Technical Report

FlexPod Ransomware Protection & Recovery

Roney John Daniel, NetApp
Oct 2025 | TR-4961

In partnership with

Abstract

This technical report starts with an overview of ransomware, how it spreads, and some of the solutions offered by NetApp® and Cisco® Systems at the storage, compute, and network layers to monitor, notify and remediate ransomware attacks. This document focuses on installing and configuring Workload Security feature of NetApp's Data Infrastructure Insights® and ONTAP Autonomous Ransomware Protection® (ARP), which is a native ONTAP security feature. It provides an overview of NetApp Console and Ransomware Resilience service, NetApp Cyber vaulting and, Data Infrastructure Insights (DII) and Ransomware Resilience integration with Splunk cloud. It also discusses NetApp's SnapCenter® plug-ins for VM and application consistent backup and recovery.

TABLE OF CONTENTS

Ransomware overview **5**
How does it spread? 5
Types of ransomware 5
What is the impact? 5
What is the solution? 6
NetApp's solutions to ransomware 6
Solution overview **8**
FlexPod overview **8**
Architecture details 9
FlexPod Infrastructure Security 11
Ransomware protection measures offered by FlexPod 11
NetApp Console overview **15**
Key Features and Capabilities 15
Integrated Services 15
Deployment modes 15
NetApp Console assistant 16
NetApp Console agent 16
NetApp Ransomware Resilience overview **16**
Ransomware Resilience Service Architecture 18
Licensing 18
Front-end Pricing model 19
Setting up Ransomware Resilience 19
Ransomware Resilience integration with Splunk 20
Data Infrastructure Insights (DII) overview **21**
Data Infrastructure Insights Onboarding 21
Subscribing to Data Infrastructure Insights 21
Workload Security overview **22**
How Workload Security works 22
Workload Security components 23
Setting up Workload Security in FlexPod **24**
Install Workload Security agent on a VM to collect data 24
Configure a user directory collector 29

Configure ONTAP data collector 32
Define automated response policies....35
Configure email notification 37
Integrating ONTAP Autonomous Ransomware Protection (ARP) 37

Workload Security - Case study 46

Accidental file deletion....46
A sensitive file is copied to a public folder accidentally....47
Bulk file deletion 47
Ransomware attack simulation via Bulk File Encryption....50

Data Infrastructure Insights API and Splunk Integration 53

Data Infrastructure Insights API....53
Splunk Add-on Builder for REST API 55
Steps to integrate Data Infrastructure Insights and Splunk....56

NetApp Cyber Vaulting overview 57

NetApp Logical Air Gapping 57
Creating a NetApp Cyber vault....58

Recovering Data after Ransomware attack 62

ONTAP Volume Snapshot Restore 62
VM Consistent backup and restore using SnapCenter Plug-in for VMware vSphere 64
Application consistent backup and recovery using SnapCenter plug-ins....73
Recovering Data using Ransomware Resilience....74
Recovering data using NetApp Cyber vault....75

Conclusion 77

Acknowledgement 78

Where to find additional information 78

Version history 78

LIST OF TABLES

Table 1) Hardware and Software....10
Table 2) Agent requirements. 24
Table 3) For US-based Workload Security environments....25
Table 4) For Europe-based Workload Security environments. 25
Table 5) For APAC-based Workload Security environments. 25

Table 6) In-network rules. 25

LIST OF FIGURES

Figure 1) FPolicy External Server. 7
Figure 2) FlexPod Solution 9
Figure 3) FlexPod Topology Diagram 10
Figure 4) NetApp Console SaaS Portal 17
Figure 5) Ransomware Resilience service goals 17
Figure 6) Ransomware Resilience Architecture 18
Figure 7) Workload Security Components 23
Figure 8) Logical air gapping with NetApp SnapLock Compliance 57
Figure 9) NetApp Cyber Vault implementation steps 58
Figure 10) SnapCenter Plug-ins 73

Ransomware overview

Ransomware is a type of malware that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.

The ransomware landscape in 2025 has been marked by a significant increase in attacks, affecting a wide range of industries and highlighting the need for robust cybersecurity measures. As counter measures are taken, attackers find new ways to generate and spread the ransomware, even offering Ransomware as a service (RaaS) to other cyber criminals.

To execute a ransomware attack, the attacker must gain access to a device or network. The attacker gets you to inadvertently download an encryption malware program through normal daily operations such as email, file downloads, or URL access. When the malware is installed on your computer, it is activated at a set time and encrypts all the local client files and every single file that it can access on remote storage on the corporate network. After the files are encrypted, the original files are deleted so you cannot access them unless the files are decrypted with a decryption key held by the attacker.

How does it spread?

There are several different ways ransomware can spread from one computer system to another. The most common method includes normal daily operations such as emails, file downloads, file sharing or accessing web URLs.

The attackers could send spam emails with malicious attachments and links to many people and those who open the attachments or links could fall into the trap unknowingly. In some cases, spear phishing techniques might be used for targeted attacks, pretending to be a supervisor sending emails to the employees or likewise. Attackers can also use social engineering to trick people into opening an attachment in an email as if it comes from a trusted friend or organization.

Malware is also being distributed through new methods, including the physical mailing of USB sticks.

Types of ransomware

There are three main types of ransomware: scareware, screen lockers, and encrypting ransomware.

- **Scareware:** Typically includes rogue security software, repeatedly generating pop-up messages scaring the user that malware is detected and the only way to get rid of it is to pay for the software. If you do not pay for it, you see repeated pop-up messages, however your data might be essentially safe. Note that legitimate cybersecurity software does not solicit customers in this manner.
- **Screen locker ransomware**: A form of malware that restricts login or file access while demanding payment to lift the restriction. Often, the screen includes an official logo such as FBI or DOJ saying illegal activity has been detected on your computer and you must pay a fine. Note that the FBI or DOJ do not demand payment in this manner but rather approach the suspect in person for illegal or terrorism related activities.
- **Encrypting ransomware:** The intention is identical to lock-screen ransomware; however, the impact is very nasty. In this case, data is encrypted, and the attacker demands payment to decrypt the data and redeliver. There is no guarantee that the attacker restores the data or provides keys to decrypt the data, even if you pay the ransom.

What is the impact?

A ransomware attack can have direct and indirect impacts. The effects can vary depending on the nature of the data, duration of downtime, or the duration of time that an organization cannot access its data. A ransomware attack can lead to one or more of the following outcomes.

- **Loss of valuable data**

There is no guarantee that the data is fully recoverable even if you pay the ransom and this is due to potential decryption errors and data loss during the decryption process. If you decide to rebuild the system from backups, it is quite likely that some of the data is lost, depending on when the last backup was taken.

- **Business disruption and loss of revenue**

  Time is money and any downtime severely impacts an organization's revenue through lost opportunities, service outages, production shortages, and more.

- **Liability and compliance costs**

  If sensitive data is breached or exposed, organizations might have to handle litigation costs, fines, and identity monitoring to compensate users whose data was lost or stolen. Organizations following regulations governing the use and protection of data can also incur steep penalties and regulatory fines for non-compliance.

- **Compromised customer confidence and brand name**

  Irrespective of how quickly an organization can respond and remediate a ransomware attack, it can damage an organization's reputation and customer confidence.

What is the solution?

The ability to recover from a ransomware attack with minimal downtime is good, but preventing an attack altogether is ideal.

There is no single solution to this problem, we must constantly evaluate detection and recovery capabilities as new variants are evolving. Although there are several fronts that you must review and fix to prevent an attack, the main component that allows you to prevent or recover from an attack is the data center, where the data resides.

The data center design and the features it provides to secure the network, compute, and storage endpoints play a critical role in building a secure environment for day-to-day operations.

NetApp’s solutions to ransomware

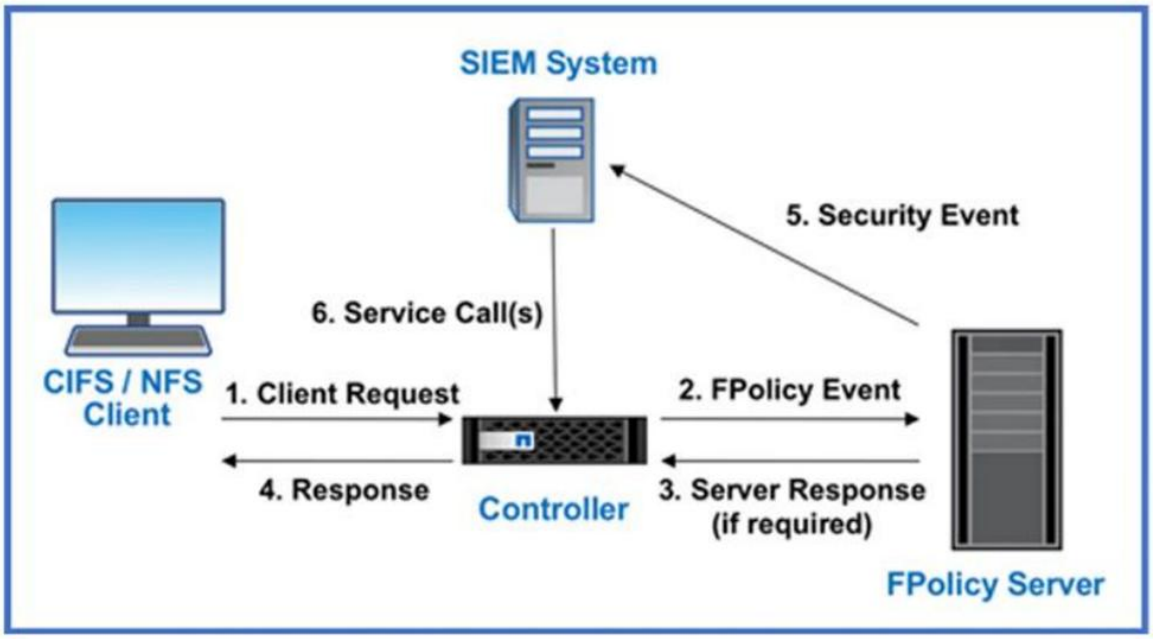
It is important for ransomware detection to occur as early as possible so that you can prevent its spread and avoid costly downtime. NetApp offers a layered defense approach with ONTAP® software and its native detection and recovery tools. This section summarizes various features and tools that NetApp offers to detect, alert, and recover from ransomware attacks.

- **NetApp® Active IQ®** (**AIQ**) checks NetApp ONTAP systems for adherence to NetApp configuration best practices such as enabling FPolicy.
- **NetApp Active IQ Unified Manager®** (**AIQUM**) generates alerts for abnormal growth of NetApp Snapshot copies or storage efficiency loss, which can indicate potential ransomware attacks.
- **ONTAP System Manager** enables analysis of Snapshot percent change or storage efficiency savings in real time.
- **Multifactor Authentication (MFA)** allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data SVM. Depending upon your version of ONTAP, you can use a combination of an SSH public key, user password, and time-based one-time password (TOTP) to set up multifactor authentication. ONTAP 9.13.1 and later allows you to use SSH public key and User password as first authentication method and time-based one-time password (TOTP) as the second authentication method.
- **Multi-Admin Verification (MAV)** ensures that certain operations, such as deleting volumes or Snapshot copies, can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data. This feature is supported since ONTAP 9.11.1.

- **NetApp Native FPolicy** is a file-access notification framework that is used to monitor and to manage file access over the NFS or SMB/CIFS protocol. This zero-trust engine is built around the concept of "not to trust and always verify". FPolicy helps you block unwanted files from being stored on the NetApp storage device. This feature can be leveraged to block known ransomware file extensions. With ONTAP 9.12.1, FPolicy can now be activated with a simple one-click in System Manager or NetApp Console. This feature protects against thousands of known, common ransomware extensions that are used for typical ransomware attacks.
- **FPolicy external mode** in ONTAP uses User Behavior Analytics (UBA), sometimes referred to as User and Entity Behavior Analytics, or UEBA as the key to stopping a zero-day ransomware attack. UBA tracks user's and group's data access patterns and reports any deviation in pattern. UBA can also deny access to files when users do something outside their usual pattern. UBA requires an external mode FPolicy server.

Figure 1 shows the functional diagram of a security information and event management (SIEM) system. Every CIFS/SMB or NFS client request is sent to the FPolicy server, which determines whether access is allowed or denied.

Figure 1) FPolicy External Server.



This extra level of analysis occurs even if users have file permissions to the file data they are trying to manipulate.

Note: Data Infrastructure Insights (DII) with Workload Security feature is NetApp's own external mode FPolicy server.

- **Autonomous Ransomware Protection® (ARP)** NetApp ONTAP 9.10.1 and later comes with anti-ransomware feature that leverages built-in on-box machine learning (ML) that looks at volume workload activity and data entropy to automatically detect ransomware.

  In ONTAP 9.11.1, this feature has been enhanced with an enhanced analytics engine that catches newer variations of ransomware that manipulates data entropy and file extensions. This feature can be integrated with Workload Security to track the status of on-box protection in NetApp's Data Infrastructure Insights (DII) dashboard. This feature is supported on Amazon FSx and Cloud Volumes ONTAP as well.

  In ONTAP 9.12.1, a volume's ARP screening profile is transferred as part of the NetApp SnapMirror® replication, resulting in ransomware protection on secondary storage.

Prior to ONTAP 9.13.1, it was recommended to run ARP in learning mode for 30 days before it is switched to Active mode. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and switches automatically to active mode in 7 to 30 days. Multi-admin verification for ARP configuration is supported since ONTAP 9.13.1.

Beginning with ONTAP 9.16.1, ARP improves cyber resiliency by adopting a machine-learning model for anti-ransomware analytics that detects constantly evolving forms of ransomware with 99% accuracy. With ARP/AI and FlexVol volumes, there is no learning period and ARP/AI is enabled and active immediately if ARP is enabled for those volumes.

ONTAP 9.17.1 introduces ARP support for SAN volumes and NAS volumes containing virtual disks from hypervisors such as VMware and Hyper-V.

- **NetApp Snapshot™ copies** Snapshot is a read-only image of a volume that captures the state of a file system at a point in time. These copies help protect data with no effect on system performance and, at the same time, do not occupy a lot of storage space. Scheduled Snapshots are useful when you need to restore the data after an attack.
- **NetApp SnapLock®** is a key component for enterprise data protection and data resiliency against ransomware. It provides a special immutable volume in which the data can be stored and committed to a non-erasable, non-rewritable state for a specific retention period. User's production data residing in FlexGroup volumes can also be created as SnapLock volumes, enabling higher performance and massive scale for indelible worm-protected data.
- **NetApp Cyber Vaulting** provides organizations with a comprehensive and flexible solution for protecting their most critical data assets. By leveraging logical air-gapping with robust hardening methodologies such as Multifactor Authentication (MFA), Multi-Admin Verification (MAV) and SnapLock compliance, ONTAP enables you to create secure, isolated storage environments that are resilient against evolving cyber threats.
- **NetApp Ransomware Resilience** is an orchestration service for ransomware protection, detection and recovery. The AI-powered service gives your organization the intelligence and help needed to minimize workload data loss and to quickly bounce back from a ransomware attack. Ransomware Resilience is accessible through NetApp Console.

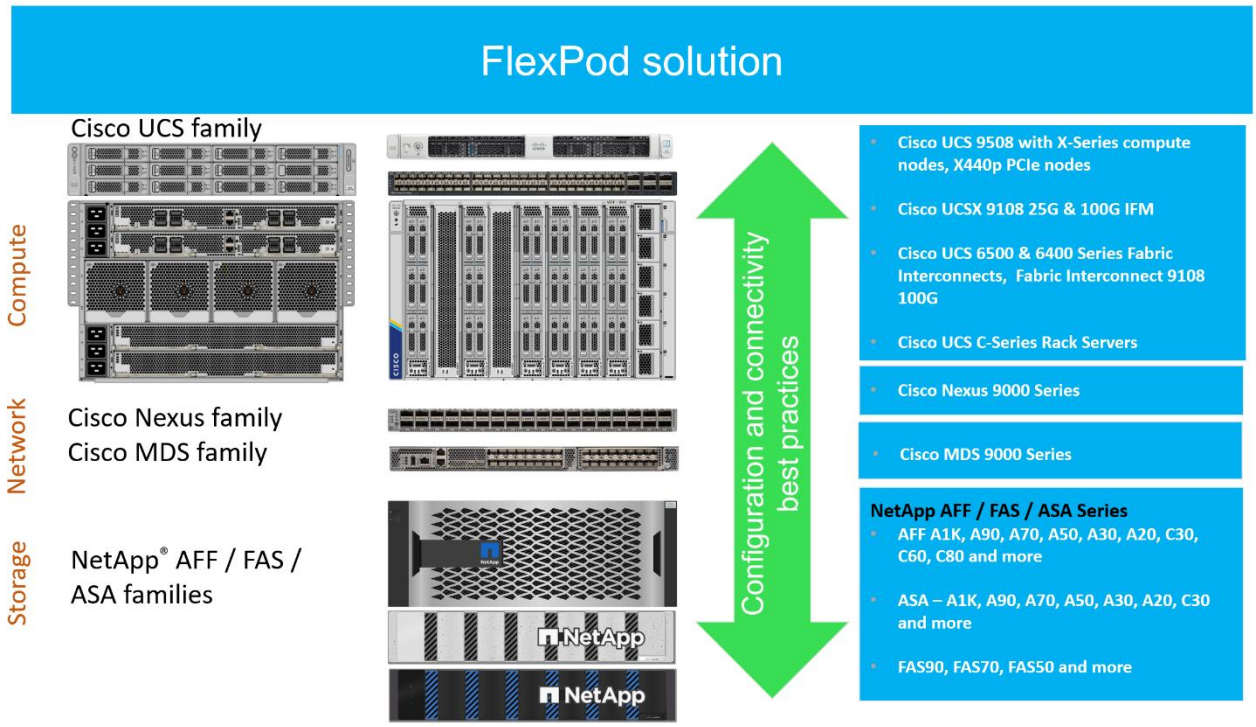
Solution overview

This document details how the Workload Security feature of NetApp Data Infrastructure Insights® can be integrated with FlexPod® hybrid cloud infrastructure to quickly block malicious user access and protect data in the event of a ransomware attack and restore the data quickly after mitigating the attack. There are few Workload Security uses cases discussed in detail to provide the reader with real world scenarios including an attack simulation and recovery. It also provides an overview of the capabilities of NetApp Console (previously BlueXP) that uses AI-driven attack detection and fast recovery process to quickly recover ONTAP workloads. Additionally, this technical report talks about NetApp Cyber vaulting, an ONTAP feature to create secure vaults of isolated storage environments to protect the most critical data assets. Finally, it goes over various options available to recover data after a ransomware attack.

FlexPod overview

FlexPod is a predesigned, validated, and widely deployed data center in a box architecture from Cisco Systems and NetApp. FlexPod has been around for over 15 years, and it evolved into a data center solution that natively supports hybrid cloud environment. FlexPod has a highly resilient, flexible, and modular architecture that enables customers to choose compute, network, and storage components based on bandwidth and workload requirements. **Figure 2** showcases components that are supported at each layer of various FlexPod designs.

Figure 2) FlexPod Solution



FlexPod comes in two major flavors, FlexPod Datacenter and FlexPod Express. FlexPod Datacenter is a massively scalable datacenter that is built around Cisco UCS C-Series and X-Series servers, Cisco UCS Fabric Interconnects, Cisco Nexus® and MDS series switches and NetApp storage. It is suitable for various enterprise workloads as well as public, private and hybrid cloud environments.

A scaled down FlexPod Datacenter can be built with Cisco UCS® X-Series Direct chassis, managed by Cisco Intersight or Cisco UCS manager. It simplifies your data center, adapting to the unpredictable needs of modern applications while also providing an edge, scaled for remote branch office workloads. The UCS X-Series Direct integrates two UCSX-S9108-100G Fabric Interconnects into the X-Series chassis there by reducing the rack space requirements and cost associated with deploying a medium scale datacenter or edge solution. The NetApp storage is directly attached to the integrated Fabric Interconnects, eliminating the need for Nexus switches between NetApp storage and UCS system.

FlexPod Express is a scaled down version with Cisco Nexus Switches, Cisco UCS C-Series servers, and NetApp Storage. It is suitable for remote offices and edge use cases.

FlexPod infrastructure can be configured using ansible playbooks and the end-to-end flow is documented in Cisco Validated Designs (CVDs) or NetApp Verified Architectures (NVAs).

Refer to the FlexPod design and deployment guides for more details.

FlexPod Solutions

FlexPod Design Guides - Cisco

Architecture details

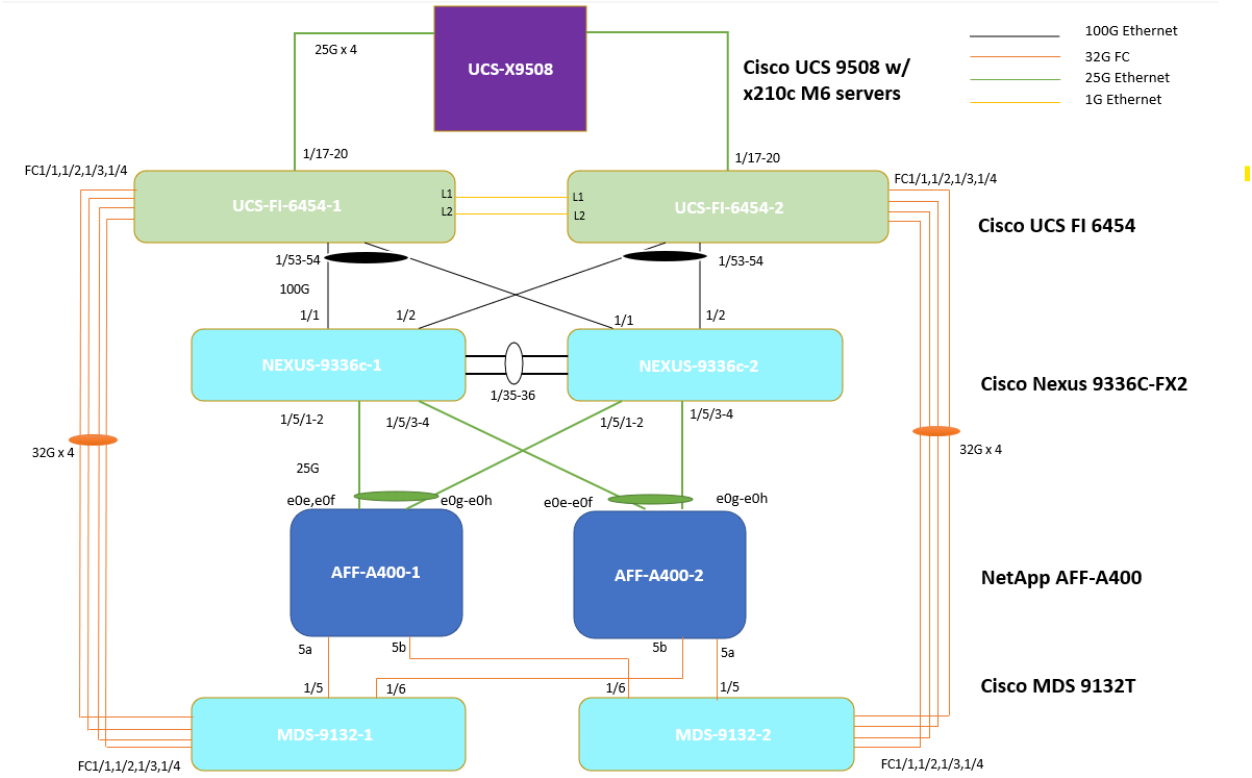
A FlexPod datacenter topology is used for validating Workload Security features in Data Infrastructure Insights. Two Ubuntu VMs are deployed in the management network which serves as the Workload Security agent machines. These machines can access the Data Infrastructure Insights Software as a

Service (SaaS) environment as well as the data collectors deployed in the FlexPod stack. Although one agent machine can track multiple data collectors, two machines are deployed in the lab, one to track SVMs on a NetApp AFF-A400 and other to track the user attributes on an Active Directory server. Two Ubuntu VMs and a Windows 11 VM are deployed in the FlexPod stack for end user activity and ransomware simulation. Additionally, a NetApp FAS 2820 is deployed as a cyber vault.

Topology

The topology under test is shown in **Figure 3**. Note that Workload Security does not have any dependency on specific hardware or software, so any FlexPod system should work seamlessly.

Figure 3) FlexPod Topology Diagram



Hardware and Software components

The hardware and software components used under the test are listed in **Table 1**.

Table 1) Hardware and Software.

Type	Version
SVM Data collector/Source cluster	NetApp AFF-A400 running ONTAP 9.16.1P5
Destination Cluster/ONTAP Cyber vault	NetApp FAS2820 running ONTAP 9.16.1P5
User Directory Data Collector	Windows Server 2022 Datacenter edition running Active Directory
Workload Security Agents (2)	Ubuntu 22.04 LTS
Linux VMs for end-user access (3)	Ubuntu 22.04 LTS
Windows VM for end-user access	Windows 11 Enterprise

Type	Version
VMware vSphere and vCenter Server	8.0.3
NetApp ONTAP Tools for VMware vSphere	10.3
NetApp SnapCenter Plug-in for VMware vSphere	6.1.P1

FlexPod Infrastructure Security

As FlexPod solutions provide the foundation infrastructure for enterprises and business across the globe, having security hardening best practices and providing insights into the tools and technologies built into the FlexPod stack to help enterprises secure their data and promptly recover from security incidents are of critical importance. The following technical report talks about securing the components of the FlexPod solutions to help enterprises enhance the overall security of their business solution.

TR 4984 FlexPod Security Hardening | NetApp

A Zero Trust Security Framework is a comprehensive approach to network security that assumes no user, system, or device can be trusted by default, regardless of its location relative to the network perimeter. It operates under the principle of "never trust, always verify," meaning that every access request is thoroughly verified before granting access, irrespective of where it originates from. The Zero Trust Framework strives to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control. For more information, refer to the following design guide.

FlexPod Datacenter Zero Trust Framework Design Guide - Cisco

Ransomware protection measures offered by FlexPod

This section describes the ransomware protection features offered by Cisco and NetApp that can be leveraged in a FlexPod solution.

Network and Cloud Layers

These are some of the Cisco security features and solutions available to implement ransomware protection in a broader manner.

- **NetFlow**

  Cisco NX-OS supports the flexible NetFlow feature that enables enhanced network anomalies and security detection. Flexible NetFlow allows you to define an optimal flow record for a particular application by selecting the keys from a large collection of predefined fields. The Nexus switches in FlexPod topology can be configured to send NetFlow records to an external collector such as Cisco Secure Cloud Analytics for further analysis and malicious activity detection. For more information, refer to the following link.

  Configuring NetFlow on Nexus 9000 Series switches

- **Cisco identity Services Engine (ISE)**

  Cisco ISE is the market-leading security policy management platform that unifies and automates highly secure access control to enforce role-based access to networks and network resources. Cisco ISE allows you to manage network devices using the TACACS+ security protocol to control and audit the configuration of network devices. ISE facilitates granular control of who can access which network device and change the associated network settings. ISE is available as physical or virtual appliances, and the virtual appliance is available across multiple host OS. For more information, refer to the following link.

  Cisco Identity Services Engine

- **Cisco Security Cloud Control**

Cisco Security Cloud Control provides a single solution for managing Hybrid Mesh Firewall and Universal Zero Trust Network Access (ZTNA), enhancing security outcomes and reducing misconfigurations. Security Cloud Control transforms security operations with its cloud-native design and AI-driven features. By consolidating security and automating tasks like device provisioning and policy updates, it improves visibility, scalability, and efficiency. It provides unified management for Hybrid Mesh Firewall, a highly distributed security fabric that stops advanced threats, protects applications, and enforces zero trust segmentation across data centers, campuses, and IoT environments.

For more information, refer to the following link.

Security Cloud Control At-a-Glance - Cisco

- **Cisco Umbrella®**

  Cisco umbrella provides secure access to the internet and usage of cloud apps everywhere. Umbrella's DNS Layer security provides the fastest, easiest way to improve your network and cloud security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints. In addition to DNS-layer protection and interactive threat intelligence, Cisco Umbrella includes secure web gateway, firewall, and cloud access security broker (CASB) functionality, plus integration with Cisco SD-WAN, delivered from a single cloud security service. For more information, refer to the following link.

  Cisco Umbrella

- **Cisco XDR**

  Cisco XDR, or Extended Detection and Response, is a cloud-based solution designed to simplify security operations and empower security teams to detect, prioritize, and respond to sophisticated threats. By integrating both Cisco and third-party security solutions into a unified platform, Cisco XDR offers a comprehensive approach to threat management.

  Integrated with the threat intelligence provided by Talos, Cisco XDR enriches incident data with additional context and asset insights, reducing false positives and enhancing overall threat detection, response, and forensic capabilities. This solution not only prioritizes alerts to ensure that critical issues are addressed promptly but also provides the shortest path from detection to response, thereby optimizing security operations.

  The extensive integration capabilities of Cisco XDR—supporting over 80 integrations with new ones continually being added—allow organizations to tailor their security environments to meet specific needs. This flexibility enhances the scope of security operations, making it easier to manage and secure complex environments.

  Core Capabilities

  Cisco XDR delivers comprehensive threat protection through the following core capabilities:

  - **Early Detection** - Cisco XDR enables security teams to detect threats sooner by assessing vulnerabilities and risk factors within the environment. Early detection is crucial for maintaining robust security measures and preventing potential breaches.
  - **Prioritization by Impact** - The solution prioritizes alerts based on their potential impact, ensuring that security teams focus on the most critical issues. This targeted approach helps allocate resources more effectively and addresses high-risk threats with urgency.
  - **Reduced Investigation Time** - With advanced tools for investigation, Cisco XDR significantly reduces the Mean Time to Resolution (MTTR). This allows security professionals to quickly understand and isolate alerts, minimizing the time between detection and remediation.
  - **Accelerated Response** - Cisco XDR facilitates a more confident and rapid response to threats by leveraging automation to streamline remediation processes. This enables security teams to respond faster and more effectively to incidents.
  - **Extended Asset Context** - Cisco XDR provides comprehensive visibility into all assets within the environment, reliably identifying users and assessing the security posture of each device. By

contextualizing assets and customizing asset values and labels, security teams gain the necessary context for impact analysis. This extended visibility is essential for maintaining a secure and well-monitored network.

For more information, refer to the following link.

Cisco XDR - Extended Detection and Response

- **Splunk Security suite of tools**

Splunk is a Cisco Company and a world leader in SIEM solution. Splunk's unified security and observability platform enables SecOps, ITOps and engineering teams to collaborate and detect potential threats, investigate and respond faster. The platform is offered as a service in two forms, Splunk® Cloud and Splunk® Enterprise.

The Splunk security suite of tools enables you to strengthen the digital resilience of your modern Security Operation Center (SOC) with unified threat detection, investigation and response. The Splunk security portfolio includes several tools and many of them are now native capability within Splunk Enterprise Security.

- **Splunk Enterprise Security** - Enterprise Security helps you manage, search, and analyze data across every domain, cloud, and device regardless of where it resides. With broad visibility, AI-driven detection, and AI-powered alert prioritization, SOC teams can focus on true positives and respond fast to high-fidelity alerts. Enterprise Security centralizes SOC workflows, streamlining every phase from detection to remediation, all within a single, intuitive workspace.
- **Splunk Security Orchestration, Automation and Response (SOAR)** - Splunk SOAR helps to orchestrate security workflows and automate tasks in seconds to empower your SOC, work smarter, and respond faster. Splunk SOAR is now a native capability within Splunk Enterprise Security.
- **Splunk User Behavior Analytics (UBA)** - Splunk User Behavior Analytics uses unsupervised machine learning algorithms to establish baseline behaviors of users, devices, and applications, then searches for deviations to detect unknown and insider threats. Splunk User Behavior Analytics visualizes threats across multiple phases of an attack to give security analysts a comprehensive understanding of attack root cause, scope, severity, and timelines. This context-rich view enables analysts to rapidly assess impact and make informed decisions quickly and confidently. Splunk UBA is now a native capability within Splunk Enterprise Security.
- **Splunk Attack Analyzer** - Splunk Attack Analyzer is a critical informational component of an organization’s overall threat detection, investigation, and response (TDIR) capabilities. It provides automated threat analysis and associated digital forensics of files and URLs to deliver consistent high-quality analysis of potential threats, save analysts time, and help SOCs achieve the operational efficiency needed to outpace adversaries. The solution uses proprietary technology to extract malicious content from text, images, macro source code, website content, and more to automatically analyze credential phishing and malware threats. With Splunk Attack Analyzer, analysts achieve unparalleled detection efficacy with accuracy, confidence, and ease.
- **Splunk Asset and Risk Intelligence** - Splunk Asset and Risk Intelligence provides a unified, continuously updated inventory of assets and identities by correlating data across multiple sources—including network, endpoint, cloud, and scanning tools. The solution provides accurate asset and identity context to focus and shorten investigations so security teams can quickly identify who is associated with what assets and when.

For more information, refer to the following link.

Security Software & Solutions | Splunk

Compute Layer

- **Cisco Secure Endpoint**

  Cisco Secure Endpoint (formerly known as AMP for Endpoints) is a comprehensive endpoint security solution designed to detect, respond, and recover from cyber threats quickly and efficiently. It offers advanced protection across various control points, ensuring that businesses remain resilient against attacks.

  Key Features

  - **Advanced Endpoint Detection and Response (EDR)**

    Cisco Secure Endpoint provides powerful EDR capabilities, allowing organizations to stop threats with built-in or fully managed endpoint detection and response. It includes threat hunting and integrated risk-based vulnerability management from Kenna Security.

  - **USB Device Control**

    The solution enables the creation, viewing, and management of rules to ensure that only approved USB devices are used within the environment. This feature provides deep visibility into events like blocked devices, aiding in the investigation of compromises.

  - **Integrated XDR Capabilities**

    Cisco Secure Endpoint offers a unified view, simplified incident management, and automated playbooks through Cisco XDR. This extended detection and response approach is one of the broadest in the industry.

  - **Talos® Threat Hunting**

    With built-in Talos Threat Hunting, businesses can proactively thwart attacks before they cause damage. This human-driven threat hunting maps to the MITRE ATT&CK framework, preparing organizations for future threats

  Licensing Options

  Cisco Secure Endpoint offers three main licensing plans:

  1. **Essentials**: Powered by Cisco Talos, this plan blocks more threats than any other security provider. It includes automated threat responses with one-click isolation of infected hosts.
  2. **Advantage**: This plan simplifies security investigations with advanced endpoint detection and response, providing access to advanced malware analysis and threat intelligence[1].
  3. **Premier**: Includes Talos Threat Hunting, where elite security experts from Cisco proactively search for threats in the environment and provide high-fidelity alerts with remediation recommendations.

  Integration with Other Cisco Products

  Cisco Secure Endpoint integrates seamlessly with other Cisco security products, enhancing overall security posture:

  - **Cisco XDR**: Detects sophisticated threats across all vectors and prioritizes them by impact for faster responses.
  - **Cisco Umbrella**: Provides automated, always-on security that works everywhere users go.
  - **Cisco Duo**: Verifies the identity of all users before granting access to corporate applications

  For more information, refer to the following link.
  Cisco Secure Endpoint

Storage

NetApp's solutions to ransomware, discussed earlier in this document can be leveraged to build a secure FlexPod environment. The next section describes some of those features in detail which are applicable to FlexPod and other infrastructure environments.

NetApp Console overview

NetApp Console (formerly NetApp **BlueXP**) is a SaaS-delivered unified control plane designed to manage, protect, and govern data across hybrid multi-cloud and on-premises environments. It simplifies operational complexity by providing a centralized platform for storage management, data mobility, protection, and governance. NetApp Console integrates seamlessly with various cloud providers like AWS, Azure, and Google Cloud, as well as on-premises storage systems such as ONTAP clusters, E-Series systems, and StorageGRID. You can manage cloud storage, on-premises flash and object storage as well as cloud object storage from NetApp Console.

Key Features and Capabilities

NetApp Console offers a **web-based console and APIs** for unified control, enabling users to manage storage and data services efficiently. Its features include:

- **Storage Management**: Discover, deploy, and manage cloud and on-premises storage through the Console canvas. It also provides alerting and life cycle planning
- **Data Protection**: Services like backup and recovery, disaster recovery, replication and ransomware resilience to ensure data security and availability.
- **Data Mobility**: Sync and replicate data between on-premises and cloud environments.
- **Optimization and Governance**: Tools like economic efficiency analysis, sustainability dashboards, and classification services help optimize resources and ensure compliance.

Integrated Services

NetApp Console offers a comprehensive suite of integrated data services, including data protection, replication, cyber resilience, and data lifecycle management. These services help you maintain the security, integrity, and availability of your data across your on-premises and cloud storage environments. Agents are required for most NetApp Data services.

- **Backup and Recovery**: Protect and restore data across environments.
- **Ransomware Resilience**: Orchestrate a comprehensive workload-centric ransomware defense from detection to recovery through a single control plane.
- **Data Classification**: Scan and classify data to achieve enhanced governance, security and privacy. This service is free of charge.
- **Tiering and Caching**: Extend on-premises storage to the cloud and speed up data access.
- **Digital Advisor**: Use predictive analytics for proactive infrastructure optimization

Deployment modes

NetApp Console supports two deployment modes, namely **standard** and **restricted,** catering to different security and connectivity requirements. Each deployment mode differs in outbound connectivity, location, installation, authentication, data services, and charging methods.

The standard mode leverages Software as a Service (SaaS) layer to provide full functionality and is accessed through a web-based hosted interface. This mode uses encrypted data transmission through the public internet.

The restricted mode is useful for organizations that have connectivity restrictions and the user access is through Console agent installed in their cloud environment. This mode is typically used by state and local governments and regulated companies.

Note: The BlueXP private mode (legacy BlueXP interface) is still supported with on-premises that do not have internet access or with secure cloud regions which includes AWS Secret Cloud, AWS Top Secret Cloud, and Azure IL6. For more information on the deployment modes, refer to the following link.

Learn about NetApp Console deployment modes

NetApp Console assistant

When you connect to the NetApp Console web UI, a Console assistant helps you to set up the environment step by step. You need to have a NetApp support account to connect to Console and manage your licensed systems. Once the support account is associated with Console, you can connect your storage estate. Refer to the following link to learn more about Console assistant.

Get started using the NetApp Console Assistant

NetApp Console agent

Many of the data services offered by Console require an agent to be deployed, either on-premises or in the cloud, to fully utilize the NetApp data services. Some features and services are available even without a Console agent. A Console agent is required for data services such as NetApp Backup and Recovery, NetApp Disaster Recovery and NetApp Ransomware Resilience.

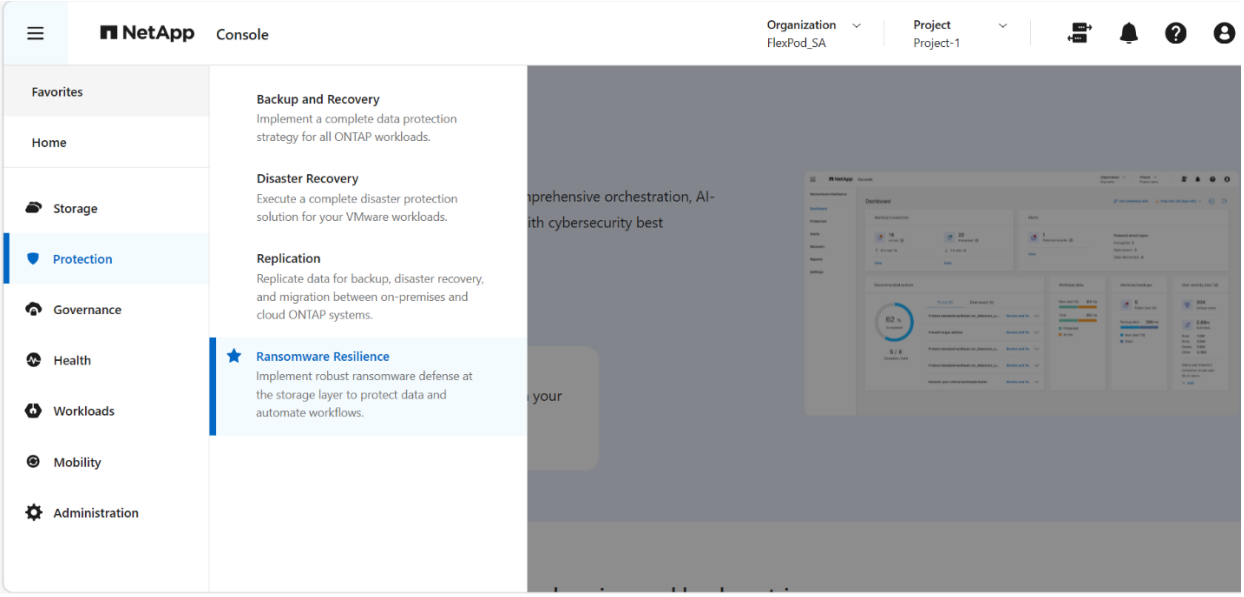
Refer to the following link to understand when a console agent is required.

Learn about NetApp Console agents

NetApp Ransomware Resilience overview

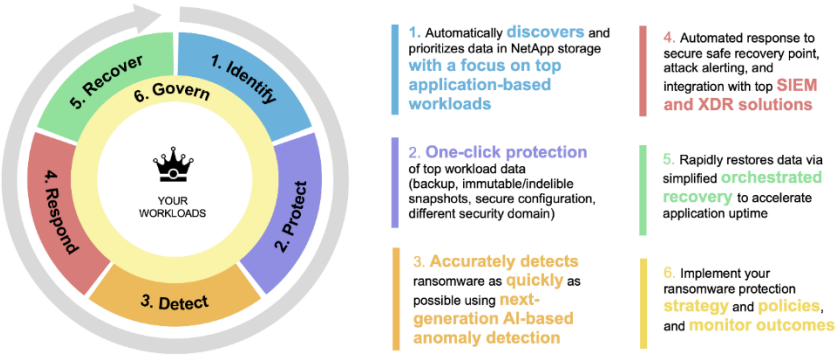
NetApp Ransomware Resilience is an orchestration service on NetApp Console that protects your on-prem as well as cloud data from ransomware attacks. The service protects application-based workloads of Oracle, MySQL, VM datastores, and file shares on on-premises NAS storage (using the NFS and CIFS protocols) and SAN storage (FC, iSCSI, and NVMe) as well as Cloud Volumes ONTAP for Amazon Web Services, Cloud Volumes ONTAP for Google Cloud, Cloud Volumes ONTAP for Microsoft Azure, and Amazon FSx for NetApp ONTAP across the NetApp Console. You can back up data to Amazon Web Services, Google Cloud, Microsoft Azure cloud storage, and NetApp StorageGRID. The NetApp Console SaaS portal for Ransomware Resilience is shown in **Figure 4**.

Figure 4) NetApp Console SaaS Portal



The Ransomware Resilience service provides full use of several NetApp technologies so that your storage administrator, data security administrator, or security operations engineer can accomplish the goals highlighted in **Figure 5**.

Figure 5) Ransomware Resilience service goals

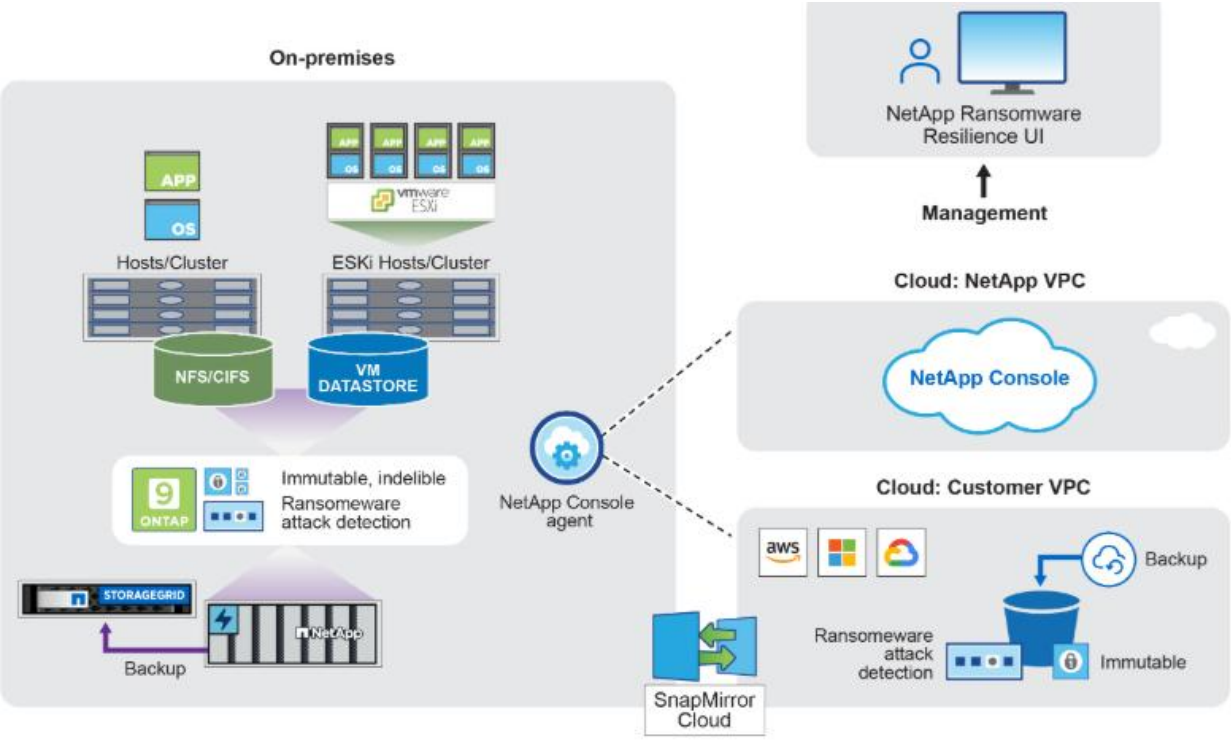


To use Ransomware Resilience, the service needs to first discover data. During discovery, Ransomware Resilience analyzes all volumes and files in working environments across all Console agents and projects within an organization. Ransomware Resilience assesses MySQL applications, Oracle applications, VMware datastores, file shares, and block storage.

Ransomware Resilience Service Architecture

Ransomware Resilence uses Backup and Recovery service in NetApp Console to discover and set snapshot and backup policies for file share workloads. It uses SnapCenter or SnapCenter for VMware to discover and set snapshot and backup policies for application and VM workloads. In addition, Ransomware Resilence uses Backup and Recovery and SnapCenter / SnapCenter for VMware to perform file- and workload-consistent recovery. Ransomware Resilence architecture is shown in **Figure 6**.

Figure 6) Ransomware Resilience Architecture



Licensing

Different licensing plans are available for Ransomware Resilience.

- Sign up for a 30-day free trial.
- Purchase a pay-as-you-go (PAYGO) subscription with Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace, or Azure Marketplace.
- Bring your own license (BYOL), which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep. You can use the license serial number to get the BYOL activated in NetApp Console.

After you set up your BYOL or purchase a PAYGO subscription, you can see the license in the licenses and subscriptions section of the Console.

For more information on Licensing, refer to the following URL.

[Set up licensing for NetApp Ransomware Resilience]

Front-end Pricing model

For Ransomware Resilience, charges are based on used capacity on the source volume. The service offers 30-day free trial for unlimited capacity. Once the trial period has ended, charges will be applied according to the selected subscription model, as illustrated in the example below.

Free Trial	Pay-As-You-Go	12 Month Subscription	36 Month Subscription
Unlimited Capacity Free for 30 days	Via Marketplace $0.07 Per GB per month	BYOL or via Marketplace $0.0665 Per GB per month	BYOL or via Marketplace $0.0595 Per GB per month

For latest pricing, refer to Pricing estimates and TCO calculators

Setting up Ransomware Resilience

This section talks about a high-level overview of the setup procedure.

Prerequisites

Following are the prerequisites to set up Ransomware Resilience in NetApp Console.

- A NetApp Console user account with Organization Admin privileges for discovering resources.
- A Console organization with at least one active Console agent connecting to on-premises ONTAP clusters or to CVO in AWS or in Azure.
- The console agent must have the **cloudmanager-ransomware-protection** container in an active state.
- At least one Console system with a NetApp on-premises ONTAP cluster or Cloud Volumes ONTAP in AWS or Azure. Ransomware Resilience supports both NAS (NFS and SMB) and SAN (iSCSI, FC, and NVMe) protocols. Note that SAN workloads are supported only in ONTAP 9.17.1 and later. If your on-premises ONTAP clusters or Cloud Volumes ONTAP in AWS or in Azure cloud are not already onboarded in Console, you need a Console agent.

For detailed information, refer to the following link.

NetApp Ransomware Resilience prerequisites

Steps to set up Ransomware Resilience

Here is an overview of the steps needed to configure Ransomware Resilience.

- Prepare NetApp StorageGRID, Amazon Web Services, Google Cloud Platform, or Microsoft Azure as a backup destination
- Setup NetApp Console agent.
- Set up licensing.
- Discover workloads in Ransomware Resilience.
- Configure backup destinations.
- Optionally enable threat detection.
- Optionally, conduct a ransomware attack readiness drill.

You can configure backup destinations, send data to an external security and event management (SIEM) system, conduct an attack readiness drill, configure workload discovery, or configure connection to Data Infrastructure Insights Workload security. This is done by accessing the **Settings** option in Ransomware Resilience.

For more information, refer to the following links.

Set up NetApp Ransomware Resilience

Configure protection settings in NetApp Ransomware Resilience

Ransomware Resilience integration with Splunk

For threat analysis and detection, it is easy to integrate Ransomware Resilience with external security and event management (SIEM) systems such as Splunk Cloud. You need to have ransomware Resilience admin role in NetApp Console to set this up and it is done from the settings menu of Ransomware Resilience.

Before you enable SIEM in Ransomware Resilience, you need to configure your SIEM system. First you need to enable an HTTP Event Collector in Splunk Cloud and then configure and event collector Token. Once this is done, you can connect to Splunk from Ransomware Resilience.

Steps to enable an HTTP Event Collector in Splunk

1. Got to Splunk Cloud.
2. Select **Settings** > **Data Inputs**.
3. Select **HTTP Event Collector** > **Global Settings**.
4. On the “All Tokens” toggle, select **Enabled**.
5. To have the Event Collector listen and communicate over HTTPS rather than HTTP, select **Enable SSL**.
6. Enter a port in **HTTP Port Number** for the HTTP Event Collector.

Steps to create Event Collector token in Splunk

1. Go to Splunk Cloud.
2. Select **Settings** > **Add Data**.
3. Select **Monitor** > **HTTP Event Collector**.
4. Enter a Name for the token and select **Next**.
5. Select a Default Index where events will be pushed, then select **Review**.
6. Confirm that all settings for the endpoint are correct, then select **Submit**.
7. Copy the token and paste it in another document to have it ready for the Authentication step.

Steps to connect to Splunk from Ransomware Resilience

1. From the Console menu, select **Protection** > **Ransomware Resilience**.
2. From the Ransomware Resilience menu, select the vertical three dots option at the top right.
3. Select **Settings**. The settings page appears.
4. In the Settings page, select **Connect** in the SIEM connection title.
5. Choose Splunk from the tiles shown.
6. Enter the token and authentication details you configured in previous step.
7. Select **Enable**. The settings page should show Splunk tile in connected state.

Note: You can also configure AWS Security Hub or Microsoft Sentinel as your SIEM system.

Data Infrastructure Insights (DII) overview

NetApp Data Infrastructure Insights (previously **Cloud Insights**) is a cloud infrastructure monitoring tool that gives you visibility into your complete infrastructure. With Data Infrastructure Insights, you can monitor, troubleshoot and optimize all your resources including your public clouds and your private data centers.

Data Infrastructure Insights offers several features and capabilities. It provides complete visibility into the multi-vendor infrastructure and applications whether it is on-prem or in the cloud. You can use the included customizable dashboards and reports for visualization and reporting or create your own dashboards with powerful creation tools. You can right-size your resources, track, visualize and highlight over utilized and underutilized infrastructure thereby optimizing the resources. With enhanced ONTAP capabilities such as Advanced Ransomware Protection (ARP), you can identify risks and protect your data from an attack. The platform comes with global region availability with a data retention of up to 13 months. For more information, refer to the following URL.

Data Infrastructure Insights: Features & capabilities | NetApp

Data Infrastructure Insights Onboarding

Before you can start working with Data Infrastructure Insights, you must sign up on the **NetApp Console** portal. During the registration process, you can choose the global region to host your DII environment. If you already have a NetApp Console login, you can start a free trial of Data Infrastructure Insights with a few quick steps.

You may refer to the following URL for more information.

Data Infrastructure Insights Onboarding

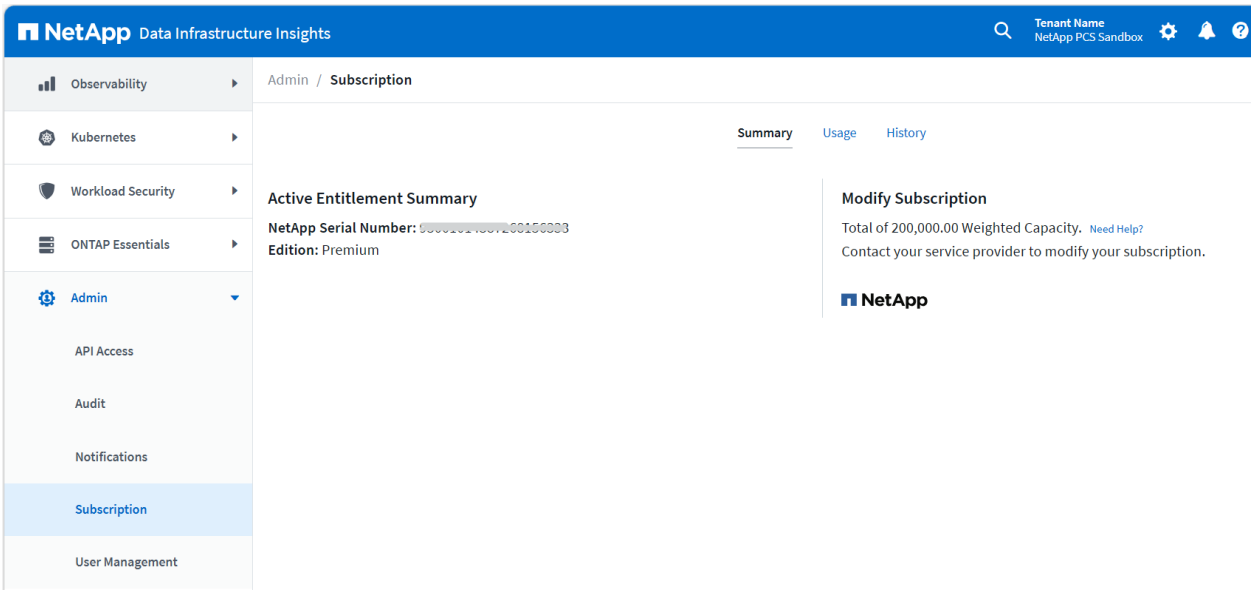
Subscribing to Data Infrastructure Insights

When you sign up for Data Infrastructure Insights and your environment is active, you enter a free, 30-day trial of Data Infrastructure Insights. During this trial you can explore the features that Data Infrastructure Insights has to offer, in your own environment. At any time during your trial period, you can subscribe to Data Infrastructure Insights. Subscribing to Data Infrastructure Insights ensures uninterrupted access to your data as well as extended product support options.

You can subscribe to DII using the following options.

- NetApp Sales direct
- AWS Marketplace
    - Fixed term subscription
    - Pay-as-you-go subscription
    - Fixed base + Pay-as-you-go overages subscription
- Azure Marketplace (all subscription options)

The following screenshot displays the Data Infrastructure Insights subscription page.



For more information subscription and metering options, refer to the following link.
[Subscribing to Data Infrastructure Insights]

Workload Security overview

Workload Security (formerly **Cloud Secure**) is a feature of NetApp Data Infrastructure Insights (DII). It provides centralized visibility and control of all corporate data access across on-premises and cloud environments to make sure that security and compliance goals are reached. It reports access activity from insiders, outsiders, ransomware attacks, and rogue users. It profiles users and groups for normal data access patterns and if risky behavior is detected, it alerts you and automatically takes a Snapshot copy which can be used to recover quickly.

Unlike perimeter security tools, which assume that insiders are trusted, Workload Security assumes zero trust for everyone. All activities on the supervised shares are monitored in real time and the data is used to automatically identify the working communities of all users.

Besides, the ability to audit all document access helps you to ensure compliance with regulatory requirements.

How Workload Security works

Workload Security is based on Zero Trust framework, so it takes a trust no one approach. All data access activity is inspected and analyzed in real time to detect malicious behaviors, and an alert is generated to notify users or administrators.

Workload Security performs four major functions:

- **Monitor user activity**.

  To accurately identify breaches, every user activity across on-premises and hybrid cloud environments is captured and analyzed. The data is collected using a lightweight, stateless data collector agent installed on a virtual machine (VM) in the customer's environment. This data also includes user data from Active Directory and Lightweight Directory Access Protocol (LDAP) servers and user file activity from NetApp ONTAP® and Cloud Volumes ONTAP® (CVO).
- **Detect anomalies and identify potential attacks.**

Today's ransomware and malware are sophisticated, using random extensions and file names that make detection by signature-based (blocked list) solutions ineffective. Workload Security uses advanced machine learning algorithms to uncover unusual data activity and detect a potential attack. This approach provides dynamic and accurate detection and reduces false detection noise.

- **Automated response policies.**

  Workload Security alerts you and automatically takes a data Snapshot when it detects risky behavior, making sure that your data is backed up for a quick recovery when needed.

- **Forensics and user audit reporting**.

  Workload Security provides a graphical interface to slice and dice activity data to perform data breach investigations and generate user data access audit reports. It allows multiple views of file data activities by user, time, activity type, and file attributes.

Workload Security components

Workload Security collects user activity using one or more agents and data collectors. Each agent can host multiple data collectors; however separate agents can be installed to monitor specific sets of data collectors. The agent sends collected data to Data Infrastructure Insights for analysis. **Figure 7** shows the architecture components of workload security.

Figure 7) Workload Security Components

As of this writing, Workload Security supports the following user directory collectors and data collectors.

- Active Directory (AD) User Directory Collector.
- LDAP Directory Server Collector.
- ONTAP SVM Data collector.
- Cloud Volumes ONTAP Data Collector (Amazon, Azure & Google Cloud).
- Amazon FSx for NetApp ONTAP.

Refer to the following link for more information.

Getting Started with Workload Security

Setting up Workload Security in FlexPod

The Workload Security agent machine can be installed within or outside the FlexPod environment. However, it must have IP connectivity to the Data Infrastructure Insights SaaS environment and data collectors in the FlexPod environment. These are the steps to configure a Workload Security agent and data collectors.

1. Install Workload Security Agent on a Linux VM to collect data.
2. Configure a user directory collector to collect user attributes from active directories (optional).
3. Configure a data collector.
4. Define automated response policies to take automatic action in the event of an attack.
5. Configure email notifications for alerts.

Install Workload Security agent on a VM to collect data

You must install an agent to acquire user and file activities from the data collectors. The Workload Security agent can be installed on the same machine as the Data Infrastructure Insights acquisition unit. However, it is best practice to install these on separate machines. Please note that a single VM running Workload Security agent can monitor up to 50 data collectors.

Agent Machine requirements

Before you install the agent, make sure that the environment meets operating system, CPU, memory, and disk space as outlined in Table 2.

Table 2) Agent requirements.

Type	Comments
Operating System	Licensed version of Linux *(RHEL 8.10 64-bit and 9.1 through 9.6 64-bit, Oracle Linux 8.10 64-bit and 9.1 through 9.6 64-bit, CentOS 9 Stream, Ubuntu 20.04 LTS through 22.04 LTS 64-bit) and many more.*
CPU	4 CPU Cores
Memory	16GB RAM
Disk Space	/opt/netapp 36GB (minimum 35GB free after file system creation)
Network	100 Mbps to 1 Gbps Ethernet connection, static IP address, IP connectivity to all devices, and a required port to the Workload Security instance (80 or 443).

Note: If the Workload Security agent and DII Acquisition Unit are installed on the same machine, there must be a minimum 50-55GB available disk space (25-30GB for /opt/netapp and 25G for /var/log/netapp).

It is strongly recommended to synchronize the time on both the ONTAP system and the Agent machine using Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP).

Inbound and outbound access rules

For the Workload Security agent to connect to the Data Infrastructure Insights SaaS environment and data collectors, specific ports must be opened on the end points, with network firewalls in between them. The following tables can be used as references to open required TCP ports.

Cloud Network access rules

Cloud Network access rules are intended to connect Workload Security agent to the Data Infrastructure SaaS environment hosted in the cloud. Refer to the following tables to open access control lists (ACLs) based on the region where your Data Infrastructure Insights environment resides (Tables Table 3,Table 4 and Table 5).

Table 3) For US-based Workload Security environments.

Protocol	Port	Destination	Direction	Description
TCP	443	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	Outbound	Access to Data Infrastructure Insights
TCP	443	agentlogin.cs01.cloudinsights.netapp.com	Outbound	Access to authentication services

Table 4) For Europe-based Workload Security environments.

Protocol	Port	Destination	Direction	Description
TCP	443	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	Outbound	Access to Data Infrastructure Insights
TCP	443	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Outbound	Access to authentication services

Table 5) For APAC-based Workload Security environments.

Protocol	Port	Destination	Direction	Description
TCP	443	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	Outbound	Access to Data Infrastructure Insights
TCP	443	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Outbound	Access to authentication services

In-network access rules

In-network access rules are intended for communication between the Workload Security agent and data collectors. Refer to Table 6 when opening ACLs on the network as well as data collectors.

Table 6) In-network rules.

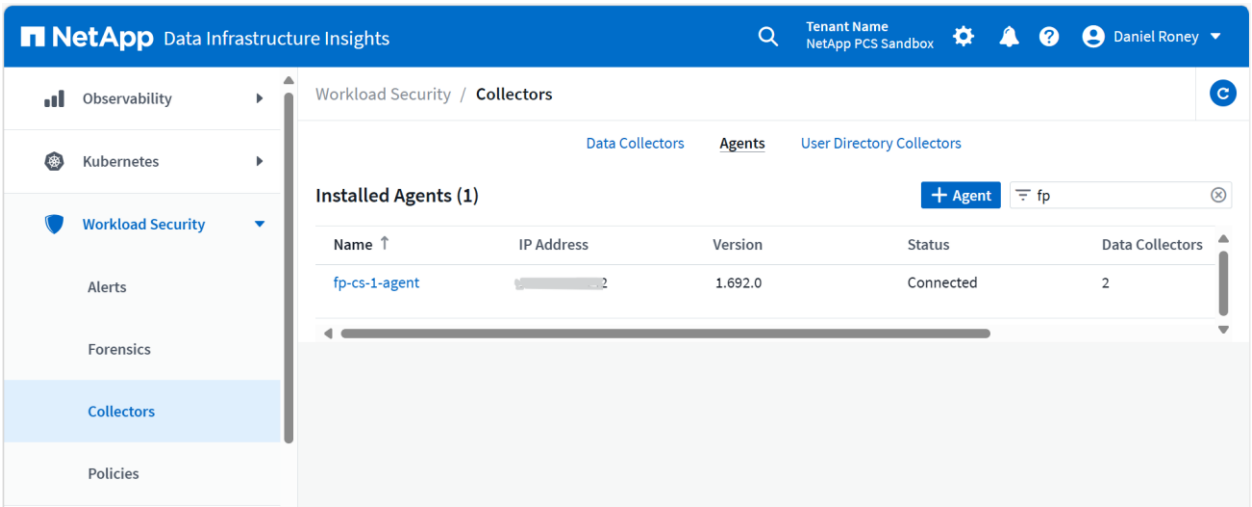
Protocol	Port	Destination	Direction	Description
TCP	389(LDAP) 636 (LDAPs / start-tls)	LDAP Server URL	Outbound	Connect to LDAP
TCP	443	Cluster or SVM Management IP Address (depending on SVM collector configuration)	Outbound	API communication with ONTAP
TCP	35000-55000	Workload Security Agent	Inbound	Communication from SVM data LIF IPs to Workload security agent for Fpolicy

Protocol	Port	Destination	Direction	Description
				events, opened on storage end. Start by reserving 100 ports and increasing as needed
TCP	35000-55000	Workload Security Agent	Inbound	Cluster mgmt IP to workload security agent for EMS events. Start by reserving 100 ports and increasing as needed
TCP	7	SVM data LIF IP Addresses	Outbound	Unidirectional between ONTAP and Workload Security. Agent pings the SVM LIFs.
SSH	22	Cluster Management	Outbound	For CIFS/SMB user blocking.

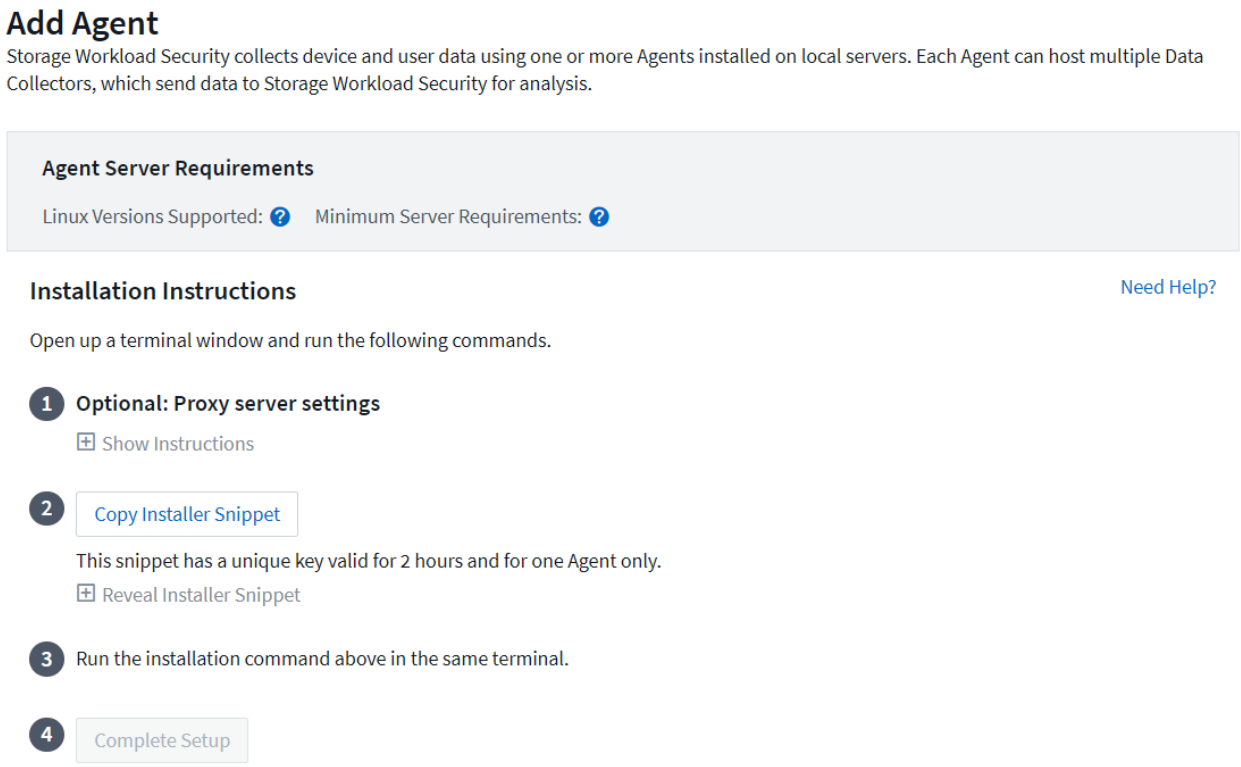
Steps to configure Workload Security agent

In the FlexPod lab setup, two Workload Security agents are configured on Ubuntu 22.04 based Linux VMs, one to monitor the ONTAP SVM data collectors and the other to monitor the Active Directory user data collector. You can use the following steps to install the agent:

1. Login to your Data Infrastructure Insights environment as Administrator or Account owner.
2. Expand **Workload Security** menu on the left pane and select **Collectors** from the list. Click on **Agents** tab on the right pane.



3. Click on **+Agent**. The system displays the **Add an Agent** page as shown below.



4. Click on the **"?"** icon to verify that the agent meets the minimum system requirements, and that the agent server is running a supported version of Linux. If the network is using a proxy server, set the proxy server details as suggested.
5. Open a terminal window and follow the procedure as described in the installation instructions in the figure above.
6. Once the installation is completed successfully, the system displays the new agent. The agent server console will start the service as shown in the following example.


```
setup cloud secure agent directory ownership
setting 700 permission to /opt/netapp/cloudsecure recursively
setting 755 permission to /var/log/netapp
Copying service file to /usr/lib/systemd/system/cloudsecure-agent.service
Setting systemd services for cloudsecure-agent.
Taking backup of the VM default rmem values to /opt/netapp/cloudsecure/sysctl.conf.bkp
Setting default and max rmem values
Starting CloudSecure Agent services.
                    Welcome to CloudSecure (R) 1.692.0
                    Agent

                     ____   _____
                    / ___|  |  ___|
                   | |      |_|___
                   | |___    ___| |
                    \____|  |_____|
  NetApp (R)

  Installation:       /opt/netapp/cloudsecure/agent
  Installation logs:  /var/log/netapp/cloudsecure/install
  Agent Logs:         /opt/netapp/cloudsecure/agent/logs

  To uninstall:
    sudo cloudsecure-agent-uninstall.sh --help
fpadmin@fp-cloud-secure-2:~$
```

7. The Data Infrastructure Insights GUI will display the new agent name with a random number as shown below. You can rename it to match the agent VM names, fp-cs-1-agent and fp-cs-2-agent.

Installed Agents (17)

+ Agent | Filter...

Name ↑	IP Address	Version	Status	Data Collectors	Last Reported
agent-2003	[redacted]	1.692.0	Connected	1	a few seconds ago *Aug 21, 2025 4:15 PM*
agent-2006	[redacted]	1.692.0	Connected	0	a few seconds ago *Aug 21, 2025 4:15 PM*

8. The status of Workload Security service on the agent VM can be verified as shown in the following example:

```
fpadmin@fp-cloud-secure-2:~$ sudo systemctl status cloudsecure-agent.service
● cloudsecure-agent.service - Cloud Secure Agent Daemon Service
     Loaded: loaded (/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2025-08-21 20:05:34 UTC; 14min ago
   Main PID: 2630 (java)
      Tasks: 35 (limit: 19050)
     Memory: 372.7M
        CPU: 18.554s
```

9. Run commands on the Linux prompt to open the ports that are used by Workload Security.

Ubuntu:

```
sudo ufw allow 35000:55000/tcp
```

Centos:


```
sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp
sudo firewall-cmd -reload
```

Note: Each SVM uses two ports, and the Workload Security database requires several ports, so a minimum range of 35000:35100 is recommended if there are security concerns opening a larger range.

10. Issue the following command to verify the ports that are opened, based on the range configured above.

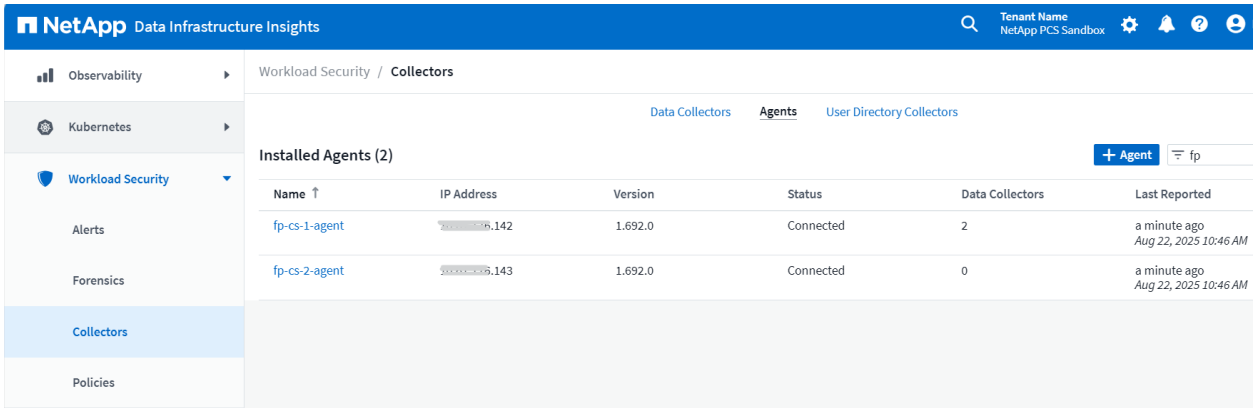
Ubuntu:

```
sudo ufw status numbered
```

Centos:

```
sudo firewall-cmd --zone=public --list-ports | grep 35000
```

11. Repeat steps 2-10 to install additional agents as required.
12. You can check the status of the agent by clicking **Workload Security > Collectors** and choosing the **Agents** tab.



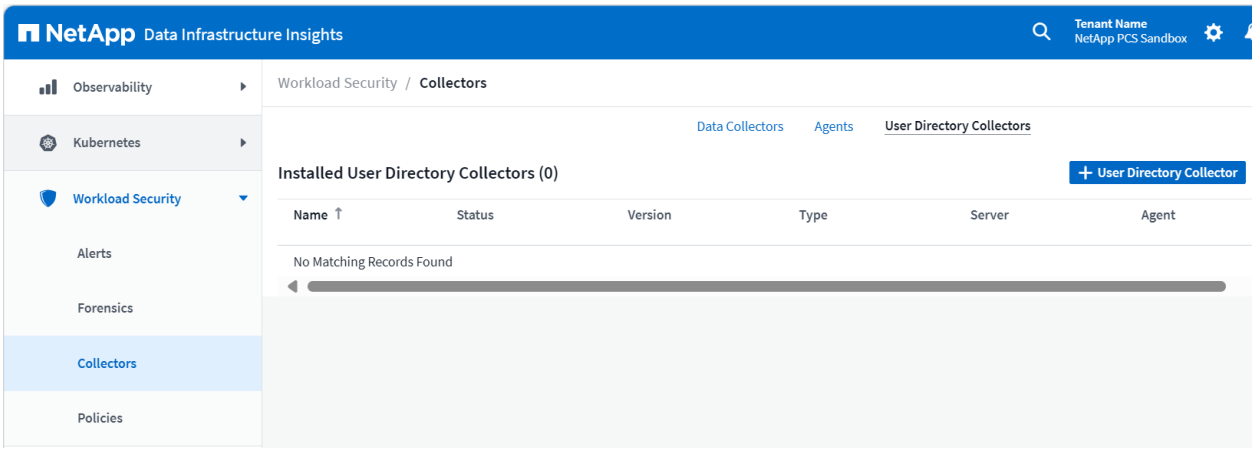
Configure a user directory collector

This step assumes that an Active Directory server already exists in the user environment, and that you have the IP address and forest information to configure the user directory collector. The Workload Security agent must be configured before this step. This task can be performed by a Data Infrastructure Insights administrator or account owner.

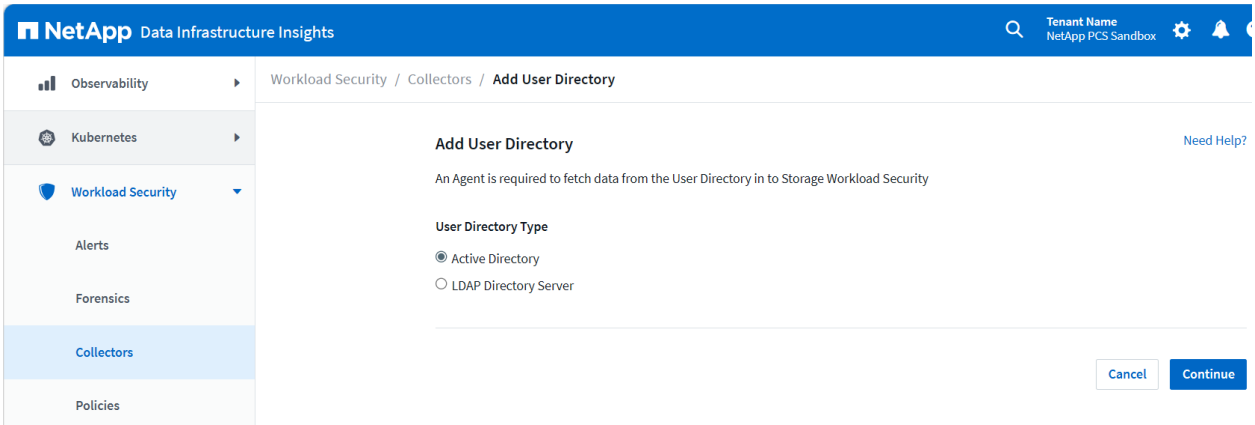
Steps to configure a user directory collector

Follow the procedure to configure a user directory collector.

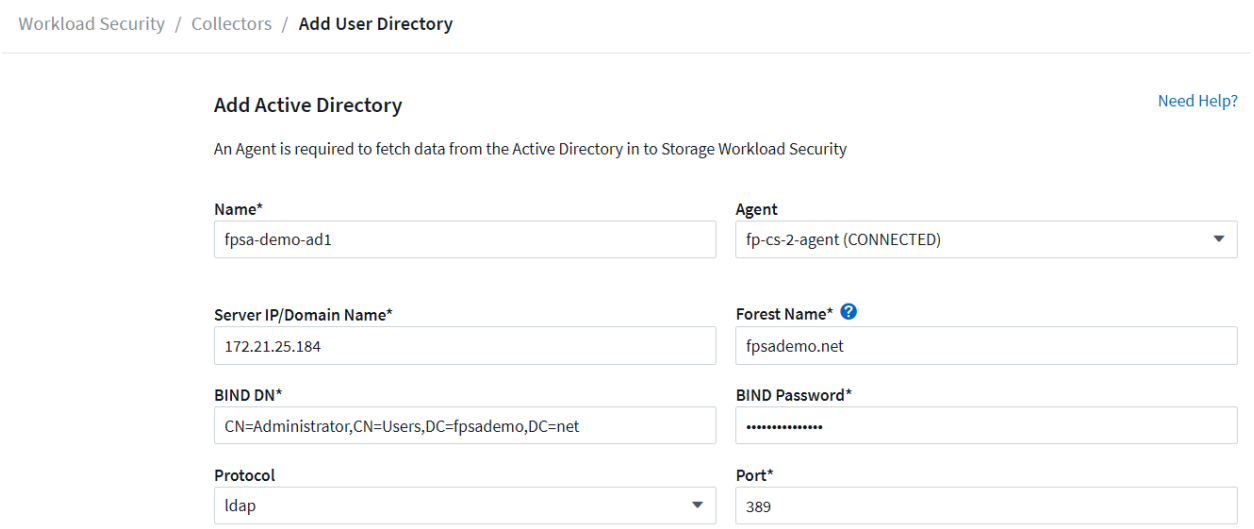
1. In the Data Infrastructure Insights menu, click: **Workload Security > Collectors > User Directory Collectors > + User Directory Collector**.



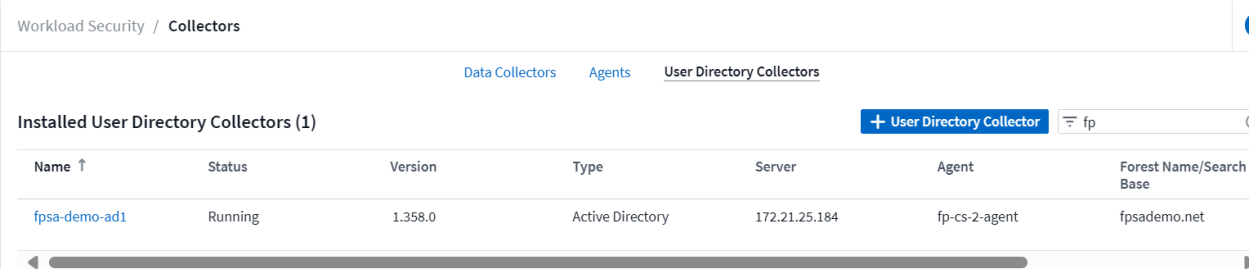
2. The system displays the **Add User Directory** screen. Choose **Active Directory** and click on **Continue.**



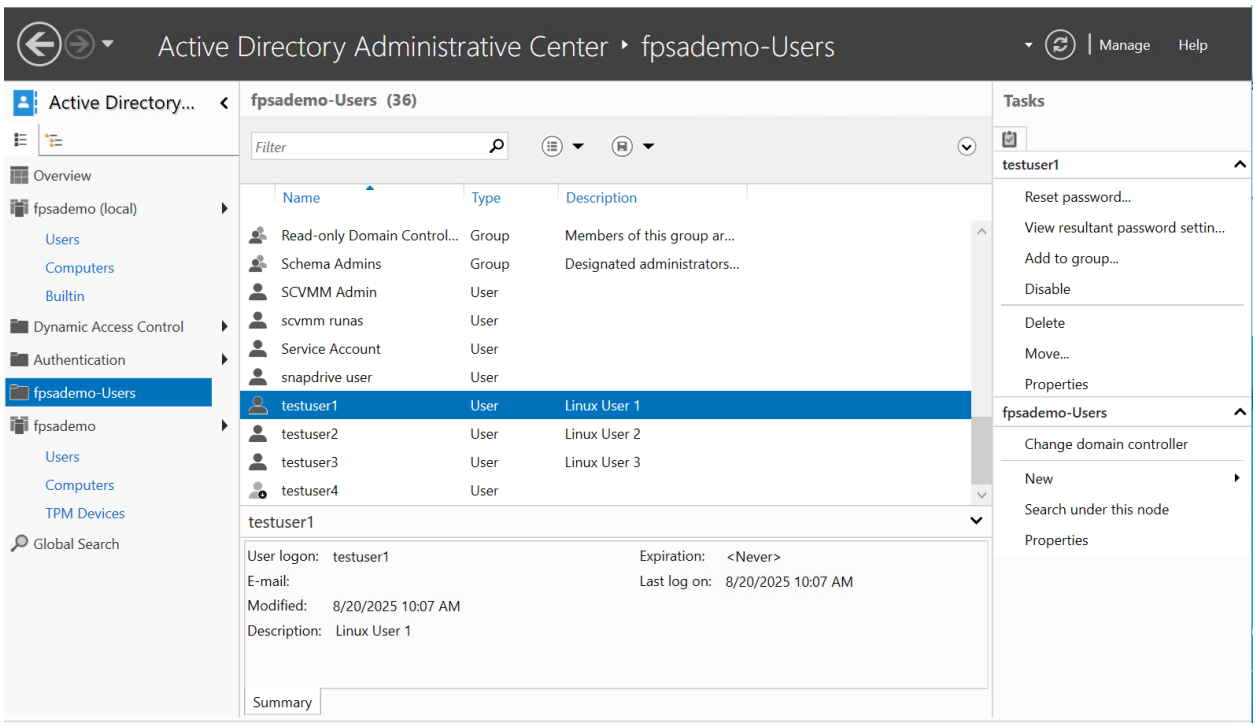
3. Select the agent that you installed previously and enter values in the remaining fields. You can leave the optional attributes with their default values. Click **Save** to add the user directory collector.



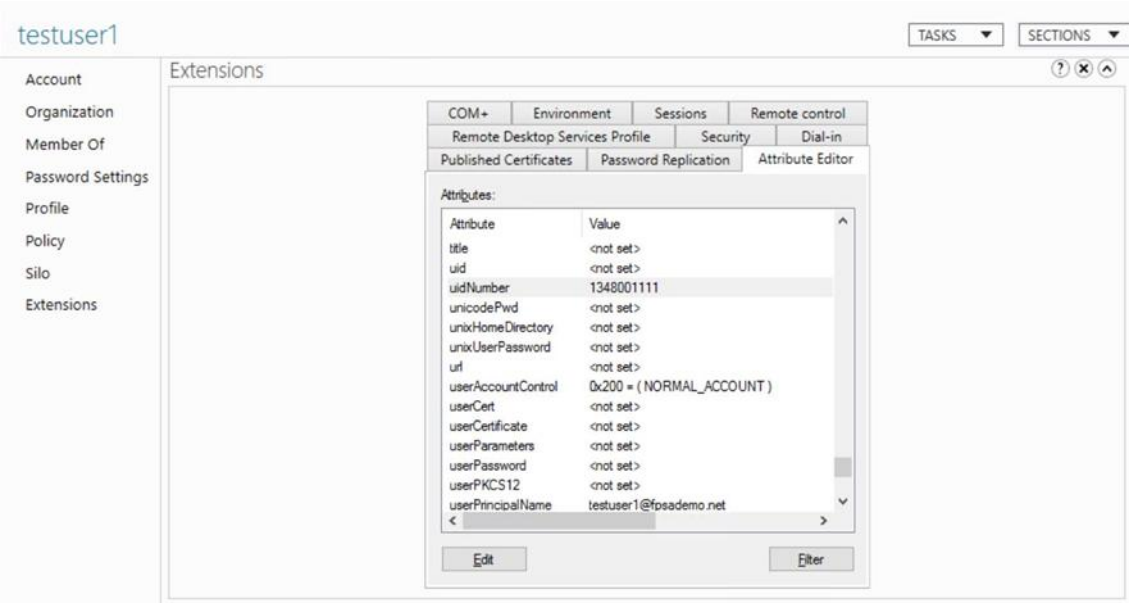
4. Verify that the collector is in the **Running** state.



In the demo environment, the Active Directory server is configured to authenticate Windows and Linux users. The following example displays the users that are configured in the Active Directory.



For the username to display in Data Infrastructure Insights instead of the encoded usernames, the **uid** attribute is configured in Active Directory for each Linux user as shown below. This example shows **testuser1.**



Note: If you have an LDAP server, you can add it to Workload Security as an LDAP directory collector. The procedure is identical to adding an Active Directory. For more information, refer to the following link:

Configuring an LDAP Directory Server Collector

Configure ONTAP data collector

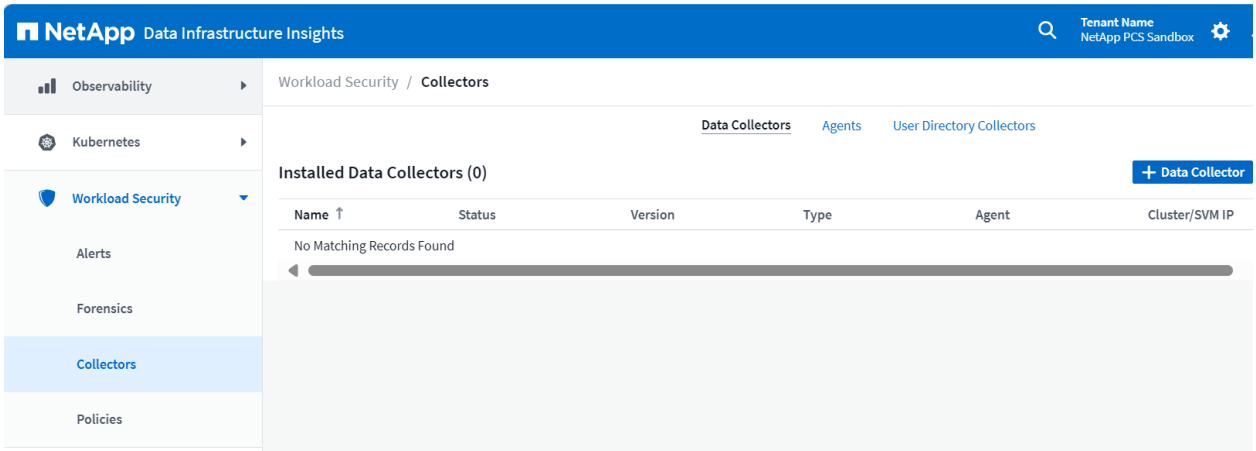
Workload Security currently supports three types of ONTAP data collectors: NetApp ONTAP SVM, NetApp Cloud Volumes ONTAP, and Amazon FSx for NetApp ONTAP. This document focuses on evaluating NetApp ONTAP SVM data collector.

In the FlexPod topology, two SVMs are configured as Workload Security data collectors, "CI_SVM" using NFS protocol and "CI_CIFS_SVM" using CIFS/SMB. Currently, NFS protocol 4.0 and earlier and SMB protocol 3.1 and earlier are supported.

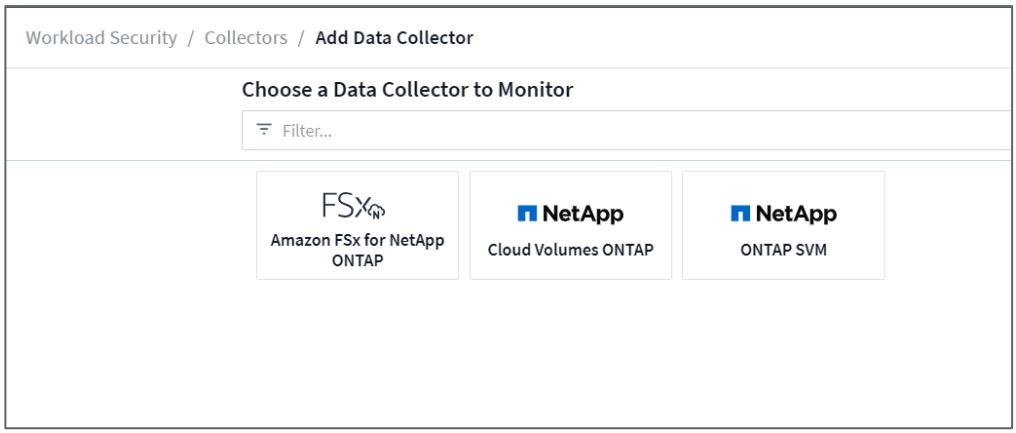
Steps to configure SVM data collector

Follow the procedure to configure two SVM data collectors, one SVM configured for CIFS/SMB protocol and the other for NFS protocol.

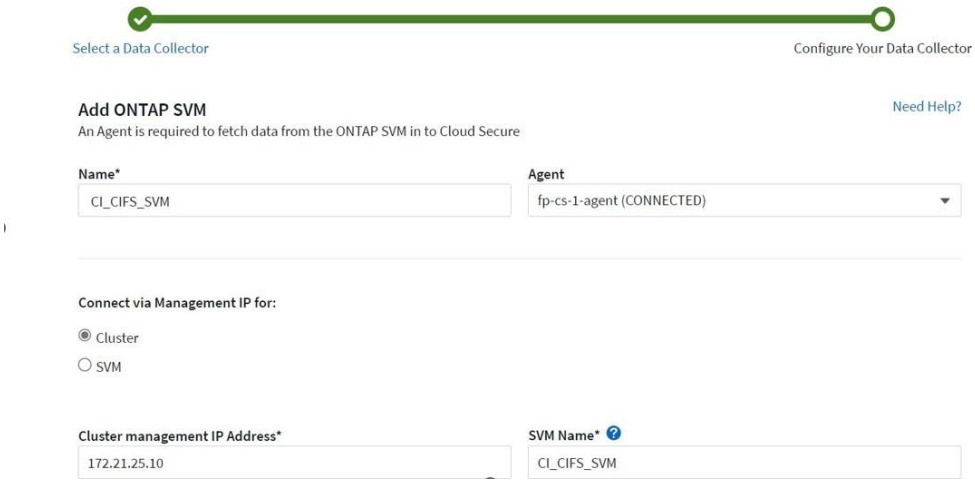
1. Log in as Administrator or Account Owner to your Data Infrastructure Insights environment.
2. Click **Workload Security > Collectors > Data Collectors > +Data Collector**.

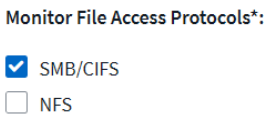


The system displays available data collectors. Choose NetApp ONTAP SVM data collector.



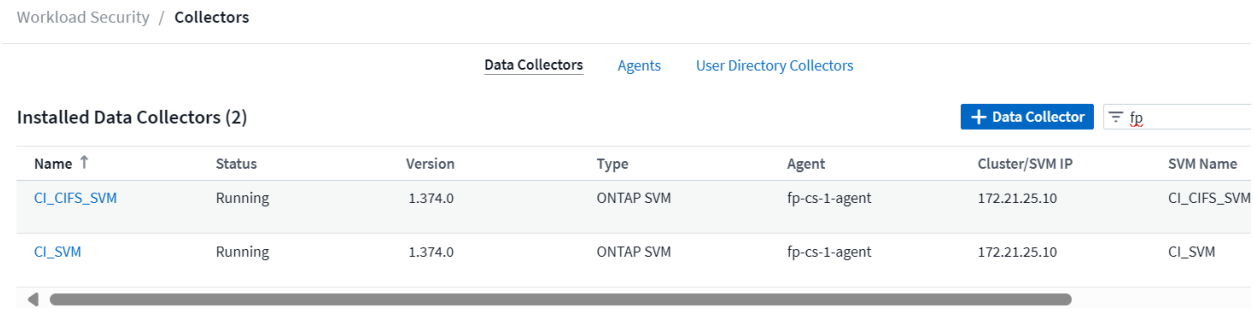
3. Hover over the NetApp SVM tile and click it**.** The system displays the ONTAP SVM configuration page. Enter the required data for each field and click **Save**.





Note: When adding an SVM using a cluster management IP, make sure that the data LIF and management LIF of the SVM are pingable from the agent VM. Check the gateway, netmask, and routes for the LIF for any issues.

4. Repeat the procedure to add the second SVM (CI_SVM) and choose NFS protocol.
5. Click **Workload Security > Collectors > Data Collectors** to verify that the data collectors are in the **Running** state.



6. Log-in to NetApp storage and issue the `<fpolicy show>` command. This command shows policy engine name and status for each SVM that is being monitored. Verify that the status is “on”.

```
A400-G0312::>   fpolicy show
  (vserver fpolicy show)
                                        Sequence
Vserver       Policy Name                Number  Status   Engine
------------- ------------------------ --------  -------- ---------
CI_CIFS_SVM   cloudsecure_CI_CIFS_            1  on       cloudsecu
              SVM1_policy                                 re_CI_
                                                          CIFS_
                                                          SVM1_
                                                          engine
CI_CIFS_SVM   cloudsecure_CI_CIFS_            2  on       cloudsecu
              SVM2_policy                                 re_CI_
                                                          CIFS_
                                                          SVM2_
                                                          engine
CI_SVM        cloudsecure_CI_SVM3_            1  on       cloudsecu
              policy                                      re_CI_
                                                          SVM3_
                                                          engine
CI_SVM        cloudsecure_CI_SVM4_            2  on       cloudsecu
              policy                                      re_CI_
                                                          SVM4_
                                                          engine
4 entries were displayed.
```

7. Issue the `<fpolicy show-engine>` command to verify the FPolicy server status on each node.


```
A400-G0312::> fpolicy show-engine
  (vserver fpolicy show-engine)
                                          FPolicy           Server         Server
Vserver Policy Name   Node                Server            Status         Type
------- ------------- ------------ ----------------- -------------- -----------
CI_CIFS_SVM                                             connected      primary
        cloudsecure_  A400-G0312-  10.61.176.142
        CI_CIFS_SVM1_ 01
        policy
CI_CIFS_SVM                                             connected      primary
        cloudsecure_  A400-G0312-  10.61.176.142
        CI_CIFS_SVM2_ 01
        policy
CI_SVM  cloudsecure_  A400-G0312-  10.61.176.142      connected      primary
        CI_SVM3_      01
        policy
CI_SVM  cloudsecure_  A400-G0312-  10.61.176.142      connected      primary
        CI_SVM4_      01
        policy
CI_CIFS_SVM                                             connected      primary
        cloudsecure_  A400-G0312-  10.61.176.142
        CI_CIFS_SVM1_ 02
        policy
CI_CIFS_SVM                                             connected      primary
        cloudsecure_  A400-G0312-  10.61.176.142
        CI_CIFS_SVM2_ 02
        policy
CI_SVM  cloudsecure_  A400-G0312-  10.61.176.142      connected      primary
        CI_SVM3_      02
        policy
CI_SVM  cloudsecure_  A400-G0312-  10.61.176.142      connected      primary
        CI_SVM4_      02
        policy
8 entries were displayed.
```

Define automated response policies

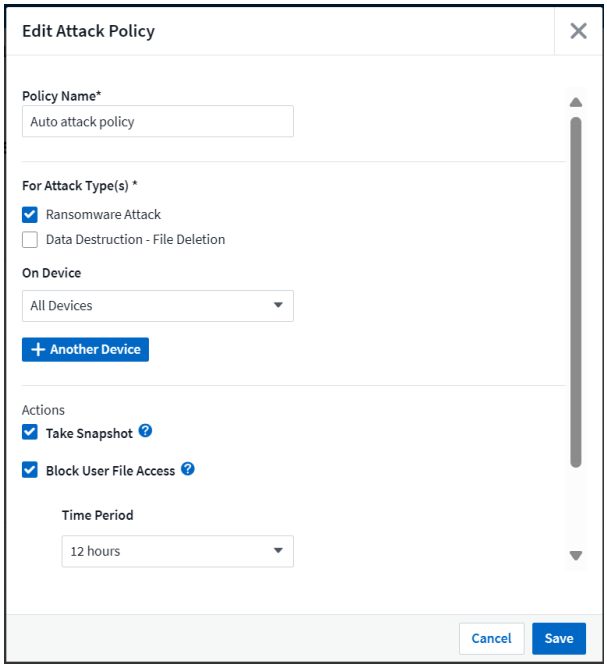
Response policies are used to trigger specific actions in the event of an attack or abnormal user behavior. You can create policies for attacks or warnings and apply them on specific devices or all devices.

Steps to configure automated response policy

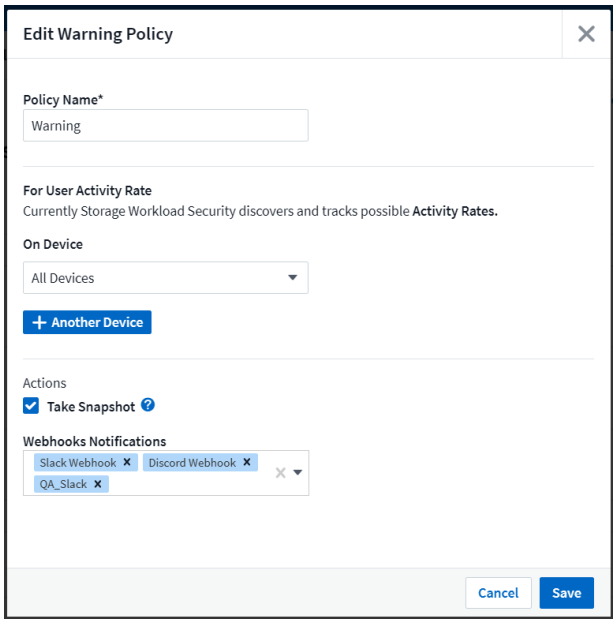
Follow the procedure to configure attack and warning policies.

1. To Create an attack policy, go to **Workload Security > Policies > +Attack Policy**

A sample attack policy is shown below. You can choose attack types and actions that are relevant and the time for which a user is denied file access. The policy can be applied on specific SVMs or all SVMs that are being monitored.

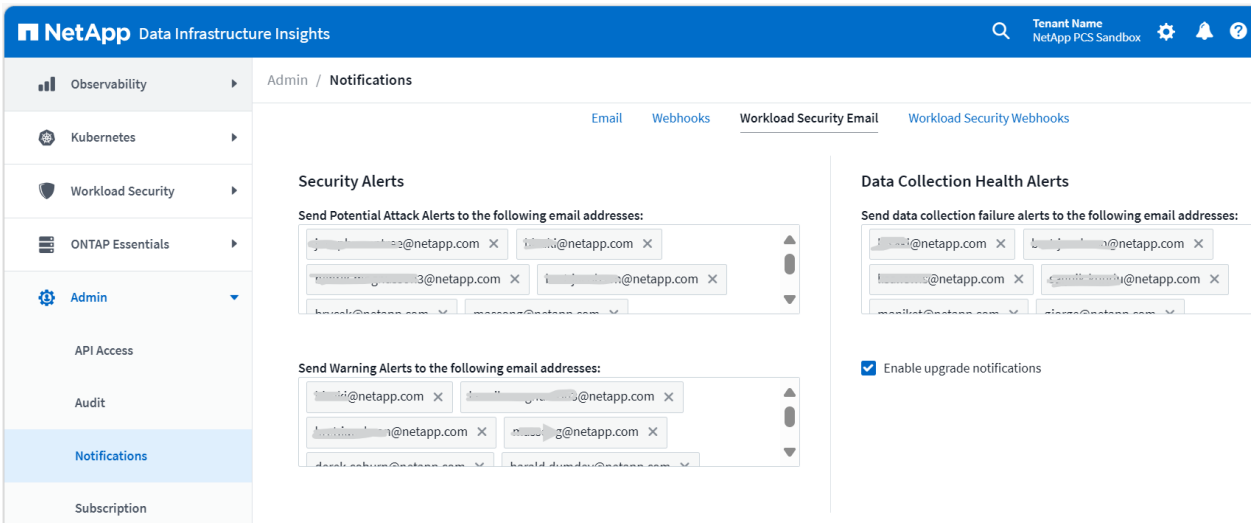


2. To Create a warning policy, go to **Workload Security > Policies > +Warning Policy**
   The attack policy and warning policy in the demo environment is shown below.



Configure email notification

Email notification can be configured for potential attacks, warnings, and agent/data collector health monitoring. To configure Workload Security alert recipients, go to **Admin > Notifications > Workload Security Email** and enter an email address in the appropriate section for each recipient.



Integrating ONTAP Autonomous Ransomware Protection (ARP)

The ONTAP Autonomous Ransomware Protection (ARP) feature uses workload analysis in NAS and SAN environments to proactively detect and warn about abnormal in-file activity that might indicate a ransomware attack. Beginning with ONTAP 9.10.1, ONTAP administrators can enable ARP to proactively detect and warn about abnormal activity that might indicate a ransomware attack. Beginning with ONTAP 9.17.1, ARP also supports block-device volumes, including SAN volumes containing LUNs, or NAS volume containing virtual disks from hypervisors such as VMware, Hyper-V, and KVM.

Workload security can be used to receive ARP events from ONTAP and take the following actions:

- Correlates volume encryption events with user activity to identify malicious user.
- Implements actions defined by automatic response policies such as taking a snapshot and blocking user file access.
- Provides forensics capabilities:

✓ Allow customers to conduct data breach investigations.

✓ Identify what files were affected, helping them to recover faster and conduct data breach investigations.

ARP is a licensed feature. ARP support is included with the **ONTAP ONE** license. If you do not have the ONTAP ONE license, other licenses are available for ARP use that differ depending on the version of ONTAP. For more information on ARP licensing, refer to the following link.

https://docs.netapp.com/us-en/ontap/anti-ransomware/index.html

Prerequisites

1. Storage VM (SVM) with NAS (NFS, SMB) or SAN (iSCSI, FC or NVMe).
2. Recommended Minimum ONTAP version: 9.11.1.

3. ARP enabled volumes.
4. Workload Security collector should be added via cluster IP.
5. Cluster level credentials must be used when adding the SVM.

Enable ONTAP Autonomous Ransomware Protection

ARP must be enabled via ONTAP System Manager or ONTAP CLI. Data Infrastructure Insights/Workload Security cannot enable ARP. ARP operational behavior changes between ONTAP releases as shown below.

- **(NAS environments only) For ONTAP 9.10.1 to 9.15.1 or ARP with FlexGroup volumes**
  For these versions of ONTAP, you should always enable ARP initially in learning mode (or "dry-run" state). When you first enable ARP in learning mode, the system analyzes the workload to characterize normal behavior. Beginning in active mode can lead to excessive false positive reports.

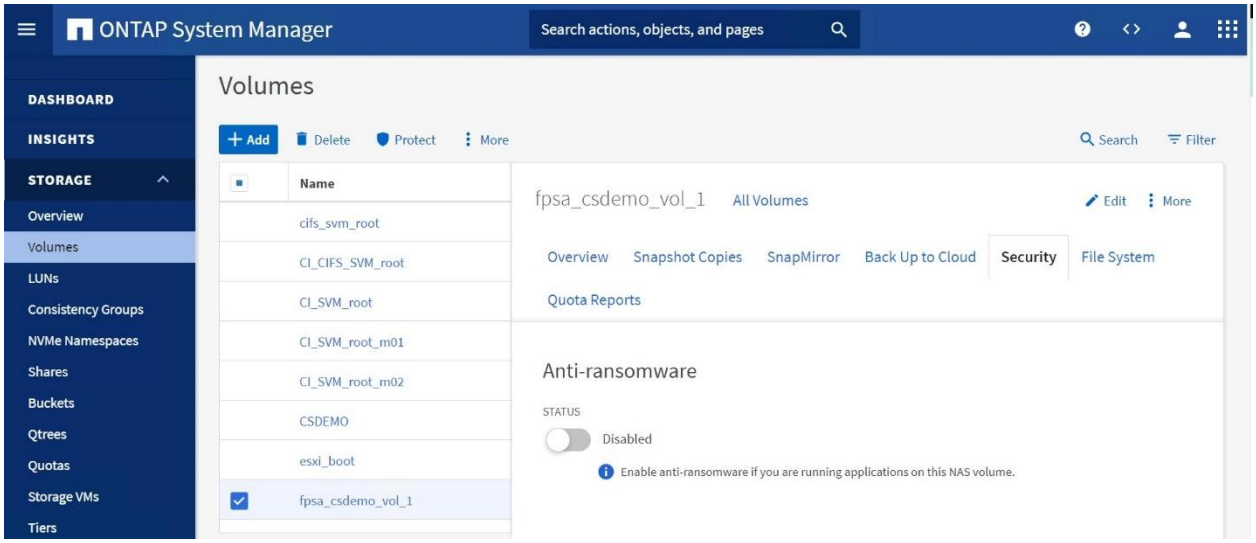
It's recommended that you let ARP run in learning mode for a minimum of 30 days. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which might occur before 30 days.

- **(NAS environments only) For ONTAP 9.16.1 and later with FlexVol volumes**
  When you enable ARP using System Manager or the CLI, ARP/AI protection is enabled and active immediately. No learning period is required.
- **(SAN environments only) For ONTAP 9.17.1 and later with FlexVol volumes**
  When you enable ARP using System Manager or the CLI, ARP/AI functionality is automatically enabled. Once enabled on a SAN volume, ARP/AI monitors data continuously during an evaluation period to determine if the workloads are suitable for ARP and sets an optimal encryption threshold for detection.

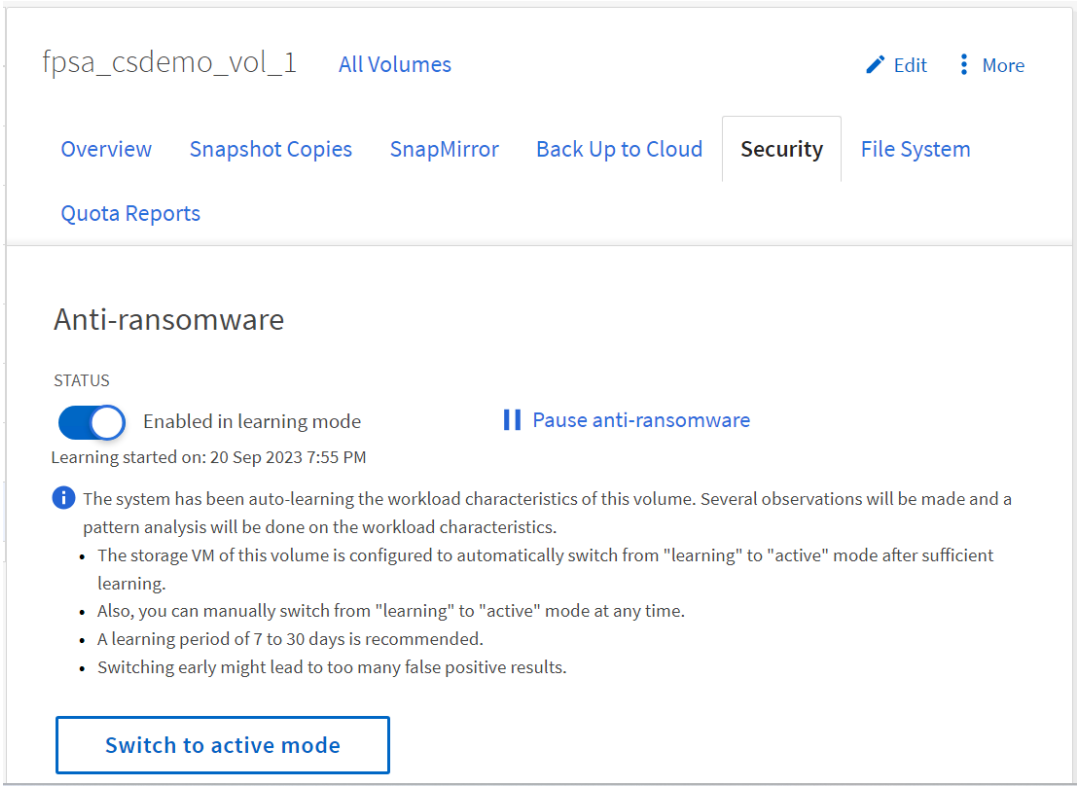
Steps:

1. In ONTAP System Manager, select **Storage > Volumes**, then select the volume you want to protect.
2. In the **Security** tab of the Volumes overview, select **Status** to switch from Disabled to Enabled.
3. When the learning period is over, switch ARP to active mode.

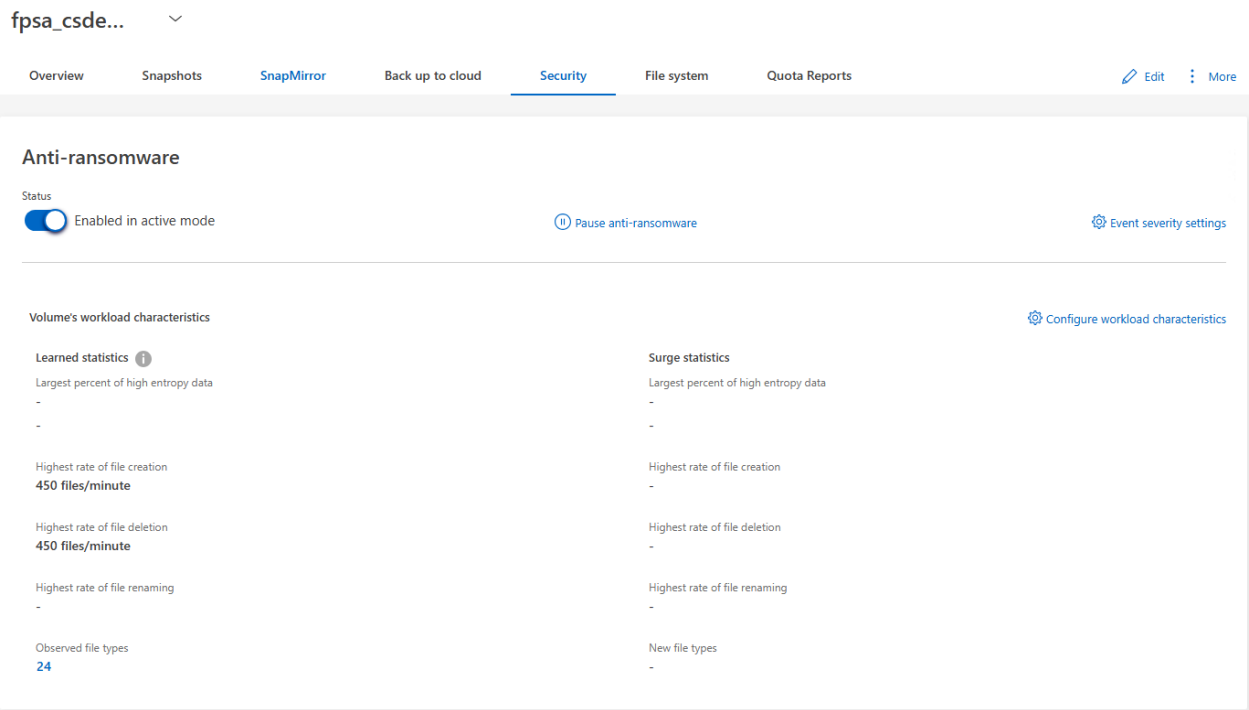
The following screenshots display ONTAP System Manager user interface to enable ARP.



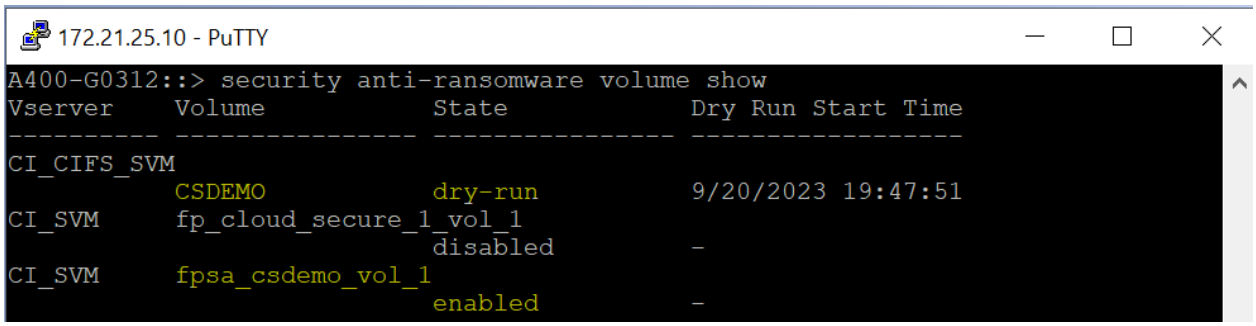
The following screenshot displays the status of ARP when it is enabled and running in learning mode (ONTAP 9.10.1-9.15.1). You can disable, pause or switch to active mode from this screen.

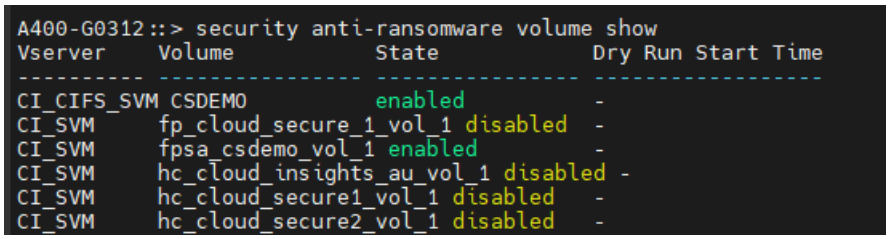


The following screenshot displays ARP running in “active” mode.



You may check the status of all ARP enabled volumes using ONTAP CLI, as shown below.





For more details on enabling and managing ARP via GUI or CLI, refer to the following link.

https://docs.netapp.com/us-en/ontap/anti-ransomware/enable-task.html

Fine tuning attack detection parameters

When Autonomous Ransomware Protection (ARP) is running in learning mode, it develops baseline values for file entropy, file extensions and IOPs for the specific ARP enabled volume. Entropy is an evaluation of the randomness of data in a file by ONTAP for use in determining suspicious file manipulation. File IOPs are a record of how many files were created, renamed, and deleted. These baselines are used to evaluate ransomware threats when ARP is switched to Active mode.

Beginning in ONTAP 9.11.1, you can modify the parameters for ransomware detection on a specific ARP-enabled volume. Adjusting detection parameters helps improve the accuracy of reporting based on your specific volume workload.

You can modify the attack detection parameters using "***security anti-ransomware volume attack-detection-parameters modify***" command. The following screenshot displays the default parameters that are enabled on ARP-enabled volume in the test environment. These parameters can be modified to suit the specific volume workload requirements.

```
A400-G0312::> security anti-ransomware volume attack-detection-parameters show -vserver CI_SVM -volume fpsa_csdemo_vol_1
                                          Vserver Name : CI_SVM
                                           Volume Name : fpsa_csdemo_vol_1
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                  Is Detection Based on File Create Rate? : true
                  Is Detection Based on File Rename Rate? : true
                  Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24

A400-G0312::>
```

ARP Thresholds

ARP assesses threat probability based on incoming data measured against learned analytics. When ARP detects an abnormality, a measurement is assigned. A snapshot might be assigned at the time of detection or at regular intervals depending on the ONTAP version.

- **Low**:

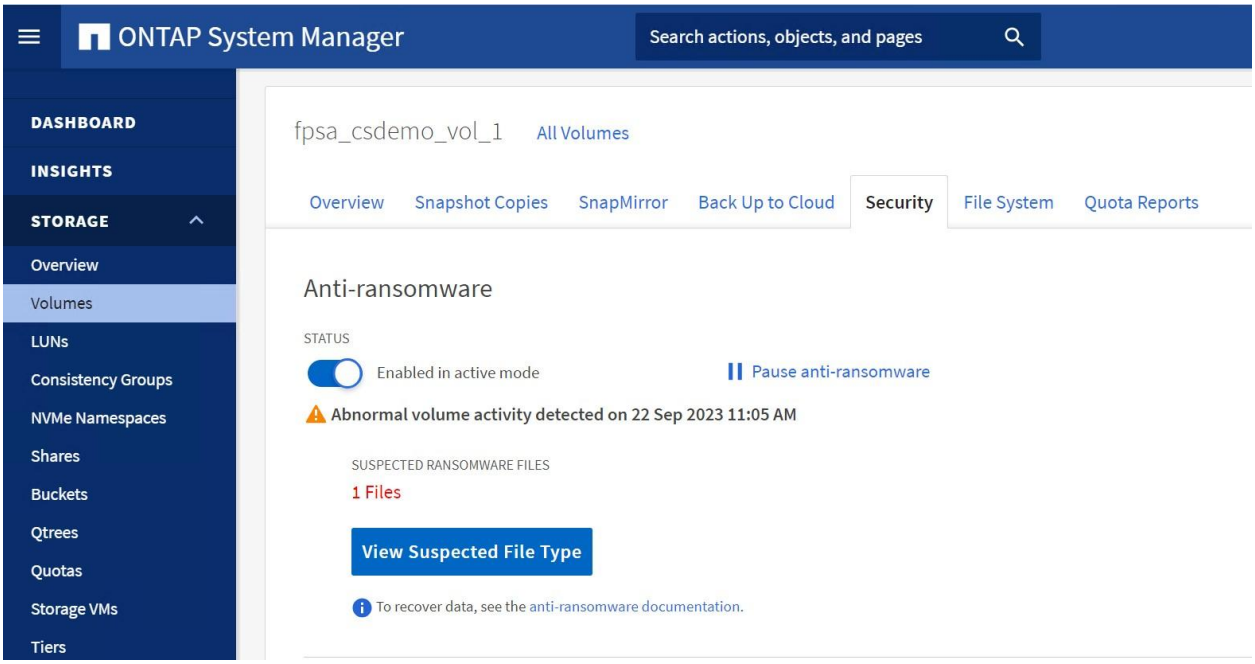
  The earliest detection of an abnormality in the volume (for example, a new file extension is observed in the volume). This level of detection is only available in versions prior to ONTAP 9.16.1 that do not have ARP/AI.

  - In ONTAP 9.10.1, the threshold for escalation to moderate is 100 or more files.
  - Beginning with ONTAP 9.11.1, you can customize the detection parameters for ARP.

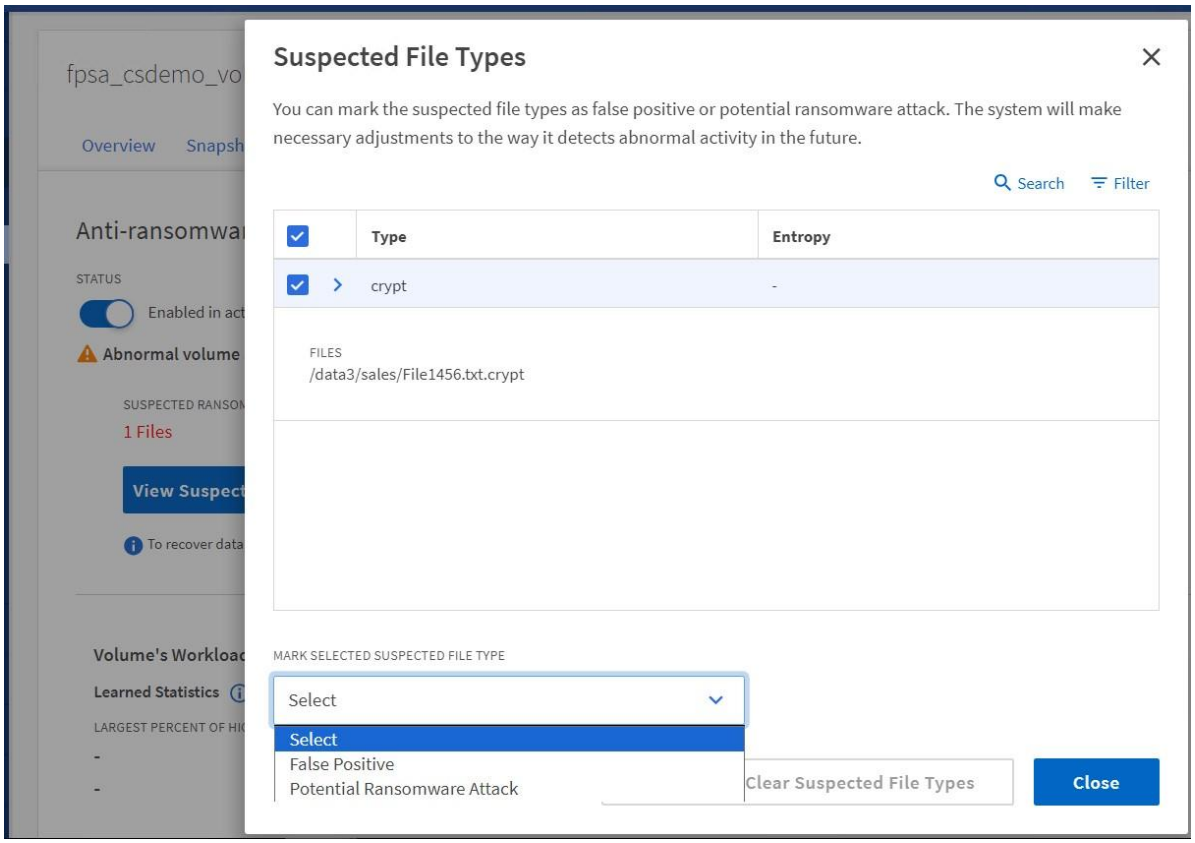
- **Moderate**:

  High entropy is detected or multiple files with the same never-seen-before file extension are observed. This is the baseline detection level in ONTAP 9.16.1 and later with ARP/AI.

By default, the never-seen-before file extension count is set to 20. When a never-seen-before file extension is detected on an ARP enabled volume, ONTAP sets **attack probability** as **low**. A volume snapshot is created proactively with a tag **anti-ransomware-backup**. The attack probability continues to be low when there are not enough file extensions, or file extension and high entropy together as defined by the attack detection parameters. When attack probability is low, an alert is not sent to event management system, however a warning will show up in system manager as shown below.



The administrator can check the suspected file type and mark it as false positive or potential ransomware attack from System Manager or CLI, as shown in the following screen. Once marked as false-positive, the newly found file extension will be considered a valid extension, and future attacks will not be reported on this file extension. The snapshot taken will be deleted immediately.



The threat escalates to moderate after ONTAP runs an analytics report determining if the abnormality matches a ransomware profile. When the attack probability is moderate, ONTAP generates an EMS notification prompting you to assess the threat. ONTAP does not send alerts about low threats; however, beginning with ONTAP 9.14.1, you can modify default alert settings.

You may view the attack probability and observe file extensions using the following CLI commands.

```
security anti-ransomware volume show -vserver <vserver name> -volume <volume name>
security anti-ransomware volume workload-behavior show -vserver <vserver name> -volume <volume
name>
```

You may mark a suspected file type as false positive using the following command.

```
security anti-ransomware volume attack clear-suspect -vserver <vserver name> -volume <volume
name> -extensions <extension name> -false-positive {true|false}
```

The following screenshot displays the attack probability and file extension information captured from the test environment.


```
172.21.25.10 - PuTTY
A400-G0312::>  security anti-ransomware volume show -vserver CI_SVM -volume fpsa_csdemo_vol_1

      Vserver Name: CI_SVM
       Volume Name: fpsa_csdemo_vol_1
             State: enabled
Dry Run Start Time: -
Attack Probability: low
   Attack Timeline: 9/22/2023 11:05:55
 Number of Attacks: 1

A400-G0312::> security anti-ransomware volume workload-behavior show -vserver CI_SVM -volume fpsa_csdemo_vol_1
                                       Vserver: CI_SVM
                                        Volume: fpsa_csdemo_vol_1
                       File Extensions Observed: swp, swx, txt~, log, log~,
                                                 sh, swpx, sh~, crypt
              Number of File Extensions Observed: 9

 Historical Statistics
              High Entropy Data Write Percentage: -
   High Entropy Data Write Peak Rate (KB/Minute): -
              File Create Peak Rate (per Minute): 150
              File Delete Peak Rate (per Minute): 150
              File Rename Peak Rate (per Minute): -

 Surge Observed
                                   Surge Timeline: -
              High Entropy Data Write Percentage: -
   High Entropy Data Write Peak Rate (KB/Minute): -
              File Create Peak Rate (per Minute): -
              File Delete Peak Rate (per Minute): -
              File Rename Peak Rate (per Minute): -
                  Newly Observed File Extensions: crypt
        Number of Newly Observed File Extensions: 1

A400-G0312::>
```

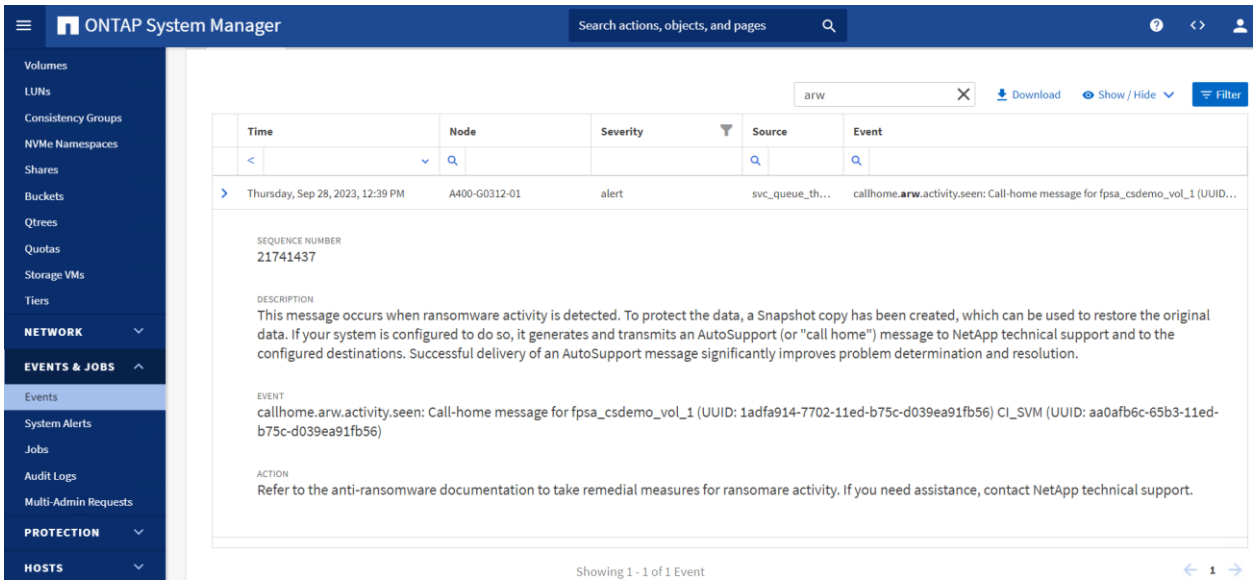
Attack probability will change from **low** to **moderate** when the never-seen-before file extension count exceeds the configured parameter. When this happens EMS notification is generated and can be observed on ONTAP CLI and System Manager Events page as shown below.

```
172.21.25.10 - PuTTY
A400-G0312::> security anti-ransomware volume show -vserver CI_SVM -volume fpsa_csdemo_v
ol_1

      Vserver Name: CI_SVM
       Volume Name: fpsa_csdemo_vol_1
             State: enabled
Dry Run Start Time: -
Attack Probability: moderate
   Attack Timeline: 9/27/2023 13:21:15
 Number of Attacks: 1

A400-G0312::> event show -message-name *arw*
Time                Node             Severity      Event
------------------- ---------------- ------------- ---------------------------
9/28/2023 12:39:04  A400-G0312-01    ALERT         callhome.arw.activity.seen: Call-home
 message for fpsa_csdemo_vol_1 (UUID: 1adfa914-7702-11ed-b75c-d039ea91fb56) CI_SVM (UUID
: aa0afb6c-65b3-11ed-b75c-d039ea91fb56)

A400-G0312::>
```

Considerations and Limitations

1. ARP runs in a learning (or dry-run) mode before it can be switched to Active mode. Beginning in ONTAP 9.13.1, adaptive learning has been added to ARP analytics, and the change over from learning mode to active mode is done automatically. Note that Workload Security feature in Data Infrastructure Insights does not have a learning mode and is fully functional from day 1.
2. With ARP/AI and FlexVol volumes, there is no learning period. ARP/AI is enabled and active immediately after installation or upgrade to ONTAP 9.16.1 for NAS and ONTAP 9.17.1 for SAN. After upgrading your cluster to these releases, ARP/AI will be automatically enabled for existing and new FlexVol volumes if ARP is already enabled for those volumes.
3. In ONTAP 9.16.1 and earlier, ARP creates a snapshot when early signs of an attack are detected. Beginning with ONTAP 9.17.1, ARP snapshots are generated at regular intervals for both NAS and SAN volumes.
4. In cases where an SVM is not monitored by Workload Security, but there are ARP events generated by ONTAP, the events will still be received by Data Infrastructure Insights. However, Forensic information related to the alert, as well as user mapping, will not be captured or shown.
5. As of this writing, ARP is not supported on ONTAP S3 environments.

For more information, refer to the following link.

Autonomous Ransomware Protection use cases and considerations (netapp.com)

Note:

No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. Although it's possible an attack might go undetected, NetApp Autonomous Ransomware Protection (ARP) acts as an important additional layer of defense if anti-virus software has failed to detect an intrusion. ARP can detect the spread of most ransomware attacks only after a small number of files are encrypted, but it takes actions automatically to protect data, and alert you that a suspected attack is happening.

Workload Security - Case study

This section describes a few use cases and examines how Workload Security can help with problem detection, alerting and data forensics.

Accidental file deletion

Problem statement

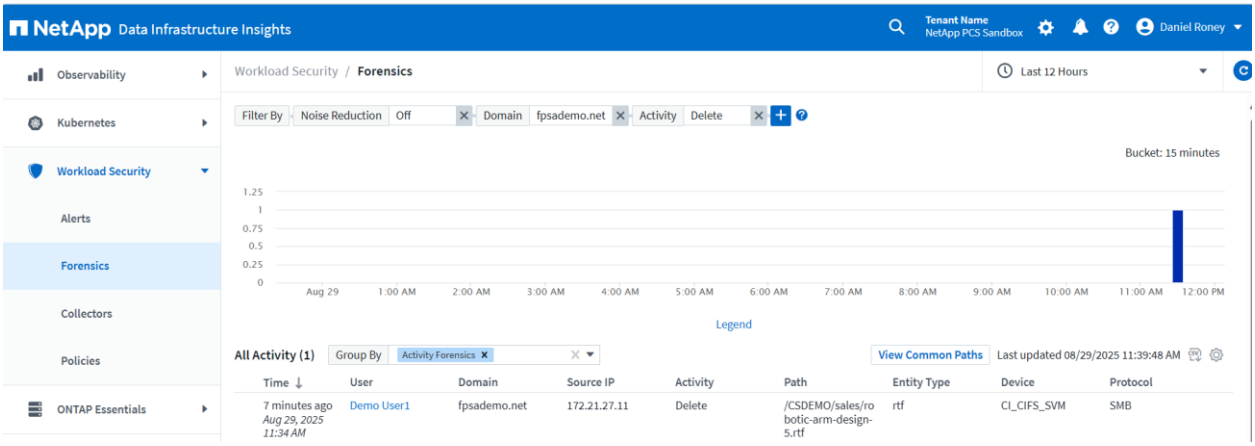
A user reported that a file “robotoc-arm-design5.rtf” that he accessed few hours ago is missing from an SMB share.

Analysis

The Workload Security forensics page can be used to look at all file deletion activities during a specified time period. The results can be filtered based on several criteria such as user, time, domain, activity, path, device (SVM) and so on.

In this example, all deletion activities in the last 12 hours are checked to track down the reported file deletion.

Go to **Workload Security > Forensics > Activity Forensics** and filter **All Activity** by “domain” and “delete” activity.



In this example, Workload Security has registered the deletion activity and displayed the username, source IP and time of the activity. This provides a baseline for additional investigation and file restoration.

Takeaway

The Workload Security forensics feature can be used to quickly identify details of a file deletion.

A sensitive file is copied to a public folder accidentally.

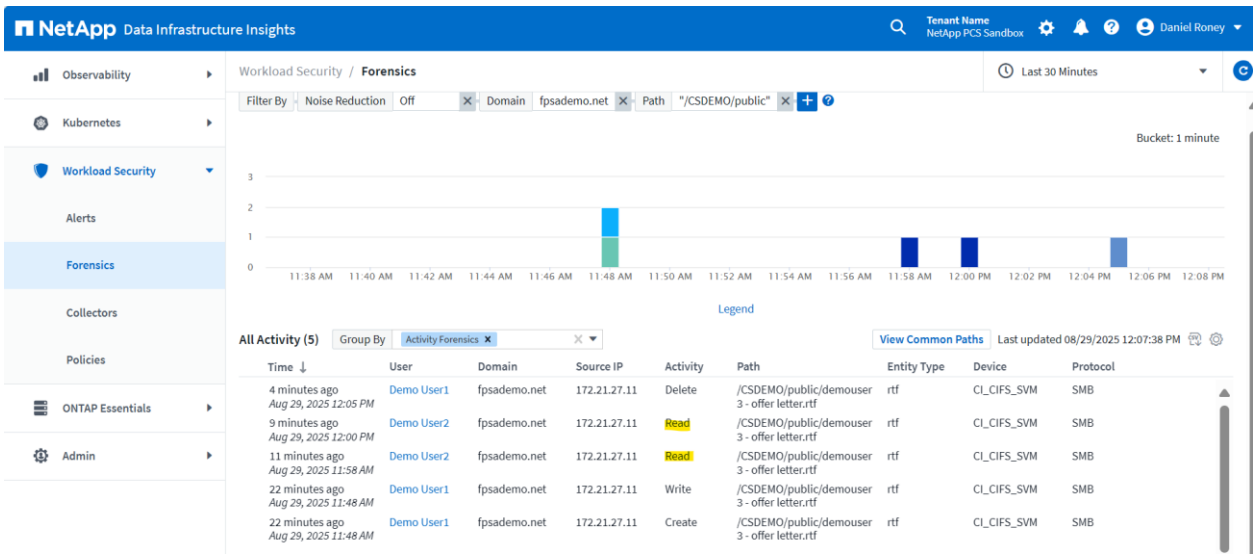
Problem statement

A HR employee has copied an offer letter to a public folder accidentally. The employee realized this mistake in 20 minutes and deleted the file, however he was not sure if someone else had copied or opened this file.

Analysis

The Workload Security forensics page is used to check all file activities in the public folder and to see if anyone has read the file.

To check this, go to **Workload Security > Forensics > Activity Forensics** and filter **All activity** by domain name and file path.



In this example, all activities related to the file are displayed with time stamp, username, and activity type. **Demo User1** is the HR employee who copied the file into the public directory and **Demo User2** is the employee who read the file. Later **Demo User1** deleted the file from public folder. Workload Security tracked all file activities on the file from creation to deletion and this helped to find out if another user had opened the file before the original user has deleted it from the public directory.

Takeaway

Workload Security can track all activities on files in a SMB/CIFS or NFS share that is being monitored. This feature is extremely useful when tracing activities related to sensitive data files.

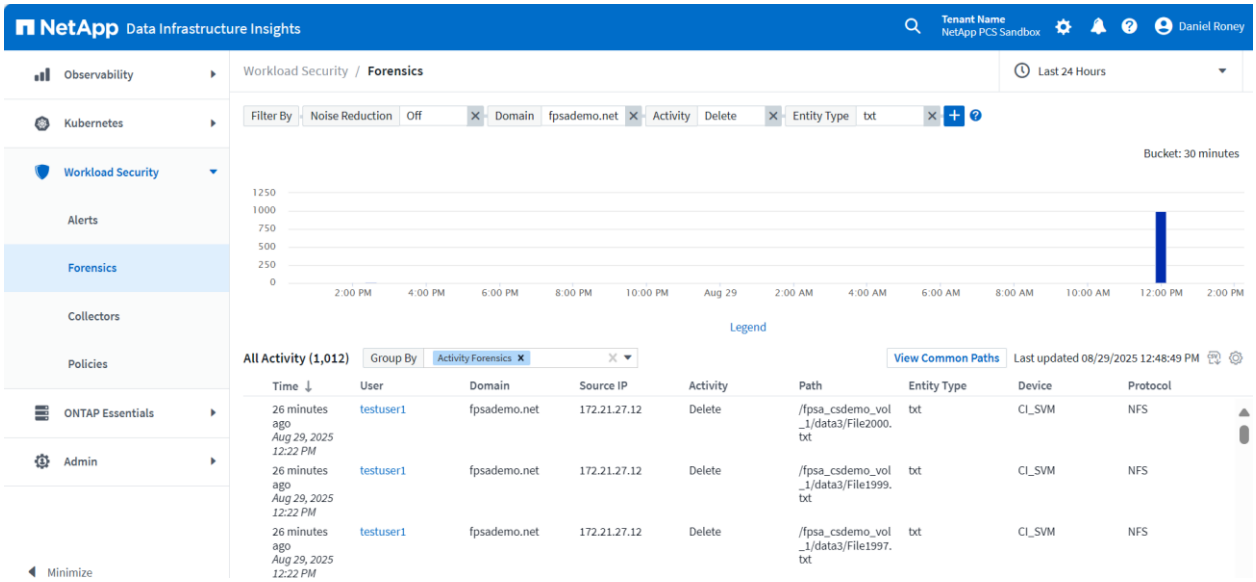
Bulk file deletion

Problem statement

A user reported that several text files that were available the previous day are missing from an NFS share.

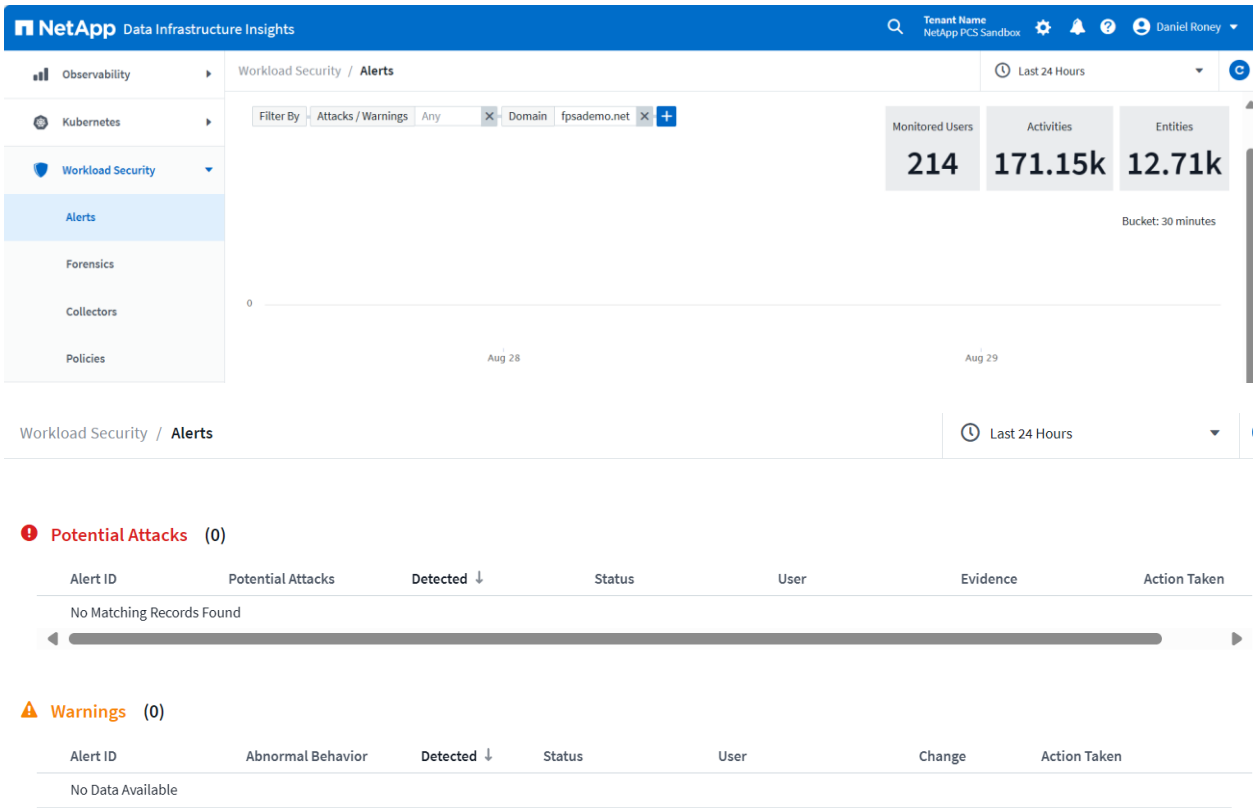
Analysis

Data Infrastructure Insights was launched to do forensics on this incident. The file activities for the last 24 hours were filtered based on activity “delete” and entity type “txt” to find details on the deletion activity.



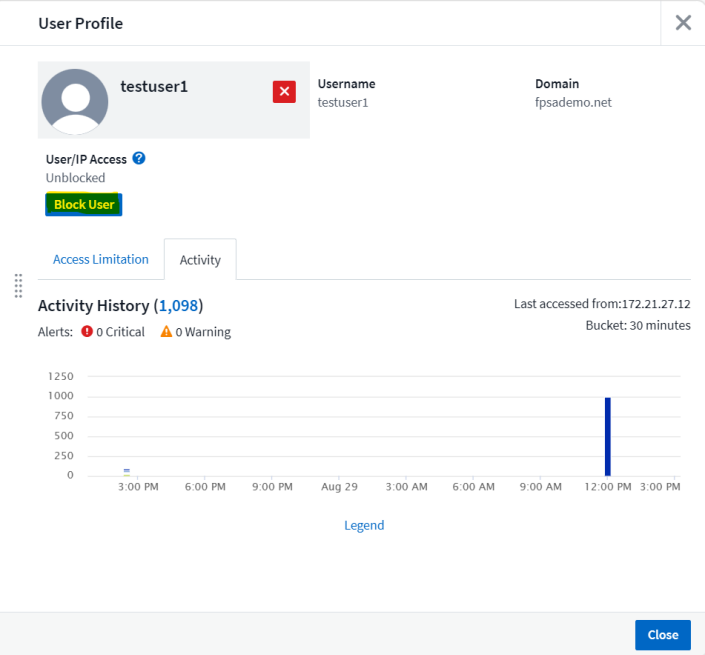
In this example, there was one bulk file deletion activity that involved 1000 text files.

There were no data destruction alerts generated for this activity and this can be checked from the **Alerts** page. Click on **Alerts** and filter by **Attack/Warnings** and choose **Data Destruction File Deletion**.

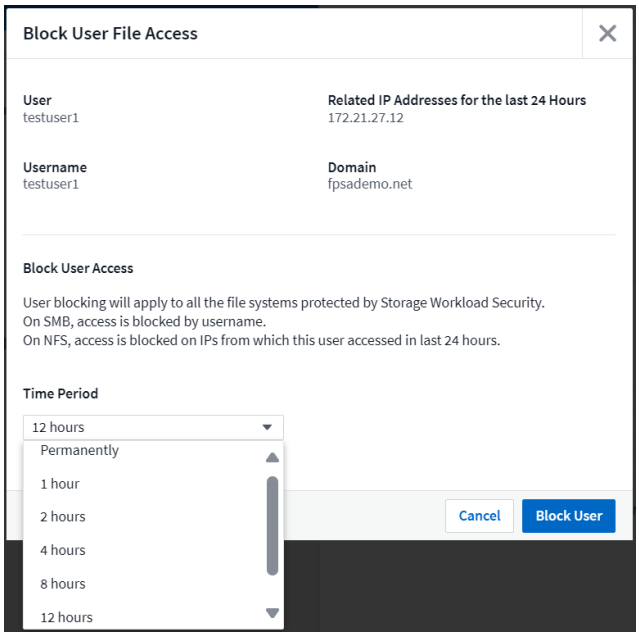


Note that the Data Infrastructure Insights administrator can block the user from accessing the shares while the investigation is ongoing. To do this, click on the **username,** this redirects to the user profile where there is an option to block the user for a specified duration. If the investigation proves the ill intent of the user, the administrator can block the user permanently.

The following example shows the user profile for “**testuser1**”.



Note that the administrator can block the user permanently or up to 24 hours by clicking on **Block User** button.



Takeaway

Using Workload Security, the Data Infrastructure Insights administrator could provide the details of the bulk file deletion activity that affected 1000 text files. The Data Infrastructure Insights administrator could also block the user for a specific duration while the investigation was in progress.

You might wonder why there were no alerts generated for bulk deletion even though the attack policy was configured for “Data destruction and File deletion”. File deletion is a common activity, and a data destruction alert is generated only for abnormal mass file deletion activity. Workload Security first needs to learn the user behavior of individual users and user groups. It then establishes a baseline and looks for a change in behavior. The baseline established for this user was not sufficient to prove any ill intent, therefore no alert was generated. Note that for ransomware detection, Data Infrastructure Insights does not require any training and is effective from day 1.

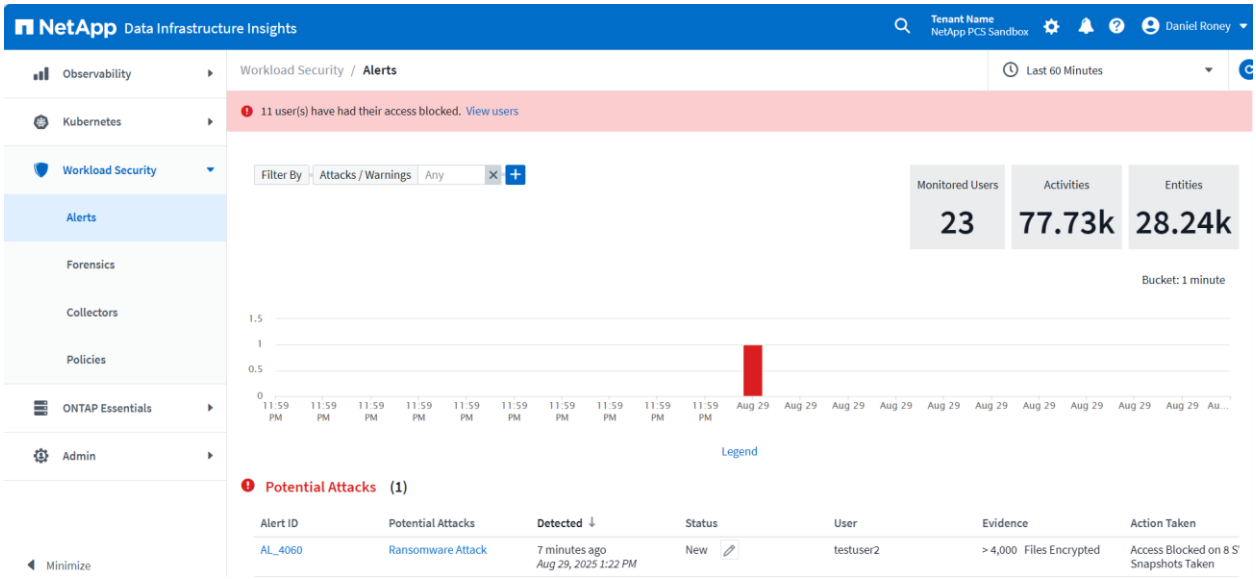
Ransomware attack simulation via Bulk File Encryption

Problem statement

Data Infrastructure Insights administrator received an email alert of a potential ransomware attack.

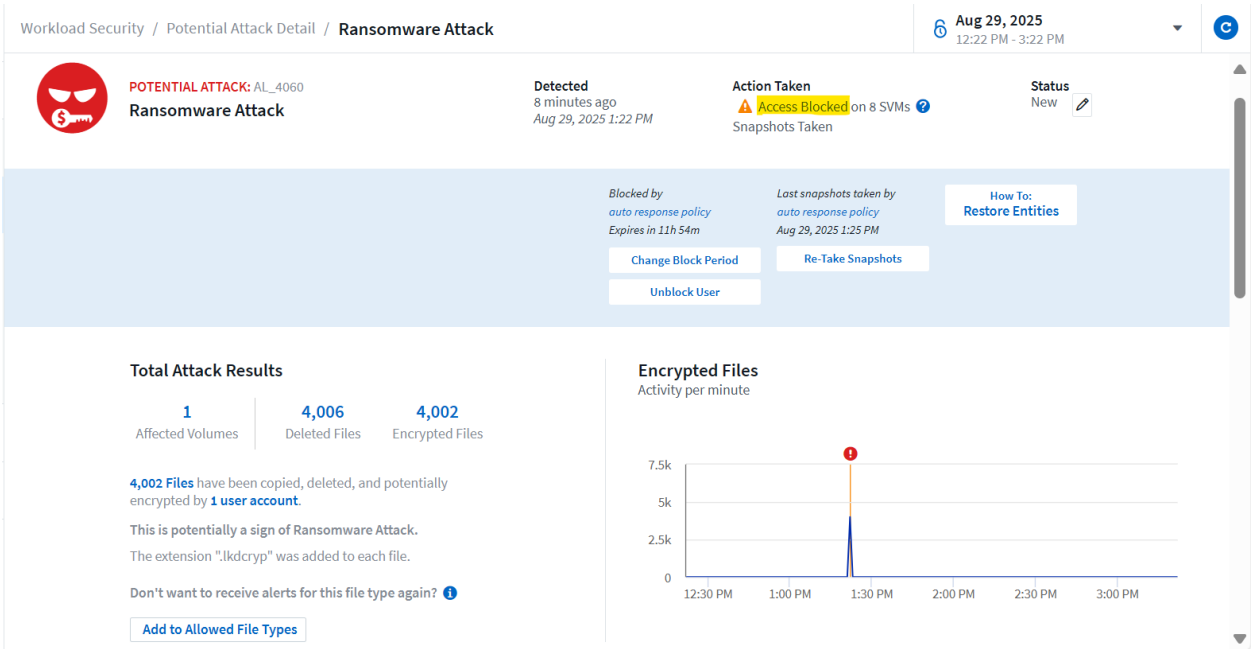
Analysis

Data Infrastructure Insights is launched to check on the alert. It reports that more than 4000 files are encrypted by **testuser2.**



.

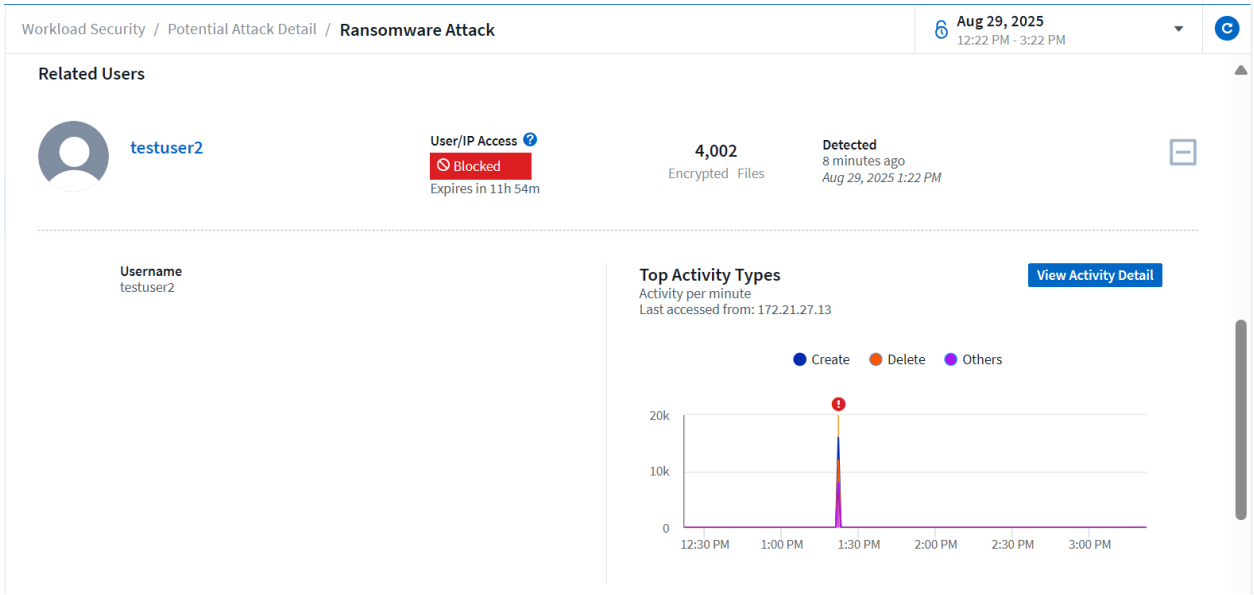
Click on the **Alert ID** to see the details of the attack and the action taken

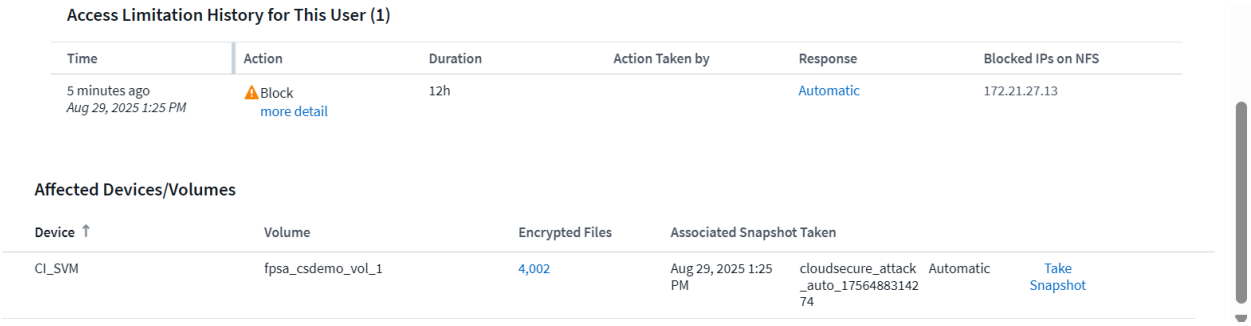


As you can see, the auto response policy is triggered, and it blocked the user for 12 hours, which is the configured duration in the auto response policy. A Snapshot is taken with the name starting with "**cloudsecure_attack_auto_**".

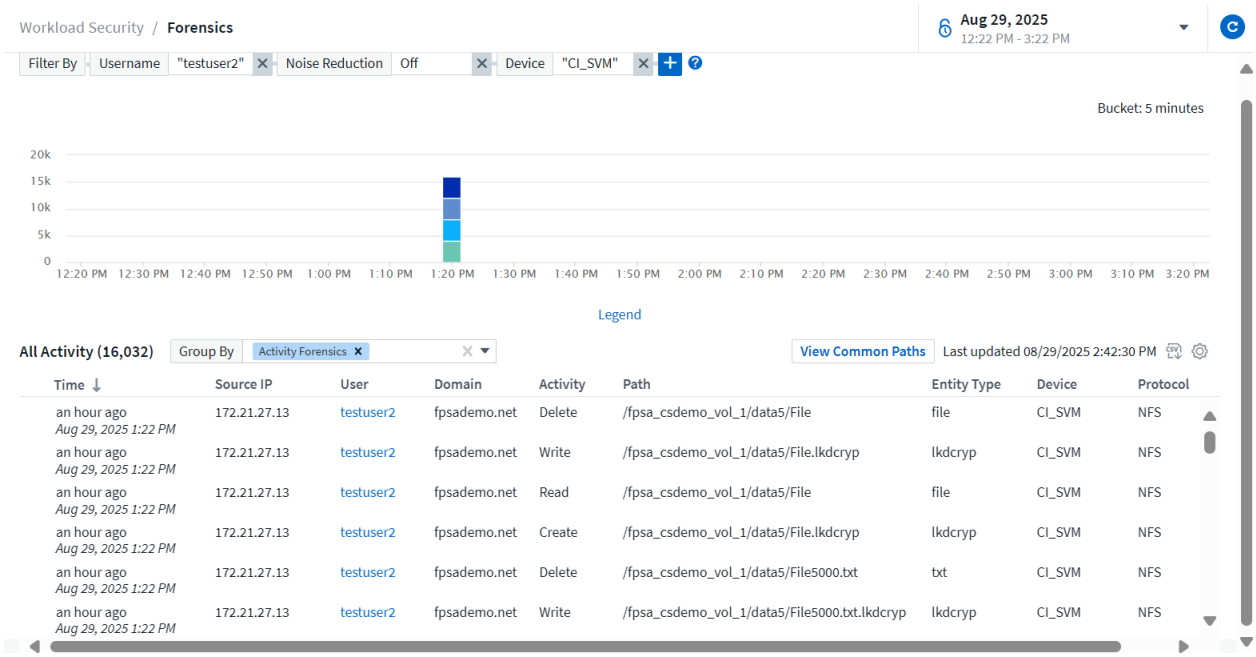
Note that this screen also provides additional options to change the block period or unlock the user if it is found to be a legitimate activity.

If you scroll down, you can see additional information on the user and IP address of last access, history, affected volume and Snapshot information.





If you click on View Activity Detail, you can see more details on the files affected.



Log in to the Linux host as **testuser2** and try to access the NFS share.

```
testuser2@fpsademo.net@fpsa-demo-linux2:/$ cd /csdemo/data5
-bash: cd: /csdemo/data5: Permission denied
testuser2@fpsademo.net@fpsa-demo-linux2:/$ df -k
Filesystem                        1K-blocks    Used Available Use% Mounted on
tmpfs                                400584    1320    399264   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  10218772 6243084   3435016  65% /
tmpfs                               2002916       0   2002916   0% /dev/shm
tmpfs                                  5120       0      5120   0% /run/lock
/dev/sda2                           1790136  257080   1423796  16% /boot
tmpfs                                400580       4    400576   1% /run/user/1348001117
testuser2@fpsademo.net@fpsa-demo-linux2:/$
```

In this example, the user cannot see the NFS mount point, and the directory access is denied.

Takeaway

Workload Security can effectively detect, and report ransomware attacks based on changes in user data access patterns. In this use case, a user encrypted large number of text files in a monitored NFS share. Workload Security quickly flagged it as a potential ransomware attack and blocked the user. An alert was generated for the Data Infrastructure Insights administrator to analyze the activity and unblock the user if it is found to be a legitimate activity. A volume Snapshot copy was also taken in case the data needs to be restored.

Data Infrastructure Insights API and Splunk Integration

This section gives a brief overview of Data Infrastructure API and how it can be integrated with external monitoring tools such as Splunk.

Data Infrastructure Insights API

The Data Infrastructure Insights API enables NetApp customers and independent software vendors (ISVs) to integrate Data Infrastructure Insights with other applications, such as ticketing systems and SIEM tools such as Splunk. The basic requirements for API access are:

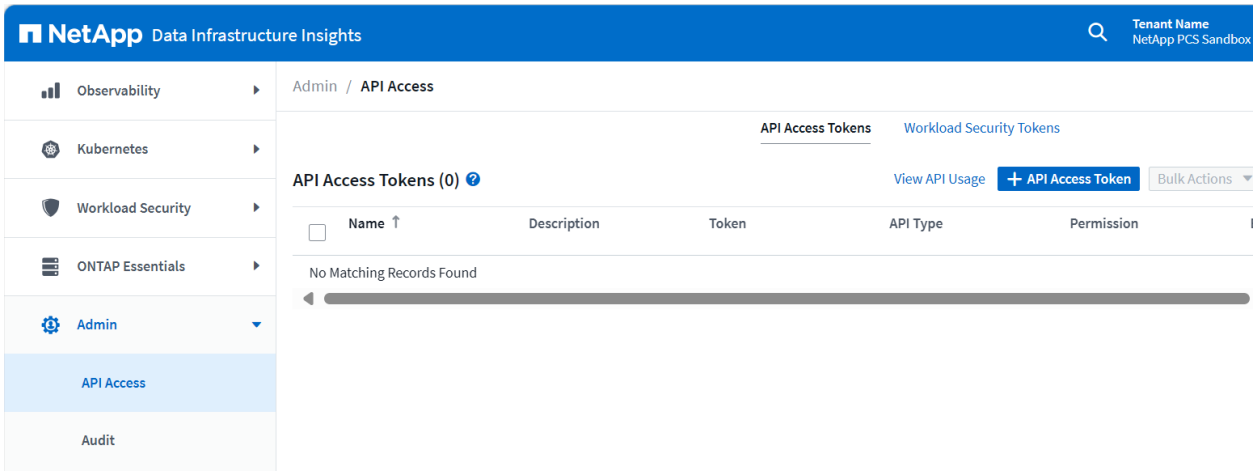
- An API access Token model that is used to grant access
- API Token management performed by Data Infrastructure Insights users with the Administrator role

Note: *Your Data Infrastructure Insights feature set role will determine which APIs you can access. For example, User and Guest roles have fewer privileges than Administrator role.*

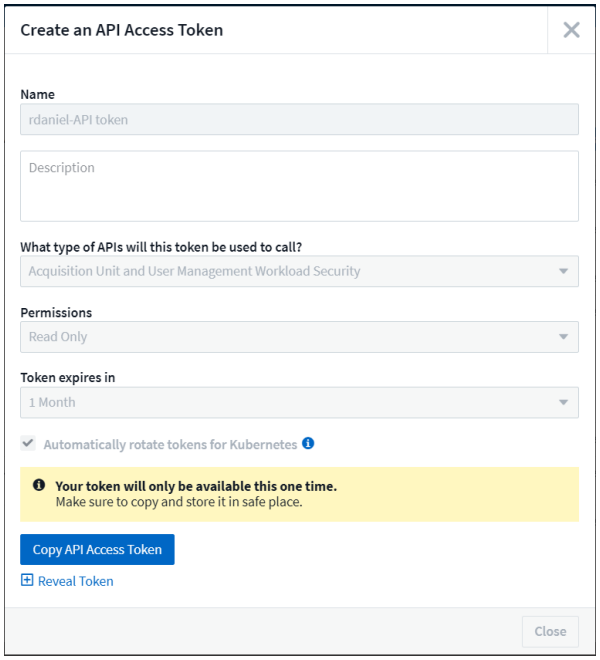
The REST API Token management and documentation can be accessed from Data Infrastructure Insights by taking the following steps:

1. Login to Data Infrastructure Insights and click on **Admin** in the navigation panel on the left side of the web browser window.

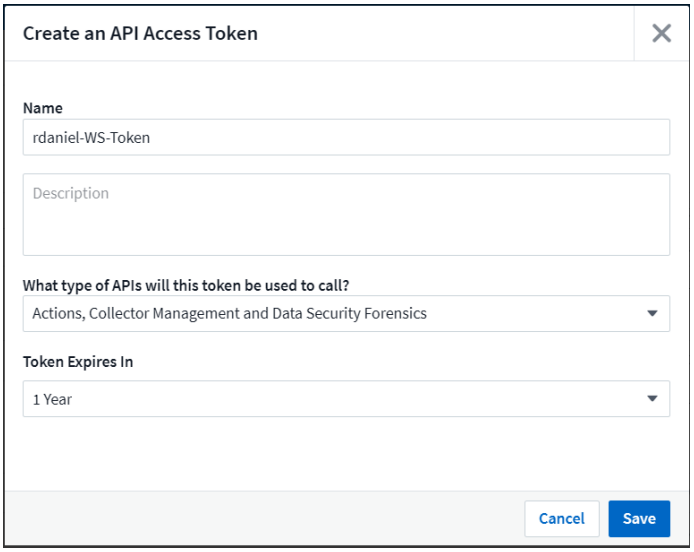
2. Click on **API Access**. From this page you can generate and manage the API Access Tokens.



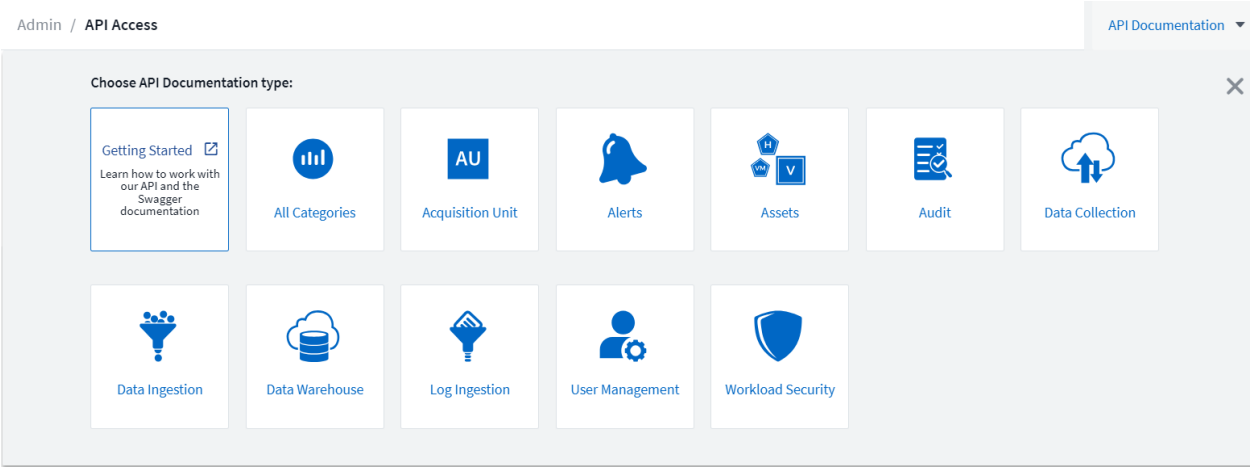
3. Generate a token for specific API Types and duration. Copy the API access Token and store it in a safe place.



4. To generate a token for Workload Security specific activities such as Data Security Forensics, choose **Workload Security Tokens** page and click on API Access Token.



5. Click the API Documentation link on the top-right corner of the page to access the REST API documentation.



For more information, refer to the following links.

[Data Infrastructure Insights API]

[Workload Security API]

Splunk Add-on Builder for REST API

Cisco's Splunk helps users collects, indexes and harnesses an organization's unstructured, time-series machine data - physical, virtual and cloud. Splunk can read data from any source, such as network traffic, web servers, custom applications, application servers, hypervisors, GPS systems, stock market feeds, social media, and preexisting structured databases.

Splunk delivers a real-time understanding of what's happening and deep analysis of what's happened across a user's IT systems and infrastructure, turning machine data into insights for informed decision making. These capabilities help organizations to manage, secure and gain operational intelligence from IT infrastructures, by enabling organizations to search and analyze their machine data from a single location in real time, troubleshoot application outages, investigate security incidents, and gain new levels of insight. When the capabilities of Data Infrastructure Insights and Splunk are combined, users have enhanced and holistic IT security protection.

The Splunk Add-on Builder simplifies the process of creating add-ons to collect and process data from REST APIs. Below is a step-by-step guide to configure data collection using a REST API in the Splunk Add-on Builder.

1. Create a New Add-on

- Open the Splunk Add-on Builder and click **"Create an Add-on"**.
- Provide details like the add-on name, author, version, and description.
- Save the settings to initialize your add-on project.

2. Configure Data Collection

- Navigate to the **"Configure Data Collection"** section on your add-on homepage.
- Click **"New Input"** to start the wizard for creating a data input.

3. Set Up REST API Input

- On the **Choose Input Method** page, select **"Modular input using a REST API"**.
- Fill in the following details: Input Name: A unique name for your input. Collection Interval: Frequency (in seconds) to fetch data from the API. REST URL: The endpoint of the REST API. HTTP Method: Choose between GET or POST. Optionally, specify headers, body parameters, or authentication details (e.g., Basic Auth or API tokens).

4. Define Parameters and Event Extraction

- Use the **Data Input Parameters** tab to define user-configurable fields (e.g., API keys).
- On the **Event Extraction Settings** tab: Specify how JSON payloads should be broken into individual events using JSON path expressions. Test your configuration to ensure proper event extraction.

5. Enable Checkpointing (Optional)

- Use checkpoints to track and fetch only new data: Define a checkpoint parameter (e.g., timestamp or ID). Configure initial values and JSON paths for checkpoint fields.

6. Validate and Save

- Test your configuration using the built-in testing tool.
- Save the input and complete the setup.

Best Practices

- Use descriptive names for inputs and parameters for clarity.
- Leverage checkpointing to avoid duplicate data ingestion.
- Validate configurations thoroughly before deployment

Once the Splunk REST API Modular Input has been installed within Splunk, a desired logo can be imported for ease recognition.

Steps to integrate Data Infrastructure Insights and Splunk

The following steps may be used to integrate Splunk with Data Infrastructure Insights using the Data Infrastructure Insights API.

1. Create a Data infrastructure Insights Token as explained above.
2. Install the Splunk Add-on builder as explained above.
3. Click the Splunk Add-on Builder icon that was created.
4. Create Data Input by entering the REST URL in the Splunk REST settings form
5. Update Event Extraction Settings – Enter “$.result[*]” in the JSON path field
6. Enable Checkpointing checkbox and update required fields
7. Click test in Splunk
8. Examine Data Infrastructure Insights Data in Splunk

The following link may be used as a reference to complete the above procedure.

Splunk_Integration_Guide_v1_4

NetApp Cyber Vaulting overview

NetApp Cyber vaulting is a multilayered data protection solution that helps to isolate your most valuable data with secure hardening technology to minimize the attack surface and keep your most critical data confidential, intact, and readily available. This cutting-edge solution combines advanced logical air-gapping techniques with robust data protection measures to create an impenetrable barrier against cyber threats. Refer to NetApp documentation on Cyber vaulting at the following link.

ONTAP cyber vault overview

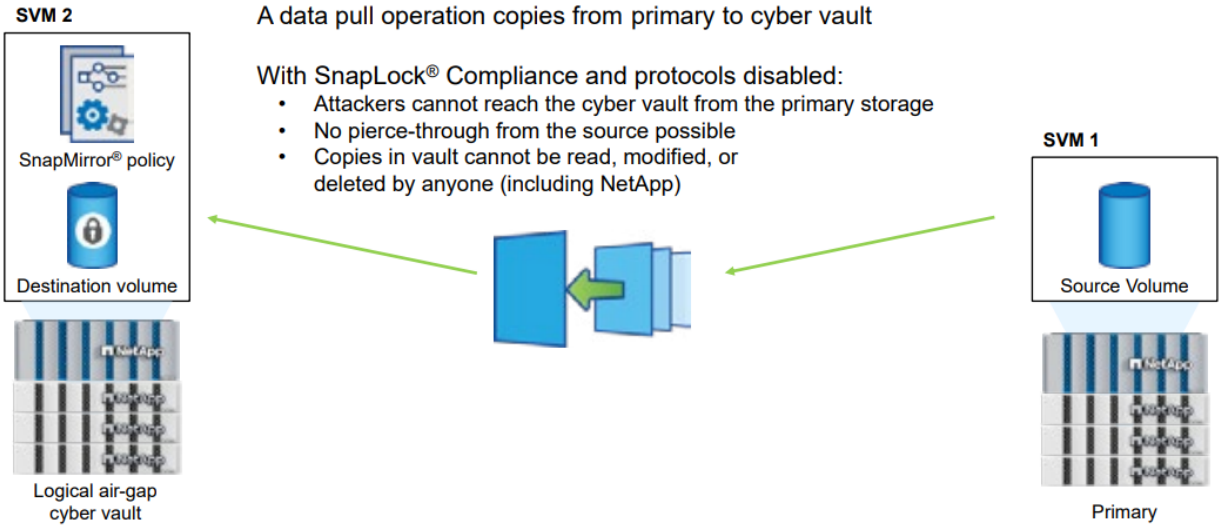
NetApp Logical Air Gapping

NetApp cyber vaulting empowers organizations to create logically air-gapped environments using NetApp ONTAP software. With ONTAP, you can:

- Create isolated storage systems that are logically separated from other networks and systems.
- Implement strict network segmentation and access controls to limit communication between storage and external networks.
- Use NetApp SnapLock® Compliance to create immutable and indelible, write-once-read-many (WORM) storage volumes that prevent data modification or deletion.

At the heart of an effective cyber vaulting strategy lies the ability to create immutable, tamper-proof backups that can withstand even the most sophisticated attacks. The NetApp SnapLock Compliance technology plays a pivotal role in the cyber vaulting equation. With SnapLock Compliance volumes, your backup data remains indelible and immune to tampering, even by privileged users or administrators—and even by NetApp Support. When combined with ONTAP Snapshot™ technology, SnapLock Compliance enables the creation of logically air-gapped cyber vaults that are dynamic, resilient and rapidly recoverable in the event of an attack. With ONTAP cyber vaulting, NetApp SnapMirror® policies and rules are managed from the vault, further protecting the vault from service disruptions. The following figure shows logical air-gapping using NetApp data protection technologies.

Figure 8) Logical air gapping with NetApp SnapLock Compliance



On both Primary and cyber vault backup data, you can further safeguard your data using ONTAP's security features such as **Multi-Admin verification** (MAV) and **Multifactor Authentication** (MFA).

To further enhance the security of the Cyber vault solution, the following guidelines may be adopted.

- Isolate the management networks in primary and secondary storage.
- Use different credentials in primary and secondary storage
- Have separate administrators for primary and secondary storage.
- Use dedicated replication network.
- Separate data centers (optional).

For more information about hardening an ONTAP cyber vault, refer to Cyber vault hardening.

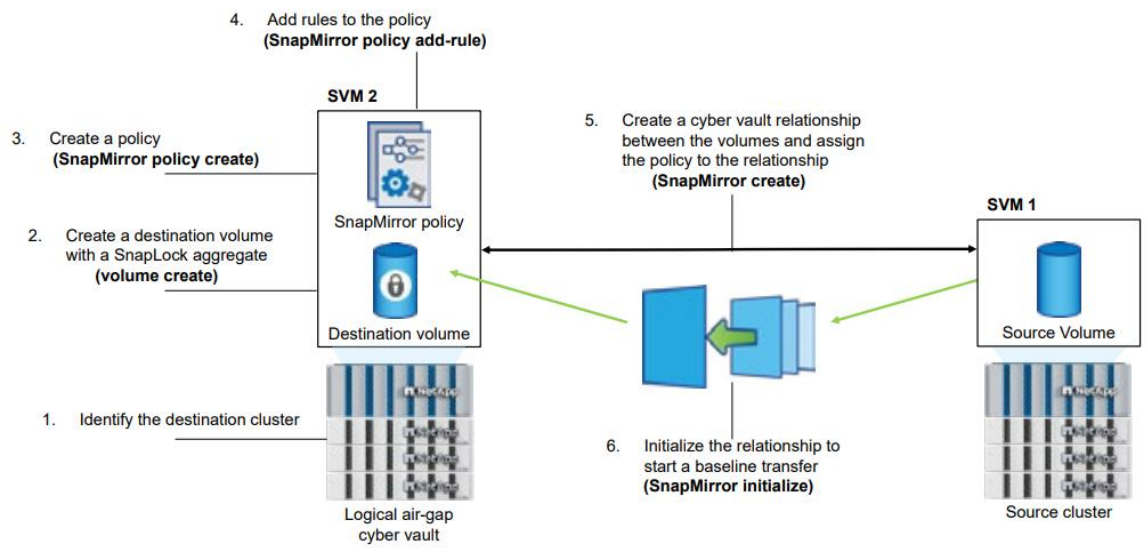
Creating a NetApp Cyber vault

Before you begin, make sure that the following requirements are met.

- The source cluster must be running ONTAP 9 or later.
- The source and destination aggregates must be 64-bit. You may use "**node run * aggr status -v**" command to check this.
- The source and destination volumes must be created in peered clusters with peered SVMs. For more information, refer to Learn about ONTAP cluster and SVM peering.
- If volume auto-grow is disabled, the free space on the destination volume must be at least five present more than the used space on the source volume

The following illustration shows the steps to assist with the creation of a cyber vault with ONTAP.

Figure 9) NetApp Cyber Vault implementation steps



Steps

1. Identify the destination array to become the cyber vault to receive the air-gapped data.

On the destination array, install the **ONTAP One license** and initialize the Compliance Clock.

On ONTAP system, you can enable SnapLock Compliance Clock synchronization using the following command.

```
snaplock compliance-clock initialize -node <node>
```

```
HC-FAS2820::> snaplock compliance-clock initialize -node HC-FAS2820-01

Warning: You are about to initialize the secure ComplianceClock of the node "HC-FAS2820-01" to the current value of the node's system clock. ComplianceClock
         re-initialization requires all nodes in the cluster to be healthy, all volumes are in online state, no volumes are present in the volume recovery
         queue and there are no SnapLock volumes or volumes with "snapshot-locking-enabled" set to true or S3 buckets with object locking enabled. Ensure
         that the system time is set correctly before proceeding. The current node's system clock is: Thu Aug 28 11:29:43 EDT 2025

Do you want to continue? {y|n}: y

HC-FAS2820::> snaplock compliance-clock initialize -node HC-FAS2820-02

Warning: You are about to initialize the secure ComplianceClock of the node "HC-FAS2820-02" to the current value of the node's system clock. ComplianceClock
         re-initialization requires all nodes in the cluster to be healthy, all volumes are in online state, no volumes are present in the volume recovery
         queue and there are no SnapLock volumes or volumes with "snapshot-locking-enabled" set to true or S3 buckets with object locking enabled. Ensure
         that the system time is set correctly before proceeding. The current node's system clock is: Thu Aug 28 11:29:53 EDT 2025

Do you want to continue? {y|n}: y

HC-FAS2820::>
```

```
HC-FAS2820::> snaplock compliance-clock show
Node                  ComplianceClock Time
------------------- ------------------------------------
HC-FAS2820-01         Thu Aug 28 11:31:23 EDT 2025 -04:00
HC-FAS2820-02         Thu Aug 28 11:31:24 EDT 2025 -04:00
2 entries were displayed.

HC-FAS2820::>
```

On ONTAP Cloud and ONTAP select platforms, you can enable SnapLock Compliance Clock synchronization when an NTP server is configured.

```
snaplock compliance-clock ntp – Enable the feature
snaplock compliance-clock ntp modify -is-sync-enabled true – Modify the feature
snaplock compliance-clock ntp show – Displays the feature
```

2. On the destination array, create a SnapLock Compliance destination volume of type DP.

```
volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -snaplock-type
compliance|enterprise -type DP -size size
```

```
HC-FAS2820::> volume create -vserver CyberVault-CI_SVM -volume fpsa_csdemo_vol_1 -aggregate aggr1_node01 -snaplock-type compliance -type DP -size 55G
[Job 62] Job succeeded: Successful

HC-FAS2820::>
HC-FAS2820::> volume create -vserver CyberVault-CI_CIFS_SVM -volume CSDEMO -aggregate aggr1_node02 -snaplock-type compliance -type DP -size 55G
[Job 63] Job succeeded: Successful
```

```
HC-FAS2820::> volume snaplock show
Vserver       Volume          SnapLock Type ComplianceClock Time
------------- --------------- ------------- ----------------------------------
CyberVault-CI_CIFS_SVM CSDEMO compliance    Thu Aug 28 12:09:53 EDT 2025 -04:00
CyberVault-CI_SVM fpsa_csdemo_vol_1 compliance Thu Aug 28 12:09:52 EDT 2025 -04:00
2 entries were displayed.
```


Modify the default retention period. In this example, the value is set to 180 days.

[Set the ONTAP SnapLock retention time]

```
HC-FAS2820::> volume snaplock show -vserver CyberVault-CI_SVM -volume fpsa_csdemo_vol_1

                        Vserver: CyberVault-CI_SVM
                         Volume: fpsa_csdemo_vol_1
                  SnapLock Type: compliance
        Minimum Retention Period: 0 years
        Default Retention Period: min
        Maximum Retention Period: 30 years
               Autocommit Period: none
   Is Volume Append Mode Enabled: false
               Privileged Delete: permanently-disabled
                     Expiry Time: none
            ComplianceClock Time: Thu Aug 28 12:10:20 EDT 2025 -04:00
                Litigation Count: 0
    Is SnapLock Audit Log Volume: false
Unspecified Retention File Count: 0
```

```
HC-FAS2820::> volume snaplock modify -vserver CyberVault-CI_SVM -volume fpsa_csdemo_vol_1 -default-retention-period 180days

HC-FAS2820::> volume snaplock modify -vserver CyberVault-CI_CIFS_SVM -volume CSDEMO -default-retention-period 180days
```

```
HC-FAS2820::> volume snaplock show -vserver CyberVault-CI_SVM -volume fpsa_csdemo_vol_1

                        Vserver: CyberVault-CI_SVM
                         Volume: fpsa_csdemo_vol_1
                  SnapLock Type: compliance
        Minimum Retention Period: 0 years
        Default Retention Period: 180 days
        Maximum Retention Period: 30 years
               Autocommit Period: none
   Is Volume Append Mode Enabled: false
               Privileged Delete: permanently-disabled
                     Expiry Time: none
            ComplianceClock Time: Thu Aug 28 12:17:58 EDT 2025 -04:00
                Litigation Count: 0
    Is SnapLock Audit Log Volume: false
Unspecified Retention File Count: 0
```

3. Create a SnapMirror policy if a custom policy is required.

   The policies *DPDefault*, *MirrorAllSnapshots*, *MirrorAndVault*, *MirrorLatest*, *Unified7year*, and *XDPDefault* are created by the system for asynchronous replication. You may use the **XDP Default** default policy if a custom policy is not required.

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type <async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror> -comment <comment> -tries <transfer_tries> -transfer-priority <low|normal> -is-network-compression-enabled <true|false>
```

4. Add rules to the policy if required.
5. Create a replication relationship between the non-SnapLock source and the new SnapLock destination.


```
snapmirror create -source-path <source-volume> -destination-path <destination volume> -vserver
<destination SVM> -policy <policy> -schedule <schedule>
```

```
HC-FAS2820::> snapmirror create -source-path CI_CIFS_SVM:CSDEMO -destination-path CyberVault-CI_CIFS_SVM:CSDEMO -policy XDPDefault -vserver CyberVault-CI_CIFS
_SVM -schedule hourly
Operation succeeded: SnapMirror create for the relationship with destination "CyberVault-CI_CIFS_SVM:CSDEMO".

HC-FAS2820::>
```

```
HC-FAS2820::> snapmirror show
                                                                          Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
CI_CIFS_SVM:CSDEMO XDP CyberVault-CI_CIFS_SVM:CSDEMO Uninitialized Idle - true -
```

6. On the destination SVM, initialize the SnapVault relationship.

```
snapmirror initialize -destination-path <destination_path>
```

```
HC-FAS2820::> snapmirror initialize -destination-path CyberVault-CI_SVM:fpsa_csdemo_vol_1
Operation is queued: SnapMirror initialize of destination "CyberVault-CI_SVM:fpsa_csdemo_vol_1".
```

```
HC-FAS2820::> snapmirror show
                                                                          Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
CI_CIFS_SVM:CSDEMO XDP CyberVault-CI_CIFS_SVM:CSDEMO Snapmirrored Idle - true -
CI_SVM:fpsa_csdemo_vol_1 XDP CyberVault-CI_SVM:fpsa_csdemo_vol_1 Snapmirrored Idle - true -
2 entries were displayed.
```

You may list the snapshot that was generated as shown below.

```
HC-FAS2820::> snapshot show
                                                          ---Blocks---
Vserver  Volume   Snapshot                                Size Total% Used%
-------- -------- ------------------------------------ -------- ------ -----
CyberVault-CI_CIFS_SVM CSDEMO
                  snapmirror.92c8f82d-83e7-11f0-84f7-d039eaaf433c_2150073589.2025-08-28_143429 172KB 0% 0%
                       CyberVault_SVM_CI_SVM_root
                  hourly.2025-08-28_1125                  140KB     0%   29%
                  hourly.2025-08-28_1205                  144KB     0%   30%
                  hourly.2025-08-28_1305                  144KB     0%   30%
                  hourly.2025-08-28_1405                  144KB     0%   30%
                  hourly.2025-08-28_1505                  140KB     0%   29%
```

You can also create ONTAP cyber vault using Power Shell scripts. Refer to the following documentation for more information.

[Implementing ONTAP cyber vault with PowerShell]

In the next section, we will examine how the data backed up in the cyber vault can be restored in the event of an attack.

Recovering Data after Ransomware attack

To recover from a ransomware attack and restore data to a pre-incident state, an organization may need access to the decryption key held by the attacker. This often entails paying ransom to the attacker, however there is no guarantee that the attacker would release the key or decrypt the data as previously promised. Moreover, paying ransom would encourage attackers to continue carrying out the attacks.

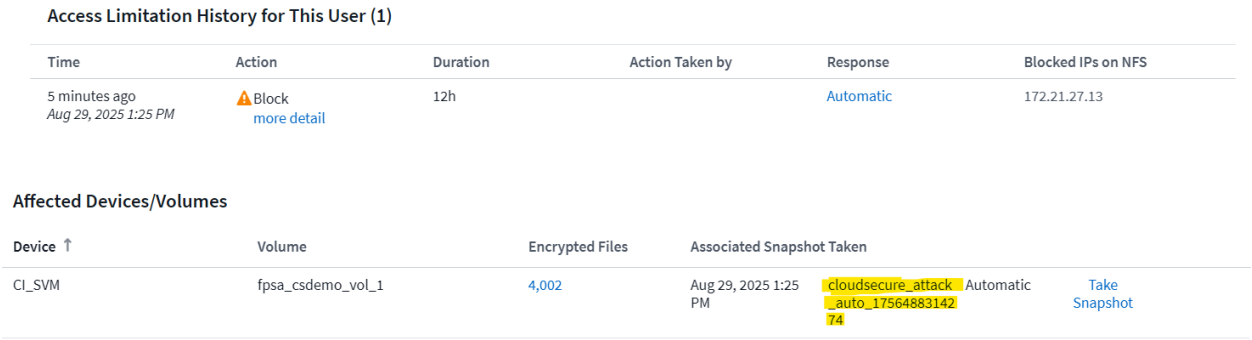
An organization can resume normal operations in a timely manner when a ransomware recovery plan is in place. The ransomware recovery plan typically includes how the organization prepares for an attack, how to handle an in-progress attack and what to do to recover from the attack. The first instinct after a ransomware attack might be to instantly recover the data. You can certainly do this, however if you do not take other steps to make sure the ransomware does not come back, you are likely to end up with reinfection and extended outage. There are three major steps to remediate your environment properly and holistically. The first step is to contain the outbreak. This involves identifying and isolating infected clients by disconnecting them from the network. Once they are disconnected, the next step is to clean up the infected systems and apply a patch if available. Applying patches would prevent the system from reinfection when they are connected back to the network. The last step is to recover and restore the data. Organizations must backup all business-critical data as often as reasonably possible to reduce data loss. Data backups are critical to restore business operations and access to backup taken as close to the attack can significantly reduce data loss following a ransomware attack.

In this section, we will discuss few methods to restore data after a ransomware attack. Volume Snapshot restore feature of ONTAP as well as NetApp's SnapCenter® plug-ins can tremendously help to recover from a ransomware attack. The SnapCenter plug-ins can be used to take VM-consistent and application-consistent backups on a scheduled basis and do a restore operation when the need arises. Additionally, we will discuss NetApp Console's Ransomware Resilience as well as recovering data from a NetApp cyber vault.

ONTAP Volume Snapshot Restore

In the ransomware attack simulation use case discussed earlier, we have seen that the auto response policy of Data Infrastructure Insight's Workload Security feature had triggered a volume snapshot as soon as the attack was detected.

In the following screenshot, we see the affected vserver, volume and the snapshot that was taken by the Workload Security auto response policy. Note that the snapshot taken by workload security begins with "**cloudsecure_attack_auto_**".



Access Limitation History for This User (1)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
5 minutes ago *Aug 29, 2025 1:25 PM*	Block more detail	12h		Automatic	172.21.27.13

Affected Devices/Volumes

Device	Volume	Encrypted Files	Associated Snapshot Taken		
CI_SVM	fpsa_csdemo_vol_1	4,002	Aug 29, 2025 1:25 PM	cloudsecure_attack_auto_1756488314274 Automatic	Take Snapshot

You may restore the volume to a snapshot using the following command.

volume snapshot restore -vserver <vserver name> -volume <vol_name> -snapshot <snapshot_name>


```
A400-G0312::> volume snapshot restore -vserver CI_SVM -volume fpsa_csdemo_vol_1 -snapshot
cloudsecure_attack_auto_1756488314274
```

Note:

Customers with core ONTAP could also get ransomware detection, alerting and snapshot capabilities through Autonomous Ransomware Protection (ARP). Unlike Data Infrastructure Insights, ARP does not provide forensics capabilities natively however integrating it with Data Infrastructure Insights adds additional layer of forensics capabilities, user mapping and analytics data retention up to 13 months. Snapshots generated by Autonomous Ransomware Protection begin with "**Anti_ransomware_backup**". For example, the following screenshot displays a snapshot that was triggered by ARP feature when a never-seen-before file extension was discovered on ARP enabled volume.

```
A400-G0312::> volume snapshot show -vserver CI_SVM -volume fpsa_csdemo_vol_1
                                                                    ---Blocks---
Vserver  Volume   Snapshot                                   Size Total% Used%
-------- -------- ------------------------------------- -------- ------ -----
CI_SVM   fpsa_csdemo_vol_1
                  weekly.2025-08-17_0015                  4.80MB     0%   20%
                  weekly.2025-08-24_0015                  3.62MB     0%   16%
                  daily.2025-08-28_0010                    424KB     0%    2%
                  Anti_ransomware_backup.2025-08-28_1550  2.88MB     0%   13%
                  daily.2025-08-29_0010                    232KB     0%    1%
                  hourly.2025-08-29_0805                   180KB     0%    1%
                  hourly.2025-08-29_0905                   176KB     0%    1%
                  hourly.2025-08-29_1005                   180KB     0%    1%
                  hourly.2025-08-29_1105                   200KB     0%    1%
                  hourly.2025-08-29_1205                   616KB     0%    3%
                  hourly.2025-08-29_1305                   708KB     0%    3%
                  Anti_ransomware_backup.2025-08-29_1322  1.64MB     0%    8%
                  cloudsecure_attack_auto_1756488314274    324KB     0%    2%
13 entries were displayed.
```

Check the snapshots triggered by ARP and Workload Security.

```
A400-G0312::> volume snapshot show -vserver CI_SVM -volume fpsa_csdemo_vol_1 -snapshot Anti_ransomware_backup.2025-08-29_1322

                                 Vserver: CI_SVM
                                  Volume: fpsa_csdemo_vol_1
                cp Count (for sorting): 295368
                                Snapshot: Anti_ransomware_backup.2025-08-29_1322
                           Creation Time: Fri Aug 29 13:22:28 2025
                           Snapshot Busy: false
                          List of Owners: -
                           Snapshot Size: 1.64MB
               Percentage of Total Blocks: 0%
                Percentage of Used Blocks: 8%
```

```
A400-G0312::> volume snapshot show -vserver CI_SVM -volume fpsa_csdemo_vol_1 -snapshot cloudsecure_attack_auto_1756488314274

                                 Vserver: CI_SVM
                                  Volume: fpsa_csdemo_vol_1
                cp Count (for sorting): 295372
                                Snapshot: cloudsecure_attack_auto_1756488314274
                           Creation Time: Fri Aug 29 13:25:13 2025
                           Snapshot Busy: false
                          List of Owners: -
                           Snapshot Size: 372KB
               Percentage of Total Blocks: 0%
                Percentage of Used Blocks: 2%
```


The snapshot generated by ARP is closer to the attack time than the one generated by Workload Security, so the administrators have the option to analyze both snapshots and restore as many files as possible. In this example, when the snapshot generated by ARP was restored, we see that about 78% of files were still not encrypted when ARP triggered the snapshot.

```
File1403.txt.lkdcryp    File1848.txt.lkdcryp  File2292.txt  File2737.txt  File3182.txt  File3627.txt  File4072.txt  File4517.txt  File4962.txt
File1404.txt.lkdcryp    File1849.txt.lkdcryp  File2293.txt  File2738.txt  File3183.txt  File3628.txt  File4073.txt  File4518.txt  File4963.txt
File1405.txt.lkdcryp    File1850.txt.lkdcryp  File2294.txt  File2739.txt  File3184.txt  File3629.txt  File4074.txt  File4519.txt  File4964.txt
File1406.txt.lkdcryp    File1851.txt.lkdcryp  File2295.txt  File2740.txt  File3185.txt  File3630.txt  File4075.txt  File4520.txt  File4965.txt
File1407.txt.lkdcryp    File1852.txt.lkdcryp  File2296.txt  File2741.txt  File3186.txt  File3631.txt  File4076.txt  File4521.txt  File4966.txt
File1408.txt.lkdcryp    File1853.txt.lkdcryp  File2297.txt  File2742.txt  File3187.txt  File3632.txt  File4077.txt  File4522.txt  File4967.txt
File1409.txt.lkdcryp    File1854.txt.lkdcryp  File2298.txt  File2743.txt  File3188.txt  File3633.txt  File4078.txt  File4523.txt  File4968.txt
File1410.txt.lkdcryp    File1855.txt.lkdcryp  File2299.txt  File2744.txt  File3189.txt  File3634.txt  File4079.txt  File4524.txt  File4969.txt
File1411.txt.lkdcryp    File1856.txt.lkdcryp  File2300.txt  File2745.txt  File3190.txt  File3635.txt  File4080.txt  File4525.txt  File4970.txt
File1412.txt.lkdcryp    File1857.txt.lkdcryp  File2301.txt  File2746.txt  File3191.txt  File3636.txt  File4081.txt  File4526.txt  File4971.txt
File1413.txt.lkdcryp    File1858.txt.lkdcryp  File2302.txt  File2747.txt  File3192.txt  File3637.txt  File4082.txt  File4527.txt  File4972.txt
File1414.txt.lkdcryp    File1859.txt.lkdcryp  File2303.txt  File2748.txt  File3193.txt  File3638.txt  File4083.txt  File4528.txt  File4973.txt
File1415.txt.lkdcryp    File1860.txt.lkdcryp  File2304.txt  File2749.txt  File3194.txt  File3639.txt  File4084.txt  File4529.txt  File4974.txt
File1416.txt.lkdcryp    File1861.txt.lkdcryp  File2305.txt  File2750.txt  File3195.txt  File3640.txt  File4085.txt  File4530.txt  File4975.txt
File1417.txt.lkdcryp    File1862.txt.lkdcryp  File2306.txt  File2751.txt  File3196.txt  File3641.txt  File4086.txt  File4531.txt  File4976.txt
File1418.txt.lkdcryp    File1863.txt.lkdcryp  File2307.txt  File2752.txt  File3197.txt  File3642.txt  File4087.txt  File4532.txt  File4977.txt
File1419.txt.lkdcryp    File1864.txt.lkdcryp  File2308.txt  File2753.txt  File3198.txt  File3643.txt  File4088.txt  File4533.txt  File4978.txt
File1420.txt.lkdcryp    File1865.txt.lkdcryp  File2309.txt  File2754.txt  File3199.txt  File3644.txt  File4089.txt  File4534.txt  File4979.txt
File1421.txt.lkdcryp    File1866.txt.lkdcryp  File2310.txt  File2755.txt  File3200.txt  File3645.txt  File4090.txt  File4535.txt  File4980.txt
File1422.txt.lkdcryp    File1867.txt.lkdcryp  File2311.txt  File2756.txt  File3201.txt  File3646.txt  File4091.txt  File4536.txt  File4981.txt
File1423.txt.lkdcryp    File1868.txt.lkdcryp  File2312.txt  File2757.txt  File3202.txt  File3647.txt  File4092.txt  File4537.txt  File4982.txt
File1424.txt.lkdcryp    File1869.txt.lkdcryp  File2313.txt  File2758.txt  File3203.txt  File3648.txt  File4093.txt  File4538.txt  File4983.txt
File1425.txt.lkdcryp    File1870.txt.lkdcryp  File2314.txt  File2759.txt  File3204.txt  File3649.txt  File4094.txt  File4539.txt  File4984.txt
File1426.txt.lkdcryp    File1871.txt.lkdcryp  File2315.txt  File2760.txt  File3205.txt  File3650.txt  File4095.txt  File4540.txt  File4985.txt
File1427.txt.lkdcryp    File1872.txt.lkdcryp  File2316.txt  File2761.txt  File3206.txt  File3651.txt  File4096.txt  File4541.txt  File4986.txt
File1428.txt.lkdcryp    File1873.txt.lkdcryp  File2317.txt  File2762.txt  File3207.txt  File3652.txt  File4097.txt  File4542.txt  File4987.txt
File1429.txt.lkdcryp    File1874.txt.lkdcryp  File2318.txt  File2763.txt  File3208.txt  File3653.txt  File4098.txt  File4543.txt  File4988.txt
File1430.txt.lkdcryp    File1875.txt.lkdcryp  File2319.txt  File2764.txt  File3209.txt  File3654.txt  File4099.txt  File4544.txt  File4989.txt
File1431.txt.lkdcryp    File1876.txt.lkdcryp  File2320.txt  File2765.txt  File3210.txt  File3655.txt  File4100.txt  File4545.txt  File4990.txt
File1432.txt.lkdcryp    File1877.txt.lkdcryp  File2321.txt  File2766.txt  File3211.txt  File3656.txt  File4101.txt  File4546.txt  File4991.txt
File1433.txt.lkdcryp    File1878.txt          File2322.txt  File2767.txt  File3212.txt  File3657.txt  File4102.txt  File4547.txt  File4992.txt
File1434.txt.lkdcryp    File1878.txt.lkdcryp  File2323.txt  File2768.txt  File3213.txt  File3658.txt  File4103.txt  File4548.txt  File4993.txt
File1435.txt.lkdcryp    File1879.txt          File2324.txt  File2769.txt  File3214.txt  File3659.txt  File4104.txt  File4549.txt  File4994.txt
File1436.txt.lkdcryp    File1880.txt          File2325.txt  File2770.txt  File3215.txt  File3660.txt  File4105.txt  File4550.txt  File4995.txt
File1437.txt.lkdcryp    File1881.txt          File2326.txt  File2771.txt  File3216.txt  File3661.txt  File4106.txt  File4551.txt  File4996.txt
File1438.txt.lkdcryp    File1882.txt          File2327.txt  File2772.txt  File3217.txt  File3662.txt  File4107.txt  File4552.txt  File4997.txt
File1439.txt.lkdcryp    File1883.txt          File2328.txt  File2773.txt  File3218.txt  File3663.txt  File4108.txt  File4553.txt  File4998.txt
File1440.txt.lkdcryp    File1884.txt          File2329.txt  File2774.txt  File3219.txt  File3664.txt  File4109.txt  File4554.txt  File4999.txt
File1441.txt.lkdcryp    File1885.txt          File2330.txt  File2775.txt  File3220.txt  File3665.txt  File4110.txt  File4555.txt  File5000.txt
File1442.txt.lkdcryp    File1886.txt          File2331.txt  File2776.txt  File3221.txt  File3666.txt  File4111.txt  File4556.txt
File1443.txt.lkdcryp    File1887.txt          File2332.txt  File2777.txt  File3222.txt  File3667.txt  File4112.txt  File4557.txt
testuser3@fpsademo.net@fpsa-demo-linux3:/csdemo/data5$
```

The files that are still encrypted could be restored using backup copies of ONTAP hourly or daily snapshots, whichever is closer to the attack time.

Refer to the following link for more information on recovering data using volume Snapshot restore.

[Restore data from ONTAP ARP snapshots after a ransomware attack]

VM Consistent backup and restore using SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere (SCV), formerly **NetApp Data Broker**, is a Linux-based standalone virtual appliance that supports SnapCenter data protection operations on virtualized databases and file systems. It provides fast, space-efficient, crash-consistent, and VM-consistent backup and restore operations for VMs, Datastores, and VMDKs. The SnapCenter plug-in for VMware vSphere can work with SnapCenter application-based plug-in such as MS-SQL, Exchange, Oracle, and SAP-Hana for application consistent backup and restore operation in VMware environments.

Note:

- VMware Tools is required for VM consistent Snapshot copies. If VMware tools is not installed and running, the file system is not quiesced and a crash-consistent Snapshot is created. For VM-consistent and crash-consistent data protection, you do not need to install SnapCenter Server.
- For application-consistent (application over virtual-machine disk (VMDK) or raw device mappings (RDM)) data protection operations, you need to install SnapCenter server. SnapCenter natively leverages the SnapCenter VMware plug-in for all data protection operations on VMDKs, raw device mappings (RDMs), and NFS datastores.

Using the SnapCenter Plug-in for VMware in vCenter, users can do the following:

- Create policies, resource groups, and backup schedules for virtual machines.
- Backup virtual machines, VMDKs, and datastores.
- Restore virtual machines, VMDKs, and files and folders (on Windows guest OS).
- Attach and detach VMDK.
- Monitor and report data protection operations on virtual machines and datastores.
- Support RBAC security and centralized role delegation.
- Support guest file or folder (single or multiple) support for Windows guest OS.
- Restore an efficient storage base from primary and secondary Snapshot copies through Single File SnapRestore.
- Generate dashboard and reports that provide visibility into protected versus unprotected virtual machines and status of backup, restore, and mount jobs.
- Attach or detach virtual disks from secondary Snapshot copies.
- Attach virtual disks to an alternate virtual machine.

You can use the VMware vSphere client GUI in vCenter for all backup and restore operations of VMware virtual machines (traditional VMs and vVol VMs), VMDKs, and datastores. For vVol VMs (VMs in vVol datastores), only crash-consistent backups are supported. You can also restore VMs and VMDKs and restore files and folders that reside on a guest OS.

Deploying SnapCenter Plug-in for VMware vSphere

The SCV deployment procedure is different for new and existing SnapCenter users.

If you have not used SnapCenter before and do not have any SnapCenter backups, then use the following workflow to get started.

Deployment workflow for new users

If you are a SnapCenter user and have SnapCenter backups, then use the following workflow to get started.

Deployment workflow for existing users

Steps

1. Install the Open Virtual Appliance (OVA) and Entrust root and intermediate certificates.

In VMware vCenter 7.0.3 versions and higher, the OVA signed by the Entrust certificate is no longer trusted. You must download the .tar file containing the OVA and certificates folder and follow the procedure below to install the certificates.

Download the Open Virtual Appliance (OVA)

2. Deploy SnapCenter Plug-in for VMware vSphere.

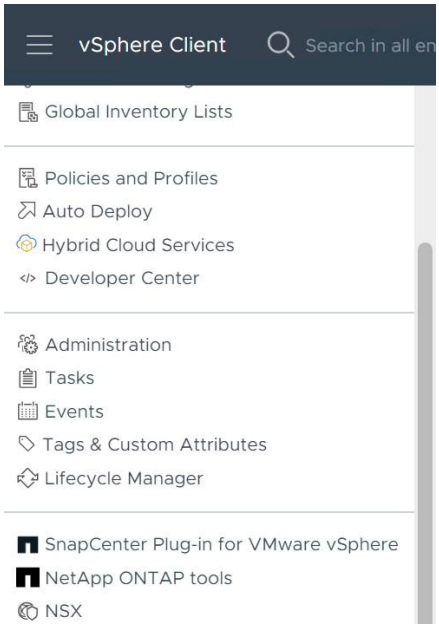
To use SnapCenter features to protect VMs, datastores, and application-consistent databases on virtualized machines, you must deploy SnapCenter Plug-in for VMware vSphere. Refer to the following procedure for more details.

Deploy SnapCenter Plug-in for VMware vSphere

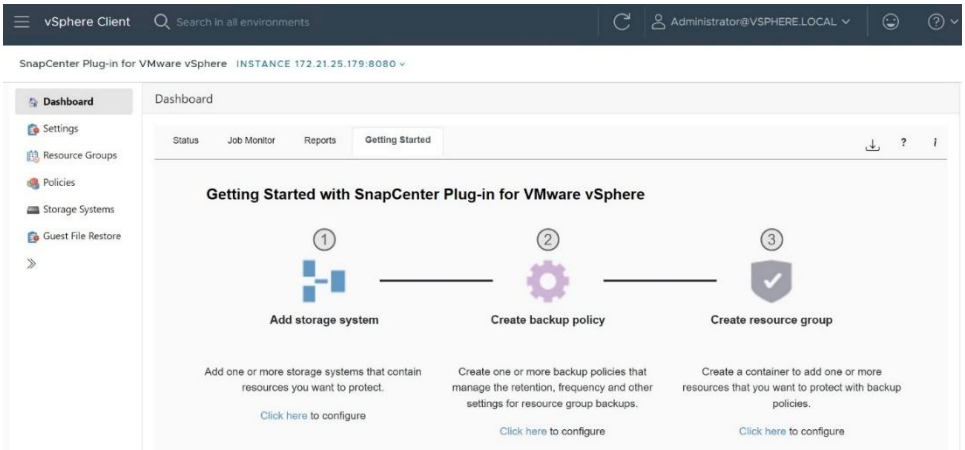
Backing up VMs and datastores

Before you can take backups, you need to configure backup policies, attach storage, and create resource groups using SnapCenter Plug-in for VMware vSphere.

Open VMware vSphere client GUI and click on the **Menu** button and select **SnapCenter Plug-in for VMware vSphere** from the pull-down list.



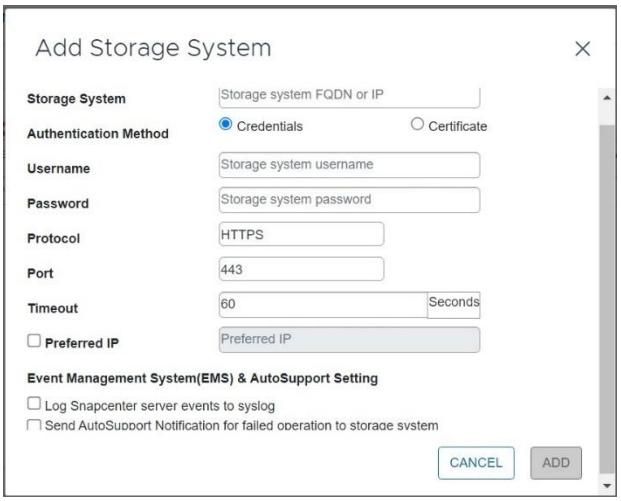
When SCV plug-in is opened, click on **Dashboard** on the left pane and select **Getting Started** tab on the right pane. This tab lists the steps to configure SCV plug-in for backing up VMs and datastores. You can click on the hyperlink under each step to open the wizard for the respective step. Alternatively, you can open the configuration wizard by right clicking on storage systems, policies, or resource groups on the left pane and creating a new item.



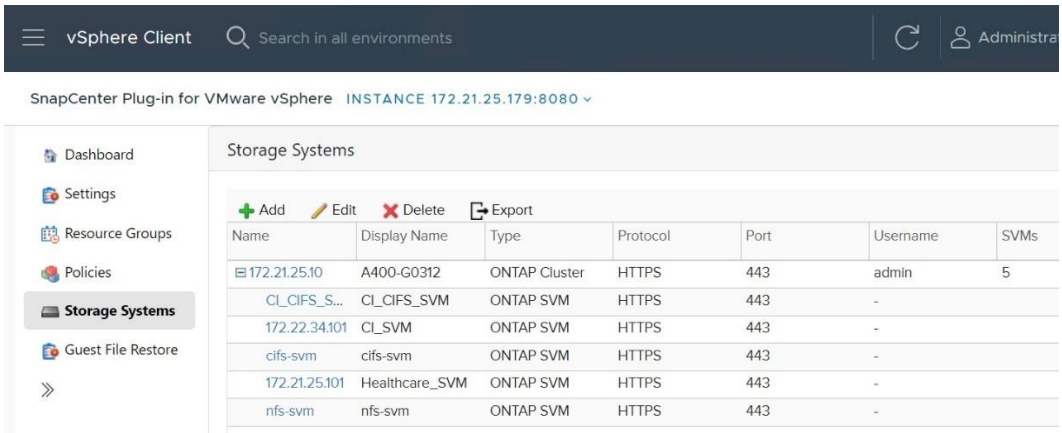
1. **Add storage clusters and storage VMs.**

In the left Navigator pane of the SCV plug-in, click **Storage Systems** and then select **Add** button.

On the Add Storage System dialog box, enter the basic SVM or Cluster information, and select Add.

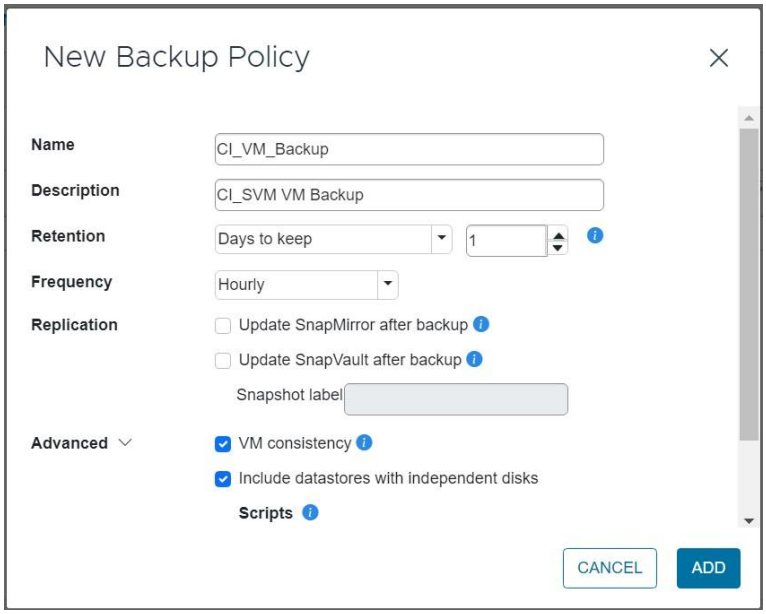


The following screen shot shows a storage cluster and SVMs that are added.

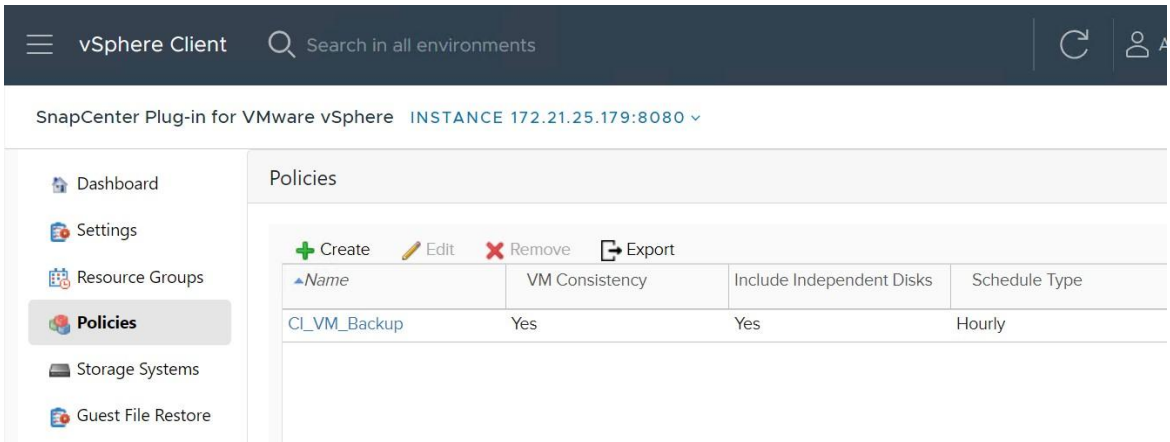


2. Create backup policies

In the left Navigator pane of the SCV plug-in, click **Policies**, and then click on **Create** button. On the New Backup Policy page, enter the policy configuration information, and then click **Add**.



In this example, an hourly backup policy is created, and the backups taken using this policy are retained for 1 day.

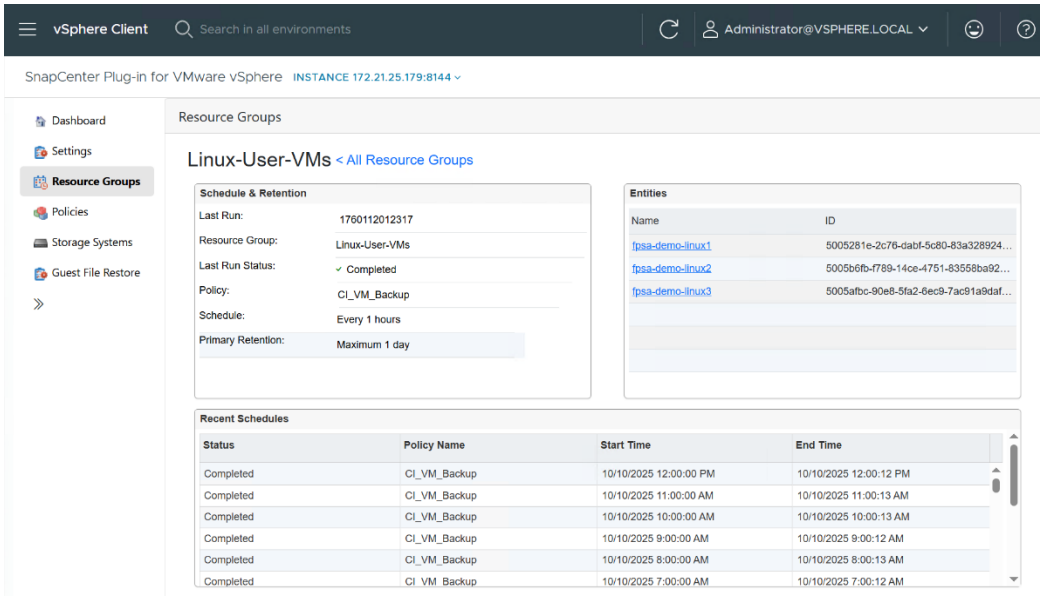


3. Create resource groups

In the left Navigator pane of the SCV plug-in, click **Resource Groups**, and then select **Create**.

Enter the required information on each page of the Create Resource Group wizard, select VMs and datastores to be included in the resource group, and then select the backup policies to be applied to the resource group and specify the backup schedule.

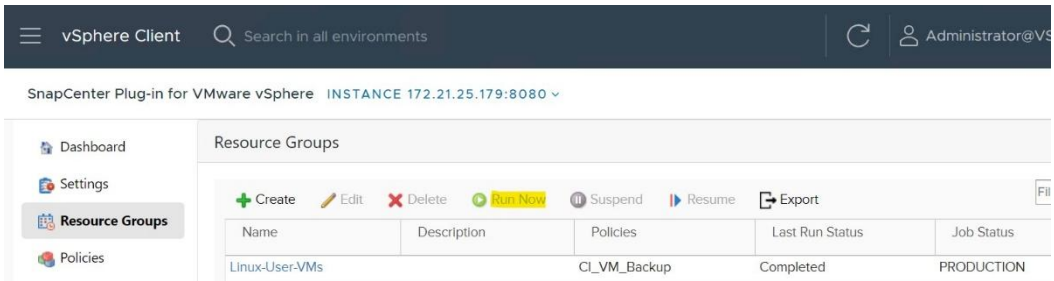
In this example, a resource group is created to backup 3 linux VMs.



4. Performing Backup

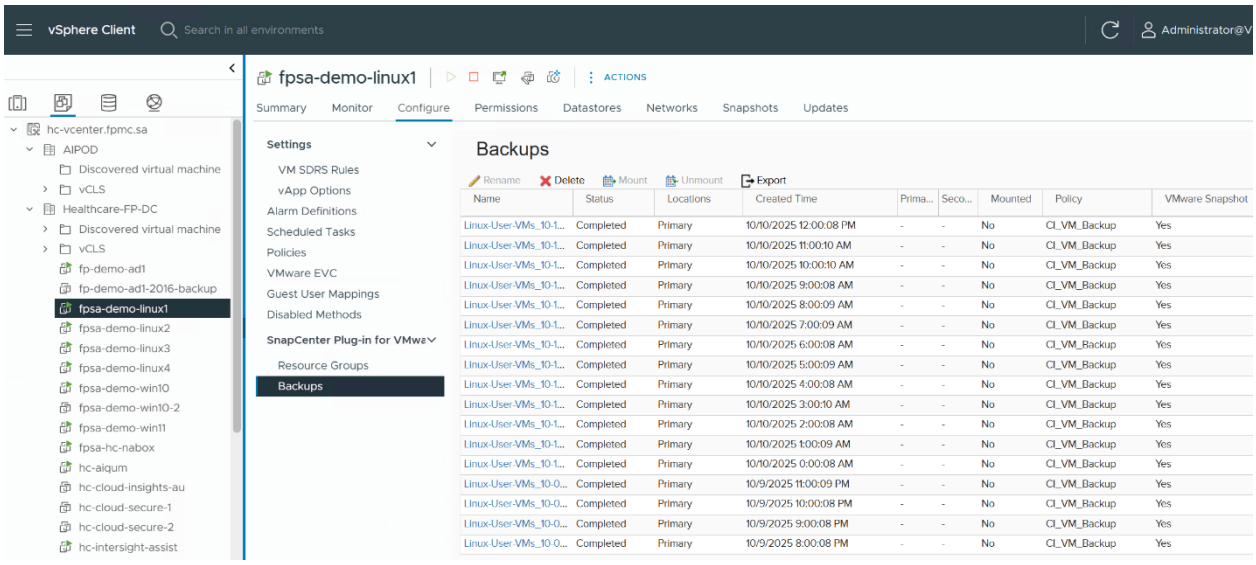
Backups are performed as specified in the backup policies that are configured for the resource group.

You can also perform an on-demand backup from the Resource Groups page by clicking "**Run Now**' after selecting the resource group.



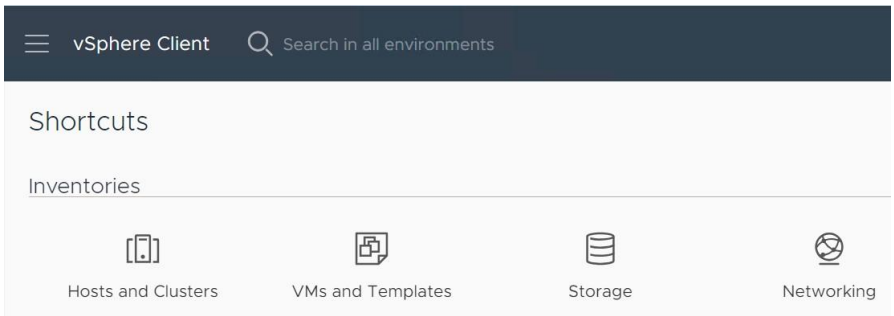
5. Viewing backups of a VM

To view the backups of a VM, open **Hosts and Clusters** in the inventory list, then select a VM, then select the **Configure** tab, and then click **Backups** in the **SnapCenter Plug-in for VMware vSphere** section. All available backups are listed in the right pane.

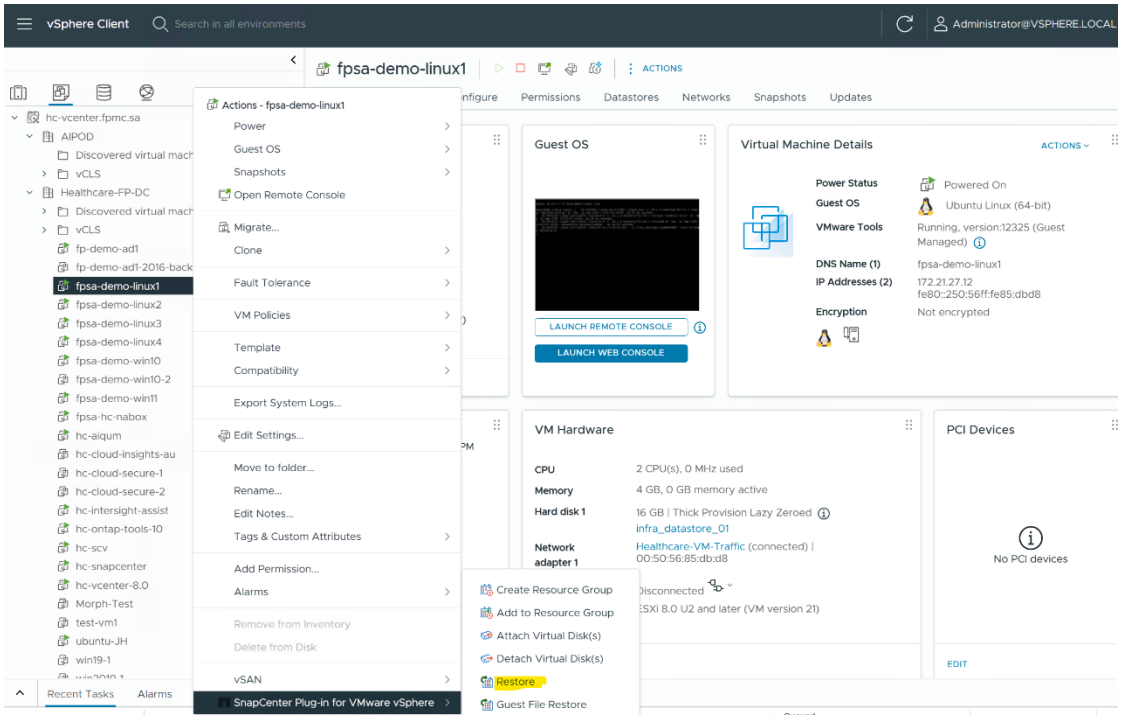


Restoring VMs from backup

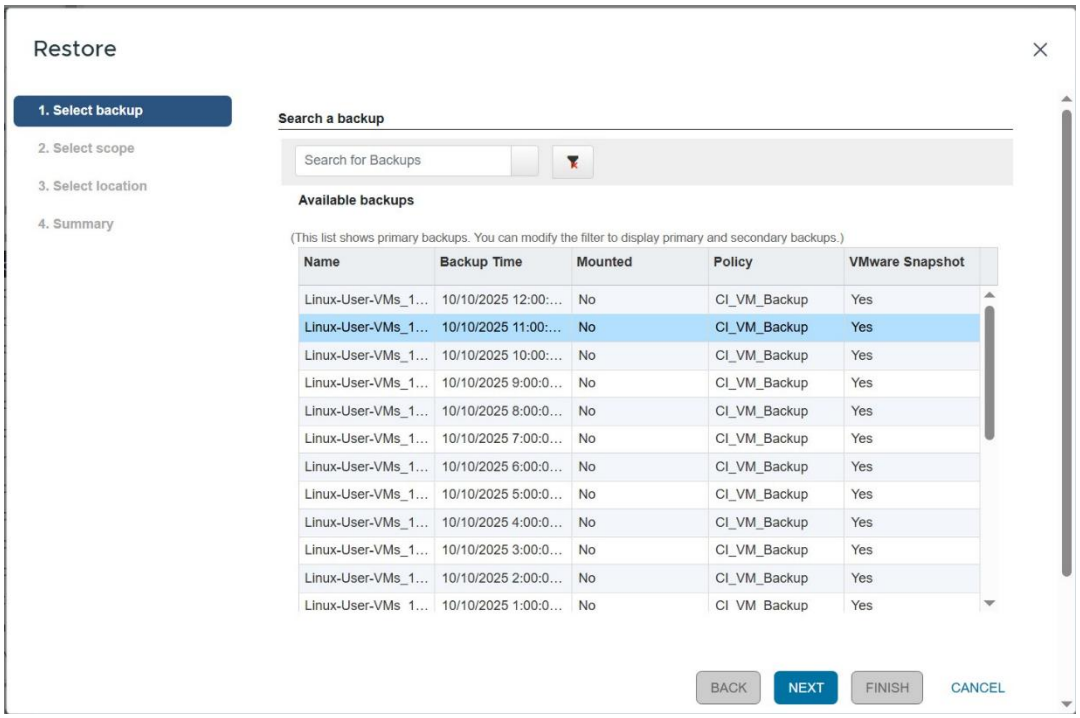
In the VMware vSphere client GUI, click Menu button on the top left corner and select shortcuts, and then select VMs and Templates from the inventory list.



In the left Navigator pane, right-click a VM, then select **NetApp SnapCenter Plug-in for VMware vSphere** in the drop-down list, and then select **Restore** in the secondary drop-down list to start the wizard.



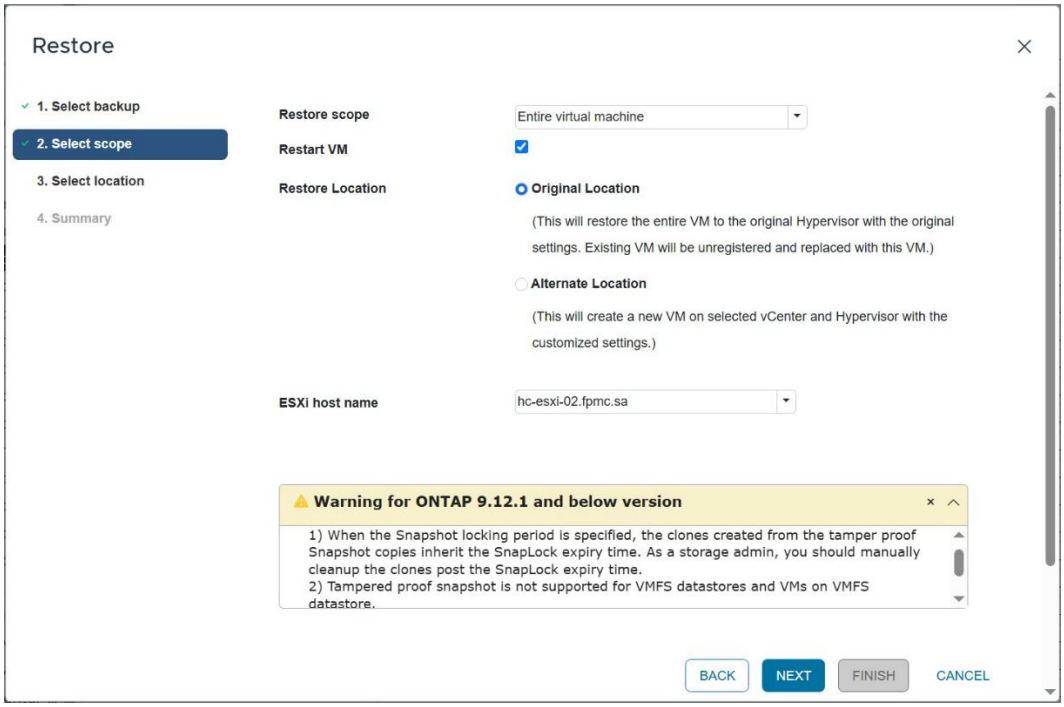
In the **Restore** wizard, on the **Select Backup** page, select the backup Snapshot copy that you want to restore and click NEXT.



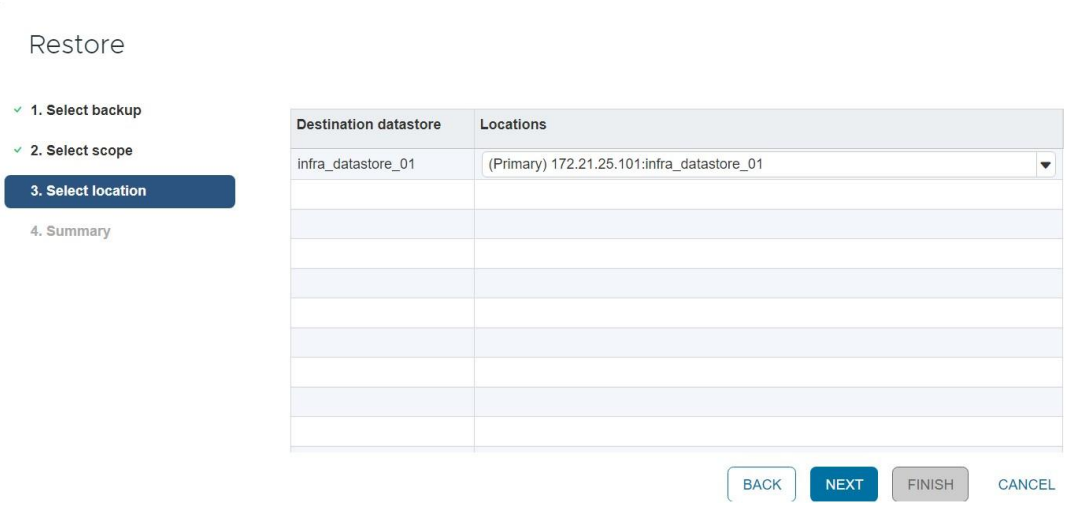
On the **Select Scope** page, select Entire virtual machine in the Restore scope field, then select the restore location, and then enter the destination information where the backup should be mounted. You may choose to restart the VM by clicking the check box.

If you choose **Alternate Location** as restore location, a new VM will be created on selected vCenter and hypervisor with customized settings.

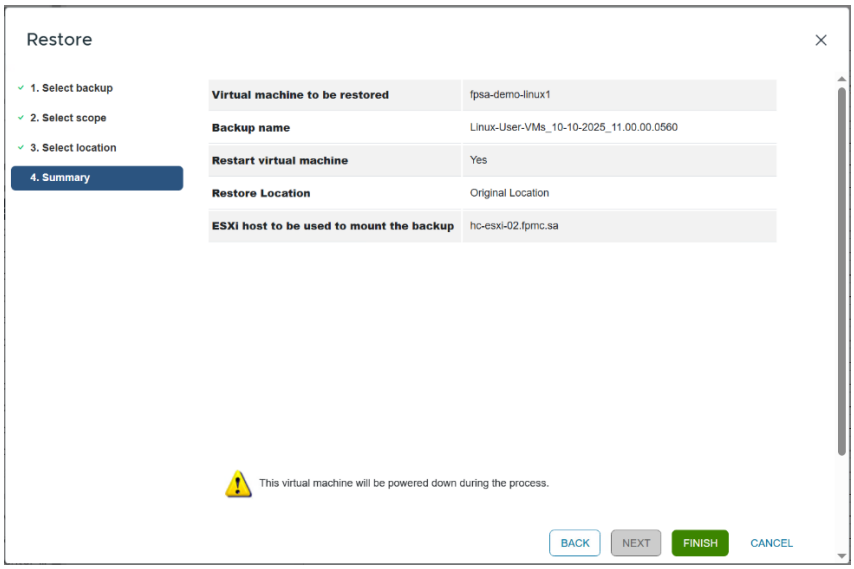
In this example, **Original Location** is chosen as restore location.



On the **Select Location** page, select the location for the restored datastore and click NEXT.



Review the Summary page and then click Finish.



Note: You may monitor the operation progress by clicking **Recent Tasks** at the bottom of the screen.

Refresh the screen to display updated information.

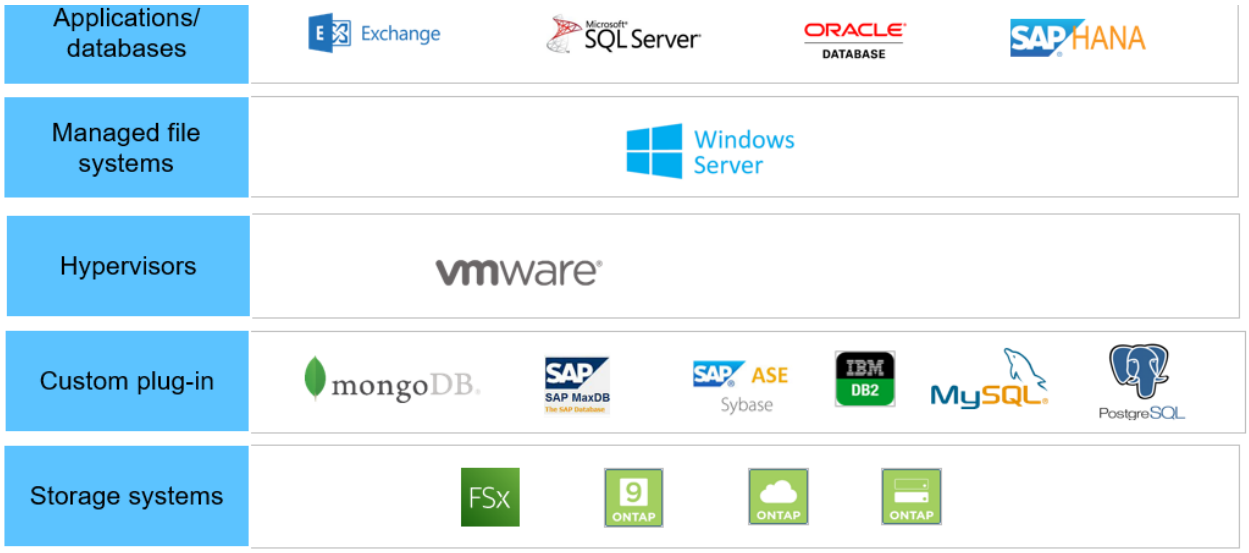
Application consistent backup and recovery using SnapCenter plug-ins

SnapCenter is a software package from NetApp that focuses on application and database consistent backup, verification, cloning, and recovery. SnapCenter is composed of the SnapCenter Server and SnapCenter Plug-ins.

SnapCenter Server is a centralized server with a common interface that supports Plug-ins for a variety of applications, databases, file systems, and hypervisors. Through SnapCenter, you can centrally deploy Plug-ins to remote hosts and schedule and monitor backup, verification, clone, and restore operations.

SnapCenter Plug-ins are shown in the following figure.

Figure 10) SnapCenter Plug-ins



- Plug-in for Microsoft Windows – This Plug-in handles backup, recovery, and cloning of Windows file systems. It is also used for provisioning disks on Windows, resizing disks, creating SMB shares, iSCSI connections and igroup connections. This is also used as a background component for the Microsoft SQL Server and Microsoft Exchange Server Plug-ins.
- Plug-in for Microsoft SQL Server – This Plug-in handles backup, recovery, and cloning of Microsoft SQL Server databases.
- Plug-in for Microsoft Exchange Server – This Plug-in handles backup and recovery of Microsoft Exchange Server databases.
- Plug-in for SAP HANA Database – This Plug-in handle backup, recovery, and cloning of SAP HANA databases.
- Plug-in for Oracle Database – This Plug-in handles backup, recovery, and cloning of Oracle Databases.
- Plug-in for UNIX – This Plug-in is used as a background component for the Oracle Database Plug-in. As of this writing, you cannot use this Plug-in to backup Linux file system however this capability is planned for early CY24.

In addition, SnapCenter has the following capabilities:

- The ability to create custom Plug-ins which will allow you to create your own Plug-ins and use them in SnapCenter. You may refer to NetApp Automation Store for more details on these community supported plug-ins.

SnapCenter also uses centralized role-based access control (RBAC) and offers reports and a centralized dashboard across all Plug-ins.

For more information on SnapCenter, refer to the following link.

NetApp Support Site - All Products - SnapCenter (Guide Me)

Protect Microsoft SQL Server databases

The following Cisco Validated Design (CVD) document talks about backup, restore and cloning of SQL databases using NetApp SnapCenter. It also talks about backup to cloud using NetApp SnapMirror technology for disaster recovery use cases.

FlexPod Datacenter for Microsoft SQL Server 2022 and VMware vSphere 8.0 - Cisco

Recovering Data using Ransomware Resilience

When workloads are protected by Ransomware Resilience feature in NetApp Console, workload recovery can be initiated from the recovery page on the Ransomware Resilience. After the incidents are neutralized and workloads have been marked “Restore needed”, NetApp Ransomware Resilience recommends a recovery point actual (RPA) and orchestrates the workflow for a crash-resistant recovery.

- If the application or VM is managed by SnapCenter, Ransomware Resilience restores the application or VM back to its previous state and last transaction using the application-consistent or VM-consistent process. The application or VM-consistent restore adds any data that did not make it into storage, for example, data in cache or in an I/O operation, to the data in the volume.
- If the application or VM is *not* managed by SnapCenter and is managed by NetApp Backup and Recovery or Ransomware Resilience, Ransomware Resilience performs a crash-consistent

restore, where all the data that was in the volume at the same point of time is restored, for example, if the system crashed.

You can restore the workload by selecting all volumes, specific volumes, or specific files.

A workload can have one of the following restore statuses:

- **Restore needed**: The workload needs to be restored.
- **In progress**: The restore operation is currently underway.
- **Restored**: The workload has been restored.
- **Failed**: The workload restore process could not be completed.

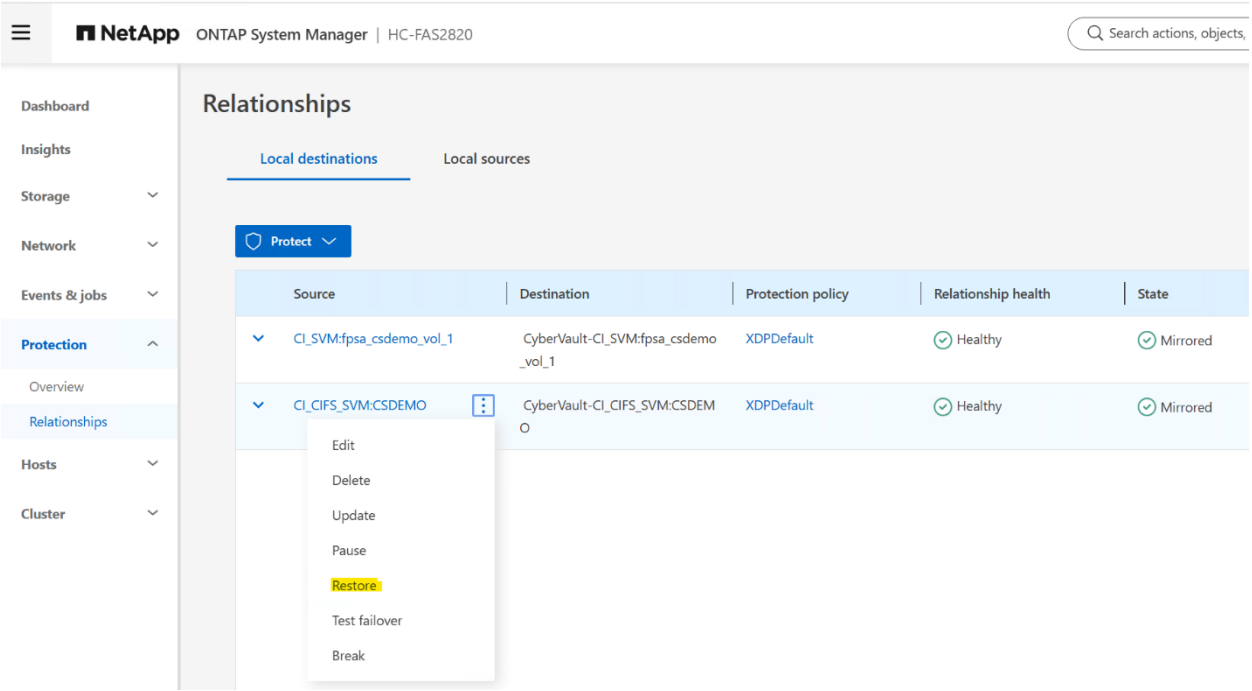
Refer to the NetApp documentation for detailed procedure on restoring workloads managed by SnapCenter, workloads that are not managed by SnapCenter, application workload recovery at the volume and file level and, recovery of file share or datastore.

[Recovering from a ransomware attack with Ransomware Resilience]

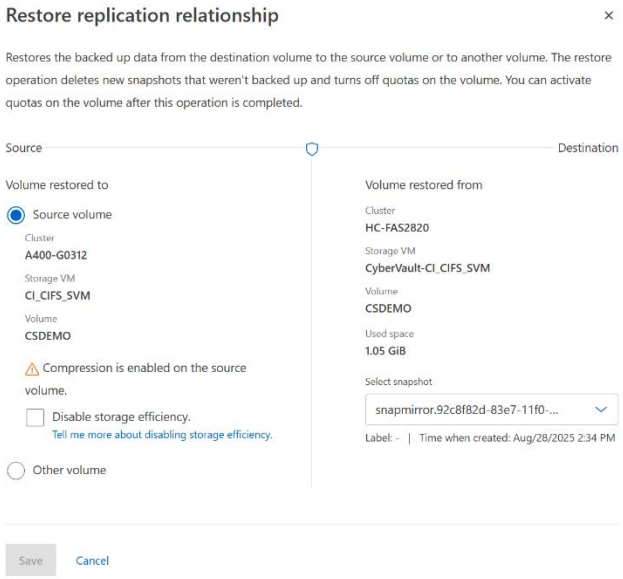
Recovering data using NetApp Cyber vault

In the event of ransomware attack and there is a need for recovering data from the cyber vault, the recovery process is simple and easy. The snapshot copies stored in the cyber vault can be used to restore the data as illustrated in the following screen shots.

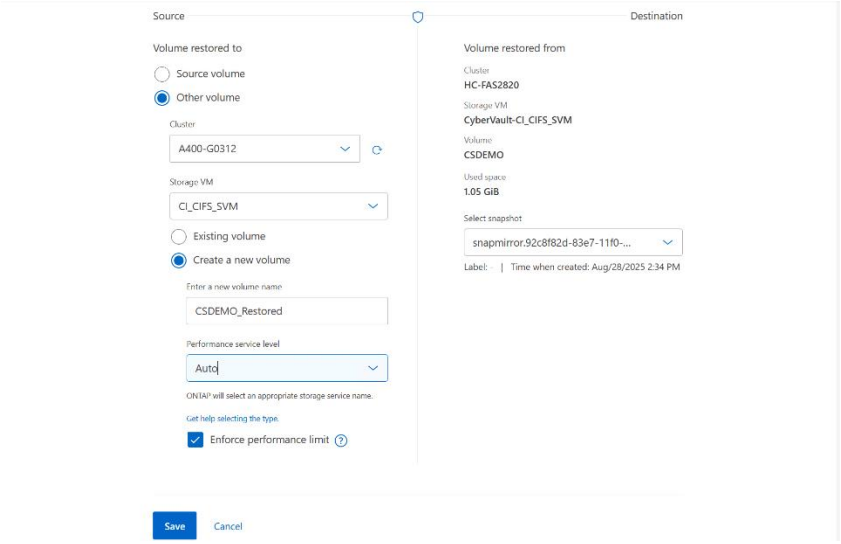
On the destination cluster hosting the cyber vault, click on **Relationships** under **Protection** on the left menu. From Local destinations tab, click on the three vertical dots next to the volume that you want to restore and choose **Restore**.



You can restore the backed-up data from the destination volume to the source volume or another volume.



In this example, a new volume is created on the source SVM.

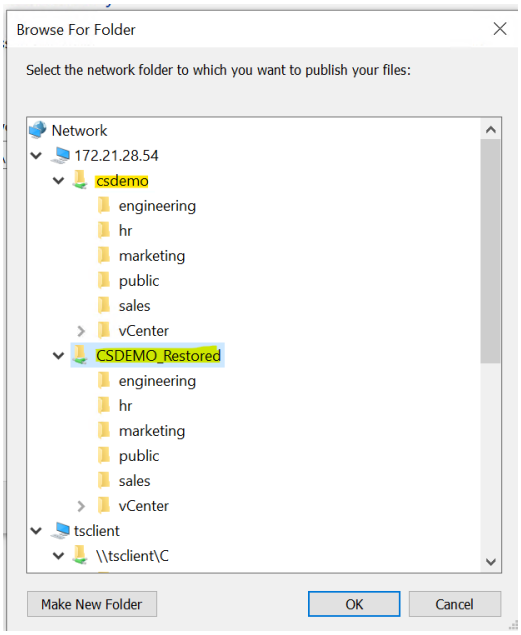


Check the source cluster for the new volume created with data from cyber vault.

```
A400-G0312::> volume show -vserver CI_CIFS_SVM
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
CI_CIFS_SVM CI_CIFS_SVM_root aggr1_A400_G0312_02 online RW 1GB    971.2MB    0%
CI_CIFS_SVM CSDEMO     aggr1_A400_G0312_02 online RW   10.53GB     9.05GB    9%
CI_CIFS_SVM CSDEMO_Restored aggr1_A400_G0312_01 online RW 1.20GB  206.3MB   82%
3 entries were displayed.

A400-G0312::>
```


You can create a new CIFS share for this volume and connect from a windows client to verify the content as shown below. As you can see, the new share “CSDEMO_Restored” has the same content as the original CSDEMO share.



Conclusion

As attackers find newer ways to generate and spread ransomware, newer techniques must be developed and adopted for ransomware detection and removal. Both Cisco and NetApp are continuously developing and updating their tools in their security arsenal to protect against ransomware attacks. The Workload Security feature of Data Infrastructure Insights is a great tool in the NetApp Security arsenal that can detect potential ransomware attacks based on changes in user’s data access patterns and block user access to limit the damage. The file and user activity data collected can be used for forensics activities and user audit reporting for up to 13 months. Customers with core ONTAP could get granular detection capabilities from Autonomous Ransomware Protection (ARP) and it can further be integrated with Data Infrastructure Insights for alerting and forensics activities. The Snapshot copy generated by either detection method is useful to restore data to a point closer to the attack, thereby minimizing the damage caused by the attack. For additional data protection and security, customers can implement NetApp cyber vault, which would isolate and secure the most valuable data and keep it confidential, intact and readily available when needed.

Data backup and restore operations play a crucial part in ransomware recovery. Therefore, they are strategically important for business planning. The implementation of these activities should be included in the ransomware recovery plan so that there are no compromises on reporting and recovery capabilities in the event of an attack. The most important thing is to select the right technology partners who can help in ransomware detection, removal, and restoration of data. FlexPod with Data Infrastructure Insights provides the capabilities needed to monitor and detect potential ransomware attacks and insider threats, while the NetApp SnapCenter products help to take VM and application consistent backups and restore the data when needed. Additionally, customers can integrate their on-prem and cloud environment with NetApp Console unified SaaS platform and make use of the services such as Backup and Recovery and Ransomware Resilience. When combined with Cisco’s security products at the Network and compute layers, you have a comprehensive solution to defend against Ransomware threat detection, protection and recovery.

Acknowledgement

The author would like to thank the following people for their support in the creation of this document:

- Mark Conahan, DII PM
- Amit Schwartz, Workload Security PM
- Sandeep Putrevu, Mgr. Insight Engineering
- FlexPod TME team (Cisco & NetApp)

Where to find additional information

- NetApp Data Infrastructure Insights Documentation
  https://docs.netapp.com/us-en/data-infrastructure-insights/index.html
- ONTAP cyber vault
  https://docs.netapp.com/us-en/netapp-solutions-dataops/cyber-vault/ontap-cyber-vault-overview.html#what-is-a-cyber-vault
- SnapCenter software documentation
  https://docs.netapp.com/us-en/snapcenter/index.html
- Autonomous Ransomware Protection (ARP)
  https://docs.netapp.com/us-en/ontap/anti-ransomware/
- NetApp Console
  https://docs.netapp.com/us-en/console-setup-admin/index.html
- NetApp Ransomware Resilience
  https://docs.netapp.com/us-en/data-services-ransomware-resilience/index.html
- TR-4572: The NetApp solution for ransomware
  https://www.netapp.com/media/7334-tr4572.pdf

Version history

Version	Date	Document version history
Version 1.0	Mar 2023	Initial version.
Version 2.0	Sep 2023	▪ Added SnapCenter Plug-in for VMware vSphere, for VM consistent backup and restoration as part of ransomware recovery plan. ▪ Replaced Cloud Secure with Workload Security to reflect name change. ▪ Updated the text and screenshots based on current Workload Security graphical user interface.
Version 3.0	Oct 2025	▪ Added NetApp Console and Ransomware Resilience ▪ Ransomware Resilience and DII Integration with Splunk ▪ Added NetApp Cyber vaulting ▪ Updated screen shots and content to reflect name change from Cloud Insights to Data Infrastructure Insights

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp