Automated Safeguards for Application Load Balancer (ALB)

Amazon Web Services Application Load Balancers automatically balance HTTP and HTTPS traffic from client to server, allowing you to easily distribute load across multiple servers and Availability Zones, as well as build fault tolerate web applications. Application Load Balancers (ALB) also provide advanced routing and traffic management designed to support modern application architecture. Customers can use ALBs to process sessions that contain Protected Health Information (PHI) provided all session connectivity is transmitted over an encrypted connection.

Application Load Balancers are priced based on each hour or partial hour that an Application Load Balancer is running and the number of Load Balancer Capacity Units (LCU) used per hour.

LCU Details

An LCU measures the dimensions on which the Application Load Balancer processes your traffic (averaged over an hour). The four dimensions measured are:

- New connections: Number of newly established connections per second. Typically, many requests are sent per connection.
- Active connections: Number of active connections per minute.
- Bandwidth: The amount of traffic processed by the load balancer in Mbps
- Rule evaluations: It is the product of number of rules processed by your load balancer and the request rate. The first 10 processed rules are free (Rule evaluations = Request rate * (Number of rules processed - 10 free rules)

You are charged only on the dimension with the highest usage. An LCU contains:

- 25 new connections per second.
- 3,000 active connections per minute.
- 2.22 Mbps (which translates to 1 GB per hour)
- 1,000 rule evaluations per second

Further details about ALB pricing and LCU can be found at https://aws.amazon.com/elasticloadbalancing/pricing/
Amazon ALB offers a large suite of features that are purpose built for modern application architectures, including microservices and container-based applications. ALBs support Layer 7 load balancing, Web Application Firewall integration, content based routing, access logging, high availability across physical locations, health checks, and many more features. ClearDATA recommends visiting https://aws.amazon.com/elasticloadbalancing/features/#Details_for_Elastic_Load_Balancing_Products for up to date features and architecture guidance.

Compliance Guidance

ClearDATA's Automated Safeguard for ALB ensures that all all of the compliance requirements are met for all newly created ALBs. ClearDATA reviews newly created load balancers to ensure the endpoints are all using HTTPS, the Target Groups are all using HTTPS communication, and the appropriate TLS version is selected. If these settings are not properly configured, the load balancer will be deleted shortly after creation. ClearDATA will also automate the enforcement of audit logging after an ALB is created, since audit logging enablement during creation is only available via API/CLI.

Encrypted Connections

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption addressable standard strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (ePHI). ClearDATA's interpretation of this regulation is that all connections from both the client to the ALB and the ALB to the Target Group must use an HTTPS connection, ensuring the data transmitted from client to and from the web services is encrypted. If a Target Group is provisioned which is not configured for HTTPS, the Automated Safeguard will remove the Target Group. The ALB will remain online and a new Target Group can be configured.

Remediation

If the target group does not use encrypted connections, it will be removed from the ALB configuration. If the ALB listener does not use encrypted connections, the listener is removed from the ALB.

Automated Safeguards for Security Groups

ClearDATA's Automated Safeguards for ALB pairs with the Automated Safeguards for Security Groups, ensuring that Security Groups used by ALBs are approved for use. For more information on how to use Automated Safeguards for Security Groups please click here.

TLS Version

The United States Health and Human Services (HHS) publishes guidance for appropriate encryption protocols, ensuring that the version of the protocol used meets appropriate standards. According to HHS Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52 Rev 1. ClearDATA considers TLS v1.1 and above as appropriate controls. ALBs use Security Policies to assign a TLS version. The following Security Policies are approved for use:

- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-1-2017-01

Remediation

If a listener is created without one of the policies listed above, the Automated Safeguard will remove the listener. The ALB will remain online and a new listener can be configured.

Audit Logging

HIPAA Technical Safeguard 45 CFR § 164.312(b) requires a Covered Entity to “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred. ClearDATA recommends our customers utilize access logging in the application load balancer that will record the activity requests.

Remediation

Access Logging is enabled after the ALB is provisioned, so as a result ClearDATA will create a compliant S3 bucket and configure the ALB to send Access Logs to that bucket.

Shared Responsibility

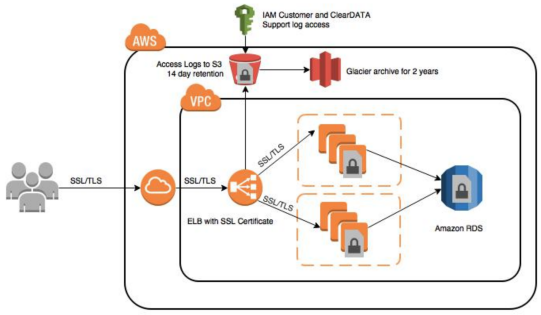
ClearDATA ensures that all all of the compliance requirements are met for all newly created ALBs. ClearDATA reviews newly created load balancers to ensure the endpoints are all using HTTPS, the Target Groups are all using HTTPS communication, and the appropriate TLS version is selected. If these settings are not properly configured, the load balancer will be deleted shortly after creation. ClearDATA will also automate the enforcement of audit logging after an ALB is created, since audit logging enablement during creation is only available via API/CLI.

Customers are responsible for ensuring the SSL/TLS Certificates used on the ALB and the Target Group instances meet the TLS versions listed above.

Please contact your ClearDATA team for a copy of the full Responsibilities Matrix.

Exclusion

Disabling automated remediation is at the load balancer level. Please contact ClearDATA Support to request that an exclusion be placed to allow for the load balancer to be created.



Users can be added to the DPHI-ALB IAM group in order to access the ALB service

Item	ClearDATA	Customer
Enforcement of Automated Safeguards	RA	IC
Procurement/Renewal of SSL/TLS Certificates	IC	RA