01.15 | White Paper

Security In a Public Cloud

How Mambu Keeps Your Data Safe with AWS

MAMBU

Table of Contents

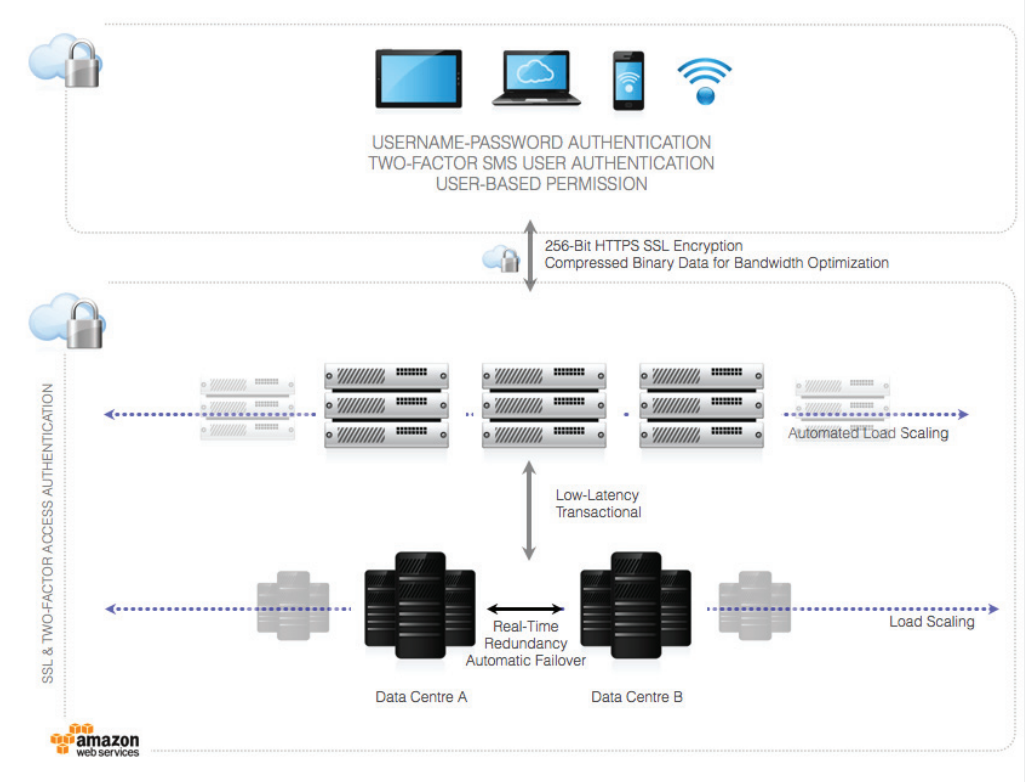
MAMBU

Security Practices at Mambu Using the AWS Public Cloud

Technical Overview

Mambu is offered as Software-as-a-Service and relies on public cloud infrastructure. *Figure 1* outlines the architecture of Mambu's cloud banking platform.

Users can access Mambu either through a web application or APIs. The web application can be used on a desktop computer or tablet and mobile applications or integration solutions can use APIs to access core features of Mambu. All communication with the Mambu platform is securely channeled through



Channels

Software & Hardware Independent
Desktop
Smartphone
Tablet
APIs

Application Servers

Fully Managed
Elastic Load Balancing
Multiple Locations
Automated CPU & Latency Monitoring
Each up to 244GB Memory & 32 vCPU Cores
Linux

Database Servers

Fully Managed
MySQL or Oracle
Automated Backups
Automated Logging
DB Snapshotting
30-Day Transaction-Based Rollback
Each up to 244GB Memory & 32 vCPU Cores
Isolated & Secure

Figure 1. **Mambu Cloud System Architecture** (Overview)

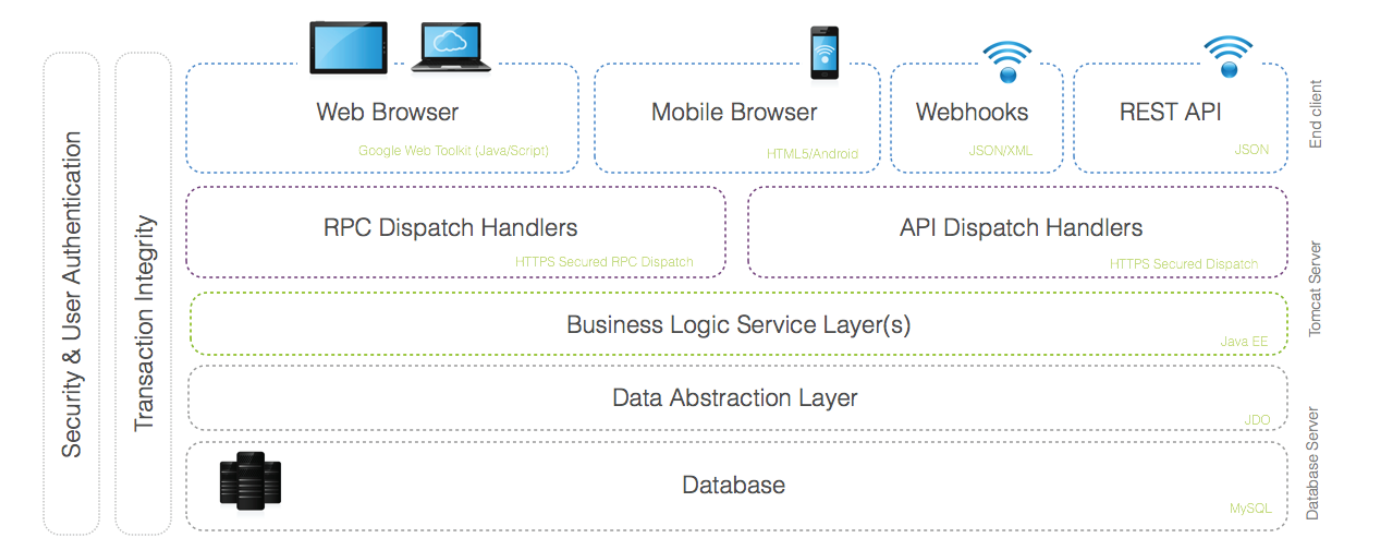


Figure 2. **Mambu Cloud Application Architecture** (Layers/Tiers)

HTTPS requests. Every request is channeled from a public load balancer to a cluster of non-public applications servers which communicate with a non-public database server if required.

The load balancer, application server and database layer are all kept redundant in two close by data centers to ensure high system availability. There are firewalls in front of the load balancers, application servers and database servers that restrict inbound access only to whitelisted IP addresses and ports.

Taking a closer look at Mambu's internal layers, *Figure 2* illustrates how requests to the Mambu platform are processed.

An incoming HTTPS request is either parsed by RPC (Mambu web application) or API dispatch handlers, which invoke service methods from the business logic layer. If required, the service methods make calls to the database over a database abstraction layer. Across all layers various security mechanisms like user authentication, authorization or virus scans are implemented to protect the Mambu cloud banking platform. Transactions triggered on the user interface or via APIs are end-to-end managed, which means their success is reported back to the user interface or API user. In case of non-success, the complete transaction is rolled back to ensure the database is alway in a consistent state (Transaction Integrity).

Platform Details

Table 1 outlines all third party infrastrastructure and software components that are used to develop and operate Mambu.

	Technical Requirement	Used Software / Library Name
OPERATION	Server Infrastructure	Mambu runs on Amazon Web Services Infrastructure in the region US-East-1, it uses the following services: - IaaS (EC2 [Network, CPU, Memory, Disk]) - PaaS (Elastic Beanstalk, Relational Database Service, Simple Email Service, Simple Notification Service, CloudWatch, ElastiCache)
	Operating System	Amazon Linux
	File Store	Amazon S3 (redundant and highly available file store)
	Web/Application Server	Apache / Apache Tomcat on Java EE (OpenJDK)
	Database Server	Amazon Relational Database Service based on MySQL, database server deployment uses a master-slave setup where master and slave are in separate data centers.
	Infrastructure Management	All servers and services are configured via Amazon Web Services Management Console and Amazon Web Services APIs.
	Scalability / Elasticity	Based on the current load (measured in latency for response time) on the Mambu system, servers are scaled up and down without human intervention and effects on users.
	Environments	In order improve availability of the Mambu system to users there are several environments of Mambu which all serve a different purpose: - Frontend Environment, serving user and API requests - Cron Job Environment, executes regular hourly and daily jobs - Client Portal Environment, serving an organization's clients' requests - Sandbox Environment, serving trainee, tester and developer requests for test users, organization's test clients and test API users Next to these public environments Mambu uses internally several environments for different types of testing.
	Infrastructure Monitoring	All servers and services are monitored via Amazon CloudWatch. Additionally Mambu's application availability is monitored by Pingdom on a 1-minute interval and notifications are sent to operators using OpsGenie.
	Email Service	Emails to users and clients are sent via Amazon Simple Email Service.
	SMS Service (InfoBip / Twilio)	Organizations can choose to send SMS via Twilio or InfoBip for client communication and two-factor authentication of their organization's users.

Table 1, continued

	Technical Requirement	Used Software / Library Name
PRODUCTS	Application Frontend (Rich Internet Application [RIA])	Mambu's web frontend is a RIA that is written in Java and compiled to JavaScript via GWT. Several open source libraries are used to reuse common functionality. Major Libraries are: GWT (extended by GWT-DND, GWT-Log, GWT-VL, GWTUpload, GWT Highcharts, SWT Graphics 2D, GIN). The JavaScript client communicates via the GWT-RPC protocol with backend servers. For real-time client/server communication protocols like WebSockets are used via Atmosphere and Java SMPP. Client (Browser) communication is secured by a HTTPS (RSA 2048 bits key, SHA256withRSA signatures) connection.
	Application Backend & Application REST API	Mambu's backend uses the Java EE platform with several open source libraries to reuse common functionality. Major Libraries are: GWT, Quartz, Datanucleus (JDO 3.0), Liquibase, Joda Time, MySQL Connector/J, AWS Java SDK (extended by Amazon Elasti Cache Cluster Client), Apache Commons (Codec, Lang, Logging, Beanutils, Collections, DBCP, Digester, FileUpload, IO, Net, Pool), Apache HTTP Components (Core, Client), AOP Alliance, Groovy, GSON, Guava, jsoup, Log4J, Java Mail, SLF4J, SMSLib, Threescale API, Thumbnailator, Twilio Java, XOM, C3P0, ASM, CGLIB, Guice, Jasper Reports, iText, JFreeChart, Apache POI
Development, QA & Build	Software Development Operating Systems	Mambu is mainly developed on OS X using Apple computers.
	Software Development Environment	Mambu's developers use the Eclipse IDE with several open source plugins to manage tasks, software configurations and test environments.
	Testing	For unit, integration, regression and load testing frameworks like JUnit, Mockito, Objenesis, Selenium, JMeter, SOAP UI and P6Spy are used.
	Build Process	Mambu's build artifacts are reproducible due to a standard build process specified in Ant and executed on Atlassian's Bamboo build servers.

Data Isolation and Data Security

Mambu is implemented following the principles of security by design. Being a multi-tenant platform special efforts are taken to ensure data and performance isolation.

Data and Performance Isolation

Mambu being a multi-tenant Software-as-a-Service solution ensures that all client data is isolated between tenants. As shown on *Figure 3*, every tenant on the Mambu platform has his own database, which is not shared across other tenants and therefore allows clear data isolation. To ensure data isolation on the application layer, Mambu is built in a way that user requests are tied to the organization's database the user belongs to. Performance isolation is managed by scalable and real-time monitored load balancers, application servers and database servers. Based on real-time monitored metrics, enough resources are provisioned as needed.

Data Security

Physical Security

All data inside Mambu is stored in AWS data centers which have strong physical security measures, e.g. against fire or physical theft.

Protection Against Data Loss and Unauthorized Modification

All data is backed-up continuously, retained for 30 days and recoverable up until the last five minutes from 'now'. Additionally full database backups are done for the last seven days and stored off-site. Inside the Mambu application all critical events are logged in an activity log.

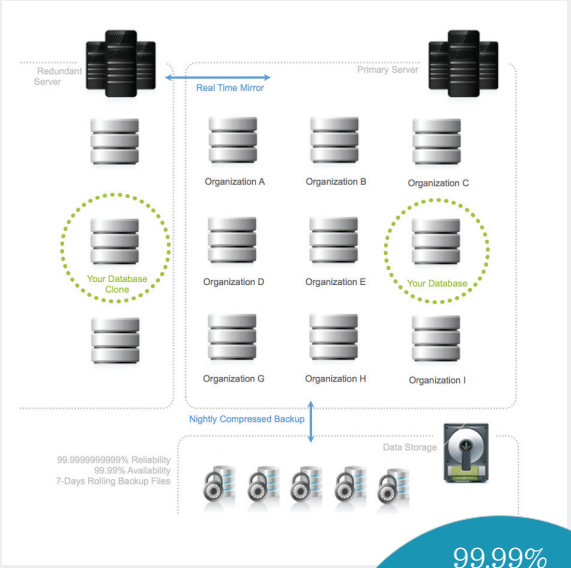
Virus Checks and File Type Validations

Files uploaded by users to Mambu like documents, images, data to be imported or custom reports are virus scanned and validated against a whitelist of allowed file types and file extensions.

Up to Date Systems

Operating systems are updated regularly to protect against known vulnerabilities. Urgent software updates e.g. due to severe security threats can be rolled out within few hours to all Mambu servers.

Figure 3. Mambu Data Isolation and Security



Complete Data Isolation & Security

Independent Databases
Isolated Schemas
Scalable Servers
Real-time Mirroring
Multiple Physical Data Centres
Off-Server Nightly Backups
7-Days Rolling Backups
30-Day Transaction-Based Rollbacks
99.9999999999% Document Reliability

99.99% Availability

30-Day Database Rollbacks

99.9999999999% Reliability

Authentication

Mambu has strong identity and access management capabilities. An organization's administrator can define password rules, activate two factor authentication and define inactivity rules (session expiration) to ensure the identity of a request. Password strength indicators inside Mambu encourage users to use strong passwords and password guessing attacks are mitigated by captchas and time constraints.

Mambu staff uses two factor authentication when accessing the Amazon Web Services administration console to manage

production infrastructure and logs all configuration changes on the production environment.

Authorisation
Fine grained permissions on a per data type and branch level as well as for all functionality can be granted on a group or individual user level.

Further each tenant can restrict access to his Mambu instance using a whitelist of IP addresses. All accesses to Mambu load balancers, application servers and database servers happen over firewalls, which allow inbound access only to whitelisted IP addresses and ports, as shown in *Figure 4*. The application, database and cache servers cannot be reached directly from the public internet. Only the load balancers can access application servers and only application servers can access database and cache servers. The only exception is Mambu's technical support and operations staff, which can whitelist their IP address for port 22 (SSH) to access Mambu's application and database servers in order to investigate and resolve problems.

If a tenant uses Mambu features like email, SMS or WebHook notifications, Mambu application servers connect directly to external services like SMS gateways or e.g. corporate networks of clients when using WebHooks. In that case the client has to ensure that access occurs over a firewall.

Inbound traffic is regularly checked for anomalies using load balancer metrics (request counts, inbound and outbound traffic size, latency, etc.) and HTTP logs.

Managing Security Throughout the Stack

Audited Physical Data Center Security

Virus Checks & File Type Validation

Up to Date Systems

Two-Factor Access Authentication

User Access Authorization Rights

Secure Data Transport Layer

Internal Controls and Complete Activity Audit Trails

Mambu's support staff is able to login to a client's Mambu instance upon client request to answer user requests or trace potential problems. Once a support request is resolved, an organisation can disable Mambu's support access again. As for any other user, activity logs are generated for Mambu's support user as well.

Secure Data Transport
Mambu users can only access the Mambu platform via HTTPs which ensures transport channel encryption (RSA 2048 bits key, SHA256withRSA signatures). Mambu system administrators login to Mambu servers only via SSH, using public/private key authentication.

Protection Against Internal Fraud
Source code changes on the Mambu platform are peer-reviewed and signed off by other experienced developers. The team developing source code is distinct from the team promoting code changes to the production environment.

Failure Prevention

Mambu offers various ways to prevent system failures and disaster scenarios in the first place.

Sandbox Environment
In order to prevent tests and trainings on production environments, Mambu offers a sandbox environment for testing and training. The sandbox environment can be reset at any time to remove all data and configurations or can contain a copy of the production

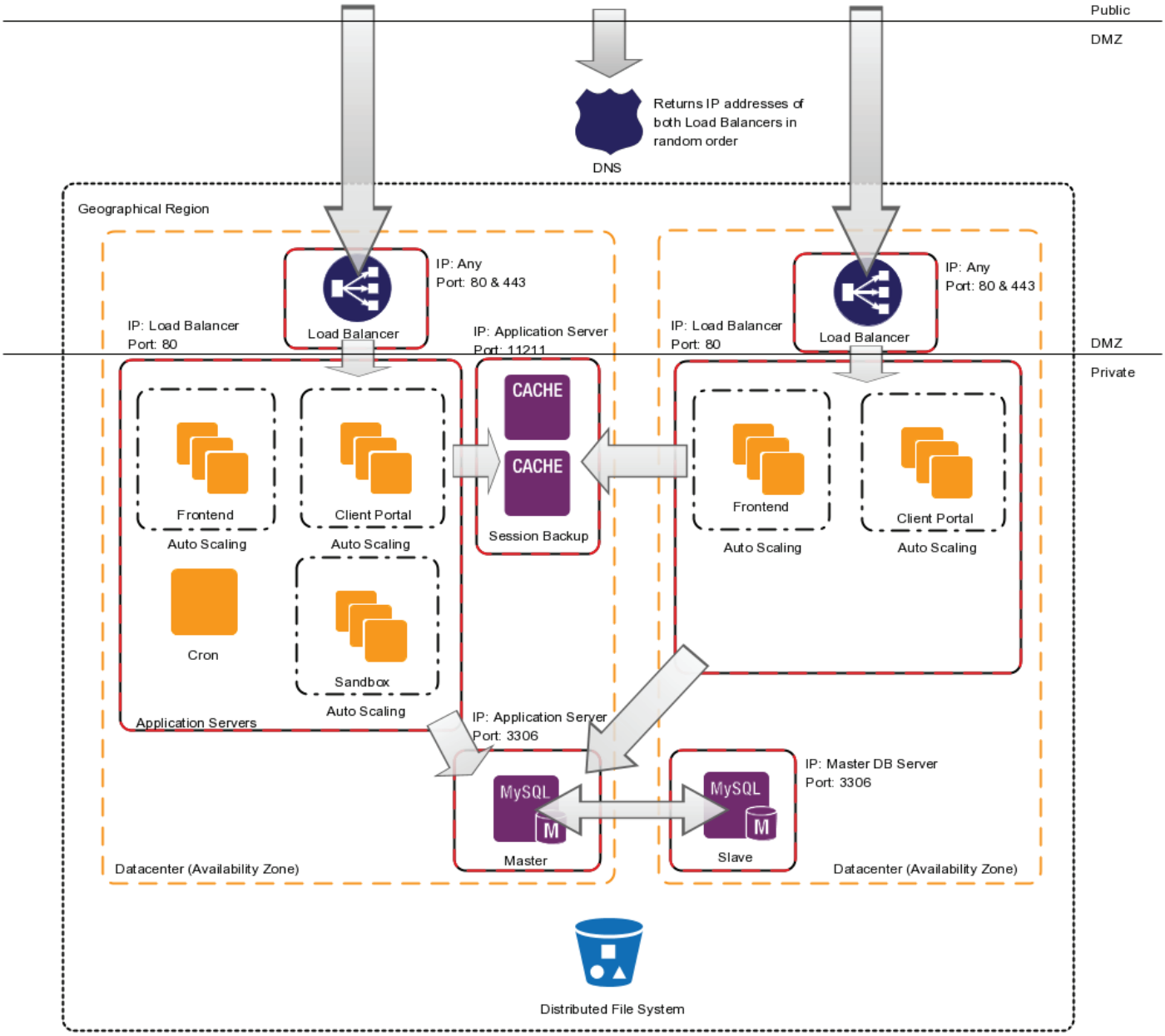


Figure 4. Mambu Firewall Settings

data, where the actual client data can be deleted so that only production settings are available in the sandbox.

Confidentiality
Additionally to fine grained permissions the communication between the client (browser) and the server is encrypted via SSL/TLS and only passwords hashes are stored.

Integrity
All transactional data is stored in relational databases that comply to the ACID principle and therefore ensure that no corrupted data is persisted. Additional audit trails ensure traceability of which user did which action in Mambu at which time. For data center security see also *Figure 5*.

Availability
All core components (database server, application server, file store) of the application and infrastructure are kept redundant. The used core infrastructure (AWS EC2) is guaranteed to have at least a 99.95% uptime, reinforced by Mambu SLA up to 99.99% availability.

Compliance
Mambu servers are located on multiple Amazon Web Service's data centers, which are certified as illustrated in *Figure 5* (HIPAA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP(SM), DIACAP and FISMA, ITAR, FIPS 1402, CSA, MPAA).

Managed Datacenters
Amazon Web Service's infrastructure is connected to uninterruptible power supplies (UPS), power outages are covered by generators and fire detection and prevention equipment is installed in all data centers as well. All hardware maintenance is covered by Amazon Web Services.

External Audits
Mambu employs Plynt and Schutzwerk for independent annual penetration tests and security audits. These tests ensure compliance with e.g. OWASP Top 10 and safeguard against popular attacks based on standard web and custom financial application thread profiles.

Figure 5.

Mambu Security and Compliance

Knowledge Sharing
Mambu developers and operators document and share critical knowledge to ensure independence of individual employees in case an employee is not available anymore short- or long-term.

Backup and Disaster Recovery

Mambu is designed for failure, so that in case something fails, there is a backup strategy. This allows to recover quickly or even automatically without notice in case a disaster prevention mechanism fails.

Backup Procedures

Client Data Backup
Client data stored in a relational database is backed up continuously for the last 30 days, additionally daily snapshots are kept for 7 days and a failover database server (slave) is kept in sync in a separate data center. For backup structure and data isolation see also *Figure 3*.

Mambu's document management module stores files on Amazon S3, which is internally backuped at Amazon Web Services and provides a 99.9% uptime availability SLA, though it's designed for 99.99% availability and 99.999999999% durability.

Application Configuration Backup
Mambu application configurations and binaries are backed up by Amazon Web Services internally using mainly Amazon S3.

Disaster and Recovery Plan

Hardware / Software Incident on Single Application Server

Mambu's process combines internal review and QA processes and testing with external penetration and security testing.

Mambu employs Plynt for independent annual penetration tests and security audits.

Unhealthy application servers are automatically identified and terminated, a replacement is launched automatically and immediately after termination of the faulty server.

In case a database server becomes unhealthy, every primary/master database server has a failover secondary/slave database server in a different datacenter (AWS Availability Zone) that is kept automatically in-sync. On incidents the master database server cannot recover from a failover event is automatically triggered, the former secondary database server (slave) becomes the new primary database server (master) and a new secondary database server (slave) is provisioned and brought up to date. This failover is transparent to the Mambu application servers.

Mambu application servers only store transient files on their local file system and follow a utility computing model. All customer uploaded files are permanently stored on a distributed file store, which is redundant on multiple servers and data centers. In case a file on the distributed file store is lost or a whole disk is unhealthy, it is restored from one of the many backups, this replication procedure is managed by Amazon Web Services (S3).

Hardware / Software / Configuration Incident in Single Data Center
All client requests are served by multiple servers which are located in at least two data centers redundantly, as illustrated in *Figure 4*. In case of an incident in one data center, all requests are served by the nonaffected data

center and additional server capacity is automatically provided to cope with additional load in a failover datacenter (Availability Zone). Once the the first data center is fully recovered the load is once again distributed over both data centers and resource capacities are adjusted accordingly.

Monitoring and Alerting
All machines and services are constantly monitored on a one minute interval at machine and application service level.

At least two operators are notified via email, SMS and phone calls 24/7 to take care of incidents in case manual intervention is required.

Platform Maintenance

Upgrade and Migration Process
During the time an infrastructure component like the database server, all application servers or the Mambu application itself is updated the users of the application cannot access the application. For such events a scheduled maintenance window is used which is announced at least 48 hours ahead of the release event via email and on every user's login screen.

For all patch releases or security fix deployments which may not require a downtime, all users are notified on the login screen.

Before any updates and migrations snapshots are taken as recovery points from all affected database servers, which ensures the last working point in time can be restored in case the migration fails.

Once the snapshots are completed all required infrastructure and application components are updated and once finished, users are allowed to access the application again.

Additional References

AWS Security Best Practices
View PDF >

Amazon Web Services:
Overview of Security Processes
View PDF >

Backup, Archive, and Restore
Approaches Using AWS
View PDF >

Amazon Web Services:
Risk and Compliance
View PDF >

About Mambu

Mambu enables financial institutions of any size to rapidly create, launch and service loan and deposit products through its agile, flexible and affordable cloud banking platform. An alternative to legacy in-house systems and cumbersome core banking systems, Mambu accelerates time to market for new consumer and SME banking products.

Mambu helps new institutions and business units to bring new products to new markets via new channels quickly and affordably. We also help transform smaller financial institutions from legacy in-house systems to give them the ability to digitize their business and better service their customers at the fraction of the cost, time and risk of traditional core banking system implementations.

Mambu is delivered in a SaaS model and can be deployed in any cloud environment. Our agile development process bring accelerated feature development to our customers, our technology infrastructure provides world-class security and scalability and our open integration protocol enables swift and simple integrations, extensions and automations.

Our vision is to enable institutions around the world to provide essential loan and deposit services to underserved individuals and emerging enterprises empowering them to pursue their own economic opportunities. We strive to be the trusted technology partner of our customers, allowing them to focus on rapid product, channel and business model innovation while we provide their core platform enabling them to manage and grow their business securely and cost-effectively.

www.mambu.com

Mambu GmbH
Jüdenstr. 50
10178 Berlin
Germany
hello@mambu.com

MAMBU