

# Ransomware Defense Strategy with HDPS and AWS Immutability

Using Hitachi Cloud Connect for Equinix

Hitachi Vantara March 2024

# Table of **Contents**

Notices and Disclaimer	2
About This Guide	3
Intended Audience	
Value Proposition	3
Document Revisions	
References	
Comments	4
Executive Summary	5
Introduction	6
Solution Overview	7
Business Benefits	7
Objective	7
Key Components	7
Validation	8
Validation Method	
High Level Diagram	8
Hardware and Software	9
Test Scenarios	
Validation Results	11
Test 1: Prepare the Environment	
Test 2: Install and Configure HDPS	
Test 3: Secure and Harden the Components	
Test 4: Simulate Ransomware Infection and Recovery	
Conclusion	

# **Notices and Disclaimer**

© 2024 Hitachi Vantara LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara (collectively, "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability or contact Hitachi Vantara at https://support.HitachiVantara.com/en\_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara.

By using this software, you agree that you are responsible for:

1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and

2) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls: The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

EXPORT CONTROLS: Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Hitachi is a registered trademark of Hitachi, Ltd., In the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, Flash Copy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, BCPii<sup>™</sup> and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screenshots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or web site are properties of their respective owners.

# **About This Guide**

This guide describes:

- Deploying a multi-layered ransomware protection and recovery solution.
- Tightening the security of an end-to-end data landscape through:
  - Security assessments.
  - Implementing Operating System (OS) hardening based on Center for Internet Security (CIS) level 1 best practices.
  - Implementing air gapping and data isolation.
  - Leveraging the immutability and WORM (S3 object lock) capabilities of Amazon Web Services (AWS).
- Setting up a backup plan to set Amazon S3 bucket as the primary backup target.
- The end-to-end solution guidelines using a ransomware simulator covering key features such as File Activity anomaly
  detection through Honeypots, threat removal, air gapping and isolation, and S3 object-locking through an Amazon S3
  bucket.



**Note**: The information shared here is specific to our requirements. It can be used as a guideline or a starting point; however, you can conduct a proof-of-concept in a non-production, isolated test environment matching your production environment before implementing this solution.

#### Intended Audience

This document is intended for Hitachi Vantara staff and IT professionals of Hitachi Vantara customers and partners responsible for planning and deploying such solutions.

#### Value Proposition

Our Cyber-resilient Backup solution acts as the final line of defense, safeguarding against ransomware threats. By aligning with the NIST Cybersecurity Framework, we specifically target features that address customer pain points, bolstering their confidence.

Hitachi Data Protection Suite (HDPS) offers comprehensive data protection and seamless management—from the edge to the core and into the cloud. Beyond defending businesses from cyber threats and ransomware, it incorporates cutting-edge AI/ML algorithms for threat removal and forensic analysis.

In collaboration with Equinix, Hitachi Vantara introduces Hitachi Cloud Connect for Equinix, a near-cloud hybrid solution. It provides high-speed, low-latency connections to major hyperscalers such as Amazon Web Services (AWS).

At the near-cloud data center, the robust Hitachi Virtual Storage Platform E1090 (VSP E1090) storage system hosts clients and backup infrastructure. Known for its impressive capacity, enterprise-class capabilities, and resilience, the VSP E1090 storage system ensures data security.

The Amazon S3 bucket serves as the primary backup target, leveraging the immutability and WORM (S3 object lock) capabilities of AWS.

#### **Document Revisions**

Revision Number	Date	Author	Details	
v1.0	March 2024	Hitachi Vantara LLC	Initial Release	

#### References

- NIST Cybersecurity Framework: <u>https://www.nist.gov/cyberframework</u>
- HDPS documentation: <u>https://documentation.commvault.com/2022e/expert/7877\_ransomware\_protection\_01.html</u>
- For details on WORM and immutability feature of AWS: https://aws.amazon.com/s3/features/object-lock/

## Comments

Send any comments on this document to <u>GPSE-Docs-Feedback@hitachivantara.com</u>. Include the document title, including the revision level, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you.

# **Executive Summary**

This guide describes how to set up an end-to-end cyber resilient backup solution to keep ransomware threats at bay.

The environment used for this validation includes a Hitachi Virtual Storage Platform E1090 (VSP E1090) storage system at the near-cloud data center hosting the clients and backup infrastructure (Commserve). The near-cloud data center is an Equinix colocation. In addition, we used the Equinix Fabric to connect to AWS cloud, allowing us to use an AWS S3 bucket as the primary backup target and AWS EC2 instances for hosting the MediaAgent and VSA cloud provider.

We selected the Equinix colocation because it offers high-speed and low latency connections to major hyperscalers, such as Amazon Web Services (AWS). Hitachi Vantara collaborated with Equinix to offer a near-cloud hybrid solution called **Hitachi Cloud Connect for Equinix**.

This offering allows clients to locate Hitachi products such as the VSP storage system family and Hitachi NAS (HNAS) platform at Equinix International Business Exchange<sup>™</sup> (IBX) data centers worldwide and includes the option for customers to procure this solution through one agreement and invoice, greatly simplifying and accelerating their time to market. By using Equinix IBX data centers and Equinix Fabric<sup>™</sup> to interconnect sources of data to applications, organizations can locate their data stored on VSP storage systems and HNAS systems next to clouds to leverage hybrid- or multi-cloud capabilities while still maintaining physical control of the data.

If you want to discuss options for hosting a disaster recovery solution at Equinix, contact your Hitachi Vantara sales team. For more information, visit the Hitachi Cloud Connect for Equinix webpage at: <u>https://hitachivantara.com/en-us/products/storage/flash-storage/cloud-connect-for-equinix.html</u>.

# Introduction

#### What is a ransomware attack?

A ransomware attack is a classic example of a ticking bomb. Your critical business data is suddenly taken hostage. Hackers used advanced encryption to render it inaccessible, and now they are demanding money to decrypt it. How will you respond? Can you ensure the safety of your data if you refuse to pay — or even if you do? While you consider your options, your organization remains paralyzed. Every passing minute increases the pressure to make the right choice.

This scenario has already struck companies of all sizes across industries worldwide. Yours could be next. Are you ready?

Gartner defines ransomware as "cyber extortion that occurs when malicious software infiltrates computer systems and encrypts data, holding it hostage until the victim pays a ransom."

There is a reason ransomware makes the headlines. It is the kind of attack that gets attention — it is sudden, brutal, and leaves the victim feeling helpless.

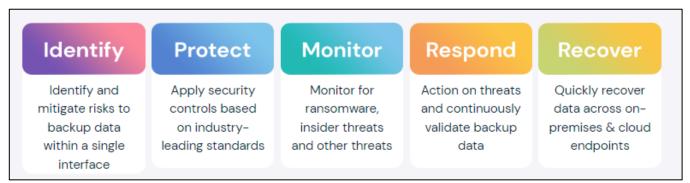
#### What is ransomware protection?

The cyber threat landscape, including ransomware, has transitioned to a case of "when," not "if."

Organizations require tools such as anomaly detection, immutable backups, air gapping, and multi-factor authentication (MFA) controls to continually measure and protect their recovery readiness state. They do this to expose and remediate problems, validate their data and business application recoverability, and to improve their security to reduce their risk profile.

#### Multilayered Approach to Ransomware Protection and Recovery

To help strengthen the data infrastructure and better address the various threats, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is widely used. It focuses on five primary pillars for a successful and holistic cybersecurity program. These pillars can aid your organization in developing a comprehensive risk management strategy.



The end-to-end framework follows NIST and Zero Trust principles, providing class-leading protection and recovery capabilities.

# **Solution Overview**

The combination of Hitachi Data Protection Suite (HDPS) and AWS can be used together as a powerful anti-ransomware solution.

This enables customers to have the best of both worlds in a single solution:

- The class leading scale-out backup and NIST complaint data protection capabilities of HDPS paired with an intuitive software suite.
- The Amazon S3 Object Lock feature allows you to store objects using a write once, read many (WORM) models. S3 Object Lock is the industry standard for object storage immutability for ransomware protection and prevents objects from accidental or malicious deletions and overwrites.

This solution protects and isolates data, provides proactive monitoring and alerts, and enables fast restores. Advanced technologies powered by artificial intelligence and machine learning, including honeypots, make it possible to detect and provide alerts on potential attacks as they happen, enabling you to respond quickly.

#### **Business Benefits**

Organizations can adopt multilayered security frameworks to deal with various vulnerabilities – an approach that offers the best blueprint for protecting against and recovering from ransomware attacks.

#### Objective

This document describes the steps to deploy a multilayered ransomware protection and recovery solution by using HDPS and an AWS S3 bucket.

For more information, contact hdps@hitachivantara.com, your partner manager, or authorized distributor.

#### **Key Components**

The following lists the key components of the solution. For specifications, see the Hardware and Software section.

- Hitachi Data Protection Suite: Backup and restore software with the following components:
  - CommServe: Command and control center of the software that is responsible for handling all activity between agents, such as initiating backup and recovery jobs. In this solution, CommServe is built on top of a VMware ESXi virtual machine using Microsoft Windows Server 2019 CIS Level L1 (Layer 1) hardened OVA (Open Virtual Application).
  - MediaAgent: Oversees the transfer of data between backup targets and storage libraries. Each MediaAgent communicates locally to one or more storage libraries. In this scenario, the MediaAgent was set up on AWS as an EC2 instance, and CommServe and MediaAgent were deployed independently.
- VSP Storage System: A VSP E1090 storage system was used as the backend storage system in the near-cloud setup. Storage for the four-node VMware ESXi 7.0u2 cluster (for setting up CommServe and backup client) was provided by the VSP E1090 storage system.

Note: The Microsoft Windows Server 2019 backup client also ran the ransomware simulator tool.

- Equinix Fabric: Equipment at the Equinix near-cloud data center for connecting to AWS cloud and other hyperscalers.
- AWS Cloud: Equipment at Equinix was connected to AWS cloud through a 10 Gbps Direct Connect link. On AWS, a Virtual Private Cloud was created in the region us-west-1.
- Network Switch: Cisco Nexus 9000 Series switch was used to connect to AWS Direct Connect.
- Amazon S3: Amazon Simple Storage Service (S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. S3 Object Lock blocks permanent object deletion during a customer-defined retention period so that you can enforce retention policies as an added layer of data protection or for regulatory compliance. S3 Object Lock prevents object versions from being deleted (accidental or intentional) or overwritten using write-once-read-many (WORM) models.

S3 Object Lock is the gold standard for achieving object storage immutability for ransomware protection in cloud storage by AWS Storage partners.

**Note**: Air gapping is implemented using virtual machine power management. The cloud controller used for powering on and off the MediaAgent is another EC2 instance configured as a Virtual Server Agent. The AWS S3 bucket (with object lock enabled) was used as the primary backup target.

# Validation

This section describes the method, test environment, hardware and software, and test scenarios used in the validation.

#### Validation Method

- Discovered AWS S3 bucket as cloud storage in the CommServe User Interface (UI).
- Set up a plan from the CommServe UI with the goal of performing primary backup to the AWS S3 bucket.
- Onboarded the client virtual machine in the CommServe UI and associated it with the plan created.
- Triggered a full backup from the client virtual machine.
- Used the client virtual machine prefilled with data as the backup source and later infected it with malware using the ransomware simulator tool.
- Triggered a restore operation directly from the Primary backup.
   Note: Before restoring, data is deleted from the client virtual machine.
- Replenished the client virtual machine with data after restoring successfully.

#### **High Level Diagram**

Figure 1 shows the test environment used to run the validation.

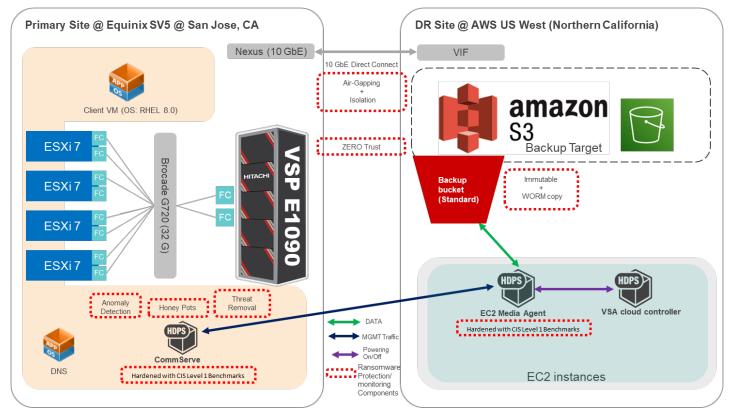


Figure 1: High Level Diagram

## Hardware and Software

Table 1 provides the hardware and software specifications of the equipment used in this validation.

	Item	Description	Version	Function
	Hitachi VSP E1090	<ul><li>1,024 GB cache</li><li>(2) 32-core MPUs</li><li>(3) RAID6 6D+2P parity groups</li><li>(2) 32 Gbps FC ports</li></ul>	SVOS RF 9.8.1 93-06-21-80/00	Storage for source client and CommServe backup repository.
Equinix Near-Cloud Data	Hitachi Advanced Server DS220	<ul> <li>(2) 18-core Intel Xeon Gold</li> <li>6140 @ 2.3 GHz</li> <li>128 GB cache</li> <li>Emulex LPe32002 HBA</li> <li>Intel Ethernet Network Adapter XXV710</li> </ul>	BMC 4.70.06 BIOS S5BH3B22.H00 vSphere: 7.0u2	4-node vSphere cluster used to host source client virtual machine and CommServe virtual machine.
Cloud Data Ce	CommServe Virtual Machine	8-core virtual CPU Xeon Gold 6226R CPU @ 2.90 GHz 32 GB memory 500 GB virtual disk	OS: Windows Server 2019 HDPS: 11.28.44	Manages all activity between MediaAgents and storage libraries.
Center	Source Client Virtual Machine	4-core virtual CPU Xeon Gold 6226R CPU @ 2.90GHz 32 GB memory 200 GB virtual disk	OS: Windows Server 2019	Backup source; houses ransomware simulator tool.
	Cisco Nexus C93180YC-FX	(48) 1/10/25-Gbps fiber ports (6) 40/100-Gbps QSFP28 ports	NXOS 9.3(4)	Provided network connectivity between equipment at Equinix and AWS cloud.
AWS US Wes	MediaAgent on AWS EC2	<ul> <li>(1) 300 GB EBS volume</li> <li>(1) 2 TB EBS volume</li> <li>NOTE: AMI located at aws-marketplace/Commvault Linux</li> <li>FR28 Cloud Data Manager- c3fdde77-53ca-46ca-9ae7- 20256d9e9899</li> </ul>	Instance type: x2.large OS: RHEL 8.7 HDPS: 11.28.44	Responsible for backups and restores. Transfers data between backup clients and storage libraries.
est (North California)	VSA Proxy on AWS EC2	<ul> <li>(1) 300 GB EBS volume</li> <li>(1) 2 TB EBS volume</li> <li>NOTE: AMI located at aws- marketplace/Commvault Linux</li> <li>FR28 Cloud Data Manager- c3fdde77-53ca-46ca-9ae7- 20256d9e9899</li> </ul>	Instance type: x2.large	For air-gapping implementation.
	AWS S3 Bucket	S3 Standard bucket: Object Lock enabled with custom retention period set.		Storage for primary backups.

Table 1: Hardware and Software Components

#### **Test Scenarios**

Table 3 lists the test scenarios performed in the validation.

#	Description	Success Criteria
1	<ol> <li>Prepare the environment:</li> <li>Deploy one Windows Server 2019 virtual machine in the near-cloud data center to act as backup source client.</li> <li>Provision storage from the VSP E1090 storage system to CommServe and source client.</li> <li>In AWS, deploy two RHEL 8.7 EC2 instances for the MediaAgent and VSA.</li> <li>Set up the AWS S3 bucket.</li> <li>Note: Steps 1-3 are common operations; therefore, they are not documented in the Validation Results section.</li> </ol>	Environment is set up as per specifications.
2	<ol> <li>Install and configure HDPS:</li> <li>Deploy CommServe by downloading and installing OVA "CIS L1 hardened Commserver 11.28" as a virtual machine. Download link: <u>https://store.commvault.com/webconsole/softwarestore/#!/130/704/25600</u>.</li> <li>Deploy MediaAgent on an AWS EC2 instance. Note1: Use the BYOL custom image that is available in the AWS Marketplace. See <u>https://documentation.commvault.com/2022e/essential/43647_installing_and_config</u> <u>uring_new_mediaagent.html</u>. Note2: Other than the BYOL prepackaged installer, you can use the standalone MediaAgent installer with only root user privileges (local user cannot be used to trigger the installer script).</li> <li>Add a 300 GB EBS volume to the MediaAgent to serve as a DDB disk.</li> <li>Register the MediaAgent with CommServer. Ensure that Commserve and MediaAgent are on the same code level. Otherwise, the registration fails.</li> <li>Install and configure VSA cloud provider.</li> <li>Configure the AWS S3 bucket.</li> </ol>	Installed and configured successfully.
3	<ol> <li>Secure and harden the components:</li> <li>After deploying the hardened CommServe through the OVA, verify whether ransomware protection is enabled.</li> <li>Harden the MediaAgent virtual machine based on CIS Level 1 standards.</li> <li>Harden the VSA cloud provider virtual machine based on CIS Level 1 standards.</li> <li>Secure the AWS S3 bucket by enabling Object Lock and Retention.</li> </ol>	Environment is hardened based on the NIST guidelines.
4	<ol> <li>Simulate ransomware infection and recovery:</li> <li>Prepare the backup client for the ransomware simulation.</li> <li>Install and configure the ransomware simulation tool.</li> <li>Prepare a set of files.</li> <li>Simulate a ransomware attack on the files.</li> <li>After the ransomware simulation, verify that anomaly alerts are reflected in CommServe.</li> <li>Restore the original, clean files.</li> </ol>	Generates anomaly alerts after ransomware simulation and restores clean files.

# **Validation Results**

This section contains specific steps to validate the end-to-end solution.

#### **Test 1: Prepare the Environment**

#### Setting up S3 bucket in AWS

The following screenshot shows the S3 bucket that will be used as the primary backup target:

aws III Services Q Search	(Alt+5)	C	<b>D</b> 4	0 4	Global •	
Amazon S3 ×	Amazon 53 > Buckets > worm-immutable-ransomware-proj					
Buckets Access Points Object Lambda Access Points Multi-Region Access Points	Worm-immutable-ransomware-proj         Info           Objects         Properties         Permissions         Metrics         Access Points					
Batch Operations IAM Access Analyzer for \$3	Objects (2) Objects are the fundamental entities stored in Amazon S1. You can use Amazon S1 investory 😰 to get a list of all objects in your bucket. For others to access your objects, you'li need to explicitly grant them permission	ss. Learn more 🖸				
Block Public Access settings for this account	C Copy S3 URI Copy URL Download Open C Delete Actions V Create folder (R) Upload Q. Find abjects by prefix O Show versions					
Dashboards AWS Organizations settings	Name         Type         V         Last modified           D         365R0J_02.07.2023_08.07/         Foldor         -           D         11Y103_02.203.2023_08.07/         Foldor         -           D         11Y103_02.203.2023_08.07/         Foldor         -	v Size			Storage c	last
Feature spotlight						

#### Bucket properties:

Object Lock Shere slights using a write-once-read-many (WORM) model to help you prevent objects from being defeted or overwritten for a flowd amo	t of time or todefinitaly. Learn more 🖸	j.
Object Lock Enabled		
Default retention Automatically protect new objects put into this bucket from being deleted or overwritten.		
Disabled		

#### **Test 2: Install and Configure HDPS**

#### Register MediaAgent in CommServe

The following screenshots show the process to register the MediaAgent (IP address: 10.77.25.101) to CommServe.

```
[root@10 ec2-user]# subscription-manager register --auto-attach
/usr/lib/python3.6/site-packages/requests/__init__.py:91: RequestsDependencyWarning: urllib3 (1.26.13) or ch
 RequestsDependencyWarning)
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: redhattammy
Password:
The system has been registered with ID: 82558c64-8f42-467d-be86-8dce9816ddb4
The registered system name is: 10.77.25.101
Installed Product Current Status:
Product Name: Red Hat Enterprise Linux for x86_64
                Subscribed
[root@10 ec2-user]#
[root@10 ec2-user]#
[root@10 ec2-user]# sudo su
[root@10 ec2-user]#
[root@10 ec2-user]# cd /etc/
[root@10 etc]# ./commvaultRegistration.sh
Welcome to Commvault Registration Process, provide below details to initiate the registration
Enter Client Name : MAforAWS
Enter Client Hostname : 10.77.25.101
Enter CS Name : commvault
Enter CS Hostname : 172.23.30.212
Enter CS Username : admin2
Is CS behind a firewall? (yes/no) : yes
True
[Option 1] CS f/w tunnel port (client can connect to CS)
[Option 2] Client f/w tunnel port (CS can connect to client)
[Option 3] CS reachable via proxy
Enter the option (1/2/3) : 1
Enter the tunnel port number the client can use to open a connection to the CommServe system : 8403
Is HTTP proxy used for communication between the CommServe host and the client ? (yes/no) : no
Do you wish to proceed with registration using the above information? (yes/no)yes
```

TERM=xterm	
SHLVL=1	
LOGNAME=root	
PATH=/sbin:/bin:/usr/sbin:/usr/bin	
HISTSIZE=1000	
=/bin/env	
Redirecting starting service for Instance001 to systemd	
Running "systemctl start commvault.Instance001.service"	
Waiting 60 seconds for cvd to settle	
/etc/init_frel_cloud: line 663:	
retryCt=2	
if [ -n \$FWON ]; then	
retryCt=5	
fi	
if [ \$logindone -eq 0 ]; then	
while [ \$retryCt -ge 0 ]; do	
./qlogin -u \$csUserName \$parg	
ret=\$?	
if [ \$ret -eq 0 ]; then	
break	
else	
retryCt=\$((retryCt-1))	
echo "Login failed. retry in 60 secs"   tee -a \$LOGFILE	
sleep 60	
fi	
done	
else	
ret=0 fi	
: No such file or directory	
Redirecting stopping service for Instance001 to systemd	
Redirecting stopping service for instance001 to systema Running "systemctl stop commvault.Instance001.service"	
Stopping Commvault services for Instance001	
Cleaning up /var/log/commvault/Log_Files/locks All services stopped.	
Redirecting starting service for Instance001 to systemd	
Running "systemetl start commyault.Instance001 to systeme	
Client registration for auto CV deployment complete!	
frontero crolt	

#### Add Cloud Storage to CommServe

To create storage libraries in the Command Center, complete the following steps:

- 1. From the Command Center UI, select **Storage > Cloud > Add > Cloud Storage**.
- 2. Add the bucket as a cloud storage.
- 3. Create a cloud storage library with Deduplication enabled.

	Q Search or type / for a command	table-ransomware-proj			🗟 🗘 📰 🔒 admin2
Filter navigation	Cloud				
🛠 Guided setup	worm-immutable-ransomw	are-proj			
🗶 Dashboard	Overview Configuration Associat	ed plans			
C Protect	General				
Activate	Туре	Cloud			
Disaster recovery	Vendor type	Amazon S3			
dobs	Size on disk	9.42 GB			
@ Reports	Bucket			Add Q	с III і
Monitoring					
Storage	All				\$
HyperScale X	+ Add filter				
	Name 1		Status		Actions
Metallic Recovery R	[awsma2] worm-immutable-ransomware-proj		Ready		
Distributed Storage	[MAforAWS] worm-immutable ransomware-proj		Ready		
Disk					
Cloud					
Tape					
3 Manage					
Developer tools					

The following screenshot shows the configuration properties (WORM enabled) of the added Cloud Storage:

	Q Search or type / for a command			6 A 20	L admin2
Filter navigation R Guided setup Dashboard	Cloud worm-immutable-ransomware-proj Overview Configuration Associated plans				
<ul> <li>Protect</li> <li>Activate</li> <li>Disaster recovery</li> <li>Jobs</li> </ul>	Encryption Encrypt IIII Key management server Built-in	0	Security No associations defined on this object Show inherited association		0
<ul> <li>Reports</li> <li>Monitoring</li> <li>Storage</li> </ul>	Tags No tags associated with	0	Cache	0	
HyperScale X Metallic Recovery R Distributed Storage Disk			WORM WORM storage lock Compliance lock	-0	
Cloud Tape			Note : Retention setting of dependent	nt backup destinations will be used for WORM storage lock	×
Manage     Developer tools     Workflows					

#### **Discover S3 Bucket in CommServe**

The AWS S3 bucket is added as a cloud storage library:

	Q Search or type / for a command				L admin2
Filter navigation	Cloud / worm immutable ransomware proj [awsma2] worm-immutable-rans	Edit cloud access path	×		
it Dashboard D Protect Activate	General Normet	Access Type Amazon 03 Name * worm immutable ransomware proj	-		
<ul> <li>Disaster recovery</li> <li>Jobs</li> <li>Reports</li> </ul>		Mudiulyerst * anitms2 situmsa host * s3.us-west 1.amazonaws.com	<u> </u>	• + 0	
Monitoring	Cloud access paths	Automotication * Access and secret keys Credentials * cred human *	• • + 0	Add mediaagent Q. C	: III 3 \$
HyperScale X Metallic Recovery R Distributed Storage Disk	MediaAgent 1 B areama2 re MAACOAWS a	ouum - minimutableransomware.proj Storage class - S3 Standard-Infrequent Access	•	Accessible Yes Yes	Actions
Cloud Tape ﷺ Manage		Http proxy server Advanced	×		
Developer tools     Workflows		EQUIVALENT API CA	INCEL SAVE		

**Note**: Before discovering the AWS S3 bucket in CommServe, ensure IP address resolution from CommServe to AWS S3 bucket and vice-versa is functional.

The following screenshot shows the creation of a backup plan utilizing the AWS S3 bucket.

	Q Search or type / for a co	mmand					8	4 ₽	L admin2
Filter navigation  Filter navigation  Guided setup  Dashboard	Plans ~ FileActivity DEMO						Delete	Derive and	d create new
<ul> <li>Protect</li> <li>Activate</li> <li>Disaster recovery</li> </ul>	Backup destina	tions			ADD 🗸	RPO Backup frequency No backup scheduled			Add
<ul> <li>Jobs</li> <li>Reports</li> <li>Monitoring</li> <li>Storage</li> </ul>	Name snap copy snaphor primay Primary Primary	Storage worm-immutable-ransomware-proj coso worm-immutable-ransomware-proj	Retention period 1 day 1 day	Source	Action (	Backup window Full backup window SLA	Monday : 4am-5am Monday : 3am-4am 1 week, inherited from CommCell		0 0
菱 Manage CommCell Servers	Database optio	ns			_	Snapshot options Enable backup copy			
Server groups Companies Plans Tags Infrastructure	Log backup RPO Full backup frequency Use disk cache for log back	ups	Runs every 4 hour(s) Runs every 1 week		0	Backup content Windows Mac Unix C:Users/Administrator/Desktop/FileActivity			0

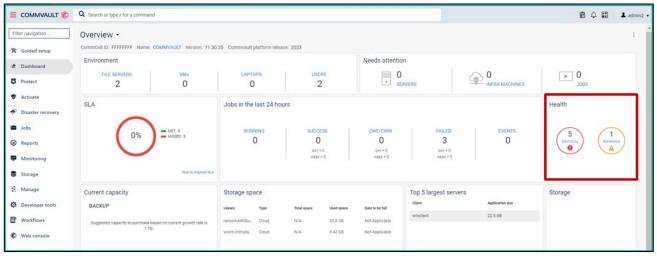
#### **Test 3: Secure and Harden the Components**

This solution was built keeping the five pillars of NIST framework in mind. After the basic building blocks are set up, you must identify and fix the loopholes in the environment.

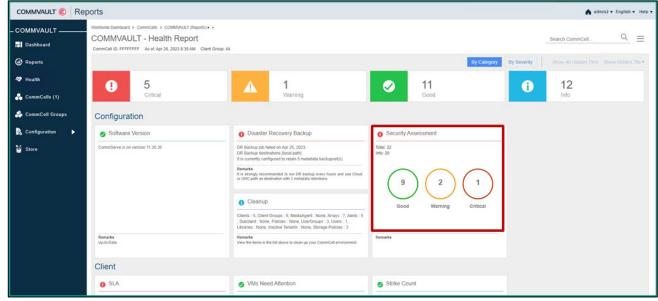
#### Identify: Mitigate Threats to Backup Data Through a Security Assessment

- Identify risk exposure and coverage status quickly by using the Command Center dashboard.
- Provide complete control over who has access and what they have access to through zero-trust principles.
- Eliminate accidental or malicious administrative actions by requiring dual authorization to implement changes.
- Verify authentication support through a broad range of multi-factor authentication (MFA) options.

#### 1. From the dashboard, click Health.



#### 2. Click Security Assessment.



You can modify other security parameters from the dashboard.

	Reports					
COMMVAULT	Security Assessment				Search CommCell	Q
	CommCell ID: FFFFFFF As of: Apr 26, 2023	9.02 AM Time zone: UTC				
Dashboard	O Access Security					
0	Parameter	Status	Remarks	Action		
Reports	Two-factor authentication	otni 🕕	Disabled Commvault recommends you enable this feature	How to enable two factor authentication		
🧇 Health	Single sign-on	O Info	No Single sign-on Providers are configured.			
	Password complexity level	A Warning	Level 2	Set password complexity level to 3		
🐣 CommCells (1)	Failed log-on attempts limit	🕝 Good	The account will lock after 5 failed log-on attempts.	How to set a failed log-on attempts limit		
	Account lock duration	otni 🕕	The account will be locked for 1 hour	How to set the account lock duration		
A CommCell Groups	Command Center timeout period	olni ()	Command Center will timeout after 30 minutes.	How to change the timeout period		
Configuration	Commcell Console timeout period	😋 Good	Commcell Console will timeout after 30 minutes.	How to set the timeout period		
Store	Auditing					
	Parameter	Status	Remarks	Action		
	Security Cleanup report	otni 🕕	3 user groups without users     3 users without security associations     1 users not logged-in in 30 days	View report		
	User and user group permissions report	1 Info	View users in master group	View report		
	Activity of the second second second second second	Good	Current setting: 1 year Recommended: 1 year			
	Critical priority audit trail retention	and the second second				
	Critical priority audit trail retention	@ Good	Current setting : 1 year Recommended: 1 year			
			Current setting : 1 year			

Under Platform Security, the Ransomware Protection status shows Enabled.

Note: By default, the protection status is enabled.

© Auditing								
⊖ Platform Security								
Parameter	Status	Remarks	Action					
Storage pools without encryption	1 Info	3 storage pools without encryption	View report					
Ransomware protection	Good Good	All mount paths are secured against ransomware.						
File Activity Anomaly alert	Good Good	Enabled						
Disaster Recovery Backup	🔥 Warning	DR backup is not configured to cloud or UNC path	How to configure DR backup					
Key Management Server for Password Encryption	() Info	Built-in key management service is used.	How to configure a key management service					

#### **Protect: Apply Security-based Controls**

- Reduce the attack surface and better safeguard your data through intuitive dashboards and simplified processes.
- Reduce your overall attack surface by isolating networks and data management using the multitenancy functionality.
- · Securely air gap your backup copies to mitigate lateral moving threats.
- Protect against changes from within and outside the backup solution by implementing immutability with your choice of hardware.

Note: For this solution, the immutability and WORM capabilities of AWS S3 bucket were used.

#### Air Gapping

An air gap isolates the data by breaking communication with the machine that contains or manages the data.

To achieve air gapping, use any of the following methods:

- Use virtual machine power management to automatically shut down a MediaAgent virtual machine when not in use.
- Create blackout windows on storage targets or network devices using scripts and workflows.

In this solution, we implemented air gapping using option 1.

For more information, see the following pages:

- https://documentation.commvault.com/2023/expert/151540\_air\_gapping\_01.html
- https://documentation.commvault.com/2022e/essential/101313\_cloud\_mediaagent\_power\_management.html
- <u>https://documentation.commvault.com/2022e/essential/101354</u> enabling power management for cloud mediaagent.ht <u>ml</u>

#### After implementation:

	Q Search or type / for a command			ß	
Filter navigation	Infrastructure / MediaAgents / awsma2 Overview	Edit power management	×	Mark for maintenance	Upgrede software 💮
<ul> <li>Protect</li> <li>Activate</li> <li>Disaster recovery</li> </ul>	General	Use server group settings Use MediaAgent settings Enable power management		-0	
<ul> <li>Disaster recovery</li> <li>Jobs</li> <li>Reports</li> </ul>	OS Version Communat platform nérese Xestus	Rec Cloud controller * 11 VSAAccessNode 20. Rec	CANCEL SAVE	• •	
Monitoring Storage	Security	t	Paralle data transfer contrainer.	100	0
CommCell Servers Server groups	No associations defined on this object Show inherited association		Power management	VSAAccessNode	Ø
Companies Plans	Index Cache	// mmt/commvault_indexcache/commvault/MediaAgent/IndexCa che	Shalos	Running, online	
Tags Infrastructure	Enable logs cache				

The MediaAgent is powered on by the Cloud controller node only when backups and restores are happening.

😮 COMMVAULT - v11 Commo	ell Console		
Home Tools Storage	Configurati	on Reports View Support	
✓ Status Bar □ Tasks Refresh	Previous	KediaAgent Properties for awsma2	
View	Window	General         Control         Catalog         File Server         Version         Security         Associated Storage Policies         Deduplication Partitions         Advanced           Additional Settings         Logging         Network Route Configuration         Network Throttle         Index Server         VM Management         Audit	
CommCell Browser	ucket	O Use Client Group settings   Client Group Name : Not Applicable   Power Management : Not Applicable   Ouse Media Agent settings   ✓ Enable Power Management   Cloud Controller : VSAAccessNode   Power Off Status: Running Online   Reason:	ited N
Agents		OK Cancel Help	
🔶 My Favorites			1

#### Enable WORM Copy

To enable WORM storage for the cloud library, download a workflow template from the following URL: <u>https://store.commvault.com/webconsole/softwarestore/#!/136/671/20812.</u>

#### For instructions to enable WORM copy, see:

https://documentation.commvault.com/2023/expert/9251\_configuring\_worm\_storage\_mode\_on\_cloud\_storage.html.

To enable hardware WORM at the library level, follow the procedure in the aforementioned URLs.

COMM	VAULT - v	11 Commce	ll Console											-	- 0
Home	Tools	Storage	Configuratio	on Reports	View	Support									
Status	Bar	Refresh	Previous Window		Iose Clos	All Maxir		mCell Re	eset Til yout Horizo		у			COMMV	AULT 💰
View	/			Window	s				Layout						0.00
Comm		er	Q		ng Started 🗙	D Job Contro	ller 🗙 🔋 Eve	ent Viewer 🗙	😪 worm-im	mutable-ransom	ware ×	Schedule Polici	es X		4 ا
COMMV		ter Groups	^	🔏 соммия	iult > 🌒 si	orage Resources	> Libraries	> 😪 worm-in	nmutable-ranson	nware-proj >					<b>₽ □</b>
	nt Compu			E Content											
Sto	urity rage Reso Deduplica Index Sto Libraries	tion Engines re Pools		Cibrary Prop		Ready m-immutable-ra	Access Read/Write		Capacity N/A < N/A	Do Not Cons	Reserved Sp N/A N/A	Sparse Supp	Job ID	Total Streams	MediaAgent
-0 -0 -0 -0 -0 -0 -0 -0 -0 -0 -0 -0 -0 -	worm a [a [a [w] Locations Media Age Orphaned RP Store Storage P VaultTrac cies	nts Media ools	ansomware	Library Nam Cloud vende Associated	ne: or type: MediaAgents: Mount Paths: age Lock:	worm-immutal	Disk Usage An ble-ransomware-p AWS			- worm-immu nesday, April 20					
Comme Comme Comme Agent:	itent Direc rkflows Cell Brows		>	Hide Lib Hide Lib Mark Lib Timeouts (i Mount	rary Offline for n minutes) 10 그	Maintenance	10 - J K Cance	>	•						

**Note**: For maximum protection at bucket level, use the Enable Worm Storage workflow on the cloud libraries instead of the ransomware workflow. Additionally, you can enable WORM Copy on a storage policy copy.

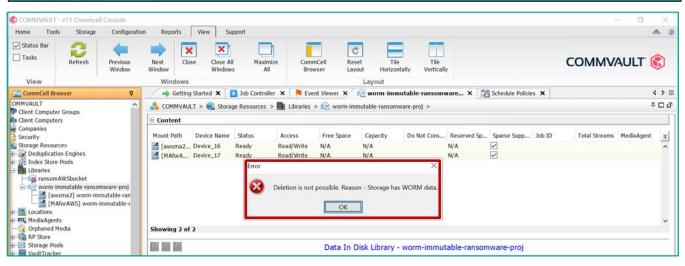
#### For more information, see:

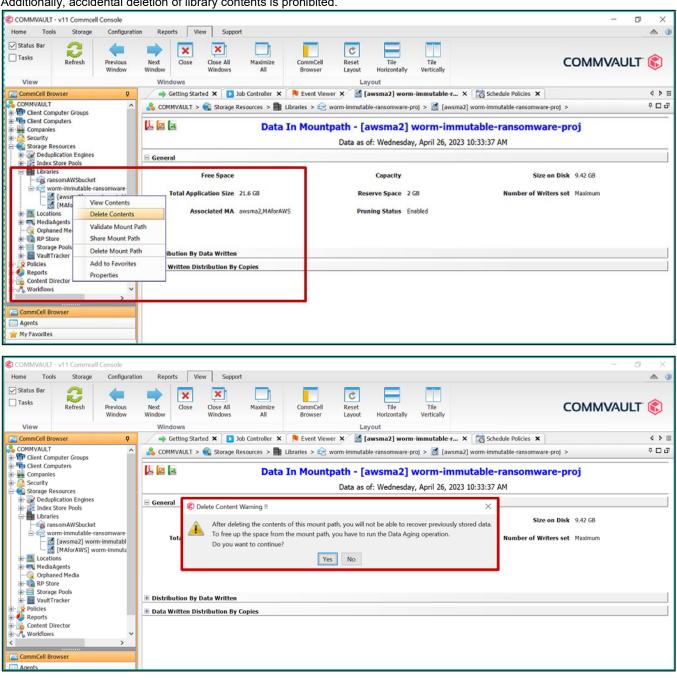
https://documentation.commvault.com/2022e/expert/112844 enabling worm copy on storage policy copy.html.

COMMVAULT - v11 Commcell Console		- a ×
Home Tools Storage Configuration	n Reports View Support	۵ ک
Status Bar Tasks Refresh Previous View	Next Window         Close All Windows         Maximize All         CommCell Browser         CommCell Layout         Tile Horizontally         Tile Vertically	COMMVAULT 🎼
CommCell Browser	🛶 Getting Started 🗙 📘 Job Controller 🗴 📜 Event Viewer 🗙 🥅 Primary 🗴 📅 Schedule Policies 🗴	٩ ﴾ ۵
	Scommulation > Policies > Storage Policies > FileActivity DEMO > Primary >	÷08
Companies     Companies     Companies     Companies     Security     Configuration Policies     Policies     Policies     Policies     Configuration Policies     Schedule Policies     Schedule Policies     Schedule Policies     Schedule Policies     Schedule Policies     Subclient Policies     Subclient Policies     Virtual Machine Policies     Virtual Mach	Storage Policy Copy properties of Primary   Associations Media Advanced Deduplication Provisioning Configuration Audit   General Retention Data Paths Data Path Configuration Selective Copy   Copy Information Copy Name: Primary Compliance Lock   Copy Name: Primary WORM Storage Lock Compliance Lock   Storage Pool: worm-immutable-ransomware-proj MediaAgent: awsma2   Drive Pool: N/A   Description OK Cancel Help	

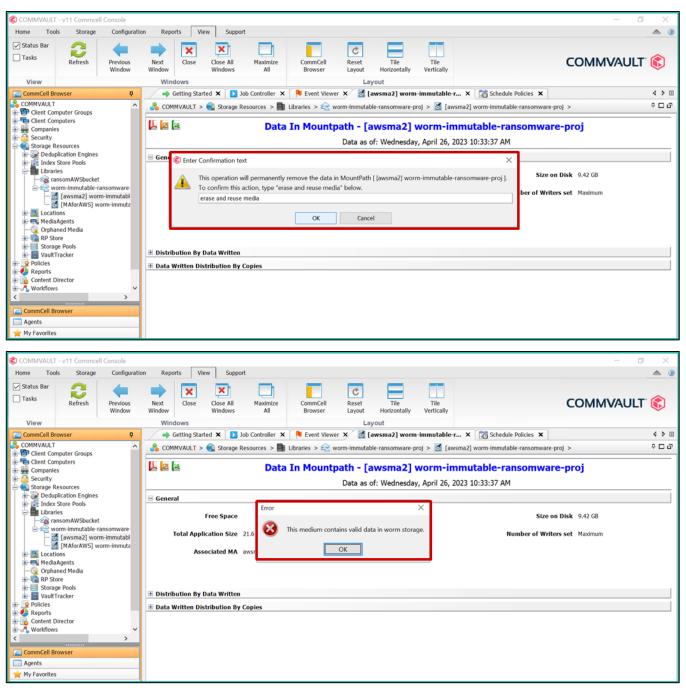
After WORM is enabled at both AWS S3 bucket and CommServe levels, the library cannot be deleted.

COMMVAULT - V	11 Commoell Console										i. <del>.</del>	- 0	×
Home Tools	Storage Configuration	n Reports View	Support										-
☑ Status Bar ☐ Tasks	Refresh Previous Window	Next Window	Close All Maxim Windows All		mCell Rese wser Layo		Tile Tile Vertically				сомму	AULT	\$
View		Windows				Layout							
CommCell Brow	ser 🛛 🖓	🚽 Getting Starte	d 🗙 🚺 Job Controll	er 🗙 🔋 🗎 Eve	nt Viewer 🗙 💈	🗟 worm-imm	utable-ransomv	vare X	👼 Schedule Polici	es 🗙			4 0 1
OMMVAULT	^	🚴 COMMVAULT > (	Storage Resources	> 📑 Libraries	> 😪 worm-imm	utable-ransomw	vare-proj >						₽ 🗆 d
Client Computer C	sroups	∈ Content											-
Companies		1 12 12 11		1	1		1	1	1	1.02	11.5	1	
Security			e Name Status	Access	Free Space	Capacity			. Sparse Supp	Job ID	Total Streams	MediaAgent	¥ ¥
Storage Resource		awsma2 Device		Read/Write	N/A	N/A		N/A					^
Index Store Po		MAforA Device	e_17 Ready	Read/Write	N/A	N/A		N/A	$\checkmark$				
	VSbucket Add Mount Path Disk Library Maintenance												
Locations	Delete												
Q Orphaned	View	> owing 2 of 2											
RP Store	Add to Favorites				Data In D	isk Library -	worm-immut	able-ranso	nware-proi				
VaultTrac	Properties		201		Data In Di	an elerary	in strin in interest	abre runsor	intere proj				





Additionally, accidental deletion of library contents is prohibited.



#### **Monitor: Find Anomalous Threats**

- Stay up to date through easy-to-use dashboards that provide early warning alerts of suspicious and malicious activities.
- Easily monitor, manage, protect, and secure the environment using a single interface.
- Actively monitor abnormal activities for more significant insights, alerts, and faster response.
- Detect ransomware and other suspicious activities.

#### **Respond: Analyze Data and Perform Orchestrated Actions**

- Ensure clean backup copies to avoid business interruptions and minimize risk.
- Automatically isolate suspected files to minimize ransomware spread and for further investigation.
- Prevent backup copies from retiring by automatically retaining the last known good copy.

• Review comprehensive reports and alerts through integration with industry-leading monitoring tools for greater security coverage.

#### **Recover: Restore Clean Data**

- Ensure consistent recovery across all data and workloads to restore on-premises, in the cloud, or wherever the data is needed.
- Avoid ransomware file reinfections by surgically deleting suspicious or unnecessary files.
- Ensure clean file recoveries by quickly isolating suspected backup copies or restoring to a safe location.

#### **Test 4: Simulate Ransomware Infection and Recovery**

To validate the Monitor, Respond, and Recover pillars of the NIST framework, we used a ransomware simulator to generate File Activity anomalies.

#### **Reproduce Activity Anomalies**

Run the Ransomware Simulation tool on the files you are backing up to encrypt them to simulate a ransomware attack. This triggers a file activity anomaly.

- 1. Take a full backup of the clean files.
- 2. Ensure that the files are not encrypted and are valid.

#### The following screenshot shows clean uninfected files after data generation.

$\leftarrow \rightarrow \cdot \uparrow$	> File	Activity				v ♡	Search FileActivity
🖈 Quick access		Name	Date modified	Туре	Size		
Desktop		FileGen 99927735334	3/29/2023 11:29	BIN File	17,409 KB		
Downloads	4	FileGen 99878638540	3/29/2023 11:29	BIN File	17,409 KB		
	<i>.</i>	FileGen 99638568977	3/29/2023 11:29	BIN File	17,409 KB		
Documents	*	FileGen 99534119015	3/29/2023 11:29	BIN File	17,409 KB		
Pictures	*	FileGen 99441740132	3/29/2023 11:29	BIN File	17,409 KB		
FileActivity		FileGen 99384946069	3/29/2023 11:29	BIN File	17,409 KB		
📜 Ransomware		FileGen 99243719498	3/29/2023 11:29		17,409 KB		
		FileGen 99175659812 - Notepad	3/30/3033 44.30	DIALCIA	47.400 KD		- 🗆 X
3D Objects		File Edit Format View Help					
Desktop		Hello World !!					^
Documents		Hello World !! Hello World !!					
Downloads		Hello World !! Hello World !! Hello World !!	Hello World !!				
Music		Hello World !! Hello World !!					
Pictures		Hello World !! Hello World !! H	Hello World !!				
Videos		Hello World !! Hello World !! Hello World !!					
_		Hello World !! Hello World !! H	Hello World !!				
Local Disk (C:		Hello World !!					
🖆 DVD Drive (D)	555_	Hello World !! Hello World !!					
📣 Network		Hello World !! Hello World !! Hello World !!	Hello World !!				
🧢 tsclient		Hello World !! Hello World !!					
S WINCLIENT		Hello World !! Hello World !! H	Hello World !!				
		Hello World !! Hello World !! Hello World !!					
		Hello World !! Hello World !! H	Hello World !!				
		Hello World !!					
1,000 items 1 ite	o color	Hello World !! Hello World !!					

#### Because the files are clean, no unusual file activity is detected.

	Q Search or type / for a command					6	4	上 admin2 •
Filter navigation		1						
🛠 Guided setup	Unusual file activity 2 Monitored   0 Affected				٩			С Ш :
🖈 Dashboard	All File activity File type							٥
B Protect	+ Add filter	-						
Activate								
🔊 Disaster recovery								
🚔 Jobs								
@ Reports								
Monitoring								
Alerts								
Events								
Unusual file activity								

3. Run a full backup: Initiate a full backup of the client to back up the clean files.

E COMMVAULT 💰	Q Search or type / for a command	d				Backup
Filter navigation	File servers					Select a subclient to back up
🔆 Guided setup						Subclients FileActivity •
🖄 Dashboard	Type * All *) (+ Add filter)					Name † E Backup content E Last successful back E
C Protect	Name 1	Configured	Last backup	Application size	Plan	✓ default C:\Users\Administrator\ Mar 29, 8:11 AM
Virtualization	• 🌉 COMMVAULT	~	Never backed up	0.8	Not assigned	Plan FileActivity DEMO Backup content derived fr
Kubernetes	• 🌉 winclient	~	Mar 29, 8:11 AM	95.76 GB	FileActivity DEMO	Excluded from backup No exclude content
File servers						Last backup size 96.68 GB
Databases						
Laptops						
Office 365 Exchange						
Activate						
<ul> <li>Disaster recovery</li> </ul>						
Jobs						
Reports						
Monitoring						
Storage						
茎 Manage						Cancel Select
🔅 Developer tools						Cancel Select
-	0					
	Q Search or type / for a comman	d				Select backup level ×
E COMMVAULT ©		d				Select backup level × Subclient or instance being backed up : default Backup level
	File servers	d				Subclient or instance being backed up : default
Filter navigation	File servers	d				Subclient or instance being backed up : <b>default</b> Backup level
Filter navigation	File servers		Last backup	Application size	Pin	Subclent or instance being backed up : default Backup level
Filter navigation	File servers	id Configured	Last backup Never backed up	Application size 0 B	Plan Not assigned	Subclent or instance being backed up : default Backup level
Filter navigation	File servers All (Type + All *) + Add filter) Name †	Configured				Subclient or instance being backed up : default Backup level
Filter navigation % Guided setup & Dashboard Protect Virtualization	File servers All (Type + All *) + Add title Name † • E COMMANDIT	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation	File servers All (Type + All *) + Add title Name † • E COMMANDIT	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation  Curried Control	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation *C Guided setup *Dashboard Protect Virtualization Kubernetes File servers Databases Laptops Office 365 Exchange Activate *Disaster recovery Jobs @ Reports	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation <sup>™</sup> Guided setup <sup>™</sup> Dashboard <sup>™</sup> Protect <sup>™</sup> Virtualization <sup>™</sup> Kubernetes <sup>™</sup> File servers <sup>™</sup> Databases  Laptops <sup>™</sup> Activate <sup>™</sup> Disaster recovery <sup>™</sup> Jobs <sup>™</sup> Reports <sup>™</sup> Monitoring	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation         % Guided setup         & Dashboard         Image: Dashboard         Image: Protect         Virtualization         Kubernetes         File servers         Databases         Laptops         Office 365         Exchange         Image: Activate         Image: Disaster recovery         Image: Jobs         Image: Reports	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level
Filter navigation <sup>™</sup> Guided setup <sup>™</sup> Dashboard <sup>™</sup> Protect <sup>™</sup> Virtualization <sup>™</sup> Kubernetes <sup>™</sup> File servers <sup>™</sup> Databases  Laptops <sup>™</sup> Activate <sup>™</sup> Disaster recovery <sup>™</sup> Jobs <sup>™</sup> Reports <sup>™</sup> Monitoring	File servers All (Type + All *) + Add title Name † • E COMMYAUX	Configured	Never backed up	0.8	Not assigned	Subclient or instance being backed up : default Backup level

4. Reproduce activity anomaly by encrypting the contents using the ransomware simulation tool.

→ - ↑ 🔋 F	ileActivity				✓ U Search File/	Activity
	Name	Date modified	Type	Size		
Quick access	COMMVAULT ENCRYPTION DONE	3/30/2023 12:28	Text Document	85 KB		
Desktop 3	FileGen 99927735334.bin	3/30/2023 12:28	CVENCRY File	17.410 KB		
Downloads 🔋	FileGen 99878638540.bin	3/30/2023 12:28	CVENCRY File	17,410 KB		
Documents >	FileGen 99638568977 bin	3/30/2023 12:28	CVENCRY File	17,410 KB		
Pictures >	FileGen 99534119015.bin	3/30/2023 12:28	CVENCRY File	17,410 KB		
FileActivity	FileGen 99441740132.bin	3/30/2023 12:28	CVENCRY File	17,410 KB		
RansomwareD	FileGen 99384946069.bin	3/30/2023 12:28	CVENCRY File	17.410 KB		
Concerner of	FileGen 99243719498.bin	3/30/2023 12:28	CVENCRY File	17.410 KB		
This PC	FileGen 99175659812.bin	3/30/2023 12:28	CVENCRY File	17.410 KB		
3D Objects	FileGen 99010716836.bin	3/30/2023 12:28	CVENCRY File	17.410 KB		
Desktop	FileGen 98930988400.bin	3/30/2023 12:28	CVENCRY File	17.410 KB		
Documents	FileGen 98878600019.bin	3/30/2023 12:28	CVENCRY File	17,410 KB		
Downloads	FileGen 98768414858.bin	3/30/2023 12:28	CVENCRY File	17,410 KB		
Music	FileGen 98630552540.bin	3/30/2023 12:28	CVENCRY File	17.410 KB		
Pictures	FileGen 99175659812.bin - Notepad					- 0
Videos	File Edit Format View Help					
				š""B" BPP00 - \$""B"		

5. Verify air gap implementation and run another full backup job to protect the encrypted files.

Air gap implementation validation: Power management powers on the MediaAgent before backing up.

	Search or type / for a command			🗟 🗘 🔛 💄 admin2 🗸
Filter navigation	lob 741 - [Backup]			Suspend V Resume
🛠 Guided setup	verview Events Retention			
Le Dashboard				
B Protect	General		Progress	
Activate	Type Backup type	Backup Full	Start time Current phase	Mar 30, 2023, 6:56:43 AM Scan
A	Status	Pending	Elapsed time	0 seconds
Jobs .	Job started by Encryption enabled	admin2 (Started interactively) No	Current throughput	N/A
Reports	System state	Yes		
Monitoring			Item status	
Storage	Associations		Failures	0 Folders, 0 Files
	Agent	Windows File System	Data transferred on network Scanned objects	N/A 0 Folder(s), 0 File(s)
Developer tools	Media agent	awsma2		
	Backup set Source client computer	FileActivity winclient		
	Subclient	default		
C Web console	Plan	FileActivity DEMO		
	Error oursmoor			
	Error summary			
	62:2947 Power Management is enabled on this Vir Source: COMMVAULT, Process: JobManager	rtual Machine(s)[MAforAWS]. Waiting on the Virtual Machine(s) to power on.		

E COMMVAULT	Q Search or type / for a command			書 众 詔 💧 admin2
Filter navigation	Active jobs Job 741 - [Backup] Overview Attenuits Events Streams Retention			Surgend ~ Kill 🤆
Protect	General		Progress	
Activate     Disaster recovery	Type Backup type	Backup Full	Start time Current phase	Mar 30, 2023, 6:56:43 AM Backup
<ul> <li>Jobs</li> <li>Reports</li> </ul>	Status Job staried by Encryption enabled	Running admin2 (Started interactively) No	Progress Elapsed time Estimated completion time	72% 1 minutes 2 seconds Mar 30, 2023, 7:02:26 AM
Monitoring  Storage	System state	Yes	Last update time Current throughput Average throughput	Mar 30, 2023, 7:02:17 AM 2:25 TB/hr 1.46 TB/hr
S Manage	Associations		Load Currently backing up	(Read: 88.89%), Network: 11.11%) C:\Users V.dministraton/Desktop/FileActivity/FileGen 405001727 Disk,C:\Users V.dministrator/Desktop/FileActivity/FileGen
Developer tools     Workflows	Agent Media agent Backup set	Windows File System MAforAWS FileActivity	Currency backing up	4000 (12). bits: Users Administrator Desktop/FileActivity/FileGen 6131181550.bin 1127066026.bin;C:/Users/Administrator/Desktop/FileActivity/FileGen 6131181550.bin
Web console	Source client computer Subclient Plan	winclent default FiloActivity DEMO	Item status	750
			Fallows Das Standarding of nationals Scienced algorithm Size of application No of adjustman spatial for backup	0 Frádska Office 817 54 40 Trádarát, 1000 Fice) 1246 60 1000

The following screenshot shows the anomalies in the unusual file activity dashboard.

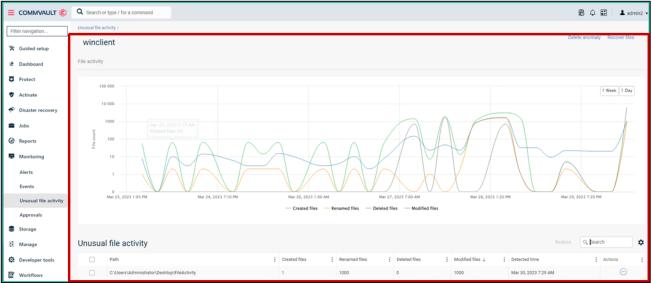
#### Events tab: Picks up the File Activity Anomaly.

	Q Search or t	type / for a c	ommand							🗟 🗘 📰 🗎 🛓 admin2
Filter navigation										
🔆 Guided setup	Events								Q	C III : 1-25 of 100
	All	Info	Mine	or Major	Critical	Critical (last 24 hours)	Focused (last 24 hours)			
2 Dashboard	+ Add filter									
C Protect	Event ID 4	Severity	Job Id	Date	Program		Computer	Event code		Description
Activate	16697	Critical		Mar 30, 7:29 AM	cvd		winclient	7.333		Detected file activity anomaly of type [Renamed Mod
Disaster recovery	16694	Major	741	Mar 30, 7:01 AM	clBackup		winclient	32:265		Detected file activity anomaly of type [Renamed Modified ] on the machine [winclient] in last 5 minutes.
💼 Jobs	16693	Major	741	Mar 30, 7:01 AM	clBackup		winclient	32:265		Number of files Modified [1002] Deleted [0] Renamed [1000] and Created [1]. Please click <u>here</u> for more details.
Reports	16692	Major	741	Mar 30, 7:01 AM	elBackup		winclient	32.265		This client is a VMware hosted virtual machine with a
Monitoring	16691	Major	741	Mar 30, 7:01 AM	clBackup		winclient	32.265		This client is a VMware hosted virtual machine with a
Alerts	16690	Info	741	Mar 30, 7:01 AM	JobManager		COMMVAULT	19:1056		Job [741] has been automatically resumed. Client [wi
Events	16689	Info		Mar 30, 7:00 AM	MediaManager		COMMVAULT	32.43		MediaAgent [MAforAWS] is ready.

#### Unusual file activity: Details on the File Activity anomaly shows up here.

	${\bf Q}_{\rm c}$ Search or type / for a command					🗟 🗘 📰 🗆 🛓 admini
Filter navigation	Universal file potitivity in a	Inclosed 1.4 Affected			0	a III -
🛠 Guided setup	Unusual file activity 2 M				٩	C III :
📽 Dashboard	All File activity	File type				\$
C Protect	Name	File anomaly type	Detected time	File count	Tags	Actions
Activate	winclient	File activity	Mar 30, 7:29 AM	2003	No tags	()
Disaster recovery						Details
i Jobs						Delete anomaly Manage tags
Reports						Recover as VM
Monitoring						
Alerts						
Events						
Unusual file activity						
Approvals						
Storage						

Further breakdown shows created, renamed, deleted, and modified files.



6. To simulate malware containment and clean up the simulation tool, delete the ransomware simulation tool from the server.

	Q Search or type / for a command				₿4 #	🛓 admin2 🗸
Filter navigation  K Guided setup	Active jobs Job 745 - [Backup]				Suspend V	кііі 💬
📽 Dashboard	Overview Attempts Events Streams Re	tention				
B Protect	General		Progress			
🕏 Activate	General		Flogless			
Disaster recovery	Type Backup type	Backup Full	Start time Current phase	Mar 30, 2023, 11:01:39 AM Backup		
i Jobs	Status	Running	Progress	7	\$	
Reports	Job started by Encryption enabled System state	admin2 (Started interactively) No Yes	Elapsed time Last update time Current throughput	28 seconds Mar 30, 2023, 11:02:15 AM N/A		
Monitoring						
茎 Manage	Associations		Item status			
R Developer tools	Agent	Windows File System	No of objects backed up	0		
Workflows	Media agent Backup set	MAforAWS FileActivity	Failures	0 Folders, 0 Files		
Web console	Source client computer Subclient	winclient default	Data transferred on network Scanned objects No of objects qualified for backup	N/A 1 Folder(s), 1001 File(s) 1001		
	Plan	FileActivity DEMO				_

Note: Wipe out the source directory before performing a fresh restore of clean files.

Y Quick access Desktop ★ ↓ Downloads ★	Date modified	~		
		Туре	Size	
Downloads *			This folder is empty.	
• • • • • • • • • • • • • • • • • • • •				
🖺 Documents 🖈				
📰 Pictures 🛛 🖈				
FileActivity				
📜 RansomwareD				
🍤 This PC				
🧊 3D Objects				
📃 Desktop				
Documents				
🖶 Downloads				
👌 Music				
E Pictures				
💾 Videos				
👟 Local Disk (C:)				
🖆 DVD Drive (D:) SSS_				
🧼 Network				
🧢 tsclient				
S WINCLIENT				
0 items				

- 7. From the unusual file activity dashboard, select **Recover Files**.
- 8. Proceed to restore.

**Note**: Ensure that the files were recovered with the most recent valid version and that there has been no reinfection since the ransomware was deleted from backups.

Restore: Getting back the clean files from last backup.

	Q Search or type / for a command					Restore options			
Filter navigation	File servers * / winclient / Backup content					Destination	winclient		
🛠 Guided setup		E	Restore Download 🖂			Restore	ACLS	🔽 Data	
2 Dashboard						Restore to original folder			
B Protect	FileActivity     [System State]	File N	Activity	Size	Modified	Destination path			Browse
Virtualization	♥ C: ♥ Users		System State]	14.85 GB	Mar 30, 7	oncontaining or crime in	t already exists		
Kubernetes	* Administrator	2 0	2	16.60 GB	Mar 29, 1	When the job completes, not	ify me via email		
File servers	V Desktop					- manual per competent int	ing the the circuit		
Databases									
Databases									
Laptops									
Office 365									
Office 365 Exchange									
Exchange									
Exchange Activate									
Exchange Activate Disaster recovery									
Exchange Activate Disaster recovery Jobs									
Exchange  CActivate  Disaster recovery  Jobs  Reports									
Exchange  Activate  Activate  Disaster recovery  Jobs  Reports  Monitoring									

**Note**: An additional option is available to browse and delete the infected file from the CommCell UI. You can download the infected files and the clean files to a separate location for further forensic analysis.

After restoration: Clean files are restored to the client. The encryption is removed and the file extension is restored to its original clean form.

ightarrow 🔶 🕆 Yile	Activity				~ U	Search FileActivity
	Name	Date modified	Туре	Size		
Quick access	FileGen 99927735334	3/29/2023 11:29	BIN File	17,409 KB		
	FileGen 99878638540	3/29/2023 11:29	BIN File	17,409 KB		
Downloads	FileGen 99638568977	3/29/2023 11:29	BIN File	17,409 KB		
Documents 🖈	FileGen 99534119015	3/29/2023 11:29	BIN File	17,409 KB		
E Pictures 🖈	FileGen 99441740132	3/29/2023 11:29	BIN File	17,409 KB		
FileActivity	FileGen 99384946069	3/29/2023 11:29	BIN File	17,409 KB		
RansomwareD	FileGen 99243719498	3/29/2023 11:29	BIN File	17,409 KB		
This PC	FileGen 99175659812	3/29/2023 11:29	BIN File	17,409 KB		
	FileGen 99010716836	3/29/2023 11:29	BIN File	17,409 KB		
3D Objects	FileGen 98 EileGen 991756598	12 - Notepad				- 0
Desktop	FileGen 98 File Edit Format View					
Documents	FileGen 98 Hello World !!	м нер				
Downloads	FileGen 98 Hello World !! I	Hello World !!				
Music	FileGen 98 Hello World !! I	Hello World !! Hello	World !!			
Pictures	FileGen 98 Hello World !!	Halla Hanld II				
Videos	FileGen 98     Hello World !!       Hello World !!	Hello World !! Hello	World !!			
Local Disk (C:)	FileGen 98. Hello World !!					
DVD Drive (D:) : SS	FileGen 98 Hello World !! I					
_ 010 0iiic (0.) .00_	FileGen 98 Hello World !! I FileGen 97 Hello World !!	Hello World !! Hello	World !!			
Network		Hello World !!				
🤜 tsclient	FileGen 97 Hello World !! I	Hello World !! Hello	World !!			
S WINCLIENT	FileGen 97 Hello World !!					
	FileGen 97 Hello World !! I FileGen 97 Hello World !! I Hello World !! I	Hello World !! Hello World !! Hello !	World II			
	FileGen 97     Hello World !!     FileGen 97     Hello World !!		10110 11			

Additionally, the following option is available:

#### Clear Anomaly:

	Q Search or type / for a command						🗟 🗘 🔛 上 admin2
Filter navigation	1 row(s) selected 🛛 Show selected	Clear all	Delete anomaly		×	Delete anomaly Recover as vm Q	c 🖬 i
笑 Guided setup 建 Dashboard	All File activity File type						0
B Protect	+ Add the	File anomal	Servers	winclient		Tegs	Actions
<ul> <li>Activate</li> <li>Disaster recovery</li> </ul>	winchant	File activity	Anomaly types	File activ 🔘	(1) -	No taga	
Jobs					CANCEL DELETE		
Reports							
Monitoring							

For further forensic investigation and clean-up of infected files, the following options are available:

- Download
- Delete

COMMVAULT 🕲	Q Search or type / for a command				🖻 🗘 📰 🛛 🛓 adm
Filter navigation	File servers + / winclient / Backup content				
🛠 Guided setup	Backup content	Restore Download (1)		Showing backup from 2023-03-27 06:1	2 to 2023-03-30 06:12 V Q. Search for files
📽 Dashboard		Hide deleted items		showing backup from 2023-03-27 06.1	C to 2023-03-00 06:12 V Q Search for files
C Protect	FileActivity     [System State]	FileActivity at View versions	or / Desktop / FileActivity / f1 Size	Modified time	Backup time
Virtualization	V C:	COMMV. Show hidden items	127.85 KB	Mar 28, 10:59 AM	Mar 29, 8:21 AM
Kubernetes	Users     Administrator	CVRansonwareamurator.exe	393.50 KB	Nov 8, 2022 2:38 PM	Mar 29, 8:21 AM
File servers	Desktop     FileActivity	FileGen 100074377288.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Databases	v fi	FileGen 100135210821.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Laptops	▶ f2 ▶ f3	FileGen 100282337436.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Office 365		FileGen 10035445934.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Exchange		FileGen 100446768838.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Activate		FileGen 100549302036.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Disaster recovery		FileGen 10061644432.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Jobs		FileGen 100787153470.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
		FileGen 100885759151.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Reports		FileGen 100919465983.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM
Monitoring		FileGen 10098130210.bin.cvencry	14 MB	Mar 28, 10:58 AM	Mar 29, 8:21 AM

# Conclusion

This end-to-end ransomware solution follows a multilayered approach complying with the NIST cyber security framework. The ability to support layered defenses for securing datasets against ransomware ensures that your organization benefits from a sound cyber recovery-ready architecture. The addition of object locking, and the immutability feature of AWS further strengthens this solution.