Infrastructure Requirement for Private-Box on Public Cloud

We are preparing this document considering Azure as Cloud Service Provider.

For architecture we are considering deploying microservice on Kubernetes which allow us cloud independence, high availability, scalability, security, observability and best practices of software development life cycle.

**Pre-requisites**

Master and Worker nodes (Virtual Machines) in Kubernetes cluster are SEV (Secure Encrypted Virtualization) are SEV enabled. Although everything on cloud is encrypted yet we will use encrypted storage for files.

**SID Services and Components**

**Infrastructure Components**

Cloud Load Balancer

Cloud Firewall (For Infrastructure Security)

Cloud Based IPS/IDS/SIEM/UEBA

ISTIO for policy and internal routing

File Storage (Azure Data Lake Storage)

* For storing encrypted files

MySQL-backed database (Azure SQL Database)

* For User metadata

No-SQL Database (Azure Cosmos DB ()

* For storing unstructured files metadata
* Index of File (Encrypted addresses and Encrypted Values)

Cache Server (Azure Caching)

* Cache file previews

In-Memory Data Store (Azure Redis Cache)

* For user’s session management

Queueing Server (Azure Queue Service)

* Queue files for upload

**Privacy-Box Services**

To deploy SID as Dopbox there are also some other services required as mentioned below.

**SID Services**

**Client-Side Application**

A client-side service with following functions.

SID Setup (SID)

* To generate Keys and Index words to files

Add/Delete/Modify Function

* To add, delete or modify a file

Update Function

* Update no. of Files, no. of searches arrays and Mappings

Send-Indexes-to-TA Function

* To send KG and updated no. of Files, no. of searches arrays

Send-Mappings-to-CSP Function

* Send Encrypted Mappings to TA

**Trusted Third Party Server**

TA Service (SID)

* To receive no. of Files, no. of searches arrays and send them to users on request

**Server-Side Services**

**Front-End Service**

* Dashboard to perform various management activities and endpoints for web, Desktop and Mobile clients

**Back-End Services**

Encrypted-Map-Receiver Service (SID)

* To receive encrypted Map of addresses and encrypted values

API Service

* For routing requests to respective back-end service endpoints

User Sign-Up

* To signup new User

SSO service

* Redirect User if he wants to sign up using third party or cloud AD like office 365

User Login

* To login Users

Password Reset

* To reset user password

User Metadata Storage Service

* A backend service to read and retrieve metadata from in DB

Files Metadata Storage Service

* For storing files metadata

Notification Service

* Notify new files, updates and modification

Files Sync Service

* Sync changes

Email Service

* To send sharing links and notifications

Verification Service

* To verify domains while sign-up

SMS Service

* For multifactor Authentication

User Management Service

* To manage users and their roles

Snapshotting

* To take snapshot of a state

Backups/Recovery Service

* To backup and restore a specific file

Business continuity

* Disaster recovery
  + Privacy-Box will be deployed in multiple regions to ensue disaster recovery