kyndryl

Cloud Resiliency Orchestration by Kyndryl

Automated, reliable and fast recovery for hybrid cloud environments

Contents

A future with zero tolerance for failure

Organizations on the journey to a hybrid multicloud future are discovering how difficult it is to manage their disaster recovery workflows across increasingly diverse, interconnected environments. As a result, many organizations end up undermining the primary reasons for adopting hybrid multicloud in the first place: to gain better capabilities and deliver a superior customer experience.

Hybrid multicloud environments come with operational complexities and demands. They also provide more opportunities for cyberattackers. These realities increase the risks of outages and unplanned downtime—and the business impact of service disruption in today's fast-paced world can be devastating.

To mitigate or otherwise help prevent costly outages and service disruptions in a hybrid multicloud world, you need hybrid cloud platform for data protection and recovery, combined with highly specialized skills, an integrated strategy and technologies such as orchestration for cyber and disaster recovery. These foundations for true resiliency must be integrated into your hybrid multicloud strategy before you embark on your digital transformation journey. If you treat data protection and disaster recovery as an afterthought, you do so at your own peril.

To mitigate costly outages and service disruptions in a hybrid multicloud world, you need highly specialized skills, an integrated strategy and technologies for data protection and recovery.

Simplified disaster recovery for a complex hybrid world

Kyndryl Cloud Resiliency Orchestration is a suite of managed services that helps you elevate your IT service resiliency in the face of heightened expectations, exponential data growth and an increased number of cyber threats. The service uses an orchestration platform—driven by Kyndryl Resiliency Orchestration software—bundled with its own replicator and anomaly detection too. The combination provides push-of-a-button automation to failover and recover applications in the event of an outage. Failover automation enables recovery within business-set recovery time objectives (RTOs). Application recovery becomes predictable when operator errors are eliminated, and human dependency is reduced.

With Kyndryl Cloud Resiliency Orchestration you can simplify your disaster recovery management to reduce risk and improve availability, efficiency and business continuity. It provides intelligent automation of data protection and disaster recovery workflows, and it enables complete disaster recovery (DR) lifecycle management and cyber incident recovery orchestration for complex, hybrid infrastructures.

Repeatable and reliable recovery workflows

Kyndryl Cloud Resiliency Orchestration has an extensive library of the most commonly used application and database patterns as well as intelligent workflow automation options. You can choose from more than 800 industry-standard predefined workflow patterns and automation options, and assemble them to create repeatable, reliable recovery workflows. You can also scale up, scale down and streamline your recovery process. This also enables rapid disaster recovery in the cloud with automation that minimizes human error and ensures SLA performance is maintained.

Real-time disaster recovery readiness

Through its user-friendly web-based management dashboard, Kyndryl Cloud Resiliency Orchestration lets you automate, monitor and manage all of your disaster recovery operations in real time, including the management of failover and recovery for physical or virtual systems.

Meanwhile, day-to-day operations covering disaster recovery monitoring and management are performed by Kyndryl Resiliency Services. In the event of a disruption, you're notified based on your policies and provided with compliance reports through your dashboard.

Robust reporting and feature-rich

Kyndryl Cloud Resiliency Orchestration offers a comprehensive disaster recovery audit and compliance dashboard and reporting platform. It generates deviation reports for your recovery point objective (RPO) and RTO, so C-suite executives have better insight into recovery performance and you can ensure regulatory requirements are being met. Additionally, Kyndryl Cloud Resiliency Orchestration alerts you in the event of a deviation, and it provides drill-down functionality so you can gain deeper insight into recovery issues.

Kyndryl Cloud Resiliency Orchestration platform simplifies and automates recovery of data and applications in the event of a disaster or a cyber outage through intelligent recovery workflow automation across hybrid multicloud and multi-technology environments.

Optimized resiliency for reinforced business continuity

The intelligent automation and optimized resiliency helps you reduce recovery time in the event of a disaster or outage by:

- Automating complex recovery for multi-vendor physical, virtual and container environments
- Providing data protection on top of native replication
- Enabling anomaly scan on backed-up data for enhanced cyber resilience
- Managing changes in platform configuration
- Providing real-time insight into application data loss and recovery time
- Using dry run capabilities to detect environment changes that cause recovery failure
- Automating redundant, resource-intensive and costly disaster recovery processes
- Designing recovery workflows to meet SLAs and RTOs/RPOs
- Enabling global recovery audit reporting and documentation

Efficient functionality and ease of use for IT teams

IT users and risk managers using Kyndryl Cloud Resiliency Orchestration may experience a reduction in their disaster recovery exercise times. They also benefit from one-click failover and recovery, as well as quick and easy provisioning of resources and environments.

Kyndryl Cloud Resiliency Orchestration reduces the need for manual efforts and resource-intensive and costly IT recovery processes.

Benefits of Kyndryl Cloud Resiliency Orchestration

Speed
Disaster recovery automation and testing cuts provisioning time from hours or days down to minutes for faster RTO and RPO.

Scale
The dashboard for real-time monitoring and management scales across multiple data centers and supports heterogenous environments.

Simplicity
An application-aware approach makes it easier to deploy and manage multi-tier recovery for enterprise applications.

Adaptability
Recovery for enterprise applications that span multiple technologies helps meet audit and compliance management requirements.

Reliable, smart data protection for multicloud environments

Built-in, continuous block replication
Kyndryl Cloud Resiliency Orchestration delivers continuous block replication for increased flexibility in public and private clouds by leveraging the built-in Resiliency Block Replicator (RBR). The features of Resiliency Block Replicator are:

- VMware hypervisor-based continuous asynchronous data replication for enterprise workloads that run on Microsoft Windows and Linux® systems
- Host-based data replication fornon-VMware workloads
- Automated deployment of the replication components that enable low-deployment effort
- Failover and failback disaster recovery workflows

Cyber Recovery as a Service (CRaaS)
The Cyber Recovery as a Service offering is a fully managed service that enables customers to recover from a cyberattack on their systems. It is designed for quick recovery that will minimize the impact to business due to the attack.

Kyndryl Resiliency Orchestration includes Cyber Incident Recovery capabilities. This capability is built using state-of-the-art technologies such as immutable WORM storage, air-gap protection, copy data management, point-in-time copies and anomaly detection.

Orchestrated Disaster Recovery as a Service (DRaaS)
Kyndryl Orchestrated DRaaS for IBM Cloud® can simplify DR automation with orchestration and replication technology. Integrated solutions are designed to enable simple automated recovery of VMware and Hyper-V workloads to one of the IBM Cloud data centers, providing real-time DR-readiness validation that can reduce DR test times and DR failover. This can result in a more cost-effective DR experience that is smarter, more tailored and more agile than ever before.

Optional value-add services
Kyndryl Cloud Resiliency Orchestration also offers specially designed optional services including consulting, application and IT discovery, which enhance the client experience and help enable end-to-end and predictive enterprise resiliency.

Resiliency orchestration consulting
Kyndryl Cloud Resiliency Orchestration with optional consulting helps enable comprehensive enterprise resiliency.

- Orchestration readiness assessment: Examines 10 areas essential to orchestration and determines level of readiness to migrate
- Application dependency analysis: Identifies critical application dependencies for recovery/restart workflows and procedures
- Resiliency program management: Manages development of recovery workflows, test exercise coordination and provides overall DR program management

Application and IT discovery
Cloud Resiliency Application and IT Discovery for Orchestration helps automate the discovery process of logically segmenting the infrastructure

- Identifies multi-level server dependencies
- Faster and more accurate than manual grouping techniques

Why Kyndryl?

Kyndryl has deep expertise in designing, running and managing the most modern, efficient and reliable technology infrastructure that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We're building on our foundation of excellence by creating systems in new ways: bringing in the right partners, investing in our business, and working side-by-side with our customers to unlock potential.

To learn more about Cloud Resiliency Consulting Services by Kyndryl, please contact your Kyndryl representative or visit us at kyndryl.com

kyndryl™

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America

July 2021

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.