Elastic Load Balancing FAQs - Amazon Web Services

aws.amazon.com (https://aws.amazon.com/elasticloadbalancing/faqs/)

General

Q: How do I decide which load balancer to select for my application?

A: Elastic Load Balancing supports three types of load balancers. You can select the appropriate load balancer based on your application needs. If you need to load balance HTTP requests, we recommend you to use Application Load Balancer. For network/transport protocols (layer4 – TCP, UDP) load balancing, and for extreme performance/low latency applications we recommend using Network Load Balancer. If your application is built within the EC2 Classic network then you should use Classic Load Balancer.

Q: Can I privately access Elastic Load Balancing APIs from my Amazon Virtual Private Cloud (VPC) without using public IPs?

A: Yes, you can privately access Elastic Load Balancing APIs from your Amazon Virtual Private Cloud (VPC) by creating VPC endpoints (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html). With VPC endpoints, the routing between the VPC and Elastic Load Balancing APIs is handled by the AWS network without the need for an Internet gateway, NAT gateway, or VPN connection. The latest generation of VPC Endpoints used by Elastic Load Balancing are powered by AWS PrivateLink, an AWS technology enabling the private connectivity between AWS services using Elastic Network Interfaces (ENI) with private IPs in your VPCs. To learn more about AWS PrivateLink (http://aws.amazon.com/privatelink), visit the AWS PrivateLink documentation (http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html#what-is-privatelink).

Q: Is there an SLA for load balancers?

A: Yes, Elastic Load Balancing guarantees a monthly availability of at least 99.99% for your load balancers (Classic, Application or Network). To learn more about the SLA and know if you are qualified for a credit, visit https://aws.amazon.com/elasticloadbalancing/sla/. (https://aws.amazon.com/elasticloadbalancing/sla/)

Application Load Balancer

Q: Which operating systems does an Application Load Balancer support?

A: An Application Load Balancer supports targets with any operating system currently supported by the Amazon EC2 service.

Q: Which protocols does an Application Load Balancer support?

A: An Application Load Balancer supports load balancing of applications using HTTP and HTTPS (Secure HTTP) protocols.

Q: Is HTTP/2 Supported on an Application Load Balancer?

A: Yes. HTTP/2 support is enabled natively on an Application Load Balancer. Clients that support HTTP/2 can connect to an Application Load Balancer over TLS.

Q: What TCP ports can I use to load balance?

A: You can perform load balancing for the following TCP ports: 1-65535

Q: Is WebSockets supported on an Application Load Balancer?

A: Yes. WebSockets and Secure WebSockets support is available natively and ready for use on an Application Load Balancer.

Q: Is Request tracing supported on an Application Load Balancer?

A: Yes. Request tracing is enabled by default on your Application Load Balancer.

Q: Does a Classic Load Balancer have the same features and benefits as an Application Load Balancer?

A: While there is some overlap, there is no feature parity between the two types of load balancers. Application Load Balancers are the foundation of our application layer load-balancing platform for the future.

Q: Can I configure my Amazon EC2 instances to accept traffic only from my Application Load Balancers?

A: Yes.

Q: Can I configure a security group for the front-end of an Application Load Balancer?

A: Yes.

Q: Can I use the existing APIs that I use with my Classic Load Balancer with an Application Load Balancer?

A: No. Application Load Balancers require a new set of APIs.

Q: How do I manage both Application and Classic Load Balancers simultaneously?

A: The ELB Console will allow you to manage Application and Classic Load Balancers from the same interface. If

you are using the CLI or an SDK, you will use a different ‘service’ for Application Load Balancers. For example, in the CLI you will describe your Classic Load Balancers using `aws elb describe-load-balancers` and your Application Load Balancers using `aws elbv2 describe-load-balancers`.

Q: Can I convert my Classic Load Balancer to an Application Load Balancer (and vice versa)?

A: No, you cannot convert one load balancer type into another.

Q: Can I migrate to Application Load Balancer from Classic Load Balancer?

A: Yes. You can migrate to Application Load Balancer from Classic Load Balancer using one of the options listed in this document (https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/migrate-to-application-load-balancer.html).

Q: Can I use an Application Load Balancer as a Layer-4 load balancer?

A: No. If you need Layer-4 features, you should use Network Load Balancer.

Q: Can I use a single Application Load Balancer for handling HTTP and HTTPS requests?

A: Yes, you can add listeners for HTTP port 80 and HTTPS port 443 to a single Application Load Balancer.

Q: Can I get a history of Application Load Balancing API calls made on my account for security analysis and operational troubleshooting purposes?

A: Yes. To receive a history of Application Load Balancing API calls made on your account, use AWS CloudTrail (https://aws.amazon.com/cloudtrail/).

Q: Does an Application Load Balancer support HTTPS termination?

A: Yes, you can terminate HTTPS connection on the Application Load Balancer. You must install an SSL certificate on your load balancer. The load balancer uses this certificate to terminate the connection and then decrypt requests from clients before sending them to targets.

Q: What are the steps to get a SSL certificate?

A: You can either use AWS Certificate Manager (https://aws.amazon.com/certificate-manager/) to provision an SSL/TLS certificate or you can obtain the certificate from other sources by creating the certificate request, getting the certificate request signed by a CA, and then uploading the certificate either using AWS Certification Manager or the AWS Identity and Access Management (https://aws.amazon.com/iam/) (IAM) service.

Q: How does an Application Load Balancer integrate with AWS Certificate Manager (ACM)?

A: An Application Load Balancer is integrated with AWS Certificate Management (ACM). Integration with ACM makes it very simple to bind a certificate to the load balancer thereby making the entire SSL offload process very easy. Purchasing, uploading, and renewing SSL/TLS certificates is a time-consuming manual and complex process. With ACM integration with Application Load Balancer, this whole process has been shortened to simply requesting a trusted SSL/TLS certificate and selecting the ACM certificate to provision it with the load balancer.

Q: Is back-end server authentication supported with an Application Load Balancer?

A: No, only encryption is supported to the back-ends with an Application Load Balancer.

Q: How can I enable Server Name Indication (SNI) for my Application Load Balancer?

A: SNI is automatically enabled when you associate more than one TLS certificate with the same secure listener on a load balancer. Similarly, SNI mode for a secure listener is automatically disabled when you have only one certificate associated to a secure listener.

Q: Can I associate multiple certificates for the same domain to a secure listener?

A: Yes, you can associate multiple certificates for the same domain to a secure listener. For example, you can associate:

ECDSA and RSA certificates

Certificates with different key sizes (e.g. 2K and 4K) for SSL/TLS certificates

Single-Domain, Multi-Domain (SAN) and Wildcard certificates

Q: Is IPv6 supported with an Application Load Balancer?

A: Yes, IPv6 is supported with an Application Load Balancer.

Q: How do you set up rules on an Application Load Balancer?

A: You can configure rules for each of the listeners that you have on the load balancer. The rules include conditions and corresponding actions if the conditions are satisfied. The supported conditions are Host header, path, HTTP headers, methods, query parameters, and source IP CIDRs. The supported actions are redirect, fixed response, authenticate, and forward. Once you have set this up, the load balancer will use the rules to determine how a particular HTTP request should be routed. You can use multiple conditions and actions in a rule and in each condition can specify a match on multiple values.

Q: Are there limits on the resources for an Application Load Balancer?

A: Your AWS account has these limits (http://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-

balancer-limits.html) for an Application Load Balancer.

Q. How can I protect my web applications behind a load balancer from web attacks?

A: You can integrate your Application Load Balancer with AWS WAF, a web application firewall that helps protect web applications from attacks by allowing you to configure rules based on IP addresses, HTTP headers, and custom URI strings. Using these rules, AWS WAF can block, allow, or monitor (count) web requests for your web application. Please see AWS WAF developer guide (http://docs.aws.amazon.com/console/waf) for more information.

Q: Can I load balance to any arbitrary IP address?

A: You can use any IP address from the load balancer's VPC CIDR for targets within load balancer's VPC and any IP address from RFC 1918 ranges (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) or RFC 6598 range (100.64.0.0/10) for targets located outside the load balancer's VPC (for example, targets in Peered VPC, EC2-Classic and on-premises locations reachable over AWS Direct Connect or VPN connection).

Q: How can I load balance applications distributed across a VPC and on-premises location?

A: There are various ways to achieve hybrid load balancing. If an application runs on targets distributed between a VPC and an on-premises location, you can add them to the same target group using their IP addresses. To migrate to AWS without impacting your application, gradually add VPC targets to the target group and remove on-premises targets from the target group. If you have two different applications such that the targets for one application are in a VPC and the targets for other applications are in on-premises location, you can put the VPC targets in one target group and the on-premises targets in another target group and use content based routing to route traffic to each target group. You can also use separate load balancers for VPC and on-premises targets and use DNS weighting to achieve weighted load balancing between VPC and on-premises targets.

Q: How can I load balance to EC2-Classic instances?

A: You cannot load balance to EC2-Classic Instances when registering their Instance IDs as targets. However if you link these EC2-Classic instances to the load balancer's VPC using ClassicLink and use the private IPs of these EC2-Classic instances as targets, then you can load balance to the EC2-Classic instances. If you are using EC2 Classic instances today with a Classic Load Balancer, you can easily migrate to an Application Load Balancer.

Q: How do I enable cross-zone load balancing in Application Load Balancer?

A: Cross-zone load balancing is already enabled by default in Application Load Balancer.

Q: When should I authenticate users using the Application Load Balancer's integration with Amazon Cognito vs. the Application Load Balancers' native support for OpenID Connect (IODC) identity providers (IdPs)?

A: You should use authentication through Amazon Cognito if:

- You want to provide flexibility to your users to authenticate via social network identities (Google, Facebook, and Amazon) or enterprise identities (SAML) or via your own user directories provided by Amazon Cognito's User Pool.
- You are managing multiple identity providers including OpenID Connect and want to create a single authentication rule in Application Load Balancer (ALB), that can use Amazon Cognito to federate your multiple identity providers.
- You have a need to actively manage user profiles with one or more social or OpenID Connect identity providers from one central place. For example, you can put users in groups and add custom attributes to represent user status and control access for paid users.

Alternatively, if you have invested in developing custom IdP solutions and simply want to authenticate with a single identity provider that is OpenID Connect-compatible, you may prefer using Application Load Balancer's native OIDC solution.

Q: What type of redirects does Application Load Balancer support ?

A: The following three types of redirects are supported.

Types of redirects Examples HTTP to HTTP http://hostA to http://hostB HTTP to HTTPS

http://hostA to https://hostB
https://hostA:portA/pathA to https://hostB:portB/pathB

HTTPS to HTTPS https://hostA to https://hostB

Q: What content types does ALB support for the message body of fixed-response action?

A: The following content types are supported: text/plain, text/css, text/html, application/javascript, application/json.

Q: How does Lambda invocation via Application Load Balancer work?

A: HTTP(S) requests received by a load balancer are processed by the content-based routing rules. If the request content matches the rule with an action to forward it to a target group with a Lambda function as a target then the corresponding Lambda function is invoked. The content of the request (including headers and body) is passed on to the Lambda function in JSON format. The response from the Lambda function should be in JSON format. The response from the Lambda function is transformed into an HTTP response and sent to the client. The load balancer invokes your Lambda function using the AWS Lambda Invoke API and requires that you have provided invoke permissions for your Lambda function to Elastic Load Balancing service.

Q: Does Lambda invocation via Application Load Balancer support requests over both HTTP and HTTPS protocol?

A: Yes. Application Load Balancer supports Lambda invocation for requests over both HTTP and HTTPS protocol.

Q: In which AWS Regions can I use Lambda functions as targets with the Application Load Balancer?

A: You can use Lambda as a target with the Application Load Balancer in US East (N. Virginia), US East (Ohio), US West (Northern California), US West (Oregon), Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Canada (Central), EU (Frankfurt), EU (Ireland), EU (London), EU (Paris), South America (São Paulo), and GovCloud (US-West) AWS Regions.

Application Load Balancer Pricing FAQs

Q: How does Application Load Balancer pricing work?

A: You are charged for each hour or partial hour that an Application Load Balancer is running and the number of Load Balancer Capacity Units (LCU) used per hour.

Q: What is a Load Balancer Capacity Unit (LCU)?

A: An LCU is a new metric for determining how you pay for an Application Load Balancer. An LCU defines the maximum resource consumed in any one of the dimensions (new connections, active connections, bandwidth and rule evaluations) the Application Load Balancer processes your traffic.

Q: Will I be billed on Classic Load Balancers by LCU?

A: No, Classic Load Balancers will continue to be billed for bandwidth and hourly usage.

Q: How do I know the number of LCUs an Application Load Balancer is using?

A: We expose the usage of all four dimensions that constitute an LCU via CloudWatch.

Q: Will I be billed on all the dimensions in an LCU?

A: No. The number of LCUs per hour will be determined based on maximum resource consumed amongst the four dimensions that constitutes a LCU.

Q: Will I be billed on partial LCUs?

A: Yes.

Q: Is a free tier offered on an Application Load Balancer for new AWS accounts?

A: Yes. For new AWS accounts, a free tier for an Application Load Balancer offers 750 hours and 15 LCUs. This free tier offer is only available to new AWS customers, and is available for 12 months following your AWS sign-up date

Q: Can I use a combination of Application Load Balancer and Classic Load Balancer as part of my free tier?

A: Yes. You can use both Classic and Application Load Balancers for 15GB and 15 LCUs respectively. The 750 load balancer hours are shared between both Classic and Application Load Balancers.

Q: What are rule evaluations?

A: Rule evaluations are defined as the product of number of rules processed and the request rate averaged over an hour.

Q: How does the LCU billing work with different certificate types and key sizes?

A: Certificate key size affects only the number of new connections per second in the LCU computation for billing. The following table lists the value of this dimension for different key sizes for RSA and ECDSA certificates.

RSA certificates Key Size <=2K <=4K <=8K >8K New connections/sec 25 5 1 0.25
ECDSA Certificates Key Size <=256 <=384 <=521 >521 New connections/sec 25 5 1 0.25

Q: Am I charged for regional AWS data-transfer for cross-zone load balancing in Application Load Balancer?

A: No. Since cross-zone load balancing is always on with Application Load Balancer, you are not charged for this type of regional data transfer.

Q: Is user authentication in Application Load Balancer charged separately?

A: No. There is no separate charge for enabling the authentication functionality in Application Load Balancer. When using Amazon Cognito with Application Load Balancer, Amazon Cognito pricing will apply.

Q: How do you charge for Application Load Balancer usage with Lambda targets?

A: You are charged as usual for each hour or partial hour that an Application Load Balancer is running and the number of Load Balancer Capacity Units (LCU) used per hour. For Lambda targets, each LCU offers 0.4 GB processed bytes per hour, 25 new connections per second, 3,000 active connections per minute and 1000 rule evaluations per second. For the processed bytes dimension, each LCU provides 0.4 GB per hour for Lambda targets versus 1GB per hour for all other target types like EC2 instances, containers and IP addresses. Please note that usual AWS Lambda charges apply to Lambda invocations by Application Load Balancer.

Q: How can I know the bytes processed by Lambda targets versus bytes processed by other targets (EC2, containers, and on-premises servers)?

A: Applications Load Balancers emit two new CloudWatch metrics. LambdaTargetProcessedBytes metric indicates the bytes processed by Lambda targets and the StandardProcessedBytes metric indicates bytes processed by all other target types.

Network Load Balancer

Q: Can I create a TCP or UDP (Layer 4) listener for my Network Load Balancer?

A: Yes. Network Load Balancers support both TCP, UDP, and TCP+UDP (Layer 4) listeners, as well as TLS listeners.

Q: What are the key features available with the Network Load Balancer?

A: Network Load Balancer provides both TCP and UDP (Layer 4) load balancing. It is architected to handle millions of requests/sec, sudden volatile traffic patterns and provides extremely low latencies. In addition Network Load Balancer also supports TLS termination, preserves the source IP of the clients, and provides stable IP support and Zonal isolation. It also supports long-running connections that are very useful for WebSocket type applications.

Q: Can Network Load Balancer process both TCP and UDP protocol traffic on the same port?

A: Yes. To achieve this, you can use a TCP+UDP listener. For example, for a DNS services using both TCP and UDP you can create a TCP+UDP listener on port 53, and the load balancer will process traffic for both UDP and TCP requests on that port. You must associate a TCP+UDP listener with a TCP+UDP target group.

Q: How does Network Load Balancer compare to what I get with the TCP listener on a Classic Load Balancer?

A: Network Load Balancer preserves the source IP of the client which in the Classic Load Balancer is not preserved. Customers can use proxy protocol with Classic Load Balancer to get the source IP. Network Load Balancer automatically provides a static IP per Availability Zone to the load balancer and also enables assigning an Elastic IP to the load balancer per Availability Zone. This is not supported with Classic Load Balancer.

Q: Can I migrate to Network Load Balancer from Classic Load Balancer?

A: Yes. You can migrate to Network Load Balancer from Classic Load Balancer using one of the options listed in this document.

Q: Are there limits on the resources for my Network Load Balancer?

A: Yes, please refer to Network Load Balancer limits documentation for more information.

Q: Can I use the AWS Management Console to set up my Network Load Balancer?

A: Yes, you can use the AWS Management Console, AWS CLI, or the API to set up a Network Load Balancer.

Q: Can I use the existing API for Classic Load Balancers for my Network Load Balancers?

A: No. To create a Classic Load Balancer, use the 2012-06-01 API. To create a Network Load Balancer or an Application Load Balancer, use the 2015-12-01 API.

Q: Can I create my Network Load Balancer in a single Availability Zone?

A: Yes, you can create your Network Load Balancer in a single availability zone by providing a single subnet when you create the load balancer.

Q: Does Network Load Balancer support DNS regional and zonal fail-over?

A: Yes, you can use Amazon Route 53 health checking and DNS failover features to enhance the availability of the applications running behind Network Load Balancers. Using Route 53 DNS failover, you can run applications in multiple AWS Availability zones and designate alternate load balancers for failover across regions. In the event that you have your Network Load Balancer configured for multi-AZ, if there are no healthy EC2 instances registered with the load balancer for that Availability Zone or if the load balancer nodes in a given zone are unhealthy, then R-53 will fail away to alternate load balancer nodes in other healthy availability zones.

Q: Can I have a Network Load Balancer with a mix of ELB-provided IPs and Elastic IPs or assigned private IPs?

A: No. A Network Load Balancer’s addresses must be completely controlled by you, or completely controlled by ELB. This is to ensure that when using Elastic IPs with a Network Load Balancer, all addresses known to your clients do not change.

Q: Can I assign more than one EIP to my Network Load Balancer in each subnet?

A: No. For each associated subnet that a Network Load Balancer is in, the Network Load Balancer can only support a single public/internet facing IP address.

Q: If I remove/delete a Network Load Balancer what will happen to the Elastic IP addresses that were associated with it?

A: The Elastic IP Addresses that were associated with your load balancer will be returned to your allocated pool and made available for future use.

Q: Does Network Load Balancer support internal load balancers?

A: Network Load Balancer can be set-up as an internet-facing load balancer or an internal load balancer similar to what is possible with Application Load Balancer and Classic Load Balancer.

Q: Can the internal Network Load balancer support more than one private IP in each subnet?

A: No. For each associated subnet that a load balancer is in, the Network Load Balancer can only support a single private IP.

Q: Can I set up Websockets with my Network Load Balancer?

A: Yes, configure TCP listeners that route the traffic to the targets that implement WebSockets protocol (https://tools.ietf.org/html/rfc6455). Because WebSockets is a layer 7 protocol and Network Load Balancer is operating at layer 4, no special handling exists in Network Load Balancer for WebSockets or other higher level protocols.

Q: Can I load balance to any arbitrary IP address?

A: Yes. You can use any IP address from the load balancer's VPC CIDR for targets within load balancer's VPC and any IP address from RFC 1918 ranges (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) or RFC 6598 range (100.64.0.0/10) for targets located outside the load balancer's VPC (EC2-Classic and on-premises locations reachable over AWS Direct Connect). Load balancing to IP address target type is supported for TCP listeners only, and is currently not supported for UDP listeners.

Q: Can I use Network Load Balancer to setup PrivateLink?

A: Yes, Network Load Balancers with TCP and TLS Listeners can be used to setup PrivateLink. You cannot setup PrivateLink with UDP listeners on Network Load Balancers.

Q: What is a UDP flow?

A: While UDP is connectionless, the load balancer maintains UDP flow state based on 5-tuple hash, making sure that packets sent in the same context are consistently forwarded to the same target. The flow is considered active as long as traffic is flowing and until the idle timeout is reached. Once the timeout threshold is reached, the load balancer will forget the affinity, and incoming UDP packet will be considered as a new flow and load-balanced to a new target.

Q: What is the idle timeout supported by Network Load Balancer?

A: Network Load Balancer idle timeout for TCP connections is 350 seconds. The idle timeout for UDP flows is 120 seconds.

Q: What benefit will I get by targeting containers behind a load balancer with IP addresses instead of instance IDs?

A: Each container on an instance can now have its own security group and does not need to share security rules with other containers. You can attach security groups to an ENI and each ENI on an instance can have a different security group. You can map a container to the IP address of a particular ENI to associate security group(s) per container. Load balancing using IP addresses also allows multiple containers running on an instance use the same port (say port 80). The ability to use the same port across containers allows containers on an instance to communicate with each other through well-known ports instead of random ports.

Q: How can I load balance applications distributed across a VPC and on-premises location?

A: There are various ways to achieve hybrid load balancing. If an application runs on targets distributed between a

VPC and an on-premises location, you can add them to the same target group using their IP addresses. To migrate to AWS without impacting your application, gradually add VPC targets to the target group and remove on-premises targets from the target group. You can also use separate load balancers for VPC and on-premises targets and use DNS weighting to achieve weighted load balancing between VPC and on-premises targets.

Q: How can I load balance to EC2-Classic instances?

A: You cannot load balance to EC2-Classic Instances when registering their Instance IDs as targets. However if you link these EC2-Classic instances to the load balancer's VPC using ClassicLink and use the private IPs of these EC2-Classic instances as targets, then you can load balance to the EC2-Classic instances. If you are using EC2 Classic instances today with a Classic Load Balancer, you can easily migrate to a Network Load Balancer.

Q: How do I enable cross-zone load balancing in Network Load Balancer?

A: You can enable cross-zone loading balancing only after creating your Network Load Balancer. You achieve this by editing the load balancing attributes section and then by selecting the cross-zone load balancing support checkbox.

Q: Am I charged for regional AWS data-transfer when I enable cross-zone load balancing in Network Load Balancer?

A: Yes, you will be charged for regional data transfer between Availability Zones with Network Load Balancer when cross-zone load balancing is enabled. Check the charges in the data-transfer section at Amazon EC2 On-Demand Pricing page.

Q: Is there any impact of cross-zone load balancing on Network Load Balancer limits?

A: Yes. Network Load Balancer currently supports 200 targets per Availability Zone. For example, if you are in 2 Availability-Zones, you can have up to 400 targets registered with Network Load Balancer. If cross-zone load balancing is on, then the maximum targets reduces from 200 per Availability Zone to 200 per load balancer. So, in the example above when cross-zone load balancing is on, even though your load balancer is in 2 Availability Zones, you are limited to 200 targets that can be registered to the load balancer.

Q: Does Network Load Balancer support TLS termination?

A: Yes, you can terminate TLS connections on the Network Load Balancer. You must install an SSL certificate on your load balancer. The load balancer uses this certificate to terminate the connection and then decrypt requests from clients before sending them to targets.

Q: Is source IP is preserved when terminating TLS on Network Load Balancer?

A: Source IP continues to be preserved even if you terminate TLS on the Network Load Balancer.

Q: What are the steps to get a SSL certificate?

A: You can either use AWS Certificate Manager (https://aws.amazon.com/certificate-manager/) to provision an SSL/TLS certificate or you can obtain the certificate from other sources by creating the certificate request, getting the certificate request signed by a CA, and then uploading the certificate either using AWS Certification Manager (ACM) or the AWS Identity and Access Management (https://aws.amazon.com/iam/) (IAM) service.

Q: How can I enable Server Name Indication (SNI) for my Network Load Balancer?

A: SNI is automatically enabled when you associate more than one TLS certificate with the same secure listener on a load balancer. Similarly, SNI mode for a secure listener is automatically disabled when you have only one certificate associated to a secure listener.

Q: How does the Network Load Balancer integrate with AWS Certificate Manager (ACM) or Identity Access Manager (IAM)?

A: Network Load Balancer is integrated with AWS Certificate Management (ACM). Integration with ACM makes it very simple to bind a certificate to the load balancer thereby making the entire SSL offload process very easy. Purchasing, uploading, and renewing SSL/TLS certificates is a time-consuming manual and complex process. With ACM integration with Network Load Balancer, this whole process has been shortened to simply requesting a trusted SSL/TLS certificate and selecting the ACM certificate to provision it with the load balancer. Once you create a Network Load balancer, you can now configure a TLS listener and then you have an option to select a certificate from either ACM or Identity Access Manager (IAM). This experience is similar to what you have in Application Load Balancer or Classic Load Balancer.

Q: Is back-end server authentication supported with Network Load Balancer?

A: No, only encryption is supported to the back-ends with Network Load Balancer.

Q: What are the certificate types supported by Network Load Balancer?

A: Network Load Balancer only supports RSA certificates with 2K key size. We currently do not support RSA certificate key sizes greater than 2K or ECDSA certificates on the Network Load Balancer.

Q: In which AWS Regions is TLS Termination on Network Load Balancer supported?

A: You can use TLS Termination on Network Load Balancer in US East (N. Virginia), US East (Ohio), US West (Northern California), US West (Oregon), Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Canada (Central), EU (Frankfurt), EU (Ireland), EU (London), EU (Paris), South America (São Paulo), and GovCloud (US-West) AWS Regions.

Network Load Balancer Pricing FAQs

Q: How does Network Load Balancer pricing work?

A: You are charged for each hour or partial hour that a Network Load Balancer is running and the number of Load Balancer Capacity Units (LCU) used by Network Load Balancer per hour.

Q: What is a Load Balancer Capacity Unit (LCU)?

A: An LCU is a new metric for determining how you pay for a Network Load Balancer. An LCU defines the maximum resource consumed in any one of the dimensions (new connections/flows, active connections/flows, and bandwidth) the Network Load Balancer processes your traffic.

Q: What is the LCU metrics for TCP traffic on Network Load Balancer?

A: The LCU metrics for the TCP traffic is as follows:

- 800 new TCP connections per second.
- 100,000 active TCP connections (sampled per minute).
- 1 GB per hour for EC2 instances, containers and IP addresses as targets.

Q: What is the LCU metrics for UDP traffic on Network Load Balancer?

A: The LCU metrics for the UDP traffic is as follows:

- 400 new flows per second.
- 50,000 active UDP flows (sampled per minute).
- 1 GB per hour for EC2 instances, containers and IP addresses as targets.

Q: What is the LCU metrics for TLS traffic on Network Load Balancer?

A: The LCU metrics for the TLS traffic is as follows:

- 50 new TLS connections per second.
- 3,000 active TLS connections (sampled per minute).
- 1 GB per hour for EC2 instances, containers and IP addresses as targets.

Q: Will I be billed on all the dimensions (Processed Bytes, New Flows and Active Flows)?
A: No, for each protocol you are charged only on one of the three dimensions (the highest for the hour).

Q: Is new connections/flows per sec same as requests/sec?

A: No. Multiple requests can be sent in a single connection.

Q: Will I be billed on Classic Load Balancers by LCU?

A: No. Classic Load Balancers will continue to be billed for bandwidth and hourly charge.

Q: How do I know the number of LCUs a Network Load Balancer is using?

A: We will expose the usage of all three dimensions that constitutes a LCU via Amazon CloudWatch.

Q: Will I be billed on all the dimensions in an LCU?

A: No. The number of LCUs per hour will be determined based on maximum resource consumed amongst the three dimensions that constitutes a LCU.

Q: Will I be billed on partial LCUs?

A: Yes.

Q: Is a free tier offered on a Network Load Balancer for new AWS accounts?

A: Yes. For new AWS accounts, a free tier for a Network Load Balancer offers 750 hours and 15 LCUs. This free tier offer is only available to new AWS customers, and is available for 12 months following your AWS sign-up date.

Q: Can I use a combination of Network Load Balancer, Application Load Balancer and Classic Load Balancer as part of my free tier?

A: Yes. You can use Application and Network each for 15 LCUs and Classic for 15 GB respectively. The 750 load balancer hours are shared between Application, Network and Classic Load Balancers.

Classic Load Balancer

Q: Which operating systems does the Classic Load Balancer support?

A: The Classic Load Balancer supports Amazon EC2 instances with any operating system currently supported by the Amazon EC2 service.

Q: Which protocols does the Classic Load Balancer support?

A: The Classic Load Balancer supports load balancing of applications using HTTP, HTTPS (Secure HTTP), SSL (Secure TCP) and TCP protocols.

Q: What TCP ports can I load balance?

A: You can perform load balancing for the following TCP ports:

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

Q: Does the Classic Load Balancer support IPv6 traffic?

A: Yes. Each Classic Load Balancer has an associated IPv4, IPv6, and dualstack (both IPv4 and IPv6) DNS name. IPv6 is not supported in VPC. You can use an Application Load Balancer for native IPv6 support in VPC.

Q: Can I configure my Amazon EC2 instances to only accept traffic from Classic Load Balancers?

A: Yes.

Q: Can I configure a security group for the front-end of Classic Load Balancers?

A: If you are using Amazon Virtual Private Cloud, you can configure security groups for the front-end of your Classic Load Balancers.

Q: Can I use a single Classic Load Balancer for handling HTTP and HTTPS requests?

A: Yes, you can map HTTP port 80 and HTTPS port 443 to a single Classic Load Balancer.

Q: How many connections will my load balanced Amazon EC2 instances need to accept from each Classic Load Balancer?

A: Classic Load Balancers do not cap the number of connections that they can attempt to establish with your load balanced Amazon EC2 instances. You can expect this number to scale with the number of concurrent HTTP, HTTPS, or SSL requests or the number of concurrent TCP connections that the Classic load balancers receive.

Q: Can I load balance Amazon EC2 instances launched using a Paid AMI?

A: You can load balance Amazon EC2 instances launched using a paid AMI from AWS Marketplace (https://aws.amazon.com/marketplace). However, Classic Load Balancers do not support instances launched using a paid AMI from Amazon DevPay (http://aws.amazon.com/devpay/) site.

Q: Can I use Classic Load Balancers in Amazon Virtual Private Cloud?

A: Yes. See the Elastic Load Balancing web page.

Q: Can I get a history of Classic Load Balancer API calls made on my account for security analysis and operational troubleshooting purposes?

A: Yes. To receive a history of Classic Load Balancer API calls made on your account, simply turn on CloudTrail in the AWS Management Console.

Q: Do Classic Load Balancers support SSL termination?

A: Yes you can terminate SSL on Classic Load Balancers. You must install an SSL certificate on each load balancer. The load balancers use this certificate to terminate the connection and then decrypt requests from clients before sending them to the back-end instances.

Q: What are the steps to get a SSL certificate?

A: You can either use AWS Certificate Manager (https://aws.amazon.com/certificate-manager/) to provision a SSL/TLS certificate or you can obtain the certificate from other sources by creating the certificate request, getting the certificate request signed by a CA, and then uploading the certificate using the AWS Identity and Access Management (IAM) service.

Q: How do Classic Load Balancers integrate with AWS Certificate Manager (ACM)?

A: Classic Load Balancers are now integrated with AWS Certificate Management (ACM). Integration with ACM makes it very simple to bind a certificate to each load balancer thereby making the entire SSL offload process very easy. Typically purchasing, uploading, and renewing SSL/TLS certificates is a time-consuming manual and complex process. With ACM integrated with Classic Load Balancers, this whole process has been shortened to simply requesting a trusted SSL/TLS certificate and selecting the ACM certificate to provision it with each load balancer.

Q: How do I enable cross-zone load balancing in Classic Load Balancer?

A: You can enable cross-zone load balacing using the console, the AWS CLI, or an AWS SDK. See Cross-Zone Load Balancing documentation (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-disable-crosszone-lb.html#enable-cross-zone) for more details.

Q: Am I charged for regional AWS data-transfer when I enable cross-zone load balancing in Classic Load Balancer?

A: No, you are not charged for regional data transfer between Availability Zones when you enable cross-zone load balancing for your Classic Load Balancer.

Learn more about Elastic Load Balancing pricing

Visit the pricing page

Learn more

Sign up for a free account

Instantly get access to the AWS Free Tier.

Sign up (https://portal.aws.amazon.com/gp/aws/developer/registration/index.html)

Start building in the console

Get started with Elastic Load Balancing in the AWS Console.

Sign in (https://console.aws.amazon.com/ec2/v2/home)

Register for re:Invent Bootcamps

Learn from AWS experts at exam prep bootcamps - space is limited!

(https://reinvent.awsevents.com/learn/bootcamps/?sc_icampaign=aware_reinvent_bootcamps2019_aws&sc_ichannel=ha&sc_icontent=awssm-2448&sc_iplace=2up&trk=ha_awssm-2448)

Get AWS Certified

AWS Certifications can help you advance your career and boost your earning power

(https://pages.awscloud.com/tc_get-aws-certified.html?sc_icampaign=aware_getcertified_evergreen2019&sc_ichannel=ha&sc_icontent=awssm-2655&sc_iplace=2up&trk=ha_awssm-2655)

AWS re:Invent | December 2 – 6, 2019 | Las Vegas, Nevada

Reserved seating opens October 15th. Register now to save your spot. View session catalog ≫

AWS re:Invent

(https://reinvent.awsevents.com/learn/?sc_icampaign=Event_reInvent_2019_1up_DG5_VIP&sc_ichannel=ha&sc_icontent=awssm-3019-a&sc_ioutcome=Strategic_Events&sc_iplace=1up&trk=ha_a131L0000058G7nQAE~ha_awssm-3019~ha_awssm-3019-a&trkCampaign=AWS_reInvent_2019)

Page Content

General Application Load Balancer Network Load Balancer Classic Load Balancer

aws.amazon.com (https://aws.amazon.com/elasticloadbalancing/faqs/)