Connectik Platform

Architecture and Technology

November, 2016
Connectik - Goals and Overview

Connectik enables an organization’s employees, teams, customers and partners to connect, communicate, and transact using powerful digital capabilities in order to achieve higher levels of productivity, increased engagement, and to find new business opportunities around the world at the click or tap of a button.

Connectik - Technology Platform

- Focuses on delivering value to products and services
- Scalable and secure by design
- Modular solution driving agility and quick time-to-market
- Best of breed architectural choices built for the future
- Versatile modules and code reuse drive efficiency
- Test automation to ensure quality over time

Connectik - Key Architecture Attributes

- Multi-Tenancy/Multi-Tier - Designed to allow for multi-tenancy with multiple application support, where each application and tenant’s data is isolated, yet allows communication and administration across applications. The multi-tenancy architecture allows a single clustered backend instance to serves multiple customers. This allows for more flexible scaling as well as more rapid development and deployment of new features.
- Scalability - Leveraging Virtual Private Networks and cloud computing, the platform is both vertically and horizontally scalable, ensuring the ability to support millions of users, spikes in traffic, while optimizing resources to save on costs.
- Security – Encrypted at rest and in transit follows best practices of financial and banking institutions.
- Authentication/Authorization –With granular levels of authentication and authorization, each service and cluster derives access rights per user based on the information provided by the authorization layer. All administration is done using multi-factor authentication to ensure highest levels of security and address privacy concerns.
- Payment - Support is available both on client devices and applications server. Currently supported payment platforms allow for PCI DSS SAQ-A compliance, thus reducing system certification process complexity and risk, and onboarding of businesses to the system.
- Backup and Recovery – All data is maintained across multiple datacenters and available live at 99.95% availability. Furthermore, all data is stored live in multiple geographical regions ensuring all data is backed up on regular basis and stored securely over multiple datacenters, to ensure survivability and quick recovery in case of a data center disaster. The system undergoes routine disaster recovery practices to ensure no data loss and minimal downtime in case of a disaster.
Major System Components

Clusters and Services

1. **Virtual Private Cloud** - The clusters and services are isolated. The clusters and services in the virtual network connect to each other without being exposed to outside networks. In addition, firewall rules are configurable and control network access to the clusters and services.

2. **Application Cluster** - The core backend service coordinating all interactions of clients. The application cluster is a redundant, distributed, set of server, capable of scaling both horizontally and vertically.

3. **Chat Cluster** - An XMPP chat cluster, based on eJabberD, provides basic messaging, group messaging, and presence features. It also provides persistency through integration with the Encrypted Database Cluster.

4. **Key Management Service** - The Key Management Service allows creating and controlling the encryption keys used to encrypt the data, and uses Hardware Security Modules (HSMs) to protect the security of your keys. Key
Management Service is integrated with the Encrypted Object Storage Cluster, Encrypted Database Cluster and Encrypted Log Cluster

5. **Logging Facilities** - A service that records the events on the application and chat clusters. The logs produced enable security analysis, resource change tracking, error monitoring and compliance auditing.

6. **Encrypted Database Cluster** - A scalable, redundant, distributed and encrypted relational database cluster. The services allow to encrypt the databases using keys managed through the Key Management Service (KMS). The data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots. GIS extensions provide a spatial database extender for the database object-relational database. It adds support for geographic objects allowing you to run location queries in SQL. The database cluster also supports Full Text Searching that provides the capability to identify natural-language documents that satisfy a query, and optionally to sort them by relevance to the query. Dictionaries, besides improving search quality, normalization and removal of stop words also improve performance of queries.

7. **Encrypted Object Storage Cluster** - The Object Storage Cluster a secure, durable, highly-scalable object storage. It provides a simple web services interface to store and retrieve any amount of data. Data is accessible based on granular rules and may be available only within the virtual private cloud or to the entire internet. Cross-region replication provides automated, fast, reliable data replication across data centers. Data is uploaded and downloaded to the object storage cluster via SSL-encrypted endpoints. It automatically encrypts the data at rest through keys provided by the Key Management Service. The cluster is designed for 99.999999999% durability and 99.99% availability of objects over a given year.

8. **Authentication and Authorization layer** - The system has granular levels of authentication and authorization. Each service and cluster derives access rights per user based on the information provided by the authorization layer. Some users may be banned from some services and capabilities of the solution.

9. **Multi-tenancy** - The multi-tenancy solution built in the authentication and authorization layer, allows supporting multiple applications as well as multiple tenants, securely and in isolation of one another on a single infrastructure.
10. **SSL Communication** - All communication is secured over an AES encrypted link. This includes all inbound and outbound communication, be it HTTP or SSH.

11. **Web and Mobile Clients** - All clients will access the system via a common API interface. This includes a web application, iOS application and Android application. The API uses authentication tokens to ensure only authorized users get access to the platform.

12. **Terminal Admin** - Access to console and administration of applications server and services over an SSH interface.

13. **Payment Platforms** - Support for multiple payment platforms. Payment platforms support is available both on client devices and applications server. Currently supported payment platforms allow for PCI DSS SAQ-A compliance, thus reducing system certification process complexity and risk, and onboarding of businesses to the system.
**High-Level Process Design**

The solution architecture allows for multi-tenancy with multiple application support, where each application and tenant’s data is isolated, yet allows communication and administration across applications. The multi-tenancy architecture allows a single clustered backend instance to serve multiple customers. This allows for more flexible scaling as well as more rapid development and deployment of new features.