancer pode encontrar ao registrar suas instâncias EC2, as possíveis causas e as etapas que você pode tomar para resolver os problemas.

Problemas

- O registro de uma instância EC2 está demorando muito (p. 124)

- Não é possível registrar uma instância iniciada a partir de uma AMI paga (p. 124)

O registro de uma instância EC2 está demorando muito

Problema: as instâncias do EC2 registradas estão demorando muito mais do que o esperado para entrarem no estado `InService`.

Causa: sua instância pode estar sendo reprovada na verificação de integridade. Após as etapas iniciais do registro da instância serem concluídas (pode levar aproximadamente 30 segundos), o load balancer iniciará o envio de solicitações de verificação de integridade. Sua instância não estará `InService` até que uma verificação de integridade seja bem-sucedida.

Solução: consulte A conexão com as instâncias expirou (p. 121).

Não é possível registrar uma instância iniciada a partir de uma AMI paga

Problema: o Elastic Load Balancing não está registrando uma instância iniciada usando uma AMI paga.

Causa: suas instâncias podem ter sido executadas usando uma AMI paga do Amazon DevPay.

Solução: o Elastic Load Balancing não oferece suporte ao registro de instâncias iniciadas usando AMIs pagas do Amazon DevPay. Observe que você pode usar AMIs pagas do AWS Marketplace. Se você já estiver usando uma AMI paga do AWS Marketplace e não conseguir registrar uma instância iniciada a partir dessa AMI paga, consulte o AWS Support Center para obter assistência.

Cotas para o seu Classic Load Balancer

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.

Para visualizar as cotas para os Classic Load Balancers, abra o console do Service Quotas. No painel de navegação, selecione AWS services (Serviços da AWS) e Elastic Load Balancing. Também é possível usar o comando describe-account-limits (AWS CLI) para o Elastic Load Balancing.

Para solicitar o aumento da cota, consulte Requesting a Quota Increase (Solicitar um aumento de cota) no Manual do usuário do Service Quotas.

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

Nome	Padrão	Ajustável
Classic Load Balancers por região	20	Sim
Listeners por Classic Load Balancer	100	Sim
Instâncias registradas por Classic Load Balancer	1.000	Sim

Histórico do documento

A tabela a seguir descreve todos os lançamentos dos balanceadores de carga clássicos.

Recurso	Descrição	Data de lançamento
Modo de mitigação da dessincronização	Adicionado suporte para o modo de mitigação de dessincronização. Para obter mais informações, consulte Configurar o modo de mitigação de dessincronização para o balanceador de carga clássico (p. 86).	17 de agosto de 2020
Classic Load Balancers	Com o lançamento dos balanceadores de carga da aplicação e balanceadores de carga da rede, os balanceadores de carga criados com a API 2016-06-01 agora são conhecidos como balanceadores de carga clássicos. Para obter mais informações sobre as diferenças entre esses tipos de balanceadores de carga, consulte O que é o Elastic Load Balancing no Manual do usuário do Elastic Load Balancing.	11 de agosto de 2016
Suporte para o AWS Certificate Manager (ACM)	Você pode solicitar um certificado de SSL/TLS do ACM e implantá-lo no seu balanceador de carga. Para obter mais informações, consulte Certificados SSL/TLS para balanceadores de carga clássicos (p. 40).	21 de janeiro de 2016
Suporte a portas adicionais	Os load balancers de uma VPC podem ouvir em qualquer porta do intervalo 1-65535. Para obter mais informações, consulte Listeners para seu balanceador de carga clássico (p. 34).	15 de setembro de 2015
Campos adicionais para entradas de log de acesso	Adicionados os campos `user_agent`, `ssl_cipher` e `ssl_protocol`. Para obter mais informações, consulte Arquivos do log de acesso (p. 101).	18 de maio de 2015
Suporte para registrar instâncias vinculadas do EC2-Classic	Adicionado suporte para registrar instâncias vinculadas do EC2-Classic no seu load balancer.	19 de janeiro de 2015
Suporte para marcação com tags do seu load balancer	Você pode usar tags para organizar e gerenciar seus load balancers. A partir desta versão, a CLI do Elastic Load Balancing (ELB CLI) foi substituída pela AWS Command Line Interface (AWS CLI), uma ferramenta unificada para gerenciar vários serviços da AWS. Novos recursos lançados após a ELB CLI versão 1.0.35.0 (datada de 24/jul/14) serão incluídos somente na AWS CLI. Se você estiver usando atualmente a ELB CLI, recomendamos que, em vez disso, comece a usar a AWS CLI. Para obter mais informações, consulte o Manual do usuário da AWS Command Line Interface.	11 de agosto de 2014

Recurso	Descrição	Data de lançamento
Tempo limite de inatividade da conexão	Você pode configurar o tempo limite de inatividade para seu load balancer.	24 de julho de 2014
Suporte para a concessão de acesso a usuários e grupos do IAM a ações específicas dos load balancers ou API	Você pode criar uma política do IAM para conceder aos usuários e grupos do IAM acesso a load balancers ou ações da API específicos.	12 de maio de 2014
Suporte ao AWS CloudTrail	Você pode usar o CloudTrail para capturar chamadas de API efetuadas por, ou em nome de, sua conta da AWS usando a API do ELB, o AWS Management Console, a CLI do ELB ou a AWS CLI. Para obter mais informações, consulte Registro de chamadas de API para seu Classic Load Balancer usando o AWS CloudTrail (p. 111).	04 de abril de 2014
Drenagem de conexão	Adicionadas informações sobre drenagem de conexão. Com esse suporte você pode ativar seu load balancer para interromper o envio de novas solicitações para a instância registrada quando o registro da instância estiver sendo cancelado ou quando a instância perder a integridade, ao mesmo tempo mantendo as conexões existentes abertas. Para obter mais informações, consulte Configurar a descarga da conexão para seu balanceador de carga clássico (p. 76).	20 de março de 2014
Logs de acesso	Você pode habilitar que seu load balancer capture informações detalhadas sobre as solicitações enviadas para o seu load balancer e armazene-as em um bucket do S3. Para obter mais informações, consulte Logs de acesso do seu Classic Load Balancer (p. 101).	06 de março de 2014
Suporte para TLSv1.1-1.2	Adicionadas informações sobre o suporte ao protocolo TLSv1.1-1.2 para load balancers configurados com listeners HTTPS/SSL. Com esse suporte, o Elastic Load Balancing também atualiza as configurações de negociação SSL predefinidas. Para obter informações sobre as configurações de negociação SSL predefinidas atualizadas, consulte Configurações de negociação SSL para balanceadores de carga clássicos (p. 41). Para obter informações sobre a atualização de sua configuração atual de negociação SSL, consulte Atualizar a configuração de negociação SSL do seu balanceador de carga clássico (p. 67).	19 de fevereiro de 2014
Balanceamento de carga entre zonas	Adição de informações sobre como habilitar o balanceamento de carga entre zonas para seu load balancer. Para obter mais informações, consulte Configurar o balanceamento de carga entre zonas para seu balanceador de carga clássico (p. 73)	06 de novembro de 2013

Recurso	Descrição	Data de lançamento
Métricas adicionais do CloudWatch	Adicionadas informações sobre as métricas adicionais do Cloudwatch relatadas pelo Elastic Load Balancing. Para obter mais informações, consulte Métricas do CloudWatch para seu Classic Load Balancer (p. 93).	28 de outubro de 2013
Suporte para o protocolo de proxy	Adicionadas informações sobre o suporte ao protocolo de proxy para balanceadores de carga configurados para conexões TCP/SSL. Para obter mais informações, consulte Cabeçalho do protocolo de proxy (p. 78).	30 de julho de 2013
Suporte para failover de DNS	Adicionadas informações sobre como configurar o failover de DNS do Route 53 para load balancers. Para obter mais informações, consulte Configure o failover de DNS para o seu balanceador de carga (p. 91).	03 de junho de 2013
Suporte do console para visualizar métricas do CloudWatch e criar alarmes	Adicionadas informações sobre a visualização de métricas do CloudWatch e criação de alarmes para um determinado load balancer usando o console. Para obter mais informações, consulte Métricas do CloudWatch para seu Classic Load Balancer (p. 93).	28 de março de 2013
Suporte para registrar instâncias EC2 em uma VPC padrão	Adicionado suporte para instâncias EC2 executadas em uma VPC padrão.	11 de março de 2013
Balanceadores de carga internos	Com esta versão, um balanceador de carga em uma Virtual Private Cloud (VPC) pode ser definido como interno ou voltado para a Internet. Um load balancer interno tem um nome DNS publicamente resolvido que resolve para endereços IP privados. Um balanceador de carga voltado para a Internet tem um nome DNS publicamente resolvido, que resolve para endereços IP públicos. Para obter mais informações, consulte Criar um balanceador de carga clássico interno (p. 11).	10 de junho de 2012
Suporte do console ao gerenciamento de listeners, configurações de cifras e certificados SSL	Para obter informações, consulte Configurar um listener HTTPS para seu balanceador de carga clássico (p. 62) e Substituir o certificado SSL do seu balanceador de carga clássico (p. 65).	18 de maio de 2012
Suporte ao Elastic Load Balancing na Amazon VPC	Adicionado suporte para a criação de um load balancer em uma VPC.	21 de novembro de 2011
Amazon CloudWatch	Você pode monitorar seu balanceador de carga usando o CloudWatch. Para obter mais informações, consulte Métricas do CloudWatch para seu Classic Load Balancer (p. 93).	17 de outubro de 2011

Recurso	Descrição	Data de lançamento
Recursos de segurança adicionais	Você pode configurar o cifras SSL, SSL de back-end e autenticação de servidor back-end. Para obter mais informações, consulte Criar um balanceador de carga clássico com um listener HTTPS (p. 48).	30 de agosto de 2011
Nome de domínio do apex de zona	Para obter mais informações, consulte Configure um nome de domínio personalizado para seu balanceador de carga clássico (p. 90).	24 de maio de 2011
Bloqueio de instância	Você pode usar o grupo de segurança fornecido pelo Elastic Load Balancing para bloquear sua instância backend. Para obter mais informações, consulte Grupos de segurança para instâncias do EC2-Classic (p. 24).	24 de maio de 2011
Suporte para IPv6	Você pode usar o protocolo de Internet versão 6 (IPv6) com o load balancer no EC2-Classic.	24 de maio de 2011
Suporte para cabeçalhos X-Forwarded-Proto e X-Forwarded-Port	O cabeçalho X-Forwarded-Proto indica o protocolo da solicitação de origem, e o cabeçalho X-Forwarded-Port indica a porta da solicitação de origem. A adição desses cabeçalhos às solicitações permite que os clientes determinem se uma solicitação recebida para seu load balancer é criptografada, e a porta específica no load balancer na qual a solicitação foi recebida. Para obter mais informações, consulte Cabeçalhos HTTP e balanceadores de carga clássicos (p. 38).	27 de outubro de 2010
Suporte para HTTPS	Com esta versão, você pode utilizar o protocolo SSL/TLS para criptografar o tráfego e descarregar o processamento SSL da instância do aplicativo para o load balancer. Esse recurso também oferece o gerenciamento centralizado de certificados de servidor SSL no load balancer, em vez de gerenciar certificados em instâncias do aplicativo individuais.	14 de outubro de 2010
Suporte ao AWS Identity and Access Management (IAM)	Adicionado suporte ao IAM.	02 de setembro de 2010
Sticky sessions	Para obter mais informações, consulte Configurar sessões persistentes para seu balanceador de carga clássico (p. 81).	07 de abril de 2010
AWS SDK for Java	Adicionado suporte a SDK for Java.	22 de março de 2010
AWS SDK for .NET	Adicionado suporte para o AWS SDK for .NET.	11 de novembro de 2009
Novo serviço	Lançamento beta público inicial do Elastic Load Balancing.	18 de maio de 2009