XaasIO Day-2 Operations Runbook (Sample) v1.0

Table of Contents

1. Operating Model (Day-2)

Day-2 operations focus on keeping the platform reliable, secure, and consistent after go-live. XaasIO recommends a 'cattle' model for instances: standard flavors + golden images + automation-first runbooks, with state kept in persistent services/volumes where possible.

- Primary interface: XaasIO CMP portal/API and OpenStack APIs; CLI for break-glass operations.
- Change management: tickets for production changes; documented approvals for networking/IAM/security changes.
- Automation: IaC/Ansible workflows preferred over manual in-instance changes to reduce drift.
- SLO/SLA: monitor availability, latency, and error rates at service level; capacity at infrastructure level.

1.1 Key Day-2 Objectives

- Maintain platform and workload availability and performance
- Minimize configuration drift using golden images + rebuild patterns
- Apply patches and security updates safely
- Ensure monitoring/logging/auditing are continuously healthy
- Perform predictable scaling using flavor catalog and horizontal scale patterns
- Operate backup and DR with regular testing

2. Access, RBAC, and Security Operations

Access should be unified and auditable using Keystone RBAC and Keycloak (AD/LDAP, SSO, and MFA). Operational tasks must follow least privilege with break-glass procedures.

Role	Typical Permissions (Example)
Tenant Admin	Project quotas, security groups, VM lifecycle, volume attach/detach
Operator (NOC)	Read-only dashboards/logs; restart services per runbooks; open incidents
Platform Admin	Hypervisor/compute scheduling, network backends, storage backends, upgrades
Security Admin	IAM policies, MFA enforcement, audit log review, key rotation

2.1 Break-Glass Procedure (Sample)

- Open incident and document reason for elevated access.
- Use time-bound privileged role (MFA enforced).
- Perform action, capture evidence, and revert privileges.
- Post-incident review with audit logs.

3. Standard Catalogs (Flavors, Images, Networks)

3.1 Flavor Catalog Operations

- Maintain a controlled flavor catalog (general purpose + performance flavors).
- Use host aggregates/AZs to enforce placement policies (e.g., performance, compliance).
- Changes to flavors require CAB approval in production.

Flavor Type	Examples	When to Use
General Purpose	m1. small/medium/large	Most application workloads
Performance	perf. * (CPU pinning/hugepages)	Low latency / high throughput requirements
Special	gpu. * / io. *	GPU workloads or storage-intensive workloads (if applicable)

3.2 Golden Image Lifecycle (Glance)

- Define image build pipeline (hardening, baseline agents, cloud-init).
- Version images (e.g., app-base-v2026.02) and deprecate old versions with timelines.
- Rebuild instances for major patch cycles (preferred) to minimize drift.
- Maintain rollback images for emergency restoration.

3.3 Network & Security Group Baselines

- Standardize security groups by app tier (web/app/db) with least privilege.
- Use project segmentation and network separation to enforce blast radius.
- Maintain change-controlled firewall/LB/VPN configurations and backout plans.

4. Observability Operations (Monitoring, Logging, Alerting)

- Monitoring: Zabbix (or equivalent) + Grafana dashboards for infra/service health.
- Logging: OpenSearch for centralized log search, retention, and audit support.
- Alerting: tiered alert policies (P1/P2/P3) with clear on-call routing.

4.1 Daily Checks (NOC)

- OpenStack control plane health: API availability, message queues, DB health (as per platform design).
- Compute capacity: hypervisor load, host availability, placement failures.
- Storage health: Ceph status, OSD warnings, pool utilization and latency.
- Network health: Neutron agents status, DHCP/L3/LB health, packet loss signals.
- Alert noise review: tune thresholds; close stale alerts.

4.2 Incident Triage (Sample Flow)

- Confirm scope: single VM vs tenant vs AZ vs control plane.
- Check dashboards/logs for correlated events (network, storage, compute).
- Apply standard runbook (restart agent, reschedule, evacuate host, etc.).
- Escalate to platform engineering if control-plane or repeated failures occur.
- Document RCA actions and follow-up remediation.

5. Common Day-2 Runbooks

5.1 Resize by Flavor (Standard Scaling)

Use resizing to change compute shape in a controlled manner. Prefer approved flavors. Validate application after resize.

- Confirm maintenance window (if required) and app owner approval.
- Select target flavor from catalog; confirm quota availability.
- Perform resize (CMP or OpenStack API).
- Confirm instance status and resource allocation.
- Run validation tests; monitor metrics for 30-60 minutes.
- If issues occur, revert to previous flavor within rollback window.

Sample OpenStack CLI (illustrative):

OpenStack server resize <VM> --flavor <FLAVOR>

OpenStack server resize confirm <VM>

5.2 Rebuild from Golden Image (Cattle Pattern)

Rebuild replaces the VM root disk from a golden image while keeping network identity; use with caution for stateful apps. Prefer boot-from-volume for stateful workloads.

- Confirm app supports rebuild (state externalized) or plan downtime.
- Snapshot/backup current state (if required).
- Rebuild from latest approved image.
- Reapply configuration via automation; validate monitoring/logging.
- Run functional tests and accept.

Sample OpenStack CLI (illustrative):

OpenStack server rebuild --image <IMAGE> <VM>

5.3 Host Maintenance / Evacuation (Compute)

- Use planned maintenance windows for hypervisor patching.
- Migrate/evacuate instances per policy; ensure capacity in target aggregates.
- After maintenance, return host to scheduler pool and validate metrics.

5.4 Network Policy Change (Security Groups / Firewall / LB)

- Open change ticket with business justification and port/protocol details.
- Apply changes in staging first; validate with app owner.
- Implement in production; capture evidence; verify no unintended exposure.
- Maintain backout plan and revert quickly if anomalies detected.

5.5 Volume Operations (Cinder/Ceph)

- Attach/detach volumes using standard procedures; validate filesystem mount points.
- Expand volumes: extend volume -> extend filesystem -> validate.
- Volume type policies: performance vs standard pools (as per design).

6. Patching, Vulnerability Management & Hardening

- Platform patching: follow vendor/upstream guidance; stage -> canary -> production rollout.
- Guest patching: prefer image-based updates for fleets; use automation for exceptions.
- Security baselines: CIS hardening, approved agents, key rotation schedules.
- Vulnerability scans and remediation SLAs aligned to severity (Critical/High/Medium/Low).

7. Backup & Disaster Recovery Operations

7.1 Backup Checks

- Daily backup success/failure review for all critical workloads.
- Periodic restore tests (monthly/quarterly) with evidence captured.
- Retention and immutability policies as required by compliance.

7.2 DR Drill (Sample)

- Select DR scope (pilot service) and schedule drill.
- Execute DR runbook: recovery order, dependencies, DNS/LB updates.
- Validate service; measure RTO/RPO; document results.
- Record improvements and update runbooks.

8. Capacity Management & FinOps (Optional)

- Track capacity by aggregate/AZ: vCPU, RAM, storage, IP pools.
- Use flavors as cost units for showback/chargeback (tenant usage reporting).
- Forecast growth and plan expansions with headroom thresholds.

9. Change Management & Compliance (Optional)

- All production changes are ticketed; evidence retained for audit (who/what/when/why).
- MFA enforced for privileged actions; periodic access reviews.
- Audit logs retained in OpenSearch as per policy.

9.1 Appendix A: Daily / Weekly / Monthly Checklist (Sample)

Frequency	Checklist Items (Examples)
Daily	Control plane health, capacity alarms, Ceph status, Neutron agent health, top incidents review
Weekly	Patch compliance report, image lifecycle review, alert tuning, backup success trend analysis
Monthly	Restore test, DR drill (selected), access review, capacity forecasting refresh

9.2 Appendix B: Standard Evidence Artifacts

- Change tickets, approvals, and backout steps
- Monitoring screenshots, logs, and incident timelines
- Patch reports and vulnerability remediation evidence
- Backup/restore and DR drill records

XAASIO DAY-2 OPERATIONS RUNBOOK (SAMPLE)

Streamline OpenStack Day-2 operations with structured runbooks, automation, and secure governance.

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

AMERICAS

+1 650 523 6628

EMEA

+44 20 3031 1074

APAC

+91 93423 61010