XaasIO Component Mapping Brief v1.0

Table of Contents

1. Purpose

This Component Mapping Brief provides a practical mapping of commonly used VMware stack components - ESXi/vCenter, NSX, SRM, and VMware Aria (vRealize) - to functional equivalents in upstream OpenStack (KVM) and XaasIO platform modules (CMP, Automation, Observability, IAM/SSO/MFA, and DR orchestration).

2. Mapping Principles

Blueprint-first: assess current VMware usage and map only the features actually used.

Upstream-first: prioritize upstream OpenStack APIs and open standards to avoid new lock-in.

Operational readiness: replacement is not complete until monitoring, logging, RBAC, and runbooks are in place.

Wave-based migration: pilot -> non-critical -> production, with rollback readiness.

Security by design: integrate AD/LDAP + SSO (Okta/Azure AD) + MFA early in the program.

3. High-Level Mapping Summary

ESXi hypervisor -> KVM (OpenStack Nova compute)

vCenter & vSphere management -> OpenStack APIs + Horizon + XaasIO CMP (portal/API)

NSX -> OpenStack Neutron + L2/L3 services + Security Groups + Firewall/LB/VPN modules (as required)

SRM -> XaasIO DR orchestration + OpenStack-aware DR runbooks (replication approach per design)

VMware Aria (vRealize) -> XaasIO CMP + Automation (Ansible/IaC) + Observability (Grafana/Zabbix/OpenSearch)

4. Detailed Component Mapping

4.1 ESXi / vCenter (Compute & Core Virtualization)

What VMware Provides

- Hypervisor virtualization (ESXi)
- Central management via vCenter
- VM lifecycle management (create, clone, templates)
- Clusters, resource pools, operational controls (HA/DRS-style patterns)
- Roles/permissions and audit trails

OpenStack + XaasIO Equivalent

- Upstream OpenStack: Nova (Compute) with KVM, Placement (scheduling), Glance (images), Cinder/Ceph (block), Horizon (UI), Keystone (RBAC).
- XaasIO: CMP / self-service portal & API for tenant onboarding, quotas, catalogs, and approvals.
- XaasIO Automation: Ansible/IaC runbooks for provisioning, patching, scaling, and Day-2 workflows.

Notes / Considerations

- OpenStack is API-centric; Horizon and CMP provide operator and tenant experiences.
- DRS-like outcomes are achieved using scheduling policies, host aggregates, flavors, and operational SOPs.

4.2 NSX (Network Virtualization & Security)

What VMware Provides

- Overlay networking, logical switching/routing
- Micro-segmentation and distributed firewall
- NAT, load balancing, VPN (depending on edition)
- Network policies, segments, groups, and security constructs

OpenStack + XaasIO Equivalent

- Upstream OpenStack: Neutron (L2 networks, subnets, routers, NAT, floating IPs) and Security Groups (stateful firewall rules).
- XaasIO Networking & NFV modules (as required): advanced L4-L7 services such as LB (Octavia), VPN, and firewall/policy engines aligned to enterprise requirements.
- Segmentation approach: security groups + project separation + network segmentation (VLAN/overlay) with optional advanced policy enforcement based on customer standards.

Notes / Considerations

- NSX replacement is designed based on actual NSX feature usage (overlay only vs firewall vs LB vs VPN).
- For regulated environments, governance and evidence mapping can be included as an optional annex.

4.3 SRM (Site Recovery Manager / DR Orchestration)

What VMware Provides

- Recovery plans and DR runbook orchestration
- Failover/failback workflows
- Protection groups, testing, and recovery automation
- Replication integration (vSphere replication or array-based replication)

OpenStack + XaasIO Equivalent

- XaasIO DR orchestration: OpenStack-aware recovery runbooks with dependency ordering, validation steps, and controlled failover/failback workflows.
- Replication approach depends on storage design: Ceph-based replication patterns, storage-array replication integration, or backup-based recovery where replication is not available.
- Assessment outputs include DR blueprint and recovery test plan aligned to target RPO/RTO.

Notes / Considerations

- DR equivalency depends on RPO/RTO targets, storage type (HCI vs external), and network reachability between sites.

4.4 VMware Aria (vRealize Suite)

What VMware Provides

- Operations monitoring and analytics (vROps)
- Automation and service catalog (vRealize Automation)
- Centralized log analytics (Log Insight)
- Dashboards, alerting, reporting, and capacity views

OpenStack + XaasIO Equivalent

- XaasIO CMP: self-service catalog, approvals, quotas, tenant views, governance workflows.
- Automation layer: Ansible/IaC workflows for provisioning, patching, configuration, and DR actions.
- Observability: Grafana dashboards, Zabbix monitoring/alerting, OpenSearch for log analytics and retention.

Notes / Considerations

- Replace Aria outcomes with CMP + automation + observability integrated to customer incident and change processes.

5. Identity & Access Mapping (Applies Across All Components)

- XaasIO standardizes access across CMP, OpenStack Horizon/APIs, automation, and observability using Keystone RBAC and Keycloak for enterprise SSO and MFA.
- Keystone RBAC for OpenStack service access control.
- Keycloak for AD/LDAP integration, SSO (Okta/Azure AD), and MFA enforcement (admin-only or all users, including step-up policies).
- Unified audit and access posture across platform services.

6. Typical Gaps & Mitigation (Example)

VMware Capability	OpenStack/XaasIO Approach	Mitigation / Notes
NSX micro-segmentation (advanced)	Security groups + segmentation + optional policy engines	Map actual rule sets; validate east-west controls
SRM with array replication	XaasIO DR runbooks + storage replication design	Choose replication method per storage architecture and RPO/RTO
DRS-style automation	Scheduling policies + host aggregates + flavors + SOPs	Define placement policies; automate common remediation
Aria unified suite	CMP + automation + observability	Integrate alerts/runbooks; define ownership/RACI

7. Outputs of the Component Mapping Brief

- Feature usage summary (what is used today across ESXi/vCenter/NSX/SRM/Aria).
- Mapping matrix for each component (functional equivalence plus gaps).
- Target architecture overlays (network, identity, observability, DR).
- Wave-plan implications (what migrates first and why).
- Operational readiness checklist (Day-1/Day-2 readiness and sign-offs).

8. Next Steps

- Confirm VMware components in active use (NSX features, SRM mode, Aria modules).
- Capture inventories and configurations (exports, DR plans, dashboards).
- Produce the final mapping matrix and architecture blueprint.
- Validate with network, security, and operations teams.
- Finalize wave plan, cutover checklists, and runbooks.

Addendum: Pets vs Cattle Architecture Shift (VMware -> OpenStack)

A.1 Conceptual Model

VMware (often operated as 'pets')

- Long-lived instances, frequently hand-tuned and changed in-place.
- VM identity and placement matter; troubleshooting often means logging into the VM and fixing it.
- Higher risk of configuration drift and slower repeatability during DR and migrations.

OpenStack (operated as 'cattle')

- Instances are replaceable and standardized; changes prefer rebuild/replace over manual edits.
- Clear separation of Image (golden template), Flavor (hardware profile), Network policy (ports/security groups), and persistent volumes.
- Automation and APIs are first-class; operations emphasize repeatability and policy.

A.2 Flavor-Based Operations (Key OpenStack Difference)

- In OpenStack, the standard compute profile is defined by a Flavor (vCPU, RAM, disk, and optional extra specs such as CPU pinning, hugepages, NUMA, and performance profiles).
- Scale and standardize using an approved flavor catalog rather than per-VM custom sizing.
- Use host aggregates / availability zones to enforce placement policies.
- Improve capacity planning and showback/chargeback using flavors as cost units.

A.3 Images and Immutable Patterns

- Adopt golden images (Glance) with hardening, baseline agents, and versioned image lifecycle.
- Use cloud-init and configuration management for deterministic initialization.
- Rebuild/replace for major changes to reduce drift and improve repeatability.

A.4 Day-2 Operations: Runbook Changes

- Runbooks shift from per-VM firefighting to policy + automation + standard workflows.
- Common runbooks: resize by flavor with validation; rebuild from hardened image; reattach volumes; rotate credentials; enforce MFA for privileged ops.

A.5 Storage and State (Persistent vs Ephemeral)

- Keep compute ephemeral where possible; keep state in persistent storage (Cinder/Ceph, databases, object storage).
- Enables rebuild-based patching and DR: rebuild compute and attach replicated volumes (per DR design).

A.6 Governance and Control

- Enforce governance through tenant/project boundaries, quotas, flavor approvals, network policies, RBAC, and audit logging.
- Shift ops model toward standardization, automation, and controlled exceptions.

XAASIO COMPONENT MAPPING BRIEF

Structured VMware-to-OpenStack component mapping with gap analysis and mitigation planning.

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

AMERICAS

+1 650 523 6628

EMEA

+44 20 3031 1074

APAC

+91 93423 61010