SLI – Shared Learning Infrastructure

Strand #4 UAT & Production Environment Specification

November 16, 2012

Copyright © 2012 Shared Learning Collaborative, LLC (SLC). All Rights Reserved.

This document and the information contained herein is provided on an "AS IS" basis and SLC DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

**Revisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| Draft v1.3 | 03/05/12 |  | Draft Released to SLC |
| V0.1 | 09/27/12 | Tony Requist | Initial version of final  Added names for review |
| V0.2 | 10/18/12 | Various | Version for final review |
| v1.0 | 10/24/12 | Various***Various2uistCastructurent Specification*** | Version for submission to SLC |
| V1.0.65 | 11/15/2012 | Tony Requist | Clarify historical data |

## 

1 Purpose and Key Notes 3

2 Scope 3

3 Audience 6

4 Production Environment Specification 7

4.1 Introduction 7

4.1.1 Architecture 8

4.1.2 Data Center 10

4.2 Configuration Manager 10

4.2.1 Hardware 10

4.2.2 Internet Connectivity & Bandwidth 16

4.3 Security Infrastructure Software 16

4.3.1 Controlled Auditable Access: 17

4.3.2 Security Event Manager: 18

4.3.3 Two-Factor Authentication: 18

4.3.4 Web Application Firewalls (WAF): 19

4.3.5 Vulnerability Management: 19

4.3.6 Non-Data Infrastructure SLI Software 21

4.3.7 Data Reliability – at rest 21

4.3.8 Data Security – at rest 21

4.4 Passphrase Security 22

4.4.1 Network Security 22

4.4.2 Staffing 23

4.4.3 Company Security Policy 23

4.4.4 Procedures 23

4.4.5 Support 23

4.4.6 Operations Management 24

4.4.7 System Monitoring and Alerting 24

4.4.8 Vendor Support Capabilities 24

4.4.9 Service Level Agreements 25

4.4.10 Hardware Points of Failure 25

4.4.11 Acceptance Testing 26

5 Summary 26

# Purpose and Key Notes

This document provides an overview of the components necessary to stand up UAT and Production Environments that are used by the SLC to provision and operate the Shared Learning Infrastructure (“SLI”).

The Data Infrastructure is the component of the SLI supplied by Wireless Generation as part of Work Order #1 and the corresponding Master Services Agreement. This document describes the environmental requirements of the 1.0 Release of the Data Infrastructure. This document also includes many of the steps the SLC needs to take to ensure that the Data Infrastructure software runs in a secure environment.

It is the responsibility of the SLC to independently ensure that both the Data Infrastructure software provided by Wireless Generation, as well as the entire SLI system, are provisioned and operated in a secure manner. This includes operating in a secure environment and operating in accordance with this document and the Data Privacy and Security Plan.

As laid out in Strand #4, this document describes the following aspects of the production environment, as well as many other aspects of the environment that are required for the production environment to perform and run securely:

* Data Center(s)
* Internet Connectivity & Bandwidth
* Hardware and off-the-shelf software
* Networking equipment
* Network security and intrusion detection equipment

Another purpose of this document is to provide guidance to the SLC on the cost of [some] third party software required for the Production Environment. After receiving bids and quotes from most of the software companies referenced herein, as well as many others, Wireless Generation believes that the third party software license costs for the Production Environment will be $500,000-$1,000,000. *This number is merely an estimate* because these quotes were obtained for hypothetical systems and the actual infrastructure and sizing that the SLC chooses has not yet been determined.

# Scope

A summary of the environments for the Data Infrastructure is provided in Table 1. This document will focus on the requirements of the Production Environment.

|  |  |
| --- | --- |
| **Environment** | **Description** |
| Development | Software engineers and architects require tools and temporary environments for personal and small-team prototyping and testing. These environments vary in scale and completeness depending on need. These environments are hosted on AWS (Amazon Web Services) and are the subject of Strand #3, previously delivered to the SLC. |
| Continuous Integration | As software changes are committed, automated tools build and test the software and report errors to the development team. These environments are hosted on AWS and are the subject of Strand #3, previously delivered to the SLC. |
| Test | QA team members manage a copy of the production environment that is used to perform automated and manual testing of the entire system. This environment must duplicate the functionality and topology of production; however, it may not have the same capacity. This environment is expected to be hosted on AWS. The “Test” environment is not the subject of this document. |
| Staging | A Staging Environment supports User Acceptance Testing. Upon successful completion of the UAT event, the Staging Environment can be placed into service as the Production Environment. This procedure can be repeated, as necessary, to create new Production Environments - with the stipulation that data that must be migrated will have to be moved into the Staging Environment as one of the last steps of “Go-live”. The Staging Environment will be provisioned and operated by the SLC Operator. |
| Sandbox | The Sandbox Environment allows LEAs and SEAs (and software developers they are working with) to test their software in a safe environment. The Sandbox Environment(s) are not specified in this document. |
| Production | Users of the SLI log in and use the Production Environment to ingest student data, store it in the data store, and access it through a set of dashboards and applications. This environment hosts PII and, therefore, must be completely secure. The security constraint exists unchanged for Alpha, Release 1.0 and Releases 1.x. |

**Table 1: Environment Summary**

# Audience

As specified in Exhibit E of Work Order #1, these specifications are being provided to the SLC in order for the SLC to procure, set up, and the configure hardware, hosting services, networking components, and commercial off the shelf software described herein.

This document is also meant to be used by the SLC in order to provision and operate the Shared Learning Infrastructure (“SLI”). Because the provisioning and operation of UAT and Production environments are a different and separate task from most SLC activities, these duties are separated and identified as belonging to the operator (“Operator”) throughout this document. Whether that Operator is the SLC itself or a third party vendor is for the SLC to decide.

# Production Environment Specification

## Introduction

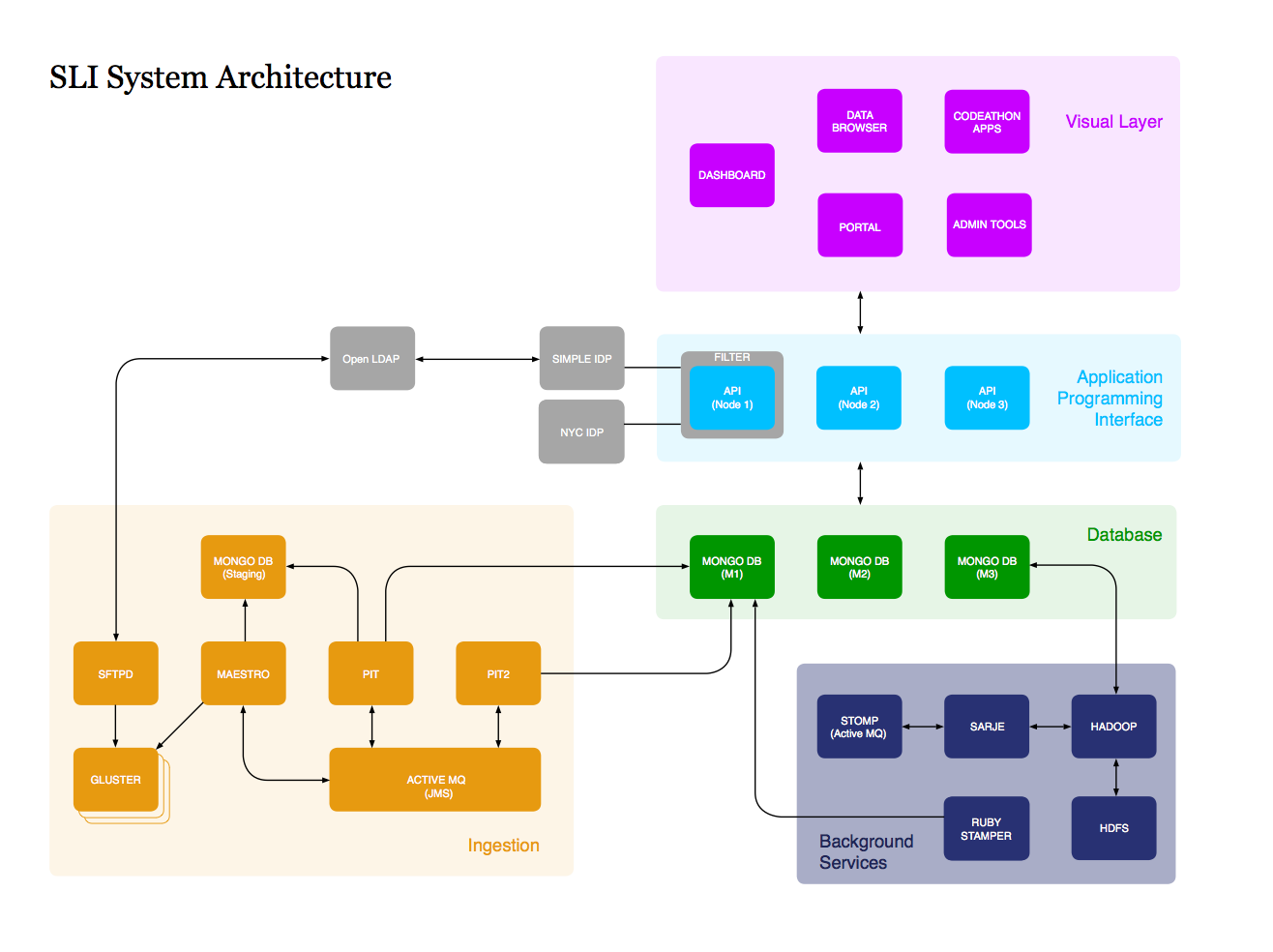
In order to define the requirements of an environment, it is best to start with a list of the characteristics of a successful deployment on that environment:

* Processes and procedures documented and formalized for all aspects of the system, including but not limited to:
  + User additions and deletions
  + Security incidents
  + Hardware failure incidents
  + Software failure incidents
  + Network failure incidents
  + Backup
  + Disaster recovery
  + Patch management for infrastructure components
  + Release management (including rollback) for major software components
* A method and protocol for users to interact with the operator for support
* An escalation procedure for all suppliers of the system (hardware or software) to be used when faults occur - either detected by users and reported to the help desk or found by operations.
* A security infrastructure that addresses external and internal (e.g. rogue operator, etc.) threats.
* Ability to accept/refuse logins and data access from authorized or unauthorized users, and to log all such attempts, whether successful or not.
* Secure storage of system operation credentials.
* Security alerting related to defined privileged operations.
* Facilitates 24/7 security monitoring.
* Can be reproduced on another environment for troubleshooting and analysis.
* Has a tiered log system so that system audit logs, network/IP logs, and application logs are separated and can be configured at differing levels.
* Isolates PII into only a contained set of logs, which are housed in a part of the system that follows the same security requirements as the ingestion or datastore elements that contain PII.
* Can scale up or down with little or no disruption to uptime or availability.
* All software can be updated transparently (whether SLI, SLC, third Party, O/S, or device drivers) without required system downtime.
* Can withstand agreed-upon points of failure, up to a certain point, with no noticeable loss of usability to the end user. Beyond those points of failure, system degrades gracefully with a clear and understood reduction in capacity, speed or functionality for each one. System has a clear set of criteria for when any component has degraded or failed beyond usability and alerts system operators.

In order for the SLI production environment to have the above characteristics, many different requirements need to be addressed. Each of these requirements is discussed in detail below.

### Architecture

The overall architecture of the system (as designed in the AWS cloud) is shown below. Note that whether or not the system is deployed in AWS or in a bare-metal data-center, the same basic elements need to exist.



### Data Center

The data center comprises the physical hardware and network connections that house the SLC system.

The SLC has expressed a desire to deploy the SLI on a cloud infrastructure using virtualized environments hosted by Amazon Web Services (AWS). This is possible when used with a diligent application of the security measures spelled out on the following pages. It should be noted that most of these procedures are considered “best practices” in a bare-metal private or hosted data center as well and the SLC should use these measures if it decides to not host the SLI on Amazon Web Services.

Though this document focuses solely on deploying on Amazon Web Services, there is only a small amount of Amazon-specifc customization in this document. The requirements presented here are very similar no matter what data center type is chosen.

For an overview of Amazon security processes, see http://aws.amazon.com/articles/1697?\_encoding=UTF8&jiveRedirect=1.

## Configuration Manager

The ability for a repeatable and manageable roll-out of a system is part of maintaining a secure system. To that end, a configuration manager such as Puppet, Chef, or cfengine is recommended.

### Hardware

For Release 1.0 of the Data Infrastructure from Wireless Generation, it is anticipated that approximately 90 AWS instances of various sizes will be needed, along with Load Balancers and layers of Amazon-compatible security software and measures, which are necessary to protect PII data at all times. For more information on the different types of instances Amazon offers, see <http://aws.amazon.com/ec2/instance-types/>.

The number of hosts is an estimate based on what Wireless Generation sees as the initial deployment for 5 million students and 4 years of data (the current year plus 3 years of historical data). The number of hosts is likely to change based on adoption timeline and actual load characteristics. The runbook will reflect changes based on post R1.0 development and based on refinements to the model for system load. The runbook will cover system architecture for different numbers of students and years of historical data and will discuss what metrics will indicate the need for additional hardware.

A note about this configuration: It is standard practice to avoid system failures by having a minimum of two instances of any critical service. One instance of any service is clearly unacceptable, as any single failure brings down the entire production environment. A second instance provides a stand-by. Having three instances provides additional safety and is often used in production environments; whether this is worth the cost is the SLC’s decision.

These systems can be broken down as follows:

* Portal Layer
  + Minimum Requirements:
    - Utilize Amazon Elastic Load Balancer
    - 2 Tomcat web servers running the LifeRay product
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
    - 2 MySQL Database servers - used as the backing store for the running LifeRay configuration
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: EBS
  + Requirements for 5M students  
    It is anticipated that 5M students will require 3 Tomcat servers.
  + Estimated requirements for each additional 1M students  
    It is anticipated that an additional Tomcat server will be required for each additional 2M-3M students.
* Dashboard Layer  
  Scaling the dashboard layer is accomplished by scaling the Tomcat web servers.
  + Minimum Requirements:
    - Utilize Amazon Elastic Load Balancer
    - 2 Tomcat web servers  
      These run the Data Infrastructure software for the Dashboard
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
  + Requirements for 5M students  
    It is anticipated that 5M students will require 3 Tomcat servers.
  + Estimated requirements for each additional 1M students  
    It is anticipated that an additional Tomcat server will be required for each additional 2M-3M students.
* Data Browser Layer  
  Scaling the Data Browser layer is accomplished by scaling Rails Web Servers. It is anticipated that these servers will be sufficient for 5M students.
  + Minimum Requirements:
    - Utilize Amazon Elastic Load Balancer
    - 2 Ruby on Rails web servers  
      These run the Data Infrastructure software for the Dashboard
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
* Admin Layer  
  Scaling the Admin layer is accomplished by scaling Rails Web Servers. It is anticipated that these servers will be sufficient for 5M students.
  + Minimum Requirements:
    - Utilize Amazon Elastic Load Balancer
    - 2 Ruby on Rails web servers  
      These run the Data Infrastructure software for the Dashboard
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
* API Layer
  + Minimum Requirements:
    - Utilize Amazon Elastic Load Balancer
    - 2 Tomcat web servers  
      These run the Data Infrastructure software for the API servers
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
  + Requirements for 5M students  
    It is estimated that 5 million students will require 7 Tomcat web servers
  + Estimated requirements for each additional 1M students  
    It is anticipated that an additional 1-2 Tomcat servers will be required for each additional 1M students. The Datastore layer will need to be scaled as well, as described below.
* Datastore Layer  
  The Datastore Layer serves both ingestion and API.
  + Minimum Requirements:
    - 3 MongoDB Servers in a replica set (one shard)  
      This means that there is one master server and two replicated backups.
      * Recommended AWS Instance Class: High-Memory Quadruple Extra Large (m2.4xlarge) 68.4GB
      * Recommended storage: RAID10 EBS with PrIOPS
    - 3 MongoDB configuration servers  
      MongoDB specifies using exactly 3 config servers
      * Recommended AWS Instance Class: Medium (m1.medium)  
        This recommendation is from 10gen
      * Recommended storage: EBS
  + The Datastore layer is scaled by adding replica sets (shards) where each replica set consists of 3 MongoDB servers as described above
  + Requirements for 5M students  
    It is estimated that 5M students will require 23 MongoDB replica sets (shards), for a total of 69 MongoDB servers (assuming each replica set consists of three instances)
  + Estimated requirements for each additional 1M students  
    It is anticipated that an additional 4-5 shards will be required for each additional 1M students.
* IDP (Identity Provider)  
  It is anticipated that these servers will be sufficient for 5M students.
  + Minimum Requirements:
    - Utilize Amazon Elastic Load Balancer
    - 2 Simple IDP Servers
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
    - 2 OpenLDAP Servers
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: EBS
* Ingestion
  + Minimum Requirements:
    - 2 Landing Zone Servers  
      One active, one stand-by. These servers run ProFTPD.
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
    - 2 GlusterFS Servers  
      These are the severs that physically store the uploaded files to be ingested. Note that for scaling these servers change to high I/O instances to stream the large files to the ingestion servers.
      * Recommended AWS Instance Class: Large (m1.large)
    - 2 ActiveMQ Servers  
      One active, one stand-by
      * Recommended AWS Instance Class: Large (m1.large) 7.5GB
      * Recommended storage: ephemeral
    - DeltaHash DB Servers - 3 MongoDB Servers in a replica set (1 shard)  
      Each shard is one master and two replicated backups.
      * Recommended AWS Instance Class: High-Memory Quadruple Extra Large (m2.4xlarge) 68.4GB
      * Recommended storage: EBS
    - 3 MongoDB configuration servers (for DeltaHash DB)  
      MongoDB specifies using exactly 3 config servers
      * Recommended AWS Instance Class: Medium (m1.medium)  
        This recommendation is from 10gen
      * Recommended storage: ephemeral
    - Staging Database Servers - 3 MongoDB Servers  
      One master and two replicated backups.
      * Recommended AWS Instance Class: High-Memory Quadruple Extra Large (m2.4xlarge) 68.4GB
      * Recommended storage: EBS
    - 3 MongoDB configuration servers (for Staging DB)  
      MongoDB specifies using exactly 3 config servers
      * Recommended AWS Instance Class: Medium (m1.medium)  
        This recommendation is from 10gen
      * Recommended storage: ephemeral
    - 2 Maestro servers  
      Two servers both for redundancy and scaling
      * Recommended AWS Instance Class: High-Memory Quadruple Extra Large (m2.4xlarge) 68.4GB
      * Recommended storage: ephemeral
    - 2 Pit servers  
      Two servers both for redundancy and scaling
      * Recommended AWS Instance Class: High-Memory Quadruple Extra Large (m2.4xlarge) 68.4GB
      * Recommended storage: ephemeral
  + Requirements for 5M students  
    Based on the SLI Ingestion Load Estimates spreadsheet, it is estimated that 5M students will require:
    - Gluster servers: 2 High I/O Quadruple Extra Large (hi1.4xlarge) instances
    - 3 DeltaHash DB shards (9 servers, assuming each replica set consists of three instances)
    - 5 Maestro servers
    - 2 Pit servers

Note: the staging database does not need to scale larger, and may be deprecated in the future.

Note: the distinction between Mastro and Pit servers will go away in the future.

* + Estimated requirements for each additional 1M students  
    It is anticipated that an additional 0.5 DeltaHash shards and 1 Maestro server will be required for each additional 1M students.

It is recommended to use Reserved Instances in order to minimize the cost of operating this infrastructure and maximize security. Reserved Instances are allocated for longer periods of time and are much more economical in exchange for the time commitment.

### Internet Connectivity & Bandwidth

Amazon provides bandwidth at a very low cost per month per GB/TB and up to petabytes. This bandwidth is simple to provision. For more information, see http://aws.amazon.com/ec2/pricing/.

It is recommended that the Operator utilize Amazon’s VPC (Virtual Private Cloud) technology in conjunction with Amazon Elastic IP’s in order to create a secure hosting cloud environment. Note: there are limitations with using Amazon VPC’s. In particular, Amazon restricts the number of Elastic (Public) IP addresses per VPC to 5 by default. However, Amazon can be engaged to increase this limit if the need should arise. Wireless Generation does not anticipate that the production environment would need more than 5 Elastic (Public) IP addresses. For more information on Amazon’s Private Cloud offering, see http://aws.amazon.com/vpc/.

## Security Infrastructure Software

In order for the Operational Software to run the systems, a secure environment must be defined, procured, installed, configured and tested.

It is recommended that all access to servers in Amazon VPC are controlled through AWS Security Groups in conjunction with local firewall rules: iptables for Linux, and Windows Firewall for Microsoft Windows. It is an absolute requirement for security that at least one of these methods be used, but preferably both.

The following is a list of components and the corresponding security goal that each provides necessary in order to ensure a secure infrastructure.

**Because the SLI in general and the Data Infrastructure in particular, will host student data for millions of students, it is critical to employ appropriate resources to withstand sophisticated cyber-attacks. For this reason, it is imperative that a defense-in-depth security philosophy be put in place. This is so that if a single layer of security is breached, there are additional security controls in place that need to be subverted for PII to be compromised. These recommendations are the most important part of this document and the most important part of the SLI Production Environment.**

### Controlled Auditable Access:

Goals:

* Access to the systems should only be allowed if there is a means of capturing what was done and by whom.
* Access to servers should be restricted, by firewall rules, and/or network ACLs, to a very small list of hosts in order to minimize attack vectors.

Recommended course of action:

OS level auditing which tracks direct OS user interaction and changes to settings and important files (including but not limited to system and software configuration files) should be implemented through **sudo** and **auditd** respectively. Both are Linux native utilities and are included with RHEL 6. Sudo and auditd logs should in this case never contain PII. Use of any Linux distribution other than RHEL 6 has not been vetted by Wireless Generation for security or applicability to running the Data Infrastructure software.

Firewall/Network ACLs that restrict access to the servers to a small list of hosts should be configured with software that provides a means of capturing the entire session’s actions. Software such as Centrify should be configured and leveraged to do this.

Recommended software: **Centrify Suite 2012 Enterprise Edition**

Centrify Suite EEcan capture an entire session’s output for replay later and provides a means of centralizing access controls on a per-user basis. Systems using Centrify should be placed within the firewalls of any organization which is accessing the AWS system. For example, this would include Wireless Generation and the SLC Operator. Each organization that accesses the system should have duplicate boxes running the Centrify software to avoid single points of failure.

### Security Event Manager:

Goals:

* A means of continuously analyzing logs generated by various systems in real-time that can then be used to send alerts based on security criteria; such as a privileged user logging into a system from some place other than the group of servers that are sanctioned to do so.
* Datastore and logs for such a system must be encrypted to protect potential PII data.
* Provides an easy way for applications and systems to export their logs in real-time.

Recommended course of action:

All servers, applications and services should be configured to log events to a centralized logging facility that has a means of analyzing and alerting based on various security criteria.

Recommended software:

It is very complex to tailor an SEM to a specific environment, and this environment will depend on the infrastructure that is chosen by the SLC Operator. It is recommended that the SLC Operator takes the above requirements into account and determines an SEM that is best suited to their environment.

### Two-Factor Authentication:

Goals:

* Access to any system that has PII data needs to be controlled through a two-factor authentication mechanism. Two-factor authentication can be best explained as a user needing to have “something they know” (like a username and password) and “something that they have” (like an RSA key that continuously changes).
* Using this approach ensures that access to a system with PII data cannot be obtained with just a username and password, but also requires access to a revolving token or key that can be revoked at any given time.

Recommended course of action:

All external (outside of the VPC) servers or hosts that are granted access to connect to the AWS cloud require a means of performing a two-factor authentication.

Recommended software: **RSA SecurID**

RSA SecurID provides a module that can be installed on every server that provides a means of facilitating the second form of authentication (something you have) that is used with a user logging in (something you know) to verify the validity of the session.

### Web Application Firewalls (WAF):

Goal:

* Web servers need to be protected from common attacks such as Cross-site Scripting and SQL Injections.

Recommended course of action:

All requests made to web servers need to be through *at minimum* a WAF that can be configured to detect a number of potential web threats and alert on violations. Also, the WAF must insure that all database software susceptible to injection attacks has the latest security patches installed at all times. Functions within the database software which protect against injection attacks should be utilized.

Recommended software: **Layer7**

Layer7 WAF gateways should be put in front of all the web servers and configured to prevent any of the common web attacks. Layer7 also provides an added functionality of learning normal system traffic. It can be configured to deny attacks on the fly when it sees that normal communication has deviated.

### Vulnerability Management:

Goals:

* A means of continuously and safely testing the infrastructure to new threats in order to close the gap between 0-day exploits and vulnerabilities is highly recommended.
* A system that can update, scan, and notify automatically is preferred.
* A system that can not only identify weakness in the infrastructure but can also be intelligent enough to know exactly what patches to recommend in order to no longer be vulnerable.

Recommended course of action:

Install a vulnerability scanner/management system that can update itself automatically in order to stay up-to-date with the latest threats. The system should also be able to scan on a regular schedule and notify on vulnerabilities it encounters in the infrastructure.

Recommended software: **Tenable Security Center**

Tenable provides all of the features necessary to stay current on the latest vulnerabilities, from automatically downloading the latest definitions for attack vectors to being able to scan on a schedule and alert accordingly. Tenable also can be configured to function as an SEM.

Possible second recommendation: Qualys

#### Data Infrastructure Software:

A release process must be defined by the SLC in order to manage software releases of the Data Infrastructure onto the SLI platform. These releases fall into the following three categories:

* Major (for example, Release Alpha, Release 1.0, Releases 1.x)
* Maintenance (for example, bugfixes or sprint releases such as 62, 63, etc)
* Emergency (when a severity 1 incident has occurred).

The software taken from the Wireless Generation repository must be managed in such a way that not only can the software be rolled forward onto a new release quickly and easily, but so that these releases can be rolled back quickly if necessary.

Wireless Generation has specified components for the operating system, interpreters, middleware, and other software components. While the Data Infrastructure software may be functional in an environment that varies from the provided specification, such variances have not been vetted by Wireless Generation for security or applicability to running the software.

In order to provide a secure environment for assisting the operator with any issues that should arise in the production environment, the SLC will need to provision a Centrify-equipped “jump box” within the AWS VPC. By doing this, all traffic from the Wireless Generation network must go through a single box in order to reach the AWS servers. Using Centrify, this traffic can be monitored and recorded for security purposes. This needs to be a duplicated system to prevent single points of failure and thus the inability of Wireless Generation to be able to troubleshoot SLI software on the system.

### Non-Data Infrastructure SLI Software

Other SLI software contracted by the SLC must be completed and certified to be ready to run on the platform, including change management and rollback. At this time, Wireless Generation has very little information on what this software might be or its’ characteristics.

### Data Reliability – at rest

All data on all disk drives should either be mirrored or RAID. The disk system will use Amazon’s Elastic Block Storage (EC2 EBS), provisioned with multiple virtual drives of 1 TB each. If a bare-metal data-center is used, RAID is even more important as it adds another barrier to somebody decrypting the drives.

### Data Security – at rest

The system must be configured so that data at rest (on disks or other persistent storage) is encrypted to the degree required to prevent compromise of PII data.

Any disk which may hold PII should be encrypted at all times. Disks that may hold passphrases or sensitive security information should also be encrypted. Gazzang, which offers asynchronous key-based encryption for the file system and the MongoDB back end, has been chosen to fill this role. In addition, for disks holding the Mongo database files, the Data Infrastructure software will add an additional layer of encryption on PII fields. Which fields exactly constitute PII is an open issue that is being resolved at the time of this writing.

One of the disadvantages of using the AWS system is that if an instance is de-allocated and thus handed back to the AWS “pool”, it is not guaranteed that AWS will wipe that space. Since this could happen as a result of disk failure, the data on disk must be encrypted at all times.

For more details on this, search for “unintentionally” on the following page: http://aws.amazon.com/articles/1697?\_encoding=UTF8&jiveRedirect=1.

For disks that are used for Ingestion Landing Zones, the encryption must be managed such that each user directory is encrypted by the user with their own key to prevent the ability for even a privileged user to gain access to the contents of the users directory. These disks should be configured to use Gazzang or a similiar tool, as well as chroot to segregate users.

## Passphrase Security

There are many areas where passphrases need to be stored in the SLI but accessed by the Data Infrastructure in order for the system to function. It is vital that passphrases never be stored in clear text on any machine. Standard security best practices for passphrase length, complexity, and expiration are to be followed.

### Network Security

The internal network data should be protected by using a product such as OpenVPN or Amazon Web Services Virtual Private Clouds (AWS VPCs). This will ensure that all “data in flight”, including PII, is always encrypted. In the case of data being sent to and from Mongo (to either the disk or the application layer) PII will be encrypted multiple times:

1. On the physical disk
2. In the Mongo layer by Data Infrastructure libraries
3. Over the session-based secure network connection inside the Amazon VPC

All servers should be instantiated in Amazon Security Zones, controlling which machines can make inbound and outbound connections to other machines.

All Web Front End browser traffic must use HTTPS connections.

The incoming connections to the SFTP landing zones will use SSL. SSL/ipsec will be used between all internal machines in the VPC.

### Staffing

Staff must be hired, trained, and assigned to the different roles on the project, including, but not limited to the following skills:

* system administration
* security administration
* network management
* help desk operations
* vendor relations
* procurement
* Linux
* AWS
* MongoDB
* Tomcat operations
* Apache operations
* LDAP operations
* Ruby on Rails administration

Because of the sensitive nature of the student data stored in the SLI in general, and the Data Infrastructure in particular, the Operator should have documented background checks for all employees with access to the system or to any data on it. In addition, the Operator should require these same employees to take security training before being given credentials to access the system.

### Company Security Policy

Wireless Generation recommends that the Operator have a written Company Security policy that is approved by the SLC.

### Procedures

Procedures must be defined on how to operate the system, and react to both routine and exceptional circumstances from both hardware and software systems. Before the Operator can open the production environment to user logins, the Operator must have documented runbooks for all operational and security situations. This includes escalation and resolution processes for situations not anticipated in the runbooks.

### Support

For the Alpha release, the SLC will need to define processes to answer user questions from the LEAs as well as SLC Vendor Parters (A&M, Applied Minds, Agilix, and so on). For subsequent releases, the SLC will need to expand these systems to support the potentially 20 million students, 40 million guardians and 1 million staff and educators using the SLI.

### Operations Management

Appropriate people, monitoring, and controls must be put in place to assure the project is proceeding correctly or whether corrective actions are needed. Additionally, if the Operator of the Production environment is not the SLC, then the SLC must be kept in the loop on system status, problems, expected resolution times, new procurement needs, and so on.

### System Monitoring and Alerting

The SLC, or the Operator, should monitor the availability, response time and overall health of the Production Environment and UAT Environment. This monitoring should be carried out on a 24x7x365 basis, except during periods of expected service unavailability or unavailability due to emergency. The Operator should maintain a historic record of the aggregated monitoring results for a period of no less than 2 months.

The Operator should define a severity scale for both operational and security incidents. With this scale, there should be a procedure to be followed for each type of event at each security level.

### Vendor Support Capabilities

The Operator must define procedures and processes to follow in the event that a software or hardware element of the system malfunctions in such a way that vendor support is needed.

The first action of the Operator should always be to define the problem and identify the system activity which led up to that problem. If the problem is not reproducible, the Operator must capture whatever relevant information they can and forward it on to the hardware or software vendor. A procedure must be put in place to ensure that diagnostic information that leaves the AWS VPC does not contain any PII.

If the initial set of information given to the vendor does not allow the vendor to find, diagnose, and repair the problem then more information may be given. If this is unsuccessful, the Operator should have the capability to reproduce the problem in a staging environment that they provision and configure. At that point, the Operator can give secure access to the vendor so that the vendor can watch the problem be reproduced.

If the above mechanisms fail, and the Operator cannot provide sufficient information for off-site analysis, or cannot reproduce the problem in a staging environment, it will be up to the SLC and the Operator to implement Escalated Support Incident procedures to allow supervised, live system analysis. While it is anticipated that these problems will be a very low percentage of the system problems found, there must be a mechanism in place for the Operator and the SLC to request such support. If the problem can be reproduced, the Operator must provision a development environment and instruct Wireless Generation on how to reproduce the problem there. Because the SLI contains PII, these procedures must be followed by the Operator at all times.

### Service Level Agreements

In order for the SLC to ensure that the production system will be performant and secure, the SLC must define Service Level Agreements (“SLAs”) with the Operator. These include (but are not limited to):

* Amount of total system downtime per year
* Time to repair broken servers
* Response time for high priority SLC-reported problems
* Response time from the help-desk for standard client-related problems
* Concurrent help-desk throughput
* Data backup regularity and frequency of checking backups via reload onto another system

### Hardware Points of Failure

In order for the system to survive system failures it is advised that redundancy be built into component planning. There should be a minimum of 2, but ideally 3 or more, servers/instances per component type. Having 3 or more will also allow the SLC to take advantage of AWS Availability Zones furthering the resiliency of the system by taking advantage of AWSs separate DataCenters.

This applies to (but is not limited to) the following components of the system:

* Ingestion servers
* Application (API) servers
* LifeRay servers
* Identification servers
* SEIM servers
* Load Balancers

In AWS, it is imperative to be cognizant of the fact that you could have multiple instances (virtual hosts) on the same physical Amazon server. While Amazon does try to mitigate this, it is not guaranteed. It is advised to take advantage of AWS’s Availability Zones to achieve maximum redundancy.

For more information on Amazon Availability Zones, please see http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html.

Amazon also provides the ability to split the Operator infrastructure across Regions. These are distributed environments that help protect against cataclysmic events such as hurricanes, earthquakes, multi-state power failures, and so on. See the above URL for more information on Amazon Regions.

For the Production Environment, Wireless Generation believes that AWS Availability zones are sufficient. Wireless Generation has not tested the software internally using multiple Availability Zones and believes that using Availability Zones should be tested in the Staging environment before a Production deployment.

### Acceptance Testing

For any environment supplied for Data Infrastructure, the SLC or a third party vendor should perform acceptance testing of that environment. Wireless Generation has the capability to assist in acceptance testing of the Production environment if the SLC desires it.

# Summary

This document described the minimum operating standards for deploying the Data Infrastructure Software onto an SLI production environment in a secure manner, as well as a tentative timeline for the Alpha and R1.0 Production Environment releases. In addition, this document described the method of scaling the environment to 5 million students and has given guidelines on what is to be expected to scale the environment beyond 5 million students.

Wireless Generation is eager to assist the SLC in this endeavor to make the SLI a success.