JioCloud

Managed Key Management Service

Overview

JioCloud's Managed KMS (Key Management Service) offers a modern, cloud-native approach to key management. With on-demand provisioning, scalable architecture, and intuitive self-service interfaces, our solution helps businesses to manage cryptographic keys seamlessly across applications, databases, and workloads. JioCloud KMS removes the complexity of manual key handling, ensuring compliance, agility, and cost efficiency.

Key Features

- **Secure key account management**
  Enables rapid account provisioning and creation, storage and management of keys with seamless automation.
- **API-driven Integration**
  REST APIs enable smooth integration with cloud-native and enterprise applications.
- **FIPS Certified**
  Enterprise Key Management as a Service provides compliance with FIPS 140-2 Level 1
- **Role-Based Access Controls (RBAC)**
  Provides fine-grained access control for account admins and users.
- **Tenant-aware design**
  Logical isolation of key associated with respective user accounts ensures secure multi-tenancy.
- **Observability**
  Built-in dashboards monitors historical key activity patterns.
- **High availability deployment**
  Clustering ensures continuous availability and minimal downtime.

JioCloud

Benefits

- **Agility**
  Simplified integration with applications via APIs, reduces developer friction.
- **Security:**
  Keys never leave the secure environment, ensuring trust and compliance.
- **Compliance**
  Meets industry regulations such as NIST, HIPAA, GDPR.
- **Efficiency**
  Centralized control prevents key sprawl and reduces operational overhead.
- **Scalability**
  Expands seamlessly across various enterprise workloads.

Technologies Supported

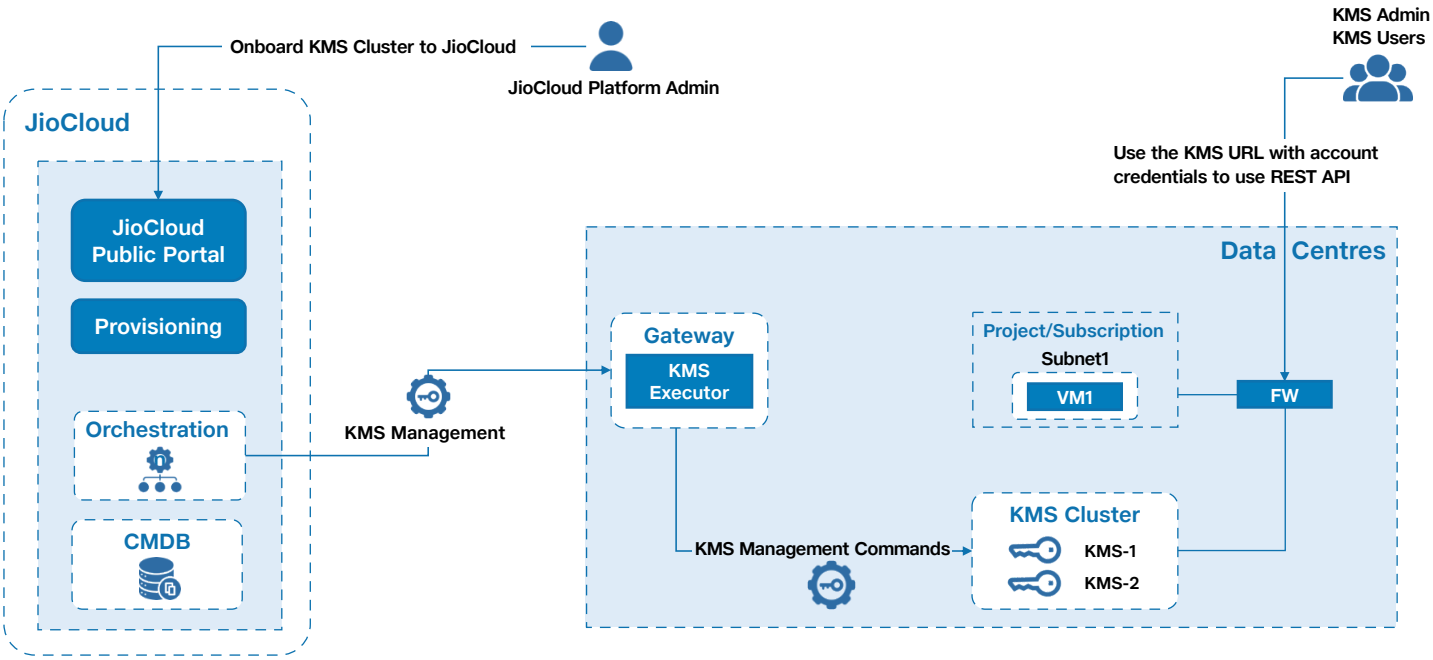
Operating Systems	Windows, Linux
Frameworks	Spring Boot, .NET Core, microservices architectures
APIs and Protocols	REST, KMIP (Optional)
Cloud Integrations	Jio Azure, On-Prem environments

Technical Specifications

Specification	Details
API Support	REST APIs
Key Algorithms	AES, RSA-2048, 3072,4096
Compliance	NIST, HIPAA, GDPR, ISO/IEC 27001,

JioCloud

Architecture Diagram



Use Cases

- **Application Layer Encryption**
  Secure storage of sensitive data by integrating KMS in applications and databases.

- **Audit-ready compliance**
  Security teams rely on built-in logs and monitoring tools to prepare for audits, flag anomalies, and enforce governance policies.

- **High availability by default**
  Clustered deployment within a zone ensures your keys remain accessible and secure even during system updates or node-level infrastructure issues.