Cloud Maturity Model
Security & Compliance

Adoption Path for

VMware Cloud Foundation 5.2

vmware by Broadcom

Table of Contents

Maturity Stage 1: Identity and RBAC

3rd Party Identity Federation

Federation with modern identity providers enables single sign-on (SSO) across multiple applications and services while centralizing user authentication, access policies, and credential management in one trusted system. This approach not only improves security by enforcing consistent authentication methods and access controls, but also enhances user experience by eliminating the need for multiple passwords while providing features like multi-factor authentication, automated user provisioning, and detailed access audit logs.

- Identity Federation in vSphere and Cloud Foundation
- Role-Based Access Control in vSphere and Cloud Foundation

Maturity Stage 2: Auditing and SIEM

System Hardening: Running a Safe and Compliant Cloud

System hardening is the methodical process of strengthening a computer system's security posture by reducing its attack surface through configuration changes, removing unnecessary services, and applying security controls. The process typically involves disabling default accounts, closing unused network ports, implementing strict access controls, keeping systems updated with security patches, and following security best practices specific to the operating system and application stack in use.

- Security Configuration & Hardening Guides
- Maintaining Compliance with vRealize Operations
- Configuring Compliance in VCF Operations Documentation
- Try the Hands on Lab - Module 4 - Running a Safe and Compliant Cloud

System Hardening: Network Security

VMware Aria Operations for Networks streamlines microsegmentation planning by analyzing existing network traffic patterns and automatically recommending security rules based on observed application behavior and dependencies. The platform's application-centric approach allows security teams to visualize communication flows between workloads, simulate proposed security policies before deployment, and gradually implement zero-trust security through iterative refinement of microsegmentation rules based on real traffic analysis.

- VCF Operations for Networks - Micro-Segmentation Planner

System Hardening: Crown Jewel Analysis

VMware Aria Operations for Networks helps security teams identify and protect critical assets ("crown jewels") by mapping application dependencies and analyzing network traffic patterns to understand which systems handle sensitive data or support essential business functions. The platform's analytics capabilities reveal the connections, access patterns, and potential attack paths to these high-value targets, enabling organizations to implement additional security controls and monitor for suspicious activities around these critical systems.

- VCF Operations for Networks Crown Jewels

Maturity Stage 2: Auditing and SIEM

Auditing and Logs: Audit Events

VMware Aria Operations for Logs (formerly vRealize Log Insight) is a centralized log management solution that provides real-time log analytics and monitoring capabilities across physical, virtual, and cloud environments. The platform includes built-in audit event monitoring functionality that allows administrators to track and set up automated alerts for security-relevant events like login attempts, configuration changes, and permission modifications across their VMware infrastructure.

- Custom Alerts in VMware Cloud Foundation Operations
- September 2024 TAM Customer Webinar - VCF Operations 8.18 What's New / Diagnostics

Auditing and Logs: Event Forwarding To 3rd Party

Organizations often forward logs from Aria Operations for Logs to third-party SIEM solutions to maintain a unified security operations view across their entire technology stack and meet compliance requirements that mandate centralized log retention and analysis. This integration allows security teams to correlate VMware infrastructure events with other security telemetry in their SIEM platform, enabling better threat detection and incident response while leveraging existing security workflows and automation.

- VMware Cloud Foundation Operations Improves Security and Compliance Posture with Audit Events

Maturity Stage 3: Constraint Based Management

Regulatory Compliance: Network Compliance

VMware Aria Operations for Networks (formerly vRealize Network Insight) is a network monitoring and analytics platform that provides deep visibility into network traffic, security policies, and compliance status across physical and virtual networks. It helps maintain compliance by automatically monitoring network segmentation, tracking configuration changes, validating security group policies against compliance requirements, and providing detailed audit trails of network modifications and security policy changes.

- VCF Operations for Networks - PCI Compliance Dashboard
- VCF Operations for Networks - PCI Compliance Dashboard Demo

Maturity Stage 4: Data Governance

Data Governance: Access Control

Data governance through access control ensures organizations can protect sensitive information by precisely managing who can view, modify, and delete data across their infrastructure, while maintaining comprehensive audit trails of all access attempts and changes. Implementing granular access controls as part of a data governance strategy helps organizations meet regulatory compliance requirements, prevent unauthorized data exposure, and maintain the principle of least privilege where users only have access to the specific data they need to perform their roles.

- Role-Based Access Control in vSphere and Cloud Foundation

Maturity Stage 5: Compliance Enforcement

Password Lifecycle Management: Password Rotation & Best Practices

Regular password rotation helps protect systems by limiting the window of time that compromised credentials can be exploited, and ensures that if passwords are exposed through breaches or unauthorized access, they become invalid before attackers can effectively use them. That said,

modern security guidance from NIST and other authorities increasingly favors strong, unique passwords combined with multi-factor authentication over mandatory rotation policies, as frequent password changes can lead users to choose weaker passwords or resort to predictable patterns.

- Remediate, Update, and Rotate Passwords in VMware Cloud Foundation

Certificate Lifecycle Management: Installation, Rotation, and Best Practices

TLS certificate lifecycle management ensures trusted communication channels by maintaining the integrity and authenticity of digital certificates that validate server identities and encrypt sensitive data between systems. A robust certificate management program builds and preserves trust across the digital ecosystem by systematically monitoring, renewing, and replacing certificates before expiration, while maintaining a comprehensive inventory to prevent trust-breaking outages that can damage relationships with users and business partners.

- Replace Certificates in a VMware Cloud Foundation Private Cloud

Data-in-Transit Protections: FIPS and Network Encryption

Transport Layer Security (TLS) is a cryptographic protocol that provides secure communication between systems over networks by using digital certificates and encryption to verify identities and protect data in transit. FIPS 140-3 is a U.S. government security standard that specifies requirements for cryptographic modules, ensuring they meet rigorous testing and validation requirements for use in securing sensitive but unclassified information in federal systems and other regulated industries.

- FIPS 140-2/140-3 Q&A
- FIPS 140-2 & 140-3 Validated Cryptographic Modules
- TLS, Cipher Suites, and TLS Profiles