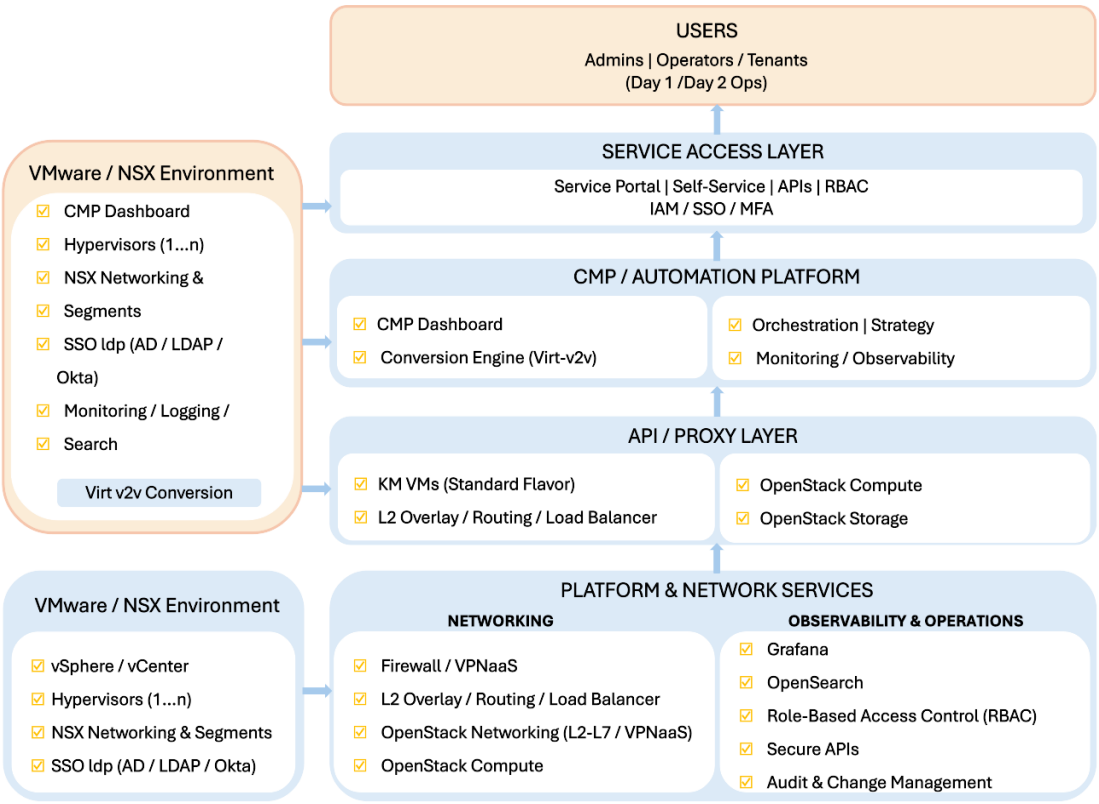
XaasIO VMware Exit Assessment Overview v1.0

Table of Contents

1. Executive Summary

The XaasIO VMware Exit Assessment is a structured engagement that delivers a migration blueprint and an execution-ready plan to transition workloads from VMware vSphere/vCenter (and optional vSAN/NSX) to upstream OpenStack (KVM virtualization).

This assessment focuses on discovery, dependency mapping, target architecture, component mapping, IAM/SSO/MFA readiness, operations, and wave-based cutover planning, ensuring a predictable migration from pilot to production with validation and rollback readiness.



Outcomes at a glance

- Clear view of the VMware estate: inventory, utilization, constraints, dependencies
- Target OpenStack landing zone blueprint: compute, storage, networking, HA
- Security and identity design: AD/LDAP + SSO (Okta/Azure AD) + MFA policy
- Wave plan: pilot -> non-critical -> core production, with cutover and rollback
- Day-2 readiness: monitoring, logging, operational runbooks, knowledge transfer (KT)

Key takeaway: This is a blueprint-first program designed to reduce risk, control downtime, and establish an operational foundation for OpenStack at scale.

2. Purpose

The purpose of this assessment is to build an actionable, risk-managed plan for VMware exit and migration to OpenStack, enabling controlled migration with defined acceptance gates, replacement mapping for VMware features, a secure enterprise identity model, and Day-2 operational readiness.

3. Objectives

- Perform structured discovery of the VMware estate and application landscape
- Identify workload readiness, risks, and migration constraints
- Design the OpenStack landing zone and operating model
- Produce a wave-based migration plan with testing, validation, and rollback
- Define component-by-component mapping (VMware -> OpenStack + XaasIO modules)
- Establish IAM integration (AD/LDAP), SSO (Okta/Azure AD), and MFA requirements
- Provide operational readiness outputs: monitoring, logging, runbooks, and KT

4. Scope of Assessment

4.1 VMware Estate Discovery

- vCenter inventory: clusters, hosts, resource pools, datastores, templates, VM list
- Compute utilization: CPU/RAM over time, peak headroom, growth trends
- Storage profile: vSAN or external storage, datastore layout, policy model, performance baseline
- Networking: VLAN/overlay topology, routing, firewall/LB/VPN functions, NSX constructs (if used)
- VM hygiene: snapshots, VMware tools status, guest OS mix, criticality classification, backup tags

4.2 Workload and Application Readiness

- Categorization: non-critical vs core production; stateful vs stateless; Windows/Linux; regulated vs general workloads
- Dependency mapping: east-west flows, north-south entry points, shared services (DNS/DHCP/NTP), backups, monitoring, CMDB integrations
- External integrations: SaaS/APIs/third-party connectivity, licensing constraints, hard-coded IP dependencies (if any)

4.3 Identity, Access, and Security Readiness (Enterprise IAM)

- Current identity sources: Active Directory / LDAP and existing access model
- Target design: AD/LDAP integration, SSO via Keycloak with Okta/Azure AD, and MFA policy definition
- RBAC model across OpenStack services and platform tooling; privileged access approach for administrators
- Security requirements: audit logging, retention, and security controls alignment

4.4 Operations and Observability Readiness

- Current monitoring/logging stack, alerting workflows, and incident response procedures
- Target approach: dashboards, alert tuning, SLO/SLA alignment, centralized log analytics and retention
- Standard operating procedures (Day-0/Day-2), escalation matrix, and operational handover plan

4.5 Compliance and Governance (Optional)

- Governance and evidence model (audit logs, change approvals, validation evidence) aligned to regulated environments, where applicable.

5. Methodology

Phase 1: Kickoff and Data Collection

- Stakeholder alignment and success metrics
- Access readiness planning (read-only preferred)
- Collection of VMware/network/security artifacts

Phase 2: Discovery and Baseline

- Inventory extraction and utilization baseline
- Workload grouping and readiness scoring
- Identification of constraints, risks, and quick wins

Phase 3: Target Blueprint and Component Mapping

- Target OpenStack blueprint (compute, storage, network, IAM, HA)
- Component mapping: ESXi -> KVM (Nova), vCenter -> OpenStack APIs + XaasIO CMP, NSX -> OpenStack networking + NFV modules
- IAM mapping: Keycloak with AD/LDAP + SSO + MFA; RBAC across platform services

Phase 4: Migration Wave Plan (Pilot -> Production)

- Wave definition: pilot wave, non-critical waves, core production waves
- Cutover planning: virt-v2v approach, change windows, validation gates, stakeholder sign-off
- Rollback plan and acceptance criteria

Phase 5: Operationalization and Handover

- Stabilization plan and Day-2 runbooks
- Knowledge transfer (KT) sessions and operating model alignment
- Go/No-Go checklist for production readiness

6. Deliverables

6.1 VMware Estate Assessment Report

- Environment summary and inventory
- Utilization trends and growth assumptions
- Risks, constraints, and readiness findings

6.2 OpenStack Target Blueprint

- Logical architecture: compute, storage, networking, HA model
- IAM architecture: AD/LDAP integration + SSO + MFA
- Operational architecture: monitoring/logging/alerting and runbooks

6.3 VMware -> OpenStack Component Mapping

- Feature mapping with gap analysis and mitigations
- Network equivalence plan (NSX replacement strategy, if applicable)

6.4 Wave-Based Migration Plan

- Workload grouping and sequencing
- Cutover approach, test plan, validation gates, and sign-off workflow
- Rollback readiness plan

6.5 Execution Readiness Pack

- Cutover and rollback checklist templates
- Day-2 operations runbook outline
- RACI (roles and responsibilities) and escalation plan
- Knowledge transfer plan (KT sessions)

6.6 Optional Compliance Annex

- Governance workflow and evidence plan for regulated workloads

7. Customer Inputs Required

7.1 VMware and Infrastructure

- VMware products/SKUs in use: vCenter, vSAN, NSX, etc.
- Deployment type: HCI vs external storage datastores
- Network details: VLAN/overlay, NSX constructs (if used), firewall/LB/VPN
- Backup/DR approach: RPO/RTO targets, tooling, DR dependencies
- Performance baselines (if available)

7.2 Identity and Security

- AD/LDAP details (domains, OU structure, groups, privileged users)
- SSO provider overview: Okta / Azure AD (authentication flow, policies)
- MFA requirement scope: admins only vs all users; step-up policies
- Security requirements: audit logging, retention, endpoint agents, compliance controls

7.3 Operations

- Monitoring/logging tools and incident workflow
- Maintenance window policy and change management approach
- Stakeholder mapping: workload owners, approvers, operations leads

8. Typical Timeline (Indicative)

- Kickoff and data collection: 2-5 business days
- Discovery and analysis: 1-2 weeks
- Blueprint, mapping and wave plan: 1-2 weeks
- Final report and readout: 2-3 business days

9. Roles and Responsibilities

9.1 Customer

- Provide access, documentation, and SMEs (VMware/network/security/application owners)
- Confirm workload criticality and validate dependencies
- Participate in testing, approvals, and sign-off gates

9.2 XaasIO Solutions Architecture Team

- Execute discovery and analysis
- Produce blueprint, mapping, wave plan, and readiness artifacts
- Define cutover approach, validation, and rollback methodology
- Lead readout and knowledge transfer sessions

10. Assumptions and Constraints

- The assessment produces an execution blueprint; production migration execution is a separate phase.
- Adequate access is provided for discovery (read-only preferred).
- Workload owners participate in dependency validation and sign-offs.
- Legacy OS and licensing constraints are documented with mitigations and exceptions.

11. Next Steps

- Schedule kickoff session (stakeholder alignment and access readiness)
- Confirm scope: number of clusters/VMs, NSX/vSAN usage, priority applications
- Enable discovery access (vCenter/NSX read-only or exports)
- Begin baseline and inventory capture
- Deliver draft blueprint and mapping for review
- Finalize wave plan and execution readiness pack

XAASIO VMWARE EXIT ASSESSMENT OVERVIEW

Discover how XaasIO enables a secure and structured transition from VMware to OpenStack.

Book a demo at https://xaasio.com/contact/

AMERICAS

+1 650 523 6628

EMEA

+44 20 3031 1074

APAC

+91 93423 61010