aws

Classic Load Balancers

Elastic Load Balancing

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

Elastic Load Balancing: Classic Load Balancers

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

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

Table of Contents

O que é um balanceador de carga clássico? 1
Visão geral do balanceador de carga clássico 1
Benefícios 2
Como começar a usar 3
Definição de preço 3
Balanceadores de carga voltados para a Internet 4
DNSNomes públicos para seu balanceador de carga 4
Criar um balanceador de carga voltado para a Internet 5
Antes de começar 5
Crie um Classic Load Balancer usando o AWS Management Console 6
Balanceadores de carga internos 9
DNSNome público do seu balanceador de carga 10
Criar um balanceador de carga interno 11
Pré-requisitos 11
Criar um balanceador de carga interno usando o console 11
Crie um balanceador de carga interno usando o AWS CLI 14
Configurar o balanceador de carga 17
Tempo limite de inatividade da conexão 17
Configurar o tempo limite de inatividade usando o console 18
Configurar o tempo limite de inatividade usando a AWS CLI 19
Balanceamento de carga entre zonas 19
Habilitar o balanceamento de carga entre zonas 20
Desabilitar o balanceamento de carga entre zonas 21
Drenagem de conexão 23
Habilitar a descarga da conexão 24
Desabilitar a descarga da conexão 25
Sessões persistentes 26
Persistência da sessão com base na duração 27
Persistência da sessão controlada pela aplicação 30
Modo de mitigação de dessincronização 33
Classificações 34
Modos 35
Modificar o modo de mitigação de dessincronização 36
Protocolo de proxy 36

Cabeçalho do protocolo de proxy ... 37
Pré-requisitos para habilitar o protocolo de proxy ... 38
Habilitar o protocolo de proxy usando a AWS CLI ... 38
Desabilitar o protocolo de proxy usando a AWS CLI ... 40
Tags ... 41
Restrições de tags ... 42
Adicione um tag ... 42
Remover uma marcação ... 43
Sub-redes e zonas ... 43
Requisitos ... 44
Adicionar uma sub-rede ... 45
Remover uma sub-rede ... 46
Grupos de segurança ... 47
Regras recomendadas para os grupos de segurança do balanceador de carga ... 47
Atribua grupos de segurança usando o console ... 49
Atribua grupos de segurança usando o AWS CLI ... 50
Rede ACLs ... 50
Nome de domínio personalizado ... 52
Como associar seu nome de domínio personalizado com o nome do seu balanceador de carga ... 53
Usando o DNS failover do Route 53 para seu balanceador de carga ... 54
Dissociar seu nome de domínio personalizado do seu balanceador de carga ... 55
Listeners ... 56
Protocolos ... 56
TCP/SSLprotocolo ... 57
HTTP/HTTPSprotocolo ... 57
HTTPS/SSLouvintes ... 58
SSLcertificados de servidor ... 58
SSLnegociação ... 58
Autenticação do servidor backend ... 59
Configurações do listener ... 59
Cabeçalhos X-Forwarded ... 62
X-Forwarded-For ... 63
X-Forwarded-Proto ... 64
X-Forwarded-Port ... 64
HTTPSouvintes ... 65

SSL/TLScertificados 66
Crie ou importe um TLS certificadoSSL/usando AWS Certificate Manager 67
Importe um TLS certificadoSSL/usando IAM 67
SSLconfigurações de negociação 67
Políticas de segurança 68
SSLprotocolos 69
Preferência ditada pelo servidor 69
SSLcifras 69
Políticas de SSL segurança predefinidas 73
Crie um HTTPS balanceador de carga 78
Pré-requisitos 78
Crie um HTTPS balanceador de carga usando o console 79
Crie um HTTPS balanceador de carga usando o AWS CLI 83
Configurar um HTTPS ouvinte 95
Pré-requisitos 96
Adicionar um HTTPS ouvinte usando o console 96
Adicione um HTTPS ouvinte usando o AWS CLI 98
Substitua o SSL certificado 100
Substitua o SSL certificado usando o console 100
Substitua o SSL certificado usando o AWS CLI 101
Atualizar a SSL configuração da negociação 102
Atualize a configuração SSL de negociação usando o console 103
Atualize a configuração SSL da negociação usando o AWS CLI 104
Instâncias registradas 109
Práticas recomendadas para as suas instâncias 109
Recomendações para o seu VPC 110
Registre instâncias com seu balanceador de carga 111
Registrar uma instância 112
Visualize as instâncias registradas em um balanceador de carga 113
Determine o balanceador de carga para uma instância registrada 113
Cancelar o registro de uma instância 113
Verificações de integridade 114
Configuração de verificação de integridade 115
Atualizar a configuração de verificação de integridade 118
Verificar a integridade das suas instâncias 118
Solucionar problemas das verificações de integridade 119

Grupos de segurança ... 119
Rede ACLs ... 120
Monitore seu balanceador de carga ... 122
CloudWatch métricas ... 122
Métricas do Classic Load Balancer ... 123
Dimensões métricas dos Classic Load Balancers ... 133
Estatísticas para métricas do Classic Load Balancer ... 133
Veja CloudWatch as métricas do seu balanceador de carga ... 134
Logs de acesso ... 136
Arquivos do log de acesso ... 137
Entradas do log de acesso ... 139
Processando logs de acesso ... 143
Habilitar logs de acesso ... 144
Desabilitar logs de acesso ... 152
CloudTrail troncos ... 153
Informações sobre o Elastic Load Balancing em CloudTrail ... 153
Noções básicas sobre entradas de arquivo de log do Elastic Load Balancing ... 154
Solução dos problemas do seu balanceador de carga ... 157
APIerros ... 159
CertificateNotFound: Indefinido ... 159
OutofService: Ocorreu um erro transitório ... 159
HTTPerros ... 160
HTTP400: BAD _ REQUEST ... 161
HTTP405: METHOD _ _ NOT ALLOWED ... 161
HTTP408: Tempo limite da solicitação ... 161
HTTP502: Gateway inválido ... 162
HTTP503: Serviço indisponível ... 162
HTTP504: Tempo limite do gateway ... 163
Métricas do código de resposta ... 163
HTTPCode_ ELB _4XX ... 164
HTTPCode_ ELB _5XX ... 164
HTTPCode_Backend_2xx ... 164
HTTPCode_Backend_3xx ... 164
HTTPCode_Backend_4xx ... 165
HTTPCode_Backend_5xx ... 165
Verificações de integridade ... 165

Erro na página de destino da verificação de integridade 166
A conexão com as instâncias expirou 167
A autenticação de chave pública não está funcionando 168
A instância não está recebendo tráfego do load balancer 168
As portas da instância não estão abertas 169
As instâncias em um grupo de Auto Scaling estão falhando na verificação de integridade ELB 169
Conectividade do cliente 170
Os clientes não conseguem se conectar a um balanceador de carga voltado para a Internet 170
As solicitações enviadas para um domínio personalizado não são recebidas pelo balanceador de carga. 170
HTTPSsolicitações enviadas para o balanceador de carga retornam "NET:: ERR _ CERT _ _ COMMON NAME _INVALID” 171
Registro de instância 171
Demorando muito para registrar uma EC2 instância 171
Não é possível registrar uma instância iniciada a partir de uma conta paga AMI 172
Cotas 173
Histórico do documento 174
..... clxxxiii

O que é um balanceador de carga clássico?

O Elastic Load Balancing distribui automaticamente seu tráfego de entrada em vários destinos, como EC2 instâncias, 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.

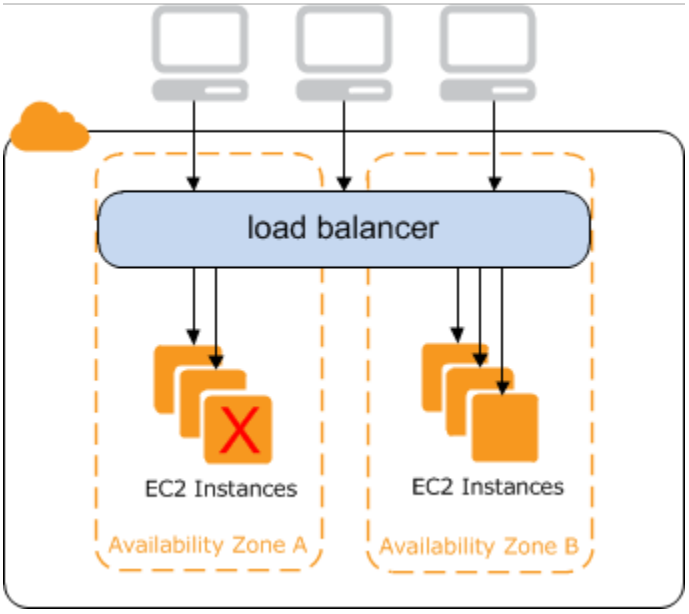
Visão geral do balanceador de carga clássico

Um balanceador de carga distribui o tráfego de entrada do aplicativo em várias EC2 instâncias em várias 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.

Benefícios

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

- Support para SSL ouvintes TCP e ouvintes

- 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

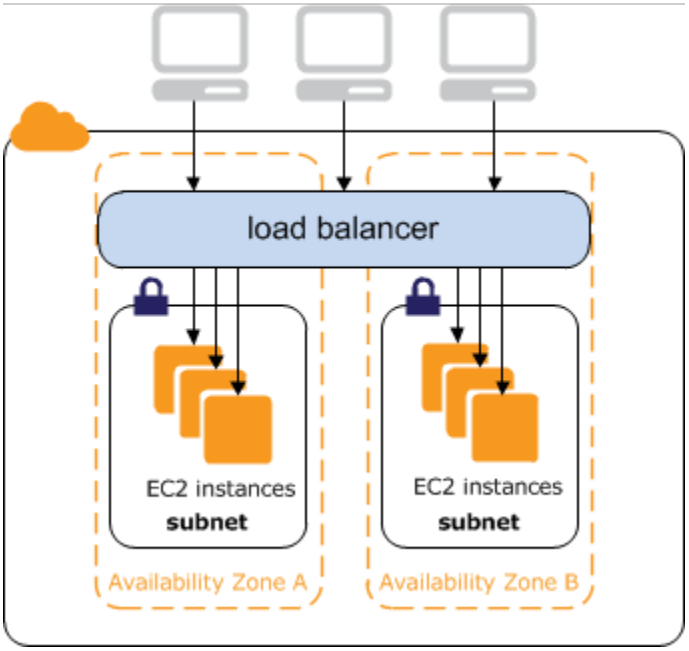
- Para saber como criar um Classic Load Balancer e registrar EC2 instâncias com ele, consulte. Crie um Classic Load Balancer voltado para a Internet
- Para saber como criar um balanceador de HTTPS carga e registrar EC2 instâncias com ele, consulteCrie um Classic Load Balancer com um ouvinte HTTPS.
- Para saber como usar os vários recursos compatíveis com os Classic Load Balancers, consulteConfigurar o Classic Load Balancer.

Definição de preço

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

Balanceadores de carga clássicos voltados para a Internet

Ao criar um Classic Load Balancer, você pode torná-lo um balanceador de carga interno ou um balanceador de carga voltado para a Internet. Um balanceador de carga voltado para a Internet tem um DNS nome que pode ser resolvido publicamente, portanto, ele pode rotear solicitações de clientes pela Internet para as EC2 instâncias registradas no balanceador de carga.



O DNS nome de um balanceador de carga interno pode ser resolvido publicamente nos endereços IP privados dos nós. Portanto, os balanceadores de carga internos só podem rotear solicitações de clientes com acesso ao VPC para o balanceador de carga. Para obter mais informações, consulte Balanceadores de carga internos.

Conteúdo

- DNSNomes públicos para seu balanceador de carga
- Crie um Classic Load Balancer voltado para a Internet

DNSNomes públicos para seu balanceador de carga

Quando seu balanceador de carga é criado, ele recebe um DNS nome público que os clientes podem usar para enviar solicitações. Os DNS servidores resolvem o DNS nome do seu balanceador de carga para os endereços IP públicos dos nós do balanceador de carga do seu balanceador

de carga. Cada nó do load balancer está conectado às instâncias back-end usando endereços IP privados.

O console exibe um DNS nome público com o seguinte formato:

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

Crie um Classic Load Balancer voltado para a Internet

Ao criar um balanceador de carga, você configura ouvintes, configura verificações de saúde e registra instâncias de 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.

Este tutorial fornece uma introdução prática aos Classic Load Balancers por meio da AWS Management Console, uma interface baseada na web. Você criará um balanceador de carga que recebe HTTP tráfego público e o envia para suas EC2 instâncias.

Para criar um balanceador de carga com um HTTPS ouvinte, consulte. Crie um Classic Load Balancer com um ouvinte HTTPS

Tarefas

- Antes de começar
- Crie um Classic Load Balancer usando o AWS Management Console

Antes de começar

- Crie uma nuvem privada virtual (VPC). Para obter mais informações, consulte Recomendações para o seu VPC.
- Execute as EC2 instâncias que você planeja registrar com seu balanceador de carga. Certifique-se de que os grupos de segurança dessas instâncias permitam HTTP acesso na porta 80.
- Instale um servidor web, como Apache ou Internet Information Services (IIS), em cada instância, digite seu DNS nome no campo de endereço de um navegador conectado à Internet e verifique se o navegador exibe a página padrão do servidor.

Crie um Classic Load Balancer usando o AWS Management Console

Use o procedimento a seguir para criar seu Classic Load Balancer. Forneça algumas informações básicas de configuração do seu balanceador de carga, como nome e esquema. Em seguida, forneça informações sobre sua rede e o receptor que roteia o tráfego para suas instâncias.

Para criar um Classic Load Balancer usando o console

1. Abra o EC2 console da Amazon 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 que você selecionou para suas EC2 instâncias.
3. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
4. Selecione Criar load balancer.
5. Expanda a seção Classic Load Balancer e escolha Criar.
6. Configuração básica
   a. Em Nome do balanceador de carga, digite um nome para o balanceador de carga.

      O nome de seu Classic Load Balancer deve ser exclusivo dentro de seu conjunto de Classic Load Balancers 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. Para Esquema, selecione Voltado para a Internet.
7. Mapeamento de rede
   a. Para VPC, selecione o mesmo VPC que você selecionou para suas instâncias.
   b. Para Mapeamentos, primeiro selecione uma zona de disponibilidade e escolha uma sub-rede pública entre as sub-redes disponíveis. Você pode selecionar somente uma sub-rede por zona de disponibilidade. Para melhorar a disponibilidade do seu balanceador de carga, selecione mais de uma zona de disponibilidade e sub-rede.
8. Grupos de segurança
   - Em Grupos de segurança, selecione um grupo de segurança existente configurado para permitir o HTTP tráfego necessário na porta 80.
9. Receptores e roteamento
   a. Para Receptor, certifique-se de que o protocolo seja HTTP e a porta seja 80.

b. Para Instância, certifique-se de que o protocolo seja `HTTP` e a porta seja `80`.

10. Verificações de integridade

    a. ParaProtocolo de ping, certifique-se de que o protocolo sejaHTTP.

    b. Para Porta de ping, certifique-se de que a porta seja`80`.

    c. Para Caminho do ping, certifique-se de que o caminho seja`/`.

    d. Para Configurações avançadas de verificação de integridade, use os valores padrão.

11. Instâncias

    a. Selecione Adicionar instâncias para abrir a tela de seleção de instâncias.

    b. Em Instâncias disponíveis, você pode selecionar entre as instâncias atuais que estão disponíveis para o balanceador de carga, com base nas configurações de rede atuais.

    c. Quando estiver satisfeito com suas seleções, selecione Confirmar para adicionar ao balanceador de carga as instâncias a serem registradas.

12. Atributos.

    • Em Habilitar balanceamento de carga entre zonas, Habilitar drenagem da conexão e Tempo limite (intervalo de drenagem), mantenha os valores padrão.

13. Tags do balanceador de carga (opcional)

    a. O campo Chave é obrigatório.

    b. O campo Valor é opcional.

    c. Para adicionar outra tag, selecione Adicionar nova tag, insira seus valores no campo Chave e, opcionalmente, no campo Valor.

    d. Para remover uma tag existente, selecione Remover ao lado da tag que você deseja remover.

14. Resumo e criação

    a. Caso precies alterar alguma configuração, selecione Editar ao lado da configuração que precisa ser alterada.

    b. Quando estiver satisfeito com as configurações mostradas no resumo, selecione Criar balanceador de carga para começar a criação do seu balanceador de carga.

    c. Na página de criação final, selecione Exibir balanceador de carga para visualizar seu balanceador de carga no console da AmazonEC2.

15. Verificar

a. Selecione o novo load balancer.

b. Na guia Instâncias de destino, marque a coluna Status de integridade. Depois que pelo menos uma de suas EC2 instâncias estiver em serviço, você poderá testar seu balanceador de carga.

c. Na seção Detalhes, copie o DNSnome dos balanceadores de carga, que seria semelhante a. `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`

d. Cole o DNSnome do balanceador de carga no campo de endereço de um navegador público conectado à Internet. Se o balanceador de carga estiver funcionando corretamente, você verá a página padrão do seu servidor.

16. Excluir (opcional)

a. Se você tiver um CNAME registro para seu domínio que aponte para seu balanceador de carga, aponte-o para um novo local e aguarde a DNS alteração entrar em vigor antes de excluir seu balanceador de carga.

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

c. Selecione o load balancer.

d. Escolha Ações, Excluir balanceador de carga.

e. Quando a confirmação for solicitada, digite `confirm` e escolha Delete.

f. Depois de excluir um balanceador de carga, as EC2 instâncias registradas com o balanceador de carga continuam em execução. Você será cobrado por cada hora parcial ou completa em que eles continuarem sendo executados. Quando não precisar mais de uma EC2 instância, você pode interrompê-la ou encerrá-la para evitar cobranças adicionais.

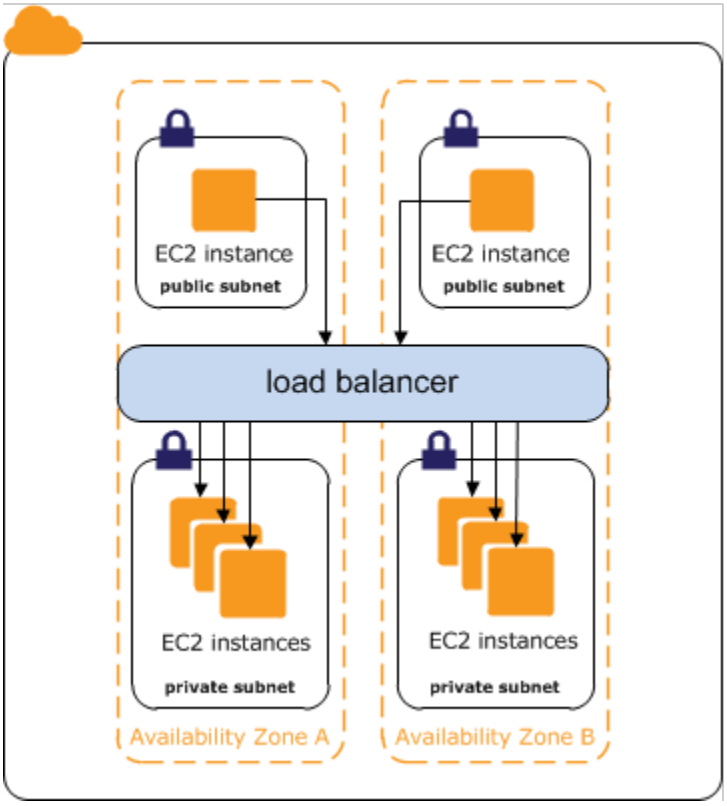
Classic Load Balancers internos

Ao criar um load balancer, você deverá optar se deve fazer dele um load balancer interno ou um load balancer voltado para a Internet.

Os nós de um load balancer voltado para a Internet têm endereços IP públicos. O DNS nome de um balanceador de carga voltado para a Internet pode ser resolvido publicamente nos 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.

Os nós de um load balancer interno têm somente endereços IP privados. O DNS nome de um balanceador de carga interno pode ser resolvido publicamente nos endereços IP privados dos nós. Portanto, os balanceadores de carga internos só podem rotear solicitações de clientes com acesso ao VPC para o balanceador de carga.

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.



Conteúdo

- DNSNome público do seu balanceador de carga
- Criar um Classic Load Balancer interno

DNSNome público do seu balanceador de carga

Quando um balanceador de carga interno é criado, ele recebe um DNS nome público com o seguinte formato:

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

Os DNS servidores resolvem o DNS nome do seu balanceador de carga para os endereços IP privados dos nós do balanceador de carga do seu balanceador de carga 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 Classic Load Balancer interno

Você pode criar um balanceador de carga interno para distribuir tráfego para suas EC2 instâncias de clientes com acesso ao VPC para o balanceador de carga.

Conteúdos

- Pré-requisitos
- Criar um balanceador de carga interno usando o console
- Crie um balanceador de carga interno usando o AWS CLI

Pré-requisitos

- Se você ainda não criou um VPC para seu balanceador de carga, deve criá-lo antes de começar. Para obter mais informações, consulte Recomendações para o seu VPC.
- Inicie as EC2 instâncias que você planeja registrar com seu balanceador de carga interno. Certifique-se de iniciá-los em sub-redes privadas na área VPC destinada ao balanceador de carga.

Criar um balanceador de carga interno usando o console

Use o procedimento a seguir para criar seu Classic Load Balancer interno. Forneça algumas informações básicas de configuração do seu balanceador de carga, como nome e esquema. Em seguida, forneça informações sobre sua rede e o receptor que direciona o tráfego para suas instâncias.

Para criar um Classic Load Balancer interno usando o console

1. Abra o EC2 console da Amazon 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 que você selecionou para suas EC2 instâncias.
3. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
4. Selecione Criar load balancer.
5. Expanda a seção Classic Load Balancer e escolha Criar.
6. Configuração básica

a. Em Nome do balanceador de carga, digite um nome para o balanceador de carga.

   O nome de seu Classic Load Balancer deve ser exclusivo dentro de seu conjunto de Classic Load Balancers 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. Para Esquema, selecione Interno.

7. Mapeamento de rede

   a. Para VPC, selecione o mesmo VPC que você selecionou para suas instâncias.

   b. Para Mapeamentos, primeiro selecione uma zona de disponibilidade e escolha uma sub-rede entre as sub-redes disponíveis. Você pode selecionar somente uma sub-rede por zona de disponibilidade. Para melhorar a disponibilidade do seu balanceador de carga, selecione mais de uma zona de disponibilidade e sub-rede.

8. Em Grupos de segurança, selecione um grupo de segurança existente configurado para permitir o HTTP tráfego necessário na porta 80. Se preferir, você pode criar um novo grupo de segurança se sua aplicação usar protocolos e portas diferentes.

9. Receptores e roteamento

   a. Para Receptor, certifique-se de que o protocolo seja `HTTP` e a porta seja `80`.

   b. Para Instância, certifique-se de que o protocolo seja `HTTP` e a porta seja `80`.

10. Verificações de integridade

    a. Para Protocolo de ping, o padrão é `HTTP`.

    b. Para Porta de ping , o padrão é`80`.

    c. Para Caminho de ping, o padrão é`/`.

    d. Para Configurações avançadas de verificação de integridade, use os valores padrão ou insira valores específicos para sua aplicação.

11. Instâncias

    a. Selecione Adicionar instâncias para abrir a tela de seleção de instâncias.

    b. Em Instâncias disponíveis, você pode selecionar entre as instâncias atuais que estão disponíveis para o balanceador de carga, com base nas configurações de rede selecionadas anteriormente.

    c. Quando estiver satisfeito com suas seleções, selecione Confirmar para adicionar ao balanceador de carga as instâncias a serem registradas.

12. Atributos.

    - Em Habilitar balanceamento de carga entre zonas, Habilitar drenagem da conexão e Tempo limite (intervalo de drenagem), mantenha os valores padrão.

13. Tags do balanceador de carga (opcional)

    a. O campo Chave é obrigatório.

    b. O campo Valor é opcional.

    c. Para adicionar outra tag, selecione Adicionar nova tag, insira seus valores no campo Chave e, opcionalmente, no campo Valor.

    d. Para remover uma tag existente, selecione Remover ao lado da tag que você deseja remover.

14. Resumo e criação

    a. Caso precies alterar alguma configuração, selecione Editar ao lado da configuração que precisa ser alterada.

    b. Quando estiver satisfeito com as configurações mostradas no resumo, selecione Criar balanceador de carga para começar a criação do seu balanceador de carga.

    c. Na página de criação final, selecione Exibir balanceador de carga para visualizar seu balanceador de carga no console da AmazonEC2.

15. Verificar

    a. Selecione o novo load balancer.

    b. Na guia Instâncias de destino, marque a coluna Status de integridade. Depois que pelo menos uma de suas EC2 instâncias estiver em serviço, você poderá testar seu balanceador de carga.

    c. Na seção Detalhes, copie o DNSnome dos balanceadores de carga, que seria semelhante a. `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`

    d. Cole o DNSnome do balanceador de carga no campo de endereço de um navegador público conectado à Internet. Se o balanceador de carga estiver funcionando corretamente, você verá a página padrão do seu servidor.

16. Excluir (opcional)

    a. Se você tiver um CNAME registro para seu domínio que aponte para seu balanceador de carga, aponte-o para um novo local e aguarde a DNS alteração entrar em vigor antes de excluir seu balanceador de carga.

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

c. Selecione o load balancer.

d. Escolha Ações, Excluir balanceador de carga.

e. Quando a confirmação for solicitada, digite `confirm` e escolha Delete.

f. Depois de excluir um balanceador de carga, as EC2 instâncias registradas com o balanceador de carga continuam em execução. Você será cobrado por cada hora parcial ou completa em que eles continuarem sendo executados. Quando não precisar mais de uma EC2 instância, você pode interrompê-la ou encerrá-la para evitar cobranças adicionais.

Crie um balanceador de carga interno usando o 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 balanceador de carga interno e registrar suas EC2 instâncias com o balanceador de carga interno recém-criado.

Para criar um load balancer interno

1. Use o create-load-balancercomando com a `--scheme` opção 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
```

O seguinte é um exemplo de resposta. 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 seguinte 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 describe-load-balancerscomando a seguir para verificar o balanceador de carga 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",
```

```
            ...
        }
    ]
}
```

Configurar o Classic Load Balancer

Depois de criar um Classic Load Balancer, você pode configurar seus atributos.

Drenagem da conexão

Se habilitado, o balanceador de carga permite que as solicitações existentes sejam concluídas antes que o balanceador de carga cancele o tráfego de uma instância não registrada ou não íntegra.

Balanceamento de carga entre zonas

Se habilitado, o balanceador de carga roteia o tráfego de solicitações de forma uniforme em todas as instâncias, independentemente das zonas de disponibilidade.

Dessincronizar o modo de migração

Determina como o balanceador de carga processa solicitações que possam representar risco de segurança para a sua aplicação. Os valores possíveis são `monitor`, `defensive` e `strictest`. O padrão é `defensive`.

Tempo limite de inatividade

Se habilitado, o balanceador de carga permite que as conexões permaneçam ociosas (nenhum dado é enviado pela conexão) pela duração especificada. O padrão é 60 segundos.

Sessões persistentes

Os Classic Load Balancers oferecem suporte à aderência de sessões com base na duração e na aplicação.

Configurar o tempo limite de inatividade da conexão para seu Classic Load Balancer

Para cada solicitação que um cliente faz por meio de um Classic Load Balancer, o balanceador de carga mantém duas conexões. A conexão front-end é entre o cliente e o load balancer. A conexão de back-end é entre o balanceador de carga e uma instância registrada. EC2 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 usa HTTP e HTTPS ouvintes, recomendamos que você habilite a opção HTTP keep-alive 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 balanceador de carga seja responsável por fechar as conexões com sua instância, certifique-se de que o valor definido para o tempo de manutenção de atividade seja maior do HTTP que a configuração de tempo limite de inatividade definida para seu balanceador de carga.

Observe que os TCP testes de manutenção de atividade não impedem que o balanceador de carga encerre a conexão porque não enviam dados na carga útil.

Conteúdo

- Configurar o tempo limite de inatividade usando o console
- Configurar o tempo limite de inatividade usando a AWS CLI

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 definir a configuração de tempo limite de inatividade para seu balanceador de carga usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, na seção Configuração de tráfego, insira 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 Salvar alterações.

Configurar o tempo limite de inatividade usando a AWS CLI

Use o modify-load-balancer-attributescomando a seguir para definir o tempo limite de inatividade do seu balanceador de carga:

```
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 Classic Load Balancer

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 balanceador de carga 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 armazenam DNS pesquisas em cache, as solicitações recebidas 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 Classic Load Balancer, o padrão para balanceamento de carga entre zonas depende de como você cria o balanceador de carga. Com o API ouCLI, 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 selecionada por padrão. Depois de criar um Classic Load Balancer, você pode habilitar ou desabilitar o balanceamento de carga entre zonas a qualquer momento.

Conteúdo

- Habilitar o balanceamento de carga entre zonas
- Desabilitar o balanceamento de carga entre zonas

Habilitar o balanceamento de carga entre zonas

Você pode habilitar o balanceamento de carga entre zonas para seu Classic Load Balancer a qualquer momento.

Para ativar o balanceamento de carga entre zonas usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, na seção Configuração de roteamento da zona de disponibilidade, habilite Balanceamento de carga entre zonas.
6. Escolha Salvar alterações.

Para habilitar o balanceamento de carga entre zonas usando o AWS CLI

1. Use o modify-load-balancer-attributescomando a seguir para definir o `CrossZoneLoadBalancing` atributo do seu balanceador de carga como`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 describe-load-balancer-attributescomando a seguir para verificar se o balanceamento de carga entre zonas está ativado para seu balanceador de carga:

```
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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, na seção Configuração de roteamento da zona de disponibilidade, desabilite Balanceamento de carga entre zonas.
6. Escolha Salvar alterações.

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 o AWS CLI

1. Use o seguinte 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 describe-load-balancer-attributescomando a seguir para verificar se o balanceamento de carga entre zonas está desativado para seu balanceador de carga:

```
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 Classic Load Balancer

Para garantir que o Classic Load Balancer 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.

Conteúdo

- Habilitar a descarga da conexão
- Desabilitar a descarga da conexão

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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, na seção Configuração de tráfego, selecione Habilitar drenagem da conexão.
6. (Opcional) Em Tempo limite (intervalo de drenagem), digite um valor entre 1 e 3.600 segundos. Caso contrário, o padrão de 300 segundos será usado.
7. Escolha Salvar alterações.

Para ativar a drenagem da conexão usando o AWS CLI

Use o seguinte 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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga , na seção Configuração de tráfego , desmarque Habilitar drenagem da conexão.
6. Escolha Salvar alterações.

Para desativar a drenagem da conexão usando o AWS CLI

Use o seguinte 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 sessões persistentes para seu Classic Load Balancer

Por padrão, um Classic Load Balancer 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.

Requisitos

- Um HTTPS balanceador de cargaHTTP//.
- Pelo menos uma instância íntegra em cada Zona de disponibilidade.

Compatibilidade

- A propriedade RFC for the path de um cookie permite sublinhados. No entanto, o Elastic Load Balancing URI codifica caracteres de sublinhado `%5F` porque alguns navegadores, como o Internet Explorer 7, esperam que os sublinhados sejam codificados como. URI `%5F` Devido ao potencial de impactar os navegadores que estão funcionando atualmente, o Elastic Load Balancing continua URI codificando 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 `secure` sinalizador ou `HttpOnly` sinalizador em um cookie de aderência de sessão controlado pelo aplicativo, ele também será definido 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.

Conteúdo

- Persistência da sessão com base na duração
- Persistência da sessão controlada pela aplicação

Persistência da sessão com base na duração

O balanceador de carga usa um cookie especial, AWSELB, para rastrear a instância de cada solicitação para cada ouvinte. 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 CORS (compartilhamento de recursos entre origens), alguns navegadores precisam ativar `SameSite=None; Secure` a aderência. Nesse caso, o Elastic Load Balancing cria

um segundo cookie de aderência AWSELBCORS, que inclui as mesmas informações do cookie de aderência original mais esse 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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Receptores, escolha Gerenciar receptores.
5. Na página Gerenciar receptores, localize o receptor a ser atualizado e escolha Editar em Durabilidade do cookie.
6. No pop-up Editar configuração de aderência do cookie, selecione Gerado pelo balanceador de carga.
7. (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.
8. Escolha Salvar alterações para fechar a janela pop-up.
9. Escolha Salvar alterações para retornar à página de detalhes do balanceador de carga.

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

1. Use o comando create-lb-cookie-stickiness-policy a seguir para criar uma política de aderência de cookies gerada pelo balanceador de carga com um período de expiração de cookies 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 seguinte comando set-load-balancer-policies-of-listener para ativar a aderência da sessão para o balanceador de carga 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 describe-load-balancerscomando a seguir para verificar se a política está 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-TLS-1-2-2017-01"
                    ]
                },
```

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

                ],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": [
                    "ELBSecurityPolicy-TLS-1-2-2017-01"
                ]
            },
            ...
        }
    ]
}
```

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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Receptores, escolha Gerenciar receptores.
5. Na página Gerenciar receptores, localize o receptor a ser atualizado e escolha Editar em Durabilidade do cookie.
6. Selecione Gerado pela aplicação.
7. Em Nome de cookie, digite o nome do cookie do aplicativo.
8. Escolha Salvar alterações.

Para ativar a aderência da sessão controlada pelo aplicativo usando o AWS CLI

1. Use o seguinte comando create-app-cookie-stickiness-policy para criar uma política de aderência de cookies 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 seguinte comando set-load-balancer-policies-of-listener para ativar a aderência da sessão para um balanceador de carga:

```
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 describe-load-balancerscomando a seguir para verificar se a política fixa 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-TLS-1-2-2017-01"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "TCP",
                        "InstanceProtocol": "TCP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [
                {
                        "PolicyName": "my-app-cookie-policy",
                        "CookieName": "my-app-cookie"
                    }
```

```
                ],
                "OtherPolicies": [
                    "ELBSecurityPolicy-TLS-1-2-2017-01"
                ]
            },
            ...
        }
    ]
}
```

Configurar o modo de mitigação de dessincronização para o Classic Load Balancer

O modo de mitigação de dessincronização protege seu aplicativo contra problemas causados pela dessincronização. HTTP 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 duradoura contra a HTTP dessincronização, mantendo a disponibilidade do seu aplicativo. Você pode alternar para o modo mais restrito para garantir que seu aplicativo receba somente solicitações que estejam em conformidade com o RFC 7230.

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

Conteúdo

- Classificações
- Modos
- Modificar o modo de mitigação de dessincronização

> **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.

Classificações

As classificações são as seguintes:

- Compatível — A solicitação está em conformidade com o RFC 7230 e não apresenta 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 e proxies da Web podem lidar com ela de forma diferente.
- 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.

Aceitável

- Um cabeçalho contém um caractere que não é de controle. ASCII
- A versão de solicitação contém um valor incorreto.
- Há um cabeçalho Content-Length com um valor de 0 para uma solicitação GET orHEAD.
- A solicitação URI contém um espaço que não está URL codificado.

Ambíguo

- A solicitação URI 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 para uma solicitação GET orHEAD.
- Há um cabeçalho Transfer-Encoding para uma GET solicitação or. HEAD

Grave

- A solicitação URI contém um caractere nulo ou uma devolução de carruagem.
- 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 RFC 7230, o balanceador de carga incrementa a métrica. `DesyncMitigationMode_NonCompliant_Request_Count` Para obter mais informações, consulte Métricas do Classic Load Balancer.

Modos

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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, em Configuração de tráfego, escolha Defensivo (recomendado), Mais estrito, ou Monitorar.
6. Escolha Salvar alterações.

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

Use o modify-load-balancer-attributescomando com o `elb.http.desyncmitigationmode` atributo definido como `monitordefensive`, 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"
        }
    ]
}
```

Configure o protocolo proxy para seu Classic Load Balancer

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 back-end, seu Classic Load Balancer encaminha solicitações para as instâncias sem modificar os cabeçalhos da 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 suporta a ativação do protocolo proxy.

Conteúdo

- Cabeçalho do protocolo de proxy
- Pré-requisitos para habilitar o protocolo de proxy
- Habilitar o protocolo de proxy usando a AWS CLI
- Desabilitar o protocolo de proxy usando a AWS CLI

Cabeçalho do protocolo de proxy

O cabeçalho do protocolo proxy ajuda a identificar o endereço IP de um cliente quando você tem um balanceador de carga usado TCP para conexões de back-end. 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 de IPv6 é o IPv6 endereço público do seu balanceador de carga. Esse IPv6 endereço corresponde ao endereço IP que é resolvido a partir do DNS nome do seu balanceador de carga, que começa com `ipv6` ou `dualstack`. Se o cliente se conectar comIPv4, o endereço do proxy no cabeçalho será o IPv4 endereço privado do balanceador de carga, que não pode ser resolvido por meio de uma pesquisa. DNS

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 proxy paraIPv4.

```
PROXY TCP4 198.51.100.22 203.0.113.7 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.

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 suportadas pelo 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 create-load-balancer-policycomando a seguir para criar uma política que habilite o protocolo 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 seguinte for-backend-server comando set-load-balancer-policies- 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 describe-load-balancerscomando a seguir para verificar se o protocolo proxy está ativado:

```
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 for-backend-server comando set-load-balancer-policies- para desativar a política do protocolo proxy omitindo-a da `--policy-names` opção, mas incluindo as outras políticas que devem permanecer 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-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 describe-load-balancerscomando a seguir para verificar se a política está desativada:

```
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": [],
            ...
        }
    ]
}
```

Colocar uma marcação em seu Classic Load Balancer

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

Você pode adicionar várias marcações a cada Classic Load Balancer. 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.

Conteúdo

- Restrições de tags
- Adicione um tag
- Remover uma marcação

Restrições de tags

As restrições básicas a seguir se aplicam a 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 valores das tags diferenciam maiúsculas de minúsculas. Os caracteres permitidos são letras, espaços e números representáveis em UTF -8, além dos seguintes caracteres especiais: + - =. _ : / @. Não use espaços no início nem no fim.
- Não use o `aws:` prefixo nos nomes ou valores de suas tags porque ele está reservado para AWS uso. Você não pode editar nem excluir nomes ou valores de tag com esse prefixo. As tags com esse prefixo não contam para as tags por limite de recurso.

Adicione um tag

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

Para adicionar uma tag usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Tags (Tags), selecione Manage tags (Gerenciar tags).
5. Na página Gerenciar tags, para cada tag, escolha Adicionar nova tag e especifique uma chave e um valor.
6. Ao terminar de adicionar tags, escolha Salvar alterações.

Para adicionar uma tag usando o 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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Tags (Tags), selecione Manage tags (Gerenciar tags).
5. Na página Gerenciar tags, escolha Remover ao lado de cada tag que você deseja remover.
6. Ao terminar de remover tags, escolha Salvar alterações.

Para remover uma tag usando o 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 sub-redes para seu Classic Load Balancer

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. 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 Recomendações para o seu VPC.

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 Classic Load Balancer.

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.

Conteúdo

- Requisitos
- Adicionar uma sub-rede
- Remover uma sub-rede

Requisitos

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 existem sub-redes separadas APIs para adicionar e remover de um balanceador de carga, você deve considerar cuidadosamente a ordem das operações ao trocar as sub-redes atuais por novas sub-redes para 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 Registre instâncias com seu Classic Load Balancer.

Para adicionar uma sub-rede ao seu load balancer usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Mapeamento de rede, escolha Editar sub-redes.
5. Na página Editar sub-redes, na seção Mapeamento de rede, selecione qual zona de disponibilidade habilitar e escolha a sub-rede a ser adicionada a essa zona de disponibilidade.
6. Ao concluir, escolha Save changes.

Para adicionar uma sub-rede ao seu balanceador de carga usando o CLI

Use o comando attach-load-balancer-to-subnets a seguir para adicionar duas sub-redes ao seu balanceador de carga:

```
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 Registre instâncias com seu Classic Load Balancer.

Para remover uma sub-rede do seu balanceador de carga usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Mapeamento de rede, escolha Editar sub-redes.
5. Na página Editar sub-redes, na seção Mapeamento de rede, selecione uma sub-rede diferente para uma zona de disponibilidade já habilitada ou desmarque uma zona de disponibilidade para removê-la e também à sua sub-rede associada.
6. Ao concluir, escolha Save changes.

Para remover uma sub-rede usando o AWS CLI

Use o seguinte comando detach-load-balancer-from-subnets para remover as sub-redes especificadas do balanceador de carga 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"
    ]
}
```

Configurar grupos de segurança para seu Classic Load Balancer

Ao usar o AWS Management Console para criar um balanceador de carga, você pode escolher um grupo de segurança existente ou criar um novo. 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.

[Não padrãoVPC] Se você usar AWS CLI ou API criar um balanceador de carga em um não padrãoVPC, mas não especificar um grupo de segurança, seu balanceador de carga será automaticamente associado ao grupo de segurança padrão do. VPC

[PadrãoVPC] Se você usar o AWS CLI ou API para criar um balanceador de carga em seu padrãoVPC, não poderá escolher um grupo de segurança existente para seu balanceador de carga. 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 somente um desses grupos de segurança por AWS conta, com um nome no formato default_elb_*id* (por exemplo,`default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE`). Os balanceadores de carga subsequentes que você cria no padrão VPC também usam esse grupo de segurança. 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.

Conteúdo

- Regras recomendadas para os grupos de segurança do balanceador de carga
- Atribua grupos de segurança usando o console
- Atribua grupos de segurança usando o AWS CLI

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.

Balanceador de carga voltado para a Internet

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

Origem	Protocolo	Port Range (Intervalo de portas)	Comentário
0.0.0.0/0	TCP	*listener*	Permite todo o tráfego de entrada na porta do listener do load balancer

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

Destination (Destino)	Protocolo	Port Range (Intervalo de portas)	Comentário
instance security group	TCP	*instance listener*	Permitir tráfego de saída para instâncias na porta do ouvinte da instância
instance security group	TCP	*health check*	Permitir tráfego de saída para instâncias na porta de verificação de integridade

Balanceadores de carga internos

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

Origem	Protocolo	Port Range (Intervalo de portas)	Comentário
VPC CIDR	TCP	*listener*	Permitir tráfego de entrada da porta do VPC CIDR ouvinte do balancead or de carga

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

Destination (Destino)	Protocolo	Port Range (Intervalo de portas)	Comentário
instance security group	TCP	*instance listener*	Permitir tráfego de saída para instâncias na porta do ouvinte da instância
instance security group	TCP	*health check*	Permitir tráfego de saída para instâncias na porta de verificação de integridade

Atribua grupos de segurança usando o console

Use o procedimento a seguir para alterar os grupos de segurança associados ao seu balanceador de carga.

Para atualizar um grupo de segurança atribuído ao seu balanceador de carga usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Segurança, escolha Editar.

5. Na página Editar grupos de segurança, em Grupos de segurança, adicione ou remova grupos de segurança conforme necessário.

   Você pode adicionar até cinco grupos de segurança.

6. Ao concluir, escolha Save changes.

Atribua grupos de segurança usando o AWS CLI

Use o comando apply-security-groups-to-load-balancer a seguir para associar um grupo de segurança a um balanceador de carga. 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"
  ]
}
```

Configure a rede ACLs para seu Classic Load Balancer

A lista de controle de acesso à rede padrão (ACL) para a VPC permite todo o tráfego de entrada e saída. Se você criar uma rede personalizadaACLs, deverá adicionar regras que permitam que o balanceador de carga e as instâncias se comuniquem.

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

Balanceador de carga voltado para a Internet

A seguir estão as regras de entrada recomendadas para um balanceador de carga voltado para a Internet.

Origem	Protocolo	Port Range (Intervalo de portas)	Comentário
0.0.0.0/0	TCP	*listener*	Permite todo o tráfego de entrada na porta do listener do load balancer
VPC CIDR	TCP	1024-65535	Permitir tráfego de entrada a partir das portas VPC CIDR efêmeras

A seguir estão as regras de saída recomendadas para um balanceador de carga voltado para a Internet.

Destination (Destino)	Protocolo	Port Range (Intervalo de portas)	Comentário
VPC CIDR	TCP	*instance listener*	Permitir todo o tráfego de saída na porta do listener da instância
VPC CIDR	TCP	*health check*	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

Balanceador de carga interno

A seguir estão as regras de entrada recomendadas para um balanceador de carga interno.

Origem	Protocolo	Port Range (Intervalo de portas)	Comentário
VPC CIDR	TCP	*listener*	Permitir tráfego de entrada da porta do VPC CIDR ouvinte do balancead or de carga
VPC CIDR	TCP	1024-65535	Permitir tráfego de entrada a partir das portas VPC CIDR efêmeras

A seguir estão as regras de saída recomendadas para um balanceador de carga interno.

Destination (Destino)	Protocolo	Port Range (Intervalo de portas)	Comentário
VPC CIDR	TCP	*instance listener*	Permitir tráfego de saída para a porta do ouvinte VPC CIDR na instância
VPC CIDR	TCP	*health check*	Permitir tráfego de saída para a VPC CIDR porta de verificação de integridade
VPC CIDR	TCP	1024-65535	Permitir tráfego de saída para as portas VPC CIDR efêmeras

Configure um nome de domínio personalizado para seu Classic Load Balancer

Cada Classic Load Balancer recebe um nome padrão de Sistema de Nomes de Domínio (DNS). Esse DNS nome inclui o nome da AWS região na qual o balanceador de carga é criado. Por exemplo, se você criar um balanceador de carga chamado `my-loadbalancer` na região Oeste dos EUA (Oregon), seu balanceador de carga receberá um DNS nome como. `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com` Para acessar o site em suas

instâncias, cole esse DNS nome no campo de endereço de um navegador da web. No entanto, esse DNS nome não é fácil para seus clientes lembrarem e usarem.

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

Conteúdo

- Como associar seu nome de domínio personalizado com o nome do seu balanceador de carga
- Usando o DNS failover do Route 53 para seu balanceador de carga
- Dissociar seu nome de domínio personalizado do seu balanceador de carga

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 Internet Corporation for Assigned Names and Numbers (ICANN) gerencia nomes de domínio na Internet. Você registra um nome de domínio usando um registrador de nomes de domínio, uma organização ICANN credenciada que gerencia o registro de nomes de domínio. O site do registrador fornecerá instruções detalhadas e informações sobre a definição de preço para registrar o nome de domínio. Para obter mais informações, consulte os seguintes recursos do :

- 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 seu DNS serviço, como seu registrador de domínio, para criar um CNAME registro para encaminhar consultas para seu balanceador de carga. Para obter mais informações, consulte a documentação do seu DNS serviço.

Como alternativa, você pode usar o Route 53 como seu DNS serviço. 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 DNS consultas para conjuntos de registros de alias, e você pode usar conjuntos de registros de alias para encaminhar DNS consultas ao seu balanceador de carga para o ápice da zona do seu domínio (por exemplo,). `example.com` Para obter informações sobre a transferência de DNS serviços de domínios existentes para o Route 53, consulte Como configurar o Route 53 como seu DNS serviço no Amazon Route 53 Developer Guide.

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.

Usando o DNS failover do Route 53 para seu balanceador de carga

Se você usa o Route 53 para rotear DNS consultas para seu balanceador de carga, você também pode configurar o DNS failover para seu balanceador de carga usando o Route 53. Em uma configuração de failover, o Route 53 verifica a integridade das EC2 instâncias registradas do balanceador de carga para determinar se elas estão disponíveis. Se não houver EC2 instâncias íntegras registradas no balanceador de carga, ou se o próprio balanceador de carga não estiver íntegro, o Route 53 encaminhará o tráfego para outro recurso disponível, como um balanceador de carga saudável 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 DNS failover, poderá especificar seus balanceadores de carga primários e secundários (de backup). O Route 53 direcionará o tráfego para o balanceador de carga primário, se estiver disponível, ou para o balanceador de carga secundário, em caso contrário.

Como usar a opção Avaliar a integridade do destino

- Quando a opção Avaliar a integridade do destino está definida como `Yes` em um registro de alias para um Classic Load Balancer, o Route 53 avalia a integridade do recurso especificado pelo valor do `alias target`. Para um Classic Load Balancer, o Route 53 usa as verificações de integridade da instância associadas ao balanceador de carga.
- Quando pelo menos uma das instâncias registradas em um Classic Load Balancer estiver íntegra, o Route 53 marcará o registro de alias como íntegro. Em seguida, o Route 53 retornará os registros de acordo com a sua política de roteamento. Se a política de roteamento por failover for usada, o Route 53 retornará o registro primário.

- Quando todas as instâncias registradas de um Classic Load Balancer não estiverem íntegras, o Route 53 marcará o registro do alias como não íntegro. Em seguida, o Route 53 retornará os registros de acordo com a sua política de roteamento. Se a política de roteamento por failover for usada, o Route 53 retornará o registro secundário.

Para obter mais informações, consulte Como configurar o DNS failover 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.

Listeners para seu Classic Load Balancer

Antes de começar a usar o Elastic Load Balancing, é preciso configurar um ou mais listeners para seu Classic Load Balancer. 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(seguroHTTP)
- TCP
- SSL(seguroTCP)

O HTTPS protocolo usa o SSL protocolo para estabelecer conexões seguras na HTTP camada. Você também pode usar o SSL protocolo para estabelecer conexões seguras na TCP camada.

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

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

Os load balancers podem ouvir nas seguintes portas: 1-65535

Conteúdo

- Protocolos
- HTTPS/SSLouvintes
- Configurações do listener para balanceadores de carga clássicos
- HTTPcabeçalhos e balanceadores de carga clássicos

Protocolos

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. A Open System Interconnection (OSI) define uma estrutura de modelo para implementar um formato padrão de comunicação, chamado protocolo, nessas camadas. Para obter mais informações, consulte o OSImodelo na Wikipedia.

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

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

TCP/SSLprotocolo

Quando você usa TCP (camada 4) para conexões front-end e back-end, seu balanceador de carga encaminha a solicitação para as instâncias de back-end sem modificar os cabeçalhos. Depois que seu balanceador de carga recebe a solicitação, ele tenta abrir uma TCP conexão com a instância de back-end na porta especificada na configuração do ouvinte.

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 Configure o protocolo proxy para seu Classic Load Balancer.

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

HTTP/HTTPSprotocolo

Quando você usa HTTP (camada 7) para conexões front-end e back-end, seu balanceador de carga analisa os cabeçalhos na solicitação antes de enviar a solicitação para as instâncias de back-end.

Para cada instância registrada e íntegra por trás de umHTTP/HTTPSload balancer, o Elastic Load Balancing abre e mantém uma ou TCP mais conexões. Essas conexões garantem que sempre haja uma conexão estabelecida pronta para receber HTTP HTTPS /requests.

As HTTP solicitações e HTTP respostas usam campos de cabeçalho para enviar informações sobre HTTP mensagens. 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.

Ao usarHTTP/HTTPS, você pode ativar sessões fixas no seu balanceador de carga. 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 Classic Load Balancer.

Nem todas as HTTP extensões são suportadas no balanceador de carga. Talvez seja necessário usar um TCP ouvinte se o balanceador de carga não conseguir encerrar a solicitação devido a métodos inesperados, códigos de resposta ou outras implementações 1.0/1.1 não HTTP padrão.

HTTPS/SSLouvintes

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

SSLcertificados de servidor

Se você usa HTTPS ou SSL para suas conexões front-end, deve implantar um certificado X.509 (certificado de SSL servidor) em seu balanceador de carga. O balanceador de carga descriptografa as solicitações dos clientes antes de enviá-las para as instâncias de back-end (conhecido como encerramento). SSL Para obter mais informações, consulte SSL/TLScertificados para balanceadores de carga clássicos.

Se você não quiser que o balanceador de carga processe o SSL encerramento (conhecido como SSLdescarregamento), você pode usá-lo TCP para as conexões de front-end e back-end e implantar certificados nas instâncias registradas que processam as solicitações.

SSLnegociação

O Elastic Load Balancing fornece configurações de SSL negociação predefinidas que são usadas para SSL negociação quando uma conexão é estabelecida entre um cliente e seu balanceador de

carga. As configurações SSL de negociação oferecem compatibilidade com uma ampla variedade de clientes e usam algoritmos criptográficos de alta resistência 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 PCISOX, e assim por diante) podem exigir um conjunto específico de protocolos e cifras dos clientes para garantir que os padrões de segurança sejam atendidos. Nesses casos, você pode criar uma configuração de SSL negociação personalizada, com base em seus requisitos específicos. Sua cifras e seus protocolos devem entrar em vigor dentro de 30 segundos. Para obter mais informações, consulte SSLconfigurações de negociação para Classic Load Balancers.

Autenticação do servidor backend

Se você usa HTTPS ou SSL para suas conexões de back-end, você pode habilitar a autenticação de 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.

Configurações do listener para balanceadores de carga clássicos

A tabela a seguir descreve as possíveis configurações HTTP e HTTPS ouvintes de um Classic Load Balancer.

Caso de uso	Protocolo de front-end	Opções de front-end	Protocolo de backend	Opções de backend	Observações
HTTPBalanceador de carga básico	HTTP	N/D	HTTP	N/D	• Oferece suporte para X-Forwarded headers (Cabeçalhos X-Forwarded)
Site ou aplicativ	HTTPS	SSLnegociação	HTTP	N/D	• Oferece suporte

Caso de uso	Protocolo de front-end	Opções de front-end	Protocolo de backend	Opções de backend	Observações
o seguro usando o Elastic Load Balancing para descarregar a decodificação SSL					para X-Forwarded headers (Cabeçalhos X-Forwarded) • Requer um SSLcertificado implantado no balanceador de carga
Site ou aplicativo seguro usando end-to-end criptografia	HTTPS	SSLnegociação	HTTPS	Autenticação de back-end	• Oferece suporte para X-Forwarded headers (Cabeçalhos X-Forwarded) • Requer SSLcertificados implantados no balanceador de carga e nas instâncias registradas

A tabela a seguir descreve as possíveis configurações TCP e SSL ouvintes de um Classic Load Balancer.

Caso de uso	Protocolo de front-end	Opções de front-end	Protocolo de backend	Opções de backend	Observações
TCPBalanceador de carga básico	TCP	N/D	TCP	N/D	• Compatível com cabeçalho de protocolo de proxy
Site ou aplicativo seguro usando o Elastic Load Balancing para descarregar a decodificação SSL	SSL	SSLnegociação	TCP	N/D	• Requer um SSLcertificado implantado no balanceador de carga • Compatível com cabeçalho de protocolo de proxy
Proteja o site ou aplicativo usando end-to-end criptografia com o Elastic Load Balancing	SSL	SSLnegociação	SSL	Autenticação de back-end	• Requer SSLcertificados implantados no balanceador de carga e nas instâncias registradas

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

HTTPcabeçalhos e balanceadores de carga clássicos

HTTPsolicitações e HTTP respostas usam campos de cabeçalho para enviar informações sobre as HTTP mensagens. 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 HTTP cabeçalho é definido em RFC 2616, Cabeçalhos de mensagens. Também há HTTP cabeçalhos não padrão disponíveis (e adicionados automaticamente) que são amplamente usados pelos aplicativos. Alguns dos HTTP cabeçalhos não padrão têm um `X-Forwarded` prefixo. Os balanceadores de carga clássicos são compatíveis com os seguintes cabeçalhos `X-Forwarded`.

Para obter mais informações sobre HTTP conexões, consulte Roteamento de solicitações no Guia do Usuário do Elastic Load Balancing.

Pré-requisitos

- 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.
- Configure o servidor web para registrar em log os endereços IP do cliente.

Cabeçalhos X-Forwarded

- X-Forwarded-For
- X-Forwarded-Proto
- X-Forwarded-Port

X-Forwarded-For

O cabeçalho da `X-Forwarded-For` solicitação é adicionado automaticamente e ajuda a identificar o endereço IP de um cliente quando você usa um balanceador de HTTPS carga HTTP or. 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 `X-Forwarded-For` solicitação para um cliente com um IPv6 endereço de`2001:DB8::21f:5bff:febf:ce22:8a2e`.

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

X-Forwarded-Proto

O cabeçalho da `X-Forwarded-Proto` solicitação ajuda você a identificar o protocolo (HTTPouHTTPS) que um cliente usou para se conectar ao seu balanceador de carga. 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.

Seu aplicativo ou site pode usar o protocolo armazenado no cabeçalho da `X-Forwarded-Proto` solicitação para renderizar uma resposta que redireciona para a apropriada. URL

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

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

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

```
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.

HTTPSouvintes para seu Classic Load Balancer

Você pode criar um balanceador de carga que usa o TLS protocoloSSL/para conexões criptografadas (também conhecido como SSLdescarregamento). Esse recurso permite a criptografia de tráfego entre seu balanceador de carga e os clientes que iniciam HTTPS as sessões e para conexões entre seu balanceador de carga e suas instâncias. EC2

O Elastic Load Balancing usa configurações de negociação Secure Sockets Layer (SSL), conhecidas como políticas de segurança, para negociar conexões entre os clientes e o balanceador de carga. Ao usarHTTPS/SSLpara suas conexões front-end, você pode usar uma política de segurança predefinida ou uma política de segurança personalizada. Você deve implantar um SSL certificado no seu balanceador de carga. 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.

Os balanceadores de carga clássicos não oferecem suporte à indicação de nome de servidor (SNI). Você pode usar uma das duas alternativas:

- Implante um certificado no balanceador de carga e adicione um nome alternativo de assunto (SAN) para cada site adicional. SANspermitem que você proteja vários nomes de host usando um único certificado. Consulte seu provedor de certificados para obter mais informações sobre o número de SANs certificados suportados por certificado e como adicionar e removerSANs.
- Use TCP ouvintes na porta 443 para as conexões front-end e back-end. O balanceador de carga transmite a solicitação no estado em que se encontra, para que você possa lidar com o HTTPS encerramento da EC2 instância.

Os Classic Load Balancers não oferecem suporte à TLS autenticação mútua (mTLS). Para meu TLS apoio, crie um TCP ouvinte. O balanceador de carga transmite a solicitação no estado em que se encontra, para que você possa implementar m TLS na EC2 instância.

Conteúdo

- SSL/TLScertificados para balanceadores de carga clássicos
- SSLconfigurações de negociação para Classic Load Balancers
- Crie um Classic Load Balancer com um ouvinte HTTPS
- Configure um HTTPS ouvinte para seu Classic Load Balancer

- Substitua o SSL certificado do seu Classic Load Balancer
- Atualize a configuração SSL de negociação do seu Classic Load Balancer

SSL/TLScertificados para balanceadores de carga clássicos

Se você usa HTTPS (SSLouTLS) para seu ouvinte de front-end, você deve implantar um TLS certificadoSSL/no seu balanceador de carga. O load balancer usa o certificado para encerrar a conexão e, em seguida, descriptografa solicitações dos clientes antes de enviá-las às instâncias.

Os TLS protocolos SSL e usam um certificado X.509 (SSL/certificado de TLS servidor) para autenticar o cliente e o aplicativo de 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 AWS Certificate Manager ou uma ferramenta que ofereça suporte aos TLS protocolos SSL e, como OpenSSL. Você especificará esse certificado ao criar ou atualizar um HTTPS ouvinte para seu balanceador de carga. Quando você cria um certificado para uso com seu load balancer, é necessário especificar um nome de domínio.

Quando você cria um certificado para uso com seu load balancer, é necessário especificar um nome de domínio. O nome de domínio no certificado deve corresponder ao registro de nome de domínio personalizado. Se não corresponderem, o tráfego não será criptografado, pois a TLS conexão não pode ser verificada.

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

Crie ou importe um TLS certificadoSSL/usando AWS Certificate Manager

Recomendamos que você use AWS Certificate Manager (ACM) para criar ou importar certificados para seu balanceador de carga. ACMse integra ao Elastic Load Balancing para que você possa implantar o certificado em seu load balancer. 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 implante o certificado em seu balanceador de carga usando o AWS Management Console, você deve permitir o acesso à ACM `ListCertificates` API ação. Para obter mais informações, consulte Listar certificados no Manual do usuário do AWS Certificate Manager .

> **Important**
>
> Você não pode instalar certificados com chaves de 4096 bits ou RSA chaves EC em seu balanceador de carga por meio da integração com o. ACM Você deve fazer upload de certificados com chaves de 4096 bits ou RSA chaves EC para IAM usá-los com seu balanceador de carga.

Importe um TLS certificadoSSL/usando IAM

Se você não estiver usandoACM, você pode usar TLS ferramentasSSL/, como OpenSSL, para criar uma solicitação de assinatura de certificado (CSR), obter a CSR assinatura de uma CA para produzir um certificado e fazer upload do certificado paraIAM. Para obter mais informações, consulte Como trabalhar com certificados de servidor no Guia IAM do usuário.

SSLconfigurações de negociação para Classic Load Balancers

O Elastic Load Balancing usa uma configuração de negociação Secure Socket Layer (SSL), conhecida como política de segurança, para negociar SSL conexões entre um cliente e o balanceador de carga. Uma política de segurança é uma combinação de SSL protocolos, SSL cifras e a opção Server Order Preference. Para obter mais informações sobre como configurar uma SSL conexão para seu balanceador de carga, consulte. Listeners para seu Classic Load Balancer

Conteúdo

- Políticas de segurança
- SSLprotocolos
- Preferência ditada pelo servidor
- SSLcifras
- Políticas de SSL segurança predefinidas para balanceadores de carga clássicos

Políticas de segurança

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

Observe que um certificado fornecido por AWS Certificate Manager (ACM) contém uma chave RSA pública. Portanto, você deve incluir um conjunto de cifras que use RSA em sua política de segurança se você usar um certificado fornecido porACM; caso contrário, a TLS conexão 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 SSL segurança predefinidas.

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 eSOC) 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 Atualize a configuração SSL de negociação do seu Classic Load Balancer.

SSLprotocolos

O SSLprotocolo estabelece uma conexão segura entre um cliente e um servidor e garante que todos os dados transmitidos entre o cliente e seu balanceador de carga sejam privados.

O Secure Sockets Layer (SSL) e o Transport Layer Security (TLS) são protocolos criptográficos usados para criptografar dados confidenciais em redes inseguras, como a Internet. O TLS protocolo é uma versão mais recente do SSL protocolo. Na documentação do Elastic Load Balancing, nos referimos a ambos TLS os SSL protocolos SSL como protocolo.

Protocolo recomendado

Recomendamos TLS 1.2, que é usado na política de segurança predefinida ELBSecurityPolicy - TLS -1-2-2017-01. Você também pode usar TLS 1.2 em suas políticas de segurança personalizadas. A política de segurança padrão oferece suporte às versões TLS 1.2 e anteriores doTLS, portanto, é menos segura do que ELBSecurityPolicy - TLS -1-2-2017-01.

Protocolo descontinuado

Se você habilitou anteriormente o protocolo SSL 2.0 em uma política personalizada, recomendamos que você atualize sua política de segurança para uma das políticas de segurança predefinidas.

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 da SSL conexão, o cliente e o balanceador de carga apresentam uma lista de cifras e protocolos que cada um suporta, em ordem de preferência. Por padrão, a primeira cifra na lista do cliente que corresponde a qualquer uma das cifras do balanceador de carga 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 balanceador de carga 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.

SSLcifras

Uma SSLcifra é um algoritmo de criptografia que usa chaves de criptografia para criar uma mensagem codificada. SSLos protocolos usam várias SSL cifras para criptografar dados pela Internet.

Observe que um certificado fornecido por AWS Certificate Manager (ACM) contém uma chave RSA pública. Portanto, você deve incluir um conjunto de cifras que use RSA em sua política de segurança se você usar um certificado fornecido porACM; caso contrário, a TLS conexão 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 predefinidas. SSL 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.

Cifras

- 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-3 DES - - 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 incluídas na política de segurança padrão, ELBSecurityPolicy -2016-08.

Políticas de SSL segurança predefinidas para balanceadores de carga clássicos

Você pode escolher uma das políticas de segurança predefinidas para seus SSL ouvintesHTTPS//. Você pode usar uma das `ELBSecurityPolicy-TLS` políticas para atender aos padrões de conformidade e segurança que exigem a desativação de determinadas versões do TLS protocolo. Como alternativa, você pode criar uma política de segurança personalizada. Para obter mais informações, consulte Atualizar a SSL configuração da negociação.

As cifras DSA baseadas em RSA - e são específicas do algoritmo de assinatura usado para criar SSL o certificado. Certifique-se de criar um SSL certificado usando o algoritmo de assinatura baseado nas cifras habilitadas para 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 Classic Load Balancers, incluindo seus SSL protocolos habilitados, SSL cifras e a 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
SSLProtocolos						
Protocolo-TLSv1	✓			✓	✓	✓
Protocolo-1TLSv1.	✓	✓		✓	✓	✓
Protocolo-2TLSv1.	✓	✓	✓	✓	✓	✓
SSLOpções						
Preferência ditada pelo servidor	✓	✓	✓	✓	✓	✓
SSLCifras						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-	✓	✓	✓	✓	✓	✓

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

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

Política de segurança	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓	✓
DHE-DSS-AES128-SHA					✓	✓
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 describe-load-balancer-policiescomando.

- 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-O penSSLDefault NegotiationPolicy ou ELBSample -O penSSLDefault CipherPolicy

Crie um Classic Load Balancer com um ouvinte HTTPS

Um balanceador de carga recebe solicitações de clientes e as distribui pelas EC2 instâncias registradas no balanceador de carga.

Você pode criar um balanceador de carga que escute nas portas HTTP (80) e HTTPS (443). Se você especificar que o HTTPS ouvinte envie solicitações para as instâncias na porta 80, o balanceador de carga encerrará as solicitações e a comunicação do balanceador de carga com as instâncias não será criptografada. Se o HTTPS ouvinte enviar solicitações para as instâncias na porta 443, a comunicação do balanceador de carga com 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 como adicionar um HTTPS ouvinte a um balanceador de carga existente, consulte. Configure um HTTPS ouvinte para seu Classic Load Balancer

Conteúdos

- Pré-requisitos
- Crie um HTTPS balanceador de carga usando o console
- Crie um HTTPS balanceador de carga usando o AWS CLI

Pré-requisitos

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

- Siga as etapas em Recomendações para o seu VPC.
- Execute as EC2 instâncias que você planeja registrar com seu balanceador de carga. Os security groups dessas instâncias devem permitir tráfego do load balancer.
- As EC2 instâncias devem responder à meta da verificação de saúde com um código de HTTP status 200. Para obter mais informações, consulte Verificações de saúde das instâncias do seu Classic Load Balancer.
- Se você planeja ativar a opção keep-alive em suas EC2 instâncias, recomendamos que você defina as configurações de keep-alive pelo menos para as configurações de tempo limite

de inatividade do seu balanceador de carga. 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 Classic Load Balancer.

- Se você criar um ouvinte seguro, deverá implantar um certificado de SSL servidor em seu balanceador de carga. 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 SSL certificado, poderá criar um. Para obter mais informações, consulte SSL/TLScertificados para balanceadores de carga clássicos.

Crie um HTTPS balanceador de carga usando o console

Neste exemplo, você configura dois listeners para o load balancer. O primeiro ouvinte aceita HTTP solicitações na porta 80 e as envia para as instâncias na porta 80 usandoHTTP. O segundo ouvinte aceita HTTPS solicitações na porta 443 e as envia para as instâncias usando a porta 80 (ou usando HTTP HTTPS a porta 443 se você quiser configurar a autenticação da instância de back-end).

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 Classic Load Balancer.

Para criar seu Classic Load Balancer seguro usando o console

1. Abra o EC2 console da Amazon 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 que você selecionou para suas EC2 instâncias.
3. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
4. Selecione Criar load balancer.
5. Expanda a seção Classic Load Balancer e escolha Criar.
6. Configuração básica

    a. Em Nome do balanceador de carga, digite um nome para o balanceador de carga.

O nome de seu Classic Load Balancer deve ser exclusivo dentro de seu conjunto de Classic Load Balancers 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. Para Esquema, selecione Voltado para a Internet.

7. Mapeamento de rede

   a. Para VPC, selecione o mesmo VPC que você selecionou para suas instâncias.

   b. Para Mapeamentos, primeiro selecione uma zona de disponibilidade e escolha uma sub-rede pública entre as sub-redes disponíveis. Você pode selecionar somente uma sub-rede por zona de disponibilidade. Para melhorar a disponibilidade do seu balanceador de carga, selecione mais de uma zona de disponibilidade e sub-rede.

8. Grupos de segurança

   • Em Grupos de segurança, selecione um grupo de segurança existente configurado para permitir o HTTP tráfego necessário na porta 80 e o HTTPS tráfego na porta 443.

     Se não existir um, você poderá criar um novo grupo de segurança com as regras necessárias.

9. Receptores e roteamento

   a. Deixe o receptor padrão com as configurações padrão e selecione Adicionar receptor.

   b. Para Receptor no novo receptor, selecione HTTPS como o protocolo, e a porta será atualizada para 443. Por padrão, a Instância usa o protocolo HTTP na porta 80.

   c. Se a autenticação de back-end for necessária, altere o protocolo da Instância para HTTPS. Essa ação também atualizará a porta da Instância para 443.

10. Configurações seguras do receptor

    Ao usar HTTPS ou SSL para seu ouvinte de front-end, você deve implantar um SSL certificado em seu balanceador de carga. 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 SSL negociação predefinidas, ou você pode criar sua própria política de segurança personalizada. Se você configurouHTTPS/SSLna conexão de back-end, você pode habilitar a autenticação de suas instâncias.

a. Para a política de segurança, recomendamos que você sempre use a política de segurança predefinida mais recente ou crie uma política personalizada. Consulte Atualizar a configuração SSL da negociação.

b. Para DefaultSSL/TLScertificate, as seguintes opções estão disponíveis:

- Se você criou ou importou um certificado usando AWS Certificate Manager, selecione De eACM, em seguida, selecione o certificado em Selecionar um certificado.
- Se você importou um certificado usandoIAM, selecione De eIAM, em seguida, selecione seu certificado em Selecionar um certificado.
- Se você tiver um certificado para importar, mas não ACM estiver disponível na sua região, selecione Importar e, em seguida, selecione Para IAM. Digite o nome do certificado no campo Nome do certificado. Em Chave privada do certificado, copie e cole o conteúdo do arquivo de chave privada (PEMcodificado em -). No corpo do certificado, copie e cole o conteúdo do arquivo de certificado de chave pública (PEMcodificado em -). Na Cadeia de certificados, copie e cole o conteúdo do arquivo da cadeia de certificados (PEMcodificado), a menos que você esteja usando um certificado autoassinado e não seja importante que os navegadores aceitem implicitamente o certificado.

c. (Opcional) Se você configurou o HTTPS ouvinte para se comunicar com as instâncias usando uma conexão criptografada, você pode, opcionalmente, configurar a autenticação das instâncias no certificado de autenticação de back-end.

> **Note**
>
> Se você não encontrar a seção Certificado de autenticação de back-end, volte para Receptores e roteamento e selecione HTTPS como o protocolo para Instância.

i. Em Nome de certificado, digite o nome do certificado de chave pública.

ii. Para o Organismo do Certificado (PEMcodificado), copie e cole o conteúdo do certificado. O load balancer se comunica com uma instância somente se sua chave pública corresponder a essa chave.

iii. Para adicionar outro certificado, escolha Adicionar novo certificado back-end. O limite é de cinco.

11. Verificações de integridade

a. Na seção Destino do ping, selecione um Protocolo de ping e Porta de ping. Suas EC2 instâncias devem aceitar tráfego na porta de ping especificada.

b. Para Porta de ping, certifique-se de que a porta seja `80`.

c. Em Caminho de ping, substitua o valor padrão por uma barra simples (`/`). 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`.

d. Para Configurações avançadas de verificação de integridade, use os valores padrão.

12. Instâncias

a. Selecione Adicionar instâncias para abrir a tela de seleção de instâncias.

b. Em Instâncias disponíveis, você pode selecionar entre as instâncias atuais que estão disponíveis para o balanceador de carga, com base nas configurações de rede selecionadas anteriormente.

c. Quando estiver satisfeito com suas seleções, selecione Confirmar para adicionar ao balanceador de carga as instâncias a serem registradas.

13. Atributos.

- Em Habilitar balanceamento de carga entre zonas, Habilitar drenagem da conexão e Tempo limite (intervalo de drenagem), mantenha os valores padrão.

14. Tags do balanceador de carga (opcional)

a. O campo Chave é obrigatório.

b. O campo Valor é opcional.

c. Para adicionar outra tag, selecione Adicionar nova tag, insira seus valores no campo Chave e, opcionalmente, no campo Valor.

d. Para remover uma tag existente, selecione Remover ao lado da tag que você deseja remover.

15. Resumo e criação

a. Caso precies alterar alguma configuração, selecione Editar ao lado da configuração que precisa ser alterada.

b. Quando estiver satisfeito com as configurações mostradas no resumo, selecione Criar balanceador de carga para começar a criação do seu balanceador de carga.

c. Na página de criação final, selecione Exibir balanceador de carga para visualizar seu balanceador de carga no console da AmazonEC2.

16. Verificar

a. Selecione o novo load balancer.

b. Na guia Instâncias de destino, marque a coluna Status de integridade. Depois que pelo menos uma de suas EC2 instâncias estiver em serviço, você poderá testar seu balanceador de carga.

c. Na seção Detalhes, copie o DNSnome dos balanceadores de carga, que seria semelhante a. `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`

d. Cole o DNSnome do balanceador de carga no campo de endereço de um navegador público conectado à Internet. Se o balanceador de carga estiver funcionando corretamente, você verá a página padrão do seu servidor.

17. Excluir (opcional)

a. Se você tiver um CNAME registro para seu domínio que aponte para seu balanceador de carga, aponte-o para um novo local e aguarde a DNS alteração entrar em vigor antes de excluir seu balanceador de carga.

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

c. Selecione o load balancer.

d. Escolha Ações, Excluir balanceador de carga.

e. Quando a confirmação for solicitada, digite `confirm` e escolha Delete.

f. Depois de excluir um balanceador de carga, as EC2 instâncias que foram registradas com o balanceador de carga continuam em execução. Você será cobrado por cada hora parcial ou completa em que eles continuarem sendo executados. Quando não precisar mais de uma EC2 instância, você pode interrompê-la ou encerrá-la para evitar cobranças adicionais.

Crie um HTTPS balanceador de carga usando o AWS CLI

Use as instruções a seguir para criar um balanceador de SSL cargaHTTPS/usando o. AWS CLI

Tarefas

- Etapa 1: Configure os listeners
- Etapa 2: Configurar a política SSL de segurança

- Etapa 3: Configure a autenticação de instância backend (opcional)
- Etapa 4: Configure as verificações de integridade (opcional)
- Etapa 5: registrar EC2 instâncias
- Etapa 6: Verifique as instâncias
- Etapa 7: Excluir o balanceador de carga (opcional)

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 Classic Load Balancer.

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 ouvinte aceita HTTP solicitações na porta 80 e envia as solicitações para as instâncias na porta 80 usandoHTTP. O segundo ouvinte aceita HTTPS solicitações na porta 443 e envia solicitações para instâncias usando a porta HTTP 80.

Como o segundo ouvinte usa HTTPS para a conexão front-end, você deve implantar um certificado de servidor no seu SSL balanceador de carga. 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 Amazon Resource Name (ARN) do SSL certificado. 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 create-load-balancercomando a seguir para configurar o balanceador de carga com os dois ouvintes:

```
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,SSLCertificateI
 --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 describe-load-balancerscomando a seguir para ver os detalhes do seu balanceador de carga:

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

Etapa 2: Configurar a política SSL de segurança

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`. Para obter mais informações, consulte SSLconfigurações de negociação para Classic Load Balancers.

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

Use o seguinte comando describe-load-balancers:

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

O seguinte é um exemplo de resposta. 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 preferir, você pode configurar a política de SSL segurança do seu balanceador de carga em vez de usar a política de segurança padrão.

(Opcional) para usar uma política de SSL segurança predefinida

1. Use o describe-load-balancer-policiescomando a seguir 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 SSL segurança predefinidas.

2. Use o create-load-balancer-policycomando a seguir para criar uma política de SSL negociação usando uma das políticas de segurança predefinidas que você descreveu 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 describe-load-balancer-policiescomando a seguir 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 seguinte comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do balanceador de carga:

```
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 describe-load-balancerscomando a seguir para verificar se a política está 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. As RSA cifras DSA e são específicas do algoritmo de assinatura e são usadas para criar o SSL certificado. Se você já tem seu SSL certificado, certifique-se de habilitar 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 SSL de segurança personalizada

1. Use o create-load-balancer-policycomando para criar uma política de SSL negociação 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 describe-load-balancer-policiescomando a seguir 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 seguinte comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do balanceador de carga:

```
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 describe-load-balancerscomando a seguir para verificar se a política está 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 configurarHTTPS/SSLna conexão de back-end, você pode, opcionalmente, configurar a autenticação de 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 da instância de back-end com a porta da instância para o HTTPS protocolo.

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 create-load-balancer-policycomando a seguir 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-----`"). O AWS CLI não aceita caracteres de espaço em branco em`--policy-attributes`.

3. Use o create-load-balancer-policycomando a seguir para criar uma política de autenticação de instância de 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 seguinte for-backend-server comando set-load-balancer-policies- para definir `my-authentication-policy` a porta da instância paraHTTPS. 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 describe-load-balancer-policiescomando a seguir para listar todas as políticas do seu balanceador de carga:

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

6. (Opcional) Use o describe-load-balancer-policiescomando a seguir para ver 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 EC2 instância registrada com base nas verificações de saúde 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 Verificações de saúde das instâncias do seu Classic Load Balancer.

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 seguinte 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: registrar EC2 instâncias

Depois de criar seu balanceador de carga, você deve registrar suas EC2 instâncias com o balanceador de carga. Você pode selecionar EC2 instâncias de uma única zona de disponibilidade ou de várias zonas de disponibilidade na mesma região do balanceador de carga. Para obter mais informações, consulte Instâncias registradas para seu Classic Load Balancer.

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 EC2 instâncias recém-registradas, use o seguinte describe-instance-healthcomando:

```
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 Classic Load Balancer: registro de instância.

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 DNS nome do balanceador de carga e cole-o no campo de endereço de um navegador conectado à Internet. Se o balanceador de carga estiver funcionando, você verá a página padrão do seu HTTP servidor.

Etapa 7: Excluir o balanceador de carga (opcional)

A exclusão de um balanceador de carga cancela automaticamente o registro das instâncias associadas. EC2 Assim que o load balancer for excluído, as cobranças desse load balancer será interrompida. No entanto, as EC2 instâncias continuam em execução e você continua incorrendo em cobranças.

Para excluir seu balanceador de carga, use o seguinte delete-load-balancercomando:

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

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

Configure um HTTPS ouvinte para seu Classic Load Balancer

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 Classic Load Balancer.

Se você tiver um balanceador de carga com um ouvinte que aceita HTTP solicitações na porta 80, você pode adicionar um ouvinte que aceite HTTPS solicitações na porta 443. Se você especificar que o HTTPS ouvinte envie solicitações para as instâncias na porta 80, o balanceador de carga encerrará as SSL solicitações e a comunicação do balanceador de carga com as instâncias não será criptografada. Se o HTTPS ouvinte enviar solicitações para as instâncias na porta 443, a comunicação do balanceador de carga com 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 como criar um novo HTTPS ouvinte, consulteCrie um Classic Load Balancer com um ouvinte HTTPS.

Conteúdos

- Pré-requisitos
- Adicionar um HTTPS ouvinte usando o console
- Adicione um HTTPS ouvinte usando o AWS CLI

Pré-requisitos

Para habilitar o HTTPS suporte para um HTTPS ouvinte, você deve implantar um certificado de SSL servidor em seu balanceador de carga. 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 SSL certificado, poderá criar um. Para obter mais informações, consulte SSL/TLScertificados para balanceadores de carga clássicos.

Adicionar um HTTPS ouvinte usando o console

Você pode adicionar um HTTPS ouvinte a um balanceador de carga existente.

Para adicionar um HTTPS ouvinte ao seu balanceador de carga usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Receptores, escolha Gerenciar receptores.
5. Na página Gerenciar receptores, na seção Receptores, escolha Adicionar receptor.
6. Em Protocolo Listener, selecione HTTPS.

   > **Important**
   >
   > Por padrão, o protocolo da instância éHTTP. Se você quiser configurar a autenticação da instância de back-end, altere o protocolo da instância para. HTTPS

7. Para a política de segurança, recomendamos que você use a política de segurança predefinida mais recente. Se você precisar usar uma política de segurança predefinida diferente ou criar uma política personalizada, consulte Atualizar a configuração de SSL negociação.
8. Em SSLCertificado padrão, escolha Editar e, em seguida, faça o seguinte:

   - Se você criou ou importou um certificado usando AWS Certificate Manager, escolha De ACM, selecione o certificado na lista e escolha Salvar alterações.

> **Note**
>
> Essa opção estará disponível apenas em regiões que suportam o AWS Certificate Manager.

- Se você importou um certificado usando IAMIAM, escolha De, selecione o certificado na lista e escolha Salvar alterações.
- Se você tiver um SSL certificado para importarACM, selecione Importar e Para ACM. Em Chave privada do certificado, copie e cole o conteúdo do arquivo PEM de chave privada codificado. No corpo do certificado, copie e cole o conteúdo do arquivo PEM de certificado de chave pública codificado. Em Cadeia de certificados - opcional, copie e cole o conteúdo do arquivo da cadeia de certificados PEM codificado, a menos que você esteja usando um certificado autoassinado e não seja importante que os navegadores aceitem implicitamente o certificado.
- Se você tiver um SSL certificado para importar, mas não ACM for suportado nessa região, selecione Importar e Para IAM. EmNome do certificado, digite o nome do certificado. Em Chave privada do certificado, copie e cole o conteúdo do arquivo PEM de chave privada codificado. No corpo do certificado, copie e cole o conteúdo do arquivo PEM de certificado de chave pública codificado. Em Cadeia de certificados - opcional, copie e cole o conteúdo do arquivo da cadeia de certificados PEM codificado, a menos que você esteja usando um certificado autoassinado e não seja importante que os navegadores aceitem implicitamente o certificado.
- Escolha Salvar alterações.

9. Para a Durabilidade do cookie, o padrão é Desabilitado. Para alterar, escolha Editar. Se escolher Gerado pelo balanceador de carga, um Período de expiração deverá ser especificado. Caso escolha Gerado pela aplicação, um Nome de cookie deverá ser especificado. Depois de selecionar, escolha Salvar alterações.
10. (Opcional) Escolha Adicionar receptor para adicionar mais receptores.
11. Escolha Salvar alterações para adicionar os receptores que você acabou de configurar.
12. (Opcional) Para configurar a autenticação de instância de back-end para um balanceador de carga existente, você deve usar o AWS CLI ou anAPI, pois essa tarefa não é compatível com o console. Para obter mais informações, consulte Configurar autenticação de instância back-end.

Adicione um HTTPS ouvinte usando o AWS CLI

Você pode adicionar um HTTPS ouvinte a um balanceador de carga existente.

Para adicionar um HTTPS ouvinte ao seu balanceador de carga usando o AWS CLI

1. Obtenha o Amazon Resource Name (ARN) do SSL certificado. 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 create-load-balancer-listenerscomando a seguir para adicionar um ouvinte ao seu balanceador de carga que aceita HTTPS solicitações na porta 443 e envia as 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
   ```

   Se você quiser configurar a autenticação da instância de back-end, use o comando a seguir para adicionar um ouvinte que aceite HTTPS solicitações 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,SSLCertificate
   ```

3. (Opcional) Você pode usar o describe-load-balancerscomando a seguir para ver os detalhes atualizados do seu balanceador de carga:

   ```
   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 HTTPS ouvinte 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-policye set-load-balancer-policies-of-listener. Para obter mais informações, consulte Atualize a configuração SSL da negociação usando o AWS CLI.
5. (Opcional) Para configurar a autenticação da instância de back-end, use o comando set-load-balancer-policies- for-backend-server. Para obter mais informações, consulte Configurar autenticação de instância back-end.

Substitua o SSL certificado do seu Classic Load Balancer

Se você tiver um HTTPS ouvinte, implantou um certificado de SSL servidor em seu balanceador de carga ao criar o ouvinte. Cada certificado vem com um período de validade. Você deve garantir que renovou ou substituiu o certificado antes do fim do período de validade.

Os certificados fornecidos AWS Certificate Manager e implantados em seu balanceador de carga podem ser renovados automaticamente. ACMtenta renovar os certificados antes que eles expirem. Para obter mais informações, consulte Renovação gerenciada no Guia do usuário do AWS Certificate Manager . Se você importou um certificado paraACM, deverá monitorar a data de expiração do certificado e renová-lo antes que ele 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.

Conteúdo

- Substitua o SSL certificado usando o console
- Substitua o SSL certificado usando o AWS CLI

Substitua o SSL certificado usando o console

Você pode substituir o certificado implantado em seu balanceador de carga por um certificado fornecido por ACM ou por um certificado enviado para. IAM

Para substituir o SSL certificado de um balanceador de HTTPS carga usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.

4. Na guia Receptores, escolha Gerenciar receptores.
5. Na página Gerenciar ouvintes, localize o ouvinte a ser atualizado, escolha Editar em SSLCertificado padrão e faça o seguinte:

   - Se você criou ou importou um certificado usando AWS Certificate Manager, escolha De ACM, selecione o certificado na lista e escolha Salvar alterações.

     > **Note**
     >
     > Essa opção estará disponível apenas em regiões que suportam o AWS Certificate Manager.

   - Se você importou um certificado usando IAMIAM, escolha De, selecione o certificado na lista e escolha Salvar alterações.
   - Se você tiver um SSL certificado para importarACM, selecione Importar e Para ACM. Em Chave privada do certificado, copie e cole o conteúdo do arquivo PEM de chave privada codificado. No corpo do certificado, copie e cole o conteúdo do arquivo PEM de certificado de chave pública codificado. Em Cadeia de certificados - opcional, copie e cole o conteúdo do arquivo da cadeia de certificados PEM codificado, a menos que você esteja usando um certificado autoassinado e não seja importante que os navegadores aceitem implicitamente o certificado.
   - Se você tiver um SSL certificado para importar, mas não ACM for suportado nessa região, selecione Importar e Para IAM. EmNome do certificado, digite o nome do certificado. Em Chave privada do certificado, copie e cole o conteúdo do arquivo PEM de chave privada codificado. No corpo do certificado, copie e cole o conteúdo do arquivo PEM de certificado de chave pública codificado. Em Cadeia de certificados - opcional, copie e cole o conteúdo do arquivo da cadeia de certificados PEM codificado, a menos que você esteja usando um certificado autoassinado e não seja importante que os navegadores aceitem implicitamente o certificado.
   - Escolha Salvar alterações.

Substitua o SSL certificado usando o AWS CLI

Você pode substituir o certificado implantado em seu balanceador de carga por um certificado fornecido por ACM ou por um certificado enviado para. IAM

Para substituir um SSL certificado 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 seguinte 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 SSL certificado por um certificado enviado para IAM

1. Se você tem um SSL certificado, mas não o carregou, consulte Carregar um certificado de servidor no Guia do IAM usuário.
2. Use o get-server-certificatecomando a seguir para obter o ARN certificado:

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

3. Use o seguinte 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
```

Atualize a configuração SSL de negociação do seu Classic Load Balancer

O Elastic Load Balancing fornece políticas de segurança que têm configurações de SSL negociação predefinidas para usar na negociação de SSL conexões entre clientes e seu balanceador de carga. Se você estiver usando o SSL protocoloHTTPS/para seu ouvinte, poderá usar uma das políticas de segurança predefinidas ou usar sua própria política de segurança personalizada.

Para obter mais informações sobre as políticas de segurança, consulte SSLconfigurações de negociação para Classic Load Balancers. Para obter informações sobre as configurações das

políticas de segurança fornecidas pelo Elastic Load Balancing, consulte Políticas de SSL segurança predefinidas.

Se você criar umHTTPS/SSLlistener sem associar uma política de segurança, o Elastic Load Balancing associará a política de segurança predefinida padrãoELBSecurityPolicy-2016-08,, ao seu load balancer.

Se você preferir, pode criar uma configuração personalizada. É altamente recomendável que você teste sua política de segurança antes de atualizar a configuração do balanceador de carga.

Os exemplos a seguir mostram como atualizar a configuração de SSL negociação para um SSL ouvinte HTTPS /. 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.

Conteúdo

- Atualize a configuração SSL de negociação usando o console
- Atualize a configuração SSL da negociação usando o AWS CLI

Atualize a configuração SSL de negociação 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 SSL de negociação para um balanceador de SSL cargaHTTPS// usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Receptores, escolha Gerenciar receptores.
5. Na página Gerenciar receptores, localize o receptor a ser atualizado, escolha Editar em Política de segurança e selecione uma política de segurança usando uma das seguintes opções:
   - Mantenha a política padrão, ELBSecurityPolicy-2016-08, e escolha Salvar alterações.

- Selecione uma política predefinida diferente do padrão e escolha Salvar alterações.
- Selecione Personalizar e habilite pelo menos um protocolo e uma cifra, da seguinte forma:

  a. Em SSLProtocolos, selecione um ou mais protocolos para habilitar.

  b. Em SSLOpções, selecione Preferência de pedido do servidor para usar o pedido listado no Políticas de SSL segurança predefinidas para SSL negociação.

  c. Em SSLCifras, selecione uma ou mais cifras para habilitar. Se você já tiver um SSL certificado, deverá habilitar a cifra usada para criar o certificado, pois as DSA RSA cifras são específicas do algoritmo de assinatura.

  d. Escolha Salvar alterações.

Atualize a configuração SSL da negociação usando o 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 SSL segurança predefinida

1. Use o describe-load-balancer-policiescomando a seguir 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 SSL segurança predefinidas.

2. Use o create-load-balancer-policycomando para criar uma política de SSL negociação usando uma das políticas de segurança predefinidas que você descreveu 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 exceder o limite do número de políticas para o balanceador de carga, use o delete-load-balancer-policycomando para excluir as políticas não utilizadas.

3. (Opcional) Use o describe-load-balancer-policiescomando a seguir 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 seguinte comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do balanceador de carga:

```
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 describe-load-balancerscomando a seguir para verificar se a nova política está habilitada para a porta do balanceador de carga:

```
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. As RSA cifras DSA e são específicas do algoritmo de assinatura e são usadas para criar o SSL certificado. Se você já tiver um SSL certificado, certifique-se de habilitar a cifra

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 SSL de segurança personalizada

1. Use o create-load-balancer-policycomando para criar uma política de SSL negociação 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 exceder o limite do número de políticas para o balanceador de carga, use o delete-load-balancer-policycomando para excluir as políticas não utilizadas.

2. (Opcional) Use o describe-load-balancer-policiescomando a seguir 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 seguinte comando set-load-balancer-policies-of-listener para habilitar a política na porta 443 do balanceador de carga:

```
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 describe-load-balancerscomando a seguir para verificar se a nova política está habilitada para a porta do balanceador de carga:

```
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"
      ]
  }
...
```

Instâncias registradas para seu Classic Load Balancer

Depois de criar seu Classic Load Balancer, você deve registrar suas EC2 instâncias com o load balancer. Você pode selecionar EC2 instâncias de uma única zona de disponibilidade ou de várias zonas de disponibilidade na mesma região do balanceador de carga. O Elastic Load Balancing executa rotineiramente verificações de saúde em EC2 instâncias registradas e distribui automaticamente as solicitações recebidas para o DNS nome do seu load balancer entre as instâncias registradas e íntegras. EC2

Conteúdo

- Práticas recomendadas para as suas instâncias
- Recomendações para o seu VPC
- Registre instâncias com seu Classic Load Balancer
- Verificações de saúde das instâncias do seu Classic Load Balancer
- Grupos de segurança para as instâncias do seu Classic Load Balancer
- Rede ACLs para as instâncias do seu Classic Load Balancer

Práticas recomendadas para as suas instâncias

- 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 Configurar grupos de segurança para seu Classic Load Balancer. 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.
- Instale um servidor web, como Apache ou Internet Information Services (IIS), em todas as instâncias que você planeja registrar com seu balanceador de carga.
- Para HTTPS ouvintes HTTP e ouvintes, recomendamos que você ative a opção keep-alive em suas EC2 instâncias, o que permite que o balanceador de carga reutilize as conexões com suas instâncias para várias solicitações de clientes. Isso reduz a carga no seu servidor web e melhora o throughput do balanceador de carga. 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 suporta o Path Maximum Transmission Unit (MTU) Discovery. Para garantir que o Path MTU Discovery funcione corretamente, você deve garantir que o grupo de

segurança da sua instância permita a ICMP fragmentação necessária (tipo 3, código 4) das mensagens. Para obter mais informações, consulte Path MTU Discovery no Guia EC2 do usuário da Amazon.

Recomendações para o seu VPC

Nuvem privada virtual (VPC)

A menos que você tenha criado o seu Conta da AWS antes de 2014, você tem um padrão VPC em cada região. Você pode usar um padrão VPC para seu balanceador de carga, se tiver um, ou criar um novoVPC. Para obter mais informações, consulte o Guia VPC do usuário da Amazon.

Sub-redes para seu balanceador de carga

Para garantir que seu balanceador de carga possa ser escalado adequadamente, verifique se cada sub-rede do seu balanceador de carga tem um CIDR bloco com pelo menos uma `/27` máscara de bits (por exemplo,`10.0.0.0/27`) e tem pelo menos 8 endereços IP livres. Seu balanceador de carga usa esses endereços IP para estabelecer conexões com as instâncias e para aumentar a escala horizontalmente, se necessário. Se não houver endereços IP suficientes, talvez o balanceador de carga não consiga escalar, causando erros 503 devido à capacidade insuficiente.

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, por padrão, VPCs há uma sub-rede pública por zona de disponibilidade.

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.

Rede ACLs

A rede ACLs para você VPC deve permitir tráfego em ambas as direções na porta do ouvinte e na porta de verificação de integridade. Para obter mais informações, consulte Rede ACLs para as instâncias do seu Classic Load Balancer.

Registre instâncias com seu Classic Load Balancer

O registro de uma EC2 instância a adiciona ao seu balanceador de carga. 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.

O cancelamento do registro de uma EC2 instância a remove do seu balanceador de carga. 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 Classic Load Balancer.

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 sua EC2 instância com seu balanceador de carga usando seu endereço IP.

[EC2-VPC] Quando você registra uma instância com uma interface de rede elástica (ENI) conectada, o balanceador de carga encaminha as solicitações para o endereço IP primário da interface primária (eth0) da instância.

Conteúdo

- Registrar uma instância
- Visualize as instâncias registradas em um balanceador de carga
- Determine o balanceador de carga para uma instância registrada
- Cancelar o registro de uma instância

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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Instâncias de destino, selecione Gerenciar instâncias.
5. Na página Gerenciar instâncias, dentro da tabela Instâncias disponíveis, selecione as instâncias a serem registradas no seu balanceador de carga.
6. Certifique-se de que as instâncias que precisam ser registradas sejam preenchidas na tabela Revisar instâncias selecionadas.
7. Escolha Salvar alterações.

Para registrar suas instâncias usando o AWS CLI

Use o seguinte 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 describe-load-balancerscomando a seguir para listar as instâncias registradas com o 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 describe-load-balancerscomando a seguir 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 Separar EC2instâncias do seu grupo de Auto Scaling no Guia do usuário do Amazon Auto EC2 Scaling.

Para cancelar o registro das suas instâncias usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Instâncias de destino, selecione Gerenciar instâncias.
5. Na página Gerenciar instâncias, dentro da tabela Instâncias disponíveis, desmarque as instâncias para cancelar seu registro do balanceador de carga.
6. Certifique-se de que as instâncias que precisam ter o registro cancelado não sejam preenchidas na tabela Revisar instâncias selecionadas.
7. Escolha Salvar alterações.

Para cancelar o registro de suas instâncias usando o AWS CLI

Use o seguinte 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"
        }
    ]
}
```

Verificações de saúde das instâncias do seu Classic Load Balancer

Seu Classic Load Balancer 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 Classic Load Balancer, 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 saúde do Elastic Load Balancing ao seu grupo de Auto Scaling no Guia do usuário do Amazon Auto EC2 Scaling.

Conteúdo

- Configuração de verificação de integridade
- Atualizar a configuração de verificação de integridade
- Verificar a integridade das suas instâncias
- Solucionar problemas das verificações de integridade

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`

Campo	Descrição
	Padrão do console: `HTTP` CLI/APIpadrão: `TCP`
Port (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 especific ada 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` CLI/APIpadrão: `TCP:80`
Path	O destino da HTTPS solicitação HTTP ou. Uma HTTPS GET solicitação HTTP or 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 especific ar 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 Intervalo	A quantidade de tempo entre as verificações de integrida de de uma instância individual, em segundos. Valores válidos: 5 a 300 Padrão: 30
Limite não íntegro	O número de verificações de saúde consecutivas com falha que devem ocorrer antes de declarar uma EC2 instância não íntegra. Valores válidos: 2 a 10 Padrão: 2
Healthy Threshold	O número de verificações de saúde consecutivas bem-sucedidas que devem ocorrer antes de declarar uma EC2 instância 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 as verificações de integridade excederem as falhas

UnhealthyThresholdCountconsecutivas, o balanceador de carga colocará a instância fora de serviço. Quando as verificações de integridade excedem os sucessos HealthyThresholdCountconsecutivos, o balanceador de carga coloca a instância novamente em serviço.

Uma verificação de HTTPS integridadeHTTP/será bem-sucedida se a instância retornar um código de resposta 200 dentro do intervalo da verificação de integridade. Uma verificação TCP de saúde será bem-sucedida se a TCP conexão for bem-sucedida. Uma verificação SSL de saúde será bem-sucedida se o SSL aperto de mão 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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Verificações de integridade, selecione Editar.
5. Na página Editar configurações de verificação de integridade, em Verificações de integridade, atualize a configuração conforme necessário.
6. Quando você estiver satisfeito com suas seleções, escolha Salvar alterações.

Para atualizar a configuração da verificação de integridade do seu balanceador de carga usando o AWS CLI

Use o seguinte 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 EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Na seção Detalhes, Status indica quantas instâncias estão em serviço.
5. Na guia Instâncias de destino, dentro da tabela Instâncias de destino, a coluna Status de integridade indica o status específico de cada instância registrada.

Para verificar o status de saúde de suas instâncias usando o AWS CLI

Use o seguinte 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 falhar em uma verificação de integridade são quando as EC2 instâncias fecham conexões com seu balanceador de carga ou quando a resposta das EC2 instâncias atinge o tempo limite. 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 Classic Load Balancer: verificações de integridade.

Grupos de segurança para as instâncias do seu Classic Load Balancer

Um security group atua como um firewall que controla o tráfego permitido de e para uma ou mais instâncias. Ao executar uma EC2 instância, você pode associar um ou mais grupos de segurança à instância. 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 os grupos EC2 de segurança da Amazon no Guia EC2 do usuário da Amazon.

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

Origem	Protocolo	Port Range (Intervalo de portas)	Comentário
load balancer security group	TCP	*instance listener*	Permitir tráfego do load balancer na porta do ouvinte da instância
load balancer security group	TCP	*health check*	Permitir tráfego do load balancer na porta de verificação de integridade

Também recomendamos que você permita que o ICMP tráfego de entrada ofereça suporte ao Path MTU Discovery. Para obter mais informações, consulte Path MTU Discovery no Guia EC2 do usuário da Amazon.

Rede ACLs para as instâncias do seu Classic Load Balancer

Uma lista de controle de acesso à rede (ACL) permite ou nega tráfego específico de entrada ou saída no nível da sub-rede. Você pode usar a rede padrão ACL para o seuVPC, ou você pode criar uma rede personalizada ACL para você VPC com regras semelhantes às regras dos seus grupos de segurança, a fim de adicionar uma camada adicional de segurança ao seuVPC.

A lista de controle de acesso à rede padrão (ACL) para o VPC permite todo o tráfego de entrada e saída. Se você criar uma rede personalizadaACLs, deverá adicionar regras que permitam que o balanceador de carga e as instâncias se comuniquem.

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 de CIDR do VPC para`0.0.0.0/0`.

A seguir estão as regras de entrada recomendadas.

Origem	Protocolo	Port Range (Intervalo de portas)	Comentário
	TCP		

Origem	Protocolo	Port Range (Intervalo de portas)	Comentário
VPC CIDR		*instance listener*	Permitir tráfego de entrada da porta do ouvinte VPC CIDR na instância
VPC CIDR	TCP	*health check*	Permitir tráfego de entrada a partir da VPC CIDR porta de verificação de integridade

A seguir estão as regras de saída recomendadas.

Destination (Destino)	Protocolo	Port Range (Intervalo de portas)	Comentário
VPC CIDR	TCP	1024-65535	Permitir tráfego de saída para as portas VPC CIDR efêmeras

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.

CloudWatch métricas

O Elastic Load Balancing publica pontos de dados na Amazon CloudWatch sobre seus balanceadores de carga e instâncias de back-end. CloudWatch permite que você recupere estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Você pode usar essas métricas para verificar se o sistema está executando conforme o esperado. Para obter mais informações, consulte CloudWatch métricas para seu Classic Load Balancer.

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 obter mais informações, consulte Logs de acesso do seu Classic Load Balancer.

CloudTrail troncos

AWS CloudTrail permite que você acompanhe as chamadas feitas para o Elastic Load Balancing API por ou em nome de sua AWS conta. 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 obter mais informações, consulte Registrando API chamadas para seu Classic Load Balancer usando AWS CloudTrail.

CloudWatch métricas para seu Classic Load Balancer

O Elastic Load Balancing publica pontos de dados na Amazon CloudWatch para seus balanceadores de carga e suas instâncias de back-end. CloudWatch permite que você recupere estatísticas sobre

esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecido como métricas. Considere uma métrica como uma variável a ser monitorada, e os pontos de dados como os valores dessa variável ao longo do tempo. Por exemplo, você pode monitorar o número total de EC2 instâncias íntegras de um balanceador de carga em um período de tempo especificado. Cada ponto de dados tem um time stamp associado e uma unidade de medida opcional.

Você pode usar métricas para verificar se o sistema está executando conforme o esperado. Por exemplo, você pode criar um CloudWatch alarme para monitorar uma métrica específica e iniciar uma ação (como enviar uma notificação para um endereço de e-mail) se a métrica estiver fora do que você considera um intervalo aceitável.

O Elastic Load Balancing reporta métricas CloudWatch somente quando as solicitações estão fluindo pelo balanceador de carga. Se houver solicitações passando pelo balanceador de carga, o Elastic Load Balancing vai medir e enviar suas métricas em intervalos de 60 segundos. Se não há solicitações passando pelo load balancer ou não há dados para uma métrica, a métrica não é reportada.

Para obter mais informações sobre a Amazon CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.

Conteúdo

- Métricas do Classic Load Balancer
- Dimensões métricas dos Classic Load Balancers
- Estatísticas para métricas do Classic Load Balancer
- Veja CloudWatch as métricas do seu balanceador de carga

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

Métrica	Descrição
	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 instância s 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`	[HTTPouvinte] O número de solicitações que não estão em conformidade com RFC 7230. Critérios de relatório: há um valor diferente de zero Estatísticas: a estatística mais útil é `Sum`.

Métrica	Descrição
`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. 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.

Métrica	Descrição
`HTTPCode_Backend_2XX`, `HTTPCode_Backend_3XX`, `HTTPCode_Backend_4XX`, `HTTPCode_Backend_5XX`	[HTTPouvinte] O número de códigos de HTTP resposta gerados pelas 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. Exemplo: suponha que seu balanceador de carga tenha 2 instâncias em us-west-2a e 2 instâncias em us-west-2b, e que as solicitações enviadas para 1 instância em us-west-2a resultem em 500 respostas. HTTP 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`	[HTTPouvinte] O número de códigos de erro do cliente HTTP 4XX gerados pelo balanceador de carga. 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. Exemplo: suponha que seu balanceador de carga tenha us-west-2 a e us-west-2b ativados e que as solicitações do cliente incluam uma solicitação malformada. URL 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	[HTTPouvinte] O número de códigos de erro do servidor HTTP 5XX gerados pelo balanceador de carga. 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 solicitaç ões. 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.

Métrica	Descrição
`Latency`	[HTTPlistener] O tempo total decorrido, em segundos, desde o momento em que o balanceador de carga enviou a solicitação para uma instância registrada até que a instância começou a enviar os cabeçalhos de resposta. [TCPlistener] O tempo total decorrido, em segundos, para o balanceador de carga estabelecer com êxito uma conexão 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). [HTTPlistener] O número de solicitações recebidas e roteadas, incluindo respostas de HTTP erro das instâncias registradas. [TCPouvinte] 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.

Métrica	Descrição
`SpilloverCount`	O número total de solicitações que foram rejeitadas porque a fila de pico está cheia. [HTTPouvinte] O balanceador de carga retorna um código de erro HTTP 503. [TCPouvinte] O balanceador de carga 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 solicitaç ões. 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 (HTTPouvinte) ou conexões (TCPouvinte) que estão pendentes de roteamento para uma instância íntegra. O tamanho máximo da fila é 1.024. As solicitaç ões ou conexões adicionais são rejeitadas quando a fila está cheia. Para obter 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-2 a 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 probabili dade 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.

Métrica	Descrição
`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 são destinadas apenas para uso informativo, não para uso com CloudWatch alarmes. 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
`EstimatedALBActive ConnectionCount`	O número estimado de TCP conexões simultâneas ativas dos clientes ao balanceador de carga e do balanceador de carga aos 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 LCUs que usa por hora. Para obter mais informações, consulte Definição de preço do Elastic Load Balancing.
`EstimatedALBNewConnectionCount`	O número estimado de novas TCP conexões estabelecidas dos clientes com o balanceador de carga e do balanceador de carga com os 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

CloudWatch fornece estatísticas com base nos pontos de dados métricos publicados pelo Elastic Load Balancing. As estatísticas são agregações de dados de métrica ao longo de um período especificado. Quando você solicita estatísticas, o fluxo de dados apresentado é identificado pelo nome da métrica e pela dimensão. Dimensão é um par de nome/valor que identifica exclusivamente uma métrica. Por exemplo, você pode solicitar estatísticas de todas as EC2 instâncias íntegras por trás de um balanceador de carga lançado 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. É possível 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. Ao usar o 99º percentil como acionador ou CloudWatch alarme do Auto Scaling, você pode ter como meta que no máximo 1% das solicitações demorem mais do que 2 ms para serem processadas.

Veja CloudWatch as métricas do seu balanceador de carga

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

Como alternativa, você pode visualizar as métricas do seu balanceador de carga usando o CloudWatch console.

Para visualizar as métricas usando o console

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

2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Escolha o nome do balanceador de carga para abrir sua página de detalhes.
4. Escolha a guia Monitoring (Monitoramento).
5. Para obter uma visão mais ampla de uma única métrica, passe o mouse sobre o gráfico e escolha o ícone `Maximize`. As seguintes métricas estão disponíveis:

   - Hosts íntegros – `HealthyHostCount`
   - Hosts não íntegros – `UnHealthyHostCount`
   - Latência média – `Latency`
   - Solicitações: `RequestCount`
   - Erros de conexão do back-end – `BackendConnectionErrors`
   - Comprimento da fila de sobretensão – `SurgeQueueLength`
   - Contagem de transmissão – `SpilloverCount`
   - HTTP2 XXs — `HTTPCode_Backend_2XX`
   - HTTP3 XXs — `HTTPCode_Backend_3XX`
   - HTTP4 XXs — `HTTPCode_Backend_4XX`
   - HTTP5 XXs — `HTTPCode_Backend_5XX`
   - ELBHTTP4 XXs — `HTTPCode_ELB_4XX`
   - ELBHTTP5 XXs — `HTTPCode_ELB_5XX`
   - Estimativa de bytes processados: `EstimatedProcessedBytes`
   - Consumo ALB estimado LCUs — `EstimatedALBConsumedLCUs`
   - Contagem estimada de conexões ALB ativas — `EstimatedALBActiveConnectionCount`
   - Contagem estimada de ALB novas conexões — `EstimatedALBNewConnectionCount`

Para visualizar métricas usando o CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, selecione Métricas.
3. Selecione o namespace 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. É possível usar esses logs de acesso para analisar padrões de tráfego e solucionar problemas.

Os logs de acesso são um recurso opcional do Elastic Load Balancing que é desabilitado por padrão. Depois que os logs de acesso para seu balanceador de carga forem habilitados, 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 criptografado automaticamente usando SSE -S3 antes de ser armazenado em seu bucket do S3 e descriptografado quando você o acessa. 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 por sua vez é criptografada com uma KMS chave que é rotacionada regularmente. Para obter mais informações, consulte Proteção de dados usando criptografia do lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3) no Guia 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.

Conteúdo

- Arquivos do log de acesso
- Entradas do log de acesso

- Processando logs de acesso
- Habilitar os logs de acesso do seu Classic Load Balancer
- Desabilitar os logs de acesso do seu Classic Load Balancer

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.

prefix

(Opcional) O prefixo (hierarquia lógica) no bucket. O prefixo especificado não pode incluir a string `AWSLogs`. Para mais informações, consulte Organizar objetos usando prefixos.

`AWSLogs`

Adicionamos a parte do nome do arquivo que começa com `AWSLogs` após o nome do bucket e o prefixo opcional que você especificar.

aws-account-id

O ID da AWS conta 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 balanceador de carga.

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.

Veja um exemplo de um nome de arquivo de log com um prefixo “my-app”:

```
s3://my-loadbalancer-logs/my-app/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

Veja um exemplo de um nome de arquivo de log sem um prefixo:

```
s3://my-loadbalancer-logs/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_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
horário	A hora em que o balanceador de carga 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.

Campo	Descrição
	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 registrad a não responder antes do tempo limite de inatividade.
request_processing _time	[HTTPlistener] O tempo total decorrido, em segundos, desde o momento em que o balanceador de carga recebeu a solicitação até o momento em que a enviou para uma instância registrada. [TCPlistener] O tempo total decorrido, em segundos, desde o momento em que o balanceador de carga aceitou uma SSL conexãoTCP/de um cliente até o momento em que o balanceador de carga envia o primeiro byte de dados para 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. Além disso, para TCP ouvintes, isso pode acontecer se o cliente estabelec er uma conexão com o balanceador de carga, mas não enviar nenhum dado. Esse valor também pode ser configurado como -1 se a instância registrada não responder antes do tempo limite de inatividade.

Campo	Descrição
backend_processing_time	[HTTPlistener] O tempo total decorrido, em segundos, desde o momento em que o balanceador de carga enviou a solicitação para uma instância registrada até que a instância começou a enviar os cabeçalhos de resposta. [TCPlistener] O tempo total decorrido, em segundos, para o balanceador de carga estabelecer com êxito uma conexão 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	[HTTPlistener] O tempo total decorrido (em segundos) desde o momento em que o balanceador de carga recebeu o cabeçalho de resposta da instância registrada até começar 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. [TCPlistener] O tempo total decorrido, em segundos, desde o momento em que o balanceador de carga recebeu o primeiro byte da instância registrada até começar 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	[HTTPouvinte] O código de status da resposta do balanceador de carga.

Campo	Descrição
backend_status_code	[HTTPlistener] O código de status da resposta da instância registrada.
received_bytes	O tamanho da solicitação, em bytes, recebida do cliente (solicitante). [HTTPlistener] O valor inclui o corpo da solicitação, mas não os cabeçalhos. [TCPlistener] O valor inclui o corpo da solicitação e os cabeçalhos.
sent_bytes	O tamanho da resposta, em bytes, enviada ao cliente (solicitante). [HTTPouvinte] O valor inclui o corpo da resposta, mas não os cabeçalho s. [TCPlistener] O valor inclui o corpo da solicitação e os cabeçalhos.
request	A linha de solicitação do cliente está entre aspas duplas e registrada no seguinte formato: HTTP Method + Protocol: //Host header:port + Path + version. HTTP O balanceador de carga preserva o URL enviado pelo cliente, como está, ao gravar a solicitação. URI Ele não define o tipo de conteúdo para o arquivo do log de acesso. Ao processar esse campo, considere como o cliente enviou URL o. [TCPouvinte] São três traços, cada um separado por um espaço e terminando com um espaço (“- - - “). URL
user_agent	[HTTP/HTTPSlistener] Uma string de agente de usuário que identific a 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	[HTTPS/SSLlistener] A SSL cifra. Esse valor é registrado somente se a TLS conexão de SSL entrada/foi estabelecida após uma negociação bem-sucedida. Caso contrário, o valor será configurado como -.
ssl_protocol	[HTTPS/SSLlistener] O SSL protocolo. Esse valor é registrado somente se a TLS conexão de entradaSSL/foi estabelecida após uma negociação bem-sucedida. Caso contrário, o valor será configurado como -.

Exemplos

Exemplo de HTTP entrada

Veja a seguir um exemplo de entrada de registro para um HTTP ouvinte (porta 80 a 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"
 - -
```

Exemplo de HTTPS entrada

Veja a seguir um exemplo de entrada de registro para um HTTPS ouvinte (porta 443 até a 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
```

Exemplo de TCP entrada

Veja a seguir um exemplo de entrada de registro para um TCP ouvinte (porta 8080 a 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 "- - - " "-" - -
```

Exemplo de SSL entrada

Veja a seguir um exemplo de entrada de registro para um SSL ouvinte (porta 8443 a 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. Talvez você não consiga processar uma quantidade tão grande de dados usando o line-by-line processamento. Assim, pode ter de usar ferramentas analíticas que forneçam soluções de processamento paralelo. Por exemplo, você pode usar as ferramentas analíticas a seguir para analisar e processar logs de acesso:

- O Amazon Athena é um serviço de consulta interativo que facilita a análise de dados no Amazon S3 usando o padrão. SQL 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.

Tarefas

- Etapa 1: Crie um bucket do S3
- Etapa 2: Anexe uma política ao seu bucket do S3
- Etapa 3: Configurar logs de acesso
- Etapa 4: Verificar permissões do bucket
- Solução de problemas

Etapa 1: Crie um bucket do S3

Ao habilitar os logs de acesso, você deverá especificar um bucket do S3 para os logs de acesso. O bucket deve atender aos seguintes requisitos:

Requisitos

- O bucket deve estar localizado na mesma região que o load balancer. O bucket e o balanceador de carga podem pertencer a contas diferentes.
- A única opção de criptografia do lado do servidor compatível são as chaves gerenciadas pelo Amazon S3 (-S3). SSE Para obter mais informações, consulte Chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3).

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 Criar bucket.
3. Na página Criar bucket, faça o seguinte:
    a. Para Nome do bucket, insira um nome para o 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 Região da AWS , selecione a região em que você criou seu balanceador de carga.
    c. Em Criptografia padrão, escolha Chaves gerenciadas pelo Amazon S3 (SSE-S3).
    d. Selecione Criar bucket.

Etapa 2: Anexe uma política ao seu bucket do S3

O bucket do S3 deve ter uma política de bucket que conceda permissão para que o Elastic Load Balancing grave os logs de acesso no bucket. As políticas de bucket são uma coleção de JSON declarações escritas na linguagem de política de acesso para definir permissões de acesso para seu bucket. Cada instrução inclui informações sobre uma única permissão e contém uma série de elementos.

Se estiver usando um bucket que já tem uma política anexada, você poderá adicionar a instrução para os logs 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.

Políticas de bucket disponíveis

A política do bucket que você usará depende Região da AWS da política do bucket.

Regiões disponíveis a partir de agosto de 2022

Esta política concede permissões ao serviço de entrega de logs especificado. Use essa política para balanceadores de carga em zonas de disponibilidade e zonas locais nas seguintes regiões:

- Ásia-Pacífico (Hyderabad)

- Ásia-Pacífico (Melbourne)
- Oeste do Canadá (Calgary)
- Europa (Espanha)
- Europa (Zurique)
- Israel (Tel Aviv)
- Oriente Médio (UAE)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*"
    }
  ]
}
```

Regiões disponíveis antes de agosto de 2022

Esta política concede permissões para o ID de conta do Elastic Load Balancing especificado. Use essa política para balanceadores de carga em zonas de disponibilidade e zonas locais nas regiões na lista abaixo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "my-s3-arn"
    }
  ]
```

```
}
```

Substituir *elb-account-id* com o ID do Conta da AWS para o Elastic Load Balancing da sua região:

- Leste dos EUA (N. da Virgínia): 127311923021
- Leste os EUA (Ohio): 033677994240
- Oeste dos EUA (N. da Califórnia): 027434742980
- Oeste dos EUA (Oregon): 797873946194
- África (Cidade do Cabo): 098369216593
- Ásia-Pacífico (Hong Kong): 754344448648
- Ásia-Pacífico (Jacarta) — 589379963580
- Ásia-Pacífico (Mumbai): 718504428378
- Ásia-Pacífico (Osaka): 383597477331
- Ásia-Pacífico (Seul): 600734575887
- Ásia-Pacífico (Singapura): 114774131450
- Ásia-Pacífico (Sydney): 783225319266
- Ásia-Pacífico (Tóquio): 582318560864
- Canadá (Central): 985666609251
- Europa (Frankfurt): 054676820928
- Europa (Irlanda): 156460612806
- Europa (Londres): 652711504416
- Europa (Milão): 635631232127
- Europa (Paris): 009996457667
- Europa (Estocolmo): 897822967062
- Oriente Médio (Bahrein): 076674570225
- América do Sul (São Paulo): 507241528517

Substituir *my-s3-arn* com a localização ARN dos seus registros de acesso. O ARN que você especifica depende se você planeja especificar um prefixo ao habilitar os registros de acesso na etapa 3.

- ARNexemplo com um prefixo

```
arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*
```

- ARNexemplo sem prefixo

```
arn:aws:s3:::bucket-name/AWSLogs/aws-account-id/*
```

AWS GovCloud (US) Regions

Esta política concede permissões para o ID de conta do Elastic Load Balancing especificado. Use essa política para balanceadores de carga em Zonas de Disponibilidade ou Zonas AWS GovCloud (US) Locais nas Regiões na lista abaixo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "my-s3-arn"
    }
  ]
}
```

Substituir *elb-account-id* com o ID do Conta da AWS para o Elastic Load Balancing da sua Conta da AWS região:

- AWS GovCloud (Oeste dos EUA) — 048591011584
- AWS GovCloud (Leste dos EUA) — 190560391635

Substituir *my-s3-arn* com a localização ARN dos seus registros de acesso. O ARN que você especifica depende se você planeja especificar um prefixo ao habilitar os registros de acesso na etapa 3.

- ARNexemplo com um prefixo

```
arn:aws-us-gov:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*
```

- ARNexemplo sem prefixo

```
arn:aws-us-gov:s3:::bucket-name/AWSLogs/aws-account-id/*
```

Para anexar uma política de bucket para logs de acesso ao seu bucket usando o console do Amazon S3

1. Abra o console do Amazon S3 em. https://console.aws.amazon.com/s3/
2. Selecione o nome do bucket para abrir sua página de detalhes.
3. Escolha Permissions (Permissões) e, em seguida, escolha Bucket policy (Política de bucket), Edit (Editar).
4. Crie ou atualize a política de bucket para conceder as permissões necessárias.
5. Escolha Salvar alterações.

Etapa 3: Configurar logs de acesso

Siga este procedimento para configurar logs de acesso a fim de capturar e entregar arquivos de log ao seu bucket do S3.

Requisitos

O bucket deverá atender aos requisitos descritos na etapa 1 e você deverá anexar uma política de bucket, conforme descrito na etapa 2. Se você especificar um prefixo, ele não deverá incluir a string "AWSLogs".

Para configurar os logs de acesso ao seu balanceador de carga usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, na seção Monitoramento, faça o seguinte:

a. Habilite os Logs de acesso.
b. Para S3 URI, insira o S3 URI para seus arquivos de log. O URI que você especifica depende se você está usando um prefixo.
   - URIcom um prefixo: `s3://bucket-name/prefix`
   - URIsem um prefixo: `s3://bucket-name`
c. Manter Intervalo de registro em log como `60 minutes - default`.
d. Escolha Salvar alterações.

Para configurar os registros de acesso para seu balanceador de carga usando o 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"
  }
}
```

Em seguida, especifique o arquivo.json no modify-load-balancer-attributescomando da seguinte forma:

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

O seguinte é um exemplo de resposta.

```
{
    "LoadBalancerAttributes": {
        "AccessLog": {
            "Enabled": true,
            "EmitInterval": 60,
            "S3BucketName": "my-loadbalancer-logs",
            "S3BucketPrefix": "my-app"
        }
```

```
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Gerenciar o bucket do S3 para os logs de acesso

Certifique-se de desabilitar os registros de acesso antes de excluir o bucket que você configurou para os logs de acesso. Caso contrário, se houver um novo bucket com o mesmo nome e a política de bucket necessária criada em um Conta da AWS que você não possua, o Elastic Load Balancing poderá gravar os registros de acesso do seu load balancer nesse novo bucket.

Etapa 4: Verificar permissões do bucket

Após o registro de acesso em logs ser habilitado para seu balanceador de carga, o Elastic Load Balancing validará o bucket do S3 e criará um arquivo de teste para garantir que a política do bucket especifique as permissões necessárias. Você pode usar o console do S3 para verificar se o arquivo de teste foi criado. O arquivo de teste não é um arquivo de log de acesso real; ele não contêm registros de exemplo.

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 o nome do bucket do S3 que você especificou para logs de acesso.
3. Localize o arquivo de teste, `ELBAccessLogTestFile`. O local dependerá de você estar ou não usando um prefixo.

   - Local com um prefixo: *`my-bucket`*`/`*`prefix`*`/AWSLogs/`*`123456789012`*`/ELBAccessLogTestFile`
   - Local sem prefixo: *`my-bucket`*`/AWSLogs/`*`123456789012`*`/ELBAccessLogTestFile`

Solução de problemas

Acesso negado para o bucket: ***`bucket-name`***. Verifique a permissão do S3bucket

Se você receber este erro, possíveis causas serão:

- A política do bucket não concede ao Elastic Load Balancing permissão para gravar logs de acesso no bucket. Confira se está usando a política de bucket correta para a região. Verifique se o recurso ARN usa o mesmo nome de bucket que você especificou ao habilitar os registros de acesso.

Verifique se o recurso ARN não inclui um prefixo se você não especificou um prefixo ao habilitar os registros de acesso.

- O bucket usa uma opção de criptografia que não é aceita no lado do servidor. O bucket deve usar chaves gerenciadas pelo Amazon S3 (SSE-S3).

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 que os logs de acesso forem desabilitados, 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 logs de acesso do seu balanceador de carga usando o console

1. Abra o EC2 console da Amazon em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing (Balanceamento de carga), escolha Load balancers (Balanceadores de carga).
3. Selecione o nome do balanceador de carga para abrir sua página de detalhes.
4. Na guia Atributos, escolha Editar.
5. Na página Editar atributos do balanceador de carga, na seção Monitoramento, desabilite Logs de acesso.

Para desativar os registros de acesso usando o AWS CLI

Use o modify-load-balancer-attributescomando a seguir para desativar os registros 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"
        }
    }
}
```

Registrando API chamadas para seu Classic Load Balancer usando AWS CloudTrail

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

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

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 obter mais informações, consulte Logs de acesso do seu Classic Load Balancer.

Informações sobre o Elastic Load Balancing em CloudTrail

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

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Elastic Load Balancing, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos

de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando SNS notificações da Amazon para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões
- Receber arquivos de log do CloudTrail de várias contas

Todas as ações do Elastic Load Balancing para Classic Load Balancers são registradas CloudTrail e documentadas na versão 2012-06-01 da Referência do Elastic Load Balancing. API Por exemplo, chamadas para as `DeleteLoadBalancer` ações `CreateLoadBalancer` e geram entradas nos arquivos de CloudTrail log.

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

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

Para obter mais informações, consulte o CloudTrail userIdentity elemento.

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

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

Os arquivos de log incluem eventos para todas as AWS API chamadas para sua AWS conta, não apenas as chamadas do Elastic Load BalancingAPI. Você pode localizar chamadas para o Elastic Load Balancing API verificando os `eventSource` elementos com o valor.

`elasticloadbalancing.amazonaws.com` Para visualizar um registro para uma ação específica, como `CreateLoadBalancer`, verifique os elementos `eventName` com o nome da ação.

A seguir estão exemplos de registros de CloudTrail log do Elastic Load Balancing para um usuário que criou um Classic Load Balancer e o excluiu usando o. AWS CLI Você pode identificar o CLI uso dos `userAgent` elementos. Você pode identificar as API chamadas solicitadas usando os `eventName` elementos. 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 Classic Load Balancer

As tabelas a seguir listam os recursos para soluções de problemas que você achará úteis à medida que trabalhar com um Classic Load Balancer.

APIerros

Erro
CertificateNotFound: Indefinido
OutofService: Ocorreu um erro transitório

HTTPerros

Erro
HTTP400: BAD _ REQUEST
HTTP405: METHOD _ _ NOT ALLOWED
HTTP408: Tempo limite da solicitação
HTTP502: Gateway inválido
HTTP503: Serviço indisponível
HTTP504: Tempo limite do gateway

Métricas do código de resposta

Métrica do código de resposta
HTTPCode_ ELB _4XX
HTTPCode_ ELB _5XX
HTTPCode_Backend_2xx

Métrica do código de resposta
HTTPCode_Backend_3xx
HTTPCode_Backend_4xx
HTTPCode_Backend_5xx

Problemas de verificação de integridade

Problema
Erro na página de destino da verificação de integridade
A conexão com as instâncias expirou
A autenticação de chave pública não está funcionando
A instância não está recebendo tráfego do load balancer
As portas da instância não estão abertas
As instâncias em um grupo de Auto Scaling estão falhando na verificação de integridade ELB

Problemas de conectividade

Problema
Os clientes não conseguem se conectar a um balanceador de carga voltado para a Internet
As solicitações enviadas para um domínio personalizado não são recebidas pelo balanceador de carga.
HTTPSsolicitações enviadas para o balanceador de carga retornam "NET:: ERR _ CERT _ _ COMMON NAME _INVALID”

Problemas de registro de instância

Problema
Demorando muito para registrar uma EC2 instância
Não é possível registrar uma instância iniciada a partir de uma conta paga AMI

Solucionar problemas de um Classic Load API Balancer: erros

A seguir estão as mensagens de erro retornadas pelo Elastic Load BalancingAPI, as possíveis causas e as etapas que você pode seguir para resolver os problemas.

Mensagens de erro

- CertificateNotFound: Indefinido
- OutofService: Ocorreu um erro transitório

CertificateNotFound: 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.

Causa 2: Se você estiver usando o AWS CLI ou API diretamente, poderá receber esse erro se fornecer um Amazon Resource Name (ARN) para um certificado que não existe.

Solução 2: use a ação AWS Identity and Access Management (IAM) GetServerCertificatepara obter o certificado ARN e verificar se você forneceu o valor correto para ARN o.

OutofService: Ocorreu um erro transitório

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: repita a API chamada. Se o problema persistir, vá para o AWS Support Center para obter assistência.

Solucionar problemas de um Classic Load HTTP Balancer: erros

O HTTP método (também chamado de verbo) especifica a ação a ser executada no recurso que está recebendo uma HTTP solicitação. Os métodos padrão para HTTP solicitações são definidos em RFC 2616, Definições de métodos. Os métodos padrão incluem GETPOST, PUTHEAD,, OPTIONS e. Alguns aplicativos da Web exigem (e às vezes introduzem) métodos que são extensões dos métodos HTTP /1.1. Exemplos comuns de métodos HTTP estendidos incluem PATCH REPORTMKCOL,PROPFIND,MOVE,, LOCK e. O Elastic Load Balancing aceita todos os métodos padrão e não HTTP padrão.

HTTPsolicitações e respostas usam campos de cabeçalho para enviar informações sobre as HTTP mensagens. 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 HTTP cabeçalho é definido em RFC 2616, Cabeçalhos de mensagens. Para obter mais informações, consulte HTTPcabeçalhos e balanceadores de carga clássicos.

Quando um balanceador de carga recebe uma HTTP solicitação, ele verifica se há solicitações malformadas e o tamanho do método. O tamanho total do método em uma HTTP solicitação para um balanceador de carga não deve exceder 127 caracteres. Se a HTTP solicitação passar nas duas verificações, o balanceador de carga enviará a solicitação para a EC2 instância. Se o campo do método na solicitação estiver malformada, o load balancer responderá com um erro HTTP400: BAD _ REQUEST. Se a duração do método na solicitação exceder 127 caracteres, o load balancer responderá com um erro HTTP405: METHOD _ _ NOT ALLOWED.

A EC2 instância processa uma solicitação válida implementando o método na solicitação e enviando uma resposta de volta ao 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

- HTTP400: BAD _ REQUEST
- HTTP405: METHOD _ _ NOT ALLOWED
- HTTP408: Tempo limite da solicitação

- HTTP502: Gateway inválido
- HTTP503: Serviço indisponível
- HTTP504: Tempo limite do gateway

HTTP400: BAD _ REQUEST

Descrição: indica que o cliente enviou uma solicitação incorreta.

Causa 1: O cliente enviou uma solicitação malformada que não atende às HTTP especificações. Por exemplo, uma solicitação não pode ter espaços noURL.

Causa 2: O cliente usou o HTTP CONNECT método, que não é compatível com o Elastic Load Balancing.

Solução: conecte-se diretamente à instância e capture os detalhes da solicitação do cliente. Revise os cabeçalhos e as URL solicitações malformadas. Verifique se a solicitação atende às HTTP especificações. Verifique se não HTTP CONNECT está sendo usado.

HTTP405: 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.

HTTP408: Tempo limite da 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.

HTTP502: Gateway inválido

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 enviada pela instância está em conformidade com as HTTP especificações. Vá para o AWS Support Center para obter assistência.

HTTP503: 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 isso examinando as `HealthyHostCount` métricas em 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 Classic Load Balancer.

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`.

HTTP504: Tempo limite 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 Classic Load Balancer 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: ative as configurações de manutenção de atividade em suas EC2 instâncias e certifique-se de que o tempo limite de manutenção de atividade seja maior do que as configurações de tempo limite de inatividade do seu balanceador de carga.

Solução dos problemas de um Classic Load Balancer: métricas do código de resposta

Seu balanceador de carga envia métricas para a Amazon CloudWatch para os códigos de HTTP resposta enviados aos clientes, identificando a origem dos erros como o balanceador de carga ou as instâncias registradas. Você pode usar as métricas retornadas CloudWatch pelo seu balanceador de carga para solucionar problemas. Para obter mais informações, consulte CloudWatch métricas para seu Classic Load Balancer.

A seguir estão as métricas do código de resposta retornadas CloudWatch pelo 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

- HTTPCode_ ELB _5XX
- HTTPCode_Backend_2xx
- HTTPCode_Backend_3xx
- HTTPCode_Backend_4xx
- HTTPCode_Backend_5xx

HTTPCode_ ELB _4XX

Causa: uma solicitação malformada ou cancelada do cliente.

Soluções

- Consulte HTTP400: BAD _ REQUEST.
- Consulte HTTP405: METHOD _ _ NOT ALLOWED.
- Consulte HTTP408: Tempo limite da solicitação.

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.

Soluções

- Consulte HTTP502: Gateway inválido.
- Consulte HTTP503: Serviço indisponível.
- Consulte HTTP504: Tempo limite do gateway.

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 HTTP solicitação que foi iniciada com um `Transfer-Encoding: chunked` cabeçalho, há um problema conhecido em que o balanceador de carga encaminha a solicitação para a instância, mesmo 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 HTTP solicitação que foi iniciada com um `Transfer-Encoding: chunked` cabeçalho, há um problema conhecido em que o balanceador de carga encaminha a solicitação para a instância, mesmo que o cliente tenha cancelado a solicitação. Isso pode causar erros de back-end.

Solução dos problemas de um Classic Load Balancer: 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 Verificações de saúde das instâncias do seu Classic Load Balancer.

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
- A conexão com as instâncias expirou
- A autenticação de chave pública não está funcionando
- A instância não está recebendo tráfego do load balancer
- As portas da instância não estão abertas
- As instâncias em um grupo de Auto Scaling estão falhando na verificação de integridade ELB

Erro na página de destino da verificação de integridade

Problema: uma HTTP GET solicitação emitida para a instância na porta ping especificada e no caminho do ping (por exemplo, ,:80/index.htmlHTTP) 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 seu balanceador de carga para suas EC2 instâncias atingem o tempo limite ou falham de forma intermitente.

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 TCP conexão:

```
telnet private-IP-address-of-the-instance port
```

Use o comando a seguir para uma HTTPS conexão HTTP or:

```
curl -I private-IP-address-of-the-instance:port/health-check-target-page
```

Se você estiver usando uma HTTPS conexãoHTTP/e obtendo uma resposta diferente de 200, consulteErro na página de destino da verificação de integridade. 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 para verificar se há sobreutilização de. CPU Para obter informações, consulte Obter estatísticas de uma EC2 instância específica no Guia do EC2 usuário da Amazon.
- Verifique a utilização de outros recursos do aplicativo, como memória ou limites, conectando-se às suas EC2 instâncias.
- Se necessário, adicione mais instâncias ou habilite o Auto Scaling. Para obter mais informações, consulte o Guia do usuário do Amazon EC2 Auto Scaling.

Causa 3: Se você estiver usando uma HTTPS conexão HTTP ou e a verificação de integridade estiver sendo executada em uma página de destino especificada no campo do caminho de ping (por

exemplo,`HTTP:80/index.html`), a página de destino pode estar demorando mais 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 balanceador de carga configurado para usar o SSL protocolo HTTPS or com a autenticação de back-end ativada falha na autenticação de chave pública.

Causa: A chave pública no SSL certificado não corresponde à chave pública configurada no balanceador de carga. 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 seja necessário atualizar seu SSL certificado. Se seu SSL certificado estiver atualizado, tente reinstalá-lo em seu balanceador de carga. Para obter mais informações, consulte Substitua o SSL certificado do seu Classic Load Balancer.

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 grupo de segurança do seu balanceador de carga não permite tráfego para as EC2 instâncias.

Solução 2: edite o grupo de segurança do seu balanceador de carga para permitir o tráfego para as sub-redes e as instâncias. EC2

Para obter informações sobre como gerenciar grupo de seguranças, consulte Configurar grupos de segurança para seu Classic Load Balancer.

As portas da instância não estão abertas

Problema: a verificação de integridade enviada à EC2 instância pelo balanceador de carga 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 de Auto Scaling estão falhando na verificação de integridade ELB

Problema: as instâncias do seu grupo de Auto Scaling passam pela verificação de integridade padrão do Auto Scaling, mas não ELB passam na verificação de integridade.

Causa: o Auto Scaling usa verificações de EC2 status para detectar problemas de hardware e software com as instâncias, mas o balanceador de carga realiza verificações de integridade enviando uma solicitação à instância e aguardando um código de resposta 200 ou estabelecendo uma TCP conexão (para uma verificação de integridade TCP baseada) com a instância.

Uma instância pode falhar na verificação de ELB integridade porque um aplicativo em execução na instância tem problemas que fazem com que o balanceador de carga considere a instância fora de serviço. Essa instância pode passar pela verificação de integridade do Auto Scaling; ela não seria substituída pela política do Auto Scaling porque é considerada íntegra com base na EC2 verificação de status.

Solução: use a verificação de ELB integridade do seu grupo de Auto Scaling. Quando você usa a verificação de ELB saúde, o Auto Scaling determina o status de saúde de suas instâncias verificando os resultados da verificação de status da instância e da verificação de ELB saúde. Para obter mais informações, consulte Adicionar verificações de saúde ao seu grupo de Auto Scaling no Guia do usuário do Amazon Auto EC2 Scaling.

Solução dos problemas de um Classic Load Balancer: conectividade do cliente

Os clientes não conseguem se conectar a um balanceador de carga voltado para a Internet

Se o balanceador de carga não estiver respondendo às solicitações, verifique os seguintes problemas possíveis:

Seu balanceador de carga voltado para a Internet está anexado a uma sub-rede privada

É necessário que você especifique sub-redes públicas para o seu balanceador de carga. Uma sub-rede pública tem uma rota para o gateway da Internet para sua nuvem privada virtual (VPC).

Um grupo de segurança ou rede ACL não permite tráfego

O grupo de segurança do balanceador de carga e qualquer rede ACLs das sub-redes do balanceador de carga deve permitir tráfego de entrada dos clientes e tráfego de saída para os clientes nas portas do ouvinte. Para obter mais informações, consulte Configurar grupos de segurança para seu Classic Load Balancer.

As solicitações enviadas para um domínio personalizado não são recebidas pelo balanceador de carga.

Se o balanceador de carga não estiver recebendo solicitações enviadas para um domínio personalizado, verifique os seguintes problemas:

O nome de domínio personalizado não corresponde ao endereço IP do balanceador de carga.

- Confirme para qual endereço IP o nome de domínio personalizado é resolvido usando uma interface da linha de comando.
  - Linux, macOS ou Unix: você pode usar o comando `dig` no Terminal. Ex.`dig example.com`
  - Windows: você pode usar o comando `nslookup` no Prompt de comando. Ex.`nslookup example.com`
- Confirme para qual endereço IP o DNS nome do balanceador de carga é resolvido usando uma interface de linha de comando.
- Compare os resultados das duas saídas. É necessário que os endereços IP sejam correspondentes.

HTTPSsolicitações enviadas para o balanceador de carga retornam "NET:: ERR _ CERT _ _ COMMON NAME _INVALID”

Se as HTTPS solicitações estiverem sendo recebidas `NET::ERR_CERT_COMMON_NAME_INVALID` do balanceador de carga, verifique as seguintes possíveis causas:

- O nome de domínio usado na HTTPS solicitação não corresponde ao nome alternativo especificado no ACM certificado associado aos ouvintes.
- O DNS nome padrão dos balanceadores de carga está sendo usado. O DNS nome padrão não pode ser usado para fazer HTTPS solicitações, pois um certificado público não pode ser solicitado para o `*.amazonaws.com` domínio.

Solução dos problemas de um Classic Load Balancer: 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 os problemas que seu balanceador de carga pode encontrar ao registrar suas EC2 instâncias, as possíveis causas e as etapas que você pode seguir para resolver os problemas.

Problemas

- Demorando muito para registrar uma EC2 instância
- Não é possível registrar uma instância iniciada a partir de uma conta paga AMI

Demorando muito para registrar uma EC2 instância

Problema: as EC2 instâncias registradas estão demorando mais do que o esperado para estarem no `InService` estado.

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.

Não é possível registrar uma instância iniciada a partir de uma conta paga AMI

Problema: o Elastic Load Balancing não está registrando uma instância iniciada usando uma instância paga. AMI

Causa: suas instâncias podem ter sido lançadas usando uma conta paga AMI da Amazon DevPay.

Solução: O Elastic Load Balancing não oferece suporte ao registro de instâncias iniciadas usando pagamentos da AMIs Amazon. DevPay Observe que você pode usar o pago AMIs do AWS Marketplace. Se você já estiver usando um formulário pago AMI AWS Marketplace e não conseguir registrar uma instância iniciada a partir desse formulário pagoAMI, acesse a AWS Support Central para obter ajuda.

Cotas para o seu Classic Load Balancer

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. 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 Serviços da AWS e Elastic Load Balancing. Você também pode usar o comando describe-account-limits(AWS CLI) para o Elastic Load Balancing.

Para solicitar o aumento da quota, consulte Solicitar um aumento de quota no Guia do usuário do Service Quotas.

Sua AWS conta 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 de documentos para Classic Load Balancers

A tabela a seguir descreve todos os lançamentos dos balanceadores de carga clássicos.

Alteração	Descrição	Data
Modo de mitigação de dessincronização	Adicionado suporte para o modo de mitigação de dessincronização. Para obter mais informações, consulte Configurar o modo de mitigação de dessincronização para seu Classic Load Balancer.	17 de agosto de 2020
Balanceadores de carga clássicos	Com a introdução dos balanceadores de carga de aplicativos e balanceadores de carga de rede, os balanceadores de carga criados com o 01/06/2016 agora API são conhecidos como balanceadores de carga clássicos. Para obter mais informações sobre as diferenças entre esses tipos de balanceadores de carga, consulte Recursos do Elastic Load Balancing.	11 de agosto de 2016
Support for AWS Certificate Manager (ACM)	Você pode solicitar um TLS certificadoSSL/ACMe implantá-lo no seu balanceador de carga. Para obter mais informações, consulte SSL// TLScertificates for Classic Load Balancers.	21 de janeiro de 2016

Support para portas adicionais	Os balanceadores de carga podem ouvir em qualquer porta no intervalo de 1 a 65535. Para obter mais informações, consulte Listeners for your Classic Load Balancer.	15 de setembro de 2015
Campos adicionais para entradas do registro de acesso	Adicionados os campos `user_agent` , `ssl_cipher` e `ssl_protocol` . Para obter mais informações, consulte Arquivos de log do Access.	18 de maio de 2015
Support para marcar seu balanceador de carga	A partir desta versão, o Elastic Load Balancing CLI (ELBCLI) foi substituído por AWS Command Line Interface (AWS CLI), uma ferramenta unificada para gerenciar vários AWS serviços. Novos recursos lançados após a ELB CLI versão 1.0.35.0 (datada de 24/07/14) serão incluídos somente na versão. AWS CLI Se você estiver usando o ELBCLI, recomendamos que você comece a AWS CLI usar o. Para obter mais informações, consulte o Guia do usuário do AWS Command Line Interface .	11 de agosto de 2014
Tempo limite de conexão ociosa	Você pode configurar o tempo limite de inatividade para seu load balancer.	24 de julho de 2014

Support para conceder a usuários e grupos acesso a balanceadores de carga ou ações específicas API	Você pode criar uma política para conceder aos usuários e grupos acesso a balanceadores de carga ou API ações específicas.	12 de maio de 2014
Support for AWS CloudTrail	Você pode usar CloudTrail para capturar API chamadas feitas por ou em seu nome Conta da AWS usando o ELB API AWS Management Console, o ELBCLI, o ou AWS CLI o. Para obter mais informações, consulte Registrar API chamadas para seu Classic Load Balancer usando. AWS CloudTrail	4 de abril de 2014
Drenagem da 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 drenagem de conexão para seu Classic Load Balancer.	20 de março de 2014

Logs de acesso	Você pode habilitar seu balanceador de carga para capturar informaçõ es detalhadas sobre as solicitações enviadas ao seu balanceador de carga e armazená-las em um bucket do Amazon S3. Para obter mais informações, consulte Registros de acesso do seu Classic Load Balancer.	6 de março de 2014
Support para TLSv1 1.1-1.2	Foram adicionadas informaçõ es sobre o suporte ao protocolo TLSv1 .1-1.2 para balanceadores de carga configurados comHTTPS/ listeners. SSL Com esse suporte, o Elastic Load Balancing também atualiza as configurações de negociaçã o predefinidasSSL. Para obter informações sobre as configurações de SSL negociação predefinidas atualizadas, consulte configura ções de SSLnegociação para Classic Load Balancers. Para obter informações sobre como atualizar sua configuração de SSL negociação atual, consulte Atualizar a configura ção de SSL negociação do seu Classic Load Balancer.	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 Classic Load Balancer.	6 de novembro de 2013
CloudWatch Métricas adicionais	Adicionadas informações sobre as métricas adicionais do Cloudwatch relatadas pelo Elastic Load Balancing. Para obter mais informações, consulte CloudWatch as métricas do seu Classic Load Balancer.	28 de outubro de 2013
Support para protocolo proxy	Foram adicionadas informações sobre o suporte ao protocolo proxy para balanceadores de carga configurados para SSL conexões TCP /. Para obter mais informações, consulte Cabeçalho do protocolo proxy.	30 de julho de 2013
Support para DNS failover	Foram adicionadas informações sobre a configuração do DNS failover do Amazon Route 53 para balanceadores de carga. Para obter mais informações, consulte Como usar o DNS failover do Amazon Route 53 para seu load balancer.	3 de junho de 2013

Suporte de console para visualização de CloudWatch métricas e criação de alarmes	Foram adicionadas informaçõ es sobre a visualização de CloudWatch métricas e a criação de alarmes para um balanceador de carga específico usando o console. Para obter mais informaçõ es, consulte CloudWatch as métricas do seu Classic Load Balancer.	28 de março de 2013
Support para registrar EC2 instâncias em um padrão VPC	Foi adicionado suporte para EC2 instâncias lançadas em um padrãoVPC.	11 de março de 2013
Balanceadores de carga internos	Com esta versão, um balanceador de carga em uma nuvem privada virtual (VPC) pode ser feito internamente ou voltado para a Internet. Um balanceador de carga interno tem um DNS nome que pode ser resolvido publicamente e é resolvido em endereços IP privados. Um balanceador de carga voltado para a Internet tem um DNS nome que pode ser resolvido publicamente e é resolvido em endereços IP públicos. Para obter mais informações, consulte Criar um Classic Load Balancer interno.	10 de junho de 2012

Suporte de console para gerenciar ouvintes, configurações de criptografia e certificados SSL	Para obter informações, consulte Configurar um HTTPS ouvinte para seu Classic Load Balancer e substituir SSL o certificado para seu Classic Load Balancer.	18 de maio de 2012
Support para Elastic Load Balancing na Amazon VPC	Foi adicionado suporte para criar um balanceador de carga em uma nuvem privada virtual (VPC).	21 de novembro de 2011
Amazon CloudWatch	Você pode monitorar seu balanceador de carga usando o. CloudWatch Para obter mais informações, consulte CloudWatch as métricas do seu Classic Load Balancer.	17 de outubro de 2011
Recursos adicionais de segurança	Você pode configurar SSL cifras, back-end e autenticação de servidor back-endSSL. Para obter mais informações, consulte Criar um Classic Load Balancer com um HTTPS ouvinte.	30 de agosto de 2011
Nome de domínio apex da zona	Para obter mais informações, consulte Configurar um nome de domínio personalizado para seu Classic Load Balancer.	24 de maio de 2011

Support 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 HTTPcabeçalhos e balanceadores de carga clássicos.	27 de outubro de 2010
Support for HTTPS	Com essa versão, você pode aproveitar o TLS protocolo SSL/para criptografar o tráfego e transferir o SSL processamento da instância do aplicativo para o balanceador de carga. Esse recurso também fornece gerenciamento centralizado de certificados de SSL servidor no balanceador de carga, em vez de gerenciar certificados em instâncias individuais do aplicativo.	14 de outubro de 2010
Support for AWS Identity and Access Management (IAM)	Foi adicionado suporte paraIAM.	2 de setembro de 2010

Sessões persistentes	Para obter mais informações, consulte Configurar sessões fixas para seu Classic Load Balancer.	7 de abril de 2010
AWS SDK for Java	Foi adicionado suporte para o SDK para Java.	22 de março de 2010
AWS SDK for .NET	Foi adicionado suporte para AWS SDK for .NET o.	11 de novembro de 2009
Novo serviço	Lançamento beta público inicial do Elastic Load Balancing.	18 de maio de 2009

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.