

. 0 . 0 0

ESSENTIAL GUIDE TO CLEANROOM RECOVERY

.

Partner v1.3 | July 11, 2024



Table of Contents

Introduction	4
WHAT IS A CLEANROOM	
CYBER ATTACKS: A RETROSPECTIVE	4
A TRUE TIMELINE OF A TRADITIONAL CYBER RECOVERY	5
OPERATIONAL RECOVERY	ə 5
DISASTER RECOVERY	6
CYBER RECOVERY	
WHY DISASTER RECOVERY ISN'T CYBER RECOVERY	6 7
RPO/RTO AND THEIR LIMITATIONS IN CYBER RECOVERY	
USE CASES	9
WHAT IS CYBER RESILIENCE	
THE FORTIFYING PILLARS OF CYBER RESILIENCE	10
WHY PRIORITIZE CYBER RESILIENCE?	11
Details of Cleanroom Recovery	11
CLEANROOM RECOVERY REQUIREMENTS	11
STRONG RECOMMENDATIONS	
CLEANROOM RECOVERY PROCEDURE SUMMARY	12
SUPPORT MATRIX	
EXAMPLE CLIENT ENVIRONMENT AND RECOVERY PROCESS	13
BUY vs BUILD	14
CONSULTING SERVICES	14
Licensing	15
SKUs	
CLEANROOM RECOVERY VS CONTROL PLANE RECOVERY & VALIDATION	15
Competitive	
KEY DIFFERENTIATION	
ANOMALY DETECTION	
COMMON MISCONCEPTIONS	
Main Competitors	16
Field Guide	
WALKTHROUGH	
RECOVER YOUR CONTROL PLANE	
MAKE SURE YOUR AZURE TARGET IS SET UP	23
Glossary	35





Frequently Asked Questions



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.¹ Within the first 84 minutes, according to CrowdStrike, attackers are moving laterally.² 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.³ 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.

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

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

³ 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
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

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:

 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.

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 adequately 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 use 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 ensures a well-rounded defense against cyber threats.

WHAT IS CYBER RESILIENCE

After examining the intricacies of cyberattacks, the nuanced differences between cyber and disaster recovery, and the critical role of cleanrooms, let's examine 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 help minimize attack surfaces and vulnerabilities, acting as your digital shield.
- **Planning:** Comprehensive cyber response, recovery plans after a breach, and business restoration procedures, as 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, helping to minimize damage and impact.
- **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 for business continuity and data integrity. This is akin to rebuilding stronger after an attack, continually building your digital infrastructure.
- 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 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 <u>Managing a Key Management Server</u>.
- 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: <u>https://azure.microsoft.com/en-us/solutions/linux-on-azure</u>
 - Microsoft server software support for Azure virtual machines: <u>https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/server-software-support</u>
 - Azure product availability by region: <u>https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/regions</u>
- 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 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.









* 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.

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-built solution.

CONSULTING SERVICES

While setting up Commvault Cleanroom Recovery is straightforward, the challenge lies in navigating the complexities of cyber recovery. This includes understanding the process, planning effectively, testing rigorously, and ensuring your overall data protection is cyber-ready.

That is where Commvault Cyber Resilience Services come in. Our team of experts combines deep Commvault knowledge with proven cyber recovery experience. This unique blend empowers us to guide you through every step of your cyber recovery journey, helping you achieve true cyber resilience.





Commvault offers a comprehensive suite of Cleanroom services tailored to your specific needs. We help you plan, test, and even execute cyber recovery when necessary, ensuring your business is prepared for any attack.

By partnering with Commvault, you gain access to years of expertise in Commvault Cloud and cyber resilience. We work collaboratively to develop a robust recovery strategy, giving you the confidence to face any cyber threat.

Licensing

SKUs

To use Cleanroom Recovery, the client will need to license:

- Commvault Cloud Software
- Air Gap Protect
- Cleanroom Recovery

Cleanroom Recovery is sold in increments of 10TB. The 10TB measurement is based on the amount of data the customer configures into a Recovery Group based on front-end terabytes. If they configure 100TB of data into the recovery groups (based on the data size at the time of configuration), they will need 10 of the CV-CLNRM-10TB SKU. If the client needs to configure 104TB of data, they must purchase 11 of the CV-CLNRM-10TB SKU. If a customer configures a recovery group within their licensed limits, that data set grows to exceed what they have purchased. In that case, they will be given notification of the overage, and no further systems/data will be able to be added to the recovery groups until the license overage is remedied. See Table 3 below for more details.

Feature	Cleanroom Recovery
Entitlement to CV Cloud Hosted Infrastructure for Control Plane Recovery (Single Node CS/MA)	Yes
License Metric	10TB per Unit/Year of configured data
Recovery Allowance	No Restriction on Recoveries. Licensing is enforced based on how much data is configured into the recovery group.
Entitlement to use Recovery Group Automation	Yes
SKU	CV-CLNRM-10TB
Revenue Classification	SaaS
Sold to	CV Software Customers (SaaS in future)
AGP Hot/Cool Egress Captured in Costs	Yes

Table 3: Cleanroom Recovery License Explanations

CLEANROOM RECOVERY VS CONTROL PLANE RECOVERY & VALIDATION

Commvault has another solution called Control Plane Recovery & Validation. While Control Plane Recovery & Validation is part of Cleanroom Recovery, it is also available as a standalone solution limited to provisioning the Control Plane for manual testing. This is not the same thing as Cleanroom Recovery as it does not include Recovery Group Automation and is limited to provisioning a hosted control plane with only manual ability to test/execute recoveries.



Competitive

No other vendor in the market has comprehensive any-to-any portability like Commvault. With the February 15th release, Commvault will begin with the most significant common denominator, VMware; in any location, Hyper-V, Azure VMs, and AWS EC2 will be available to recover into Azure. Other workloads will quickly follow as we walk through testing, beginning with File Systems, then MSSQL, and more.

KEY DIFFERENTIATION

Regardless of the data type or where it sits, we can recover it in Azure with Cleanroom Recovery. This ability allows clients to begin testing their Cyber Recovery plans. We will quickly branch out into the other cloud platforms as testing continues.

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 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. Understanding the difference between basic disaster recovery (DR) preparedness and being truly ready for malicious attacks is important. 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 about 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 of 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, for business continuity and data protection in the face of sophisticated attacks.

Main Competitors

• **Rubrik** – is aggressive with cyber recovery and data security and will say they can do the same thing as Commvault with a cleanroom. Rubrik requires a cloud cluster to facilitate its limited cross-platform restores. Their any-to-any cross-platform support matrix is far more limited than Commvault's supported matrix. Also, look for their cloud clusters to change soon as the cost and complexity of running them are prohibitive.



- Dell will lead with Cybervault coupled with Cybersense. At the surface, this is a compelling technology but does not have the same any-to-any capability we have and is built heavily on Data Domain. This high cost / high complexity solution is built on Data Domains and third-party software. Due to the cost and complexity, Dell only recommends that 10% of a client's environment resides in the Cybervault.
- **Cohesity** has story much like Rubrik's as they have the same challenges. Additionally, the recent announcement of their intent to acquire parts of Veritas calls into question their cloud readiness.
- Veeam will say they are hyper-resilient. The reality is that they offload all aspects of security onto the client. They still "require" Active Directory integration and still suffer from frequent high-profile exploits. Veeam has developed services to help clients accomplish this, but it is a new offering and a paid engagement. Additionally, without leveraging service providers, Veeam cannot provide the same experience we can with running the Control Plane in the Commvault Cloud. With the recent acquisition of Cirrus, Veeam can offer similar functionality but only for Office 365 and Azure.



Field 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**.

🕄 Commva	ult	EANOH	search serve	r groups, plan						G		CommvoultS	ystems inc 💌	- ~ ~
ashboard / Se Commva	curity posture sco ult System	= ns Inc - co	ommvai	ult										
Protecti	on Details					Reco	wery Validat	ion Test		Recovery Valid	lation De	tails		
	Last	Feb 27, 20 R backup uploo	024 Inded to cloue				Last reco	Feb 22, 2024 very validation uploaded to cloud		Recovery ⁻ 14 / 400	Test D	Man	ual Reter 0 / 400	ntion
													Expirati	on Jan 03
rotection Detai	le Recovery	Requests	Download H	latory										
rotection Detai	ls Recovery	Requests	Download H	istory .						0 -			10	
Add filter	le Recovery	Requests	Download H	latory .						¢ -			c	
Add filter CommCell ID	la Recovery 	Requests smCell Nome	Downfoad H	liatory Jule Nome	Full Jo	obs to Retain	DR Backup Met	adata Loc Upload to Network Pati	 Upload to Community 	C -	γ Log Files to	9 Backup	Stotus	
+ Add fitter CommCell ID	la Rocovery Cor	Requests smCell Name	Downfood H Scher DR Bc	listory Bule Name Ickup Full	Pull Ja B	obs to Retain	DR Bockup Met	addita Loc Upload to Network Pat LGR No	upload to Commun	C • • • • • • • • • • • • • • • • • • •	γ Log Files to None	o Bockup	Stotus Good	
C C C CommCell ID	le Recovery Cor	Requests ImCell Name	Downfood H Scher DR Be	Bule Nome	Fut Jo 5	obs to Retain	DR Bockup Met	odaha Lee Uglood to Network Pet SRF No	s Upload to Communa Vina	C Upload to Cloud Library None	y Log Files tr None	D Dackup	Btotus Good	
CommCell ID	le Recovery Cor	Requests nmCell Nome	Download H Scher DR Be	Bute Nome Schop Full	Fut Ja B	obs to Retain	DR Bookup Met Apticommond	addila Lav Uplicad la Network Poli No	1 Upload to Commun Vise	C + CA Upload to Cloud Library None Manually retain	y Log Files to None	9 Beckup	Btotus Good	
Add fitter Add fitter	le Recovery Cor	Requests nmCell Nome	Download H Scher DR Be	latory Bule Nome Jockup Full	Fuil Jo S	obe to Retain	DR Bockup Met	advite Lar Upstand its Natural Rad COR No	Upload to Commus Yes	C + Ch Uplead to Cloud Library None Manually retain C +	Y Log Files to None	b Backup	Stotus Geod	
Add filter Add filter Add filter Add filter Add filter	le Recovery Cor Backup Set	nmCell Name -	Download H Scher DR Br	Bule Nome Schup Full Backup Tim	Put Ja 5	obs to Retain	DR Bookup Met Jopticommund	adota La Upinad la Naturuk Put IOII No Monually Retained	u Upload to Commun Vea	C - Chu Uqelead to Cloud Library None Manually retain C - Advanced Units	y Log Files to None	CE QUID	Bitotus Good Compony I	Set Size S
Add filter Add filter Add filter IsGSRecon	Recovery Cor Bockup Set	Requests	Download H Scher DR Br Set ID 1975	Buckup Tim Pebruary 27	Puil Jo 5 4	obe to Retain	Dit Bookup Met Japtikommund Size 107 68	adota Las Uplicad to Notavark Pupt Cill No Manually Rotsand Q	u Upload to Commun Vea Ba	C uplood to Cloud Labor None Monually retain C -	y Log File to None Actions	cs guid saascr2e-t	Plotus Good Company I	Bet 5128 5 116036727
Add Riter Add Riter Add Riter IsCSRecov	Backup Set	nmCell Name	Download H Scher DR B Set ID 1875 1851	Bule Name schup Full Backup Tim Pebruary 27 February 26	Put Je 5 9 2024, 0811 AM 2024, 0811 AM	obe to Retain	Dit Bookup Met Aptitormmand Bize 107 GB	addia Lae Valicad la Natiwark Pati Colt No Monually Retained 0 0	Valicad to Common Ves D	A GA Uplied to Cloud Likerer Roce Monually retain Assived Unit	y Log Files to None Actiona	o Backup CS QUID 93ASCF2E-E 95OV0Y 2E-E	Bitotus Geod Company I	Set Size 5 116035727 114393473
CommCellin Detail CommCell ID C L+ Actd Riter LiCSRecon	Deckup Set SET_10 SET_10	nmGel Nome	Sicher Die Be Set 10 1975 1983	Bule Name Inde Name Indep Full Backup Tim February 27 February 28	Pull Ja 5 2024, 0811 AM 2024, 0811 AM 2024, 0810 AM	sba to Retain	Dil Backup Met Aptilionmiau Silae 107 08 107 08	adota Lan Uplicad la Naturak Pad Na Manually Batamad C C C	Ves Ves	A Ga Uplied to Cloud Librar None Manually retain () -	y Log Files to None Actions	CS GUID SAASCF2E-E SECONDY 2E-E SECONTY 2E-E	Btotus Good Company1	Bet \$120 8 115035727 114293473 115548904





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

						CommSe	Die Dessuiser Test							
							Ive Recovery lesc							
	ult Systems	Inc - com												
	ant oyotonin					You have 386	out of 400 recovery tests n	maining until your subscr	iption expires on					
	ion Details					January 03, 2	029, 07:00 PM (UTC -06:00			Recovery Valid	ation De	etails		
						Initiating a ne	w recovery requests will sto Each new recoverts will be	ige SET_112 on a commun	alt managed VM					
									and design					
		neb 27, 2024				Click submit t	is continue.						ual Reter	
									NOEL SUGMIT	14 / 400			0/400	
•										0.1				
•										0 -	8		12	
• + Add http:	x					-				0 -	8			
CommCall ID	a Come	nCeil Norne	Echedi	le Name	Full Jobs	s to Retain	DR Backup Metadeta Lo	Upload to hietwork Path	Upload to Commu	uit Ci-Upland to Cloud Librar	y Log Files t	te Backup	Stotus	
CommCall ID) Comm	nGeil Name	Echeda Dit Bac	Je Name	Pul Jobr	a to Retain	DR Bockup Metadata Lo	 Upload to Network Path No. 	Upload to Commus	uit Cis Upload to Dloud Literar	y Log Flies t	to Bockup	Btotus	
CommCall ID) Comm	rCell Name	Bchedu Dit Boo	le Norre Issp Full	Pull John	s to Retain	DR Backup Metodotis Lo Appl/common/DR	Upload to Network Path	Upload to Commut	uit Ch. Upleed to Cloud Literar None	y Log Files t None	10 Bookup	Btotus Good	
CommCell ID	a Comu	nCell Name	Echeda D# Box	le Name Isso Pull	Pul John	a to Retain	DR Backup Metadeta Lo Japi/comment/DR	Upleed to Network Path	Upload to Commus	UIT Ch. Upload to Cloud Librar None	y Log Files t None	to Beckup	Blotus Good	
CommColl IC) Comm	iCel Nome	Echeda Off Base	le Name Isip Full	Pull Jobr 5	s to Retain	DR Backup Metadeta Le Japi,kommetalitzik	Upload to Network Path No	Upload to Commus	Ult Cli Upleed to Cloud Libror None	y Log Files t None	to Backup	Biotus Good	
C Add Ittur CommCell ID	i Com	nOell Nome	Echoda Dit Bas	le Name Isup Full	Pull Jobs	s to Retain	Dil Bockup Metadeta Lo Appl/correnon.dlCill	Upload to Network Path	Upload to Commus	uit Cic Upleed to Cloud Libror None Monually retain (2) -	y Log Files t None	10 Bookup	Dtotus Good	
CommCall ID	e Com	vCell Nome	Beheda Dit Red	le Norme Ioup Fuil	Full-John	e to Retain	Dil Bookug Metadoria Lo Agit/communitàli	Upload to Network Path	Upload to Commu	C - uit Ci Upload to Oloud Libror Acres	y Log Files t None	10 Bockup	Btotus Good	
CommCell ID	Comm	NDell Nome	Beheda DR Ber	le Name kup Full	Full John	s to Retain	Dif Backug Metadoris Lo Japt/communitati	Upload to Network Path	Upload to Commun Yes	 Uplaced to Olaud Library None Mathematic Instance 	y Log Files 1 Nitrie	to Bockup	Btotus Good	
Acid Ritter Acid Ritter	Doma Dackup Set	iDell Nome	Echeda Dit Bad	le Name kup Full Backup Time	Full-John S	to Retain	DR Bookup Metadeta Le Asplicorenvoluticit	Upfood to Network Peth No.	Upload to Commun Yes	C - Upland to Cloud Library Atma Manually relation extended Until	y Log Filmst Hone Actions	to Backup C& GUID	Bioba Good Company (Bot Size
Add Riter	Convo Convo Danskup Set	VCell Nome	Echeda DR Boot	le Hame kug Full Baskup Time February 27 202	Full-Jobs 5	a to Rotoin	DR Bookup Metabelin La Agabarenveud/DR Bite 107-09	Galacia ta Network Peth No Manuathy BataIned O	Upload to Comme Yes	C - uit Ci: Uplowd to Cloud Library None None Monupath relation extensed Lined	Log Files 1 None Actions	e Beckup C& OUD SAASCHIE-E	Rtotus Good Company (Set Size
Add Pflar CommCell (D CommCell (D CommCell (D) L Add Pflar L CSRecov	Backup Set	NCell Nome	Echeda Dit find et D	le Hame kup Full Backup Time February 27 202	Pull-John 5	n tas Rantasian	Di Bockup Metadeta La Aquitorementali Bire sari ag	Galacet to Network Path No. Manually Rotatived 0	Upload to Commun Vise	the second	Log Files 1 None Actorn O	o Bookup CB OVID BAASCISE-E BAASCISE-E	Rhotus Good Company (Bet Bize 150357
Add Hase CommCell ID CommCell ID L Add Hase L Add Hase L CRecove	Comm Comm Disclup Set	nCell Nome	Rebeda DR Bost	le Hame Isap Full Backup Time February 23 202 February 26 202	Pull Jobe 5	n tas Raytasin	Dil Baskap Metadeta La Aglikoreneu.b[28] Bire Dio Gil	L. Splead to Memory, Public No. Manually Relatived C.	Upload to Commun Yes c c c	C + and Ch - Uplaned to Chool Alexen Nove Managely restore Alexender restore Alexend	Cog Files T None Actions	o Bookup CS OVID BAASCISE-E BAASCISE-E	Biotus Good Company (Sot Site 150357
Acid Hitse	Danskop Seit Danskop Seit Die Turke Die Turke Die Turke Die Turke Die Turke	NGel Morve	Schools Diff from the to r5 51 26	he Hame Isage Full Baskup Time February 27 202 February 26 202	Pull John 8 4, 0811 AM 4, 0810 AM	s to Retain	EM Bookup Meksiete La Arefvormes/dEM blas 107.00 107.00	Ciphod to Network PAD No Monuthy Retained 0 0 0	Uplead to Commu Year	C	Cog Files T None Actions Co	o Bookup CB OVID BAASCISE-E BAASCISE-E BAASCISE-E	Biotus Geod Company (Bet Site 19503572 19554600

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



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

Commve	JUIL	H Source Hilly	er groups, pians.					G		Commoult Sy	stems Inc. •	- ²⁰ - 100
ashboord / Si	ecurity posture score	c - commva	ult									
Protect	ion Details			Re	covery Validation T	est		Recovery Valido	ation D	etails		
	Fet Last DR back	o 27, 2024 up uploaded to clou ©			Feb Last recovery val	22, 2024 dation uploaded to cloud		Recovery To 14 / 400	est	Manu	al Reten 0 / 400	tion
rotection Deta	alla Recovery Reque	ata Download I	fistory								Expiratio	m Jan 03,:
-	- 4	1997 - C. B. (1999)	596965V									
•								Ø -				
+ Add filter												
CommCell ID	CommCell	Name Sche	dule Name	Full Jobs to Reta	in DR Backup Metadata Lo	Uplood to Network Path	Upload to Commvau	t Ck Upload to Cloud Library	Log Files	to Bookup	Status	
		DR 8	lackup Full		/opt/commvoultDR			None			Good	
•								Manually retain 👔 +			03	
+ Add filter	M I											
InCSRecove	Backup Set	Set ID	Backup Time		Size	Monually Retained	~	toined Until	Actions	CS GUID	Company I	Set Size B
			February 27 202	14, OB 11 AM	1.07 GB					93ASCF2E-E		1150357277
		1851	February 26 203	24, OB 09 AM	107 GB					93A5CF2E-E		114393473
										analyzer at		
		1826	February 25 202	24, 0810 AM	108 68					Bandur Dere		102003040
		1826	February 25 203	24, 0810 AM 24, 0808 AM	108 68					93A5CF2E-E		1153371884



Refreshing the page will show the Status of the recovery.

III	🕲 Commvault	SEARCH	Search server gro	sups, plans.						ଓ ⊞ ⊞	Commvault Systems	Inc • 🕺 Jo Gundiac
	Dashboard / Security p	osture score										
10	Commvault S	ystems Inc -	commvault									
	Protection D	etails			Recover	ry Validation Test			Recovery	alidation D	etails	
		Feb 27	, 2024			Feb 22, 2	2024		Recov	ery Test	Manual R	etention
		Last DR backup u	ploaded to cloud			Last recovery validation	uploaded to cloud		14	/ 400	0/4	00
											e	volution los 02 2020
	Protection Details	Recovery Requests	Download Histor									
			25 States (251, 10)	N								
	•								¢ -			
	+ Add filter											
	isCSRecoveryMana	Request ID	Backup SET	Requestor	Version	Stort	End	Quoto Used	Expiration	Status	VMID	Actions
				jo_gundlach@consensu	T.34	Feb 27, 2024 11:08:59 AM	Feb 27, 2024 11:09:06 /		Mor 03, 2024 11:08:59	Creating VM		
		2454		jo_gundlach@consensu		Feb 22, 2024 1019/10 AM	Feb 22, 2024 05:20.59		Feb 27, 2024 10 19:10 A	Finished, Removed B		
		2453		ja_gundlach@consensu		Feb 20, 2024 04:55:41 PM	Feb 21, 2024 02:46:08		Feb 25, 2024 04 55:41	Finished, Removed S		
		2452		jo_gundlach@consensu		Feb 20, 2024 02:28:46 PM	Feb 20, 2024 04:36:31		Feb 25, 2024 02:28:46	Finished, Removed B		
		2451		jo_gundloch@consensu		Feb 14, 2024 02:39:16 PM	Feb 20, 2024 12,54.13 /		Feb 19, 2024 02:3916 I	Finished, Removed S		
			SET_96	jo_gundlach@consensu		Feb 14, 2024 07:35:32 AM	Feb 14, 2024 01:36:56 (Feb 18, 2024 07:35:32 /	Finished, Removed B		
				jo_gundlach@consensu		Feb 09, 2024 12:39:39 PM	Feb 12, 2024 03:26:57 (Feb 14, 2024 12 39 39 1	Finished, Removed 9		
			SET_88	jo_gundlach@consensu		Feb 08, 2024 10:12:29 AM	Feb 08, 2024 12:04:25		Feb 13, 2024 10:12:29 A	Finished, Removed S		
				jo_gundlach@consensu		Feb 07, 2024 11:32:19 AM	Feb 08, 2024 08:31:59		Feb 12, 2024 11:32:19 A	Finished, Removed S		
	i	π	SET_77	jo_gundlach@consensu	11.34	Jan 29, 2024 12:4817 PM	Jon 29, 2024 0113 01 F	1	Feb 03, 2024 12:48:17 F	Finished, Removed S	iii	(A)

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

	Commvault	SEARCH	Search server gro	oupii, plans						6 ≣ ≣	Commvauit Systems	ne 🔹 _ 온 Jo Gundlach
a.	Dashboard / Security p	ostura acore										
10	Commvault S	ystems Inc -	commvault									
	Protection D	etails			Recovery	Validation Test			Recovery	/alidation De	etails	
0												
		Feb 27	, 2024			Feb 27, 2	024		Recov	ery Test	Manual R	etention
		Last DR backup i	ploaded to cloud			Last recovery validation	uploaded to cloud			400	0/4	00
												minution inc 09 2029
	Protection Details	Remains Personate	Download Mistor									
				·								
	•								o -			
	+ Add filter											
	IsCSRecoveryMana	Request ID	Backup SET	Requestor	Version	Blart	End	Queto Used	Expiration	Status	VM ID	Actions
		2455		jo_gundlach@consensu		Feb 27, 2024 11 08:59 AM	Feb 21, 2024 1139 59 A		Mar 03, 2024 1108.59	CS Stoped		
		2454		jo_gundlach@consensu		Feb 22, 2024 10/19/10 AM	Feb 22, 2024 05:20:59		Feb 27, 2024 10 19:10 A	Finished, Removed St		
		2453		ja_gundlach@consensu		Feb 20, 2024 04 55:41 PM	Feb 21, 2024 03:46:08		Feb 25, 2024 04:55:41	Finished, Removed St		
		2452		jo_gundlach@consensu		Feb 20, 2024 02:28:46 PM	Feb 20, 2024 04 36 31		Feb 25, 2024 02:28:46	Finished, Removed St		
		2451		jo_gundlach@consensu		Feb 14, 2024 02:39:16 PM	Feb 20, 2024 12:54:13 /		Feb 19, 2024 02:39:16 (Finished, Removed St		
			517_95	jo_gundlach@consensu		Feb 14, 2024 07:35:32 AM	Feb 14, 2024 01:36:56 (Feb 19, 2024 07:35:32	Finished, Removed SI		
			SET_90	jo_gundlach@consensu		Feb 08, 2024 12:39:39 PM	Feb 12, 2024 03:26:57 (Feb 14, 2024 12:39:39 I	Finished, Removed SI		
			SET_88	jo_gundlach@consensu		Feb 08, 2024 10/12/29 AM	Feb 08 2024 12:04:25		Feb 13, 2024 10:12:29 A	Finished, Removed St		
			SET_87	jo_gundiach@consensu		Feb 07, 2024 1132:19 AM	Feb 08, 2024 08:3159		Feb 12, 2024 11:32:19 A	Finished, Removed St		
		17	SET_77	jo,gundlach@consensu	134	Jan 29, 2024 12:4817 PM	Jan 29, 2024 (113 (1 F		Feb 03, 2024 12:48:17	Finished, Removed St		0







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

=	Commvault	SEARCH	Search server gr	oups, plans						& ⊞ ⊟	Commvoult Systems	inc 👻 🤱 Jo Gundlach
	Dashboard / Security	posture score Systems Inc -	- commvault									
	Protection	Details			Recover	y Validation Test			Recovery	Validation D	etails	
		Feb 2 Last DR backup	7, 2024 uploaded to cloud			Feb 27, 2 Last recovery validation	1024 uploaded to cloud		Recov 15	very Test / 400	Manual F 0 / •	Retention 400
												Expiration Jan 03, 2029
	Protection Details	Recovery Requests	Download Histo									
	•								Q -		é	
	+ Add filter											
	IsCSRecoveryMana	Request ID	Backup SET	Requestor	Version	Stort	End	Quota Used	Expiration	Status	VMID	Actions
		2455		ja_gundisch@consensu		Feb 27, 2024 11:08:59 AM	Feb 27, 2024 11 39 59 /		Mar 03, 2024 11.08.59	CS Stoged		
		2454		ja_gundiach@consensu		Feb 22, 2024 10:19:10 AM	Feb 22, 2024 05:20:59		Feb 27, 2024 10:19:10 A	Finished, Removed B		Extend Reservation
		2453		ja_gundlach@consensu		Feb 20, 2024 04 55:41 PM	Feb 21, 2024 03:46:08		Feb 25, 2024 04:55:41	Finished, Removed B		
		2482		jo_gundisch@consensu		Feb 20, 2024 02:28:46 PM	Feb 20, 2024 04 98 31		Feb 25, 2024 02:28:46	Finished, Removed B		
		2451	567,97	jo_gundlach@consensu		Feb 14, 2024 02:39:16 PM	Feb 20, 2024 12:54 13		Feb 18, 2024 02:39:16 1	Finished, Removed B		
			SET_95	ja_gundlach@consensu		Feb 14, 2024 07:35:32 AM	Feb 14, 2024 013656		Feb 18, 2024 07:35:32	Finished, Removed B		
			SET_90	ja_gundiach@consensu		Feb 09, 2024 12:39:39 PM	Feb 12, 2024 03 26 57		Feb 14, 2024 12:39:39 (Finished, Removed S		
			SET_88	ja_gundiach@consensu		Feb 08, 2024 1012-29 AM	Feb 08, 2024 12:04:25		Feb 13, 2024 10 12:29 A	Finished, Removed S		
			SET_87	jo_gundiach@consensu		Feb 07, 2024 11:32:19 AM	Feb 08, 2024 08.3159		Feb 12, 2024 11:32:19 A	Finished, Removed S		
			SET.77	io gundiach@consensu	T.34	Jon 29, 2024 12:4817 PM	Jan 29, 2024 0113,011		Feb 03, 2024 12:48:17 F	Finished, Removed 9		



The Access Details window appears with all the information needed to access the new instance.

				Access de	etails						
ainboard / fleourityp	ortura acore										
ommvault s	ystems inc -	- commvau		URL:			Ē				
										etails	
				Uter recoveryman	ager		D				
	Feb 2	7, 2024									
					N.	CANCE	PERPEN				
					\$						
	Recovery Requests										
A ALCOHOLD						_					
+ And Miles IeCBRecoveryMone	Request ID	Bockup SET	Requestor	Version	Start	End .	Quota Used	Expiration	Diotus	VM ID	Actions
+ Aug Mine IeOSRecoveryMand	Request ID 2455	Bockup SET SET_70	Requestor Jo.gundiach@consensu	Version TL34	SRart Feb 27, 2024 11:08:59 AM	End Feb 21 2024 112959 A	Quote Used	Expiration Mor 03, 2024 TLOB.59	Btotus CS Btoged	VMID	Actions
4 And Mee IsCBRecoveryMand 1	Request ID 2455 2454	Bookup SET SET_70 SET_107	Requestor Jo.gundlach@consensu Jo.gundlach@consensu	Version 17.54	Shart Feb 27, 2024 11:08:58 AM Feb 22, 2024 10:18:50 AM	End Feb 21 2024 1139 59 J Feb 22, 2024 05:20 59	Quoto Used 1	Expiration Mor 03, 2024 11:08:59 Peb 27, 2024 10:1910 A	Stotus CS Stoged Finished, Removed S	VM ID	Actions ©
+ and title GBRecoveryMand 1 1	Request ID 2455 2454 2453	Bockup SET SET_TO RET_TO SET_TO	Requestor 30.gundlach@consensu 30.gundlach@consensu jo.gundlach@consensu	Version 11.34 11.34	Stort Feb 22, 2024 1108 58 AM Feb 22, 2024 10 19 10 AM Feb 22, 2024 04 656 48 PM	End Feb 22 2024 1139 59 A Feb 22, 2024 05:20 59 Feb 25, 2024 05:20 59	Quota Used 1 1	Expiration Mor 03, 2024 110859 Feb 25, 2024 50 1910 A Feb 25, 2024 04 (5)-61	Btotus CS Bloged Finished, Removed S Finished, Removed S		Actions C
+ Aud Maar MCBRecoveryMone 1 1 1	Request 10 2405 2403 2403 2403	Bockup SET SET_702 SET_703 SET_703 SET_703	Requestor ja, gundlach@consensu ja, gundlach@consensu ja, gundlach@consensu ja, gundlach@consensu	Vension 11,34 11,34 11,34	Start Fels 23, 2024 11:08:59 AM Fels 23, 2024 11:08:39 AM Fels 22, 2024 12:08:39 AM Fels 20, 2024 G4:65:41 FM	End Feb 22, 2024 03,40,60 Feb 22, 2024 03,40,60 Feb 22, 2024 03,40,60 Feb 26, 2024 03,40,60 Feb 26, 2024 04,40,61 Feb 20, 2024 04,40,40 Feb 20, 2024 04,40,40 Feb 20, 2024 04,40,40 Feb 20, 2024 04,400 Feb 20,400 Feb 20,40	Quota Used 1 1 1	Expiration Mor 03, 2024 1108.69 Feb 27, 2024 50 1910 A Feb 25, 2024 04 558 41 Feb 26, 2024 02-28-46	Blotus CS Bloged Finished, Removed S Finished, Removed S	VMID 1	Actions
+ Aud Ittus Is/OBRecoveryMana 1 1 1 1	Request ID 2405 2404 2403 2403 2403 2403	Bockup SET SET_107 SET_107 SET_103 SET_103 SET_103	Requestor ja,gundischijdoniensu ja,gundischijdoniensu ja,gundischijdoniensu ja,gundischijdoniensu ja,gundischijdoniensu	Version 1234 1234 1234 1234 1234	Shart Peb 22, 2024 100838 AAA Peb 22, 2024 101830 AAA Peb 20, 2024 101830 AAA Peb 20, 2024 0238 AB Pek Peb 20, 2024 0238 AB Pek Feb 30, 2024 0238 AB Pek	End Pels 21,0004 1129/09 # Pels 22,2004 08/2018 Pels 20,2004 04/36/09 Pels 20,2004 04/36/31 Pels 20,2004 04/36/31	Quote Used 1 1 1 1	Expiration Mor 03, 2024 1108.69 Feb 25, 2024 04,05.41 Feb 25, 2024 04,05.41 Feb 25, 2024 04,05.41 Feb 25, 2024 04,02.3146 1	Blobus CS Stoped Finished, Removed S Finished, Removed S Finished, Removed S	VMID R R R R	Actions C C C C C C C C C C C C C C C C C C C
+ Add Blac IsOBRecoveryMone 1 1 1 1 1 1 1	Request ED 2465 2463 2463 2462 2463 2463 2463 2463 2463	Bockup SET BET_172 BET_173 BET_103 BET_103 BET_07 BET_05 BET_06	Requestor Jo, gundlach@consensu Jo, gundlach@consensu Jo, gundlach@consensu Jo, gundlach@consensu Jo, gundlach@consensu Jo, gundlach@consensu	Version 11.34 11.34 11.34 11.34 11.34 11.34	Shart Pelo 22,0004 100838 AAA Pelo 22,0004 100840 AAA Pelo 20,0004 00450.61 PM Pelo 20,0004 02,30 AB PM Pelo 30,0004 02,30 AB PM Pelo 30,0004 02,30 AB PM	End Peb 21, 2024 11,2669 4 Peb 21, 2024 11,2669 4 Peb 22, 2024 04,2058 9 Peb 21, 2024 04,368 9 Peb 20, 2024 04,368 9 Peb 20, 2024 04,368 9 Peb 20, 2024 01,368 9	Quarter Used	Expiration Mor 03, 3034 11/08/99 Feb 37, 3034 10/08/99 Feb 38, 2034 04/86/41 Feb 38, 2034 02/28/46 Feb 18, 2034 02/28/46 Feb 18, 2034 02/28/46	Stotus CS Shoped Finished, Removed S Finished, Removed S Finished, Removed S Finished, Removed S		Actions
+ Add Han InGBRacowryMone 1 1 1 1 1 1 1 1 1	Request ID 2455 2453 2453 2452 2452 2452 2452 2452	Bookup BET BET_170 BET_107 BET_103 BET_103 BET_105 BET_105 BET_205 BET_205	Requestor Jr.,quantischijitonsenu Jr.,quantischijitonsenu Jr.,quantischijitonsenu Jr.,quantischijitonsenu Jr.,quantischijitonsenu Jr.,quantischijitonsenu	Version 12-34 12-34 12-34 12-34 12-34 12-34	Start Peb 22, 2024 100838 AAA Peb 22, 2024 100839 AAA Peb 23, 2024 00450-61 Pea Peb 24, 2024 02,30 AB Pea Peb 24, 2024 02,30 AB Pea Peb 24, 2024 02,30 AB Pea	End Feb 22, 2024 15/868 4 Feb 22, 2024 15/868 4 Feb 22, 2024 05/868 6 Feb 22, 2024 05/868 6 Feb 20, 2024 05/868 1 Feb 20, 2024 05/868 1 Feb 30, 2024 05/868 1	Quote Used 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	Exploration Alor 03, 2024 110869 Feb 27, 2024 101950 A Feb 25, 2024 40.1950 A Feb 25, 2024 40.485441 Feb 35, 2024 40.2954 67.2954 Feb 18, 2024 40.2958 B Feb 34, 2024 40.3958 B	Blotus CS Stoped Finished, Removed S Finished, Removed S Finished, Removed S Finished, Removed S Finished, Removed S	VMID 1 1 1 1 1	Actions C C C C C C C C C C C C C C C C C C C
+ add Bar BRooverskinne 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Request ID 2455 2453 2453 2452 2452 2453 2453 2453	Bookup BET BET_170 BET_100 BET_100 BET_103 BET_07 BET_85 BET_360 BET_38	Repartor Ja. gundisch Georeanus Ja. gundisch Georeanus	Version 154 154 154 154 154 154 154 154 154	Bitard Peb 20, 0004 1108 69 AM Peb 20, 0004 1108 69 AM Peb 20, 0004 100 80 AM Peb 20, 0004 00 28 AB	End	Quoto Used 1 1 1 1 1 1 1 1 1 1 1 1 1	Exploration Alor 03, 2024 110869 Feb 27, 2024 101859 Feb 27, 2024 40 1910 A Feb 27, 2024 40 486 47 Feb 28, 2024 40 286 47 Feb 18, 2024 40 2916 1 Feb 18, 2024 40 2916 1 Feb 18, 2024 40 2918 10 1	Blotus CS Bloged Finished, Removed 8 Finished, Removed 9 Finished, Removed 9 Finished, Removed 9 Finished, Removed 9	VMID 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	
+ Add Bar BRooveryMond 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Киерьник ID 2466 2460 2460 2460 2460 2460 2460 2460	Bookup SET RET_107 RET_107 RET_103 RET_103 RET_90 RET_90 SET_97 SET_97	Reguester J. Question/Question J. Question	Version 124 124 124 124 124 124 124 124 124	Start Real 21, 2024 10 06 50 AM Real 22, 2024 10 06 50 AM Real 22, 2024 00 06 50 AM Real 22, 2024 00 06 50 AM Real 20, 2024 00 06 20 AM Real 42, 2024 00 20 20 AM	End	Queta Used 1 1 1 1 1 1 1 1 1 1 1 1 1	Exploration New 00, 0004 1108.99 Feb 27, 0004 101910 A Feb 25, 0004 001910 A Feb 25, 0004 00286-66 Feb 10, 0004 00286-66 Feb 10, 0004 00286-66 Feb 10, 0004 00286-86 Feb 10, 0004 00286-86 Feb 10, 0004 00286-86 Feb 10, 0004 00286-86	Biotus Citi Bioged Finished, Removed 8 Finished, Removed 9 Finished, Removed 9 Finished, Removed 9 Finished, Removed 9 Finished, Removed 9	VM ID	

MAKE SURE YOUR AZURE TARGET IS SET UP

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

The Azure target must have the following:

- 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 EntralD
- 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.OperationalInsights
 - h. microsoft.Network

🗊 Commvaulť



- i. microsoft.MarketplaceOrdering
- j. microsoft.MarketplaceNotfications
- k. microsoft.MachineLearning
- I. 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.

International Owner Windustain Auto resourcy Company Endpoint Data brights Select statubated Brancet Company Frider and participants Company Endpoint Data brights Needs attention Protect Frider and participants Company VMail Laptops Users Needs attention Company Frider and participants Company VMail Laptops Users Servers Jobs Company Servers VMail Laptops Users Servers Jobs O Auto recovery Servers Users Servers Jobs in the last 24 hours Participants Events Servers Servers Company Events Company Events 2 Mense Recovery Frider and participants Company Events 2 Servers Servers Company Participants Events Servers West Recovery Frider and participants Frider and participants Events Servers Mense Recovery Frider and participants Frider and participants Frider and participants Mense Recovery Frider and participants Frider and participants Frider and participants Frider and participan	≡ Commvault	Q Search or type / for a comman	d						6 0 a B 4	I recoverymanager •
 I beskedielity I beskedielity I beske hunders <lii besk<="" td=""><td>Filter navigation</td><td>Overview Virtualization</td><td>Auto recovery</td><td>Company</td><td>Endpoint</td><td>Data Insights</td><td></td><td></td><td></td><td>Select dashboard 👻</td></lii>	Filter navigation	Overview Virtualization	Auto recovery	Company	Endpoint	Data Insights				Select dashboard 👻
 Protect Dotas Insights Cherronnent File servers Velse Addressonen Addressonen Addressonen Addressonen Addressonen SLA Subas Insights Bismage Montaring Bismage Montaring Bismage Montaring Bismage Montaring Bismage Montaring Wet went Wet went Wet went Wet went Montaring Bismage <li< td=""><td>2 Dashboard</td><td>Company</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></li<>	2 Dashboard	Company								
 Addresservery Johs Banges Monitaring Banges Manges Westrikes 	 Protect Data Insights Cleanroom 	Environment File servers 2	Environment File servers VMs Laptops Users 2 15 0 5					Needs attention Servers Jobs 3 O		
Web console Last week job summary 0 Web console 0 100<	 Auto recovery Jobs Reports Manitoring Storage Manoge Workflows Web console 	SLA Jobs in the last 24 h					Success O Ovy-30 Wees-19	CWE/CWW O Cory • 0 Week • 0	e Failed 2 Day+2 Week+2	Events 2
Robury 22 - Nobury 27 © Complexed M3		Last week job summary				Top 5 largest s	No d	ata available.		





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.

\Xi 🎼 Commvault	Q Search or type /	/ for a command			🕓 🕐 🖻 🐻 🗘 📰 💄 recoveryman	nager 🔻
Filter navigation_	Hypervisors /					
🖆 Dashboard		- C				
C Protect	Co	nfigure Hypervisor				
🕏 Data Insights			Sel	ect vendor		
a Cleanroom						
Auto recovery		O Amazon Web Services	Microsoft Azure	Google Cloud Platform	O Nutanix AHV	
🚔 Jobs		aws			×.	
Reports					~	
Monitoring						
Storage		O Microsoft Hyper-V	O VMware vCenter	Alibaba Cloud	O Microsoft Azure Stack Hub	
董 Manage			l l l l l l l l l l l l l l l l l l l	C		
Workflows						
C Web console		OpenStack	Oracle Cloud Infrastructure		Red Hat Virtualization	
		VMware Cloud Director	⊖ Xen	Fusion Compute		
	CANC	EL			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.

r navigation	Comparison of the Company			
Dashboard Protect	Configure Microso	oft Azure Hypervisor		
Virtualization	Add Hypervisor	Add Hypervi	isor	
ubernetes ile servers	2 Add VM Group	Hypersisor name * Cleannoom Hypervisor		
latabases	3 Summary	Connect using managed identities for Azure resources _))		
Contractions		Subsorigion ID*	h	
Exchange		Credential* Select a saved credential	- + 0 C	
DevOps Data Insights		Access notes Click to select		
lleanroom		EQUIVALENT AP		
Jobs				
eports		CANCEL		NEXT
onitoring				
lanage				
Vorkflows				

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.

Vivalization Kademates Kademates File servers Outsoon Convent using monogeal destifies for Asses resources Convent using monogeal destifies for Asses resources Convent using monogeal destifies for Asses resources Convent Convent using monogeal destifies for Asses resources Convent Conv	Protect	Configure Microsoft A	zure Hypervisor		
Lapites Lapites Carter See Constrained Carter	Virtualization Kubernetes File servers Databases	Add Hypervisor Add VM Group Bummary	Add Hypervisor repervisor norm,* Cleannoom Hypervisor Connect using managed identities for Asure resources _ (8)		
Ato recovery EQUIVALENT AP	Laptops Office 385 Exchange DevOps Data Insights Cleanroom		Ruberspress 0 * Onsidentia* Select a superior and endertital Access notice Click to wellect	- to c	
	Auto recovery Jobs Reports Monitoring	CANC	EQUIVILINT AN		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**.

	earch or type / for a command			G Q E BUREI.	recoverymanager •
Filter novigation. Hyper	visors /				
2 Dashboard		Add credential	× .		
	Configure Microsoft Azure H				
O Protect		Assount type * Cloud Account			
Virtualization	Add Hypervisor				
Kubernetes		Vandlar type			
File servers	2 Add VM Group	SUCCESSION STREET			
Databases	3 Summary	Authoritization Figure *			
		INM AD Approxision	· ·		
Laptops		Credential Voult			
Office 365		BOLIJN	•		
Exchange		Credential name*		2 A 10 C	
DevOpe		Cleanroom Application			
Data Insights		Tenget (0 *			
6. minutes					
a Cleanroom		Application ID *			
Auto recovery					
Jobs		Application secret *			
G Reports	CANCEL				4DCT
-		Environment*			
Monitoring					
Storage		Show endpoints _ IB			
1 Manage		Description			
The second second					
- Workhows		The second se			
C Web console		EQUIVALENT API	CANDEL SAVE		
			W		

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

😑 🏽 Commvault	${\bf Q}_{\rm c}$ Search or type / for a command				0 1 1	3 🗘 📰 🛓 recoverymanager •
Filter novigation	Hypervisors /					
12 Dashboard		0	- 6 A 11 1-			
C Protect		Configure Micros	ort Azure Hypervis	br		
Virtualization		Add the ansists		Add Hypervisor		
Kubernetes		and refer that		Hypernikor nome *		
File servers		2 Add VM Group		Cleanroom Target Hypervisor		
Databases		3 Summary		Connect using managed identities for Azura resources		
Laptops				Subscription D*		
Office 365				5/13/65/0		
Exchange				CleanroomTargetApplication + / C		
DevOps				Access nodes		
Data insights				Automatic 10 *		
 Auto recovery 				Automatic		
Jobs				Access nodes		
(a) Reports			CANCEL	□ scr2-8	NET	
Monitoring			Concer	Access node groups	NEX.	
Storage				hfrostructure		
II Manage				Lob vCenter		
Workflows				Media Agents		
SU Web console						





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

≡ 🕲 Commvault	Q Search or type / for a command				6 0 B 6	📰 🛓 recoverymanager •
Filter navigation.	Overview Virtual machines	Hypervisors VM groups				dd hypervisor Add VM group
12 Dashboard	Hypervisors				Q	C HI I
Virtualization	All					٥
Kubernetes	Vendor + Ald filter					
File servers	Nome T	Vendor	Version	Configured	Togs	Actions
Databases	Cleanroom Hypervisor	Microsoft Azure	Not Applicable	-	No tage	
Laptops	Cap voenter	VMwore vCenter	VMedre vCenter Server 8.0.2 build-22385/38	~	No taga	
Office 365						
Exchange						
DevOps						
🕏 Data Insights						
🔓 Cleanroom						
Auto recovery						
Jobs	h	1				
@ Reports						
Monitoring						
Storage						
E Manage						
Workflows						
Web console						
-						

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

≡ Commvault	Q Search or type / for a command			6 0 B B 4	E 1 recoverymanager •
Filter navigation.	Targets			Utita of	с ш і
🖄 Dashboard	All				0
C Protect	+ Add filter				
Data Insights	Name †	Vendor	Application type	Destination hypervisor	Actions
Eleanroom			No data available		
Recovery groups					
Torgets					
 Auto recovery 					
Jobs					
@ Reports					
Monitoring					
Storage					
(E Manage					
Workflows					
C Web console					

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.

🗏 厳 Commvault	Q Search or type / for a command				6 0 E	80 II	L recoverymanager +
Filter navigation	Targets Add Microsoft Azure targe	t					
Protect Costs finajols Costs finajols Costs finajols Costs finajols Costs finajols Records Costs Co	Destruction Options		targat name * <u>Checrotom</u> Target Cleannoum Hypervision WM display name CRB Accords Accords Accords Becurity resource	General Ute ariginal name Add a prifit to the VM name Add a suffit to the VM name	•		
Web console		CANCEL					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.

	Toopato		
er navigation			
Dashboard	Add Microsoft Azure target		
Protect			
Data Insights	🕑 General	Destination Options	
1222010000000		Resource group 4	
Cleanroom	2 Destination Options	CleanroomGroup	
Recovery groups		Basico 1	
Targets		Central US	
the second			
Auto recovery		Disrige Account*	
adot		cleanroomstorageaccount	
Reports			
		Auto Select	
Monitoring			
Storage		Availability 2019	
		Auto	
montige		Disk type	
Workflows		Original	
Web console		With out and and	
		192-Network(192-Subnet ()	
		Benurity proup	
		Create public IP 📹	
		Nordona Sana Sana Sana Cina	
	CANCEL		TREVIOUS SUBME





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.

	Search or type / for a command					I recoverymanager •
Filter navigation	Recovery groups				ARE Q	c 🖩 :
E Dashboard	All				Ciii	•
C Protect						*
🕏 Data Insights	+ Add mar					
S Cleanroom	Name 1	rarger		Defourt recovery point		Actions
Recovery groups			No data available			
Tasaata						
e talgeta						
A. Write Lecovery						
Jobs						
@ Reports						
Monitoring						
Storage						
註 Manage						
Workflows						
 Web console 						
ap neb console						

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.

🗏 🌒 Commvault	Q Search or type / for a command			Ğ	0	國介間一	1 recoverymanager +
Filter novigation.	Recovery groups Add recovery group						
B Protect		Resovery group name * Cleansoon Recovery Group					
Cleanroom		Target " Cleanroom Target		• + (2		
Recovery groups Targets		Default recovery paint * Automatic					
 Auto recovery Jobs 		EQUIVALENT API		CANCEL SAV	Am		
 Reports Monitoring 					0		
Storage							
Workflows							
C Web console							

The Recovery group has been created.

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

Interesting Interesting </th <th>= Commvault</th> <th>Search or type / for a command</th> <th></th> <th></th> <th></th> <th></th> <th>C ③ 国 關立 間 </th> <th>1 recoverymanager</th>	= Commvault	Search or type / for a command					C ③ 国 關立 間	1 recoverymanager
Banbard	Filter navigation	Recovery groups						
In state to the second of the secon	2 Dashboard	Cleanroom Recovery Gro	oup					Recover of Delete
	 Protect Data Insights 						Add = Q	с ш і
Network print	S Cleanroom	All					Virtual repolitions	0
Image Image Image Recomposition Validation station Private Recomposition Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image <t< td=""><td>Recovery groups</td><td>+ Add filter</td><td></td><td></td><td></td><td></td><td>w and the second second</td><td></td></t<>	Recovery groups	+ Add filter					w and the second	
Autorecovery Note constraints Autor generation Autor generation Interview Interview	Targets	A O Name 1	T Porent	Server	Recovery status	Validation status	Priority Recovery point	Actions
 Joha Bandar Bandar Bandar Bandar Bandar Mangar Wathard Wathar	Auto recovery				No data available			
 Paparts Montaring Barraga Montaga Workfrees Work sensels 	dots 💼							
 Mantang Storage Mantang Wathows Wathows 	@ Reports							
 Storage Managa Wotfors ♥ Web console 	Manitaring							
A Manage Wurkfiews ● Web consule	Storage							
♥ Workflows ♥ Web console	1 Manage							
Web console	Workflows							
	Web console							



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

≡ € Commvault	Q Search or type / for a command		ى ئ	🛙 🗟 🗘 🔛 ք recoverymanager +
Filter navigation,.	Recovery group details			
2 Dashboard	Add entity			
B Protect		Browse and select VMs		
🕏 Data Insights		By hypervisor	<u> </u>	
Scleanroom		• Show selected Q, Search		
Recovery groups		•		
Torgets		Coo Air Gop Protect VMs		
Auto recovery		OR RHEL Client DHCP		
Jobs		Bosticket		
Reports		B LiveSync CS1 (Foundation)		
Manitoring		B bookstock		
Storage				
莊 Manage		a dnat		
Workflows				
C Web console		EQUIVALENT API	CANCEL 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.

2 Dashboard	Cleanroom Recovery Gr Entities Configuration Jobs	roup							Vegover all Delete
Protect Data Insights							Add + Q		c III 3
S Cleanroom	All								\$
Recovery groups	+ Add filter								
Torgeta	V D Nome 1	τ	Parent	Server	Recovery stotus	Validation status	Priority	Recovery point	Actions
Auto recovery	✓ 🔲 dnat	V	Air Gop Protect VMs	dnatCRR	Ready.	None		Automotic	
Jobs	V 🗍 RHEL Client DHCP	V	Air Gop Protect VMa	RHELCIentDHCPCRR	Ready.	None	1	Automatic	-
 Blorage Manage Warkflows Web console 									





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**.

🗮 🎼 Commvault	Q Search or type / for a command								୯ ତ		1 recoverymanager •
Filter novigation.	Recovery groups Cleanroom Recovery Group Entities Configuration Jobs	Recover entities					×	1			Rever of Delete
Data Insights		Override entities that are	already rec	covered and					Add + Q		C III
Cleanroom		A ANTINA .					сш				٥
Recovery groups	+ Addition	Name 1	Ŧ	Recovery status	Priority	Recovery point		-	and the second	Bernard	Artises
Auto recovery	v daat	dnst	v	Ready	3	Automatic			1	Automatic	
💼 Jobs	V RHEL Clent DHCP	RHEL Client DHCP	V	Ready.	1	Automatic			3	Automatic	
@ Reports		EQUIVALENT AD				CANCE	CLIDLAT				
Monitoring		EQUINEERI ANI	-	_	_		L. BODINIT				
Storage											
📰 Manage											
Workflows											
S Web console											

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.

fully - JobiD : 35522
c m
5
Actions
Θ
9
0



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.

≡ Commvaulť	Q Search or type / for a command					୯ ଓ		1 recoverymanoger +
Filter navigation	Recovery groups							
it Dashboard	Cleanroom Recovery Gr	roup						Recover all Delete
B Protect	Entries Connguration Jobs							
🕏 Data Insights						Add + Q		C III i
Seanroom	All							0
Recovery groups	+ Add fillar							2
Targets	Nome 1	T Parent	Server	Recovery status	Validation status	Priority	Recovery point	Actions
Auto recovery	v L deal	V_ Air Gop Protect VMs	dra1CRR	Recovered	None	1	Automatic	
💼 Jobs	RHEL Client DHCP	V. Air Gop Protect VMs	RHELCIentDHCPCRR	Recovered	None	1.	Automatic	
@ Reports								
Monitoring								
Storoge								
🔨 Manage								
Workflows								
C Web console								

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

Virtual machines 👒										×
CWroductReadiness		k		and the second second						
+ Create V 27 Switch to classic U Reservato	ons 🗢 🥹 Manage view 🛇	Refresh 👱 Export to	CSV 15 Open query	O Aergn tags (22 Star	t 🥄 Restart 🛄 Stop	E Detata III Services V 🖉	Mantenance V			
Filter for any field. Subscription equals all	Type equals all	Resource group equals all $ imes$	Location equals all \times	Ty Add filter						
Showing 1 to 2 of 2 records.								No grouping	✓ III List view	\sim
Name T.	Туре то	Subscription $ \hat{\tau}_{\hat{\omega}} $	Resource group To	Location 7.	Status 14	Operating system \uparrow_{\downarrow}	Size 14	Public IP address $\uparrow_{\dot{\psi}}$	Disks †4	
🔲 🐺 dms1CRR	Virtual machine	Product Readiness	deanroomgroup	Central US	Running	Windows	Standard_D16a_v4	40.122.38.85	1	
	Virtual machine	Product Readiness	deanroomgroup	Central US	Running	Linux	Standard_D16a_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.

Frequently Asked Questions

What is Cleanroom as a Service?

Commvault does not currently offer Cleanroom as a Service, and this term should not be used. Currently, Commvault has a Cleanroom Recovery solution that helps automate a client's environment recovery.

Is it automated for recovery?

Yes, recovery of the control plane (CommServe) and servers defined in the recovery groups is automated once the destination tenant has been fully configured and presented to Commvault.

Can we automate Entra ID (Azure AD) or AD in general?

Entra ID (Azure AD) or AD recovery is not automated. It is recommended that a clean Entra ID or classic AD environment be created free from any anomalies.

Whose tenant is it in?

The control plane (CommServe) is recovered in Commvault's SaaS environment, and the client's servers are recovered to an Azure tenant that they provide.





How is it paid for today and tomorrow (if known)?

The client will pay for their own Azure subscription to restore and the costs associated with the cloud environment. Cleanroom Recovery covers the cost of recovering and running the Control Plane into the Commvault cloud and the egress costs for recovering data out of Air Gap Protect.

What does the customer need to purchase?

The client will need Commvault Foundation, Air Gap Protect, and Cleanroom Recovery.

Does Cleanroom Recovery work with replication?

Cleanroom Recovery is designed with the idea that a client is recovering from a cyber event. In these events, it is best to recover from a secured air gap copy of backups and not leverage replication since replication will also be open to compromise.

How often should data be kept in Air Gap Protect/ How long should the data be retained?

How often and long data is kept in Air Gap Protect should be driven by business legal and regulatory requirements. A strong recommendation is that the copy of data in Air Gap Protect be equal to backup retentions. Cleanroom Recovery is not designed for long-term archives and cannot be used as such. Cleanroom Recovery is intended to get the business back from a cyber-event.

How often should Fulls be copied to Air Gap Protect for Cleanroom Recovery?

Fulls and incremental should follow the backup policies. At least one full is required to be in Air Gap Protect, but careful consideration should be taken when designing the Full/Incremental cycle, as this can impact the amount of data stored. The general recommendation is to have one full pure retention cycle (e.g., if we are keeping 14 days, the recommendation is to have a full/syn full every 14 days at minimum). This is industry backup best practice and not specific to Cleanroom Recovery.

Can Cleanroom Recovery be utilized with Air Gap Protect cool?

Yes, Cleanroom Recovery can be used with Air Gap Protect cool.

What recovery time can clients achieve with Cleanroom Recovery?

We need to stop thinking about standard disaster recovery concepts for recovery time. Most of the time, a cyber recovery is consumed outside of data recovery. This is why we promote testing so heavily with Cleanroom Recovery; the more a client tests and practices, the quicker they will be in an actual cyber recovery. In terms of the speed of recovering data, Cleanroom Recovery auto-scales the restores and utilizes the Microsoft main backbone to scale to the needs of the recovery.

To learn more, visit the Cleanroom Recovery Partner Resource Page on the Partner Portal.

To learn more, visit commvault.com



commvault.com | 888.746.3849

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