Service Definition: Millersoft Managed Apache Druid Service

1. Service Overview

Millersoft provides a managed, bespoke Apache Druid service designed for deployment on UK Government-aligned cloud infrastructure. The service supports Apache Druid installations on either bare metal infrastructure or Kubernetes (K8s), depending on customer requirements. The service is suitable for OFFICIAL and OFFICIAL-SENSITIVE workloads, subject to customer assurance and platform controls.

The service includes design, deployment, operation, monitoring, security management, and support of Apache Druid as a high-performance analytics datastore.

2. Scope of Service

The managed service covers: - Architecture and design of Apache Druid clusters - Installation and configuration of Apache Druid - Deployment on bare metal or Kubernetes platforms - Secure configuration and hardening - Ongoing operational management - Monitoring, alerting, and incident response - Patch and vulnerability management - Backup and recovery configuration - Support and service management

3. Supported Deployment Models

3.1 Bare Metal Deployment

- Dedicated physical hosts or virtualised infrastructure
- Operating system hardening aligned with CIS or equivalent benchmarks
- Direct-attached or networked storage
- Isolated network segments

3.2 Kubernetes Deployment

- Deployment to customer-provided or managed Kubernetes clusters
- Helm or manifest-based deployments
- Integration with Kubernetes-native networking, storage, and secrets management
- Horizontal scalability using Kubernetes primitives

4. Security and Compliance

Millersoft applies supplier-defined security controls aligned with UK Government Cloud Security Principles.

4.1 Identity and Access Management

- Role-based access control (RBAC)
- Least privilege access

- Strong authentication and MFA for administrative access
- Separation of duties between operational roles

4.2 Network Security

- Private network deployment
- Network segmentation between Druid components
- Encrypted communications using TLS
- Restricted management access via VPN or IP allow-listing

4.3 Vulnerability Management

- Monitoring of Apache Software Foundation security advisories
- CVE tracking for Druid and dependencies
- Timely deployment of security patches
- Mitigating controls applied where immediate patching is not possible

4.4 Protective Monitoring

- Centralised logging of system and application events
- Monitoring of authentication, access, and administrative actions
- Alerting on anomalous behaviour
- Incident triage and investigation

5. Service Management

5.1 Incident Management

- Supplier-defined incident management process
- Incident classification by severity and impact
- Rapid response to high-severity incidents
- Root cause analysis and corrective actions

5.2 Change Management

- Controlled change process for configuration and upgrades
- Planned maintenance windows
- Rollback procedures where applicable

5.3 Backup and Recovery

- Configuration of backups for metadata and configuration data
- Support for customer-defined backup policies
- Assistance with restore testing

6. Support Model

- Named support contacts
- Incident reporting via agreed support channels
- Defined response and resolution targets
- Regular service reviews

7. Customer Responsibilities

Customers are responsible for: - Providing the underlying infrastructure and cloud platform - Data classification and handling decisions - Network connectivity and perimeter controls - Application-level access controls

8. Assumptions and Dependencies

- Apache Druid is provided under the Apache License 2.0
- The service does not include application development
- Compliance accreditation depends on the customer platform and operating model

9. Exit and Portability

- Assistance with service termination
- Export of configuration and metadata
- Knowledge transfer to the customer or successor supplier

10. Service Availability

Service availability targets and maintenance arrangements are agreed contractually and documented separately.

11. Service Levels (SLAs and SLOs)

Millersoft provides service level objectives (SLOs) and service level agreements (SLAs) appropriate to the criticality of the service and customer requirements. Unless otherwise agreed, the following targets apply.

11.1 Availability SLO

- Target service availability: **99.5% per calendar month** (excluding planned maintenance)
- Availability applies to core Apache Druid query and ingestion services

11.2 Incident Response SLAs

Incidents are prioritised by severity and impact:

- **Severity 1 (Critical):** Service unavailable or major data access failure
- Response target: **1 hour**
- Ongoing updates: At least every **4 hours** until resolution
- **Severity 2 (High):** Significant degradation with no workaround
- Response target: **4 hours**
- **Severity 3 (Medium):** Limited impact or workaround available
- Response target: **1 business day**

- **Severity 4 (Low):** Minor issue or service request

- Response target: **2 business days**

11.3 Resolution Targets (SLOs)

- Severity 1: Restore service as soon as practicable, target **within 1 business day**
- Severity 2: Target **within 3 business days**
- Severity 3: Target **within 10 business days** or via planned change

11.4 Planned Maintenance

- Planned maintenance is scheduled in advance and notified to customers
- Maintenance windows are excluded from availability calculations

11.5 Service Reporting

- Regular service reviews may include availability, incidents, and performance metrics
- SLA performance is reviewed jointly with the customer

These service levels may be tailored contractually to meet specific operational or regulatory requirements.