

KUBERNETES CLUSTER CONFIGURATION MANUAL

Summit Digital Solutions, Inc.

Document Version: 2.4

Last Updated: January 9, 2024

Classification: CONFIDENTIAL - Internal Use Only

1. INTRODUCTION AND SCOPE

1. This Kubernetes Cluster Configuration Manual ("Manual") is the proprietary and confidential property of Summit Digital Solutions, Inc. ("Company"). This Manual establishes the standard operating procedures and configuration requirements for all Kubernetes clusters deployed within the Company's Peak Performance Platform(TM).

2. This Manual is subject to the Company's Master Technology Documentation Protocol (Reference: TD-2023-114) and incorporates all security requirements specified in the Company's Information Security Policy (Reference: SEC-2023-089).

2. DEFINITIONS

1. "Cluster" means a Kubernetes deployment consisting of at least one control plane and associated worker nodes.

2. "Production Environment" refers to any cluster hosting customer-facing workloads or processing customer data.

3. "Peak Performance Platform" means the Company's proprietary digital transformation platform, including all associated microservices and containerized applications.

3. CLUSTER CONFIGURATION REQUIREMENTS

1. ****Minimum Configuration Standards****

- a) All production clusters must maintain N+1 control plane redundancy
- b) Minimum worker node count: 3 per availability zone
- c) Required Kubernetes version: 1.25.x or higher
- d) Container runtime: containerd 1.6.x or higher

2. ****Network Configuration****

- a) Pod CIDR: 10.32.0.0/12
- b) Service CIDR: 10.96.0.0/12
- c) NodePort range: 30000-32767
- d) Maximum pods per node: 110

3. ****Security Requirements****

- a) RBAC enforcement mandatory
- b) PodSecurityPolicy implementation required
- c) Network policies must enforce zero-trust architecture
- d) Admission controllers must include:
 - NodeRestriction
 - PodSecurityPolicy
 - ResourceQuota
 - LimitRanger

4. DEPLOYMENT PROCEDURES

1. All cluster deployments must follow the Company's Infrastructure as Code (IaC) methodology using approved templates maintained in the central repository.

2. Pre-deployment Requirements:

- a) Security review completion
- b) Capacity planning documentation
- c) Disaster recovery plan
- d) Service Level Agreement definition

3. Deployment Validation:

- a) Conformance testing
- b) Security scanning
- c) Performance baseline establishment
- d) High availability verification

5. MONITORING AND MAINTENANCE

1. Required Monitoring Components:

- a) Prometheus deployment
- b) Grafana dashboards
- c) Alert manager configuration
- d) Logging stack implementation

2. Maintenance Windows:

- a) Regular maintenance: Second Sunday of each month, 01:00-05:00 EST
- b) Emergency maintenance: As required with CTO approval
- c) Version upgrades: Quarterly schedule per Technology Roadmap

6. COMPLIANCE AND AUDIT

1. All clusters must maintain compliance with:

- a) SOC 2 Type II requirements
- b) ISO 27001 standards
- c) Company security baselines
- d) Customer-specific compliance requirements as applicable

2. Audit Requirements:

- a) Quarterly internal audits
- b) Annual external security assessment
- c) Continuous compliance monitoring
- d) Monthly configuration drift analysis

7. DISASTER RECOVERY

1. Recovery Time Objectives (RTO):

- a) Production clusters: 4 hours
- b) Non-production clusters: 8 hours

2. Recovery Point Objectives (RPO):

- a) Production clusters: 15 minutes
- b) Non-production clusters: 4 hours

8. PROPRIETARY RIGHTS AND CONFIDENTIALITY

1. This Manual contains trade secrets and confidential information of Summit Digital Solutions, Inc. All rights reserved.

2. No part of this Manual may be reproduced, distributed, or transmitted in any form without prior written permission from the Company's Chief Technology Officer.

9. DOCUMENT CONTROL

Version History:

- 2.4: January 9, 2024 - Updated security requirements
- 2.3: October 15, 2023 - Added compliance sections
- 2.2: July 1, 2023 - Updated network configurations
- 2.1: April 15, 2023 - Initial release

Approved by:

—

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

Date: January 9, 2024

10. LEGAL DISCLAIMER

This Manual is provided "as is" without warranty of any kind, either express or implied. Summit Digital Solutions, Inc. reserves the right to modify this Manual at any time without notice. This document is controlled under document number KUBE-CONFIG-2024-001.