



# ESSENTIAL GUIDE TO CLEANROOM RECOVERY

Cleanroom Feedback & Reference Program | July 11, 2024

# Table of Contents

<b>About the Feedback &amp; Reference Program .....</b>	<b>3</b>
<b>Introduction.....</b>	<b>4</b>
<i>WHAT IS A CLEANROOM .....</i>	<i>4</i>
CYBER ATTACKS: A RETROSPECTIVE .....	4
A TRUE TIMELINE OF A TRADITIONAL CYBER RECOVERY .....	5
DIFFERENT TYPES OF RECOVERY .....	5
OPERATIONAL RECOVERY .....	5
DISASTER RECOVERY .....	6
CYBER RECOVERY .....	6
WHY DISASTER RECOVERY ISN'T CYBER RECOVERY .....	6
WHY DISASTER RECOVERY PLANS WON'T WORK IN A CYBER RECOVERY .....	7
RPO/RTO AND THEIR LIMITATIONS IN CYBER RECOVERY .....	8
<i>USE CASES .....</i>	<i>9</i>
<b>Details of Cleanroom Recovery .....</b>	<b>10</b>
<i>CLEANROOM RECOVERY REQUIREMENTS.....</i>	<i>10</i>
<i>STRONG RECOMMENDATIONS.....</i>	<i>11</i>
<i>CLEANROOM RECOVERY PROCEDURE SUMMARY.....</i>	<i>11</i>
<i>SUPPORT MATRIX.....</i>	<i>11</i>
<i>EXAMPLE CLIENT ENVIRONMENT AND RECOVERY PROCESS.....</i>	<i>12</i>
<b>Guide.....</b>	<b>13</b>
<i>WALKTHROUGH.....</i>	<i>13</i>
RECOVER YOUR CONTROL PLANE .....	13
MAKE SURE YOUR AZURE TARGET IS SET UP .....	18
<b>Glossary .....</b>	<b>30</b>

# About the Feedback & Reference Program

## WHAT YOU GET

- 10 TB of Cleanroom Recovery & Air Gap Protect for 12 months
- Getting Started Kit
- Commvault Expertise to help deploy your first test quickly

## WHAT YOU NEED

- Azure environment
- Latest Commvault release – version 11.34 – can be in lab environment

## WHAT TO DO

- Join the sessions below
- Deploy and run a recovery
- Provide product feedback
- Be a referenceable customer

## PROGRAM SESSIONS

- Session 1 (30 mins): Demo of the Cleanroom Recovery solution and introduction to the Feedback and Reference Program
- Session 2 (30 mins): Review setup checklist, prerequisites, and configuration steps
- Session 3 (variable): Configure and run an initial Cleanroom test, discuss feedback

# Introduction

## 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.

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.
- According to IBM's Security Group, once the attacker has gained access, the average time they are in an enterprise is 204 days.<sup>1</sup> Within the first 84 minutes, according to CrowdStrike, attackers are moving laterally.<sup>2</sup> This means that during those 204 days, attackers quietly move east and west throughout the environment. These 204 days are known as left of bang.
- When attackers enact the encryption event, "bang," the damage is so pervasive that, on average, recovery from a cyber attack takes 21 days just to restore their critical systems. The days spent analyzing and recovery from the cyber attack 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 of their data back; on average, they recover less than 70% of their data.<sup>3</sup> Additionally, companies are discovering that decryption times far exceeds the time it would have taken to restore from backups.
- Businesses that pay the ransom are attacked again within a month because they are still operating in an infected environment.

---

<sup>1</sup> <https://www.ibm.com/reports/threat-intelligence>

<sup>2</sup> <https://www.crowdstrike.com/resources/reports/threat-hunting-report/>

<sup>3</sup> <https://www.sophos.com/en-us/content/state-of-ransomware>

## 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.

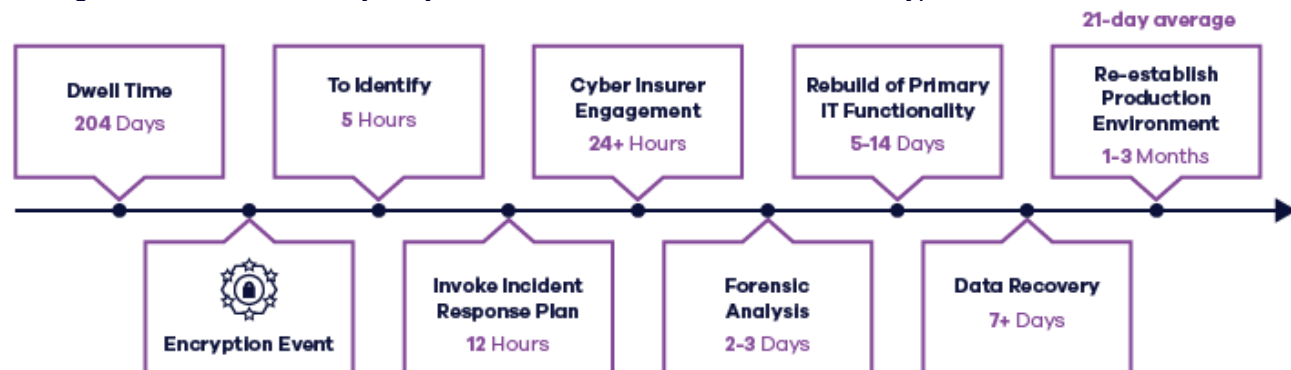


Figure 1: Cyber Recovery Timeline

- This timeline has been generated based on actual client recoveries. Let's examine some of the critical points of the timeline.
- After a confirmed attack, 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 companies use Active Directory, which is attacked in almost every breach. Therefore, a clean Active Directory must be recovered or created before any other data recovery can begin.
- Many attacks are so devastating that recovering from the environment under attack is impossible. Clients 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 your last line of defense, allowing you to recover, and they are a single repository holding all the companies' critical data.

## DIFFERENT TYPES OF RECOVERY

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

Table 1: General Recovery Types

## 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 ensure no malware or exploits remain.
- 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.

Figure 2 below summarizes these key differences visually.

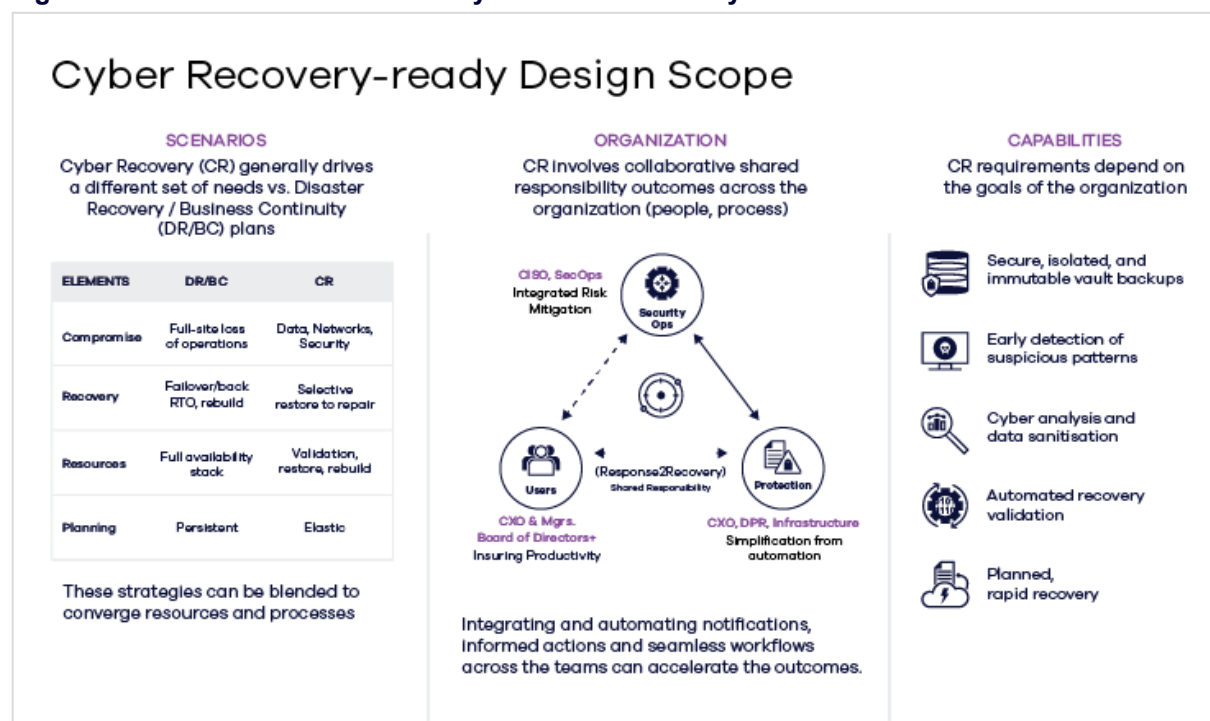


Figure 2: Disaster Recovery vs. Cyber Recovery

## 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 guarantee data integrity confidently 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 Downtime (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. 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.

# 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 defined recovery groups.

It is important to note that Commvault is not offering Azure tenant as a service. Our focus initially lies on simplifying and streamlining our clients' cleanroom recovery process within their own Azure tenant. The term "Cleanroom as a Service" should not be used to refer to our Cleanroom Recovery solution.

## CLEANROOM RECOVERY REQUIREMENTS

- Must have access to cloud.commvault.com.
- Must have any Commvault Cloud Software license, version 11.34.13 or higher.
- Must be actively backing up virtual machines to be recovered in the cleanroom.
- Must be using Air Gap Protect as secondary/tertiary copy for those virtual machines to be recovered from previous requirement.
- Commvault software clients must have the control plane (CommServe) database backup configured to go to Commvault Cloud.
- A client provided clean Azure subscription and tenant.
- A resource group and storage account are created in the Azure cleanroom.
- 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.
- IAM access is set up to access the Azure resources.
- 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](#)
- Active Directory, free of infection, available in the cleanroom.
- 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>
- Ensure at least one full backup for each virtual machine to be recovered is present in Air Gap Protect.
- VM names cannot contain special characters, whitespace or begin with '\_' or end with '.' or '-' for Azure.
- Ensure your Control Plane (CommServe) database backup is newer than the required recovery date.

- Ensure that Linux servers have Hyper-V drivers installed. [See documentation.](#)
- Remote Desktop Protocol (RDP) or SSH must be enabled on the source VM.

## STRONG RECOMMENDATIONS

Beyond the environmental requirements, there are some strong recommendations to make Cleanroom Recovery successful.

- Ensure Commvault software has local users not tied to Active Directory.
- For Linux VMs, integration services should be enabled on the source VMs if they will be powered on automatically after conversion.
- For Windows VMs, enable SAN policy for the source VM.
- VMs that are encrypted on AWS are created as VMs with no encryption on Azure.
- Recovered VMs will be automatically cleaned up (deleted from the cleanroom target) four 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.

## CLEANROOM RECOVERY PROCEDURE SUMMARY

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

- **Recover the control plane:** Log into [cloud.commvault.com](https://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.
- **Add target Azure hypervisor:** Log into the newly recovered Commvault UI and add the Azure hypervisor as a destination for recovery.
- **Add a cleanroom recovery target:** Log into the Commvault UI and create the recovery target that points to the Azure environment created in step 2.
- **Create a recovery group:** Create a recovery group, 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 broader range of sources and targets; as those workloads are tested, 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
Standalone MS-SQL in Windows VM*	Yes
Standalone DB2 in Linux VM**	Yes

Table 2: Cleanroom Recovery Support Matrix

\*MS-SQL backed up in a Windows VM must be a VM application consistent backup.

\*\*DB2 backed up in a Linux VM in a crash consistent VM backup.

## EXAMPLE CLIENT ENVIRONMENT AND RECOVERY PROCESS

Figure 5 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.

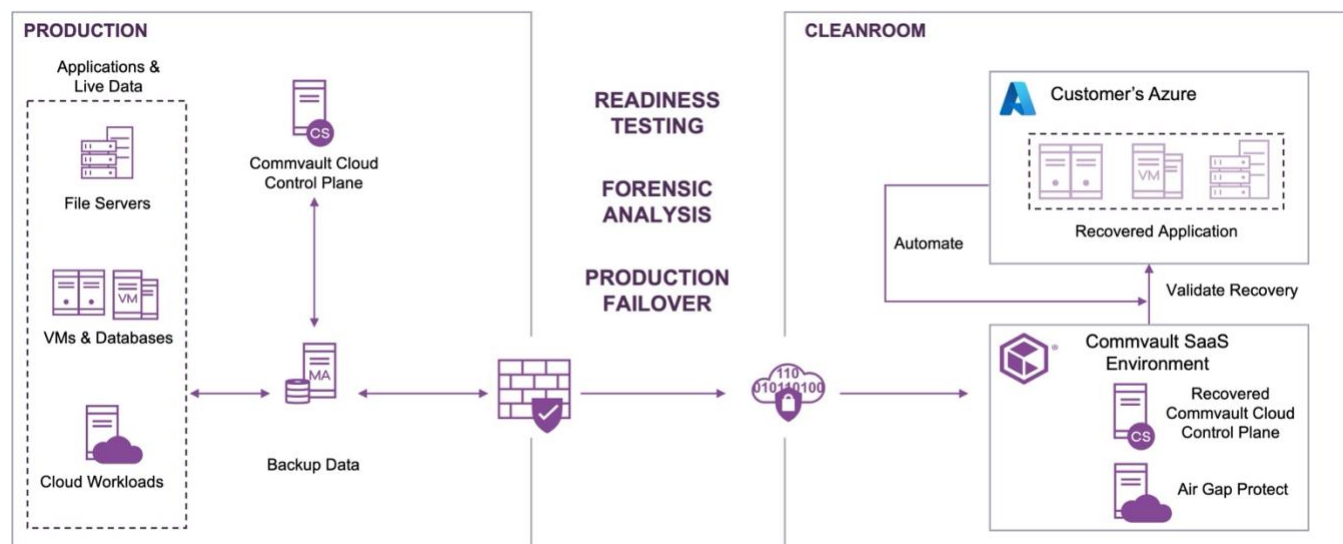


Figure 3: Sample Cleanroom Recovery Architecture (Blue is client-owned Azure environment, Purple is Commvault SaaS)

\* Recovered VMs will be automatically cleaned up (deleted from the cleanroom target) **four 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.

# Guide

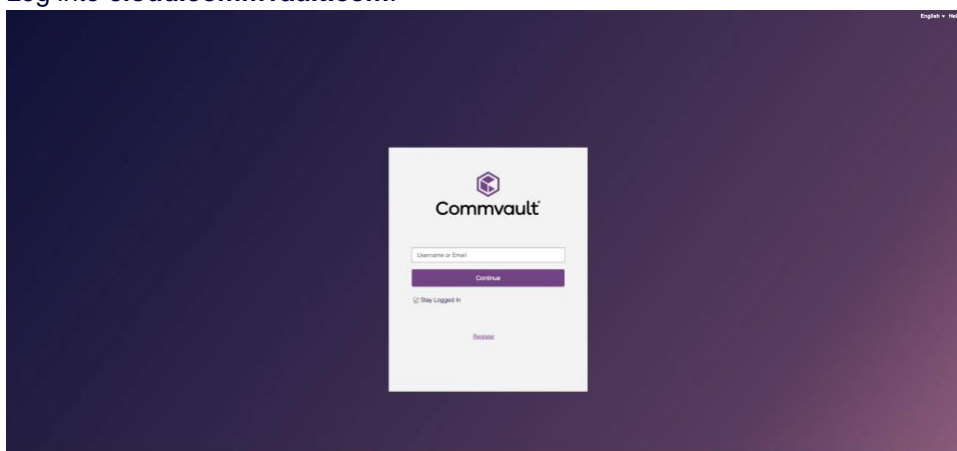
## WALKTHROUGH

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:

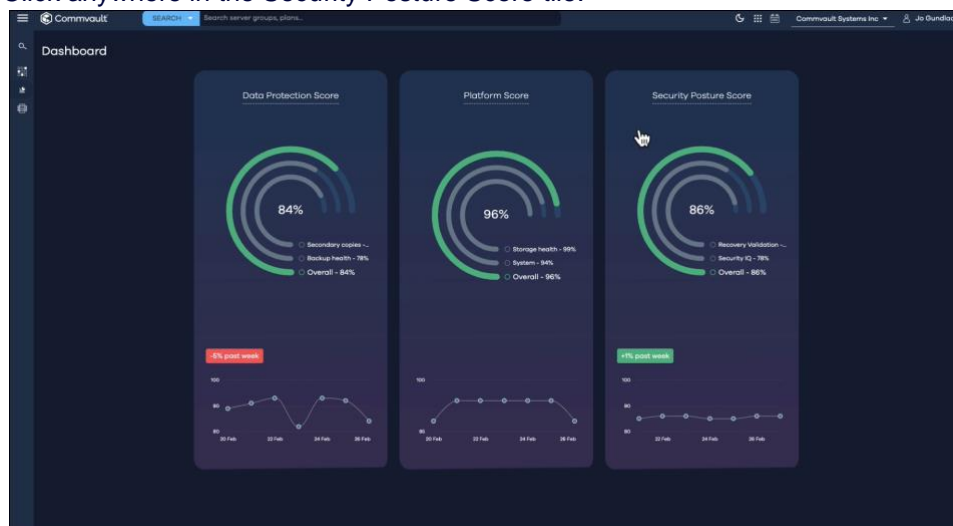
- Commvault Software has been licensed and actively backing up an environment.
- Control Plane database backups are going to cloud.commvault.com.
- Air Gap Protect has been licensed with backups going to Air Gap Protect.
- Cleanroom Recovery Licensing has been applied.
- An Azure subscription is available,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

## RECOVER YOUR CONTROL PLANE

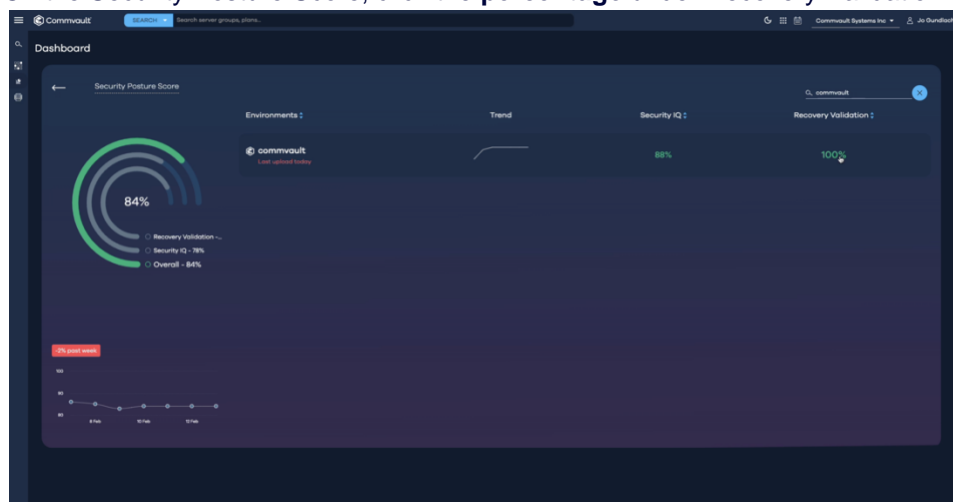
Log into **cloud.commvault.com**.



Click anywhere in the Security Posture Score tile.



On the Security Posture Score, click the **percentage** under Recovery Validation.



On the Security Posture Score Details screen, find the backup set to recover, click the ellipse on the line of the backup set, and then click **Start Recovery**.

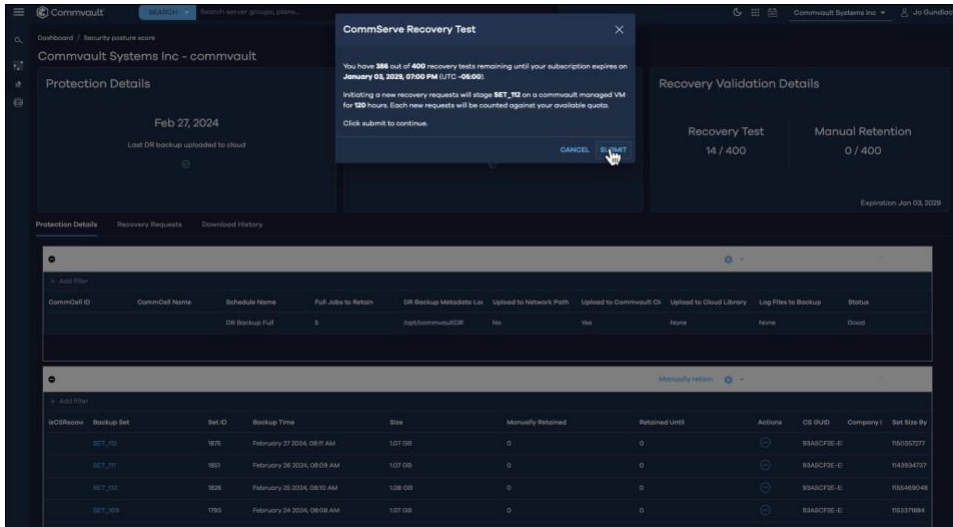
The screenshot shows the Commvault Security Posture Score Details screen. It features three main sections: Protection Details, Recovery Validation Test, and Recovery Validation Details. Below these, there are two tables. The first table shows backup sets with columns for CommCell ID, CommCell Name, Schedule Name, Full Jobs to Retain, DR Backup Metadata Len, Upload to Network Path, Upload to Commvault Cloud, Upload to Cloud Library, Log Files to Backup, and Status. The second table shows backup sets with columns for Backup Set, Set ID, Backup Time, Size, Manually Retained, Retained Until, Actions, CS GUID, Company, and Set Size By. A 'Start Recovery' button is highlighted on the 'Start Recovery' link in the Actions column of the second table.

CommCell ID	CommCell Name	Schedule Name	Full Jobs to Retain	DR Backup Metadata Len	Upload to Network Path	Upload to Commvault Cloud	Upload to Cloud Library	Log Files to Backup	Status
	DR Backup Full	5	1000000000	No	Yes	None	None	None	Good


Backup Set	Set ID	Backup Time	Size	Manually Retained	Retained Until	Actions	CS GUID	Company	Set Size By
SET_10	1875	February 27 2024, 08:11 AM	107 GB	0	0	Start Recovery	85A0CF3E-E	150387277	150387277
SET_11	1881	February 28 2024, 08:09 AM	107 GB	0	0	Start Recovery	85A0CF3E-E	143934737	143934737
SET_12	1886	February 28 2024, 08:10 AM	108 GB	0	0	Start Recovery	85A0CF3E-E	150469048	150469048
SET_109	1793	February 24 2024, 08:08 AM	107 GB	0	0	Start Recovery	85A0CF3E-E	150371884	150371884

A window will pop up asking to submit the CommServe Recovery Test. Click **Submit**.



CommServe Recovery has been submitted. The account initiating the recovery will **also receive an email**.

From: "cloudservices-donotreply@commvault.com" <cloudservices-donotreply@commvault.com>  
 Subject: CommServe Recovery Request Received :: Request ID [REDACTED]  
 Date: January 25, 2024 at 3:25:37 PM CST  
 To: Jo Gundlach <[REDACTED]>  
 Cc: "cloudrbackup@commvault.com" <cloudrbackup@commvault.com>

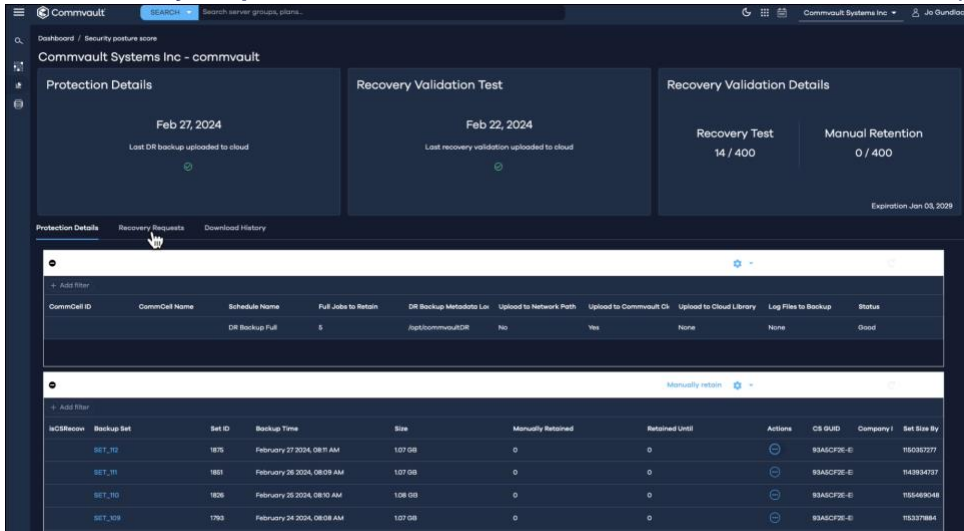


Hello Jo Gundlach,

Your request for CommServe Recovery has been received.  
 You will receive an email upon request completion.

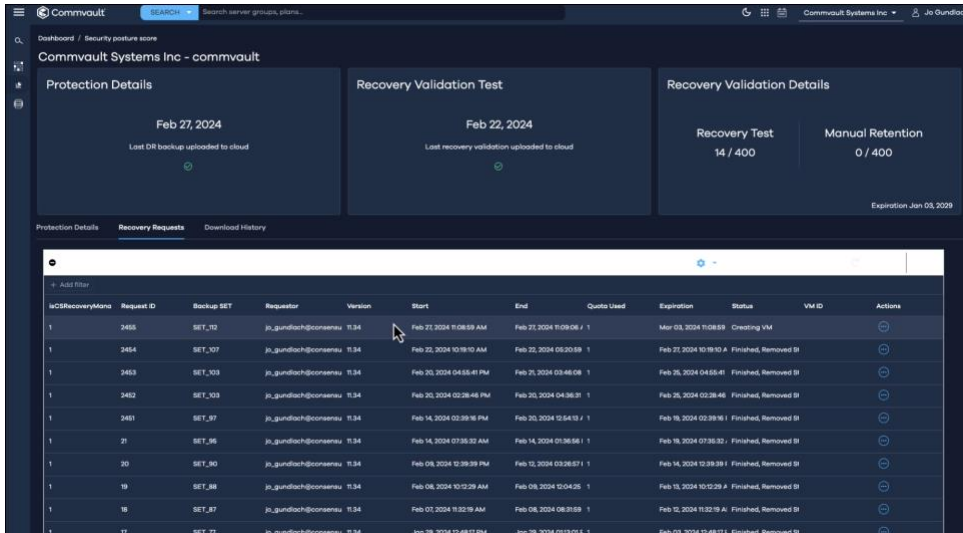
Request ID- [REDACTED]

Click **Recovery Requests** on the left middle of the screen to monitor the restore process.





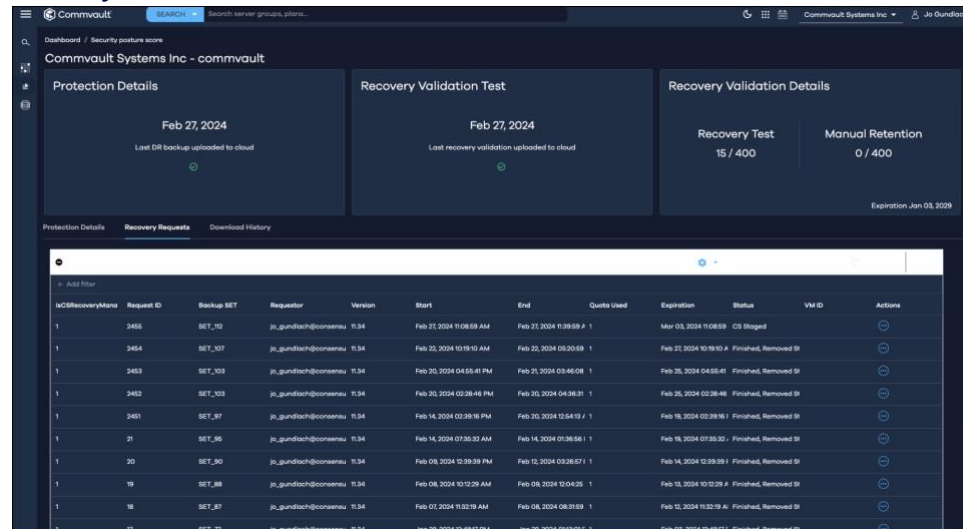
Refreshing the page will show the **Status** of the recovery.



The screenshot shows the Commvault dashboard for 'Commvault Systems Inc - commvault'. The 'Recovery Validation Test' section indicates the test is in progress as of Feb 22, 2024. The 'Recovery Validation Details' section shows 'Recovery Test 14 / 400' and 'Manual Retention 0 / 400'. The table below lists recovery requests with their status.

Request ID	Backup SET	Requestor	Version	Start	End	Quota Used	Expiration	Status	VM ID	Actions
2455	SET_102	ju.gundlach@commvault	1.34	Feb 21, 2024 11:08:59 AM	Feb 21, 2024 11:09:08 AM	1	Mar 03, 2024 11:08:59 AM	Creating VM		
2454	SET_107	ju.gundlach@commvault	1.34	Feb 22, 2024 10:19:10 AM	Feb 22, 2024 03:20:59 PM	1	Feb 21, 2024 10:19:10 AM	Finished, Removed SR		
2453	SET_103	ju.gundlach@commvault	1.34	Feb 20, 2024 04:55:41 PM	Feb 21, 2024 03:46:08 PM	1	Feb 26, 2024 04:55:41 PM	Finished, Removed SR		
2452	SET_103	ju.gundlach@commvault	1.34	Feb 20, 2024 02:28:46 PM	Feb 20, 2024 04:36:31 PM	1	Feb 26, 2024 02:28:46 PM	Finished, Removed SR		
2451	SET_97	ju.gundlach@commvault	1.34	Feb 14, 2024 02:39:16 PM	Feb 20, 2024 12:54:12 PM	1	Feb 19, 2024 02:39:16 PM	Finished, Removed SR		
21	SET_36	ju.gundlach@commvault	1.34	Feb 14, 2024 07:35:32 AM	Feb 14, 2024 01:36:56 PM	1	Feb 19, 2024 07:35:32 AM	Finished, Removed SR		
20	SET_30	ju.gundlach@commvault	1.34	Feb 08, 2024 12:39:39 PM	Feb 12, 2024 03:26:57 PM	1	Feb 14, 2024 12:39:39 PM	Finished, Removed SR		
19	SET_38	ju.gundlach@commvault	1.34	Feb 08, 2024 10:12:29 AM	Feb 08, 2024 12:04:25 PM	1	Feb 13, 2024 10:12:29 AM	Finished, Removed SR		
18	SET_37	ju.gundlach@commvault	1.34	Feb 07, 2024 11:32:19 AM	Feb 08, 2024 08:31:59 PM	1	Feb 12, 2024 11:32:19 AM	Finished, Removed SR		
17	SET_37	ju.gundlach@commvault	1.34	Jan 29, 2024 12:48:17 PM	Jan 29, 2024 01:13:01 PM	1	Feb 03, 2024 12:48:17 PM	Finished, Removed SR		


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



The screenshot shows the Commvault dashboard after refreshing. The 'Recovery Validation Test' section now shows the test is completed as of Feb 27, 2024. The 'Recovery Validation Details' section shows 'Recovery Test 15 / 400' and 'Manual Retention 0 / 400'. The table below shows the updated status of the recovery requests.

Request ID	Backup SET	Requestor	Version	Start	End	Quota Used	Expiration	Status	VM ID	Actions
2455	SET_102	ju.gundlach@commvault	1.34	Feb 21, 2024 11:08:59 AM	Feb 21, 2024 11:09:08 AM	1	Mar 03, 2024 11:08:59 AM	CS Staged		
2454	SET_107	ju.gundlach@commvault	1.34	Feb 22, 2024 10:19:10 AM	Feb 22, 2024 03:20:59 PM	1	Feb 21, 2024 10:19:10 AM	Finished, Removed SR		
2453	SET_103	ju.gundlach@commvault	1.34	Feb 20, 2024 04:55:41 PM	Feb 21, 2024 03:46:08 PM	1	Feb 26, 2024 04:55:41 PM	Finished, Removed SR		
2452	SET_103	ju.gundlach@commvault	1.34	Feb 20, 2024 02:28:46 PM	Feb 20, 2024 04:36:31 PM	1	Feb 26, 2024 02:28:46 PM	Finished, Removed SR		
2451	SET_97	ju.gundlach@commvault	1.34	Feb 14, 2024 02:39:16 PM	Feb 20, 2024 12:54:12 PM	1	Feb 19, 2024 02:39:16 PM	Finished, Removed SR		
21	SET_36	ju.gundlach@commvault	1.34	Feb 14, 2024 07:35:32 AM	Feb 14, 2024 01:36:56 PM	1	Feb 19, 2024 07:35:32 AM	Finished, Removed SR		
20	SET_30	ju.gundlach@commvault	1.34	Feb 08, 2024 12:39:39 PM	Feb 12, 2024 03:26:57 PM	1	Feb 14, 2024 12:39:39 PM	Finished, Removed SR		
19	SET_38	ju.gundlach@commvault	1.34	Feb 08, 2024 10:12:29 AM	Feb 08, 2024 12:04:25 PM	1	Feb 13, 2024 10:12:29 AM	Finished, Removed SR		
18	SET_37	ju.gundlach@commvault	1.34	Feb 07, 2024 11:32:19 AM	Feb 08, 2024 08:31:59 PM	1	Feb 12, 2024 11:32:19 AM	Finished, Removed SR		
17	SET_37	ju.gundlach@commvault	1.34	Jan 29, 2024 12:48:17 PM	Jan 29, 2024 01:13:01 PM	1	Feb 03, 2024 12:48:17 PM	Finished, Removed SR		



**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 <img alt="redacted" data-bbox="205 180 415 190"/>>  
**Cc:** "cloudbackup@commvault.com" <cloudbackup@commvault.com>



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

To access the newly recovered instance, click the ellipses on the line of the recovered backup set and click **Access Details**.

Commvault

SEARCH

Search across groups, plans...

Dashboard / Security posture score

Commvault Systems Inc - commvault

Protection Details

Feb 27, 2024

Last DR backup uploaded to cloud

Recovery Validation Test

Feb 27, 2024

Last recovery validation uploaded to cloud

Recovery Validation Details

Recovery Test

15 / 400

Manual Retention

0 / 400

Expiration Jan 03, 2029

Protection Details

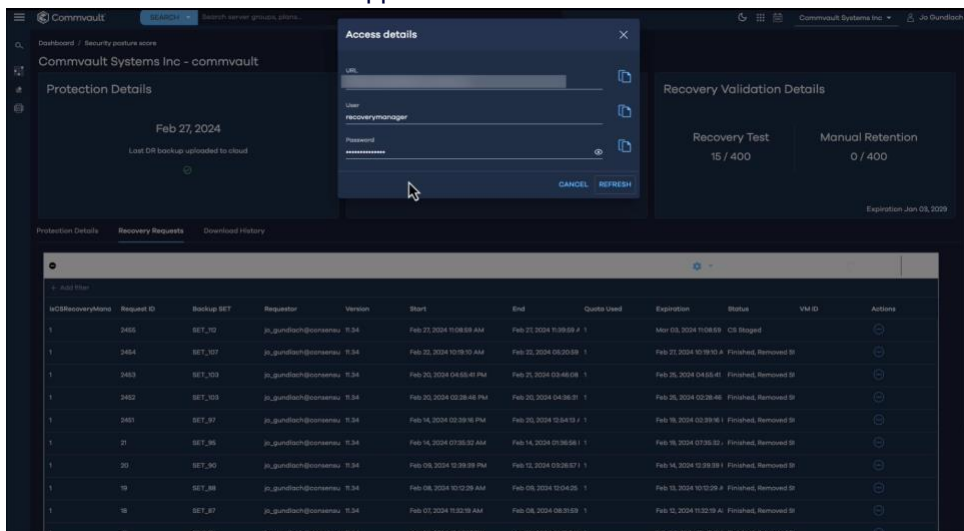
Recovery Requests

Download History

+

Add filter

HCSDRecoveryMans	Request ID	Backup SET	Requestor	Version	Start	End	Quota Used	Expiration	Status	VM ID	Actions
1	2455	SET_102	jo.gundlach@commvault.com	9.34	Feb 27, 2024 11:08:59 AM	Feb 27, 2024 11:39:59 AM	1	Mar 03, 2024 11:08:59 AM	CS Staged		<div><div>?</div><div>Extend Reservation</div><div>Access Details</div></div>
1	2454	SET_107	jo.gundlach@commvault.com	9.34	Feb 25, 2024 10:19:10 AM	Feb 25, 2024 05:20:59 AM	1	Feb 27, 2024 10:19:10 AM	Finished, Removed St		<div><div>?</div><div>?</div></div>
1	2453	SET_103	jo.gundlach@commvault.com	9.34	Feb 25, 2024 04:55:41 PM	Feb 25, 2024 03:46:08 AM	1	Feb 26, 2024 04:55:41 PM	Finished, Removed St		<div><div>?</div><div>?</div></div>
1	2452	SET_103	jo.gundlach@commvault.com	9.34	Feb 25, 2024 02:36:46 PM	Feb 25, 2024 04:36:31 AM	1	Feb 26, 2024 02:36:46 PM	Finished, Removed St		<div><div>?</div></div>
1	2451	SET_97	jo.gundlach@commvault.com	9.34	Feb 14, 2024 02:39:16 PM	Feb 20, 2024 12:54:19 AM	1	Feb 19, 2024 02:39:16 PM	Finished, Removed St		<div><div>?</div></div>
1	21	SET_95	jo.gundlach@commvault.com	9.34	Feb 14, 2024 07:35:32 AM	Feb 14, 2024 07:35:32 AM	1	Feb 19, 2024 07:35:32 AM	Finished, Removed St		<div><div>?</div></div>
1	20	SET_95	jo.gundlach@commvault.com	9.34	Feb 09, 2024 12:39:39 PM	Feb 12, 2024 03:26:57 AM	1	Feb 14, 2024 12:39:39 PM	Finished, Removed St		<div><div>?</div></div>
1	19	SET_88	jo.gundlach@commvault.com	9.34	Feb 09, 2024 10:12:29 AM	Feb 09, 2024 10:04:25 AM	1	Feb 13, 2024 10:12:29 AM	Finished, Removed St		<div><div>?</div></div>
1	18	SET_87	jo.gundlach@commvault.com	9.34	Feb 07, 2024 11:32:19 AM	Feb 08, 2024 08:35:59 AM	1	Feb 12, 2024 11:32:19 AM	Finished, Removed St		<div><div>?</div></div>
1	17	SET_77	jo.gundlach@commvault.com	9.34	Jan 29, 2024 12:48:17 PM	Jan 29, 2024 01:13:01 AM	1	Feb 03, 2024 12:48:17 PM	Finished, Removed St		<div><div>?</div></div>

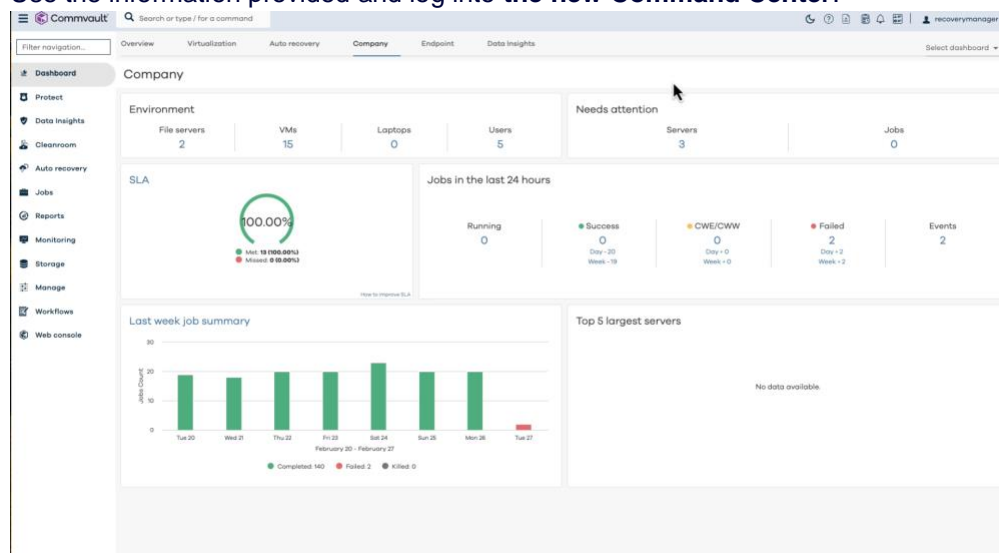


**Azure requires that VM names do not contain special characters, whitespace or begin with '\_' or end with '\_' or '-'**

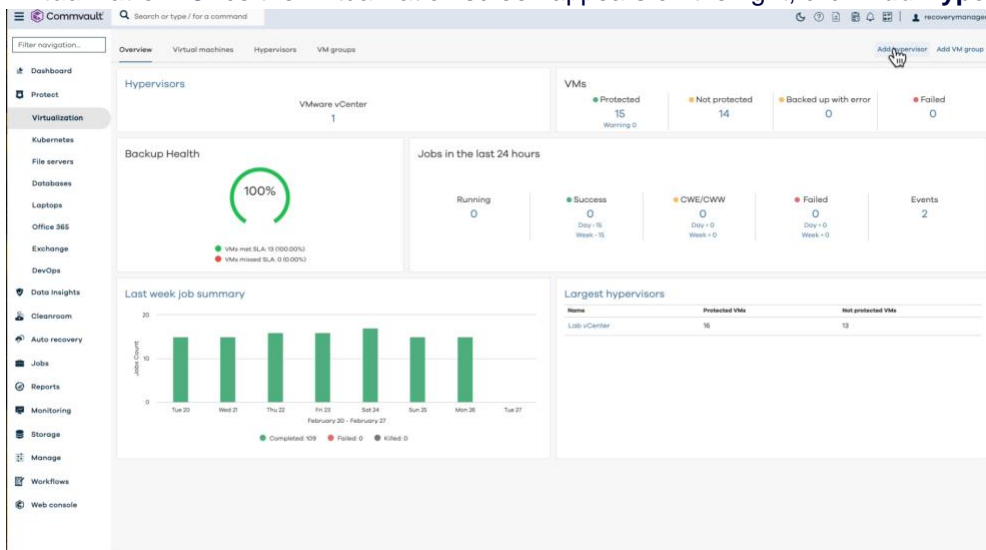
1. An enterprise application
2. Application Secret
3. Resource Group
4. A Storage Account within the Resource Group
5. A Network Group within the Resource Group
6. A Network Security Group within the Resource Group
7. The application must be assigned a contributor role in EntraID
8. The following resource groups should be registered to the subscription.
  - a. microsoft.support
  - b. microsoft.Storage
  - c. microsoft.SerialConsole
  - d. microsoft.Resourcesmicrosoft.ResourceNotifications
  - e. microsoft.ResourceGraph
  - f. microsoft.Portal
  - g. microsoft.Operationallnsights
  - h. microsoft.Network

- i. microsoft.MarketplaceOrdering
- j. microsoft.MarketplaceNotifications
- k. microsoft.MachineLearning
- l. microsoft.GuestConfiguration
- m. microsoft.Features
- n. microsoft.CostManagement
- o. microsoft.Consumption
- p. microsoft.Compute
- q. Microsoft.Commerce
- r. microsoft.CloudShell
- s. microsoft.ClassicSubscription
- t. microsoft.ChangeAnalysis
- u. microsoft.Billing
- v. microsoft.Authorization
- w. microsoft.ADHybridHealthService

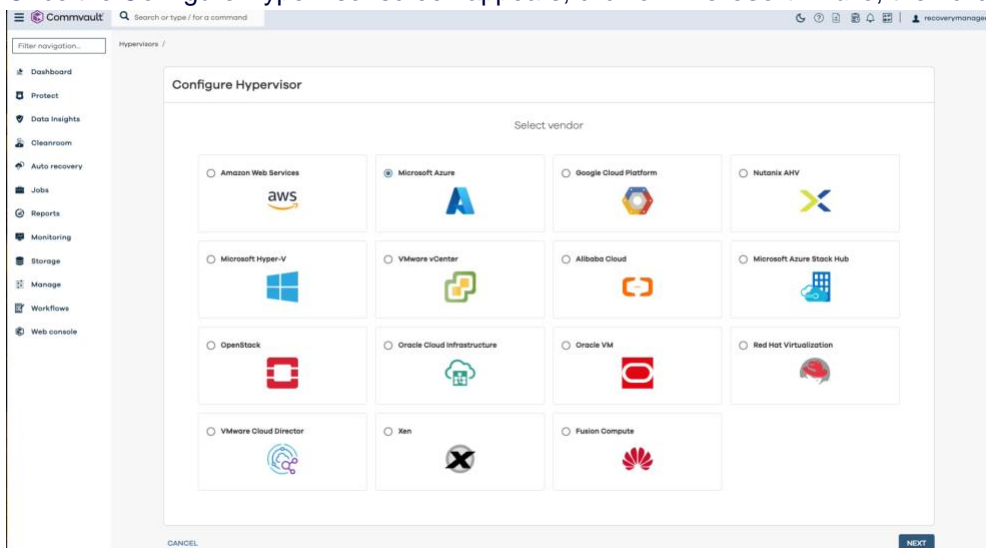
Use the information provided and log into **the new Command Center**.



Add target **Azure Hypervisor** to the newly recovered control plane. In the left-hand navigation, click **Protect** -> **Virtualization**. Once the Virtualization screen appears on the right, click **Add Hypervisor** on the top right.



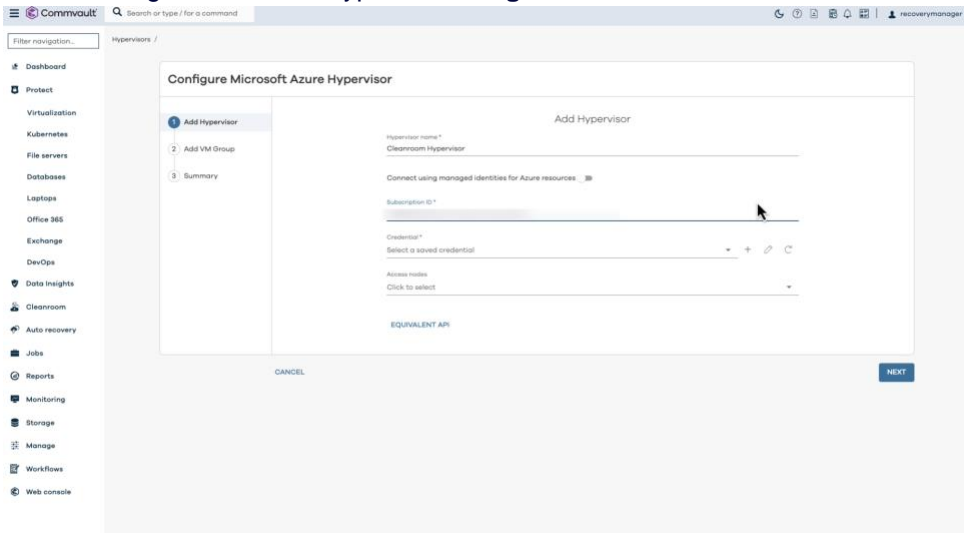
Once the Configure Hypervisor screen appears, click on **Microsoft Azure**, then click **Next**.



Now, we need to configure the Azure Hypervisor. For this step, you will need:

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

We need to give the Azure Hypervisor a **logical name** for reference later and the subscription ID.



Configure Microsoft Azure Hypervisor

Add Hypervisor

Hypervisor name \*

Cleanroom Hypervisor

Connect using managed identities for Azure resources

Subscription ID \*

Credential \*

Select a saved credential

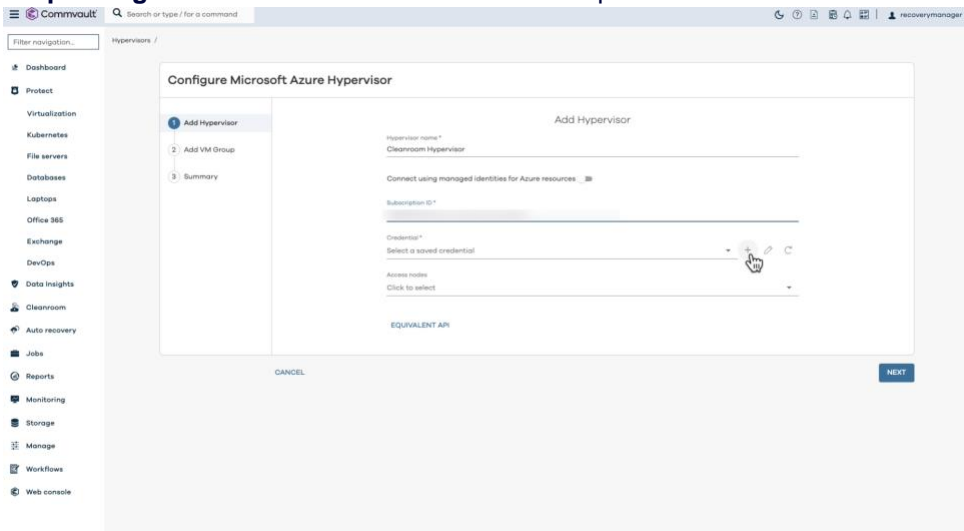
Access nodes

Click to select

EQUIVALENT API

CANCEL NEXT

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.



Configure Microsoft Azure Hypervisor

Add Hypervisor

Hypervisor name \*

Cleanroom Hypervisor

Connect using managed identities for Azure resources

Subscription ID \*

Credential \*

Select a saved credential

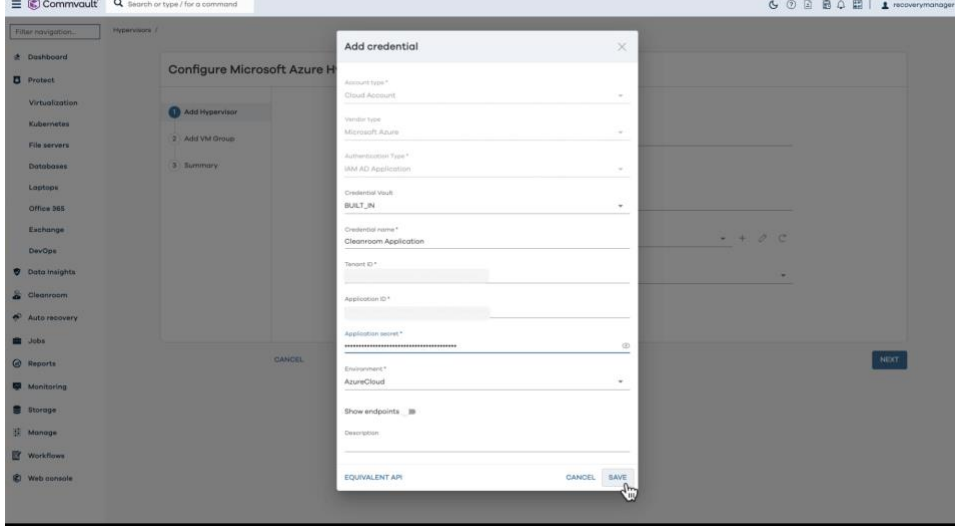
Access nodes

Click to select

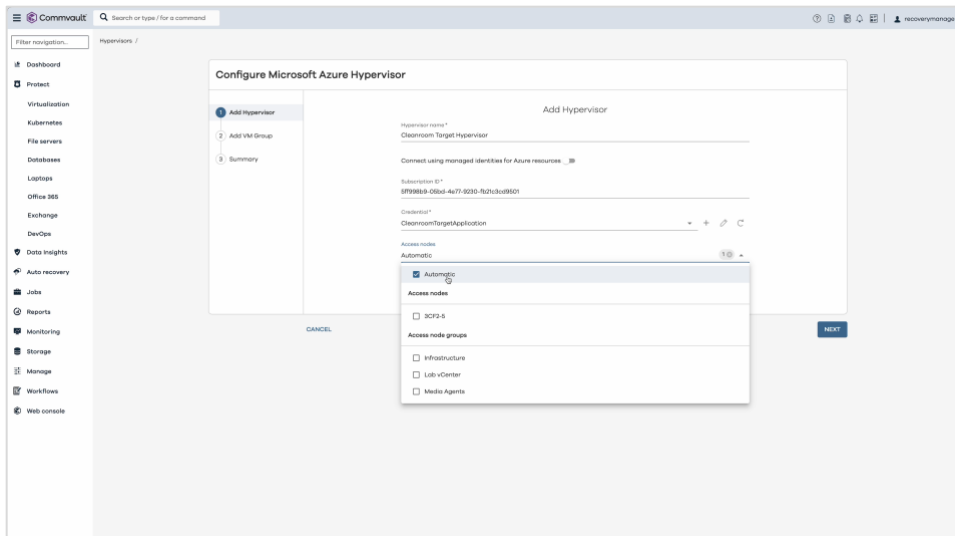
EQUIVALENT API

CANCEL NEXT

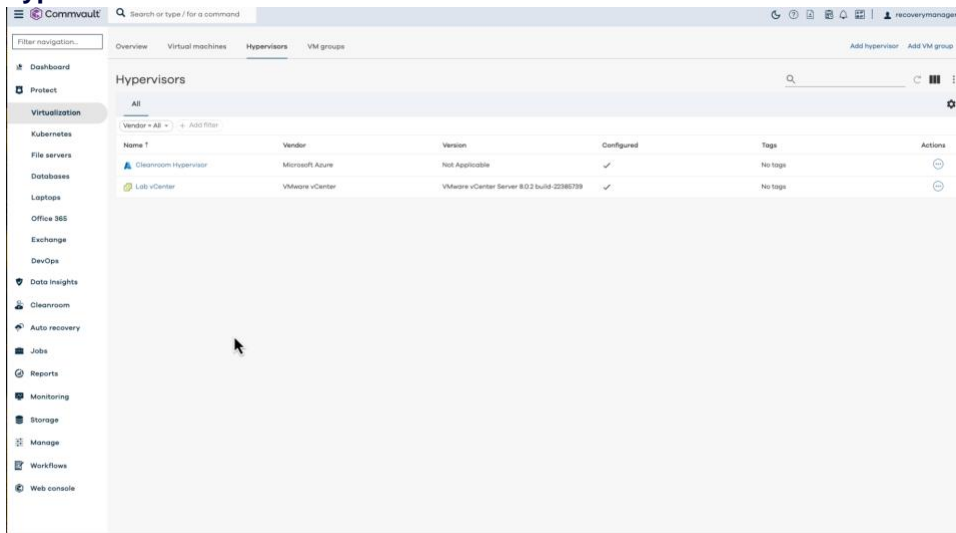
In the **Add Credential Wizard**, we will give the credentials a logical name we can reference later, the Tenant ID, Application ID, and Application Secret. Fill in all of the appropriate information and click **Save**.



This now populates the credential field with the access credentials that were created. Select access node, **Automatic**.

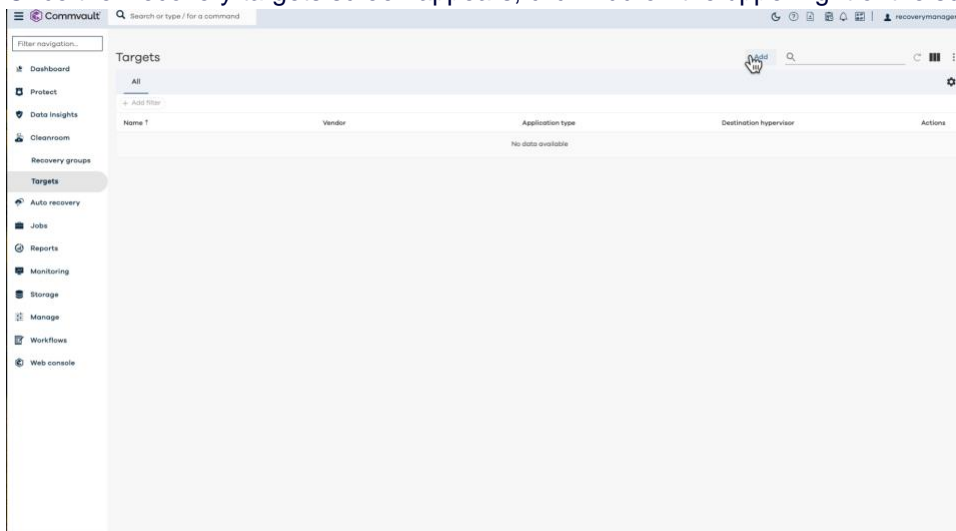


Select **Next**. On the Add VM Group step, you can click **Cancel**. At this step, **you have added the target hypervisor**.



**Now, we need to add a Cleanroom Recovery Target.** In the left-hand navigation, click Cleanroom -> Targets.

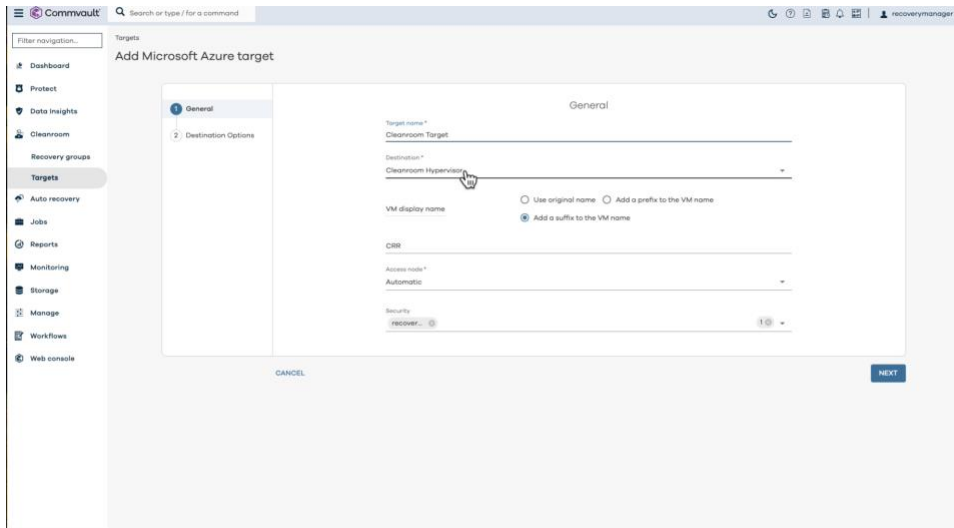
Once the Recovery targets screen appears, click Add on the upper right of the screen.



Now, **fill out the information** for your recovery target.

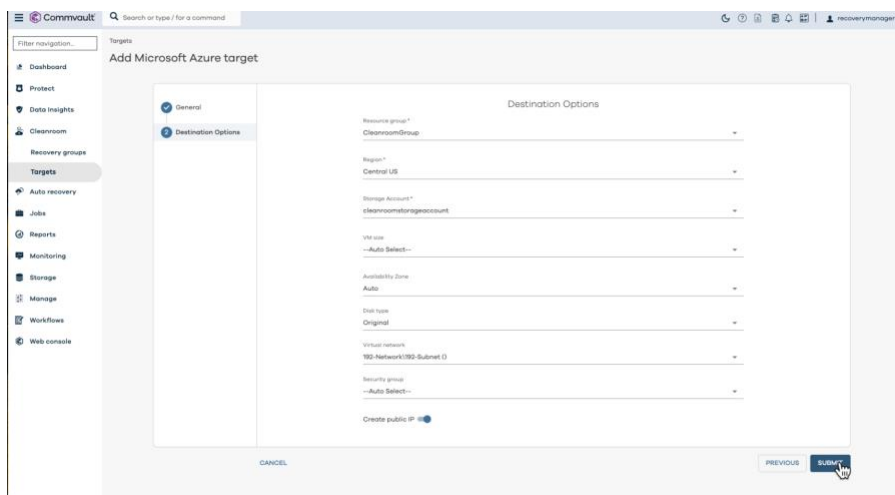
- Give the target a logical name we will reference later.
- Select the Destination (previously created Azure Hypervisor).
- Choose how you want the VM names to appear. We chose to add a suffix of CRVM.
- Select the access node; this can be the recovered control plane selected when the Hypervisor was defined.

Click **Next**.



On the **Destination 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.
- Select **Create public IP** to let Commvault auto-assign a public IP from your Azure subscription.
- Click **Submit**.



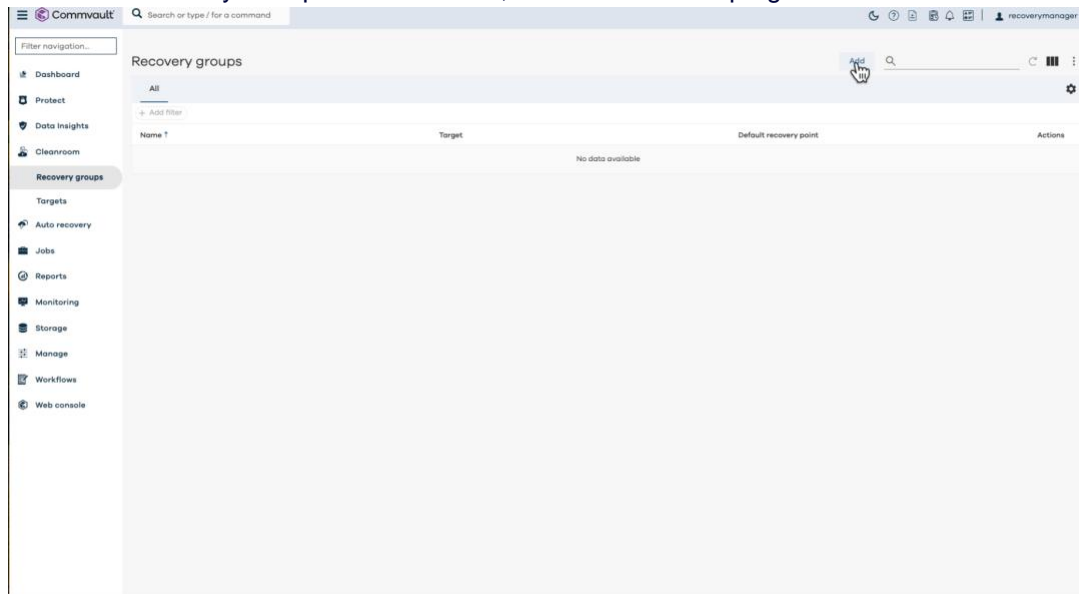


A recovery target has now been created. **We now need to create a Recovery Group.**

The Recovery Group is the logical group of servers that will be recovered together.

On the left-hand navigation, click **Recovery Groups**.

Once the Recovery Groups screen shows, click **Add** in the top right.

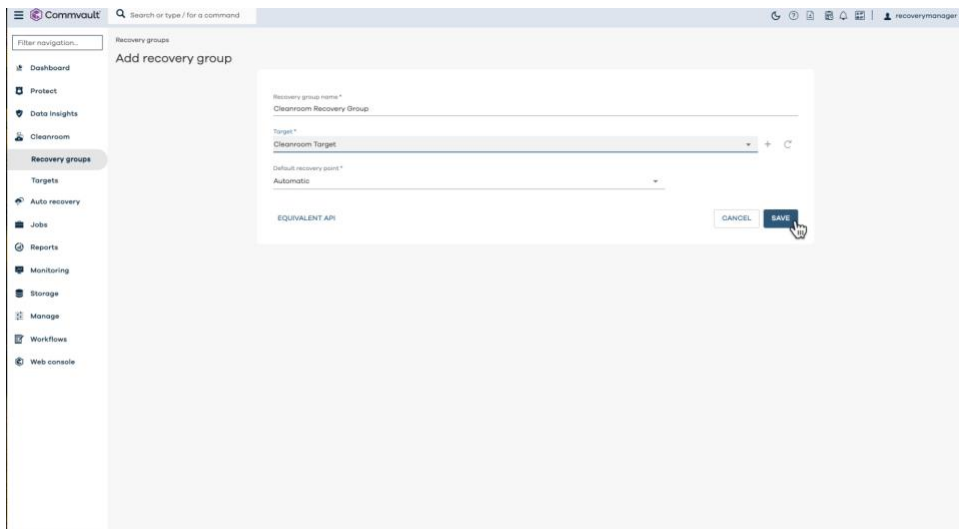


Once the Add Recovery Group screen loads, define the group. The settings we set here will default for all entities added later.

- Enter a **logical name** for the recovery group.
- Select the **Recovery target** that you previously created.
- Select the **automatic** for the point in time to recover to.

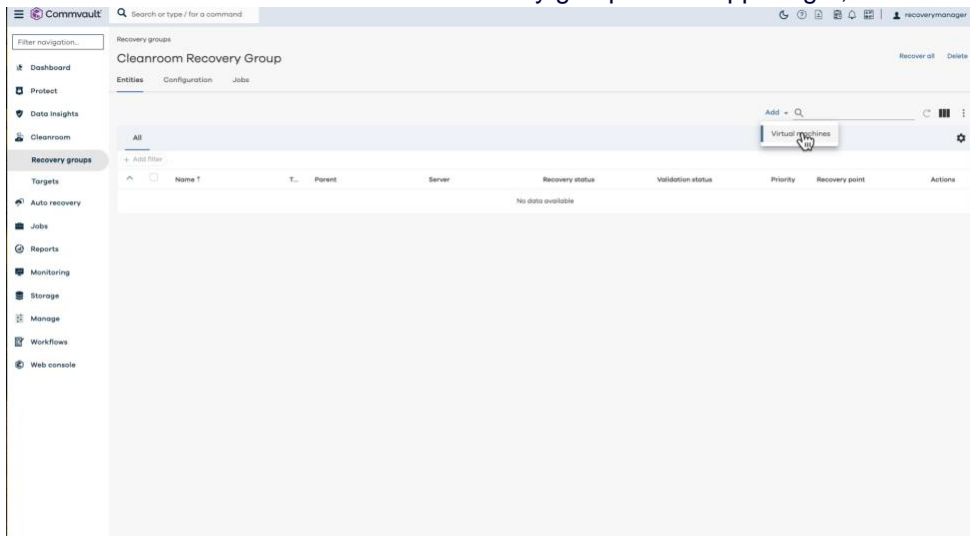
Automatic recovery points streamline the cyber recovery process by integrating with external security tools like SIEM/SOARs. These tools pinpoint compromised servers and their exact time of infection, allowing Commvault to rewind to the last known good state automatically. Instead of external tools,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

Click **Save**.

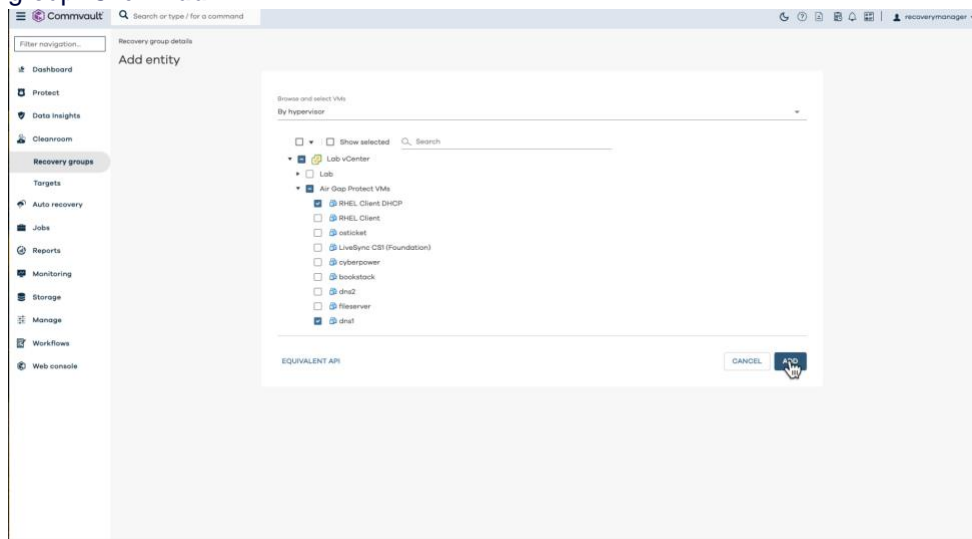


The **Recovery group** has been created.

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

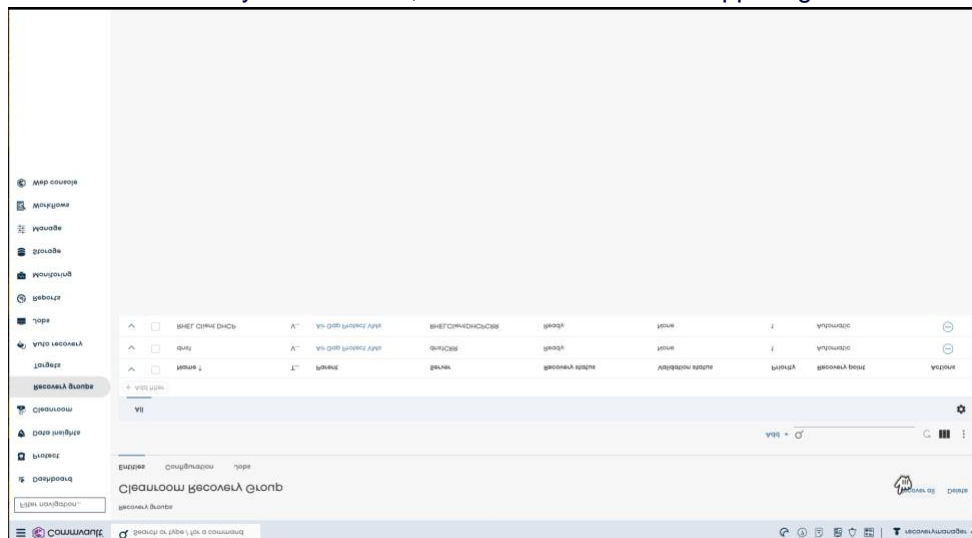


Once the Add entity screen loads, expand the list of hypervisors and select the virtual machines to add to the group. Click **Add**.

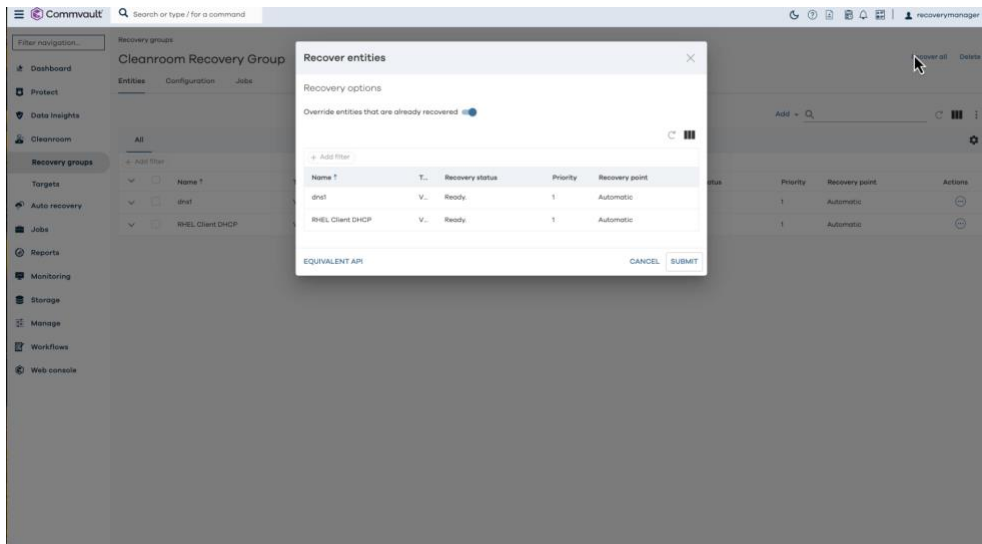


The Recovery Group is **now populated** with entities to recover.

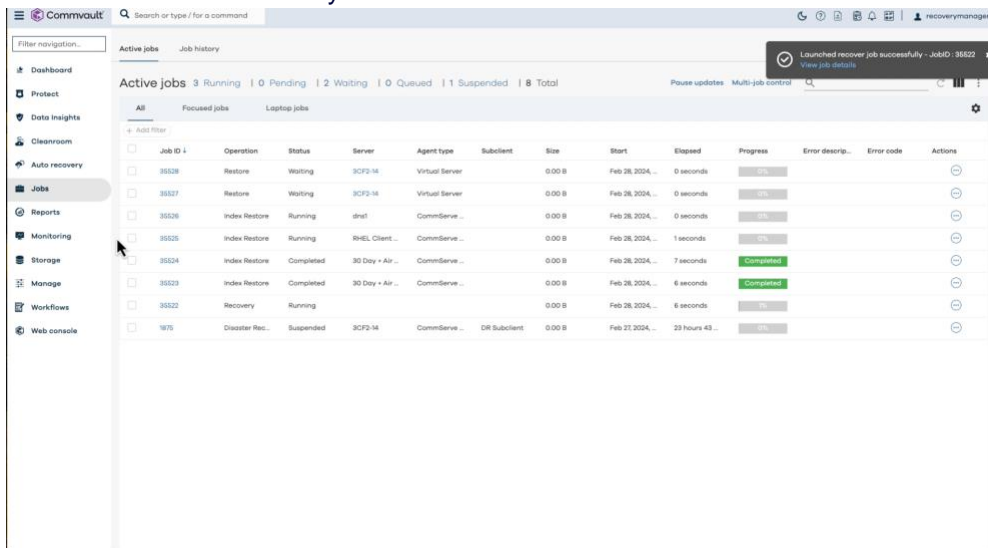
To initiate a recovery of all entities, click **Recover all** in the upper right of the Recovery group screen.



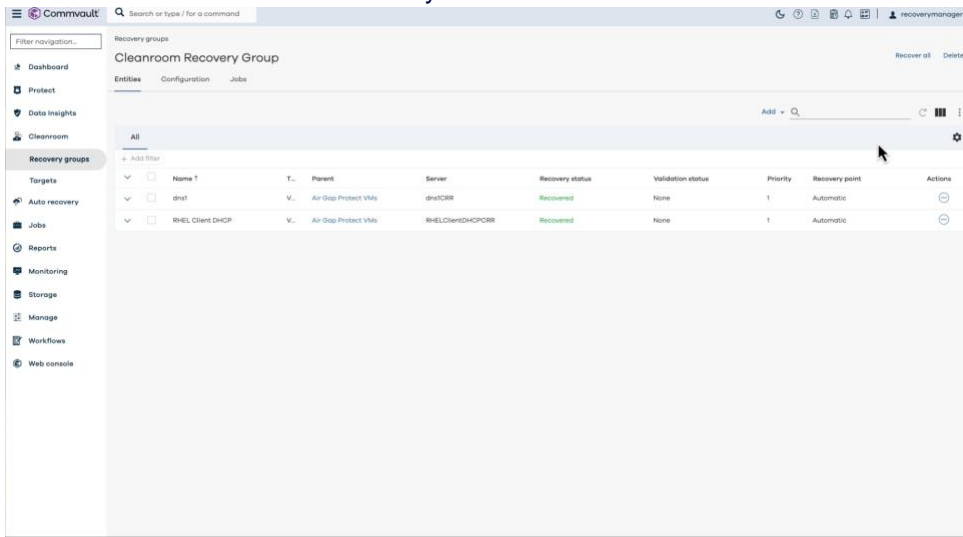
Alternatively, if you click the checkbox next to a specific machine(s) **Recover** appears next to Add. Clicking **Recover** will initiate a recovery of only the selected machine(s). Once the Recover entities screen loads, click on **Submit**.



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.

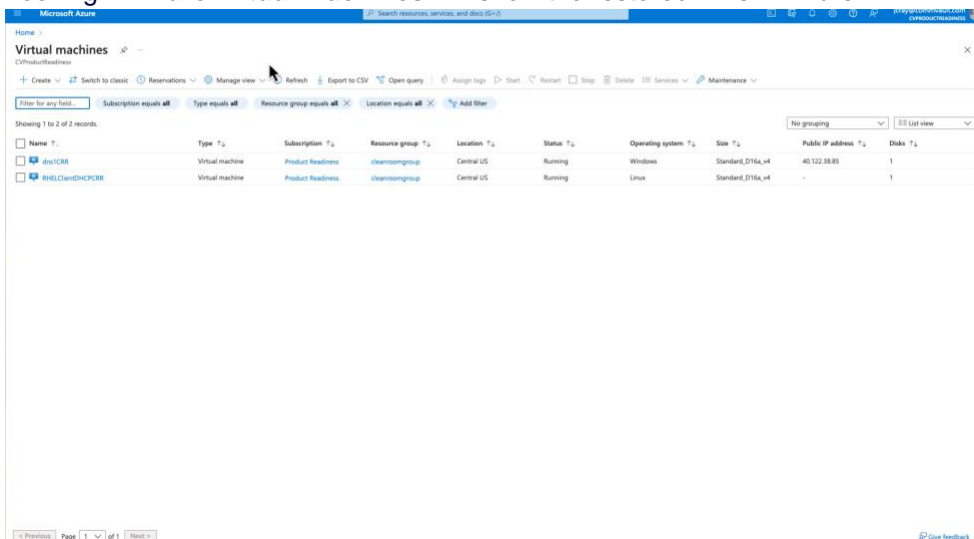


To monitor the state of each VM **click Cleanroom -> Recovery group -> recovery group** name and the list of entities are listed with their Recovery status.



Name	Parent	Server	Recovery status	Validation status	Priority	Recovery point	Actions
dm1	Air Gap Protect VMs	dm1CRR	Recovered	None	1	Automatic	
RHELClientDHCPDR	Air Gap Protect VMs	RHELClientDHCPDR	Recovered	None	1	Automatic	

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



Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk
dm1CRR	Virtual machine	Product Readiness	cleanroomgroup	Central US	Running	Windows	Standard_D16s_v4	40.122.38.85	1
RHELClientDHCPDR	Virtual machine	Product Readiness	cleanroomgroup	Central US	Running	Linux	Standard_D16s_v4	-	1

\* Recovered VMs will be automatically cleaned up (deleted from the cleanroom target) four 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.

# 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](https://commvault.com)



commvault.com | 888.746.3849

© 1999-2024 Commvault Systems, Inc. All rights reserved. A list of our trademarks and patents is available [here](#). Other third-party brands, product names, and trademarks are the property of their respective owners and used solely to identify their products or services.