AiX Operations & Maintenance

v2026.3

DDX Business Solutions Limited

Customer Reference

Table of Contents

1. Operations & Maintenance

1.1 Overview

■# Operations & Maintenance Overview

This section defines product-level operating guidance for AiX. Customer-specific schedules, tools, responsibilities, retention periods, RPO/RTO values and infrastructure procedures belong in `aix-docs-<customer>`.

Core areas include service management, backup/recovery, data lifecycle and cleanup, health checks, monitoring, performance, logging, audit, patching and disaster recovery.

Download Documentation

Prefer an offline or printable copy of this section?

Download Operations & Maintenance (PDF)

The PDF contains the complete Operations & Maintenance documentation for this release and is generated from the same documentation source as this website.

1.2 Service Management

Document supported procedures for starting, stopping, restarting and checking AiX components. Include dependency/order considerations and safe maintenance procedures for the current deployment architecture.

Customer-specific container/service names and infrastructure commands should be recorded in the customer repository.

1.3 Backup & Recovery

A complete AiX backup strategy should consider the database, file storage, configuration, customer-managed integrations, and any other state required to restore service.

Mermaid diagram source

```
flowchart LR
    DB[(Database)] --> Backup[Backup Set]
    Files[File Storage] --> Backup
    Config[Configuration] --> Backup
    Backup --> Verify[Verify / Test Restore]
    Verify --> Recovery[Recovery Procedure]
```

Document what must be backed up, supported recovery sequence, consistency considerations, and restore validation. Customer-specific frequency, retention and backup technology belong in customer documentation.

1.4 Data Lifecycle & Cleanup

AiX deployments may accumulate multiple classes of operational and business data. Cleanup must be deliberate and must not remove records required for audit, recovery or customer retention requirements.

| Data Area | Examples | Cleanup Consideration | |---|---|---| | Database | application, execution, interaction records | retention and referential integrity | | Audit | user/actions/AI interaction audit | compliance retention | | File Storage | input, working, output, temporary files | business retention and active jobs | | Knowledge Base | source files, chunks, vectors | KB lifecycle and re-index requirements | | Logs | application/service logs | rotation and retention | | Cache | temporary/cache data | safe expiry/invalidation | | AI Worker | temporary processing artifacts | active-job safety |

Cleanup Principles

- Define retention before automated deletion.
- Separate temporary/cache cleanup from business-record deletion.
- Preserve required audit/provenance records.
- Validate backups where recovery may be required.
- Record customer-specific retention policies in the customer repository.

1.5 Health Checks

Define health checks for AiX web/application services, database, storage, AI Worker, AI Engine/model runtime, scheduler and required integrations.

Health checks should distinguish service availability from deeper functional readiness where practical.

1.6 Monitoring

Document availability and operational monitoring for AiX services and dependencies. See also Health Checks and Performance Monitoring.

Customer-specific monitoring products, alert thresholds, recipients and escalation procedures belong in the customer documentation.

1.7 Performance Monitoring

Monitor both infrastructure and application/model behavior. Relevant measures may include CPU, memory, disk, accelerator utilization, service response time, worker queue/load, model response latency and database/storage performance.

AiX may rely on customer/infrastructure monitoring tooling for metrics not exposed by the application. Document that boundary explicitly.

1.8 Logging

Document log locations/sources, log levels, rotation, retention, access control and safe diagnostic handling for AiX components.

Do not intentionally log secrets. Customer-specific forwarding/SIEM configuration belongs in the customer repository.

1.9 Audit

This section defines product-level operating guidance for AiX. Customer-specific schedules, tools, responsibilities, retention periods, RPO/RTO values and infrastructure procedures belong in `aix-docs-<customer>`.

Core areas include service management, backup/recovery, data lifecycle and cleanup, health checks, monitoring, performance, logging, audit, patching and disaster recovery.

1.10 Patching & Maintenance

Document the supported maintenance lifecycle for AiX application releases and relevant runtime dependencies. Coordinate OS, container runtime, database and infrastructure patching with the responsible customer/infrastructure teams.

Validate significant changes in UAT before Production where applicable and maintain an explicit rollback/recovery path.

1.11 Disaster Recovery

Document the standard DR planning framework, recovery sequence, validation, and customer-specific RTO/RPO considerations.