January 2025

Commvault®

CLEANROOM RECOVERY

Essential Guide

Table of Contents

Overview

A cleanroom, often termed an Isolated Recovery Environment (IRE), is a secure, separate environment that's uncontaminated . 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. It requires 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.

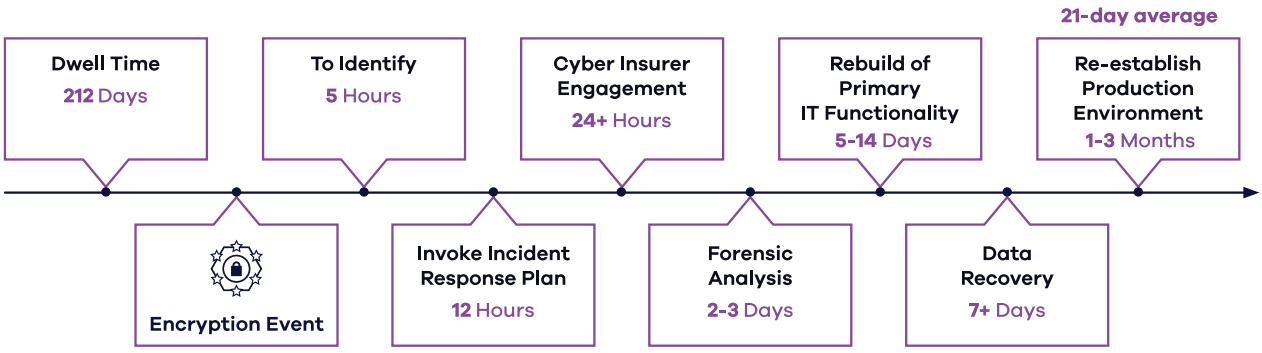
To truly appreciate the power of a cleanroom, you must first understand the challenges that necessitate its existence. Cyberattacks have escalated dramatically in recent years, posing a substantial threat to organizations across all industries. These attacks can have devastating consequences, including data breaches, financial losses, and irreparable reputational damage.

CYBER ATTACKS: A RETROSPECTIVE

- Let's go back and look at why cleanrooms have become **critical** to your overall cyber-resiliency posture.
- Most cyberattacks begin without malware. This means that regardless of how strong of a frontline defense your security has, it will not stop the attackers from gaining access. Attackers today no longer hack in. They login.
- Once the attacker has gained access, the average time they are in an enterprise, according to IBM's Security Group, is 212 days. Within the first 84 minutes, according to CrowdStrike, attackers are moving laterally. This means that during those 212days, attackers quietly move east and west throughout the environment. These 212days are known as left of bang.
- When attackers enact the encryption event, "bang", the damage is so pervasive that on average recovery from a cyberattack takes 24 days just to restore their critical systems. The days spent analyzing and recovery from the cyberattack are known as right of bang.
- Companies that don't have a recovery option and decide to pay the ransom do not fare better. Over 90% of companies that pay the ransom do not get all their data back. On average they recover less than 70% of their data. Additionally, companies are discovering that decryption times far exceeds the time it would have taken to restore from backups.
- Often, businesses that pay the ransom are attacked again within a month because they are still operating in an infected environment.

A TRUE TIMELINE OF A TRADITIONAL CYBER RECOVERY

Having established the severity of cyberattacks, let's take a closer look at a typical incident timeline.



- This timeline has been generated based on actual cyber recoveries. Let's examine some of the critical points of the timeline.
- After signs of an attack have been identified, an individual with the proper authority must declare the breach and initiate the Incident Response Plan.
- Once initiated, the first three to four days are taken up by processes outside of recovery.
- 98% of all companies use Active Directory; Active Directory is attacked in almost every breach. Therefore, a clean Active Directory must be recovered or created before any other recovery can begin.
- Many attacks are so devastating that the environment cannot be fully recovered. Businesses are left scrambling for hardware and a location to recover when this happens.
- Data protection solutions are often targeted during an attack because they are a single repository holding all the companies' critical data and are the last line of defense for recovery.

DIFFERENT TYPES OF RECOVERY

There are three types of recovery: operational, disaster, and cyber. These terms deal with restoring systems after disruptions but have distinct scopes and approaches. Here's a breakdown of the differences:

Operational recovery

- **Scope:** Recovering specific system components, files, applications, or virtual machines after a minor disruption or outage.
- **Examples:** Restoring accidentally deleted files, recovering from application crashes, and fixing corrupted data.
- **Goals:** Minimize downtime and data loss and quickly resume normal operations.
- **Methods:** Granular backups, point-in-time recovery, automated recovery processes.

Disaster recovery

- **Scope:** Restoring entire systems and infrastructure after a large-scale event like a natural disaster, major hardware failure, or long-term power outages.
- **Examples:** Recovering from a server room fire, rebuilding systems after a major hardware failure, and restoring data after a flood.
- **Goals:** Ensure business continuity, minimize long-term impact, and protect critical data.
- **Methods:** Full system backups, off-site replication, and disaster recovery plans.

Cyber recovery

- **Scope:** Recovering specifically from cyberattacks, including data breaches, ransomware, and malware. This could be a subset of data or the entire infrastructure.
- **Examples:** Isolating and eradicating malware, restoring compromised data from clean backups to a clean environment, and identifying and patching vulnerabilities.
- **Goals:** Minimize damage from cyberattacks, prevent data loss, and maintain security posture.
- **Methods:** Security information and event management (SIEM), cyber recovery plan, anomaly detection, air gap, cleanroom.

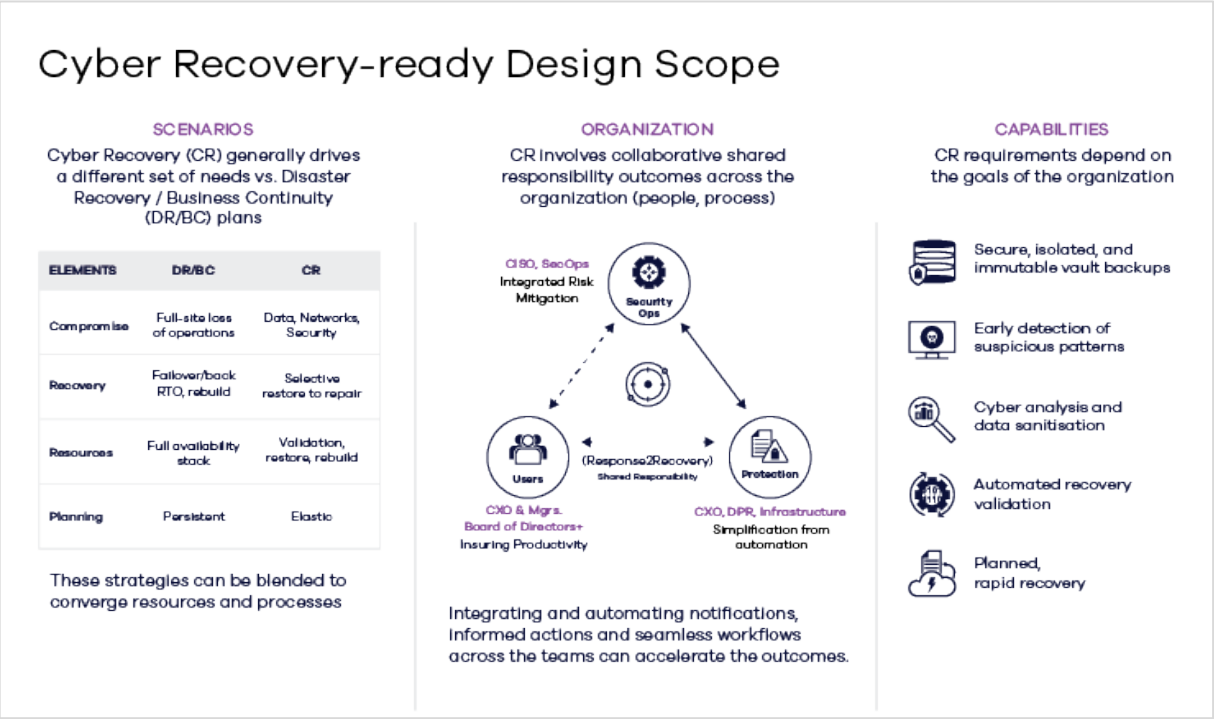
	Operational Recovery	Disaster Recovery	Cyber Recovery
Scope	Individual components	Entire systems and infrastructure	Cyberattacks
Example	Recovering deleted files, application crashes	Server room fire, ransomware attack, flood	Data breach, malware infection
Goals	Minimize downtime, resume normal operations	Business continuity, protect critical data	Minimize cyberattack damage, prevent data loss
Methods	Granular backups, point-in-time recovery	Full system backups, off-site replication	SIEM, cyber recovery plan, anomaly detection, air gap, cleanroom

WHY DISASTER RECOVERY ISN'T CYBER RECOVERY

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

1) 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.
2) 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 check for malware or any remaining exploits.
3) 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.



WHY DISASTER RECOVERY PLANS WON'T WORK IN A CYBER RECOVERY

While both aim to restore operational functionality after disruptions, fundamental differences necessitate distinct responses. Traditional disaster recovery (DR) plans struggle to effectively address the nuanced threats and complexities posed by cyberattacks. Here is why:

Nature of the threat: Unlike natural disasters or hardware failures, cyberattacks are deliberate acts of aggression orchestrated by intelligent actors. These adversaries actively exploit vulnerabilities and target specific data, necessitating a more meticulous and security-centric approach than a standard disaster recovery playbook.

Scope and focus: Disaster recovery primarily focuses on rapid system restoration and minimizing downtime, even if some data loss occurs. In contrast, cyber recovery prioritizes isolating the attack, eradicating malware, and ensuring complete security before initiating data restoration. This involves forensic investigations, vulnerability patching, and potentially longer remediation processes for thorough cleansing and enhanced security posture.

Methods and tools: Disaster recovery typically relies on readily available backups in combination with replication and established procedures for quick system rollback. Cyber recovery, however, necessitates specialized tools and expertise in malware analysis, incident response, immutable/indelible backups, cleanrooms, anomaly detection, and secure data extraction. Additional skills in patching vulnerabilities and hardening the environment are critical to prevent future intrusions.

Data integrity and vulnerability: Cyberattacks can compromise backups and specific data within systems. Disaster recovery plans cannot effectively identify and restore clean data, potentially propagating the infection. Additionally, security vulnerabilities exploited during the attack may require patching before restoring backups, introducing another layer of complexity to the recovery process.

Therefore, while disaster recovery plans provide a valuable foundation for incident response, relying on them in the face of a cyberattack can be perilous. A dedicated cyber recovery plan, backed by specialized tools, personnel, and frequent testing, is essential for mitigating these malicious attacks' specific risks and complexities.

RPO/RTO AND THEIR LIMITATIONS IN CYBER RECOVERY

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are invaluable metrics in disaster recovery, defining acceptable data loss and restoration timeframes. However, several factors make their direct application problematic in cyber recovery.

Identifying and isolating clean data from potentially infected backups can be challenging, making it difficult to define a clear RPO. Forensic investigations and deep analysis may be required to confidently deliver data integrity before restoration.

The time needed for investigation, remediation, and secure restoration can vary significantly depending on the attack's complexity and scope. Setting a fixed RTO in a fluid environment can be misleading and counterproductive.

While minimizing data loss is important, cyber recovery prioritizes securing the entire environment and preventing further compromise. This holistic approach, encompassing system hardening and vulnerability patching, extends the recovery timeline beyond a pre-defined RTO.

RTO and RPO strategies rely heavily on critical items of the environment, such as Active Directory, databases, and even network switch configurations, leveraging replication for protection. During a cyberattack, replication cannot be trusted since replication has no built-in anomaly detection propagating compromised accounts, exploits, or hidden infections. Since replication cannot be trusted, these items must be rebuilt, adding to the time required for recovery going beyond the standard RTO and RTO.

Sole reliance on conventional disaster recovery plans and rigid adherence to RPO/RTO metrics during cyberattacks can leave organizations exposed. Recognizing this, CISOs are shifting their focus toward Maximum Allowable Downtime (MAD) or Maximum Tolerable Downtown (MTD).

MAD or MTD offers a more holistic perspective on cyber resilience. Rather than solely emphasizing data and system restoration to a specific point, it defines the maximum duration of outage an organization can sustain without significant harm. This comprehensive lens encompasses the entire incident response lifecycle, from initial attack to full business resumption, including impacts on people, processes, and technology.

Implementing a dedicated, security-focused cyber recovery plan with tools and expertise is crucial for achieving successful and secure restoration while minimizing damage and enhancing future resilience. Remember, disaster recovery and cyber recovery plans are essential for robust organizational resilience against any disruption.

USE CASES

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 the integrity of production is in question, a cleanroom allows for 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 into and begin running the business from. If a new production environment is desired, clients can move workloads out of the cleanroom when ready.

By leveraging these capabilities, cleanrooms are critical in any organization's cyber recovery strategy, enabling faster recovery, minimizing data loss, and improving overall resilience against cyber threats.

When is Cleanroom Recovery Not Recommended

While cleanrooms offer significant advantages for cyber recovery, there are situations where there might be better solutions. Here are some cases where using a cleanroom might not be recommended:

Insufficient data redundancy:

- Cleanroom Recovery relies on clean backups for restoring data. If adequate backups are unavailable or have not been properly isolated from the attack, the cleanroom environment becomes less helpful.

Highly specialized systems:

- Certain complex systems might depend on specific hardware or software configurations that cannot be easily replicated in a Cleanroom Recovery.

Inability to use the cloud:

- If regulations do not allow clients to run workloads in a cloud environment, they cannot take advantage of Cleanroom Recovery.

The decision to use a cleanroom for cyber recovery depends on many factors, including the organization's risk profile, resources, and the nature of the cyberattack. Carefully evaluating the specific situation and comparing the benefits and drawbacks is crucial for choosing the most effective approach.

Remember, a cyber recovery strategy should be comprehensive and multi-layered, utilizing different methods and tools depending on the circumstances. While cleanrooms provide valuable capabilities, considering alternative approaches and understanding their limitations deliver a well-rounded defense against cyber threats.

WHAT IS CYBER RESILIENCE

Having delved into the intricacies of cyberattacks, the nuanced differences between cyber and disaster recovery, and the critical role of cleanrooms, let's now explore the essential concept of cyber resilience.

Imagine your organization's digital infrastructure as a sophisticated organism. Much like a robust immune system protects against physical threats, cyber resilience empowers your systems and data to withstand, recover from, and adapt to cyberattacks and digital disruptions. This holistic approach transcends technology, demanding seamless collaboration across people, processes, and technology within every department.

The Fortifying Pillars of Cyber Resilience

- **Prevention:** Proactive security measures like firewalls, intrusion detection systems, and data encryption minimize attack surfaces and vulnerabilities, acting as your digital shield.
- **Planning:** Comprehensive cyber response and recovery plans outline breach handling and business restoration procedures, ensuring preparedness for any digital onslaught.
- **Testing:** Regular simulated cyberattacks refine and validate response plans, simulating real-world scenarios and demonstrating your organization's ability to recover.
- **Detection:** Swift identification and understanding of attacks enable rapid response and mitigation, minimizing damage and impact before they escalate.
- **Response:** Immediate action to contain the attack and its consequences, preventing further disruption and loss. Think of this as the digital equivalent of quarantining a virus.
- **Recovery:** Efficient restoration of systems and data to ensure business continuity and data integrity. This is akin to rebuilding stronger after an attack, ensuring your digital infrastructure remains robust.
- **Adaptation:** Continuous learning and adaptation from past tests and incidents refine security and recovery posture, preparing for future threats. Think of this as evolving your digital immune system to be even more resilient.

Why Prioritize Cyber Resilience

The pervasiveness of cyber threats necessitates a collective effort towards resilience. By securing digital assets, actively learning about threats, adhering to best practices, rigorously testing recovery plans, and practicing recovery strategies, everyone within your organization contributes to building a fortress against digital threats.

Remember:

- Regular security assessments, penetration testing, and recovery testing expose vulnerabilities for proactive remediation, ensuring your digital defenses are constantly patched and updated.
- Employee training in cyber awareness and best practices combats human error risks, empowering your team to be the first line of defense against phishing and social engineering attacks.
- Continuous updates on emerging threats, implementation of appropriate security measures, and ensuring systems can be recovered are crucial for staying ahead of the curve and adapting your defenses to the ever-evolving threat landscape.
- By fostering a culture of cyber resilience, we collectively build a more secure and resilient digital landscape for everyone.

Details of Cleanroom Recovery

Currently, Commvault Cleanroom Recovery automates the recovery of the Commvault Cloud Control Plane into a Commvault Cloud SaaS tenant. Then, it automates the recovery of virtual machines out of Commvault Cloud Air Gap Protect into a client-provided Azure tenant based on the recovery groups that are defined.

It is important to note that we are not the target Azure tenant as a service; our focus initially lies on simplifying and streamlining our client's cleanroom recovery process within their Azure tenant. The term "Cleanroom as a Service" should not be used to refer to our Cleanroom Recovery solution.

AUTO-SCALING RECOVERY

In the face of increasingly sophisticated cyberattacks, organizations need a robust and agile data protection strategy. Auto-scaling recovery is a cornerstone of Commvault's Cleanroom Recovery solution, designed to address the complexities of modern data recovery. When disaster strikes, the last thing clients want to worry about is managing the underlying infrastructure. Auto-scaling eliminates this concern by automatically adjusting the number of recovery machines based on workload demands. This intelligent approach delivers optimal performance, rapid recovery times, and cost-efficiency.

By dynamically scaling resources up or down, auto-scaling not only accelerates recovery but also drives cost efficiency. Additionally, it optimizes resource utilization, reducing unnecessary expenses. For Cleanroom Recovery, these scaling operations occur within the client's Azure environment, preserving data sovereignty and control. This unique combination of automation, performance, and security makes auto-scaling an invaluable asset for any organization seeking to bolster its cyber resilience.

REPAVE VM

Following a sophisticated cyberattack involving exploits and compromised accounts, the cleanliness of the data is the key to a successful recovery. The Repave process provides a robust solution by providing an unaffected system and reinstalling them with clean, verified software. This approach effectively creates a fresh starting point for recovery.

While malware can be removed, there may still be other vulnerabilities or backdoors that the attacker has exploited. To verify the integrity of restored systems, Repaving the virtual machine using a trusted known-good image acts as a safeguard against such risks. This process involves reinstalling the VM's operating system from a known-clean, verified image. By using this method, organizations can be sure that recovered applications are free from malware and other threats. This results in a more robust and secure system.

The Pave and Repave process, coupled with the use of secure known-good images, is a critical component of a comprehensive cyber-recovery strategy. By implementing these measures, organizations can significantly reduce the risk of reinfection and improve their overall cyber resilience.

RECOVERY SCRIPTS

Following a recovery, various actions may need to be taken to ensure data integrity and identify potential threats. This often involves executing pre-defined scripts to validate data or using third-party tools to scan for Indicators of Compromise (IoCs), Indicators of Attack (IoAs), or malware.

To mitigate the risk of executing compromised scripts, cleanroom recovery groups and individual entities should store scripts in a secure, isolated repository. This prevents accidental access to infected servers and reduces the likelihood of encountering encrypted or malicious scripts.

In a cleanroom environment, safe, protected scripts can be uploaded directly to the isolated recovery environment for the entire group or individual entities. Once uploaded, these scripts can be reordered to execute in the desired sequence, providing flexibility and control over the recovery process.

For information on how to configure recovery scripts please see documentation online.

GENERAL RECOMMENDATIONS

1. Confirm Commvault has local users not tied to Active Directory
2. Verify at least one full backup for each virtual machine to be recovered is present in Air Gap Protect
3. Must have access to cloud.commvault.com
4. Must have recovery manager rights within cloud.commvault.com
5. Must have any Commvault Cloud Software license, version 11.34.13 or higher
6. The source VMs must use Indexing Version 2. If the source VMs are using Indexing Version 1, migrate them to Indexing Version 2 using the VSA V1 to V2 Migration workflow.
7. Azure requires VM names do not contain special characters, whitespace or begin with '_' or end with '.' or '-'.
8. Must be actively backing up virtual machines to be recovered in the cleanroom
9. Must be using Air Gap Protect as secondary / tertiary copy for those virtual machines to be recovered from previous requirement
10. Ensure your Control Plane (CommServe) database backup is newer than the required recovery date.
11. A client provided clean Azure subscription and tenant.
12. A resource group and storage account are created in the Azure cleanroom.
13. The following network resources are already configured in the Azure cleanroom site:
    - Gateway, IPv4/IPv6 ranges defined, DNS, firewall policies, DNS updates, TTL, public and private IP registration, and network encapsulation to prevent outbound communication.
14. IAM access is set up to access the Azure resources.
15. Ensure that Linux servers have Hyper-V drivers installed. See documentation.
16. Ensure Azure VM agent is installed on virtual servers
17. Remote Desktop Protocol (RDP) or SSH must be enabled on the source VM.
18. For Linux VMs, integration services should be enabled on the source VMs if they will be powered on automatically after conversion.
19. For Windows VMs, enable SAN policy for the source VM.
20. VMs that are encrypted on AWS are created as VMs with no encryption on Azure.

21. If your source data is encrypted, you have the key management service and encryption key configured in the Azure cleanroom recovery site. Also, the key management service has been added to Commvault. For more information, see Managing a Key Management Server
22. Active Directory, free of infection, available in the cleanroom.
23. Supported source virtual machines also supported by Azure
    - Supported Azure virtual machines (VMs) for Linux and **Windows:** https://azure.microsoft.com/en-us/solutions/linux-on-azure
    - **Microsoft server software support for Azure virtual machines:** https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/server-software-support
    - **Azure product availability by region:** https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/regions
24. Recovered VMs will be automatically cleaned up (deleted from the cleanroom target) seven days after the Control Plane Recovery. Contact support if you would like to request the recovered VMs be kept for a longer. If you want to transition the recovered VMs into production, please work with Commvault professional services and your local service providers.

SECURING SYSTEM AND APPLICATION ACCESS CREDENTIALS STORED IN THE CONTROL PLANE

This Control Plane contains a secure set of system and application credential passwords to connect and orchestrate various data management operations automatically. We recommend that users secure and encrypt those records using one of the two approaches. When the records are encrypted, the critical data remains encrypted across all recovery instances and recovery scenario.

Option#1 Password store is secured with an External KMS

This option will encrypt the credential password collection and an external KMS relationship. This security lock confirms that persistent password records in the DB are secured from prying eyes who may gain access to the production Control Plane, any recovery instance, DR testing, or Cleanroom scenarios.

The password collection cannot be unlocked without the authorized access/public key delivered from the external KMS service. This authorization action is session-based; the decryption key is not stored or cached in the Control Plane.

- This method requires the external KMS service to be always available for CS operations.
- See documentation.commvault.com for Modifying the Key Management Server That Stores Passwords for a CommCell Environment

#2 Password store is secured with a local passphrase KMS.

This option will encrypt the credential password collection using a local passphrase KMS. The passphrase will be stored locally in a minimum of (2) locations but external to the Control Plane. All access will require successful resolution to the passphrase file. This security lock ensures that persistent

password records in the Control Plane are secured from prying eyes who may gain access to the production Control Plane, any recovery instance, DR testing, or Cleanroom scenarios.

This method ensures that the password collection can only be unlocked by resolving to the proper local passphrase key file. This authorization action is session-based; the decryption key is not stored or cached in the Control Plane.

- This method requires the Administrator to ensure the passphrase file is protected and secured external to the Control Plane.
- As the file will reside on the host system, if it is lost during a system reboot, upgrade, or compromise, the Administrator will need to replace it for normal operations.
- In a DR or Cleanroom recovery scenario where the Control Plane will be recovered on a new system, the administrator will need to reapply the passphrase file and register the new location to enable the relationship.
- See documentation.commvault.com for Adding a Passphrase Key Management Server

In both scenarios, the user has complete control over the master encryption keys that protect the credentials. This approach, where you control the encryption keys, provides a robust layer of security for your credentials. When the encryption controls are active, the credential data is fully protected and severs all connections to external systems. Commvault Support or Engineering cannot revoke or bypass the encryption state. Administrators must take precautions to secure the external keys (KMS) to confirm they are always available for the Control Plane.

CLEANROOM RECOVERY PROCEDURE SUMMARY

Here are the steps you will take to initiate Cleanroom Recovery.

- **Recover the control plane:** Log into cloud.commvault.com and initiate the Control Plane recovery process. You will receive emails notifying you of the start and completion of the Control Plane recovery.
- **Prepare the recovery environment:** Create a separate Azure tenant.
- **Create a recovery group:** Create a recovery group by walking through the initial setup wizard, then add the workloads you want to recover, or choose an already existing recovery group and initiate the recovery.

  *For a fully detailed walkthrough, please see the field guide below.

SUPPORT MATRIX

The below list shows the tested any-to-any cross hypervisor restore into Cleanroom Recovery. Commvault organically supports a much broader range of sources and targets; as those workloads are validated, they will be supported in Cleanroom Recovery.

Source	Destination: Cleanroom Recovery Azure
On Premises VMware	Yes
AWS VMC	Yes
Azure VMware Solution	Yes
Google Cloud VMware Engine	Yes
Oracle Cloud VMware Solution	Yes
Azure VMs	Yes
AWS EC2	Yes
Hyper-V	Yes

Application	VM Operation System	VM Backup Type
Active Directory	Windows	Application consistent backup
DB2	Windows	Application consistent backup
DB2	Linux	Crash consistent backup
Oracle	Windows	Application consistent backup
Oracle	Linux	Crash consistent backup
MS-SQL	Windows	Application consistent backup
MS-SQL	Linux	Crash consistent backup
EPIC (InterSystems IRIS/Caché database)	Linux	Crash consistent backup

Note:

- Only standalone Active Directory recovery is supported.
- Only databases that are hosted in a standalone setup are supported.
- VMs with independent disks are not supported.
- If a file system that is hosting EPIC database is directly on a disk, identify the correct disk and update the fstab file with an appropriate restored disk for the file system.

Validation Checks for Active Directory

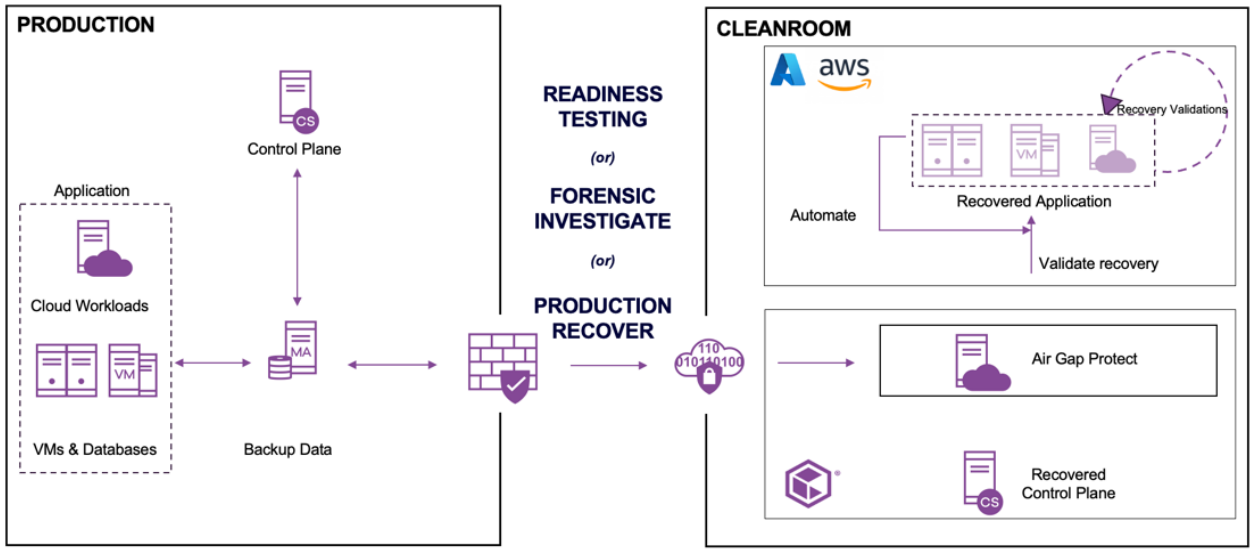
Leveraging Cleanroom Recovery's application validation capabilities, you can verify the health of your Active Directory environment after a recovery. For VMs containing Active Directory, Cleanroom Recovery automatically performs health checks if the Commvault AD agent is installed within the VM. During this process, the software validates critical Active Directory services essential for user authentication and domain functionality. These checks include:

- Netlogon Service: Manages authentication health check in Active Directory.
- NTDS Service: Stores and replicates the Active Directory database.
- KDC Service: Issues Kerberos tickets for user authentication.

- DFSR Service: Replicates Active Directory data between Domain Controllers (DCs).

EXAMPLE CLIENT ENVIRONMENT AND RECOVERY PROCESS

Figure 4 below illustrates what a client environment would look like today for a Commvault software client. The Recovered Control Plane will be in the same region as the Air Gap Protect storage (e.g., US Central). The target environment should be in the same region.



* Recovered VMs will be automatically cleaned up (deleted from the cleanroom target) seven days after the Control Plane Recovery. Contact support if you would like to request the recovered VMs be kept for a longer. If you want to transition the recovered VMs into production, please work with Commvault professional services and your local service providers.

BUY VS. BUILD

While creating a custom cleanroom target on-premises or in the cloud is technically feasible, replicating the comprehensive functionality and ongoing development of Cleanroom Recovery presents a significant challenge. This situation reflects a classic "buy vs. build" decision with trade-offs to consider. While building a custom solution offers initial flexibility, the effort required to maintain feature parity with Cleanroom Recovery (including evolving workloads, security enhancements, automation tools, and integrations) can quickly become resource-intensive and unsustainable. As Cleanroom Recovery continuously adds new features and capabilities, the gap between a custom solution and its offerings will widen. Organizations considering this path should carefully evaluate the long-term development and maintenance costs compared to the immediate benefits of a custom- built solution.

Building your own “Cleanroom-like” functionality like Cleanroom Recovery can accomplished by manually purchasing Control Plane Recovery & Validation and Auto Recovery to set up your own cleanroom. However, as previously mentioned, while this is possible, there is no entitlement to future improvements packaged within Cleanroom Recovery, widening the gap between Cleanroom Recovery and a custom solution.

KEY DIFFERENTIATION

Regardless of the data type or where it sits, we can recover it in Azure with Cleanroom Recovery. This ability allows everybody to begin testing their Cyber Recovery plans, something that has been very challenging before. As validation continues other cloud platforms will soon be available.

Commvault can dynamically convert source data to the target, allowing us to facilitate cost-effective cyber recovery tests. Since we can convert to a dynamic environment, we can simplify and reduce the overall cost of testing – which is a key differentiator.

ANOMALY DETECTION

Commvault is the only solution that will do anomaly detection in all aspects: on the source machines, in flight, after the backup, and in threat deception. These measures will help clients to quickly identify if they have been a victim of a cyber event, assist in establishing the blast radius and reduce the time to recovery.

COMMON MISCONCEPTIONS

The reality is that many organizations conflate disaster recovery with cyber recovery. It's important to understand the difference between basic disaster recovery (DR) preparedness and being truly ready for malicious attacks. While traditional disasters offer a degree of predictability, cyberattacks are chaotic and unpredictable.

The pervasive and adaptable nature of attackers creates a fundamental uncertainty: we can never be confident to the true extent of the compromise. This inherent ambiguity demands a proactive approach beyond static plans. Continuous testing is the cornerstone of building cyber resiliency.

Traditional DR exercises, often scripted and predictable, fall short in simulating the complexities of cyberattacks. Tabletop exercises run through realistic attack scenarios more effectively, mimicking the chaos and pressure of a real-world incident. This helps you identify weaknesses in your plan and response procedures before an actual attack occurs. The problem, however, is that performing a true real-world recovery requires a place to recover, which is complex and cost prohibitive. Commvault Cleanroom Recovery, however, offers a cost-effective and flexible solution to bridge this gap by providing a secure, isolated environment for realistic cyber-recovery testing.

Your organization can confidently navigate the ever-evolving cyber landscape by embracing continuous testing within a secure, controlled environment. Commvault Cleanroom Recovery empowers you to build true cyber resilience, delivering continuous business and data protection in the face of sophisticated attacks.

Field Guide

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.

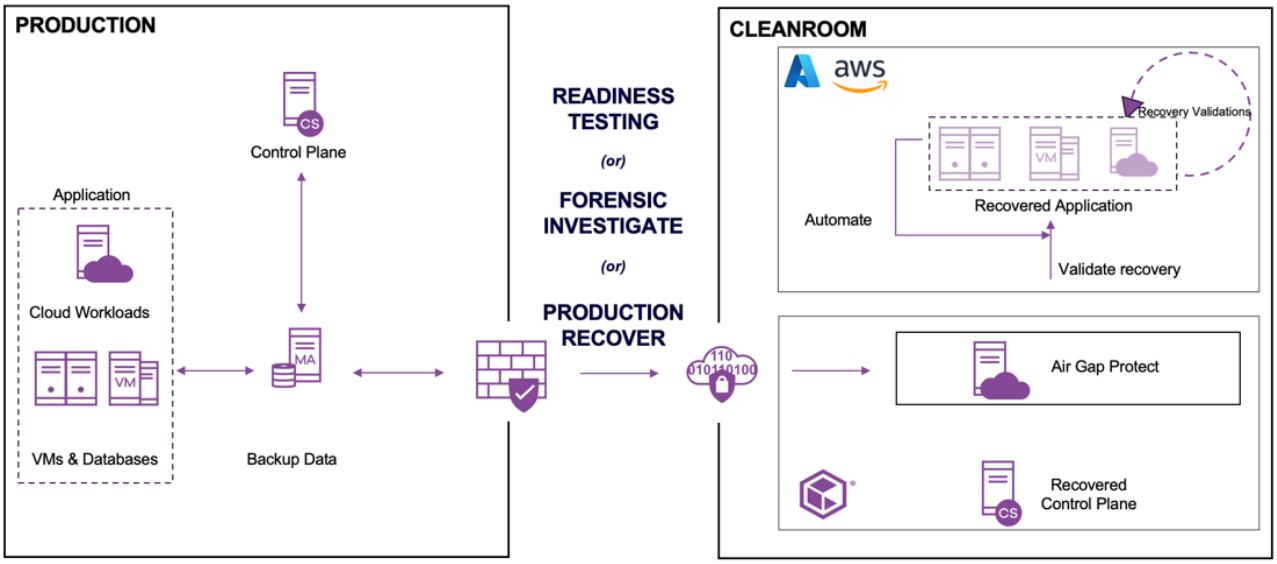
This document aims to provide more technical details to but does not substitute Commvault Documentation which is constantly updated. For future reference, this is the link to Commvault Documentation for Cleanroom Recovery.

USE CASES

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 the integrity of production is in question, a Cleanroom allows for 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 into and begin running the business temporarily from. If a new production environment is desired, clients can move workloads out of the Cleanroom when ready.

By leveraging these capabilities, Cleanrooms are critical in any organization's cyber recovery strategy, enabling faster recovery, minimizing data loss, and improving overall resilience against cyber threats.



Design guidelines

Introduction Azure and Commvault features & items description

Azure environment must be built to represent an isolated environment hosting recovered resources. A Cleanroom is based on multiple items, which will be described in the below table.

Item	Description	Setup best practices
Commvault Cloud Subscription	This is the Azure subscription, owned by Commvault. This is where Cleanroom Control Plane and Air Gap Protect are hosted.	None
Cleanroom Control Plane	The Cleanroom Control Plane is a recovered CommServe, locked in “Cyber Recovery” mode, which means it is activated only for Cleanroom recovery purposes. No backup can be done nor other activities. Cleanroom CommServe is available via Command Center only.	None
Air-Gap-Protect (AGP)	Commvault Air Gap Protect is an air-gapped, immutable online cloud storage, hosted on Microsoft Azure or Oracle Cloud.	
Regions	An Azure region is a geographical area in which one or more physical Azure data centers reside. These data centers exist as part of a latency-defined perimeter to offer the best possible performance and security to users. Azure has more than 60 announced regions, which is more than all other cloud providers to date.	Take note of AGP region. Build the Cleanroom(s) in the same region as AGP region(s).
Azure Subscription	An Azure subscription is a logical container used to provision resources in Azure. It holds the details of all your resources like virtual machines (VMs), databases, and more.	Create a dedicated subscription to host the Cleanroom. An existing one should not be used.
Azure Virtual Network (VNET)	Azure Virtual Network is a service that provides the fundamental building block for your private network in Azure. An instance of the service (a virtual network) enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. A VNet exists within a single region, and all subnets within that VNet must reside in the same region.	At least 1 VNET needs to be present in Azure Cleanroom subscription. In case of multiple regions involved, you would need to build multiple VNETs. Connectivity between VNETs and region is not required on Commvault side but depends on customers’ decision about which kind of testing needs to be done.

Azure Subnet	A subnet is a range of IP addresses in the virtual network. You can divide a virtual network into multiple subnets for organization and security. Each NIC in a VM is connected to one subnet in one virtual network.	At least 1 Subnet should be built for Access Nodes (Auto-Scale / CloudBurst) as it needs outbound access towards Cleanroom and AGP IPs. At least 1 Subnet should be built for recovered VMs – the subnet represents the real Cleanroom.
Azure Resource Group	A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group.	At least 1 Resource Group should be built for everything related to Commvault Infrastructure. At least 1 Resource Group should be built for VMs recovered in the Cleanroom. Customer can create 1 RG per Cleanroom or 1 RG representing all Cleanrooms.
Azure Network Security Groups	Azure Network Security Groups (NSGs) are vital for controlling network traffic in virtual networks within the Azure platform. They employ a set of rules that allow or deny network traffic based on specified conditions, including source and destination IP addresses, ports, and protocols.	Cleanroom Infrastructure (Access Nodes): if enabled via Public IPs, nothing is required. But as this might be a security issue, it's recommended to allow outbound traffic from Infrastructure Subnet to: Cleanroom CS IP (discovered only during CR Recovery), ports 8400 / 8403 TCP AGP, port 443/TCP
Commvault Hypervisor Pseudo Client	A pseudo-client is a logical CommCell entity that represents an Azure Subscription. It needs to have at least one Access Node enabled (the machine which will interact with Azure APIs).	Create a Cleanroom Hypervisor Pseudo Client on source environment.
Commvault Auto-Scale for restores / Cloudburst recovery	With auto-scaling, the Commvault software deploys access nodes in Azure regions only when they are needed, and then uses power management (enabled by default) to power off and decommission the access nodes soon after you use them. Auto-scaling, combined with power management, can reduce the cost of using Azure access nodes to back up VMs.	Enable it on the Cleanroom Hypervisor.

Cleanroom use cases – design & illustrations

- Simple Cleanroom – Single region

A "single-region" Cleanroom deployment is best suited for organizations that want a straightforward, **isolated recovery environment** without extending across multiple geographic locations. In this scenario, **all Cleanroom resources** live in a single Azure region (e.g., West Europe), greatly simplifying networking and deployment.

This requires:

One Virtual Network (VNET)

- As shown in the diagram's right-hand (blue) box for the "Customer CleanRoom Subscription," there is a **single Azure VNET** dedicated to the Cleanroom.
- This VNET provides a **logical boundary** that segments your recovery environment from your production workloads.

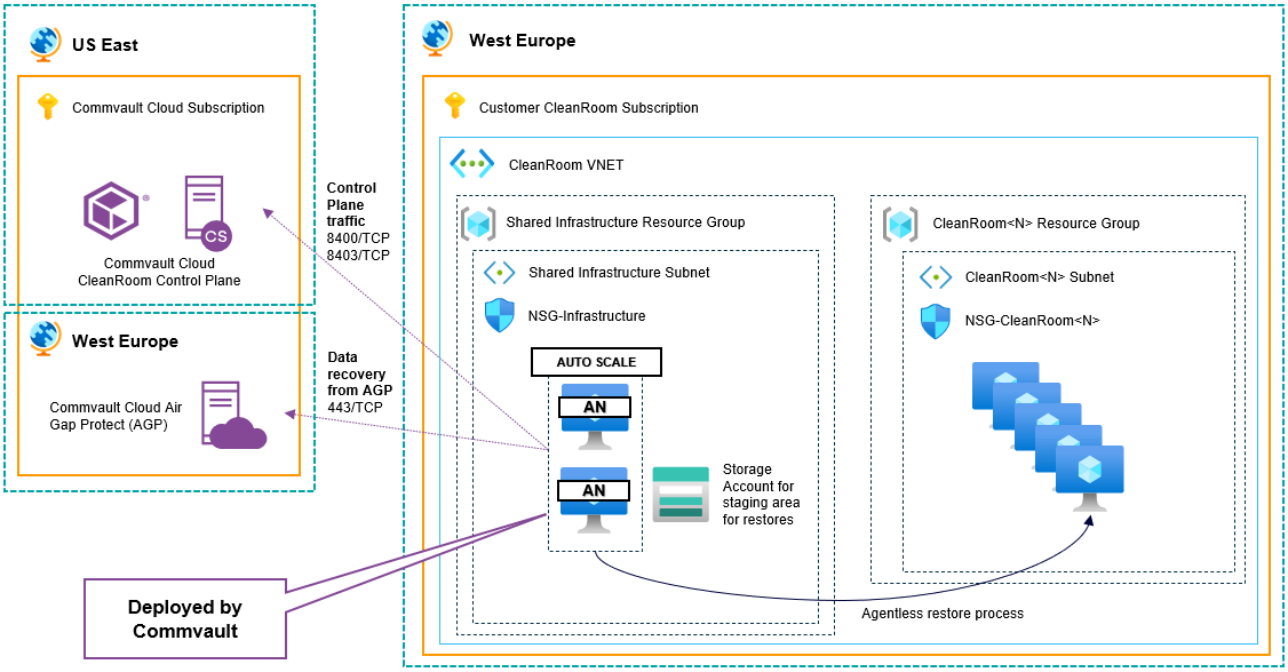
Minimum Two Subnets

- Inside this single VNET, you typically define **two subnets**:
- **Infrastructure Subnet** – Hosts shared infrastructure components, such as the **auto-scaling Access Nodes (AN)** and a **storage account** for staging area restores. It is visually represented in the "Shared Infrastructure Resource Group" portion of the diagram. Outbound connectivity is **enabled** here—often via public IP addresses on the Access Nodes or security rules in the Network Security Group (NSG)—so that it can communicate with Commvault Cloud and fetch data from AGP.
- **Cleanroom Subnet** – A dedicated isolated subnet (or potentially multiple subnets) where **actual Cleanroom workloads** are restored and validated. This is shown in the diagram under "Cleanroom- Resource Group."
- Each subnet has its own **Network Security Group** (NSG) to restrict and control inbound/outbound traffic. In the figure, you see NSG-Infrastructure for the Infrastructure Subnet and NSG-CleanRoom- for each Cleanroom Subnet. These NSGs ensure **isolation** and security of restored data, helping prevent any unwanted traffic between the infrastructure components and the Cleanroom environment.

Auto-Scaled Access Nodes

- In the Shared Infrastructure Subnet, you can see multiple Access Nodes (AN), this **auto-scaling** feature dynamically adjusts the number of Access Nodes available based on workload demand, ensuring **optimal performance** during large or parallel restore operations.
- **Control-plane traffic** (ports 8400/TCP and 443/TCP) flows between Commvault Cloud and the Cleanroom, while **data recovery traffic** (443/TCP) comes from the Commvault Cloud Air Gap Protect (AGP) service.
- This design allows Commvault to **securely provision** and manage Cleanroom resources within the customer's Azure subscription, while maintaining a strong **air-gapped** posture.

Control-plane traffic (ports 8400/TCP and 443/TCP) flows between Commvault Cloud and the Cleanroom, while **data recovery traffic** (443/TCP) comes from the Commvault Cloud Air Gap Protect (AGP) service. This design allows Commvault to **securely provision** and manage Cleanroom resources within the Azure subscription, while maintaining a strong **air-gapped** posture.



Advanced Cleanroom – Multi-Region Cleanrooms

In an advanced deployment, you may choose to provision **multiple Cleanrooms** across **different Azure regions**—each with its own virtual network—to further **enhance resilience** and **reduce regional dependency**. The diagram shows how multiple Air Gap Protect (AGP) endpoints, each located in distinct Azure regions, feed backups into separate Cleanrooms.

This requires:

One Virtual Network (VNET) per Region

- For **each region**, you see a dedicated VNET that encapsulates the Cleanroom resources.
- This per-region VNET model allows for **clear segmentation** of traffic and isolated infrastructure in each region.

Minimum Two Subnets per VNET

- **Infrastructure Subnet**:
  - Hosts shared components such as **Access Nodes** (AN), a **storage account** for staging areas, and other core services.
  - Outbound connectivity is **enabled** here—often via public IP addresses on the Access Nodes or security rules in the Network Security Group (NSG)—so that it can communicate with Commvault Cloud and fetch data from AGP.
- **Cleanroom Subnet**:
  - Each VNET includes **at least one** Cleanroom Subnet, where restored workloads live in a **fully isolated** environment.

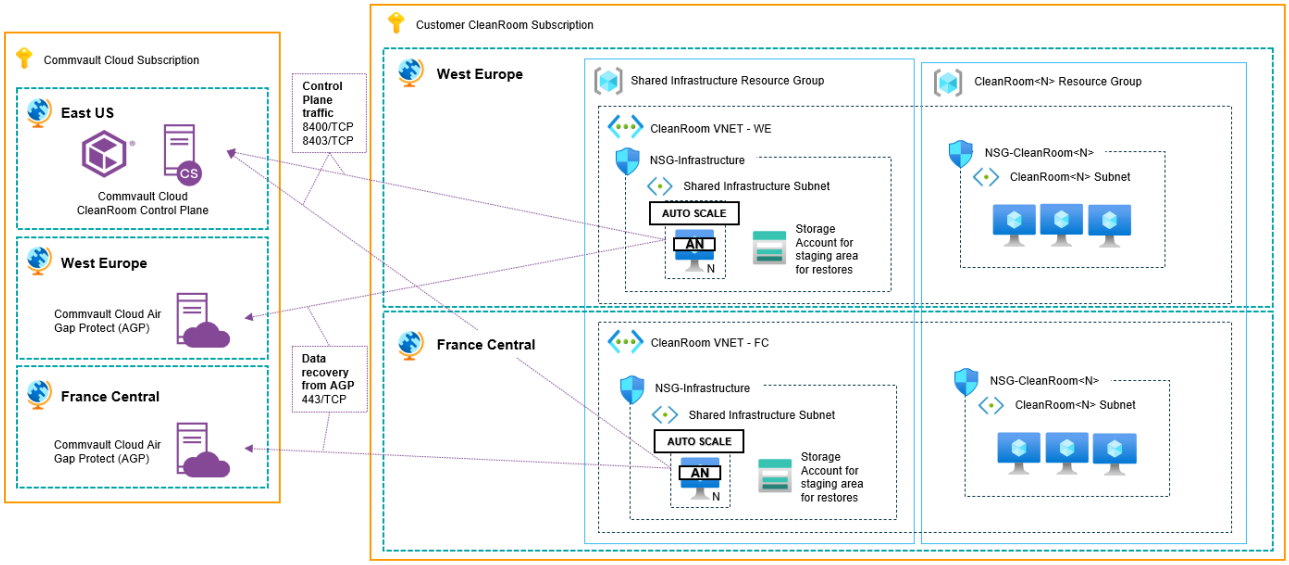
- This subnet typically has **no outbound internet access** to prevent unauthorized egress traffic, keeping the Cleanroom isolated and secure.
- Each subnet has its **own NSG** to fine-tune traffic policies. In the example, the **Infrastructure Subnet** uses an NSG that **permits outbound** traffic for Access Nodes to contact the Commvault Cloud or external endpoints, while the **Cleanroom Subnet** NSG is locked down to **no outbound** paths. This dual-NSG design enforces strict boundary control between the Infrastructure and the Cleanroom workloads.

Auto-Scale Access Nodes

- As shown in the diagram, Access Nodes (AN) within each Infrastructure Subnet can **auto-scale** based on demand. This ensures that we can **spin up** additional Access Nodes quickly to handle **large volumes** of data transfers or complex recovery tasks.

Multiple AGP (Air Gap Protect) Copies

- Each region should have its **own AGP** copy, creating **redundant** backup repositories.
- In the diagram, you can see two (or more) distinct AGP copies, each sending recovery data to its respective Cleanrooms.



Advanced Cleanroom – Single Region, with Agent-Based restores of DBs and other application running inside the VMs

In this setup, you have a **single Azure region** (e.g., West Europe) for your Cleanroom environment but require a **dedicated VM** to handle agent-based restore operations. This VM combines the **MediaAgent** and **Network Gateway** roles. This is required since some workloads (e.g., specific databases) require an **agent** installed inside the target VM for granular restores.

This requires:

One Virtual Network (VNET)

- As shown in the diagram's right-hand (blue) box for the "Customer CleanRoom Subscription," there is a **single Azure VNET** dedicated to the Cleanroom.
- This VNET provides a **logical boundary** that segments your recovery environment from your production workloads.

Minimum Two Subnets

- Inside this single VNET, you typically define **two subnets**:
- **Infrastructure Subnet** – Hosts shared infrastructure components, such as the **auto-scaling Access Nodes (AN)** and a **storage account** for staging area restores. It is visually represented in the "Shared Infrastructure Resource Group" portion of the diagram. Outbound connectivity is **enabled** here—often via public IP addresses on the Access Nodes or security rules in the Network Security Group (NSG)—so that it can communicate with Commvault Cloud and fetch data from AGP.
- **Cleanroom Subnet** – A dedicated isolated subnet (or potentially multiple subnets) where **actual Cleanroom workloads** are restored and validated. This is shown in the diagram under "Cleanroom- Resource Group."
- Each subnet has its own **Network Security Group** (NSG) to restrict and control inbound/outbound traffic. In the figure, you see NSG-Infrastructure for the Infrastructure Subnet and NSG-CleanRoom- for each Cleanroom Subnet. These NSGs ensure **isolation** and security of restored data, helping prevent any unwanted traffic between the infrastructure components and the Cleanroom environment.

Auto-Scaled Access Nodes

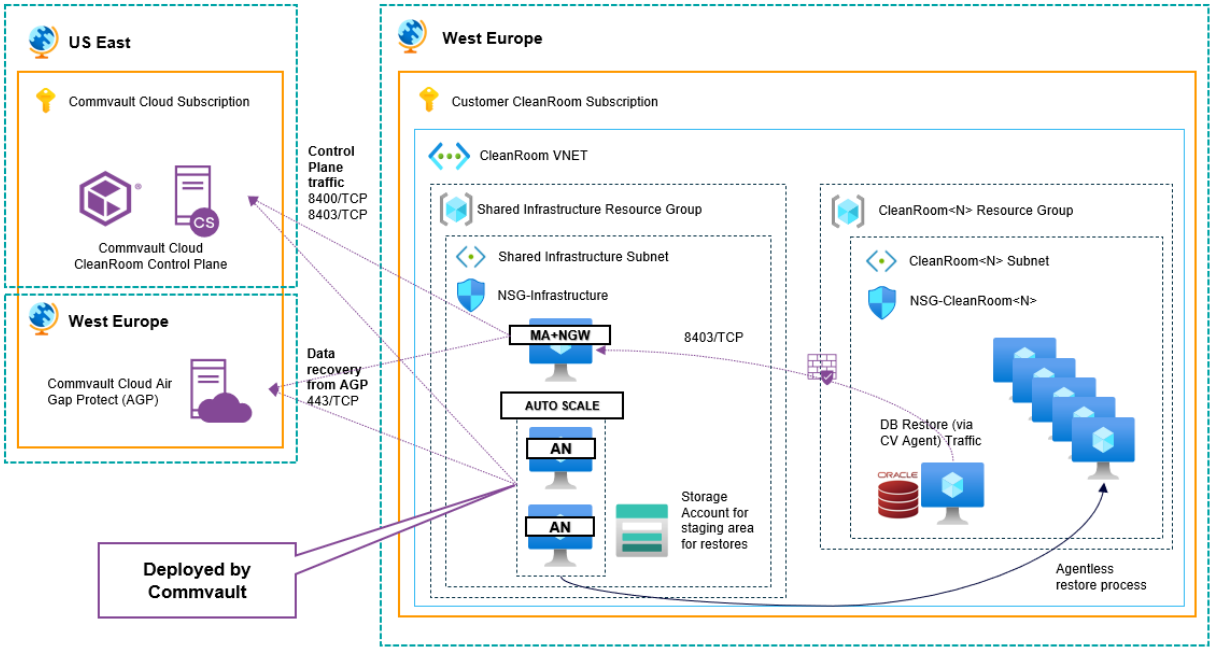
- In the Shared Infrastructure Subnet, you can see multiple Access Nodes (AN), this **auto-scaling** feature dynamically adjusts the number of Access Nodes available based on workload demand, ensuring **optimal performance** during large or parallel restore operations.
- **Control-plane traffic** (ports 8400/TCP and 443/TCP) flows between Commvault Cloud and the Cleanroom, while **data recovery traffic** (443/TCP) comes from the Commvault Cloud Air Gap Protect (AGP) service.
- This design allows Commvault to **securely provision** and manage Cleanroom resources within the customer's Azure subscription, while maintaining a strong **air-gapped** posture.

Dedicated VM: MediaAgent + Network Gateway

- A **specialized VM** (often shown as "MA + NGW") is deployed inside the Infrastructure Subnet:
    - **MediaAgent Role**: Allows local staging and processing of backup data.
    - **Network Gateway Role**: Manages secure connections between the **Cleanroom** and external resources (AGP, recovered CS).

- **Deployment & Teardown**:
    - This VM must be **manually deployed** (or automated via Terraform) each time you stand up the Cleanroom.
    - You then **register** the VM to the external CommServe so it knows how to route restore jobs.
    - Finally, once the Cleanroom operation is complete, this VM is **manually deleted** to maintain the air-gapped nature of the Cleanroom and avoid leaving any persistent, potentially exploitable gateway.

Control-plane traffic (ports 8400/TCP and 443/TCP) flows between Commvault Cloud and the Cleanroom, while **data recovery traffic** (443/TCP) comes from the Commvault Cloud Air Gap Protect (AGP) service. This design allows Commvault to **securely provision** and manage Cleanroom resources within the Azure subscription, while maintaining a strong **air-gapped** posture.



REQUIREMENTS

The below lists must be shared with customers at the kickoff of Cleanroom activities. You can use this table as a checklist if you please.

General Requirements

Use case	Item	Areas	Guideline
All	Commvault version	Commvault Requirements	Commvault version needs to be at least 11.34.13.
All	Commvault storage	Commvault Requirements	VMs which will require to be tested in Cleanroom require a copy of the backups in Air-Gap-Protect (AGP) storage.
All	Commvault CS Backup	Commvault Requirements	CommServe DR Backup needs to be configured to Commvault Cloud.
All	Licensing	Commvault Requirements	Commvault Air Gap Protect license: CV-MCS-EC-TB | CV-MCS-EH-TB Commvault Cleanroom license: CV-CLNRM-10TB
All	Commvault Cleanroom Hypervisor Pseudo Client	Configuration of Service Principal	During configuration, you need to create an Azure App as Managed Identities are not supported with Auto-Scale yet.
All	Commvault Cleanroom Hypervisor Pseudo Client	FinOps, Performance	Enable Auto-Scaling for Azure Access Nodes.
All	Commvault Cleanroom Hypervisor Pseudo Client	Principle of Least Privilege	You need Contributor permissions for the machine / app you have configured, or you can use this restricted custom role (for encrypted VMs, use this role). Consider that Cleanroom environment is an empty environment so Contributor should not be a big deal, but this depends on customer security team.
All	Commvault Cleanroom Hypervisor Pseudo Client, Customer Cleanroom Subscription	Restore Requirements	During full VM restores, a Storage Account must exist in the subscription **and** in the region of the restored VM (an Azure Standard or Premium general-purpose storage account), LRS resiliency. This account acts as a staging area when VM is restored as managed VM. Restoring Azure VMs and Files (commvault.com).
All	Customer Cleanroom Subscription	Principle of Least Privilege	You need the Storage Account Contributor & Storage Blob Data roles towards the Storage Account used as a Staging location for restore to work correctly.

All	Customer Cleanroom Subscription	Performance	It is recommended to enable Azure Service Endpoints for Microsoft.Storage in order to ensure that all network traffic from the proxy machine to the Azure storage account is securely flowing through the Microsoft Azure backbone network.
All	Customer Cleanroom Subscription	Resource Providers	Ensure all of these providers are enable on Cleanroom Subscription • microsoft.support • microsoft.Storage • microsoft.SerialConsole • microsoft.Resourcesmicrosoft.ResourceNotifications • microsoft.ResourceGraph • microsoft.Portal • microsoft.OperationalInsights • microsoft.Network • microsoft.MarketplaceOrdering • microsoft.MarketplaceNotfications • microsoft.MachineLearning • microsoft.GuestConfiguration • microsoft.Features • microsoft.CostManagement • microsoft.Consumption • microsoft.Compute • microsoft.Commerce • microsoft.CloudShell • microsoft.ClassicSubscription • microsoft.ChangeAnalysis • microsoft.Billing • microsoft.Authorization • microsoft.ADHybridHealthService
Advanced Cleanroom – Single Region, Agent-Based restore required	Customer Cleanroom Subscription	Networking and air-gap	To guarantee that Cleanroom remains a safe area, air-gapped from any other network, but still guarantee agent-based recoveries, the only solution is to spin-up a network gateway able to be reached from machines with agent-in-guest (i.e., pave and repave, existing ones, or new ones) during registration towards Cleanroom CS. This machine(s) should have both Network Gateway and MediaAgent roles. A Network Topology should be built in the source environment for this purpose.

Firewall Requirements

Use case	Source	Destination	Port Range	Notes
All	Cleanroom Shared Infrastructure Subnet	IP of Cleanroom CommServe	8400, 8403/TCP	In case customer does not allow Public IPs being set on Auto-Scaled Access Nodes.
All	Cleanroom Shared Infrastructure Subnet	*.blob.core.windows.net (see https://www.microsoft.com/en-us/download/details.aspx?id=56519 for IP ranges) https://login.microsoftonline.com (see https://learn.microsoft.com/it-it/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide for IP ranges) api.mcss.metallic.io / 40.75.17.108	443/TCP	Air-Gap Protect; customer can decide to open just the range of IPs associated with the right region and not the entire Azure ranges for Microsoft.Storage.
Advanced Cleanroom – Single Region, Agent-Based restore required	Cleanroom Subnet	Cleanroom Shared Infrastructure Subnet Network Gateway	8403/TCP	For client registration

PREPARATION

This is the checklist of the activities that need to be performed when involved in Cleanroom engagements. Even if shared with customer, always make a quick session with them looping all of these points together to ensure everything has been set.

Area	Check	Task Description	Instructions
Cleanroom Subscription Setup	Subscription Check	Check if subscription has been created.	Follow this Azure guide.
Cleanroom Subscription Setup	Resource Providers Check	Double check if resource providers are enabled on the new subscription. Usually, this is not done even if asked.	Follow this Azure guide.
Cleanroom Subscription Setup	App Registration for Commvault	Ensure that App Registration has been created with right permissions towards the entire Cleanroom subscription.	Follow this Commvault guide and this guide or this to follow the Principle of Least Privilege.
Cleanroom Subscription Setup	Staging Storage Account Check	Check that the Storage Account created is with the right configuration (only locally-redundant storage (LRS) and StorageV2 - general purpose v2 - accounts that are associated with the selected region for the restored VM are supported).	Follow this Azure guide. Ensure that each Storage Account is created with LRS redundancy. Then ensure to have at least 1 Storage Account in the same region of the VMs being recovered.
Cleanroom Subscription Setup	Staging Storage Account Check	Ensure that App Registration has been created with right permissions towards the Storage Account (Storage Account Contributor, Storage Blob Data Contributor).	Follow this Azure guide.
Cleanroom Subscription Setup	Access to CleanRoom VMs	Ensure a bastion host or an alternative way to access the recovered machines is setup.	As an example, follow this Azure guide for bastion host setup. But discuss with customer their preference.
Commvault Source environment	Version Check	Check that Commvault environment is at least in version 11.34.13.	N/A
Commvault Source environment	CommServeDR Backup on Commvault Cloud Check	Ensure that Commvault CommServeDR Backup is uploaded in Commvault Cloud.	Follow this Commvault guide.
Commvault Source environment	Customer Access to Cloud Command Check	Have customer login to Commvault Cloud (cloud.commvault.com) with recovery manager rights.	Login to https://cloud.commvault.com/ with customer credentials.
Commvault Source environment	Auxiliary Copies to AGP Check	Ensure that auxiliary copy jobs on AGP are not fallen behind and that the day of the Cleanroom Recovery activity there will be some backups hosted in Cleanroom to perform the tests.	CommCell Console: follow this Commvault Guide. Command Center: follow this Commvault Guide. Then check for Available Jobs inside the AGP copy. There should be at least 1 Full Backup per VM.

Commvault Source environment	Create the Cleanroom Hypervisor	While this task can be done in Cleanroom, every time Cleanroom spins up it should be repeated. To improve customer's User Experience, prepare in advance the Cleanroom Hypervisor(s).	Follow this Commvault Guide.
Commvault Source environment	Create the Cleanroom Target	While this task can be done in Cleanroom, every time the Cleanroom spins up it should be repeated. To improve customer's User Experience, prepare in advance the Cleanroom Target(s).	Follow this Commvault Guide.
Commvault Source environment	Create the Cleanroom Recovery Groups	While this task can be done in Cleanroom, every time the Cleanroom spins up it should be repeated. To improve customer's User Experience, prepare in advance the Cleanroom Recovery Groups(s).	Follow this Commvault Guide.
Commvault Source environment	Backups	In case of VM with databases, ensure to apply whatever option to guarantee consistency (pre-scripts, application-aware backups, application-consistent). This to avoid going into an agent-based Cleanroom design.	Pre / Post scripts: follow this Commvault Guide (VMware). For other Hypervisors, look at the documentation. Bear in mind that in other hypervisors scripts are usually run by the Access Node. Application Aware: follow this Commvault Guide.
Commvault Cloud	Cleanroom feature Check	Login into https://cloud.commvault.com with an account that has recovery manager permissions and check that CSDR Backups are correctly uploaded.	N/A

VMS PREPARATION

OS	Prerequisite
Windows	Enable SAN Policy on the Source VM. See this Commvault Guide. No reboot is required but is still recommended.
Linux	**Note: always make a snapshot / backup of the source VM before modifying it.** Install Hyper-V drivers on the Source VM. See this Commvault Guide. In case the steps are not enough, these steps, **community driven**, have been tested and worked as well. Edit **/etc/dracut.conf**, add content: **add_drivers+="hv_vmbus hv_netvsc hv_storvsc"** Verify that no dracut conf files (for example, **/usr/lib/dracut/dracut.conf.d/01-dist.conf**) contains the following line. In that case, comment the line. **hostonly="yes"** Rebuild the initramfs: **sudo dracut -f -v** Reboot the VM and check that it still boots fine.
Linux	Install Azure Linux Agent on Source VMs. Follow this Microsoft Guide. No reboot is required but is still recommended.

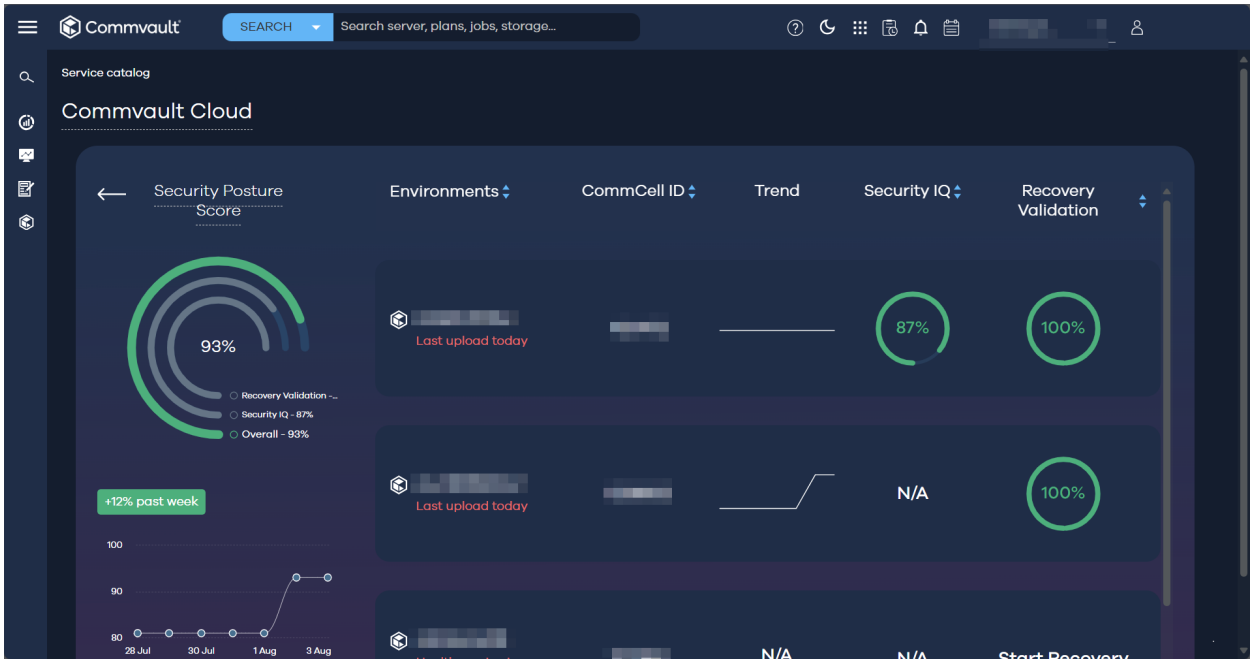
CLEANROOM SPIN UP

The following walkthrough will cover how to set up and use Cleanroom Recovery if nothing has been pre-defined. In this walkthrough, the assumptions are:

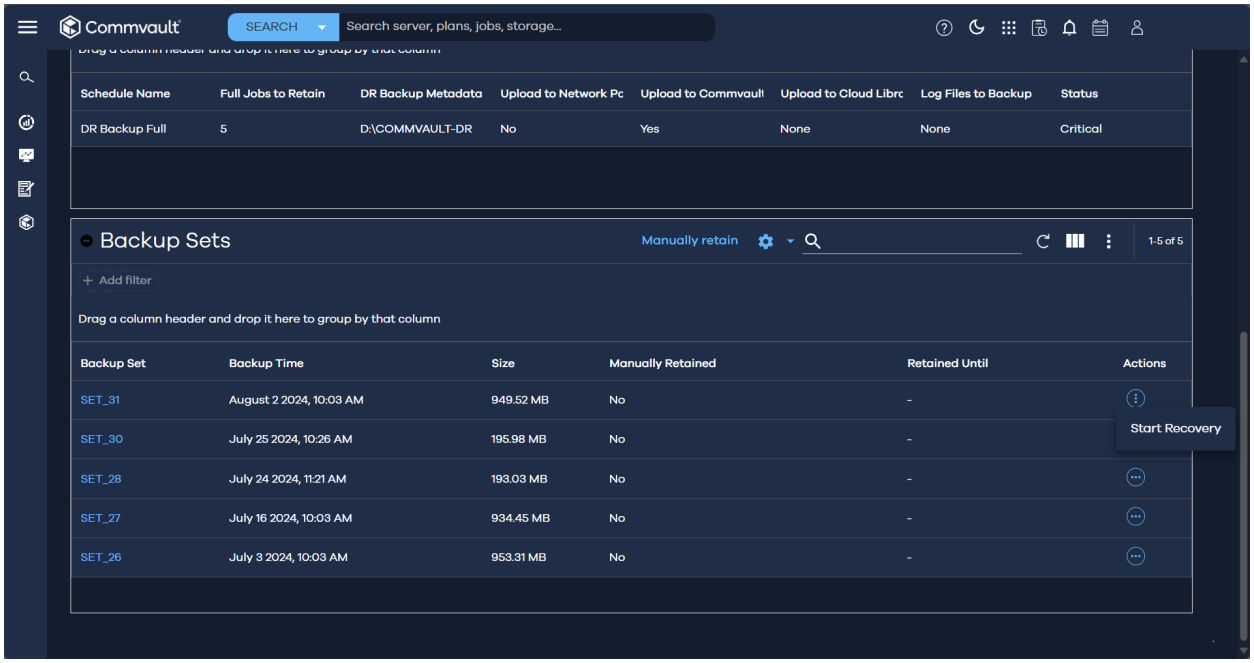
- Commvault Software has been licensed and actively backing up an environment
- Control Plane database backups are going to cloud.commvault.com
- Air Gap Protect has been licensed with backups going to Air Gap Protect
- Cleanroom Recovery Licensing has been applied
- An Azure subscription is available, and it is at least minimally configured as above

Login into Commvault Cloud.

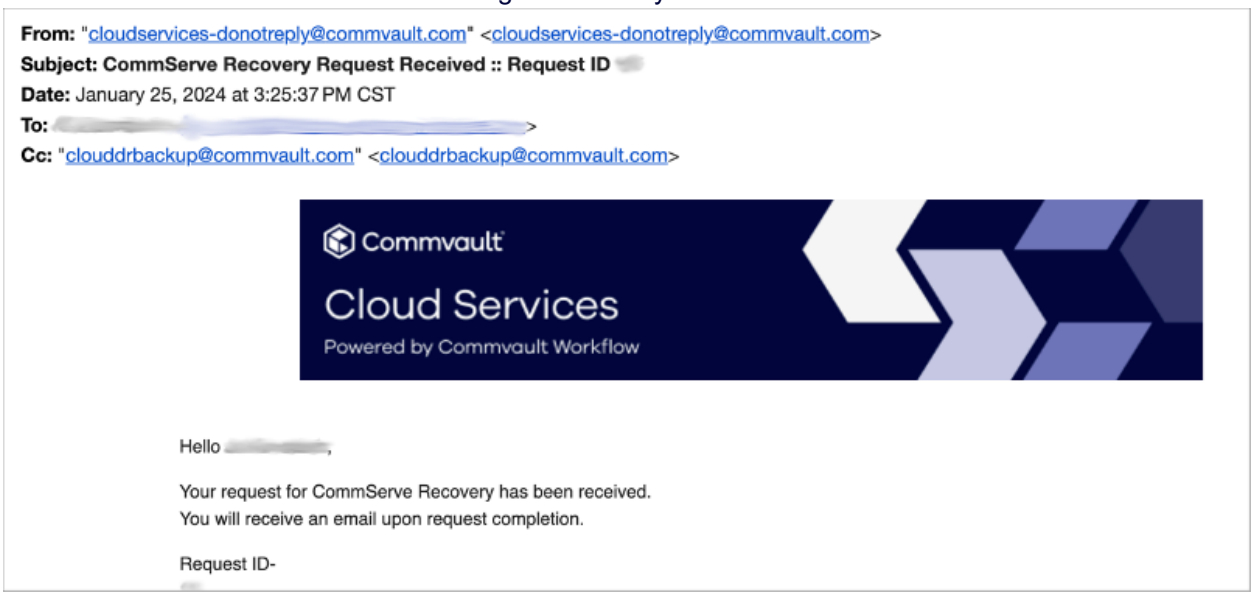
Click on “Security Posture Score” on the right.



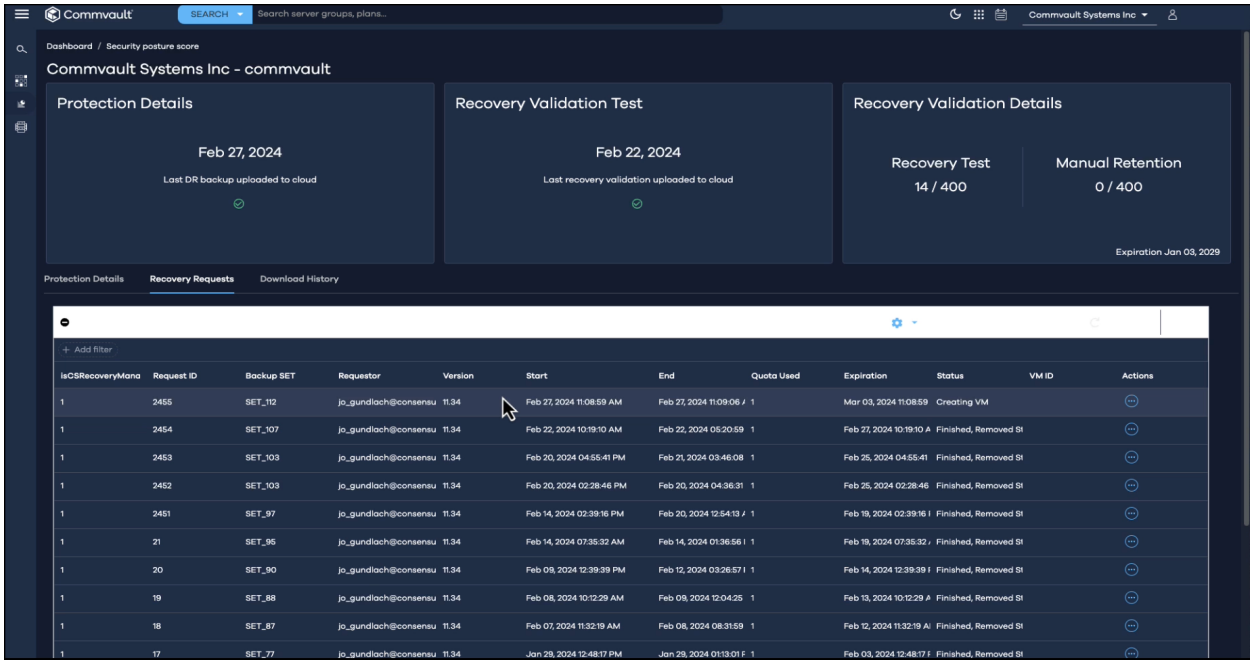
Choose the environment. Then click on “Recovery Validation”. You will see the current status and DR configuration. Scroll to the bottom, choose the last DR backup and click into Actions. Then, click on “Start Recovery”.



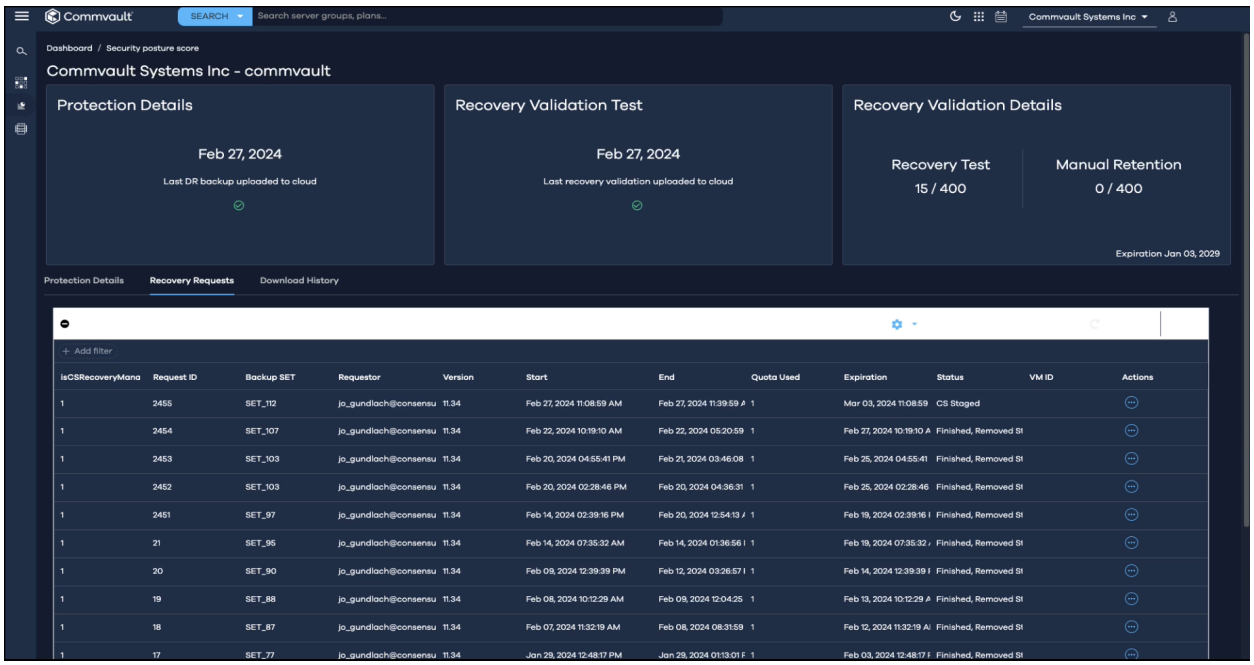
The account initiating the recovery will **also receive an email**.



The process should take from 30 minutes to 2 hours, depending on the Control Plane DB size. To monitor the progress, click on “Recovery Requests” and then monitor the “Recovery History” table every 5 to 10 minutes. Initially, it should be in status “Staging CS”.



Once the Recovery Status says CS Staged, and/or the Recovery Successfully Completed **email is received the recovery is finished**.



From: "cloudservices-donotreply@commvault.com" <cloudservices-donotreply@commvault.com>
Subject: CommServe Recovery Successfully Completed :: Request ID
Date: January 25, 2024 at 3:54:18 PM CST
To: Jo Gundlach <[redacted]>
Cc: "clouddrbackup@commvault.com" <clouddrbackup@commvault.com>

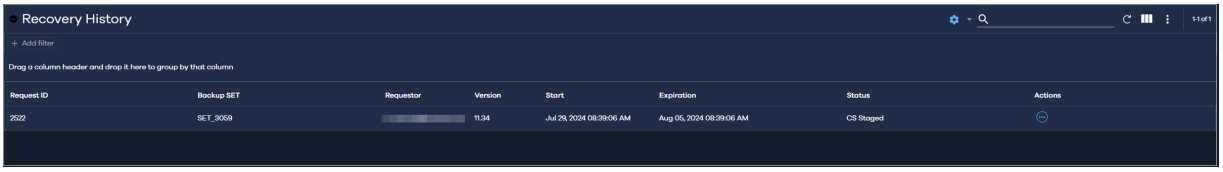
Commvault
Cloud Services
Powered by Commvault Workflow

Hello Jo Gundlach,

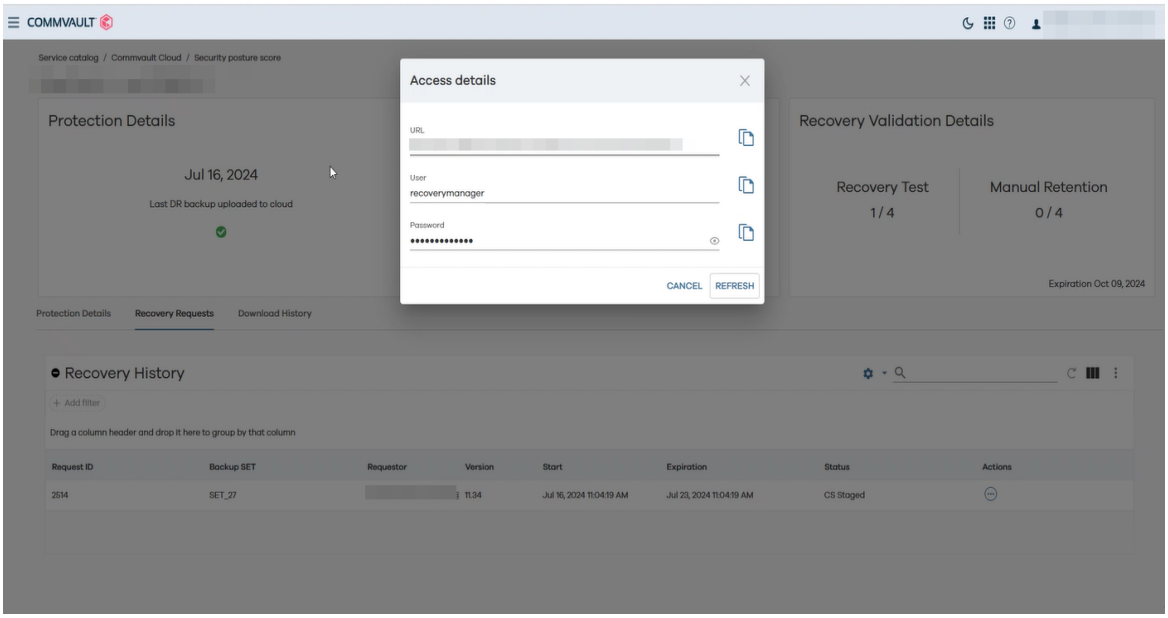
Your request for CommServe Recovery is complete.
You can find the request details from the page where the request was launched.

Thank you,
Commvault Cloud Services

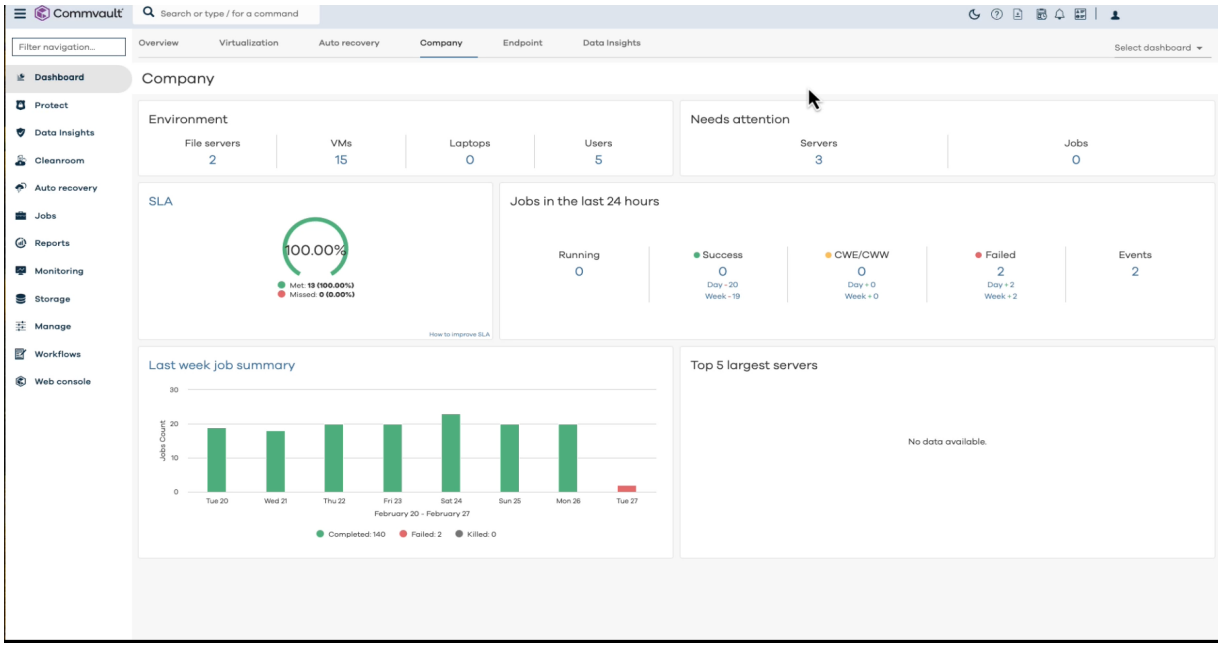
If after the 2 hours you don't receive an e-mail saying the recovery has completed and you do not see "CS Staged" as Status (see next screenshot), **open a support case**.



When recovery is successfully completed, you will be able to see into the "Actions" button inside the recovery history the access details. Click on it and then login to the Cleanroom Command Center.



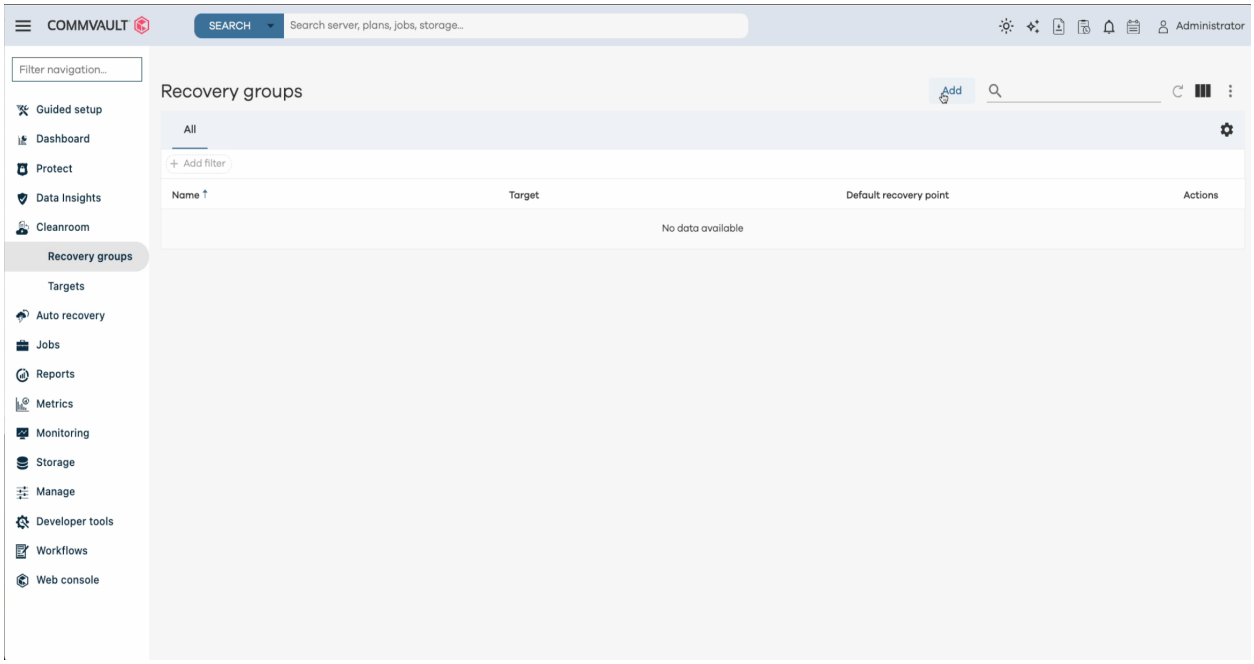
Use the information provided and log into **the new Command Center**.



Add cleanroom recovery configuration to the newly recovered control plane.

In the left-hand navigation, click Cleanroom -> **Recovery groups.**

Once the Recovery groups screen appears on the right, click **Add** on the top right.

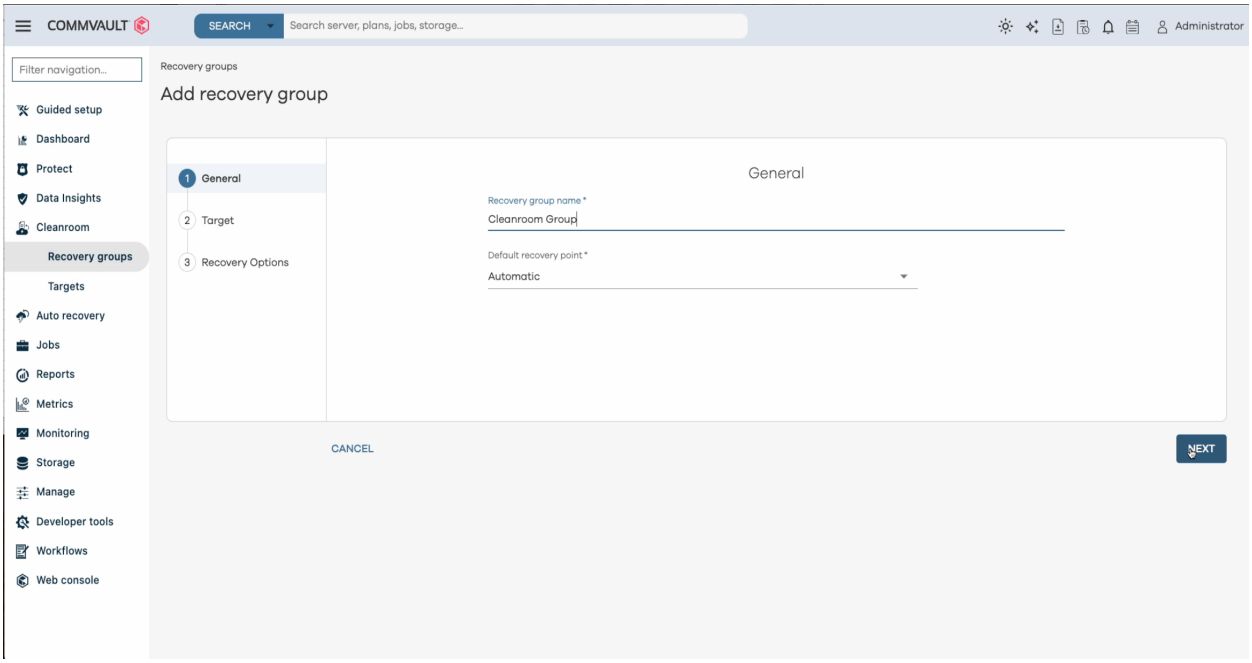


Once the Add Recovery Group screen loads, define the group. The settings we set here will default for all entities added later.

- Enter a **logical name** for the recovery group.
- Select the **automatic** for the point in time to recover to.

Automatic recovery points streamline the cyber recovery process by integrating with external security tools like SIEM/SOARs. These tools pinpoint compromised servers and their exact time of infection, allowing Commvault to automatically rewind to the last known good state. In lieu of external tools, blast radius reports or delimited files can be utilized to determine last known good state, instead of manually picking the point in time for every server. Finally, Commvault's anomaly detection excludes infected backups, further safeguarding recovered data. If no such exclusions exist, the latest recovery point is chosen.

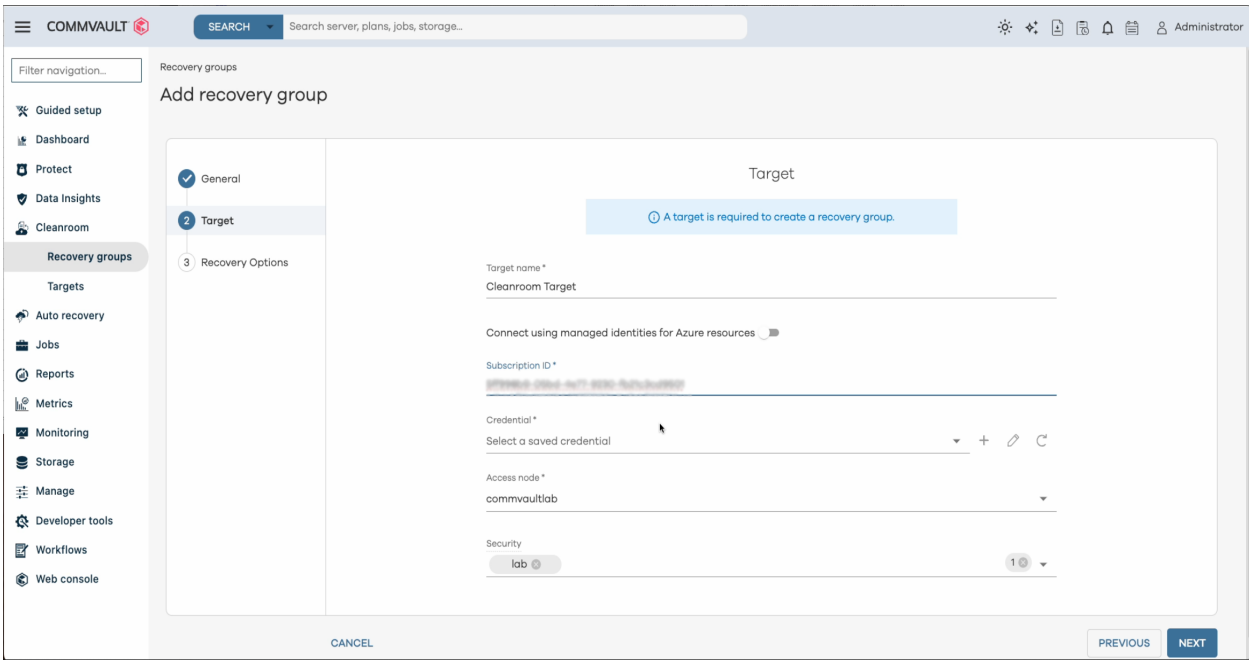
Click **Next**.



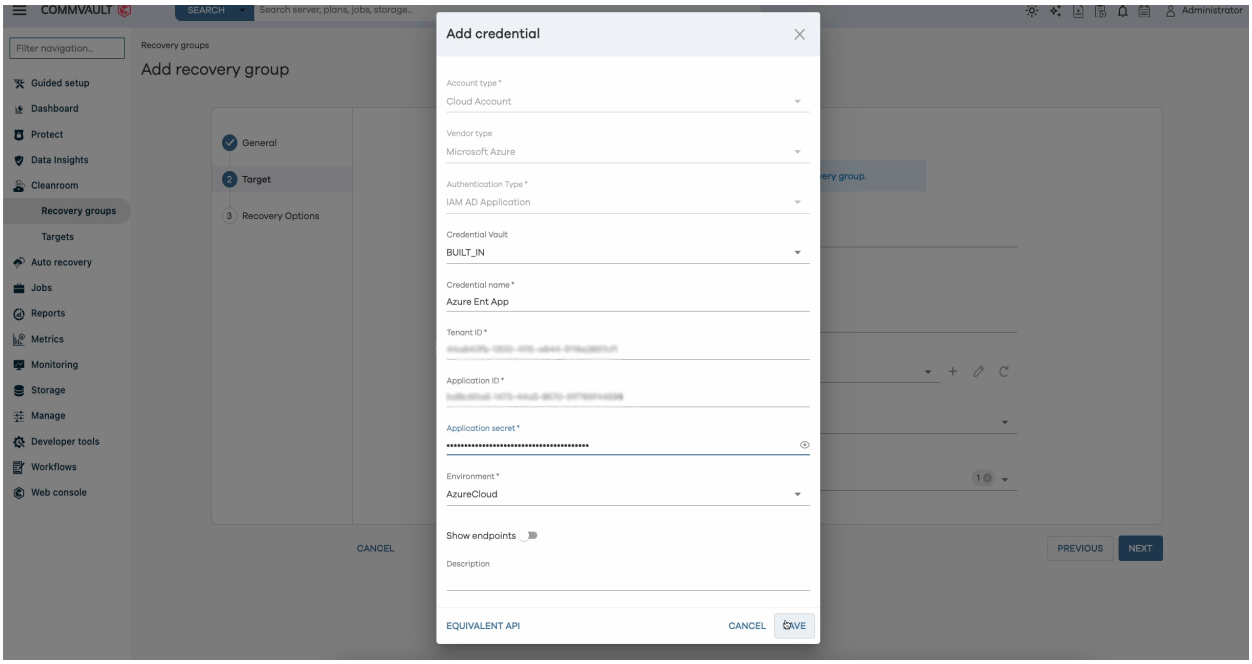
Once the Target screen appears fill in a logical name for the target and the subscription ID (This assumes that no recovery target has been created previously).

For this step, you will need:

- Your Azure Subscription ID
- Entra ID Tenant ID
- Application ID
- Application Secret



If you have not already stored the credentials to access your Azure Target, we can create them now by clicking the **plus sign + on the Credential line**. This will open the Add Credential Wizard.



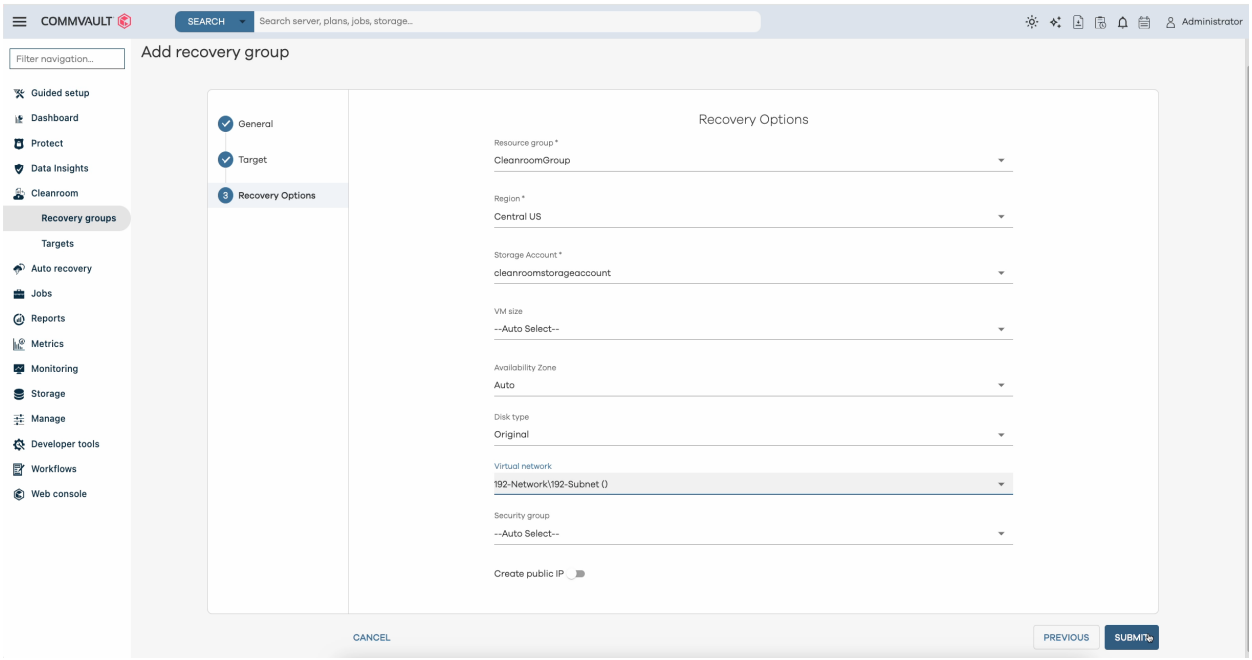
Select the **Access Node** as **Automatic**.

Click **Next**.

Now the **Recovery Options** screen appears.

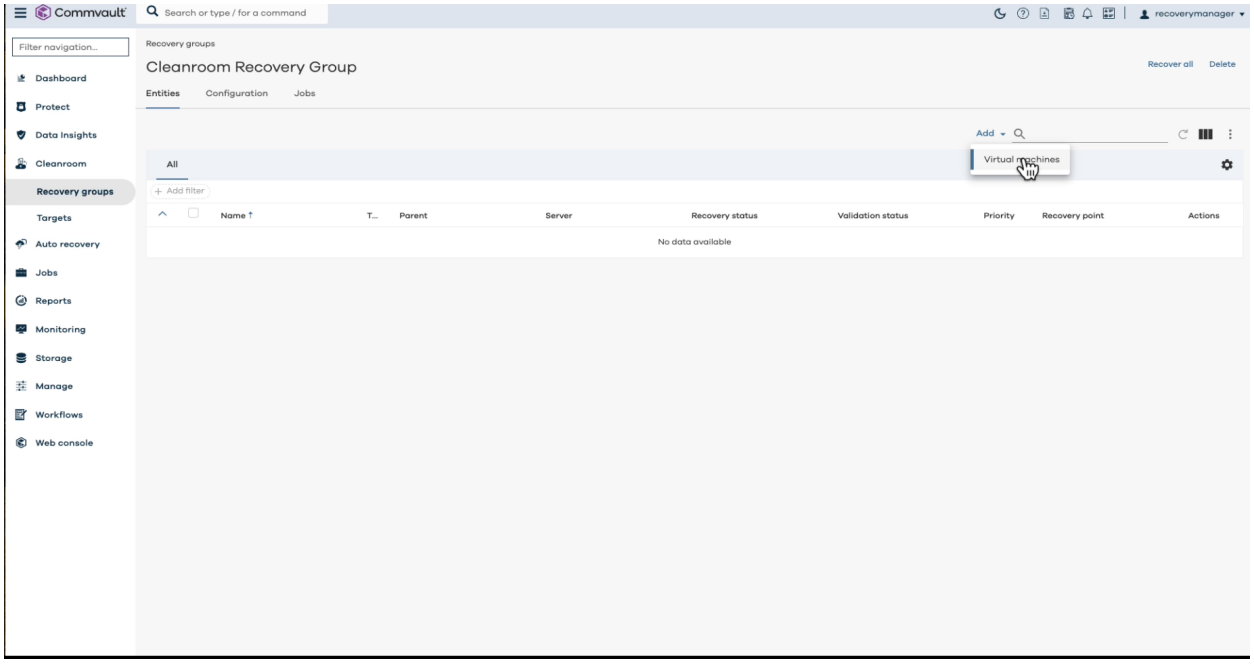
On the **Recovery Options screen**, we will configure where in Azure Hypervisor we will restore into.

- The resource group will auto-populate from the available resource groups in the Azure subscription.
- On the region line, select the region that is the same as the region housing the Air Gap Protect copies.
- Leave VM size auto. Commvault will look at the configuration of the original VM and select the most appropriate Azure VM size.
- Availability Zone can be left auto.
- Leave the Disk type as original.
- Select **virtual network** if there are multiple.
- Select **Azure Network Security Group** if you have multiple.
- If you want a public IP, this is only recommended for specific VM, select **Create public IP** to let Commvault auto-assign a public IP from your Azure subscription.
- Click **Submit**.

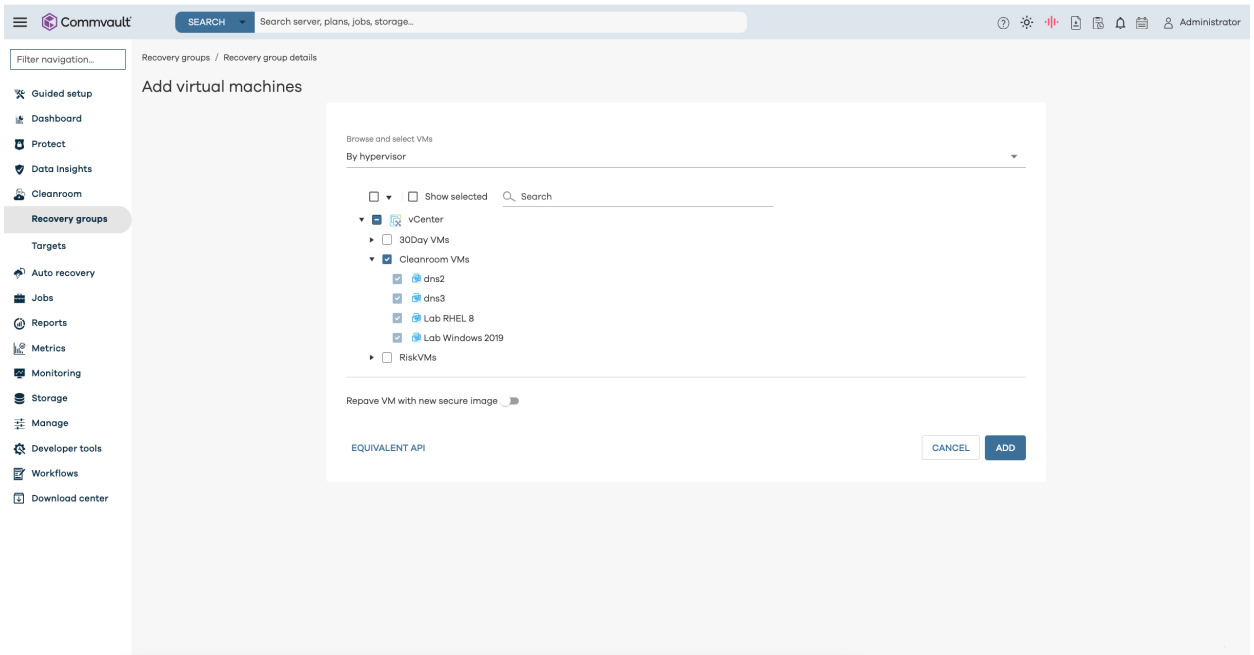


The **Recovery group and target** have been created.

Entities now need to be added to the recovery group. In the upper right, click **Add → Virtual machines**.

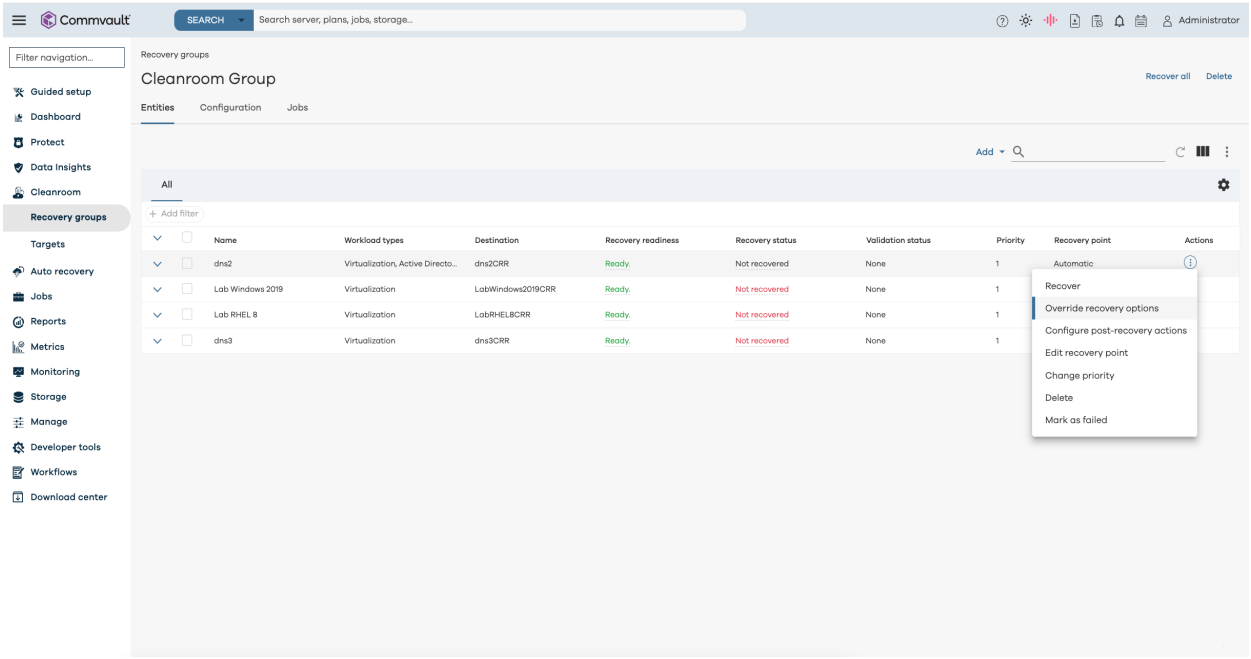


Once the Add entity screen loads, expand the list of hypervisors and select the virtual machines to add to the group. If you want to Repave your VMs you can select Repave VM with new Secure image, we did not since we have mixed machines in this group. Instead, you can select repave in the individual VM options later. Click **Add**.

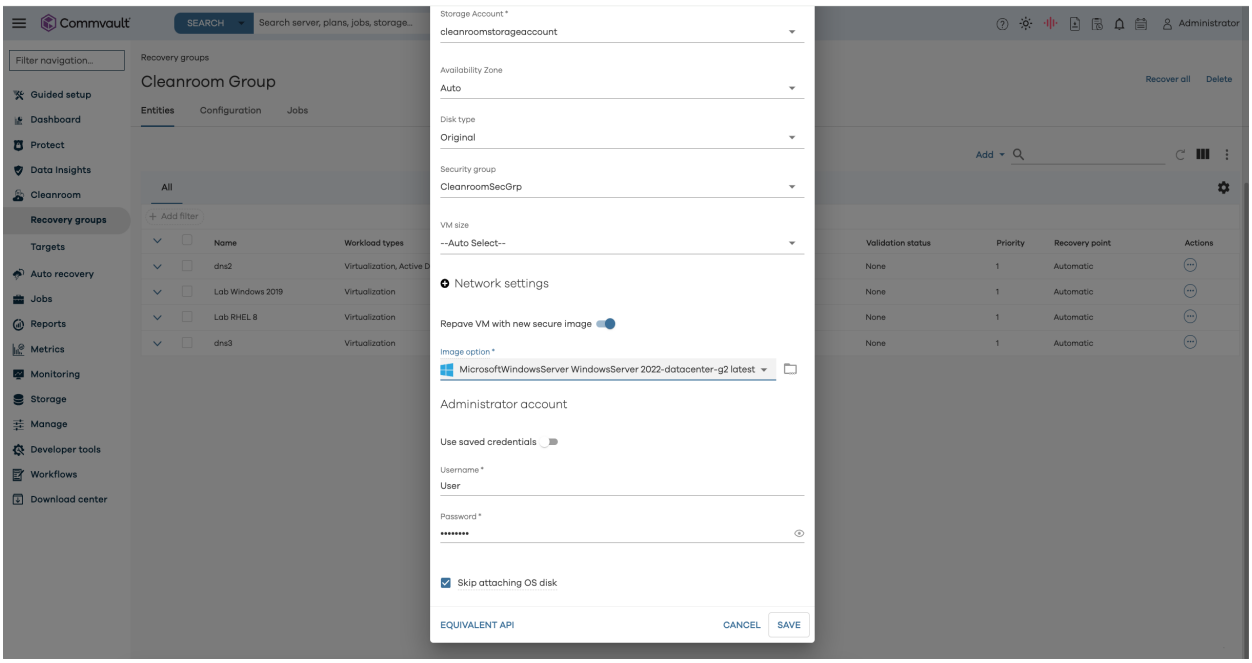


The recovery group has now been populated.

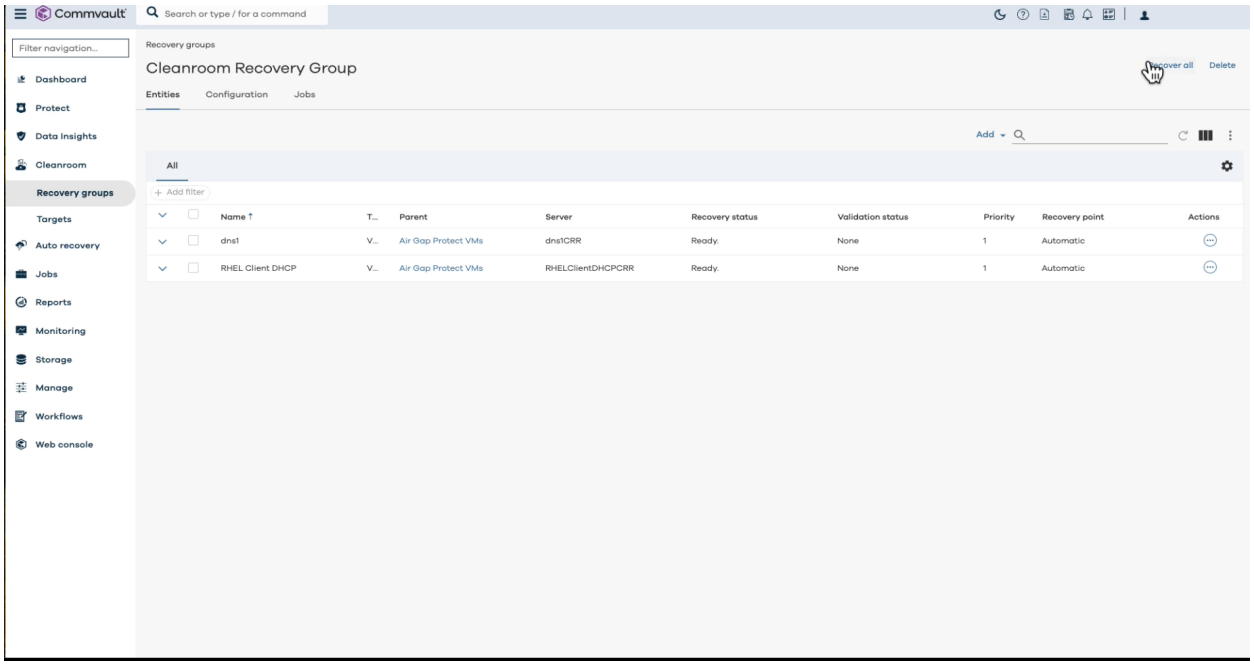
(Optional) To select Repave options for a single VM click the Actions ellipsis ➔ Override recovery options.



The **Override recovery options** window appears. At the bottom select **Repave VM with new Secure image.** You can now select what image and user credentials to use to create the new OS for the recovered VM. This has now set the options for this specific server and can be repeated for any other server. Click **Save**.

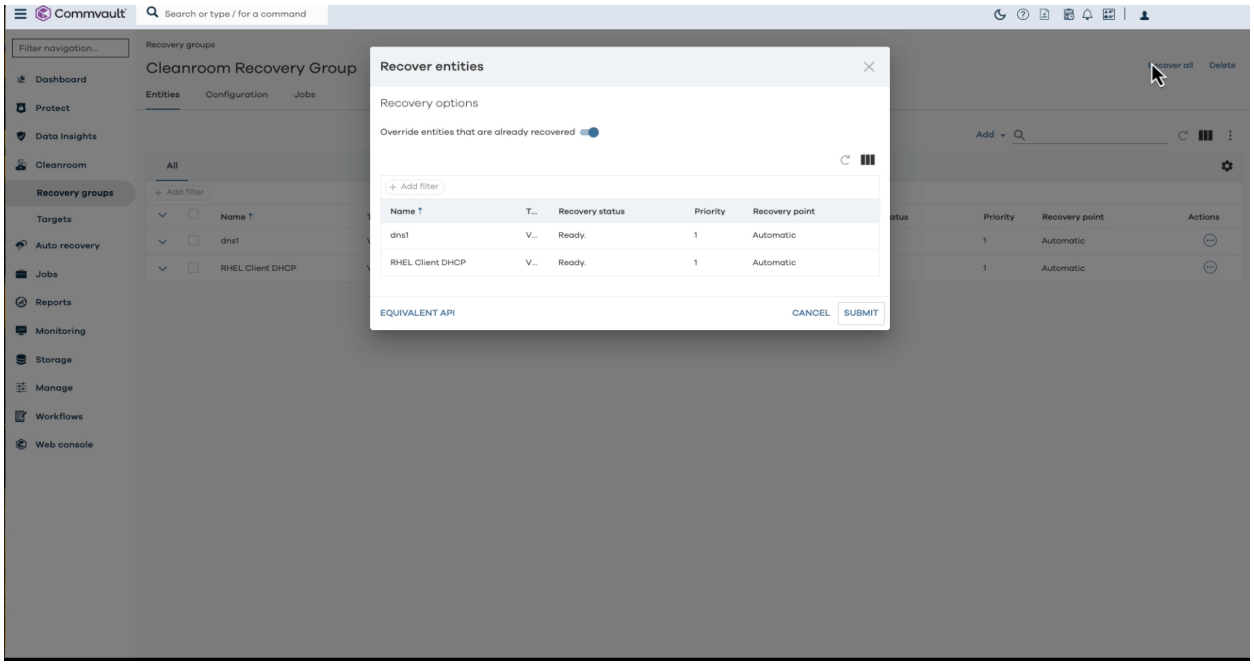


To initiate a recovery of all entities, click **Recover all** in the upper right of the Recovery group screen.



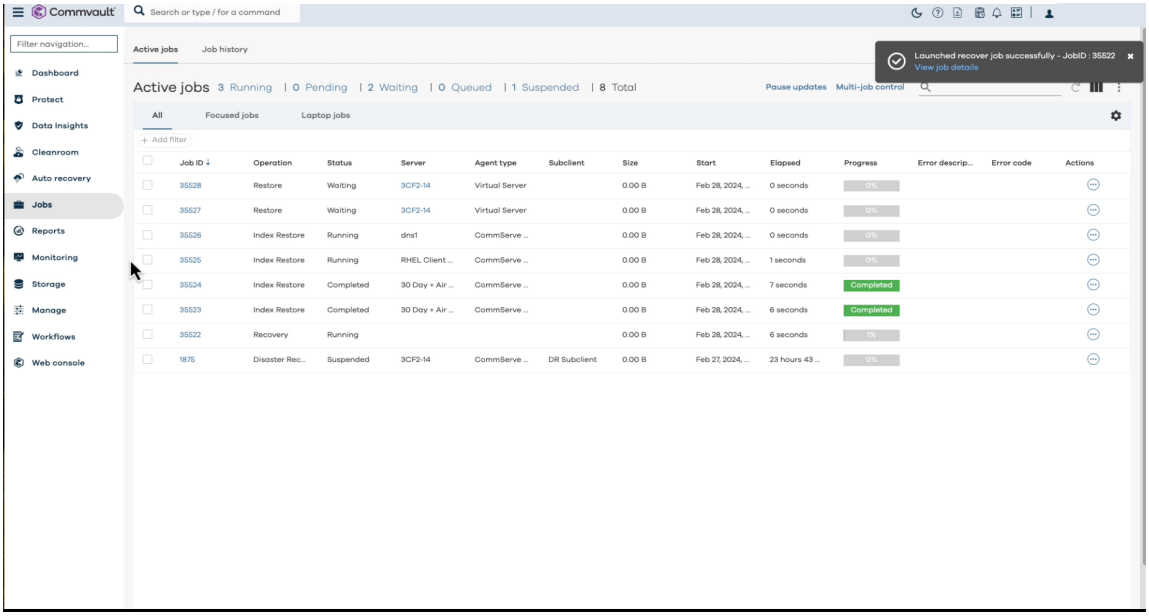
Alternatively, if you click the checkbox next to a specific machine(s) **Recover** appears next to Add. Clicking **Recover** will initiate a recovery of only the selected machine(s).

Once the Recover entities screen loads, click on **Submit**.



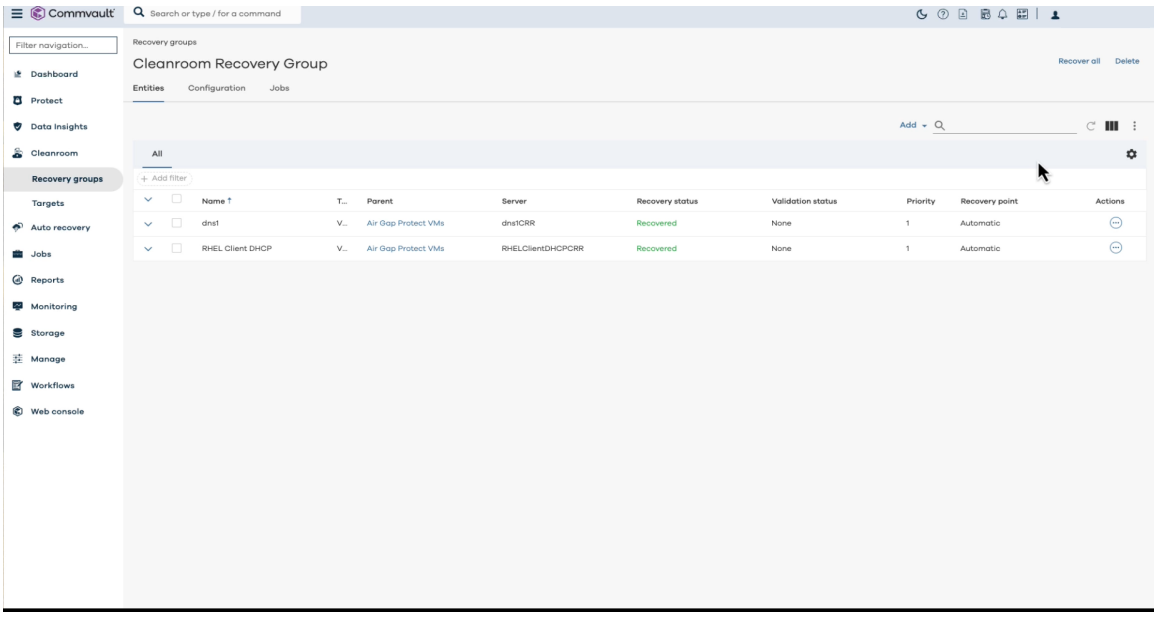
After clicking **Submit**, a job is created to orchestrate and initiate the recovery.

To monitor the jobs, click on **Jobs** in the left-hand navigation. This brings up the Active jobs screen, where we see a job for each VM being recovered and the Recovery Job.

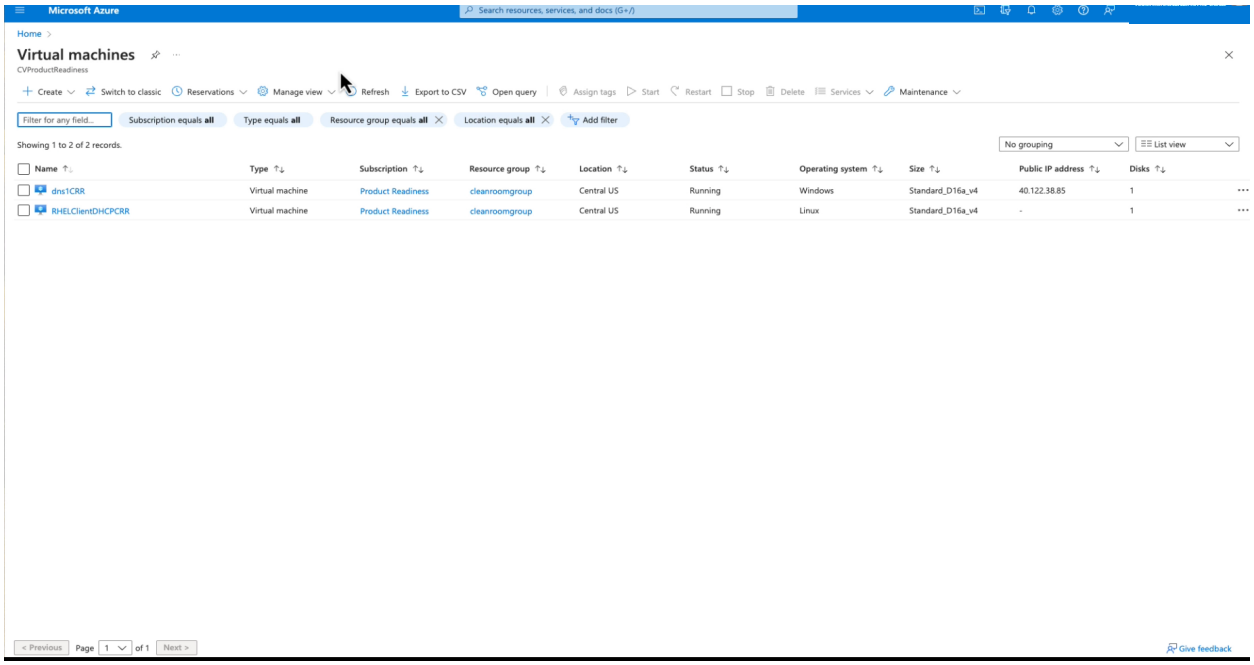


To monitor the state of each VM **click Cleanroom → Recovery group → recovery group** name and the list of entities are listed with their Recovery status.

Monitor the Cleanroom Recovery Jobs from the Jobs panel or from the Cleanroom Recovery Groups page (https://documentation.commvault.com/2024/essential/monitoring_Cleanroom_recovery.html).



Looking in **Azure virtual machines** will show the restored VMs in Azure.



Recovered VMs will be automatically cleaned up (deleted from the cleanroom target) seven days after the Control Plane Recovery. If you would like the recovered VMs to be held longer than default seven days remember to set cleanup options of the recovery group. If you want to transition the recovered VMs into production, please work with Commvault professional services and your local service providers.

Accessing and testing

There are multiple ways to access recovered VMs, but general recommendations are:

- Public IP, this is not a recommended practice, unless no other option is available.
- Bastion host: deploy a bastion host (can still be the MediaAgent / NGW in “Advanced Cleanroom – Single Region, Agent-Based restore required” described in Use Cases section.
- Adding network inbound rules from external existing networks into the Cleanroom VNETs. This should be used cautiously because it now opens the cleanroom up to possible contamination.

Whitepapers

TECHNICAL WHITEPAPERS

The Critical Role of Cleanroom Recovery and Cyber Testing in Today's Threat Landscape

Executive Summary

Cyberattacks have evolved into a pervasive and sophisticated threat, posing a significant danger to organizations of all sizes. The ever-changing nature of cyber threats necessitates a robust and adaptable approach to cyber recovery. Commvault Cloud's Cleanroom Recovery addresses this critical need by providing a comprehensive testing and failover solution that enables organizations to mitigate cyber risk effectively.

This white paper delves into the importance of cyber recovery testing and the role of cleanroom environments in ensuring a strong incident response capability. It explores the challenges of testing cyber recovery plans in hybrid environments and highlights how Commvault Cloud's Cleanroom Recovery simplifies and streamlines the process.

Introduction

The frequency and severity of cyberattacks have escalated dramatically in recent years, posing a substantial threat to organizations across all industries. These attacks can have devastating consequences, including data breaches, financial losses, and irreparable reputational damage.

Effective cyber recovery is crucial for organizations to minimize downtime, restore business operations, and safeguard their reputation after a cyberattack. However, many organizations struggle to adequately test their cyber recovery plans, leaving them vulnerable to real-world attacks.

The Limitations of Traditional Cyber Recovery Testing

Traditional cyber recovery testing methods, such as tabletop exercises, often fail to adequately prepare organizations for the complexities and chaos of real cyber recovery scenarios. These exercises typically involve discussions and simulations that lack the realism and urgency of an actual attack.

Moreover, testing cyber recovery plans in hybrid environments can be time-consuming, complex, and expensive. With workloads spread across multiple clouds, on-premises hypervisors, and physical servers, organizations must perform testing within each environment separately.

The Need for Cleanroom Recovery

Cleanroom recovery provides a safe and isolated environment where organizations can test their cyber recovery plans without disrupting production systems. This environment allows organizations to identify and address gaps in their plans before an actual attack occurs.

In addition to testing, cleanroom environments can be used for forensic analysis of known infected systems. This analysis can help organizations understand the root cause of an attack and take steps to prevent future incidents.

Commvault Cloud's Cleanroom Recovery: A Comprehensive Solution

Commvault Cloud's Cleanroom Recovery is a comprehensive testing and failover solution enabling organizations to mitigate cyber risk effectively. It provides a safe and isolated environment for testing cyber recovery plans, conducting forensic analysis, and ensuring business continuity in case of a breach.

Key Features of Commvault Cloud's Cleanroom Recovery

- **Comprehensive testing environment:** Cleanroom Recovery provides a safe and isolated environment where organizations can test their cyber recovery plans without the risk of disrupting production systems.
- **Secure forensic analysis:** Cleanroom Recovery can be used to conduct forensic analysis of known infected systems and identify the root cause of an attack.
- **Faster recovery times:** Cleanroom Recovery can help organizations recover from cyberattacks more quickly by providing a streamlined recovery process.
- **Reduced downtime:** Cleanroom Recovery can help organizations minimize downtime by providing a production failover solution.

Benefits of Commvault Cloud's Cleanroom Recovery

- **Improved cyber resilience:** Cleanroom Recovery can help organizations improve their cyber resilience by providing a comprehensive testing, analysis, and failover solution.
- **Reduced risk of re-infection:** Cleanroom Recovery provides a safe and isolated environment where workloads can be recovered without re-infection risk.
- **Enhanced security:** Cleanroom Recovery can be used to identify and address security vulnerabilities in cyber recovery plans.
- **Simplified failover:** Cleanroom Recovery can serve as a production failover solution in the event of a breach, ensuring that production operation recovery is conducted within a sanitized environment.

Deep Dive into Cleanroom Recovery

Testing Cyber Recovery Plans in a Hybrid Environment: Commvault Cloud's Cleanroom Recovery simplifies and streamlines the process of testing cyber recovery plans in hybrid environments. With its Any-to-Any portability feature, Cleanroom Recovery allows organizations to recover workloads from multiple clouds, on-premises hypervisors, and physical servers to a common environment within the cleanroom. This eliminates the need to perform testing within each environment separately, saving time and resources.

Forensic Analysis of Known Infected Systems: In addition to cyber recovery testing, Commvault Cloud's Cleanroom Recovery provides a secure environment for conducting forensic analysis of known infected systems. This analysis can help organizations identify the root cause of an attack, understand how the attackers gained access to their systems, and take steps to prevent future incidents.

Production Failover in the Event of a Breach: Cleanroom Recovery can serve as a production failover solution in the event of a breach. If a cyberattack disrupts an organization's production systems, they can

quickly and easily recover their workloads to a clean environment within the cleanroom. This can help organizations minimize downtime and get their business back up and running fast.

Conclusion

In today's dynamic cybersecurity landscape, organizations must proactively address the ever-increasing threat of cyberattacks. Commvault Cloud's Cleanroom Recovery is a powerful tool for organizations to enhance their cyber resilience by providing a comprehensive testing environment, secure forensic analysis capabilities, and a production failover solution. By adopting Cleanroom Recovery, organizations can confidently test their cyber recovery plans, identify and remediate vulnerabilities, and ensure business continuity in the face of cyberattacks.

Additional Resources

[1] Commvault Cleanroom Recovery https://www.commvault.com/platform/cleanroom-recovery

[2] The Evolving Threat Landscape and the Importance of Cyber Recovery https://techbeacon.com/

[3] Cleanroom Recovery: A Comprehensive Testing and Failover Solution https://www.commvault.com/platform/cleanroom-recovery

Glossary

- **Active Directory -** A directory service used to manage user accounts and computer resources in a Windows network.
- **Ad Hoc Purchase –** Ad hoc Purchase: Buying individual Commvault features separately.
- **Cleanroom** - A safe and isolated environment where organizations can test their cyber recovery plans, conduct forensic analysis of known infected systems, and ensure business continuity in the event of a breach.
- **Commvault Cloud Control Plane** – The central management component of a Commvault software environment. Previously known as the CommServe.
- **Cyberattack** - An attack that targets a computer system or network.
- **Cyber Resilience** - An organization's ability to anticipate, prepare for, and recover from cyberattacks.
- **Cyber Recovery** - The process of restoring a computer system or network to a working state after a cyberattack.
- **IAM Access -** Identity and Access Management is a system for managing user access to resources.
- **Production Failover** - The process of switching from a production environment to a cleanroom environment in the event of a breach.
- **Recovery Group** - A collection of virtual machines or other workloads grouped for recovery purposes.
- **Recovery Point Objective (RPO)** - The acceptable amount of data loss can occur before a system outage.
- **Recovery Time Objective (RTO)** - The acceptable amount of downtime that can occur before a system is restored.

To learn more, visit commvault.com

Commvault

commvault.com | 888.746.3849