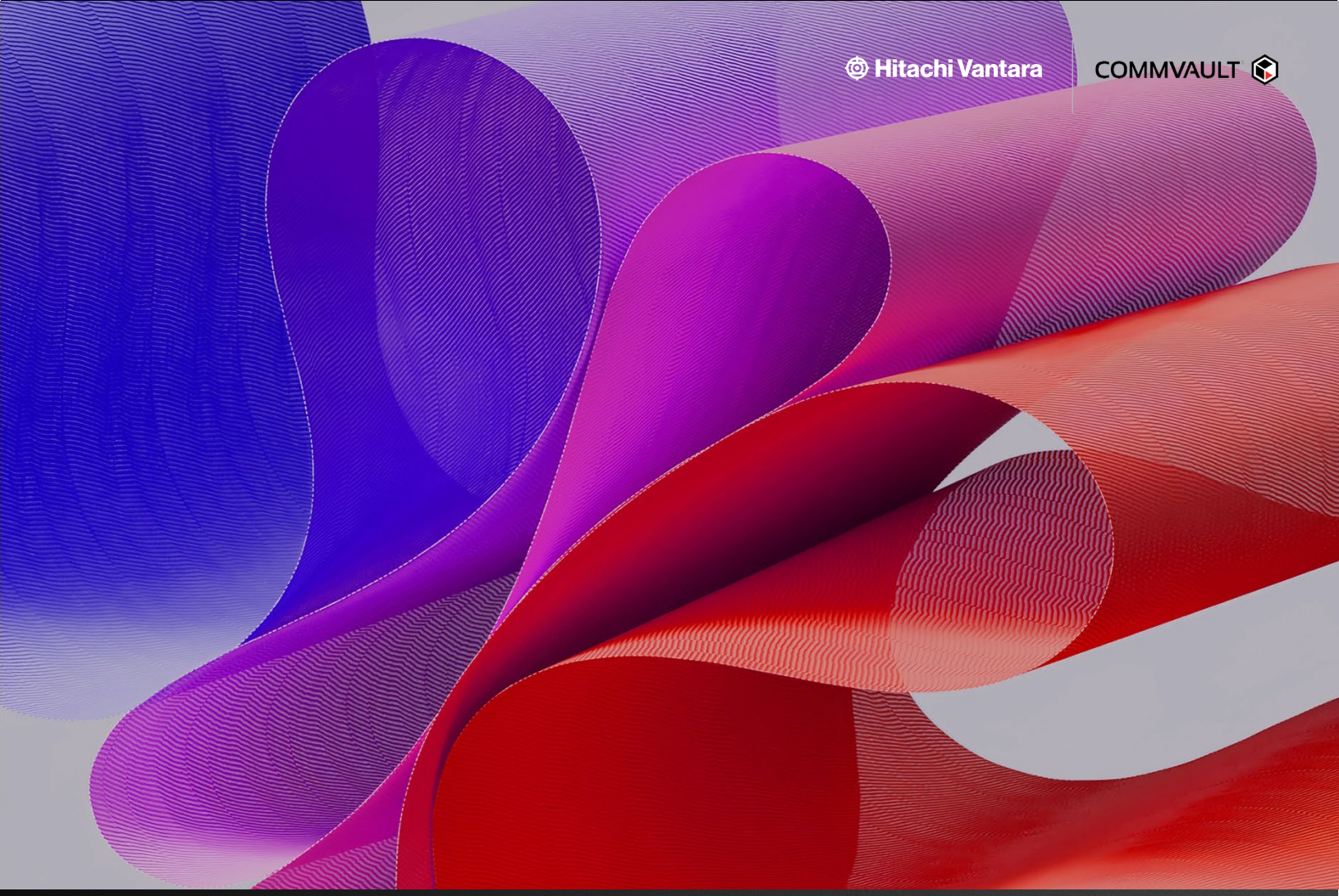


Ransomware Defense Strategy with HDPS and AWS Immutability

Using Hitachi Cloud Connect for Equinix

Hitachi Vantara
March 2024

© Hitachi Vantara LLC 2024. All Rights Reserved.

Hitachi Vantara

Table of Contents

Notices and Disclaimer 2

About This Guide 3

Intended Audience 3
Value Proposition 3
Document Revisions 3
References 3
Comments 4

Executive Summary 5

Introduction 6

Solution Overview 7

Business Benefits 7
Objective 7
Key Components 7

Validation 8

Validation Method 8
High Level Diagram 8
Hardware and Software 9
Test Scenarios 10

Validation Results 11

Test 1: Prepare the Environment 11
Test 2: Install and Configure HDPS 12
Test 3: Secure and Harden the Components 16
Test 4: Simulate Ransomware Infection and Recovery 24

Conclusion 32

© Hitachi Vantara LLC 2024. All Rights Reserved.

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™ 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.

© Hitachi Vantara LLC 2024. All Rights Reserved

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: https://www.nist.gov/cyberframework
- HDPS documentation: https://documentation.commvault.com/2022e/expert/7877_ransomware_protection_01.html
- For details on WORM and immutability feature of AWS: https://aws.amazon.com/s3/features/object-lock/

© Hitachi Vantara LLC 2024. All Rights Reserved

Comments

Send any comments on this document to GPSE-Docs-Feedback@hitachivantara.com. 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.

© Hitachi Vantara LLC 2024. All Rights Reserved

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™ (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™ 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: https://hitachivantara.com/en-us/products/storage/flash-storage/cloud-connect-for-equinix.html.

© Hitachi Vantara LLC 2024. All Rights Reserved

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.

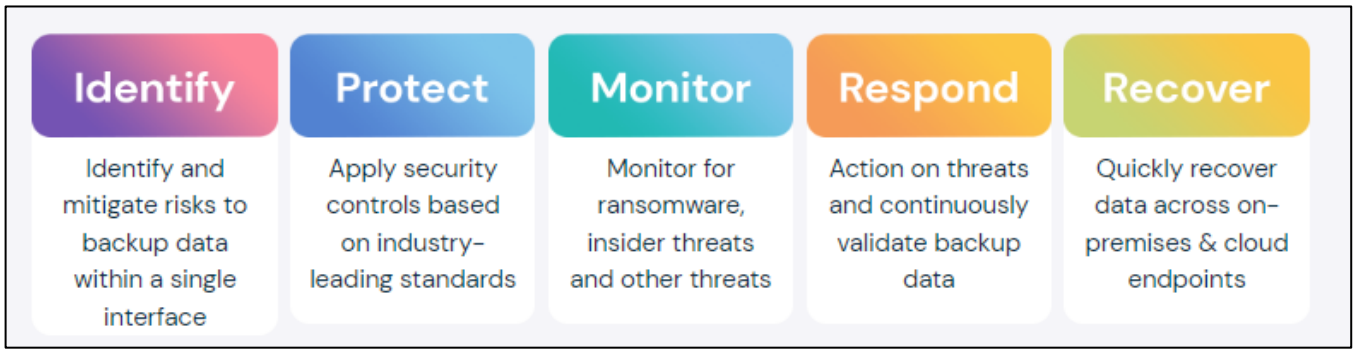
What is ransomware protection?

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.

© Hitachi Vantara LLC 2024. All Rights Reserved

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.

© Hitachi Vantara LLC 2024. All Rights Reserved

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.

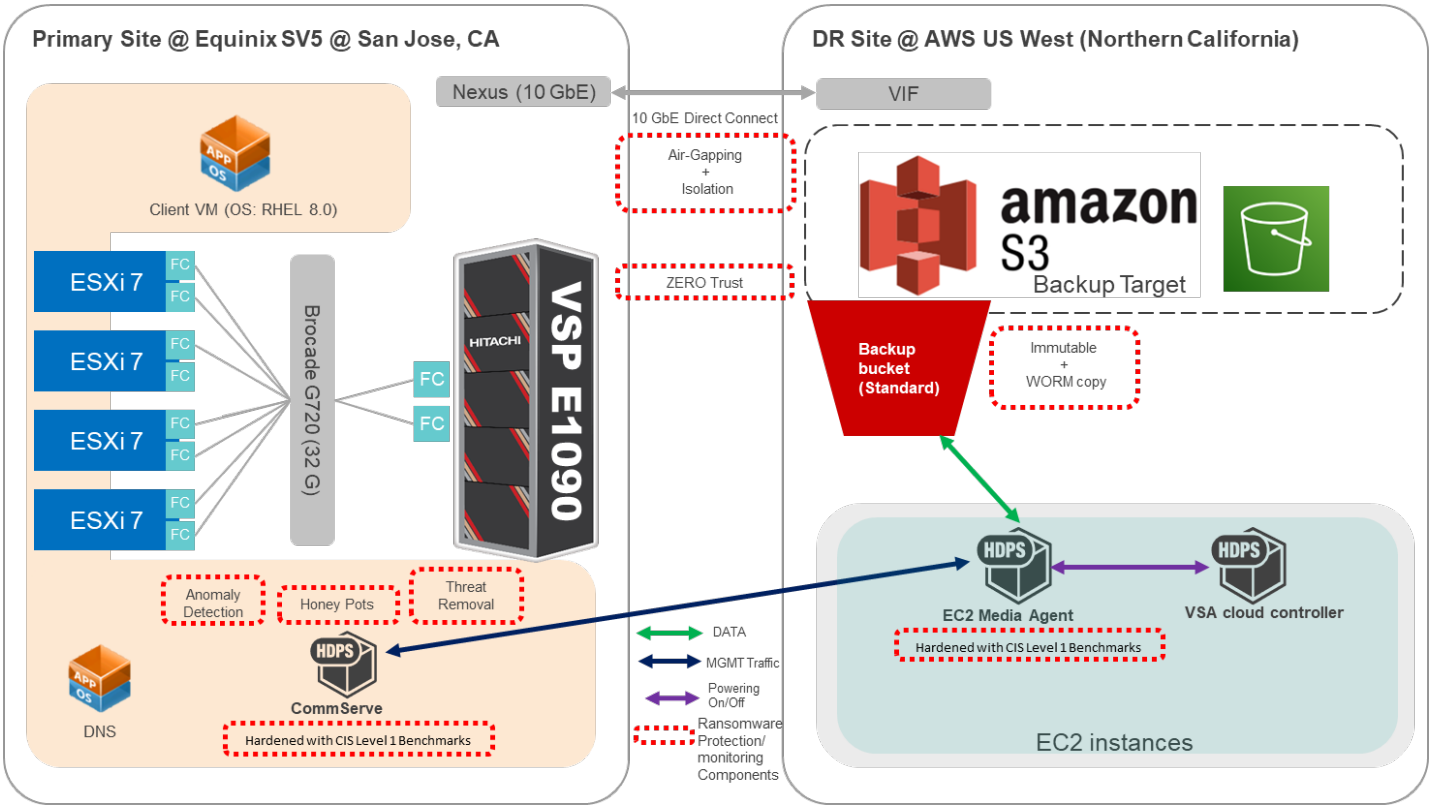


Figure 1: *High Level Diagram*

© Hitachi Vantara LLC 2024. All Rights Reserved

Hardware and Software

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

	Item	Description	Version	Function
Equinix Near-Cloud Data Center	**Hitachi VSP E1090**	1,024 GB cache (2) 32-core MPUs (3) RAID6 6D+2P parity groups (2) 32 Gbps FC ports	SVOS RF 9.8.1 93-06-21-80/00	Storage for source client and CommServe backup repository.
	Hitachi Advanced Server DS220	(2) 18-core Intel Xeon Gold 6140 @ 2.3 GHz 128 GB cache Emulex LPe32002 HBA Intel Ethernet Network Adapter XXV710	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.
	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.
	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 West (North California)	**MediaAgent on AWS EC2**	(1) 300 GB EBS volume (1) 2 TB EBS volume NOTE: AMI located at aws-marketplace/Commvault Linux FR28 Cloud Data Manager-c3fdde77-53ca-46ca-9ae7-20256d9e9899	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.
	VSA Proxy on AWS EC2	(1) 300 GB EBS volume (1) 2 TB EBS volume NOTE: AMI located at aws-marketplace/Commvault Linux FR28 Cloud Data Manager-c3fdde77-53ca-46ca-9ae7-20256d9e9899	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*

© Hitachi Vantara LLC 2024. All Rights Reserved

Test Scenarios

Table 3 lists the test scenarios performed in the validation.

#	Description	Success Criteria
1	Prepare the environment: 1. Deploy one Windows Server 2019 virtual machine in the near-cloud data center to act as backup source client. 2. Provision storage from the VSP E1090 storage system to CommServe and source client. 3. In AWS, deploy two RHEL 8.7 EC2 instances for the MediaAgent and VSA. 4. Set up the AWS S3 bucket. **Note**: Steps 1-3 are common operations; therefore, they are not documented in the Validation Results section.	Environment is set up as per specifications.
2	Install and configure HDPS: 1. Deploy CommServe by downloading and installing OVA "CIS L1 hardened Commserver 11.28" as a virtual machine. Download link: https://store.commvault.com/webconsole/softwarestore/#!/130/704/25600. 2. Deploy MediaAgent on an AWS EC2 instance. **Note1**: Use the BYOL custom image that is available in the AWS Marketplace. See https://documentation.commvault.com/2022e/essential/43647_installing_and_configuring_new_mediaagent.html. **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). 3. Add a 300 GB EBS volume to the MediaAgent to serve as a DDB disk. 4. Register the MediaAgent with CommServer. Ensure that Commserve and MediaAgent are on the same code level. Otherwise, the registration fails. 5. Install and configure VSA cloud provider. 6. Configure the AWS S3 bucket.	Installed and configured successfully.
3	Secure and harden the components: 1. After deploying the hardened CommServe through the OVA, verify whether ransomware protection is enabled. 2. Harden the MediaAgent virtual machine based on CIS Level 1 standards. 3. Harden the VSA cloud provider virtual machine based on CIS Level 1 standards. 4. Secure the AWS S3 bucket by enabling Object Lock and Retention.	Environment is hardened based on the NIST guidelines.
4	Simulate ransomware infection and recovery: 1. Prepare the backup client for the ransomware simulation. 2. Install and configure the ransomware simulation tool. 3. Prepare a set of files. 4. Simulate a ransomware attack on the files. 5. After the ransomware simulation, verify that anomaly alerts are reflected in CommServe. 6. Restore the original, clean files.	Generates anomaly alerts after ransomware simulation and restores clean files.

© Hitachi Vantara LLC 2024. All Rights Reserved

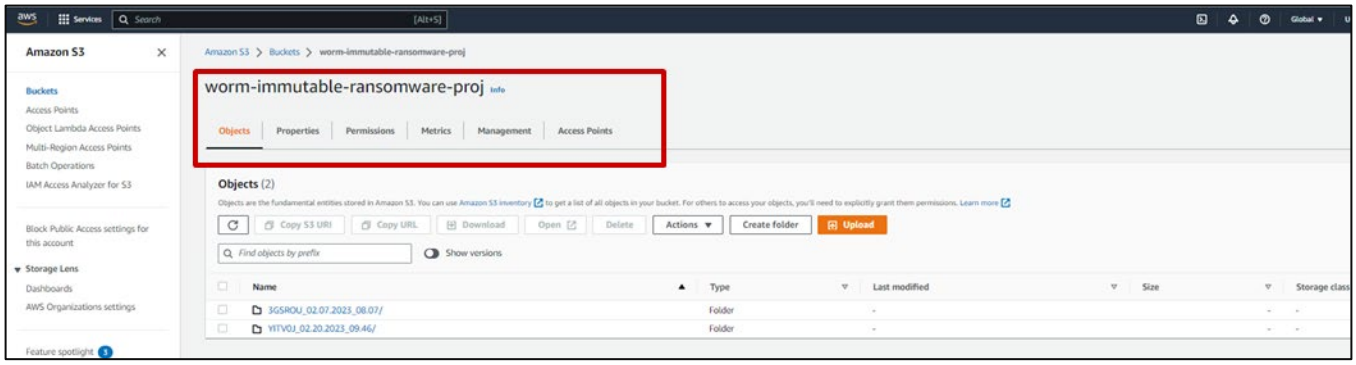
Validation Results

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:



Bucket properties:

© Hitachi Vantara LLC 2024. All Rights Reserved

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.

```
[ec2-user@10 ~]$ sudo su
[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
Status:       Subscribed

[root@10 ec2-user]#
[root@10 ec2-user]#
[root@10 ec2-user]#
[root@10 ec2-user]# sudo su
[root@10 ec2-user]#
[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 ClientGroup Name :
Enter CS Name : commvault
Enter CS Hostname : 172.23.30.212
Enter CS Username : admin2
Enter CS Password :
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
```


© Hitachi Vantara LLC 2024. All Rights Reserved

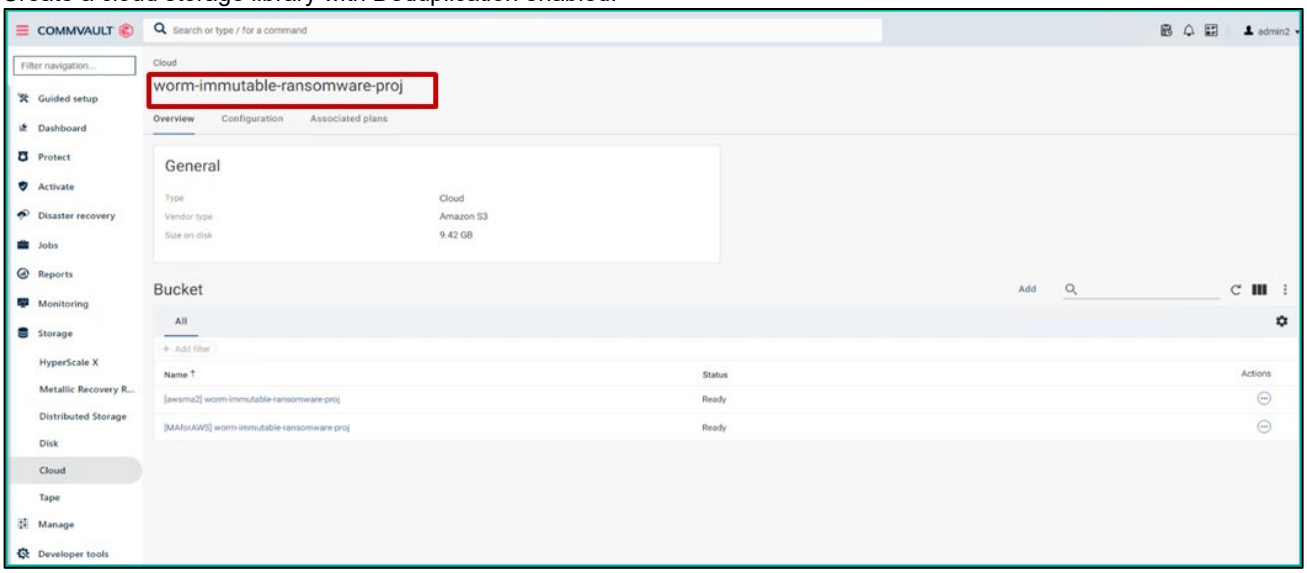
```
TERM=xterm
SHLVL=1
LOGNAME=root
PATH=/sbin:/bin:/usr/sbin:/usr/bin
HISTSIZE=1000
_=/bin/env
Redirecting starting service for Instance001 to systemd ...
Running "systemctl start commvault.Instance001.service" ...
Waiting 60 seconds for cvd to settle....
/etc/init_frel_cloud: line 663:
retryCt=2
if [ -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 ...
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 "systemctl start commvault.Instance001.service" ...
Client registration for auto CV deployment complete!
[root@10 etc]#
```

Add Cloud Storage to CommServe

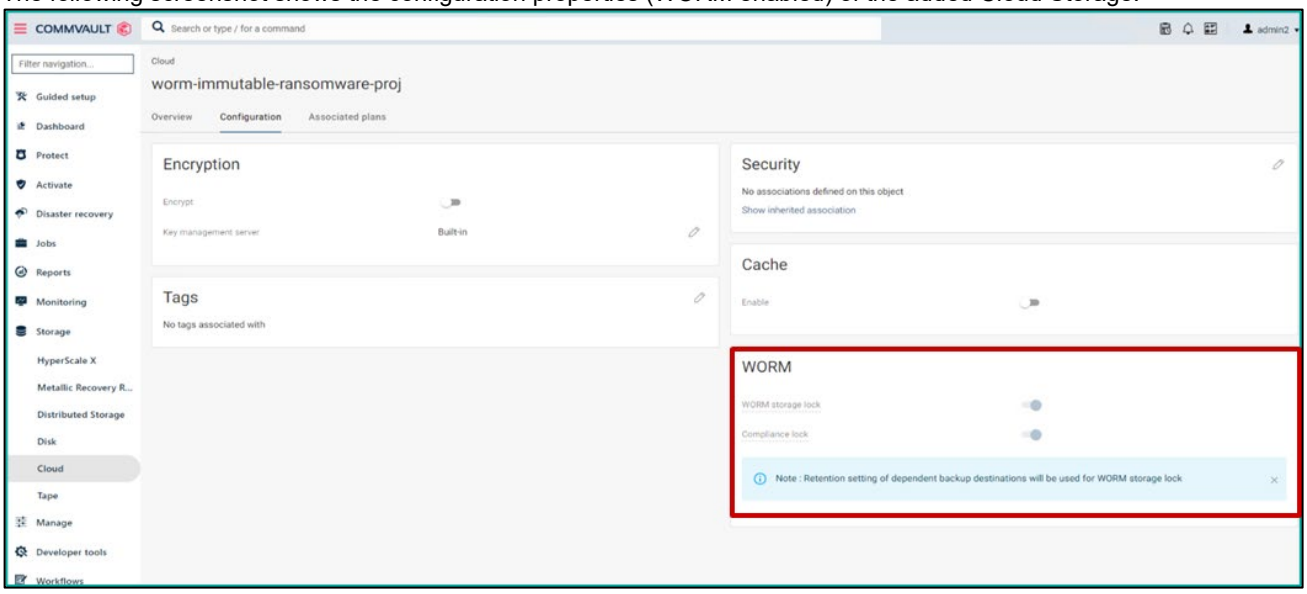
To create storage libraries in the Command Center, complete the following steps:

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.



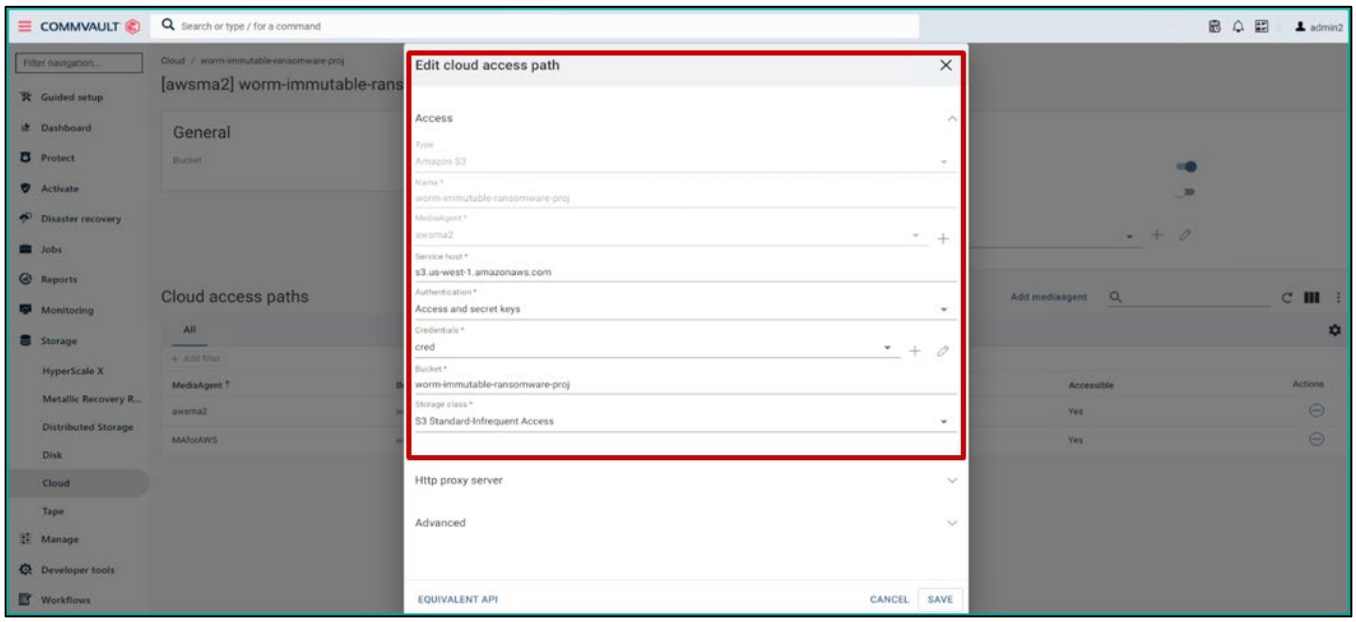
© Hitachi Vantara LLC 2024. All Rights Reserved

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



Discover S3 Bucket in CommServe

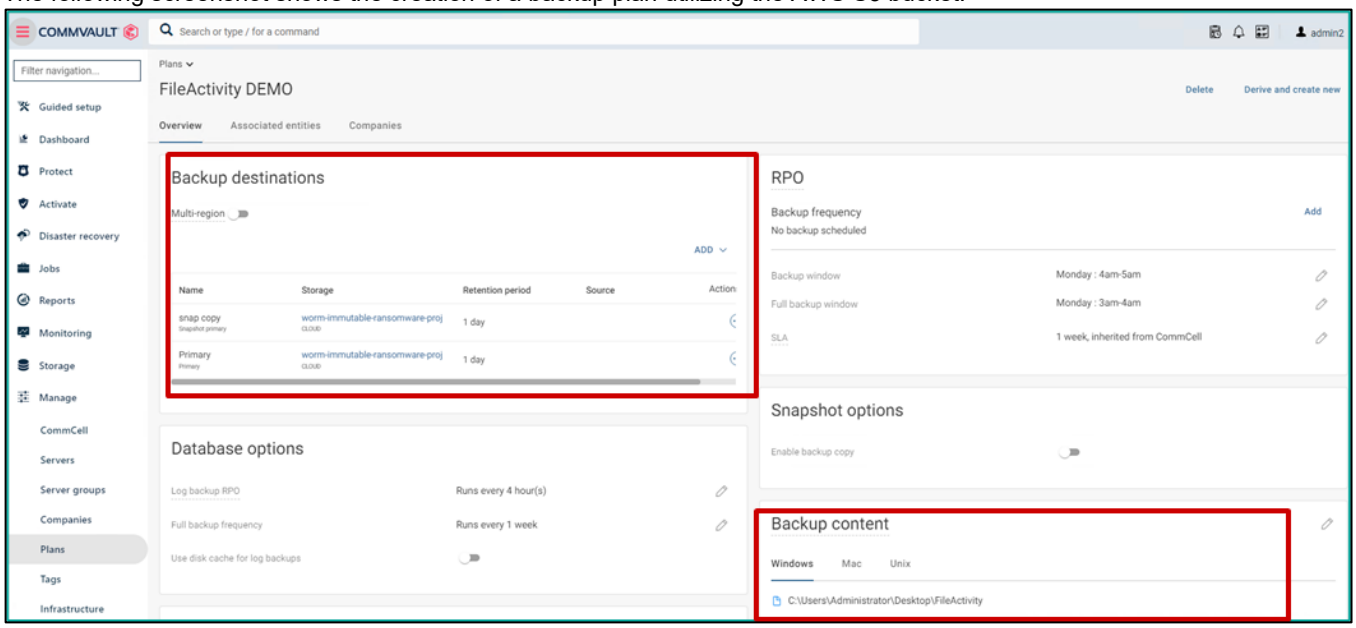
The AWS S3 bucket is added as a cloud storage library:



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

© Hitachi Vantara LLC 2024. All Rights Reserved

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



© Hitachi Vantara LLC 2024. All Rights Reserved

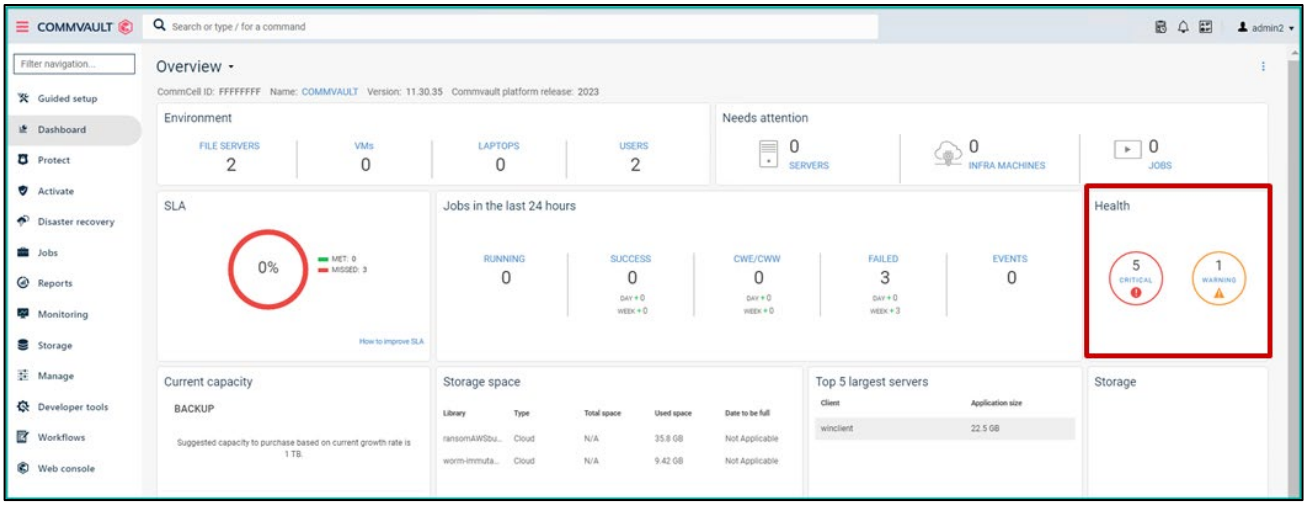
Test 3: Secure and Harden the Components

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.

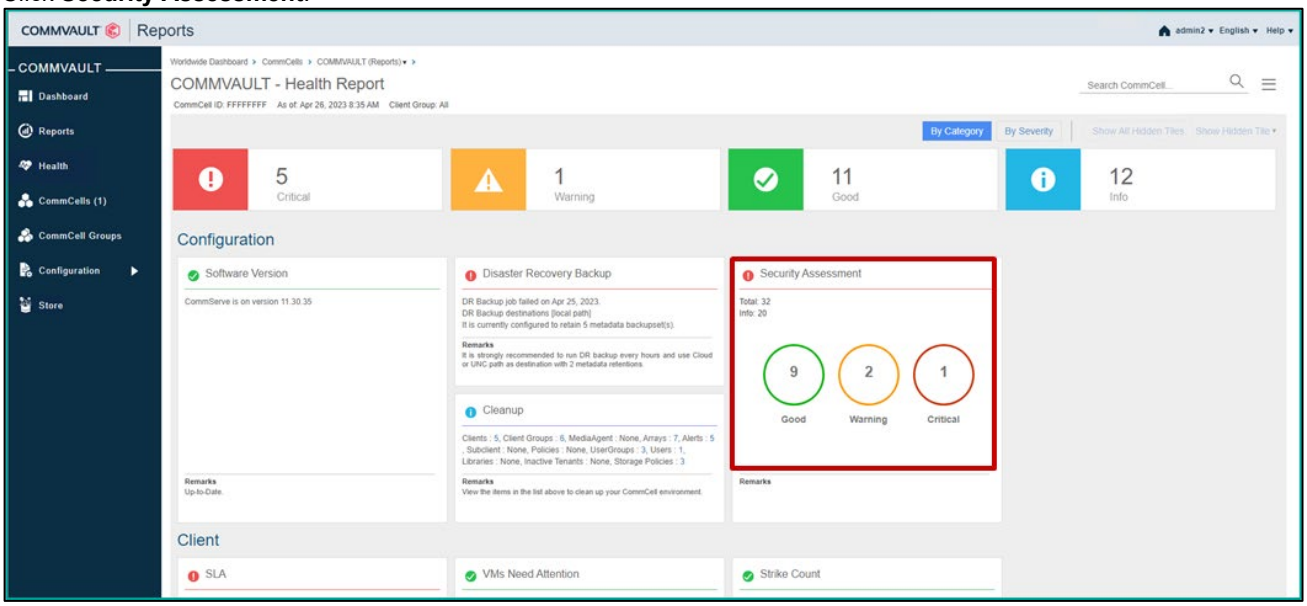
Identify: Mitigate Threats to Backup Data Through a Security Assessment

- 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**.

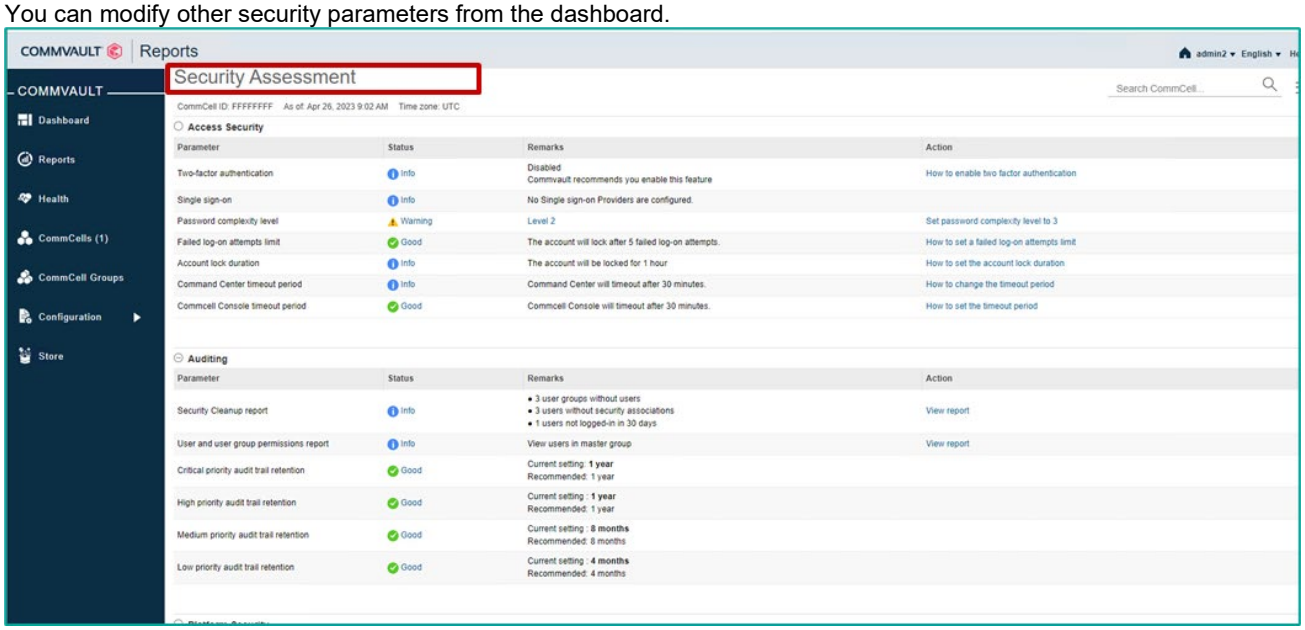


2. Click **Security Assessment**.



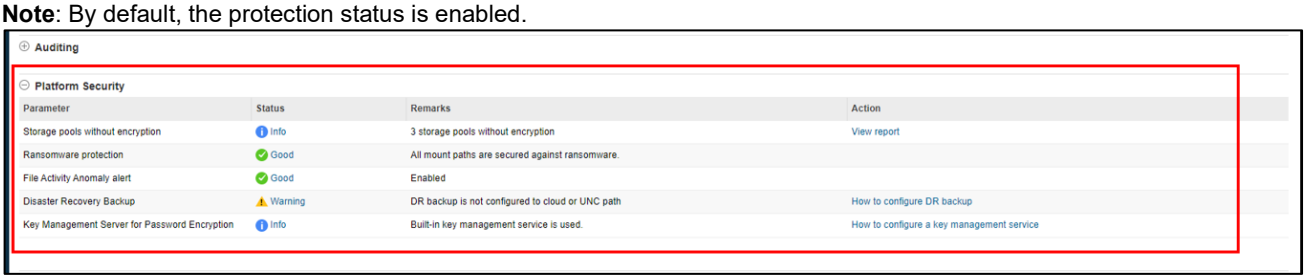
© Hitachi Vantara LLC 2024. All Rights Reserved

You can modify other security parameters from the dashboard.



Under Platform Security, the Ransomware Protection status shows Enabled.

Note: By default, the protection status is enabled.



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.

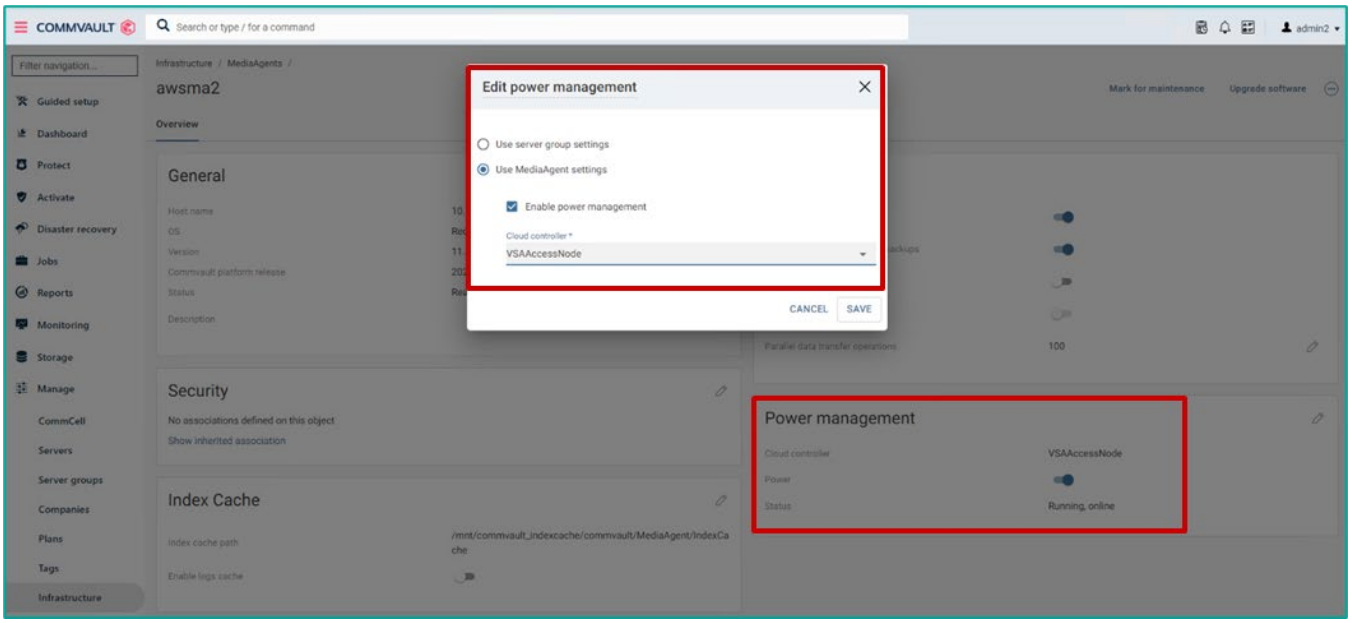
In this solution, we implemented air gapping using option 1.

For more information, see the following pages:

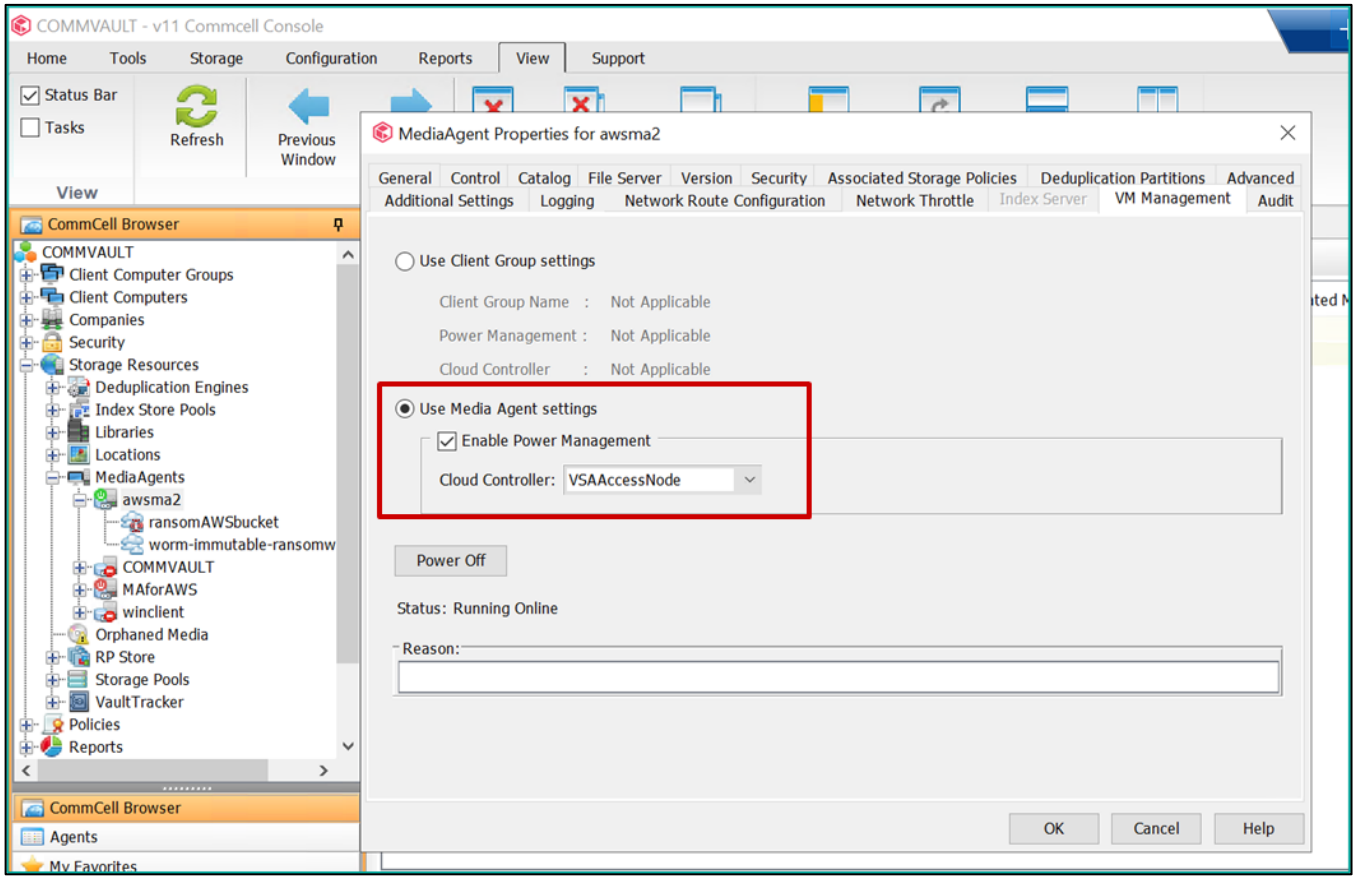
- https://documentation.commvault.com/2023/expert/151540_air_gapping_01.html
- https://documentation.commvault.com/2022e/essential/101313_cloud_mediaagent_power_management.html
- https://documentation.commvault.com/2022e/essential/101354_enabling_power_management_for_cloud_mediaagent.html

© Hitachi Vantara LLC 2024. All Rights Reserved

After implementation:



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



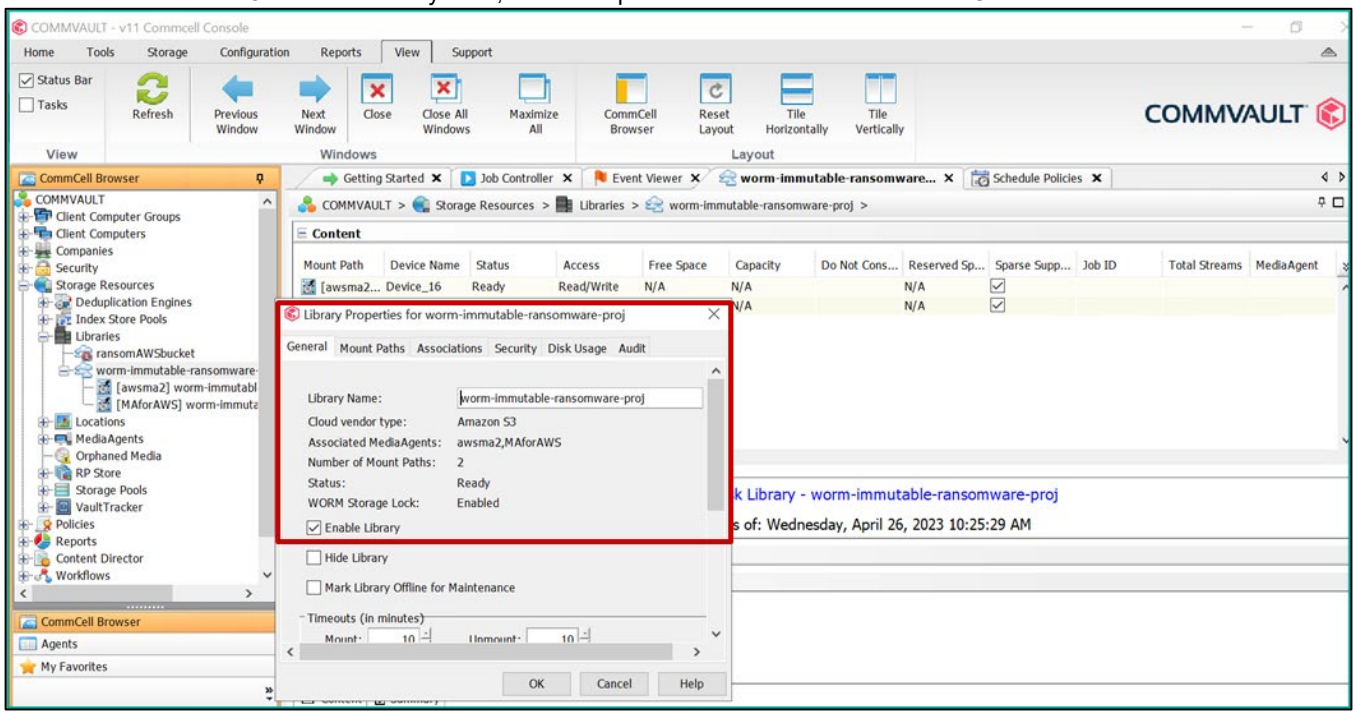
Enable WORM Copy

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

© Hitachi Vantara LLC 2024. All Rights Reserved

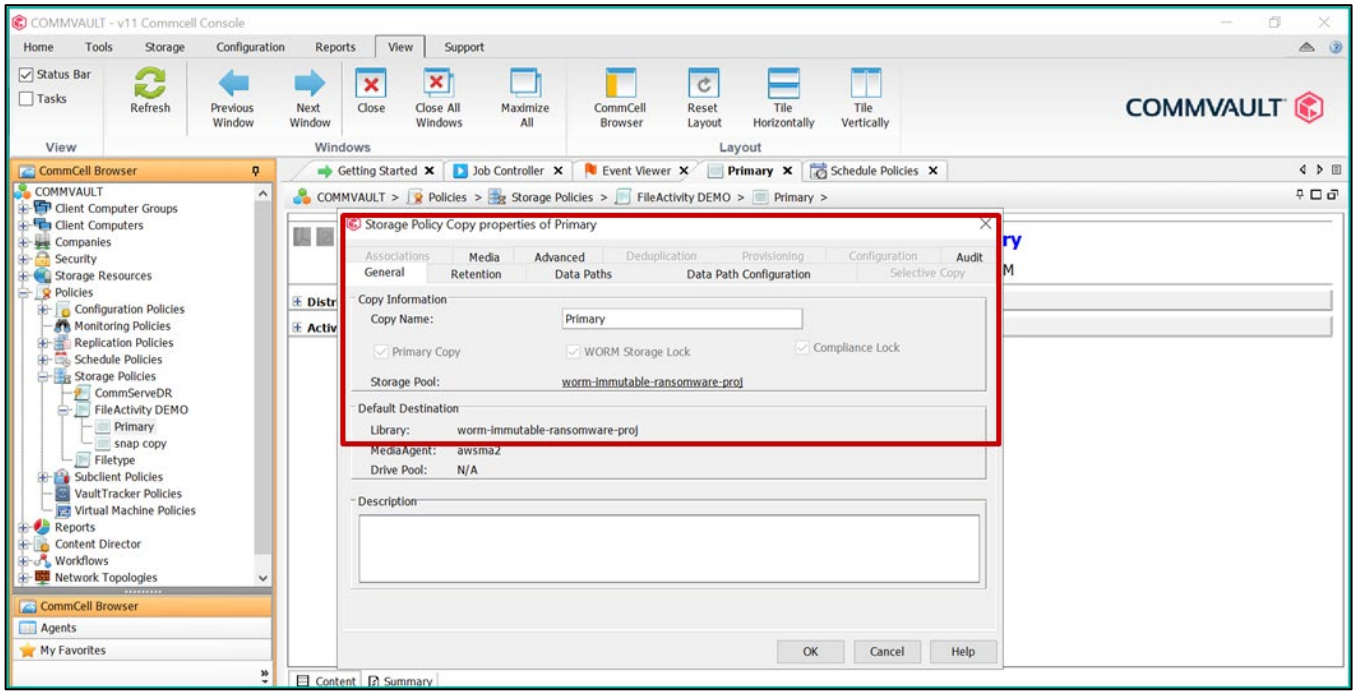
For instructions to enable WORM copy, see:
https://documentation.commvault.com/2023/expert/9251_configuring_worm_storage_mode_on_cloud_storage.html.

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



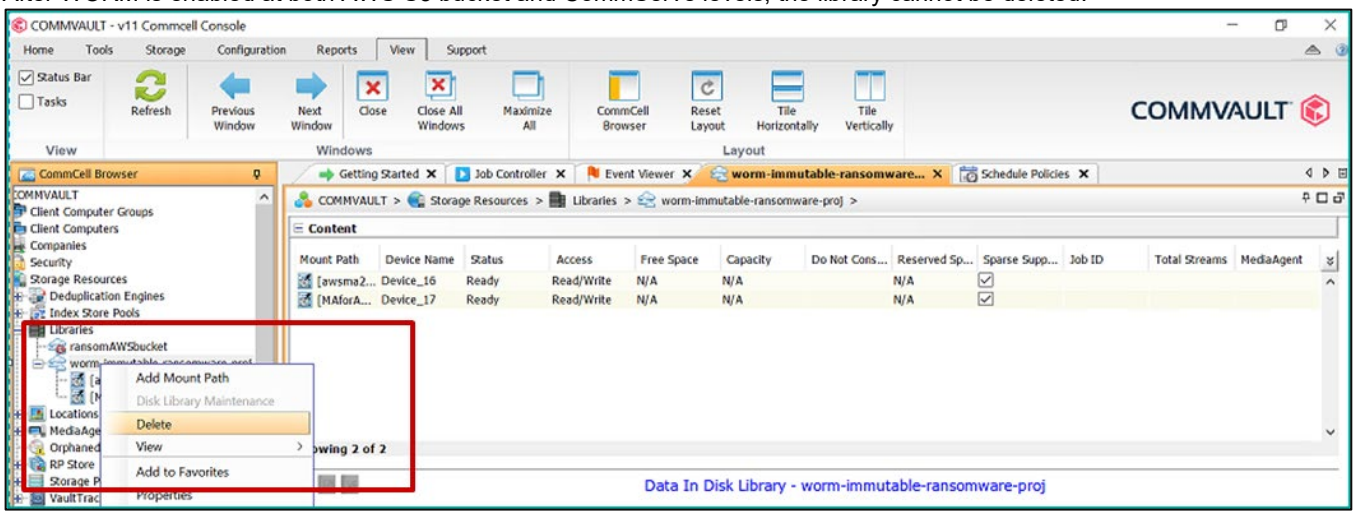
Note: For maximum protection at bucket level, use the Enable Worm Storage workflow on the cloud libraries instead of the ransomware workflow. Additionally, you can enable WORM Copy on a storage policy copy.

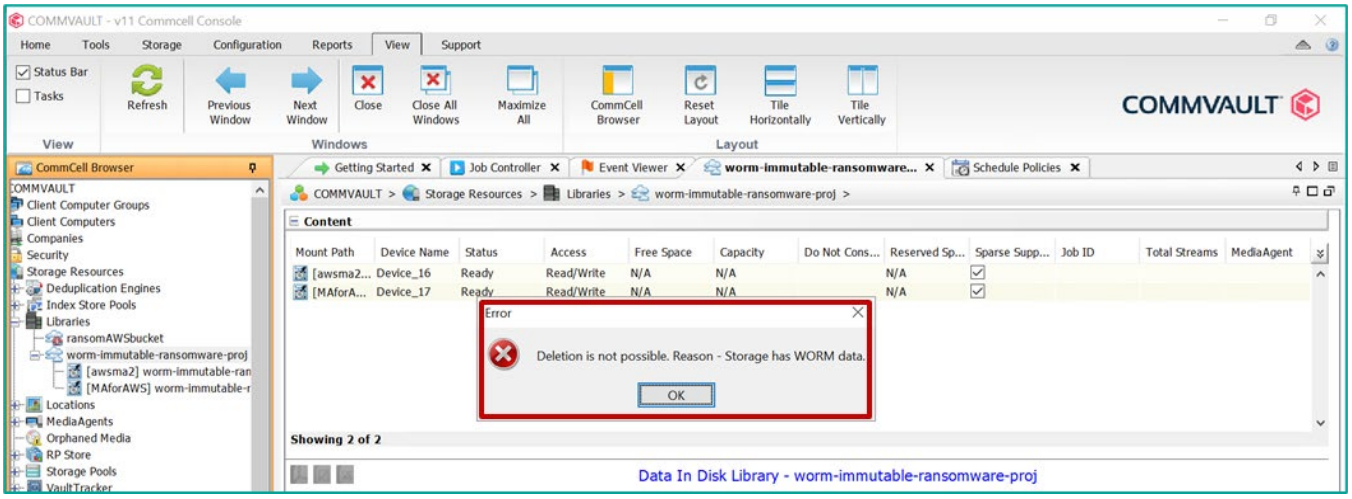
For more information, see:
https://documentation.commvault.com/2022e/expert/112844_enabling_worm_copy_on_storage_policy_copy.html.



© Hitachi Vantara LLC 2024. All Rights Reserved

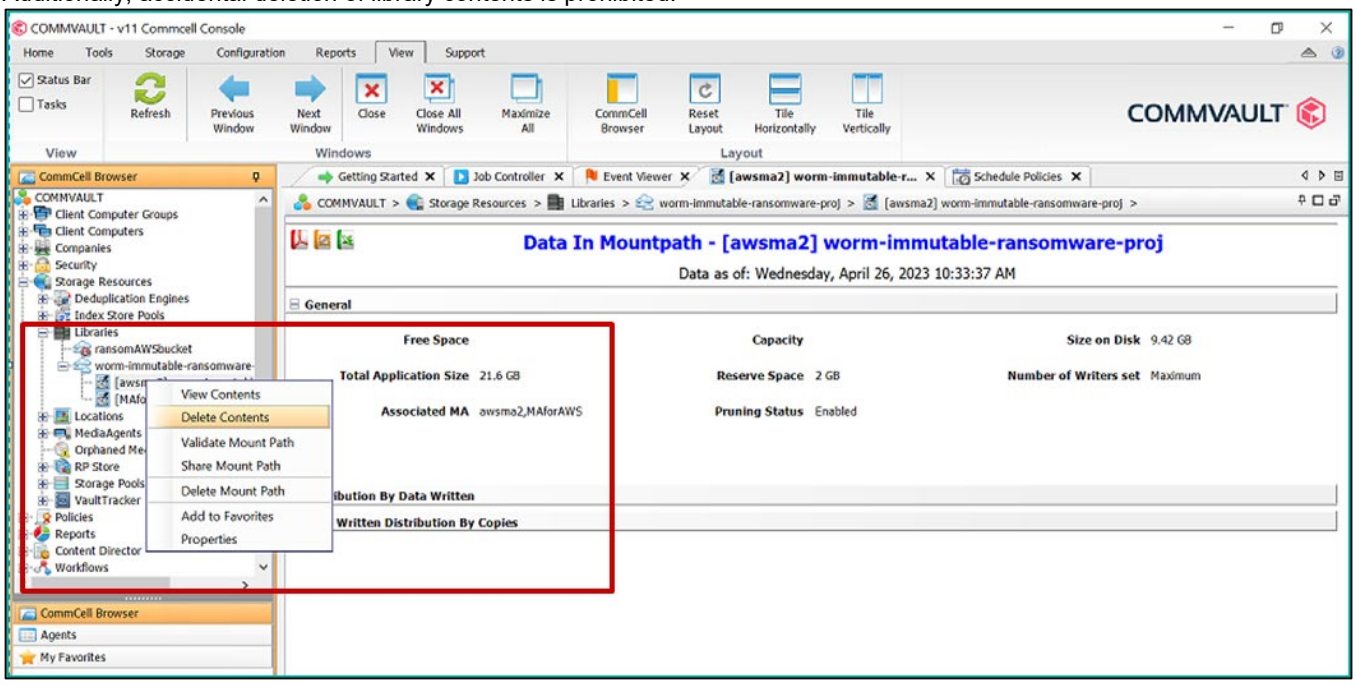
After WORM is enabled at both AWS S3 bucket and CommServe levels, the library cannot be deleted.

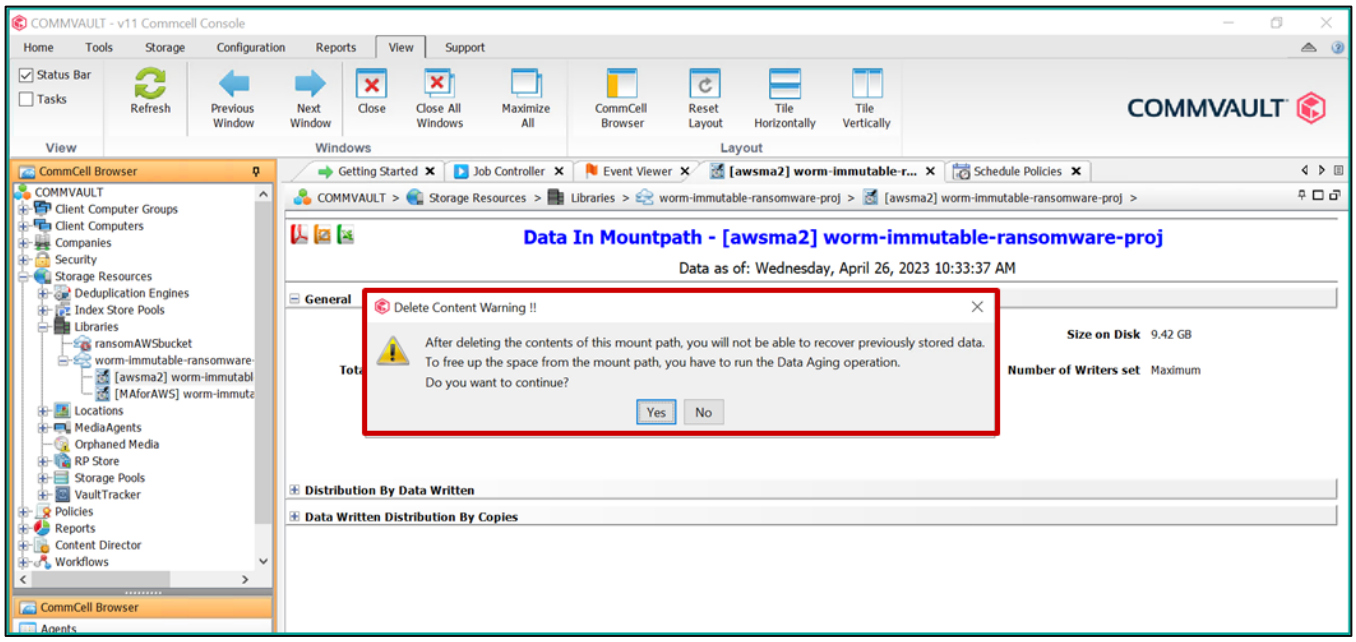




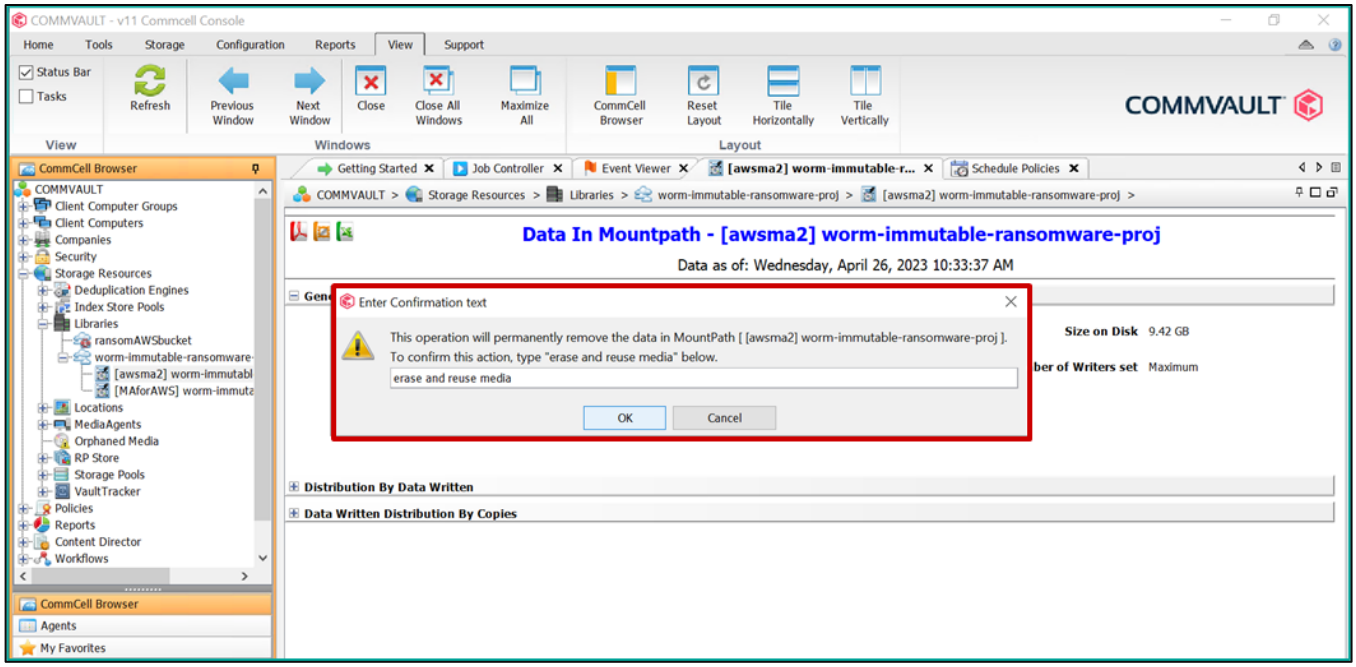
© Hitachi Vantara LLC 2024. All Rights Reserved

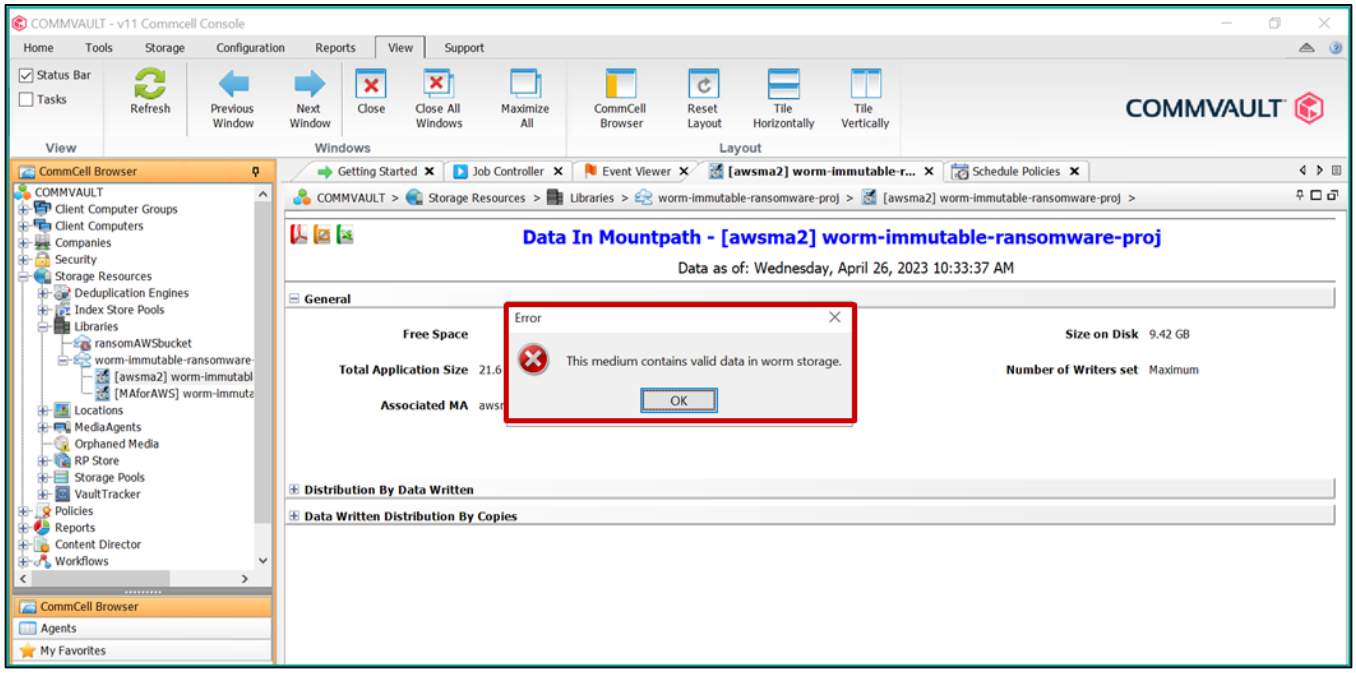
Additionally, accidental deletion of library contents is prohibited.





© Hitachi Vantara LLC 2024. All Rights Reserved





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.

© Hitachi Vantara LLC 2024. All Rights Reserved

- 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.

© Hitachi Vantara LLC 2024. All Rights Reserved

Test 4: Simulate Ransomware Infection and Recovery

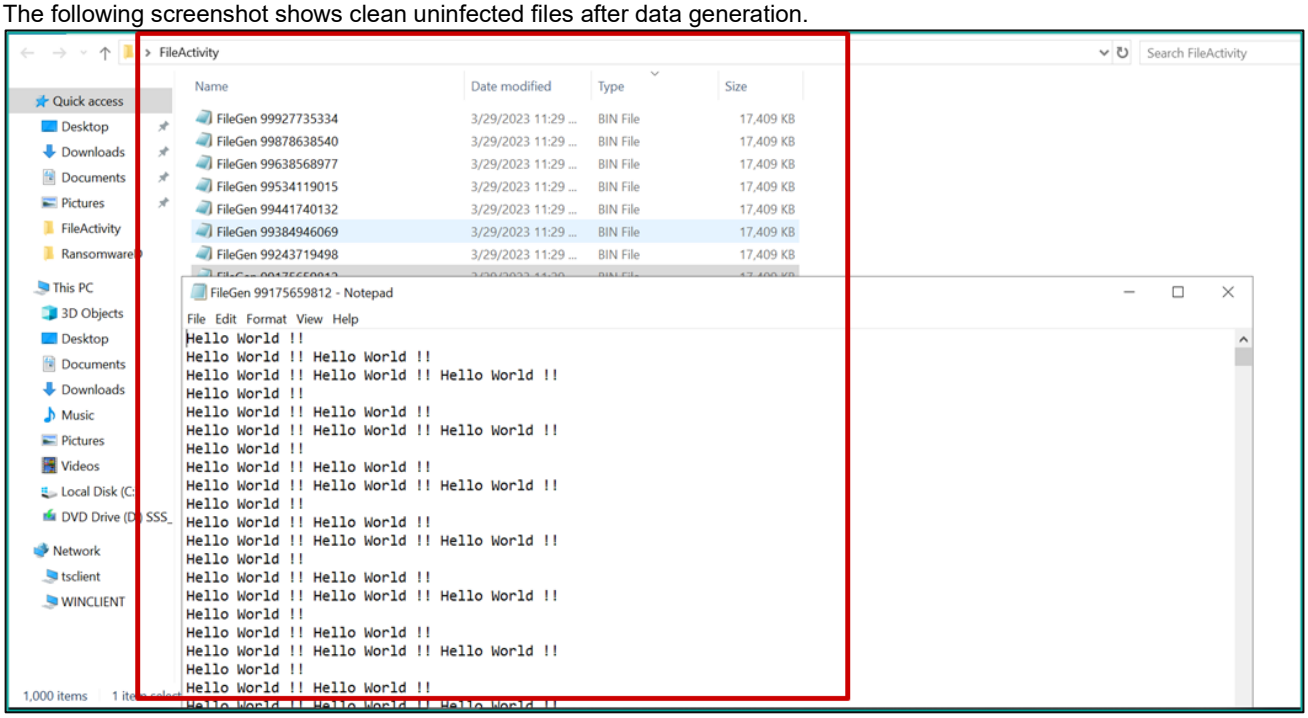
To validate the Monitor, Respond, and Recover pillars of the NIST framework, we used a ransomware simulator to generate File Activity anomalies.

Reproduce Activity Anomalies

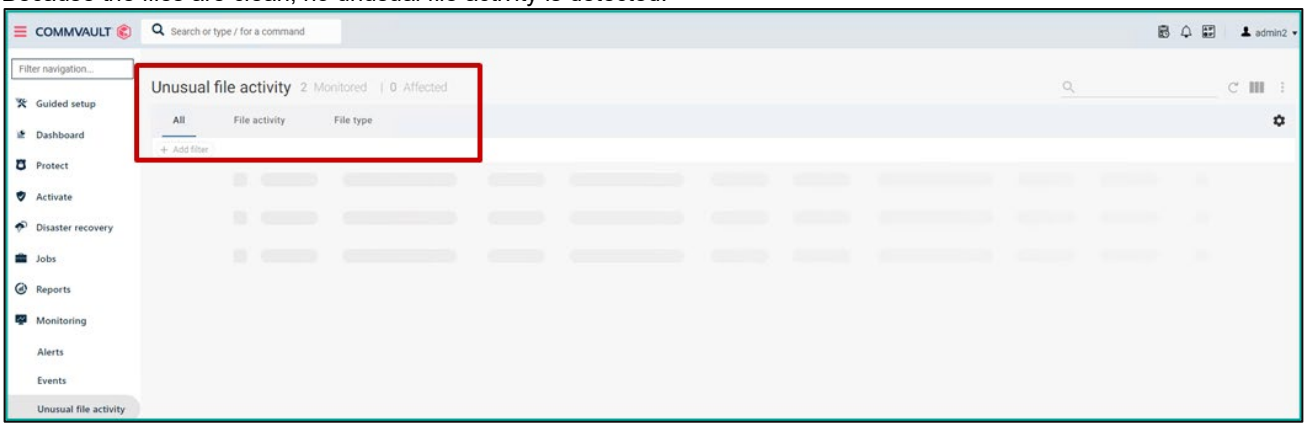
Run the Ransomware Simulation tool on the files you are backing up to encrypt them to simulate a ransomware attack. This triggers a file activity anomaly.

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.

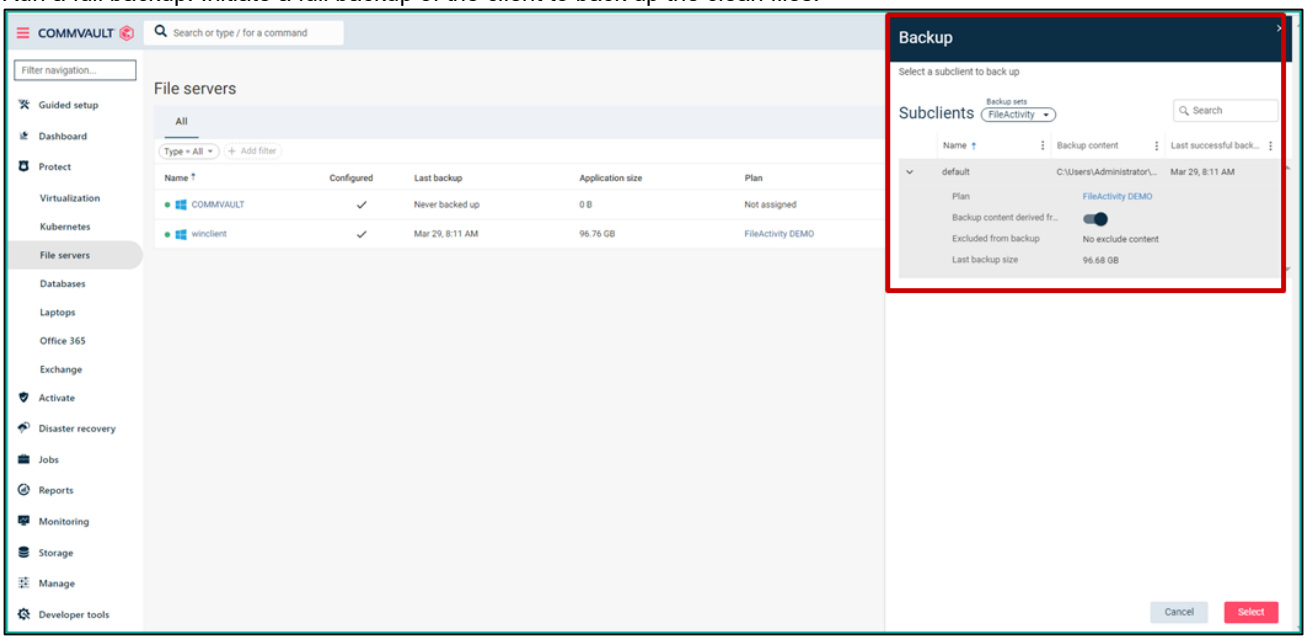


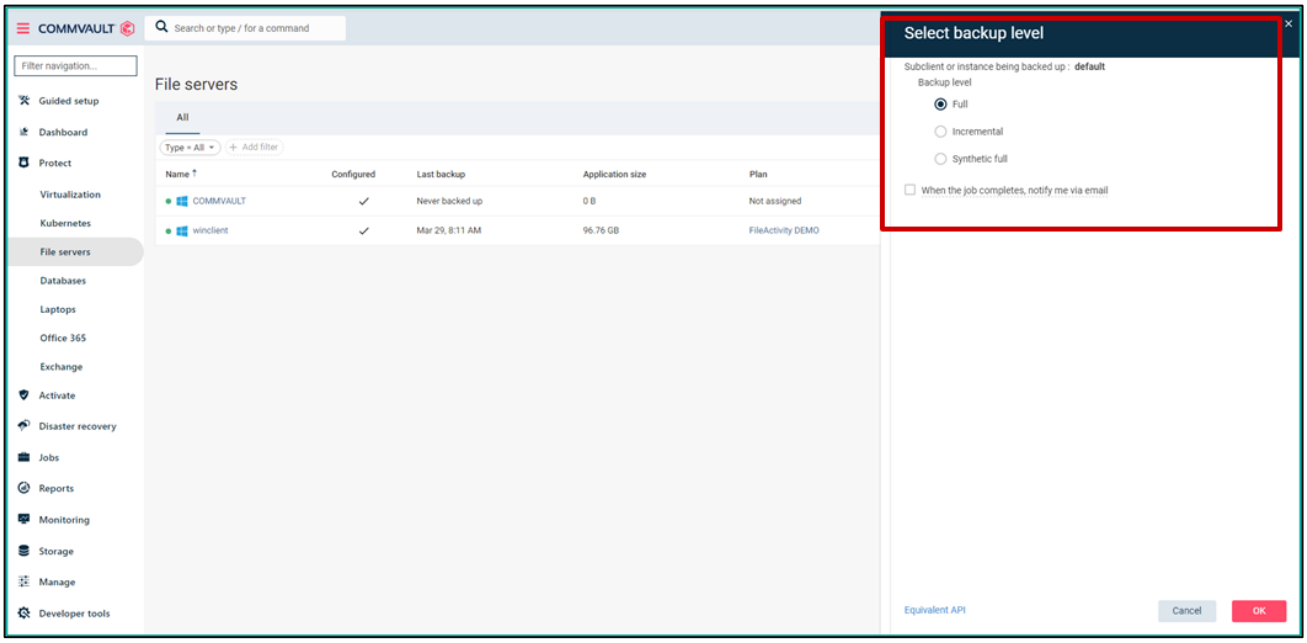
Because the files are clean, no unusual file activity is detected.



© Hitachi Vantara LLC 2024. All Rights Reserved

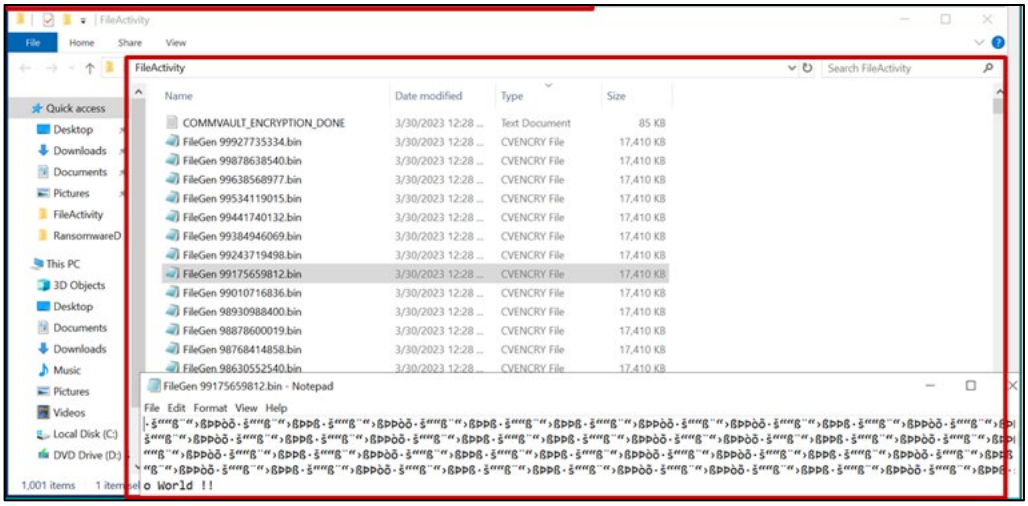
3. Run a full backup: Initiate a full backup of the client to back up the clean files.





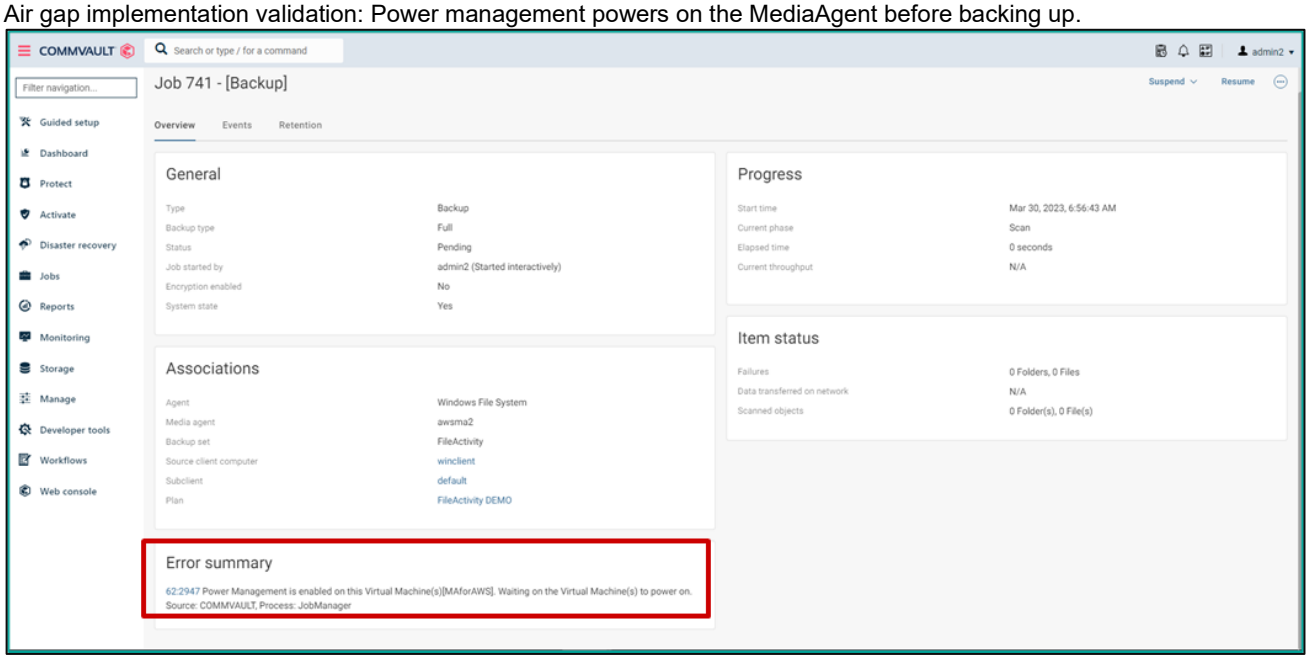
4. Reproduce activity anomaly by encrypting the contents using the ransomware simulation tool.

© Hitachi Vantara LLC 2024. All Rights Reserved

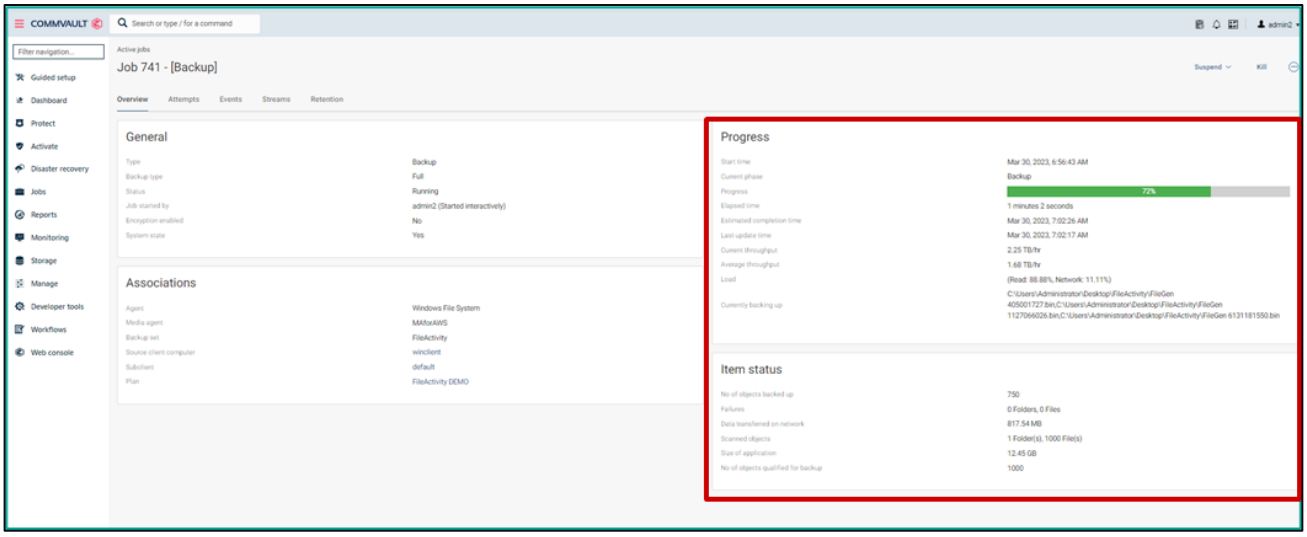


5. Verify air gap implementation and run another full backup job to protect the encrypted files.

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

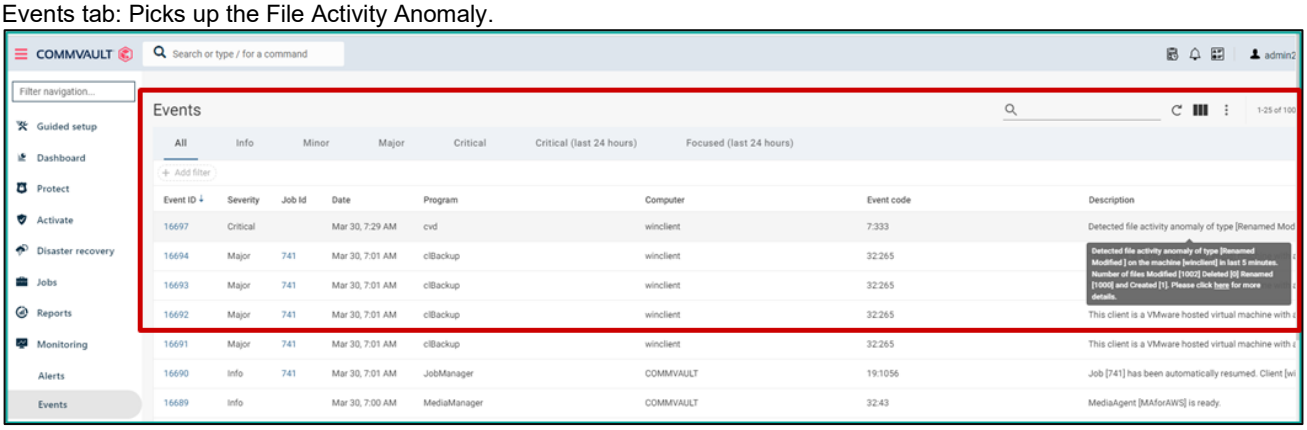


© Hitachi Vantara LLC 2024. All Rights Reserved

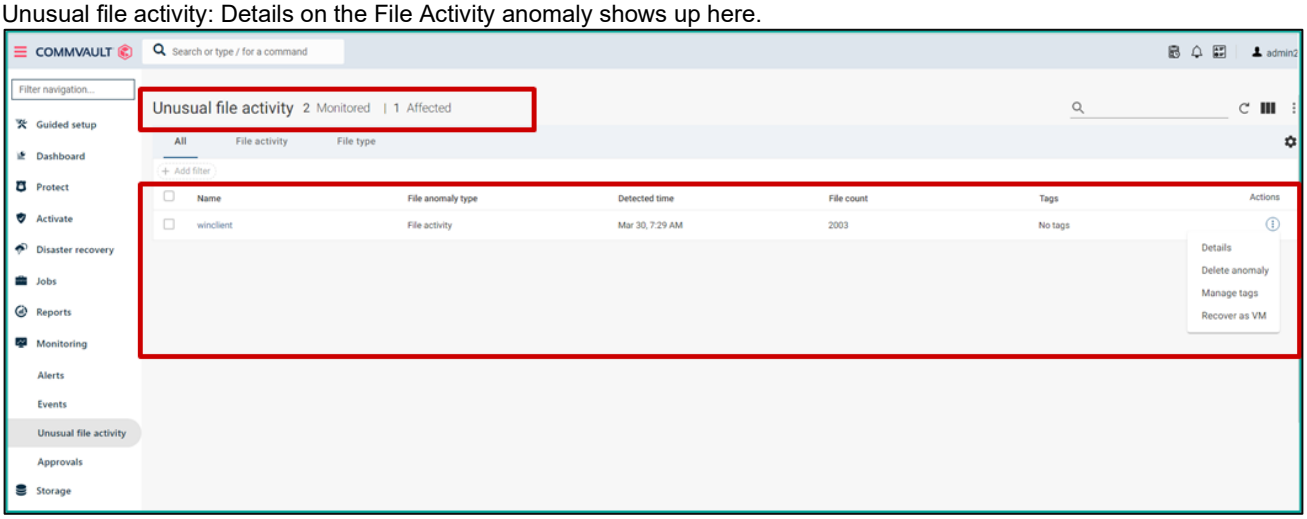


The following screenshot shows the anomalies in the unusual file activity dashboard.

Events tab: Picks up the File Activity Anomaly.

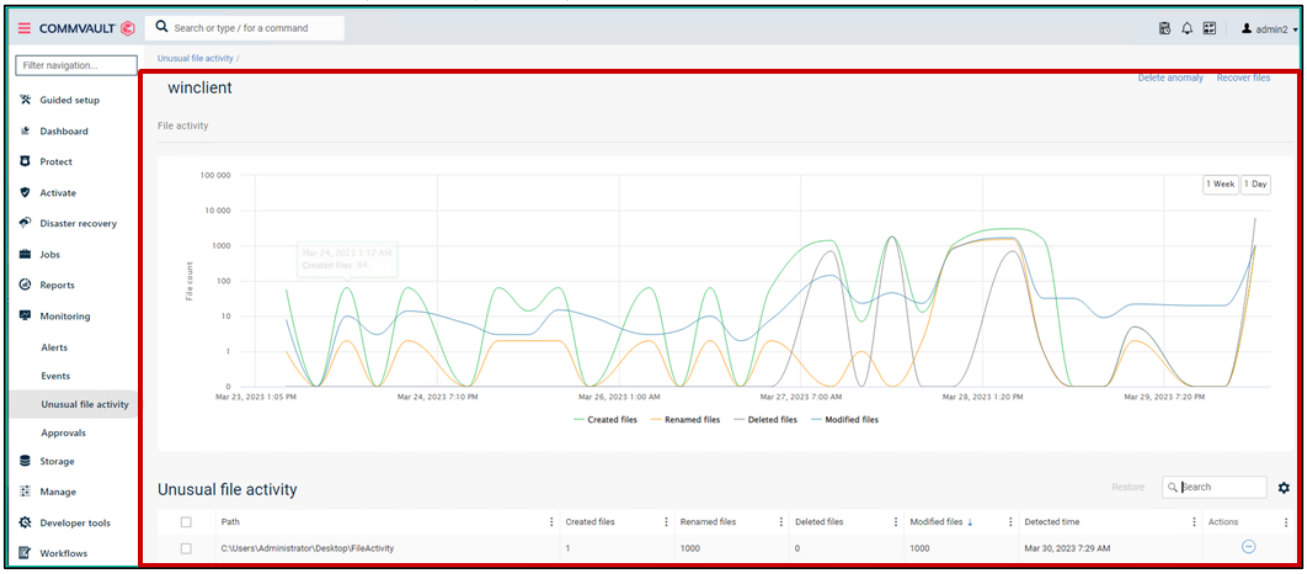


Unusual file activity: Details on the File Activity anomaly shows up here.



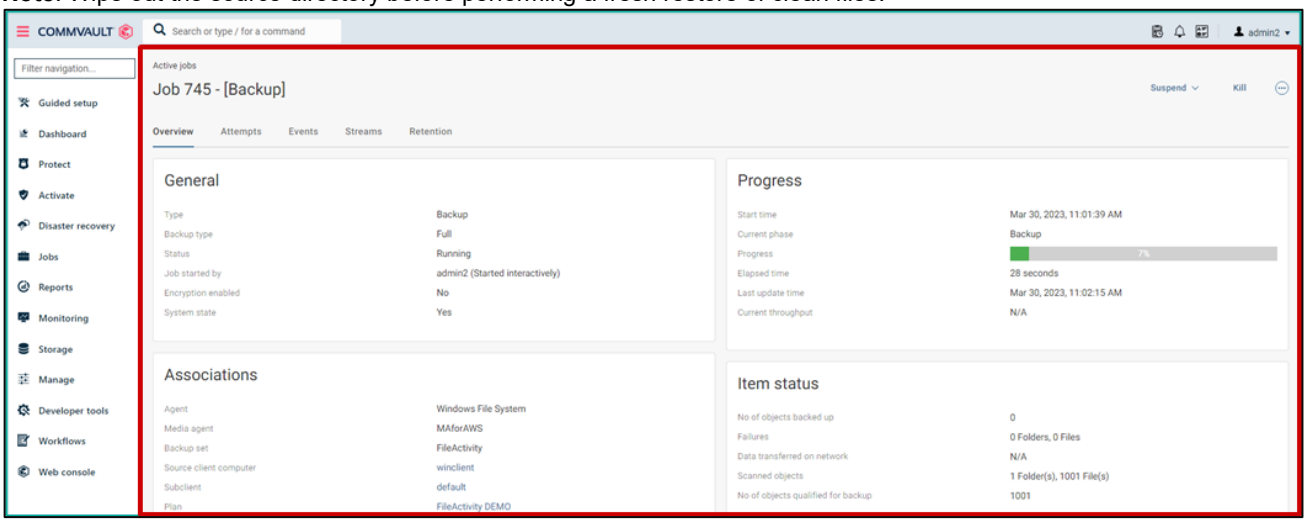
© Hitachi Vantara LLC 2024. All Rights Reserved

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

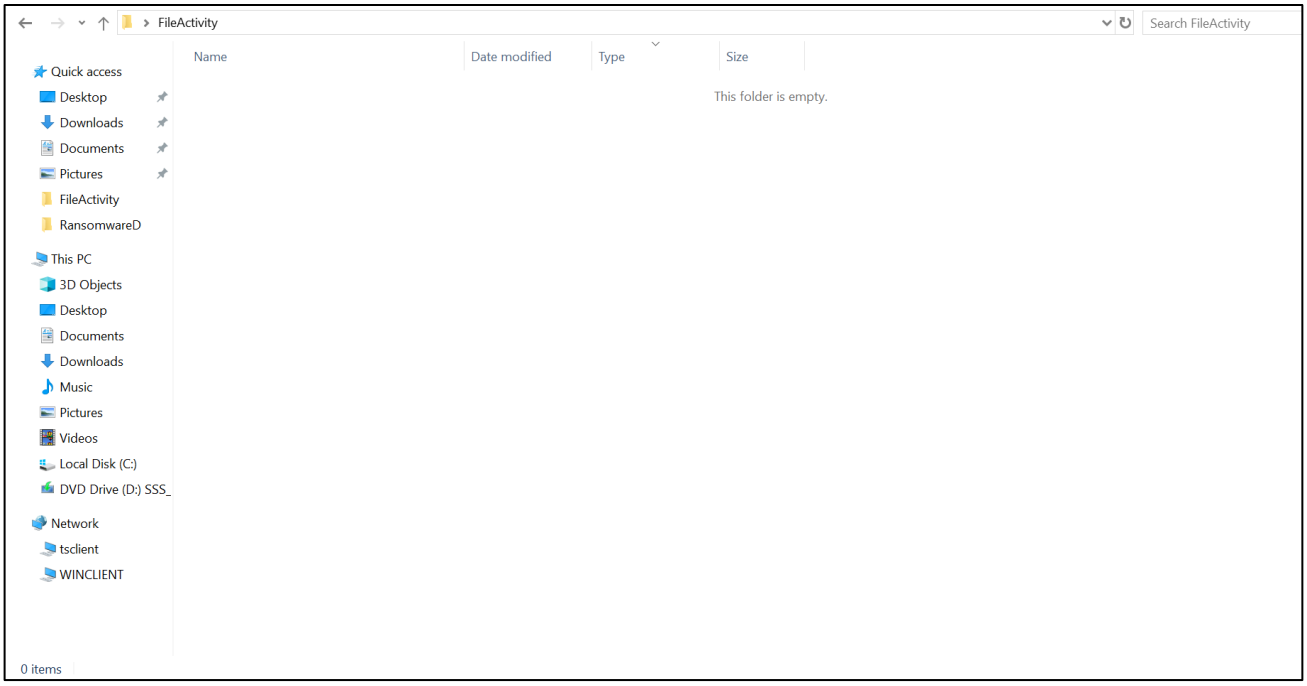


6. To simulate malware containment and clean up the simulation tool, delete the ransomware simulation tool from the server.

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



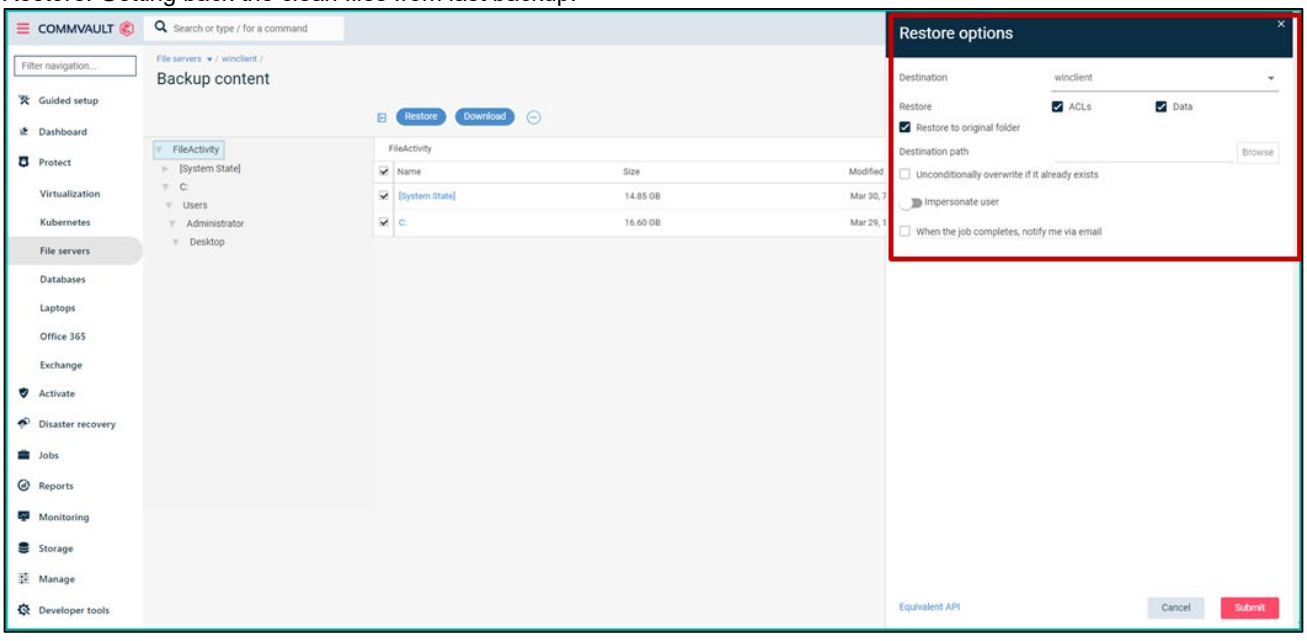
© Hitachi Vantara LLC 2024. All Rights Reserved



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.

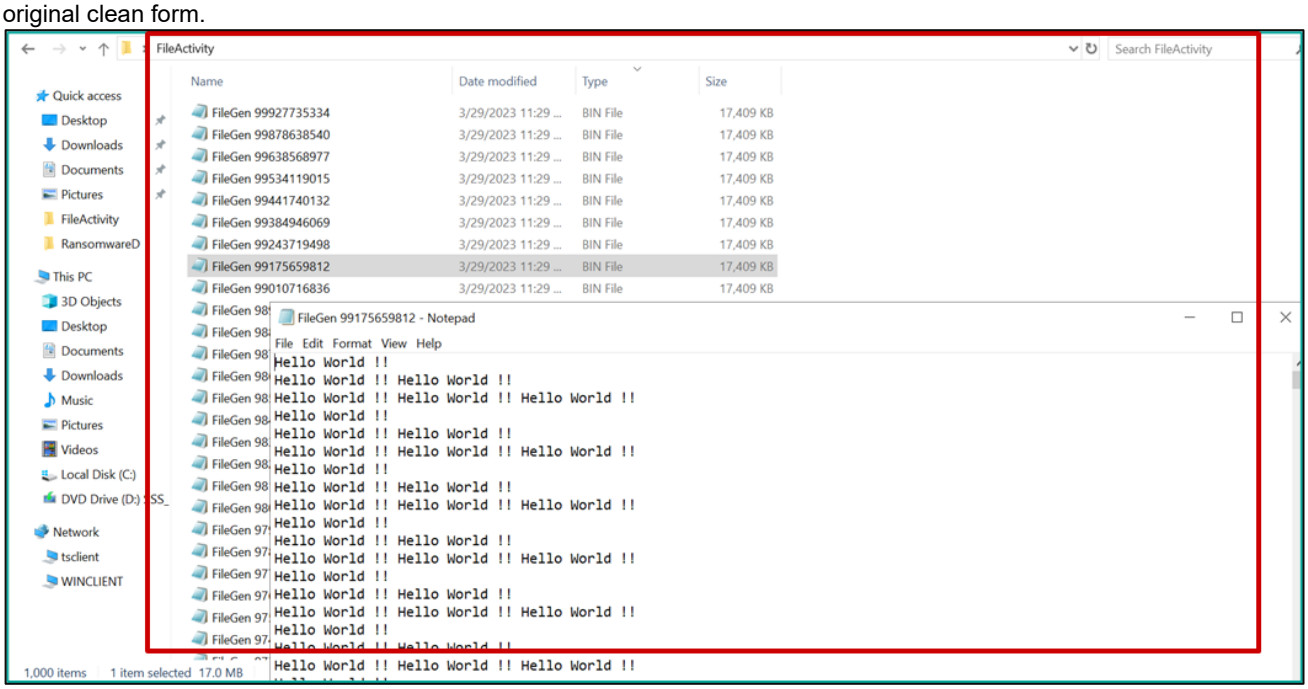
   Restore: Getting back the clean files from last backup.



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.

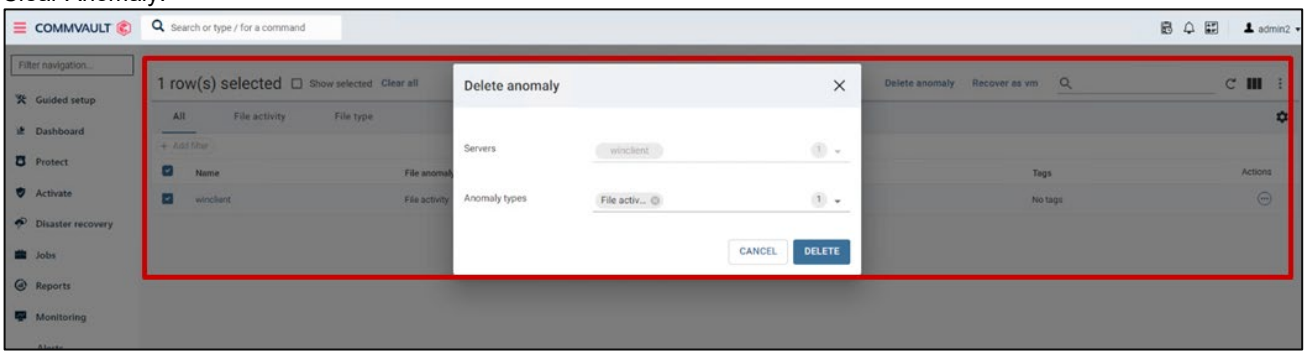
© Hitachi Vantara LLC 2024. All Rights Reserved

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



Additionally, the following option is available:

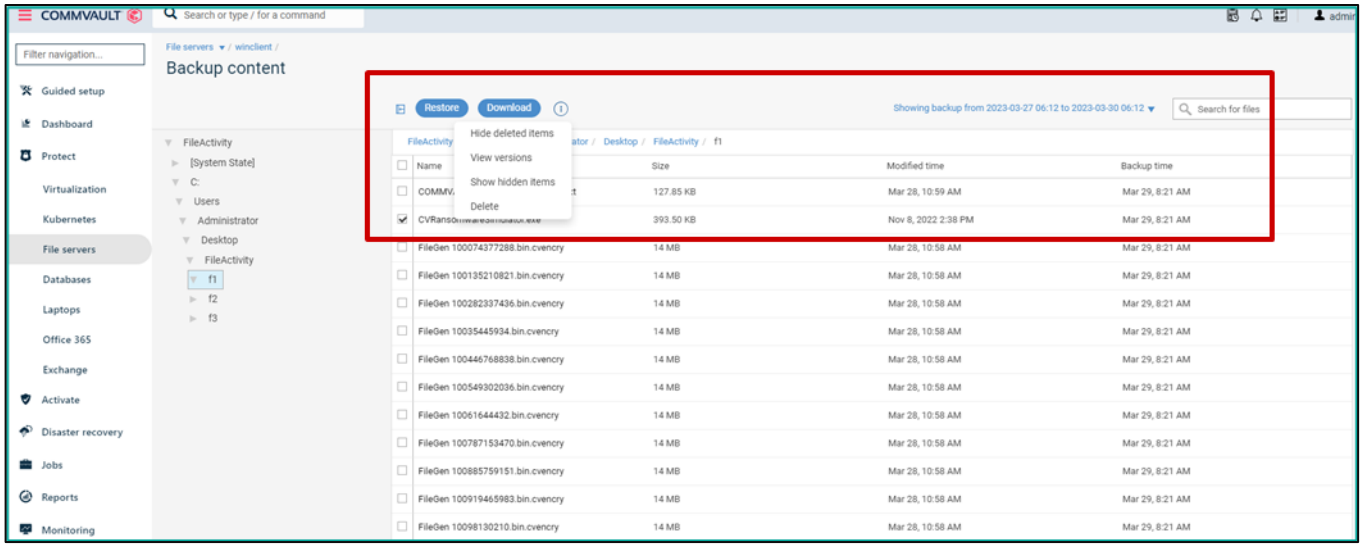
Clear Anomaly:



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

- Download
- Delete

© Hitachi Vantara LLC 2024. All Rights Reserved



© Hitachi Vantara LLC 2024. All Rights Reserved

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.

© Hitachi Vantara LLC 2024. All Rights Reserved