

UIS Cloud Product Brief

Disaster Recovery & High Availability Platform



Powered by **DaoCloud**

EU 8-Pillar Sovereign · AI Conformance · Gartner · Forrester

Executive Summary

When critical systems fail, every second costs money, reputation, and regulatory standing. UIS Cloud's Disaster Recovery & High Availability Platform —built on DCE 5.0 — is a cloud-native, application-level DR platform engineered specifically for regulated industries that demand both financial-grade recovery objectives and full EU 8-pillar sovereignty.

Unlike public cloud DR tools that recover VMs and leave your operations team to manually restart services in the right order at 3am, DCE 5.0 recovers your Kubernetes workloads — namespaces, dependencies, stateful sets, config, secrets — in the correct sequence, automatically, across every cluster and cloud you operate. No human in the loop. No manual orchestration. No missed services.

UIS Cloud is among the first 14 organisations globally to achieve CNCF AI-conformant status — the designation your regulators are moving toward. Independently recognised by Gartner and Forrester. When your procurement team asks for third-party validation, the answer already exists.

Pain Points Solved



Application Recovery Gap

Your current DR tool recovers infrastructure — not applications. After failover, your team spends hours manually identifying which services failed to start, in what order, and why. When the post-incident review happens, that gap is yours to answer for — not your vendor's.



Regulatory Mandates

DORA Article 11 requires financial institutions to demonstrate ICT continuity plans with tested, documented RTO/RPO targets. BAFIN, ACPR, and NIS2 carry equivalent mandates. If your current DR tool cannot produce a regulator-ready audit trail of your RTO/RPO performance, that is not a configuration gap — it is a compliance gap your next supervisory review will surface.



Multi-Cloud Reality

Your workloads span AWS, Azure, OCI, and on-prem. Your DR tool covers one of them. When the incident spans two — and it will — you are running manual failover procedures across environments your tool was never designed to orchestrate simultaneously. That is the scenario your DORA resilience test is designed to expose.



Sovereignty Violation

Many public cloud DR solution routes orchestration through a foreign-controlled control plane — a structural sovereignty violation for EU regulated entities.



Manual Failover Drills

Manual failover drills take days to plan, require specialist knowledge, and still fail unexpectedly in production.

Core Capabilities

Application-Level Recovery – Not Infrastructure-Level

DCE 5.0 operates at the Kubernetes workload level. Unlike VM-based recovery – which restores an entire machine at significant cost and resource overhead – it recovers your namespaces, deployments, stateful sets, services, config maps, secrets, and persistent volumes – in dependency order – to a running, verified application state.

Cross-Cluster & Cross-Cloud Failover

Automated failover across clusters within the same cloud, across different clouds, or across on-premises data centres. Active-Active and Active-Standby topologies are both supported, with real-time health monitoring and configurable eviction tolerances.

Configurable and Auditable RTO/RPO

Configurable cluster monitoring intervals, unhealthy grace periods, and eviction timeouts let teams define and achieve RTO/RPO targets that meet core banking and government SLA requirements. Parameters are fully auditable and reportable to regulators.

Automated Failure Detection & Failover

No human in the loop. DCE 5.0 continuously monitors cluster health. When a cluster crosses the unhealthy threshold, it is automatically tainted, eviction is initiated, and workload pods migrate to healthy clusters – all without operator intervention.

Full Backup Suite – Application & Cluster Configuration

Your backup strategy needs to answer two different failure scenarios: a single service failing in production ("surgical recovery"), and a full cluster event (complete state restoration). DCE 5.0 handles both. Namespace-level backups with label filtering for targeted service recovery. CronJob-scheduled incremental and full backups for cluster-level continuity. Every backup verifiable, auditable, and restorable to a clean application state – not just a filesystem snapshot.

Multi-Region High Availability

Purpose-built for geo-distributed deployments across availability zones and regions, enabling organisations to meet both technical HA requirements and regulatory mandates for geographic data separation.

Sovereignty: The EU 8 Pillars

Data sovereignty is a baseline today — and it is not sufficient. For banks under DORA, insurers under SOLVENCY II, energy operators under NIS2, and government agencies under national security frameworks, the question is not whether your data is in a European region. It is whether your DR orchestration, your failover decisions, and your recovery playbooks ever leave a jurisdiction you control. With most public cloud DR tools, the answer is: they do.



SOVEREIGNTY COMMITMENT

- ☐ DCE 5.0 is deployed entirely within your environment. There is no mandatory call-home to UIS Cloud infrastructure. Your disaster recovery orchestration, your backup data, and your failover decisions never leave your sovereign boundary. This is architecturally guaranteed — not a contractual promise.

Architecture at a Glance

DCE 5.0'S DR Architecture Operates on a hub-and-spoke multi-cloud management model

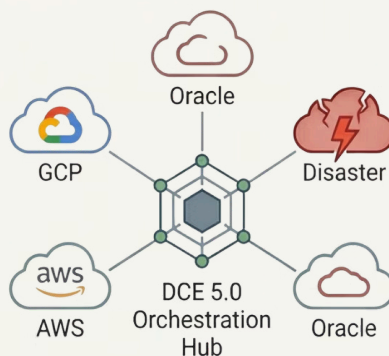
- Global Control Plane**
 A unified management cluster provides cross-cloud workload scheduling, failover policy management, and health monitoring – deployed on your infrastructure.
- Member Clusters**
 Production, standby, and DR clusters in any cloud or on-premises environment register as managed members. Scheduling policies (aggregated or dynamic-weight) govern normal operations.
- Failover Engine**
 Continuous ClusterMonitor polls registered clusters. On unhealthy detection exceeding grace period, the engine taints the cluster, drains pods via graceful eviction, and reschedules to available healthy clusters using remaining capacity.
- Backup Controller**
 CronJob-driven backup scheduler persists full and incremental snapshots of application namespaces and etcd state to your designated storage backend – S3-compatible, on-prem NFS, or private object store.
- Recovery Orchestrator**
 Namespace-level restore with label selector filtering enables surgical recovery of specific services without touching adjacent workloads – minimising blast radius and recovery time.

Automated Cross-Cluster Backup and Recovery



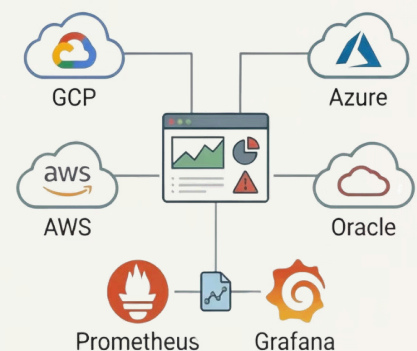
Schedule application and data volume backups to object storage for seamless recovery and migration.

Multi-Cloud Active-Active Application Failover



Automatically migrate workloads to healthy clouds during disasters to ensure Near-Zero downtime without additional redundant costs.

Unified Multi-Cluster Observability and Monitoring



Centralize metrics collection and alerting across various cloud providers using integrated Prometheus and Grafana.

Next Step

Regulated industries cannot afford DR theatre — tools that look good in demos but fail the sovereignty test, the audit test, or the 3am production incident test. DCE 5.0, having passed 1000+ references worldwide, was built by engineers who live in cloud-native infrastructure, for organisations that cannot afford to get it wrong.

Request a Sovereign DR Assessment on UIScloud.io

We will map your current DR posture against DORA/NIS2 requirements, identify your sovereignty gaps, and show you exactly how DCE 5.0 closes them — on your infrastructure, on your timeline.

*Your data stays in your environment on Day 1.
Your regulators will thank you on Day 2.*

About UIS Cloud

UIS Cloud stands as a pioneering sovereign AI infrastructure provider, empowering governments and regulated enterprises to deploy and operate advanced AI systems at scale entirely within their own jurisdictions. With over 1000 projects, UIS Cloud bridges the critical gap between stringent sovereign control requirements and the imperative for hyperscale AI performance, effectively eliminating the traditional trade-off between compliance and efficiency.

At its core, UIS Cloud transforms the concept of sovereign AI from a theoretical framework into a robust, production-ready platform. This is achieved through a meticulous combination of open standards, advanced orchestration capabilities, and deep ecosystem integration, ensuring that organisations can leverage AI while maintaining absolute control over their data and operations.