FIPS-Compliant
Apache CloudStack

Federal-Grade, Cryptographically Validated
Cloud Infrastructure

The FIPS-compliant version of Apache CloudStack is a ShapeBlue-maintained distribution designed for highly regulated environments. It enforces NIST CMVP-validated cryptographic modules and algorithms across the stack - covering TLS, SSH, key management, and internal services.
Ideal for government, defense, finance, healthcare, and critical infrastructure, this release provides secure-by-design private cloud deployments, eliminating weak ciphers, enforcing trusted algorithms, and reducing audit and regulatory risk.

In short: CloudStack becomes secure-by-design not by policy exception.

Why FIPS Compliance Matters?

Regulatory Compliance

Enables deployment in FIPS-mandated environments (Government, Defense, Healthcare, Finance).

Operational Integrity

Enforces consistent crypto behavior across hosts, VMs, APIs, and databases.

Security Maturity

Removes legacy crypto (MD5, SHA-1, RC4) ➜ reduces data breach surface.

Customer Confidence

Demonstrates alignment with NIST, ISO 27001, and FedRAMP expectations.

Audit Readiness

Simplifies compliance reporting with validated module IDs (Bouncy Castle #4943 / OpenSSL #4985).
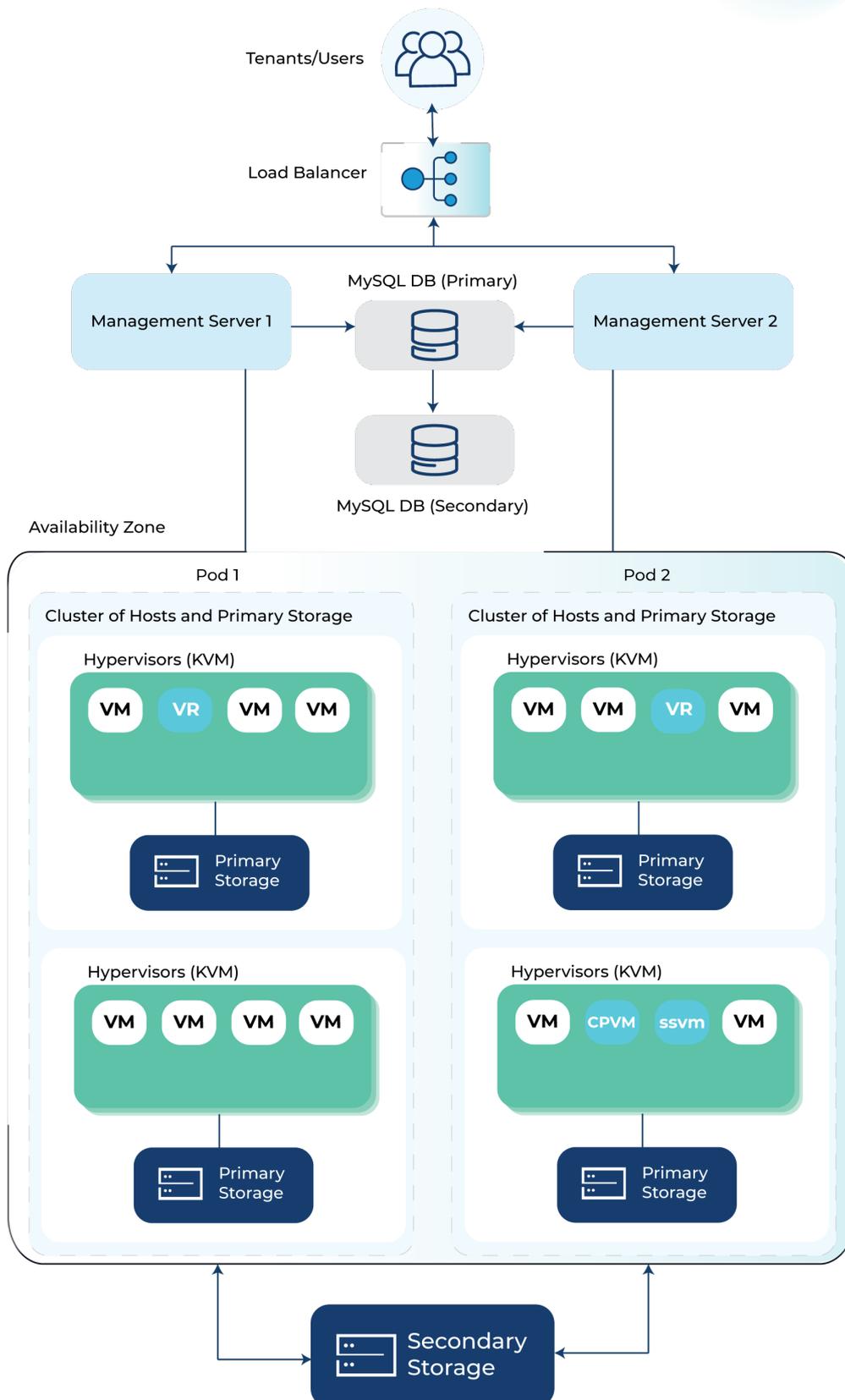
Key Technical Enhancements

Area	Standard CloudStack	FIPS-Compliant CloudStack	Business Benefit
Crypto Modules	Generic Java & OpenSSL libraries	FIPS-validated modules (Bouncy Castle FIPS, OpenSSL FIPS)	Meets federal crypto validation.
Encryption Standards	MD5, SHA-1, RC4 supported	AES, SHA-2/3, RSA, ECDSA only	Eliminates weak ciphers.
Authentication	PBKDF2-SHA1 / SAML2 / plaintext options	PBKDF2-SHA256, TLS only	Stronger credential protection.
Protocols	TLS 1.0–1.2 allowed	TLS 1.2 only, restricted ciphers	Enforced secure channels.
System VM Templates	Non-FIPS Debian	FIPS-kernel Debian 12.11	End-to-end crypto integrity.
Database	No FIPS control	MySQL ssl_fips_mode=STRICT	Data-in-transit + at-rest secured.
Upgrade Path	Self-managed	Via Shapeblue consultancy only	Maintains validation integrity.

FIPS-Compliant CloudStack transforms an open-source cloud orchestrator into a certifiable, security-governed infrastructure platform suitable for regulated industries. It reduces risk, accelerates compliance, and establishes a secure operational baseline without sacrificing CloudStack's flexibility or scalability.
It is ideal for government, defense, finance, healthcare, and critical infrastructure, this release provides secure-by-design private cloud deployments, eliminating weak ciphers, enforcing trusted algorithms, and reducing audit and regulatory risk.

CloudStack architecture, augmented with a cryptographic boundary indicating where FIPS enforcement applies across the deployment

Tenants/Users

Load Balancer

Management Server 1

MySQL DB (Primary)

Management Server 2

MySQL DB (Secondary)

Availability Zone

Pod 1

Cluster of Hosts and Primary Storage

Hypervisors (KVM)

VM | VR | VM | VM

Primary Storage

Hypervisors (KVM)

VM | VM | VM | VM

Primary Storage

Pod 2

Cluster of Hosts and Primary Storage

Hypervisors (KVM)

VM | VM | VR | VM

Primary Storage

Hypervisors (KVM)

VM | CPVM | ssvm | VM

Primary Storage

Secondary Storage

Strategic Benefits

- Compliance-ready foundation for FIPS 140-3 / NIST / FedRAMP environments
- Unified cryptographic enforcement across all layers (API   VM   storage).
- Simplified audits with verifiable crypto configurations and traceable module IDs.
- Predictable operations with validated OS and Java runtimes.
- Competitive trust advantage as an enterprise-secure cloud platform.

Implementation Path

1. Pilot / Beta Validation – Deploy in test environment using Oracle Linux 8/9 or Ubuntu 20.04 Pro.

2. Security Review – Align deployment with organization's FIPS or NIST control mapping.

3. Consultancy Engagement – Engage Shapeblue for production rollout, compliance attestation, and future upgrade planning.

Exclusive for ShapeBlue's Customers

The FIPS-validated CloudStack is available exclusively through ShapeBlue, due to ongoing specialized maintenance, security updates, and compliance monitoring. ShapeBlue ensures continuous adherence to FIPS standards, providing a high level of support and assurance for organizations with strict regulatory or contractual obligations.
This guarantees a secure, compliant, and fully supported private cloud platform in sensitive, highly regulated environments.