elb®
LEARNING

Lectora®
ReviewLink®

Security Program Overview

Table of Contents

Intended Audience:

This document was created by ELB Learning for potential and existing Lectora Online customers. The information it contains explains the way in which Lectora Online handles customer data, along with the overall technical architecture of the platform. The document addresses topics related to the Lectora Online architecture and the provision of Lectora Online cloud services. The intended audience for this document is: stakeholders from Risk Management, IT Engineering, Project Officers, Senior Consultants or Project Sponsors.

1.0 Architecture Overview

Software Architecture

The Lectora Online application is a collaborative eLearning authoring tool which is accessible via a modern internet browser. Accounts are provisioned by ELB Learning and administered by the organization administrators.

The ReviewLink application is an eLearning review tool accessible via modern internet browsers.

Languages: HTML5, Java, JavaScript

Application Architecture: J2EE, JSP, Servlets, Filters, Listeners, etc.

Third Party Software: Apache JackRabbit, jQuery, DHTML Goodies, CKEditor

Releases:

Currently we are doing quarterly minor feature releases, yearly major feature releases, monthly maintenance releases. If a major issue is found we will fix the issue in our maintenance build and do a run through QA. Depending on the severity, priority and proximity of the next maintenance release we decide how the fix would be deployed. We keep a branch with a sterile production environment in case our maintenance environment has too many fixes that have not yet been QA'd. End result we can deploy major fixes as quickly as we get them through an adequate QA cycle.

Operating System and Application Tiers

Hosted servers run on CentOS 6.10.

The application can run on Linux or Windows Server.

MySQL 5.7+
Java 8+
Tomcat 9+
Apache 2+
Modern Web Browser Client

Deployment Modes

The Lectora Online application is available in different deployment models:

1. Multi-tenant Hosted - customers share an ELB Learning Hosted server where their data is logically separated.
2. Dedicated Server Hosted - ELB Learning hosts a server for a single customer, data is physically separated.
3. Enterprise - customer self-hosts on their own server.

This document focuses primarily on the first deployment model. In special cases the documentation may refer to other deployment modes.

ReviewLink architecture is similar to Lectora Online and is currently only available in the Multi-tenant Hosted deployment model.

Web Interface

Lectora Online requires a modern web browser that supports JavaScript and does not require any third party plugins. It currently supports the following browsers:

- Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari 10 or above

These browsers are supported on the following operating systems:

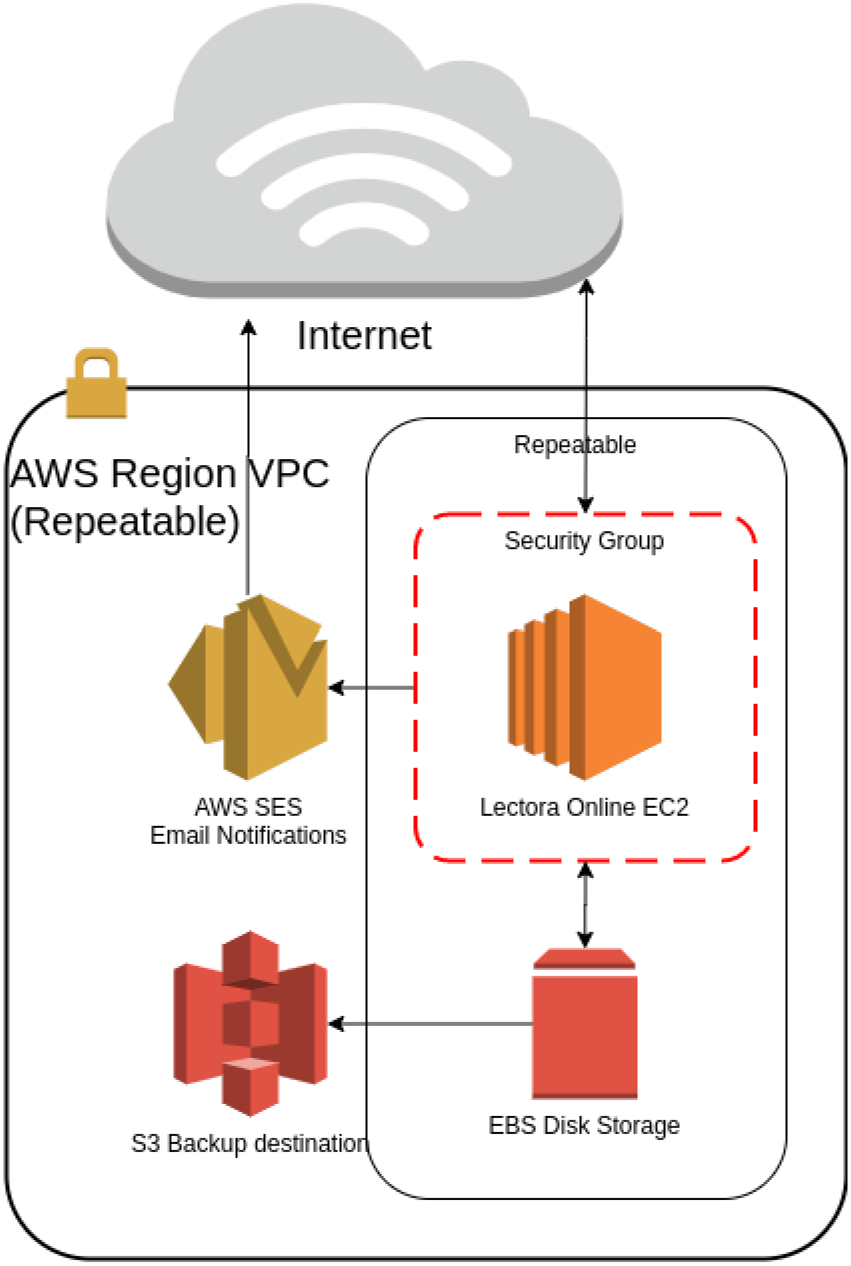
- Microsoft Windows 7 and above
- OSX

In all instances, ELB Learning strongly recommends that clients maintain updated operating systems aligned to the latest release made available by the respective vendors.

1.1 Platform Architecture

The Lectora Online architecture is stable, all pieces are reproducible at a moment's notice. The diagram below describes this architecture in greater detail.

Architecture Diagram:



Application servers are available in multiple regions of the world US-east-1 (Northern Virginia), US-west-2 (Oregon), EU-west-1 (Ireland), EU-west-2 (London), AP-southeast-2 (Sydney). Instances can be started in any of the availability zones in the region for fault tolerance. New code deployments are managed by an automated process of uploading a new application artifact and restarting services across the fleet, this happens during low traffic periods with minimal interruption to services.

The database is used to store users, settings, and user generated content. All user generated content is stored inside the database that resides on EBS, a resilient disk store with backups.

1.2 Content Delivery

Seeing as dedicated instances are the most widely used architecture, each Lectora Online instance delivers content directly. This gives the greatest control of business segregation.

1.3 Email Notifications

Lectora Online helps authors know when action is required without constant checking. When email is configured appropriately, authors are notified of actions required within the interface. Should an issue arise while sending a notification Lectora Online will automatically route the error to the administrators of the site for further remediation.

2.0 Scalability and Disaster Recovery

Scaling happens in a more classical sense for Lectora Online with vertical alteration being the primary driving force. With the power of AWS hosting, systems have a very large potential to scale to needs as they arise. Metrics and monitoring allow us to have great insight into how systems are functioning, and what actions may need to be taken.

Should something happen to the server, all configurations are captured and backed up. This allows rapid rebuild capabilities. Combined with internal and external third party monitoring allows for quick response times to incidents affecting system and performance.

3.0 Backup Policies

3.1 Database Backup Policies

An entire database backup is performed daily. Daily data is retained on a 30 day rotating cycle.

3.2 Disk Backup Policies

EC2 EBS disks have a snapshot taken every 24 hours. These snapshots are stored in the S3 service with tremendous data resiliency. Snapshots are kept for 30 days before being rotated out. These snapshots contain all necessary information to rebuild any piece of the environment.

3.3 User Retention Policies

Lectora Online:

All data is maintained within the application.

The only thing retained are customer accounts with their courses. These are retained in backups and via automation are cleaned up at specific intervals.

- For trial accounts we delete everything 90 days after expiration
- For non-trials we delete everything 1 year after expiration
- Expired accounts that have never been logged into are removed immediately, like the accounts created for LUC that were never used.
- Incremental title backups are saved for 1 month, the last incremental (a backup of current revision of the title) will be kept until deleted according to the above rules.
- When a title is deleted any incremental backups are removed and a backup of the last revision of the title is kept for 1 year.

ReviewLink:

All data is maintained within the application.

The only thing retained are customer accounts with their courses. These are retained in backups and via automation are cleaned up at specific intervals.

- For trial accounts we delete everything 90 days after expiration
- For non-trials we delete everything 1 year after expiration

3.4 User Generated Content

User generated Content is stored within the MySQL database on the EC2 EBS storage technology. This is then backed up via snapshots nightly which are replicated into AWS S3. The structure of S3 storage automatically keeps multiple copies of the same object in different Amazon servers for business continuity purposes and in order to ensure 99.999999999% data durability.

Lectora Online also does a daily backup of individual assets that changed that day (customer courses, media, etc). This data is also stored in AWS S3 and allows for quicker recovery of individual assets. Recovery can be done via the application by super administrators or manually by system administrators with access to AWS S3.

4.0 Disaster Recovery and Business continuity

4.1 Business continuity

Lectora Online leverages the fault tolerant configuration of AWS, we can rebuild instances in another availability zone in the unlikely event of failure in any availability zone. Each availability zone is designed as an independent failure zone. Recovery from an availability zone failure is quickened by third party monitoring solutions.

4.2 Disaster Recovery

In the case of a major disaster, recreation of the Lectora Online service will be done in another availability zone, or region. In general, this can be done in a matter of hours using images and backup data held in Amazon S3.

These processes are tested periodically to ensure no bugs should a recovery scenario arise.

5.0 Password Restriction Policies

Both Lectora Online and Review Link handle authentication credentials securely within their respective databases. Lectora Online allows additional customizations for dedicated server deployments:

- IP Whitelisting
- Password Policy
  - number of failed login attempts allowed before locking a user account
  - number of minutes an account is locked for after too many failed login attempts
  - minimum length required for a password
  - minimum number of numbers required for a password
  - minimum number of UPPER case letters required for a password
  - minimum number of lower case letters required for a password
  - minimum number of special characters (!@#$%^&*+-...) required for a password
  - do not allow password to contain username, first, or last name
  - do not allow consecutive characters in a password
  - common password blacklist
  - number of days a user can keep the same password (future)
  - minimum time between password changes (future)
- SAML Single Sign On

- Identity Provider Integration

6.0 Content Encryption

Content encryption over the network between the client and Lectora Online servers is achieved through the use of HTTPS. All connections to the server are forced to be via HTTPS.

7.0 Vulnerability Detection

The Lectora Online servers are scanned monthly using Tenable.io Vulnerability Management, the most accurate and comprehensive vulnerability assessment solution in the market. The Tenable.io VM software scans for more than 45,000 Common Vulnerabilities and Exposures (CVE), with new plugins released weekly, or within 24 hours of a vulnerability disclosure.

AntiVirus scanning

Lectora Online performs weekly scans of servers for virus signatures using the ClamAV scanning software.

Third Party Vulnerability Scanning

We also make use of Trustwave vulnerability scanning as an extra check on internal processes.

8.0 Monitoring

For Lectora Online and ReviewLink monitoring we do keep OS access logs, Apache Web Server access logs, Tomcat Application server logs and MySQL logs as well as an application audit log and Amazon access logs. We have two monitor applications which check that our hosted servers are alive and an Amazon based CPU usage alert set on each server. We feel this is sufficient for identifying and investigating the majority of issues that can happen to Lectora Online.

Application access, operational, and error logging are done through the Java Logging API and are written to the server instance disk. These logs are kept as long as the server instance is around, which is approximately 1 year between major releases. Log files can be accessed via the application by super administrators and via SFTP by system administrators.

The application also writes specific administrative operations into an audit log that can be inspected by system administrators. This is written to the database and is backed up with the application. This audit log is kept for several years. This log is viewable by system administrators within the application.

9.0 Audits and Certifications

As ELB Learning understands that security and reliability are critical elements in the choice of a Cloud-based software solution, it maintains high security standards and, in line with such standards, carefully selects its providers by partnering with those organizations that not only prove the highest industry ratings in their specific services but also ensure the highest level of reliability and security.

Amazon Web Services (AWS), the world's leader in Cloud and CDN provisioning for software vendors, is continuously audited, with certifications from accreditation bodies across geographies and verticals, including ISO 27001, FedRAMP, DoD CSM, and PCI DSS. The following link provides extensive information and data related to risk management and risk prevention associated due diligence:

https://aws.amazon.com/security/
http://aws.amazon.com/compliance/