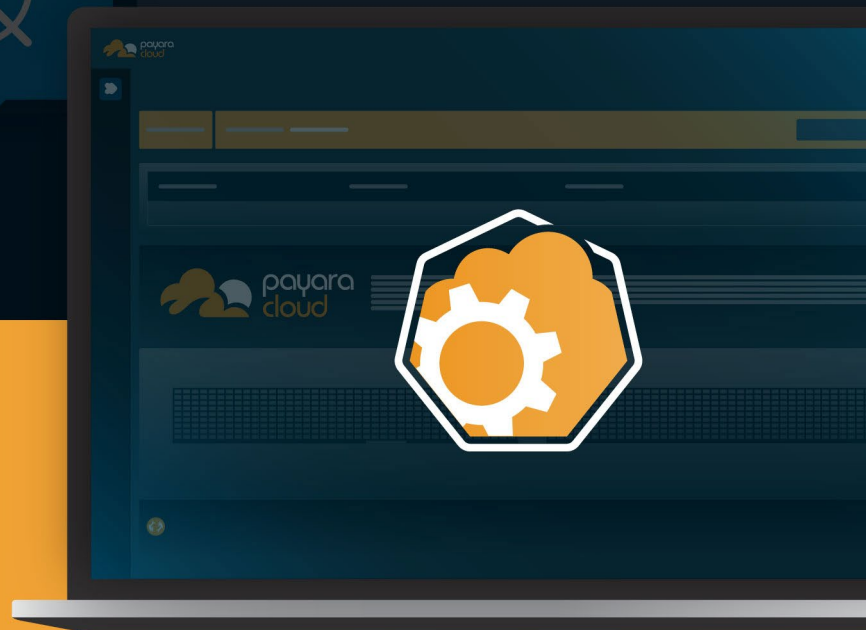




11 Kubernetes Operations Payara Cloud Eliminates for You



Contents

Guide Updated: **July 2025**

Introduction	1
1. Cluster Provisioning and Node Management	1
2. Kubernetes Version Management and Upgrades	1
3. Load Balancer and Application Gateway Configuration	2
4. DNS Management and SSL Certificate Provisioning	2
5. Security Policy Implementation and AppArmor Configuration	2
6. Comprehensive Monitoring Stack Setup	3
7. Ingress Controller Deployment and Configuration	3
8. Secret Management and Credential Rotation	3
9. Container Image Security and Vulnerability Scanning	4
10. Autoscaling Configuration and Resource Optimization	4
11. Disaster Recovery and Backup Orchestration	4
The Shift: Enabling Application Developers by Abstracting Infrastructure Complexity	5
Ready to Focus on Code Instead of Kubernetes?	6

Introduction

When developers first encounter Kubernetes (K8s), they're often drawn to its promise of scalable, resilient container orchestration. What they quickly discover is that K8s itself is just the foundation. Building a production-ready platform requires mastering dozens of interconnected systems, each introducing its own complexities and potential points of failure.

Payara Cloud eliminates this operational burden by providing a fully managed Jakarta EE and MicroProfile application deployment platform that automatically handles the entire K8s stack. Here are the 11 major K8s operations you'll never have to worry about again when you adopt Payara Cloud for your Jakarta EE production deployment.

1. Cluster Provisioning and Node Management

What your team is spared from: Manually creating K8s clusters using Terraform scripts or ARM templates, selecting appropriate node instance types, configuring node pools as well as managing the intricate relationship between cluster networking, storage and compute resources.

What Payara Cloud handles: Automatic cluster creation across Azure (AKS) and AWS (EKS) with configurations optimized specifically for Jakarta EE workloads. The platform intelligently selects node types, configures autoscaling policies, and manages node lifecycles including automated patching, upgrades and replacement of failed instances.

The complexity you avoid: Understanding the nuances of different cloud provider offerings, calculating optimal node-to-pod ratios, configuring cluster networking (CNI plugins, IP ranges, subnet allocation) as well as coordinating cluster upgrades across development, staging and production environments without breaking existing workloads.

2. Kubernetes Version Management and Upgrades

What your team is spared from: Planning and executing K8s version upgrades, which require careful coordination to avoid breaking changes, testing compatibility across all platform components as well as managing rolling upgrades across multiple clusters and environments.

What Payara Cloud handles: Automated K8s version management with intelligent upgrade orchestration. The platform tests new versions against representative workloads, implements staged roll-outs across regions, and maintains compatibility with all integrated components throughout the upgrade cycle.

The complexity you avoid: Reading through K8s changelogs to identify breaking changes, testing upgrade paths in isolated environments, coordinating upgrade timing across teams, and having rollback procedures ready when upgrades introduce unexpected issues.

3. Load Balancer and Application Gateway Configuration

What your team is spared from: Configuring cloud load balancers (Azure Application Gateway, AWS Application Load Balancer), setting up SSL termination, managing backend pools, configuring health checks, and integrating Web Application Firewall (WAF) protection.

What Payara Cloud handles: Automatic integration with cloud-native load balancing services, including SSL certificate management, intelligent routing rules and WAF configuration. The platform handles the complex integration between K8s' ingress resources and cloud load balancing infrastructure.

The complexity you avoid: Understanding the intricacies of cloud networking, configuring target groups and backend pools, managing SSL certificates across multiple endpoints, and troubleshooting load balancer misconfigurations that can take applications offline.

4. DNS Management and SSL Certificate Provisioning

What your team is spared from: Setting up external DNS controllers, configuring DNS zone permissions, managing SSL certificate provisioning through Let's Encrypt, handling ACME challenges, and ensuring certificate renewal before expiration.

What Payara Cloud handles: Complete DNS automation through External DNS integration with Azure DNS and Route53, automatic SSL certificate provisioning and renewal via Let's Encrypt, and seamless support for both wildcard certificates and custom domains.

The complexity you avoid: Debugging DNS propagation issues, configuring ACME challenge solvers (HTTP-01 vs DNS-01), managing certificate storage and distribution, and dealing with rate limiting from certificate authorities.

5. Security Policy Implementation and AppArmor Configuration

What your team is spared from: Designing and implementing multi-tenant security policies, creating AppArmor profiles for container isolation, configuring network policies for micro-segmentation, and managing service accounts with appropriate RBAC permissions.

What Payara Cloud handles: Automatic deployment of restrictive AppArmor profiles that limit filesystem access and system call permissions, intelligent network policy generation for application isolation, and managed identity integration that eliminates credential storage requirements.

The complexity you avoid: Understanding Linux security modules, writing AppArmor profiles that strike the right balance between security and application functionality, debugging network policy conflicts as well as designing RBAC hierarchies that follow the principle of least privilege.

6. Comprehensive Monitoring Stack Setup

What your team is spared from: Deploying and configuring Prometheus for metrics collection, setting up Grafana dashboards, configuring alerting rules, implementing log aggregation with tools like Fluent Bit or Fluentd, and integrating distributed tracing systems.

What Payara Cloud handles: Complete observability infrastructure including metrics collection with Jakarta EE-specific metrics, pre-built dashboards for immediate visibility, intelligent alerting based on application behavior, and automatic log enhancement with contextual metadata.

The complexity you avoid: Learning any observability platform query language, designing effective alerting rules that minimize false positives, configuring log parsing and routing as well as correlating metrics, logs and traces for effective troubleshooting.

7. Ingress Controller Deployment and Configuration

What your team is spared from: Selecting and deploying ingress controllers (Nginx, Traefik, HAProxy), configuring middleware for authentication and rate limiting, managing SSL termination as well as coordinating ingress rules across multiple applications.

What Payara Cloud handles: Automatic deployment and configuration of Traefik ingress controllers optimized for Jakarta EE applications, including pre-configured middleware for common requirements like authentication, rate limiting, and request transformation.

The complexity you avoid: Comparing ingress controller capabilities and limitations, writing complex ingress manifests with proper annotations, debugging routing issues, and managing ingress controller updates without breaking existing routes.

8. Secret Management and Credential Rotation

What your team is spared from: Implementing K8s Secrets management, configuring external secret management systems (HashiCorp Vault, Azure Key Vault), setting up automatic credential rotation, and ensuring secrets are encrypted at rest and in transit.

What Payara Cloud handles: Automated secret lifecycle management with encryption at rest using cloud provider key management services, automatic credential rotation following security best practices, and secure secret distribution without exposing credentials in logs or configuration files.

The complexity you avoid: Understanding different secret management approaches, implementing secret rotation without application downtime, debugging secret synchronization issues, and ensuring compliance with security policies around credential handling.

9. Container Image Security and Vulnerability Scanning

What your team is spared from: Setting up container image scanning pipelines, configuring vulnerability databases, implementing policies to prevent deployment of vulnerable images, and managing base image updates across multiple applications.

What Payara Cloud handles: Automated vulnerability scanning for all container images before deployment, maintenance of updated security threat databases, and prevention of deployments containing critical vulnerabilities.

The complexity you avoid: Evaluating different vulnerability scanning tools, interpreting scan results and prioritizing fixes, managing false positives, and coordinating security updates across development teams.

10. Autoscaling Configuration and Resource Optimization

What your team is spared from: Configuring Horizontal Pod Autoscaling (HPA) with appropriate metrics and thresholds, setting up Vertical Pod Autoscaling (VPA), implementing cluster autoscaling, and optimizing resource requests and limits across applications.

What Payara Cloud handles: Intelligent autoscaling that considers multiple metrics including CPU, memory, request queue depth and custom application metrics, with predictive scaling based on historical patterns and vertical resource optimization recommendations.

The complexity you avoid: Determining optimal scaling metrics and thresholds, preventing scaling conflicts between HPA and VPA, managing resource contention during scaling events, and balancing performance with cost optimization.

11. Disaster Recovery and Backup Orchestration

What your team is spared from: Designing backup strategies for persistent volumes, implementing cross-region replication, configuring disaster recovery procedures, testing backup integrity, and coordinating recovery processes across multiple components.

What Payara Cloud handles: Comprehensive disaster recovery capabilities including application configuration backups, persistent volume snapshots, cluster state preservation, and automated cross-region failover for enterprise deployments.

The complexity you avoid: Testing disaster recovery procedures regularly, coordinating recovery across interdependent services, managing data consistency during failover scenarios, and ensuring recovery time objectives (RTO) and recovery point objectives (RPO) are met.

The Shift: Enabling Application Developers by Abstracting Infrastructure Complexity

Payara Cloud significantly improves the developer experience by removing these 11 operational complexities. Instead of spending weeks or months assembling and configuring infrastructure components, development teams can focus exclusively on what matters most: building applications that deliver business value.

Time Savings: What traditionally takes months of infrastructure setup and ongoing maintenance becomes a matter of minutes for application deployment.

Risk Reduction: Production-tested configurations and automated best practices eliminate the trial-and-error learning curve that often leads to security vulnerabilities and performance issues.

Team Efficiency: Development teams no longer need dedicated DevOps specialists to manage Kubernetes infrastructure, allowing smaller teams to achieve enterprise-scale deployments.

Innovation Acceleration: With infrastructure concerns handled automatically, teams can iterate faster, experiment more freely, and respond quickly to changing business requirements.

Payara Cloud eliminates the need to become a Kubernetes expert while still providing all the benefits of modern container orchestration. Your applications get enterprise-grade infrastructure that scales automatically and operates according to industry best practices, while your team gets to focus on writing code that matters.

The result is a development experience that feels like traditional application deployment but delivers the scalability, resilience, and efficiency of modern cloud-native architecture. It's Kubernetes without the Kubernetes complexity.

Ready to Focus on Code Instead of Kubernetes?

Start building Jakarta EE applications today without the operational overhead.

Payara Cloud's pay-as-you-go (PAYG) pricing means you only pay for what you use—no upfront infrastructure costs, no minimum commitments, and no surprise bills for idle resources. Whether you're prototyping a new microservice or scaling an enterprise application, you get production-grade Kubernetes infrastructure that automatically scales with your needs.

Get started in minutes:

- Deploy your first Jakarta EE application with zero infrastructure setup
- Scale automatically from development to production workloads
- Pay only for the CPU and memory your applications actually consume

Spin up a live demo with Payara Cloud in 60 seconds — no credit card, no guesswork.

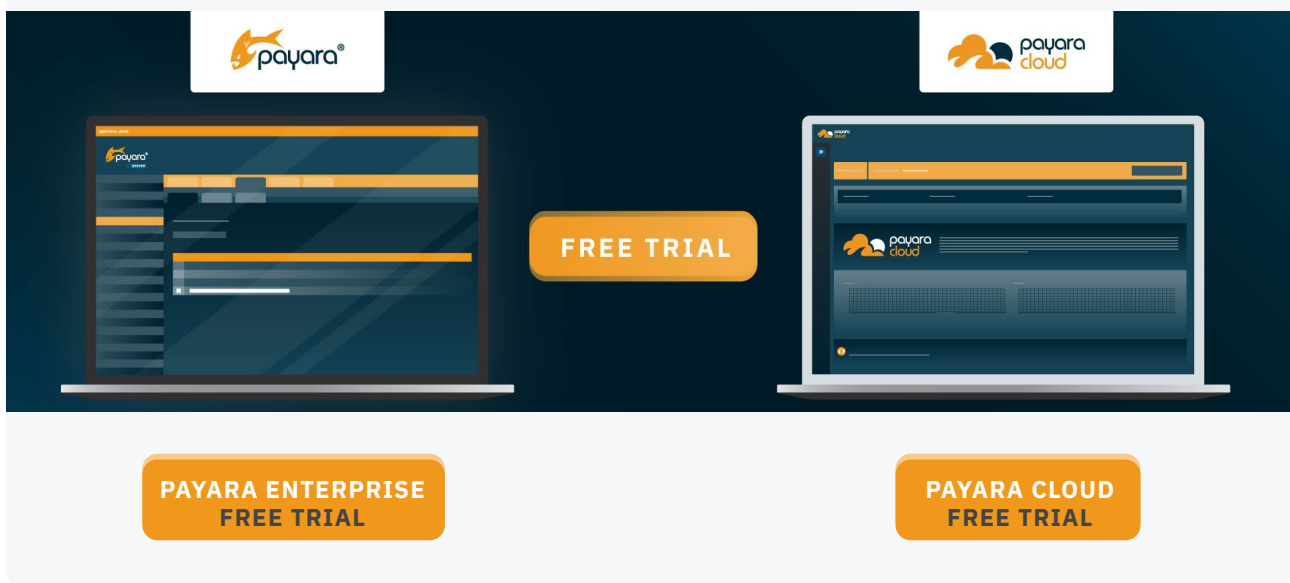
[Start Your Free Trial →](#)

Join the many developers who've already made the switch from managing K8s infrastructure to deploying Jakarta EE applications faster.

Questions? Our team is here to help you migrate existing applications or design new cloud-native solutions. [Schedule a consultation](#) or check our [getting started guide](#).

Transform your development workflow today. Your future self will thank you for choosing simplicity over complexity.

Interested in Payara? *Try Before You Buy*



The banner features two laptops on a dark blue background. The left laptop displays the Payara Enterprise interface, with the Payara logo above it. The right laptop displays the Payara Cloud interface, with the Payara Cloud logo above it. Between the laptops is a central orange button labeled 'FREE TRIAL'. Below each laptop is an orange button labeled 'PAYARA ENTERPRISE FREE TRIAL' and 'PAYARA CLOUD FREE TRIAL' respectively.



sales@payara.fish



UK: +44 800 538 5490
Intl: +1 888 239 8941



www.payara.fish

Payara Services Ltd 2025 All Rights Reserved. Registered in England and Wales; Registration Number 09998946
Registered Office: Malvern Hills Science Park, Geraldine Road, Malvern, United Kingdom, WR14 3SZ