labguru Infrastructure and Security

Infrastructure Configurations

Labguru is available in three configurations:

1. **Labguru Saas** – A shared cloud platform. BioData is responsible for server maintenance.

2. **Labguru Private Cloud** – A private cloud solution, in which BioData provisions a server set at one of our cloud host vendors which is only used by a single client. BioData is responsible for server maintenance.

3. **Labguru Local Install** – A local install solution, in which Labguru is installed on a server set provided by the customer on their own network infrastructure. BioData and the customer work together to provision and maintain the servers. BioData is responsible for the application support.

Logical Servers

The Labguru solution consists of several logical servers (*figure 1*):

1. **Application server** - An apache2 webserver and the Labguru Ruby-on-Rails application.

2. **File Attachment store** - a file server containing user attachments that have been uploaded to Labguru accounts.

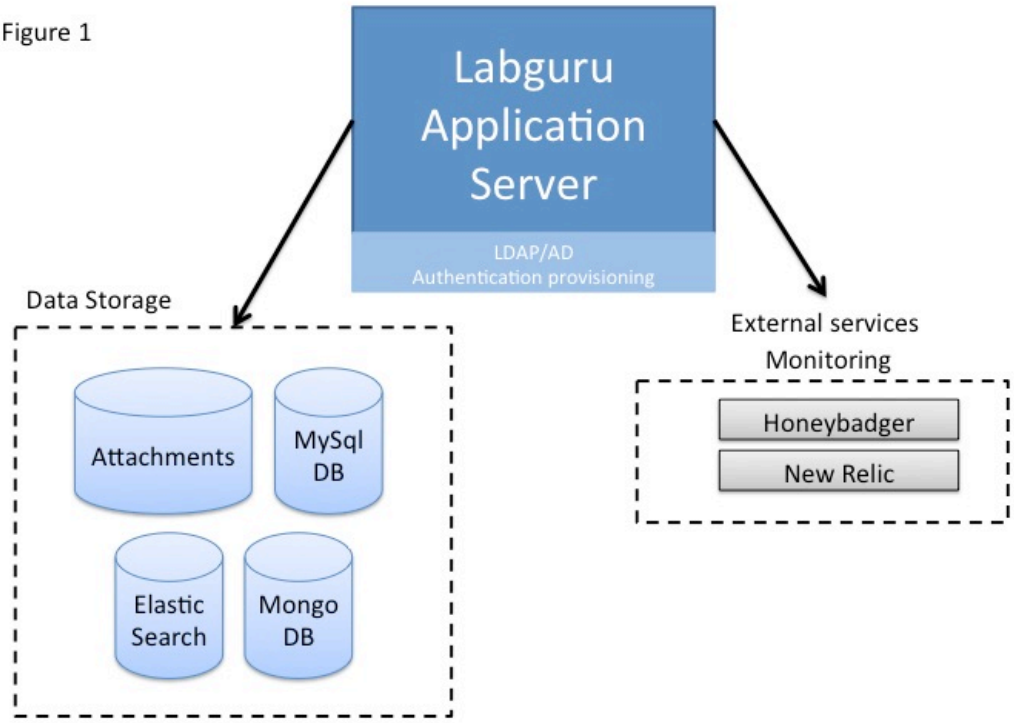
3. **MySQL DB** - The main user data store of Labguru. Each labguru account (lab) data is stored in its own logical database.

4. **Elasticsearch** - This server powers the account-wide free-text search function within the Labguru application.

5. **MongoDB** - A vendor product catalog, used in the inventory module of Labguru. Users can search and copy vendor items to their account for future reference.

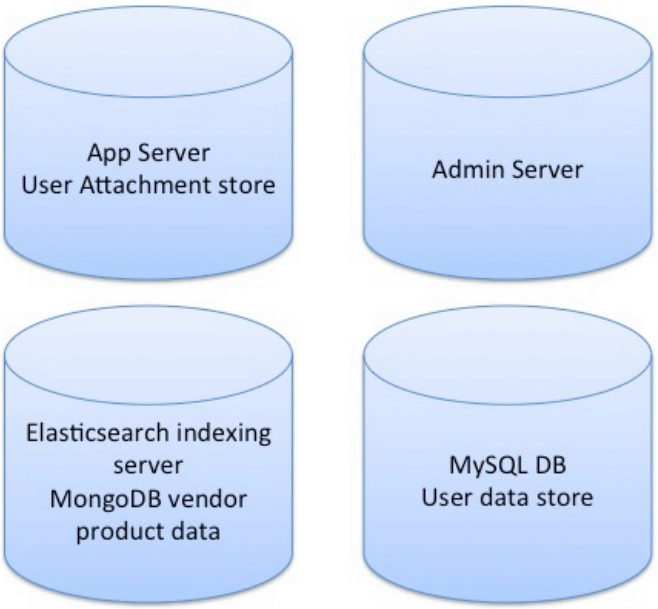
6. **Administrative server** - An apache2 webserver and the Labguru Admin application. Used by BioData customer support to monitor and resolve customer issues.

Figure 1



The 6 logical server roles are typically deployed on 4 physical or virtual hosts as follows (figure 2):

Figure 2



Application Networking

Inter-Server Communication

The application server connects to all data stores (MySQL, Elasticsearch, MongoDB, file attachment), through the appropriate protocols and ports:

- MySQL - 3306
- Elasticsearch - 9200
- MongoDB - 27017
- File - through NFS if not local to the app server host
- The admin server connects to the MySQL DB only, over port 3306

Client Application Access

Client browsers access Labguru Application and the Labguru Administration server through https (SSL) on port 443.

Administration Access

All hosts are accessed through SSH (port 22) using a public/private key login. SSH access is required for maintenance and inital/update deployments. Two public keys for BioData personnel and for cloud host vendor personnel are added to the authorized keys on each host.

Communication to and between the servers is reflected in the firewall (IPTables) rules. Each server is closed for incoming traffic on all ports excpet 22 for SSH access and any ports that are required for the logical roles it provides (e.g. port 3306 is open on the host containing the MySQL DB).

Monitoring/Error Response

The Labguru Application server sends out information to two monitoring systems:

- **Newrelic** for monitoring app performance and availability.
- **Honeybadger** for monitoring app errors.

These two services are monitored by BioData personnel and actions are taken accordingly to ensure the best experience for Labguru users.

MS Office File Editing

Viewing/Editing MS office files within the Labguru application (an opt-in feature per account) requires access to file attachments through the Labguru web app (over https) by a third party service (Zoho). i.e. the web app server has to be available for https connections from the Zoho servers without any VPN or source IP restrictions. According to the Zoho service agreement, user data is not stored on the Zoho servers.

Account Provisioning and Authentication

Labguru includes a mechanism for account provisioning and user activation/authentication within the web app or via an SAML/AD/LDAP service. Labguru has a plugin provisioning/authentication layer, to which a specific Provisioning/Authentication plugin can be created for a specific workflow/SSO requirement.

Security Practices and Procedures

Our database and file stores are backed up daily and retained for a minimum of 30 days.

We are regularly audited by Qualys (an independent 3rd party network and web application security and vulnerability management auditing solution) to ensure our cloud platform is secure and up to date.