FAQ

Commvault Cloud® Cleanroom Recovery

CYBER RECOVERY 101

1 What is the difference between Disaster and Cyber Recovery?

- **Disaster Recovery:** Restoring entire systems and infrastructure after a large-scale event like a natural disaster, major hardware failure, or long-term power outages.
  - **Example:** Recovering from a server room fire, rebuilding systems after a major hardware failure, and restoring data after a flood.
- **Cyber Recovery:** Recovering specifically from cyberattacks, including data breaches, ransomware, and malware. This could be a subset of data or the entire infrastructure.
  - **Example:** Isolating and eradicating malware, restoring compromised data from clean backups to a clean environment, and identifying and patching vulnerabilities.

Disaster recovery (DR) and cyber recovery (CR) are different approaches to restoring systems after disruptions, but they deal with different threats and challenges. Here are the three main reasons why:

- Disaster recovery handles predictable events like natural disasters or hardware failures, which aren't intentional and do not actively target your data. In contrast, cyber recovery tackles malicious attacks like ransomware or data breaches, where attackers actively try to harm your systems and corrupt your data.
- Disaster recovery usually follows a pre-defined plan with established steps to restore systems quickly. Cyberattacks often involve investigation and remediation before recovery, extending the timeline due to the need to contain the attack and ensure no malware or exploits remain.
- In Disaster recovery, restoring from backups helps get things back online even if some data is lost. However, with cyberattacks, every element of your environment, from hardware to data and backups, must be scrutinized for infection before restoring, as attackers might have hidden malware or altered backup files.

2 What is a cleanroom?

A cleanroom, often termed an Isolated Recovery Environment (IRE), is a secure, separate environment. However, the concept of a cleanroom is more than just a secure physical space. It is a comprehensive approach to cyber recovery, encompassing a secure, standalone environment separate from the production network and meticulous planning, established processes, best practices, testing, and well-defined procedures. The technology behind a cleanroom is not inherently magical; its true power lies in bringing these diverse elements together into a cohesive and effective unit.

3 What is cyber recovery testing?

Cyber recovery testing is a practice run (or operational test) of restoring an application and its data from a backup. This is the kind of restoration process that will happen in a cyber incident, and it is the process that NIST recommends.

4 Why does cyber recovery testing matter?

Resilience. Testing helps to provide resilience and business continuity. Recovering critical applications and data is fraught with complexity and issues. Testing cyber recovery ensures that errors are uncovered and resolved when the stakes are low. Testing ensures that teams are practiced and confident that they can recover all critical applications and data when a cyber incident occurs. In fact, NIST recommends that "backups of data are conducted, protected, maintained, and tested" because "it is better to identify an unexpected issue during testing than during an actual cyber event." But the reality is that very few organizations test fully, frequently, and successfully.

5 Why cleanroom recovery?

As valuable as testing is, very few organizations run comprehensive and frequent operational tests. It's too costly. To test the recovery of an application and its data, you need to be able to replicate the entire environment for each application. It's too expensive to maintain duplicate environments for all critical applications. So, most organizations have cyber recovery plans that review checklists of what needs to happen during recovery. Some organizations go further and simulate what they would need to do to recover from an attack (like a tabletop exercise). However, this leaves organizations unpracticed and unprepared for an incident that threatens their ability to deliver on their mission. Cleanroom Recovery changes that. It combines unique any-to-any portability, which makes it possible to recover ANY workload from ANY location, with an on-demand cleanroom in the cloud. So, an organization can recover any application and data from anywhere and send them to an on-demand cleanroom in the cloud. The result? Critical but ever-elusive cyber recovery testing is now a reality.

COMMVAULT CLOUD CLEANROOM RECOVERY

1 What is Commvault Cloud Cleanroom Recovery?

Cleanroom Recovery provides an affordable, clean, secure, isolated recovery environment on demand for testing cyber recovery plans, conducting secure forensic analysis, and uninterrupted business continuity.

2 What makes our Cleanroom Recovery unique?

Commvault's solution can recover workloads from ANY location to a safe, cloud-isolated cleanroom that helps deliver the strongest and most reliable cyber resilience and readiness. Our key differentiators include:

- Any-to-any portability to recover any workload from anywhere to anywhere. Traditionally, apps and data from various systems would require duplicating all environments to rest and recover.
- Able to leverage a flexible dissimilar Cleanroom target, reducing cost and complexity. Pay for what you need when you need it.
- We start off a cleanroom recovery with a read-only control plane. This helps make certain that the cleanroom environment cannot be accessed even if the production environment is compromised.
- Automated hooks into AI/ML to assist in deciding known good recovery points.

Traditional cleanroom methods are too expensive and complex for most organizations. Other data security solutions with similar offerings are limited to disaster recovery and constrained by a limited set of workloads and recovery options.

3 How can a cleanroom be leveraged?

A cleanroom environment, also known as an "isolated recovery environment" or "sandbox," plays a crucial role in cyber recovery strategies by providing a cost-effective and flexible place for testing, as well as a safe and secure space to analyze, restore, and remediate systems affected by cyberattacks. Here are some key use cases for a cleanroom in cyber recovery:

Continuous Cyber Recovery Plan Testing:

- Organizations can use the cleanroom to simulate cyberattacks and test their incident response plans, identifying and addressing potential weaknesses before facing an actual attack.
- Regular drills using the cleanroom environment can help security and IT teams stay sharp and apply continuous improvements to the cyber recovery plan for effectiveness in real cyberattacks.

Incident Response and Forensics – Post-Mortem Analysis:

- The cleanroom provides a controlled environment for forensic analysts to investigate the attack timeline, identify the attack's origin, and gather evidence for potential legal proceedings.
- Once vulnerabilities are identified, the cleanroom can be used to develop, test, and deploy security patches in a safe and controlled environment before applying them to production systems.

Secure Data Recovery:

- Even if some data is compromised on production systems, a cleanroom can be used to extract clean versions of critical data from uninfected backup sources.
- When production integrity is in question, a cleanroom provides a safe and secure place to begin recovery while the production environment is being remediated.
- In completely compromised environments, a cleanroom allows a safe target to recover from and begin running the business. If a new production environment is desired, clients can move workloads out of the cleanroom when ready.

Cleanrooms are critical in any organization's cyber recovery strategy, leveraging these capabilities to enable faster recovery, minimize data loss, and improve overall resilience against cyber threats.

4 What benefits can customers expect to see using Commvault Cloud Cleanroom Recovery?

- Reduce the complexity and time required for recovery operations with an automated, efficient process for restoring critical systems
- Gain peace of mind by minimizing the risk of malware reinfection and data breaches, leveraging a recovery process powered by a solution designed to address sophisticated cyber threats.
- Discover gaps in your recovery plan and strengthen resilience and readiness with regular recovery plan testing.
- Reduce recovery times and avoid operational downtime to minimize the financial impact of disasters.
- Gain potential cost savings through intelligent resource allocation and downsizing recommendations.

5 What does NIST promote as the best practice for cyber recovery readiness?

NIST recommends that "backups of data are conducted, protected, maintained, and tested" because "it is better to identify an unexpected issue during testing than during an actual cyber event."

6 How is Cleanroom Recovery packaged? What does it cost?

Cleanroom Recovery is currently packaged as a standalone add-on, like Air Gap Protect. It is sold in increments of 10TB. The 10TB measurement is based on the amount of data the customer configures into a Recovery Group, which is based on front-end terabytes.

For example, suppose a customer configures 100TB of data into the recovery groups (based on the data size at the time of configuration). In that case, they must purchase ten units of the 10TB SKU. If the client needs to configure 104TB of data, they must purchase eleven units of the 10TB SKU. A 10-unit SKU is $1,590 USD.

Customers will be notified of the overage if they configure a recovery group within their licensed limits and the data set grows to exceed what they have purchased. In such cases, no further systems or data can be added to the recovery groups until the license overage is remedied.

7 What does the customer need to leverage Commvault Cloud Cleanroom Recovery?

- Cleanroom Recovery SKU
- Air Gap Protect
- Backup & Recovery (from any of the packages)
  - For software: Version 11.36 or higher
  - For SaaS: Version 11.36 or higher
- Any of the Commvault Cloud tiers – Operational Recovery, Autonomous Recovery, Cyber Recovery, Platinum Resilience

8 Is hardware needed to run Cleanroom Recovery?

No hardware is required to run Cleanroom Recovery or Commvault Cloud Backup & Recovery for SaaS; however, you do need hardware to run Commvault Cloud Backup & Recovery software.

9 Does Commvault Cloud Cleanroom Recovery require its own Air Gap Protect?

Cleanroom Recovery does not require its own Air Gap Protect. If the customer is already using Air Gap Protect, they are fine and don't need another location.

10 What new Commvault Cloud Cleanroom Recovery features are now available as of August 2024?

Cleanroom Recovery for Commvault Cloud SaaS:

Commvault has launched Cleanroom Recovery for Commvault Cloud SaaS, allowing users to manage cyber recovery through the SaaS control plane. With dynamic resource adjustments for efficient restoration, receive consistent functionality across software and SaaS offerings. Cleanroom Recovery supports multi-tenancy and can be accessed via APIs for task automation and integration with other systems.

Repave VMs using a "Golden Image":

Cleanroom Recovery of VMs using Golden Image enables customers to use templates (both public marketplace and private custom templates) to create the Azure VM in the cleanroom before restoring the data to the VM. This allows for a clean and efficient restoration.

Granular AD Recovery and Cleanroom Domain Controller Recovery: Domain-wide comparisons allow you to compare the entirety of the AD domain, or a portion of it, and report on all objects and attributes that have changed between backups or between a backup and the live state of the directory. They also provide an easy way to add a single domain controller to the AD recovery group so it integrates smoothly with the existing directory services structure.