cristie
software

Financial Sector Operational Resilience

Solving the challenges of System Recovery at scale

www.cristie.com

Preface

Operational resilience refers to an organization's ability to withstand and adapt to disruptions while maintaining essential business functions. The financial services industry has placed significant attention on operational resilience with the Bank of England and the Financial Conduct Authority (FCA) establishing guidelines leading to the introduction of new requirements which come into force 31 March 2025. Within the EU similar legislative requirements are inplace under the Digital Operational Resilience Act (Regulation (EU) 2022/2554) commonly referred to as DORA. Likewise, with ongoing re-emphasis in the US on existing standards, it seems clear that operational resilience is a key focus area for financial regulators globally.

Firms will need to make sure they have sufficient internal and technological resources to carry out the assessments, mapping, testing, and additional actions the new regime requires to pass the self-assessment submissions required by the regulators. The infrastructure recovery elements concerning operational resilience are placing considerable practical consequences upon firms that fall within the scope of these new requirements. System recovery of compute server estates that number into the thousands are a reality for many critical functions within the financial sector.

Although March 2025 may sound far off, regulators will expect incremental progress during the interim period, so businesses should be prepared to demonstrate this when the next impact events occur. Cristie Software provides system recovery solutions designed for automated large scale system recovery orchestration with the ability to undertake detailed system recovery simulations to assist self-assessment and regulatory compliance. This solution brief will outline how Cristie recovery solutions can automate and simplify key aspects of infrastructure recovery to help meet the requirements of operational resilience legislation.

Contents

Introduction

The Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) respective policy statements PS21/3 & PS6/21, and the PRA Supervisory Statement SS1/21 address risks to operational resilience from the interconnectedness of the financial system and the complex and dynamic environment in which applicable firms operate. The practical implications of achieving compliance with these directives present far-reaching obligations for applicable firms and prescribe a significant increment in a firm's approach to ensuring operational resilience.

These statements outline five core intervention steps that must be transposed into solution design principles for financial business services that are identified to be of strategic and operational importance (prepare, detect, respond, recover, and adapt). Services need to be identified and mapped to processes and resources to ensure that customer, firm, and market impact tolerances are set, and plausible disruption scenarios are defined and tested.

The recovery of identified services will typically need to follow a specific hierarchy which must ensure that services are restored within defined impact tolerances. Furthermore, the directives specify that firms must regularly test their ability to remain within impact tolerances in severe but plausible disruption scenarios. Firrms are required to document a self-assessment of their compliance and document the methodologies they have used to undertake these activities.

This document will outline the advantages of using Cristie Software recovery and replication software to help determine whether impact tolerances can be met for critical services; to orchestrate and automate disaster recovery scenario testing at scale; and to support self-assessment through detailed system recovery simulation and reporting.

Facilitating large scale system recovery

Financial systems involve complex interdependent server and storage configurations that are built with redundancy to provide the utmost resilience. The deployment, maintenance, and protection of these systems presents specific challenges due to scale. For instance, a single service such as payments may be supported by thousands of server instances across multiple geographies for many financial firms. Recovery and replication solutions from Cristie Software offer several mechanisms to facilitate bulk server deployment and recovery. The Cristie Virtual Appliance (VA) is a fundamental component which provides central management, deployment, and licensing of Cristie's range of backup, recovery, and replication software. It is provided free of charge to licensed users of Cristie software products. The Cristie VA is a Linux-based virtual machine that manages Windows, Linux, AIX, and Solaris installations of Cristie Software products.

Bulk estate management parameters and CSV imports

The Cristie VA user interface provides options for bulk entry of estate management parameters and several CSV import options are available to support large scale backup and recovery operations:

- Backup agent deployment (host IP, ports, user credentials)
- Boot Management - allows the user to create minimal ISOs for network booting within a Preboot Execution Environment (PXE or iPXE) and custom ISOs for any Cristie BMR / CloneManager products.
- Boot mappings can be created on a large scale by importing a file containing details of the mappings required (MAC, IP, Netmask, Gateway, DNS1, DNS2, OS, Cristie BMR Product).
- Bulk custom product ISOs can be created for BMR recoveries or replications with a static network configuration for use in environments where DHCP is not available.

Cristie VA bulk actions using the SDK API

All recovery and replication orchestration tasks offered within the VA are also accessible through corresponding SDK APIs to facilitate the development of custom orchestration scripts. This allows detailed recovery tasks to be integrated within your internal automation tool chain or with third-party tools for maximum flexibility. All API documentation is available within the Swagger API Platform based on the OpenAPI specification which can be used to generate an SDK client in the programming language of your choice.

Intelligent Platform Management Interface (IPMI) integration

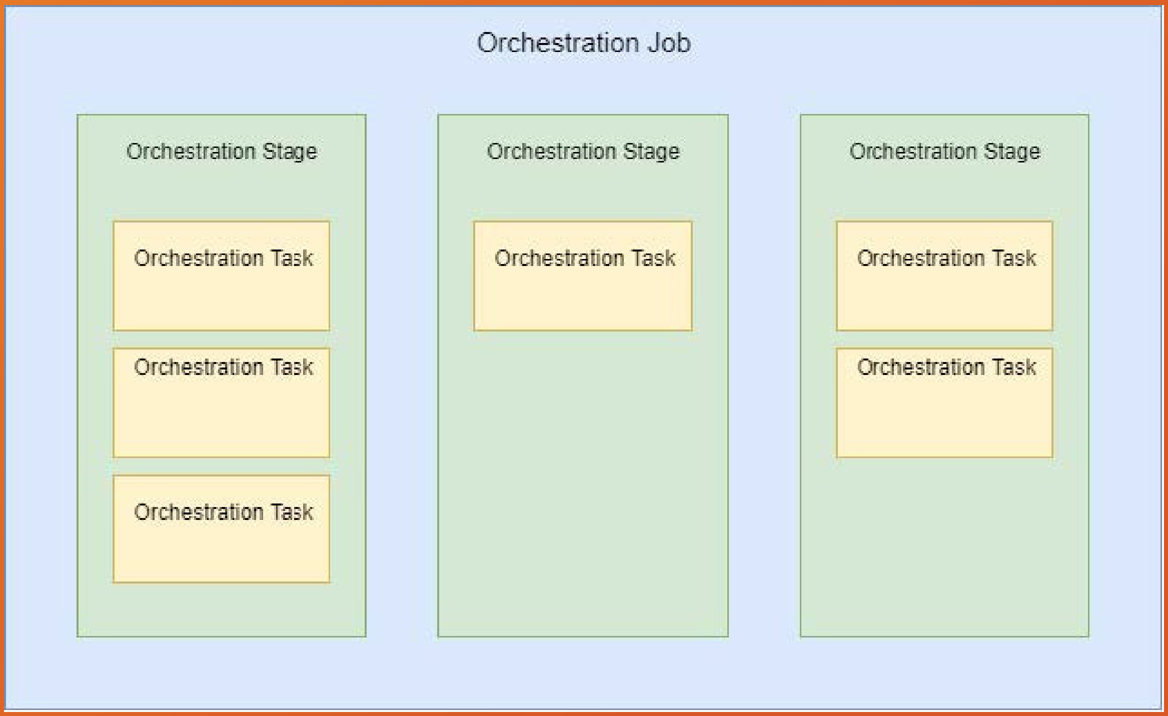
The Cristie recovery boot environment can easily be incorporated with common IPMI implementations such as iDRAC (Dell) and iLO (HP). For Out-of-Band (OOB) systems management we offer DMTF Redfish® client standard libraries to manage physical systems with the same level of automation available for virtual machines. This eliminates the need for manual intervention when recovering or provisioning physical systems at scale.

Hierarchy of recovery

Within any IT infrastructure there will be a system recovery hierarchy necessary to accommodate system interdependencies. For instance, active directory (AD) is typically the primary service required as it contains critical information regarding the environment, including users, servers, and associated permissions and privileges. Cristie Software can help facilitate tiered system recovery through the system recovery orchestration features provided within the VA.

Recovery orchestration to facilitate tiered system recovery

Orchestrations consist of user defined Jobs containing one or more Stages where each stage contains one or more Tasks. Each job can have unlimited stages and each stage can have unlimited tasks. When a job is run, it will run one stage at a time (from left to right). It will not move onto the next stage until all tasks within a stage are complete. VA orchestration can be used to initiate the ordered recovery of servers within a tiered architecture. For instance, recovery of AD services could be placed within the first stage of an orchestration job with the process managed through the definition of individual tasks within the stage.



Tasks can be defined to allow timed boot delays for specific systems and include manual intervention tasks if required. Manual intervention may be required to allow a person with authority to provide authorisation for a particular service to be placed active, or for practical purposes, for instance to allow for the insertion of media within a tape library.

Orchestration tasks allow for detailed fine tuning of system recoveries and replications including reboots, post recovery scripts, manual tasks, plus customisable options for actions following any stage failures. Full details can be found in the VA-Orchestration Guide.

[Cristie Virtual Appliance (VA) Orchestration Guide (PDF).]

System recovery monitoring to meet impact tolerances

The PRA Supervisory Statement SS1/21 section 4 outlines the actions firms need to undertake to ensure that they can deliver important business services within impact tolerances in severe but plausible scenarios. Impact tolerance is linked to the time-criticality of a business service. Time-criticality is high when the impact tolerance is set for a short amount of time. The PRA expects firms to have undertaken planning and set up recovery and response arrangements in advance to be able to respond quickly to disruptions when they occur. Similarly, EU DORA Article 12 (Backup policies and procedures, restoration and recovery procedures and methods) offers comprehensive directions regarding testing of backup procedures plus restoration and recovery procedures for critical services which must be undertaken periodically. The two key metrics used to define the performance required from a system replication or recovery operation are the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

RPO testing and reporting with Cristie Software

RPO generally refers to calculating how much data loss a firm can experience for a particular service within a period most relevant to its business before significant harm occurs. The time is measured from the point of a disruptive event to the last data backup. For systems that are replicated to a standby system for failover in the event of a disaster scenario, the RPO will be determined by the synchronization period between the active and standby systems and the rate at which changes in the active system can be synchronized to the standby target. CloneManager, the system replication solution from Cristie Software can determine if specific RPOs can be met through replication simulation monitoring. CloneManager will generate reports for replications that fall outside of target RPOs to inform administrators that the replication infrastructure requires attention. Current versus target RPO metrics can be seen immediately from the customisable Cristie VA dashboard.

RTO testing and reporting with Cristie Software

RTO refers to the amount of time that an application, system, or process can be down without causing significant damage to the business and the time spent restoring the application and its data to resume normal business operations after a significant incident. Calculating RTO for important business services will be critical to ensuring impact tolerances can be met. The Cristie VA provides reports on RTO for simulated recoveries which can provide vital insight into a firm's recovery strategy to meet impact tolerances. Reports can be generated on ongoing recovery operations for management reporting, SLA verification and FCA/PRA/DORA self-assessment.

Scenario Testing with Cristie Software Recovery Simulation

The PRA Supervisory Statement SS1/21 section 6 describes the expected scenario testing firms should undertake to ensure they can remain within impact tolerances for important business services. The nature and frequency of a firm's testing should be proportionate to the potential impact that disruption could cause and whether the operational resources supporting an important business service have materially changed.

Scheduled recovery simulation and reporting

Recovery simulation can be scheduled within the VA to test recoveries of any supported Cristie BMR product backups. The simulation frequency/interval can be set as summarised in Table 1. Recovery of selected machines can be simulated within a simulate recovery job. The recovery destination can be any physical, virtual or cloud target. With a simulation job created, and at least one recovery machine added to the job, the VA will continue to restore simulations indefinitely until either manually booted, the job is suspended, or the target machine is deleted. It is possible to add multiple simulation machines to the same job. The machines in the job do not need to be the same platform type. If the recovery target is of dissimilar hardware to the source system, then Dissimilar HardWare (DHW) mode can be enabled which provides a path to additional drivers that may be required to successfully boot the target system.

Frequency	**Description**
Hourly	Syncs run every user specified number of hours at a selected time.
Daily	Syncs run every user selected number of days at a selected time.
Weekly	Syncs run on specific user selected day(s) of the week (Monday/Tuesday etc.) at a selected time.
Monthly	Syncs run only on a specified day of the month at a selected time.

Simulated and live recovery reporting

The Cristie VA provides extensive log files detailing system recoveries and replications. The VA provides a Log File Viewer within the Tools menu which allows individual log files to be viewed and downloaded. The Tools menu also provides a Log Analysis option which is used by the Cristie VA to determine the root cause of a recovery operation failure without user intervention. This feature has been recently improved by incorporating Machine Learning (ML) techniques. These techniques are used to scan log files from failed Cristie product replications, recoveries, and simulations. ML technology is then used to pinpoint the exact issue or issues that caused a recovery to fail.

Improving scenario testing through advanced log parsing and machine learning

Log files containing runtime information are a vital tool to assist root cause analysis following a recovery failure, however they can be extensive files containing unstructured information that requires manual filtering to find specific entries, plus administrative knowledge to determine which reported events are significant when determining any failure resolution.

Cristie Software have implemented the very latest compute efficient log parsing algorithms to transform raw log messages into structured log messages which can then be compared against 'known good' recovery runtime outputs to train the VA in anomaly detection and categorization.

The recovery process and anomaly detection take place over several phases. The first step is the creation of a virtual environment in which to restore the system. The virtual environment is created according to a stored configuration and the system is restored from a backup or from a replica into the virtual environment. An attempt is then made to boot the restored system in the virtual environment with runtime logs collected during system startup.

The VA then parses the log files from the recovery simulation using machine learning rules based on known-good recoveries to identify any anomalies. The machine learning rules derived from the known-good runtime outputs train the VA on which log file entries to ignore so that only failed operations are collected for analysis. This training data is continually updated and reanalysed to ensure that accuracy improves which each new software iteration.

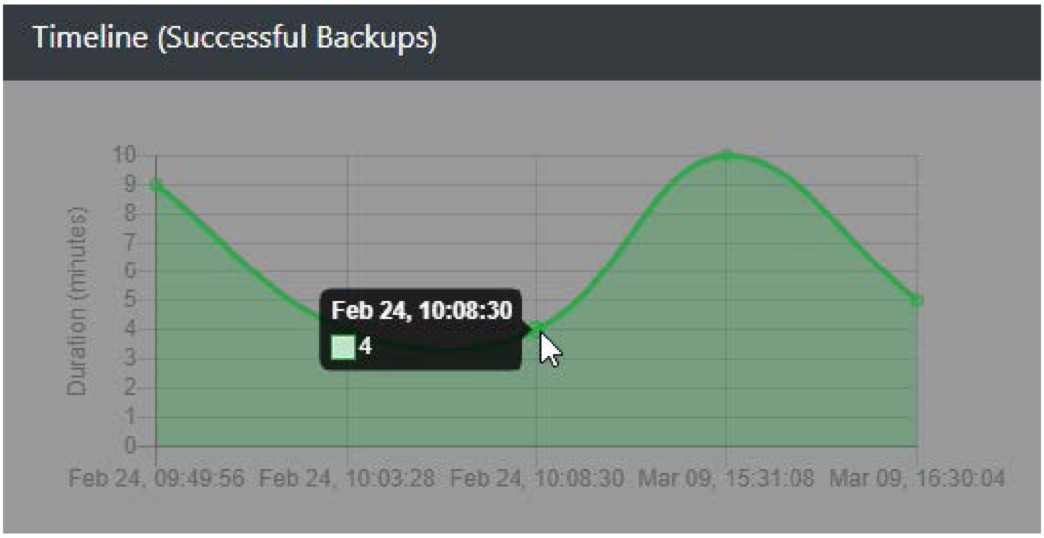
The next phase involves categorization of any runtime anomalies found to create structured log groups containing matched log events. Log groups could include errors such as connectivity, network configuration, dependant systems and user permissions. As an example, one system may be a web application server, which will not work correctly without a database server (i.e., the web application server is a dependent system of the database server within a tiered recovery scenario).

In the final phase the VA will determine any modifications required to the stored configuration of the recovery profile in the virtual test environment based on the outcome of the log file analysis and will attempt to make those changes automatically. The recovery simulation will then be repeated, and the resulting runtime logs will be parsed again to check for anomalies. This cycle will continue until the recovery simulation succeeds without errors in line with the domain knowledge provided by the baseline know-good runtime information. If the VA determines that manual intervention is necessary to resolve a recovery failure, then the ML algorithms will attempt to provide as much guidance as possible to the system administrator via the failure analysis panel within the VA user interface.

Self-assessment

Section 8 of the PRA Supervisory Statement SS1/21 outlines the self assessment requirements firms are required to present to describe their compliance with the operational resilience obligations of the policy, as well as the methodologies they have used to undertake these activities.

The extensive recovery reporting available within the Cristie VA can provide useful validation to support self-assessment documentation. The VA can provide both verbose log files detailing system recoveries in addition to interactive graphs providing a summary display of the duration of each backup. Systems can also be recovered or replicated into an isolated network for boot verification without impacting the production environment. This facility also allows for file integrity testing, the testing of post boot scripts, application verification, application interoperability checks, application upgrade testing, OS upgrades, and any additional automation to test system functionality.



Integration with leading backup solutions

Adding Cristie Recovery to your backup environment allows recovery of operating systems, applications, user configuration and data to any point in time available in your backup software. No additional infrastructure or management is required, all recovery operations can be configured and controled through the Cristie Recovery Virtual Appliance (VA) console. Cristie Recovery seamlessly integrates with backup solutions from IBM, Dell Technologies, Rubrik and Cohesity. Cristie Recovery can also operate as a standalone backup and recovery solution.

Summary

System recovery at scale presents several challenges with physical systems in particular often lacking the automation available within virtual environments. Cristie Software recovery solutions can help overcome these limitations while providing complete flexibility to restore to and from any platform type. Contact our team to learn more about simplifying key aspects of infrastructure recovery to help meet the requirements of operational resilience legislation. Visit the CloneManager® and System Recovery product pages for more information regarding the Cristie Software suite of solutions for system recovery, replication, migration, and ransomware protection.

Email: sales@cristie.com

www.cristie.com