Technical Report

FlexPod ransomware protection & recovery with NetApp Cloud Insights and SnapCenter

Roney John Daniel, NetApp
Oct 2023 | TR-4961

In partnership with

Abstract

This technical report includes 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 attacks. This document focuses on installing and configuring Workload Security, which is a security feature of NetApp's Cloud Insights® and ONTAP Autonomous Ransomware Protection® (ARP), which is a native ONTAP security feature to protect from ransomware attacks and insider threats. It also discusses NetApp's SnapCenter® plug-ins for VM and application consistent backup and recovery.

TABLE OF CONTENTS

Ransomware overview **4**

How does it spread? 4

Types of ransomware 4

What is the impact? 4

What is the solution? 5

NetApp's solutions to ransomware 5

Workload Security overview **7**

How Workload Security works 7

Workload Security components 8

Workload Security licensing 8

FlexPod overview **9**

Architecture details 10

Ransomware protection measures offered by FlexPod 11

Cloud Insights in FlexPod 12

Setting up Workload Security in FlexPod **12**

Install Workload Security agent on a VM to collect data 12

Configure a user directory collector 18

Configure ONTAP data collector 21

Define automated response policies 23

Configure email notification 25

Integrating ONTAP Autonomous Ransomware Protection (ARP) 26

Case study **33**

Accidental file deletion 33

A sensitive file is copied to a public folder accidentally. 34

Bulk file deletion 36

Ransomware attack simulation via Bulk File Encryption 38

Recovering data after ransomware attack **41**

ONTAP Volume Snapshot Restore 41

SnapCenter Plug-in for VMware vSphere (SCV) 42

SnapCenter Plugins for application consistent backup and recovery 52

Conclusion **53**

Acknowledgement **54**

Where to find additional information **54**

Version history **54**

LIST OF TABLES

Table 1) Cloud Insights editions. 8
Table 2) Hardware and Software. 10
Table 3) Agent requirements. 13
Table 4) For US-based Workload Security environments. 14
Table 5) For Europe-based Workload Security environments. 14
Table 6) For APAC-based Workload Security environments. 14
Table 7) In-network rules. 14

LIST OF FIGURES

Figure 1) FPolicy External Server. 6
Figure 2) FlexPod Solution 9
Figure 3) FlexPod Topology diagram. 10
Figure 4) Cloud and In-Network Rules 13
Figure 5) SnapCenter Plug-ins 52

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.

Ransomware continues to make headlines in 2022, from locking down a prison, leaking employee credentials and proprietary information online, to declaring a national emergency due to a cyber-attack. 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 NFS or SMB/CIFS shares 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 a large number of 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.

Attackers also find newer ways to spread malware and the latest is in the form of physically mailing 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 a 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 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.

This document details how the Workload Security feature of NetApp Cloud 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.

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.

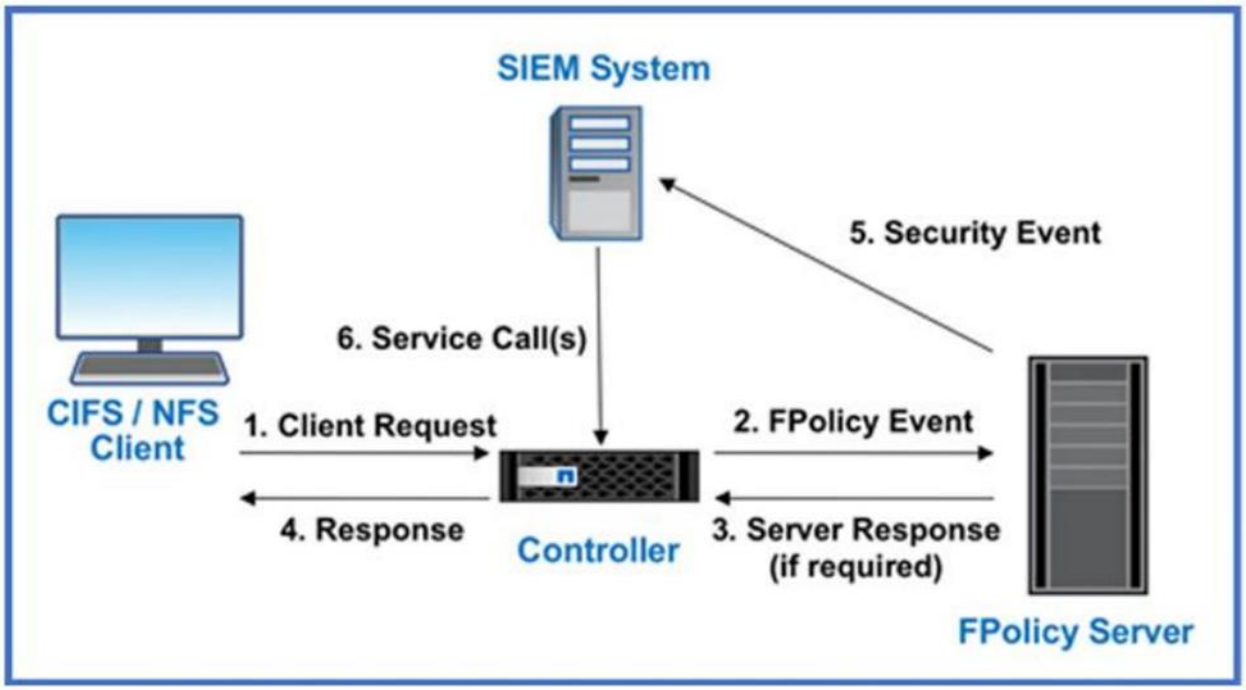
- **NetApp® Active IQ®** (**AIQ**) checks NetApp ONTAP systems for adherence to NetApp configuration best practices such as enabling FPolicy.
- **NetApp Active IQ Unified Manager®** (**AIQUM**) generates alerts for abnormal growth of NetApp Snapshot copies or storage efficiency loss, which can indicate potential ransomware attacks.
- **ONTAP System Manager** enables analysis of Snapshot percent change or storage efficiency savings in real time.
- **Multi-Factor 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.

- **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 Cloud Insights dashboard. This feature is supported on Amazon FSx and Cloud Volumes ONTAP as well. In ONTAP 9.12.1, 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 days to 30 days. Multi-admin verification for ARP configuration is supported in ONTAP 9.13.1.
- **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 BlueXP™. 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.

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

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: Cloud Insights with Workload Security feature is NetApp's own external mode FPolicy server.

- **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.

Workload Security overview

NetApp Cloud Insights is one of the offerings from NetApp BlueXP, a cloud based unified platform, and Workload Security (previously called **Cloud Secure**) is a feature of NetApp Cloud Insights. 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 a 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 assumes 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 documents 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 makes 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 Cloud Insights for analysis.

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 FSx for NetApp ONTAP

Refer to the following link for more information.

Getting Started with Workload Security

Workload Security licensing

Workload Security is offered as a feature in NetApp Cloud Insights. Cloud Insights is offered in 2 editions: basic and premium. The basic edition is free for all NetApp customers with an active NetApp support account. Workload Security is offered with the premium edition.

Follow the guidelines below to subscribe to Cloud Insights.

- Sign up for an account in BlueXP if not done already. This will enable you to access all of NetApp's cloud offerings. You can sign up using https://*cloud.netapp.com* or https://*bluexp.netapp.com*.
- You can register for a free trial of Cloud Insights to explore the features that are available. During the registration process, you can choose the global region to host your Cloud Insights environment.
- Subscribe to Cloud Insights and choose Premium edition.

Table 1 highlights the key features of Cloud Insights offerings.

Table 1) Cloud Insights editions.

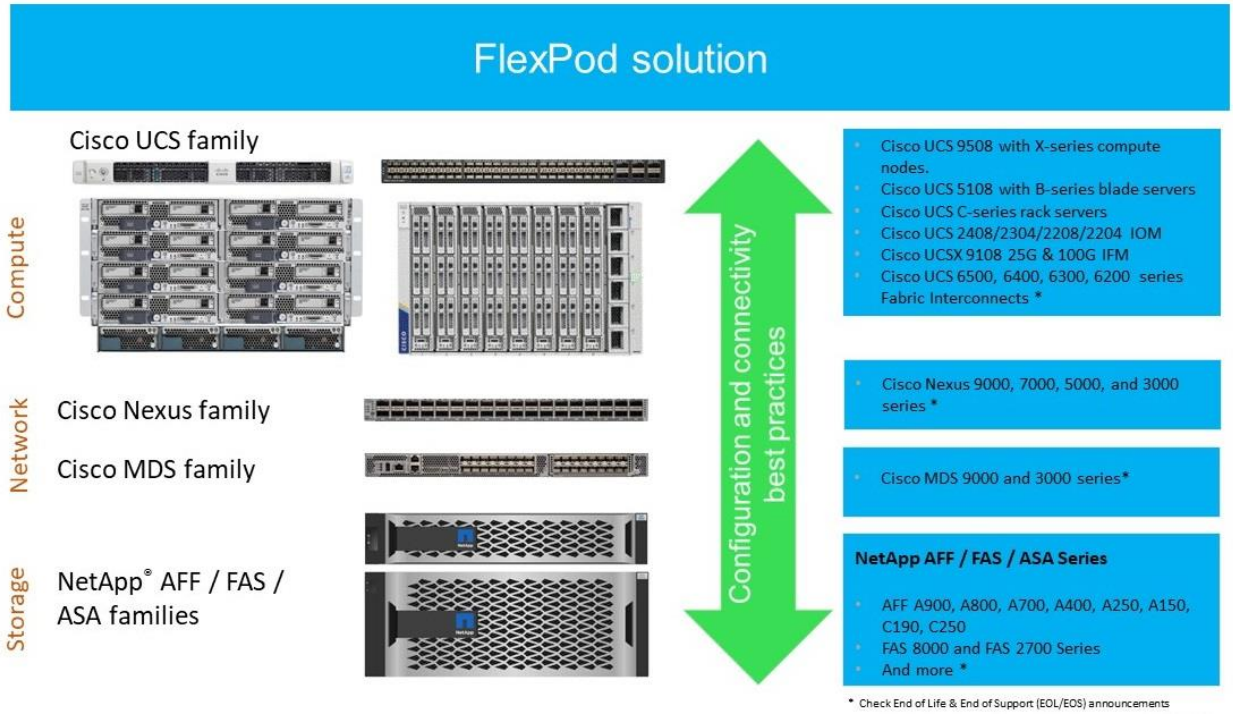
Key feature	Basic edition	Premium edition
Data Retention	7 Days	13 Months
Infrastructure & Storage Metrics	NetApp Only	Multi-Vendor
Customizable Dashboards	✓	✓
Forum, Documentation, and Training Videos	✓	✓
Live Chat and Technical Support	-	✓
VM Metrics	-	✓
Cloud Metrics	-	✓
Service Metrics	-	✓
Monitors and alerting	*	✓
API Access	✓	✓
Single Sign-On (SSO)	-	✓

Key feature	Basic edition	Premium edition
User Data Access Auditing	-	✓
Insider Threat Detection with AI/ML	-	✓
Business Intelligence and Reporting	-	✓

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 12 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 virtual datacenter that is built around Cisco UCS B, C and X series servers, Cisco UCS Fabric Interconnects, Cisco Nexus® and MDS switches and NetApp Storage. It is suitable for various enterprise workloads as well as public, private and hybrid cloud environments.

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

FlexPod XCS is the next generation FlexPod for hybrid cloud environment that uses Cisco Intersight platform for configuring, monitoring, and managing the whole stack.

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

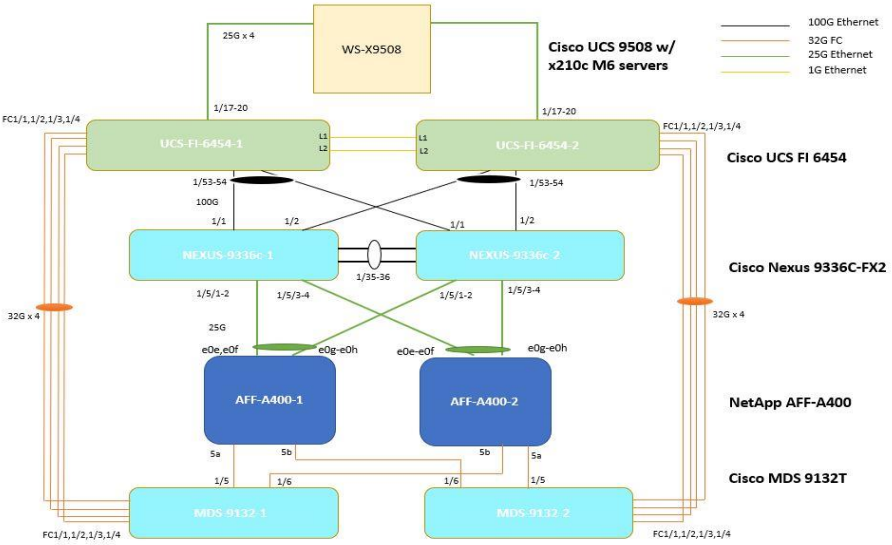
Architecture details

A FlexPod datacenter topology is used for validating Workload Security features in Cloud Insights. Two Centos Linux VMs are deployed in the management network which serves as the Workload Security agent machines. These machines can access the Cloud 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 10 VM are deployed in the FlexPod stack for end user activity and ransomware simulation.

Topology

The topology under test is shown below (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 2.

Table 2) Hardware and Software.

Type	Version
SVM Data collector	NetApp AFF-A400 running ONTAP 9.13.1
User Directory Data Collector	Windows Server 2016 Datacenter edition running Active Directory
Workload Security Agents (2)	Centos Stream 8 with Cloud Secure 1.531.0
Linux VMs for end-user access (2)	Ubuntu 22.04.1 LTS

Type	Version
Windows VM for end-user access	Windows 10 Enterprise
VMware vCenter Server	8.0
NetApp ONTAP Tools for VMware vSphere	9.12
NetApp SnapCenter Plug-in for VMware vSphere	4.9

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

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 Secure IPS (NGIPS)**

  Cisco Firepower Next-Generation IPS (NGIPS) threat appliance comes in physical and virtual form factor and provides network visibility, security intelligence, automation, and advanced threat protection. It uses industry-leading intrusion prevention capabilities and multiple techniques to detect even the most sophisticated network attacks and protect you against them.

  For more information on the family of this product, refer to the following link.

  Cisco Secure IPS - Cisco
- **Cisco Secure Cloud Analytics**

  Cisco Secure Cloud Analytics or Stealthwatch Cloud is a Software-as-a-Service (SaaS) product that you can use to identify internal and external threats in private, public, and hybrid cloud environments. It provides the actionable security intelligence and visibility necessary to identify malicious activities in real time. It analyzes network flows and traffic telemetry such as NetFlow records in real time or near real time. It monitors and analyzes north/south traffic as well as east/west traffic and if suspicious network traffic is detected, it can alert and provide automatic or manual response capabilities. Refer to the following link for more information.

  Cisco Secure Cloud Analytics

Compute

- **Cisco Secure Endpoint**

  Cisco Secure Endpoint, formerly known as Advanced Malware Protection (AMP), for endpoints offers cloud-delivered endpoint protection with advanced endpoint detection and response across multi-domain control points. Threats can take the form of software viruses and other malware such as ransomware, worms, Trojans, spyware, adware, and fileless malware. Advanced malware protection software is designed to prevent, detect, and help remove threats in an efficient manner from computer systems. Cisco Secure Endpoint is available as an offering of Cisco Secure X platform. 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 the Workload Security feature in detail.

Cloud Insights in FlexPod

As mentioned earlier, Cloud Insights is a NetApp cloud offering and Workload Security is a feature within Cloud Insights. With the premium edition, you can avail every features of Cloud Insights as well. Cloud Insights can be used to gather inventory and performance data from various data collectors such as NetApp ONTAP, NetApp Cloud Volumes ONTAP, Amazon FSx for NetApp ONTAP, VMware VCenter, Cisco MDS switches, Cisco Nexus switches and UCS Fabric Interconnects running Fiber channel services, and many more. Custom dashboards can be created to view the data collected and reports can be generated. Cloud Insights monitoring and reporting features are not explored as part of this document. However, you can refer to TR-4868: NetApp Cloud Insights for FlexPod for more details.

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 Cloud 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 a Cloud 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 3.

Table 3) Agent requirements.

Type	Comments
Operating System	Licensed version of Linux *(Red Hat Enterprise Linux 7.x, 8.x 64-bit, CentOS 7.x 64-bit, CentOS 8 Stream, or Ubuntu 20 through 22 64-bit).* **Note:** SE (Security Enhanced) Linux is not supported
CPU	4 CPU Cores
Memory	16GB RAM
Disk Space	/opt/netapp 35GB (minimum)
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).

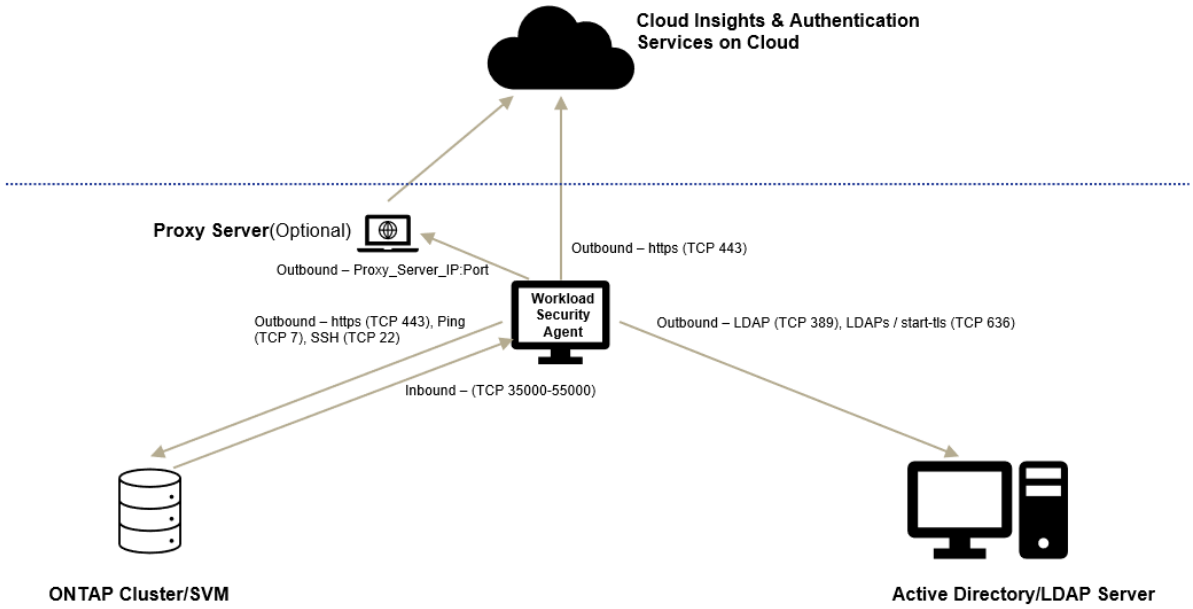
Note: If the Workload Security agent and Cloud Insights Acquisition Unit are installed on the same machine, there must be a minimum 50-55GB available disk space (25-30GB for /opt/netapp and 25G for /var/log/netapp).

Note: 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 Cloud Insights SaaS environment and data collectors, specific ports must be opened on the end points and any network firewalls in between them. The end points and ports are shown in the diagram below (Figure 4).

Figure 4) Cloud and In-Network Rules



If the Organization's security policy does not allow opening a wide range of ports as in TCP 35000-55000, a smaller range such as TCP 35000-35100 can be configured. Note that each SVM requires 2 TCP ports.

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 Cloud Insights SaaS environment hosted in the cloud. Refer to the following tables to open access control lists (ACLs) based on the region where your Cloud Insights environment resides (Tables Table 4,Table 5 and Table 6).

Table 4) 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 Cloud Insights
TCP	443	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	Outbound	Access to authentication services

Table 5) 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 Cloud Insights
TCP	443	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	Outbound	Access to authentication services

Table 6) 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 Cloud Insights
TCP	443	gateway.c01.cloudinsights.netapp.com 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 7 when opening ACLs on the network as well as data collectors.

Table 7) In-network rules.

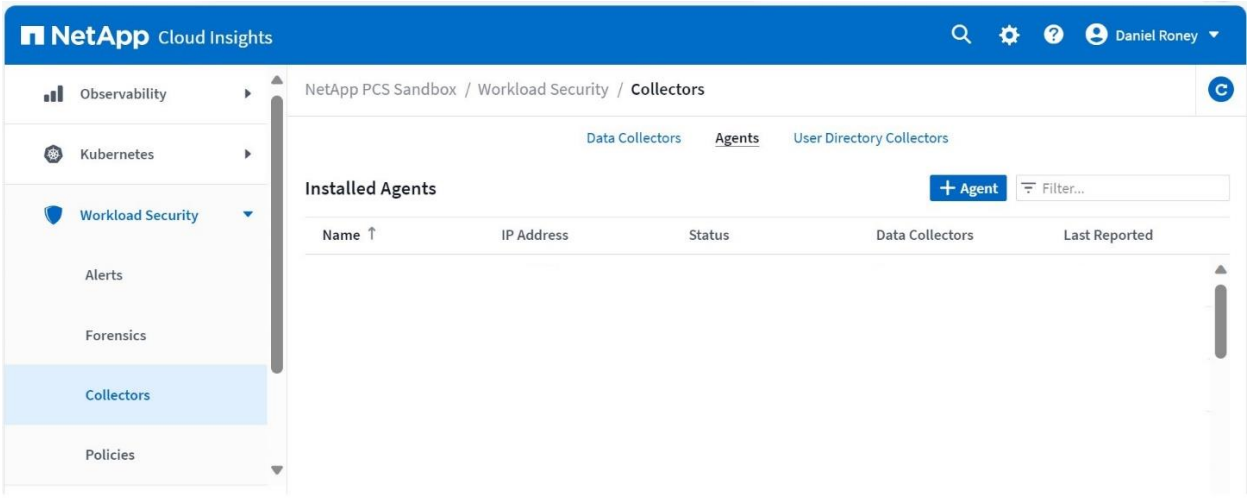
Protocol	Port	Destination	Direction	Description
TCP	389(LDAP) 636 (LDAPs / start-tls)	LDAP Server URL	Outbound	Connect to LDAP
TCP	443	Cluster or SVM Management IP Address (depending on SVM collector configuration)	Outbound	API communication with ONTAP
TCP	35000-55000	SVM data LIF IP Addresses	Inbound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

Protocol	Port	Destination	Direction	Description
TCP	7	SVM data LIF IP Addresses	Outbound	Unidirectional between Workload Security agent and ONTAP. Agent pings the SVM LIFs.
SSH	22	Cluster Management	Outbound	For CIFS/SMB user blocking.

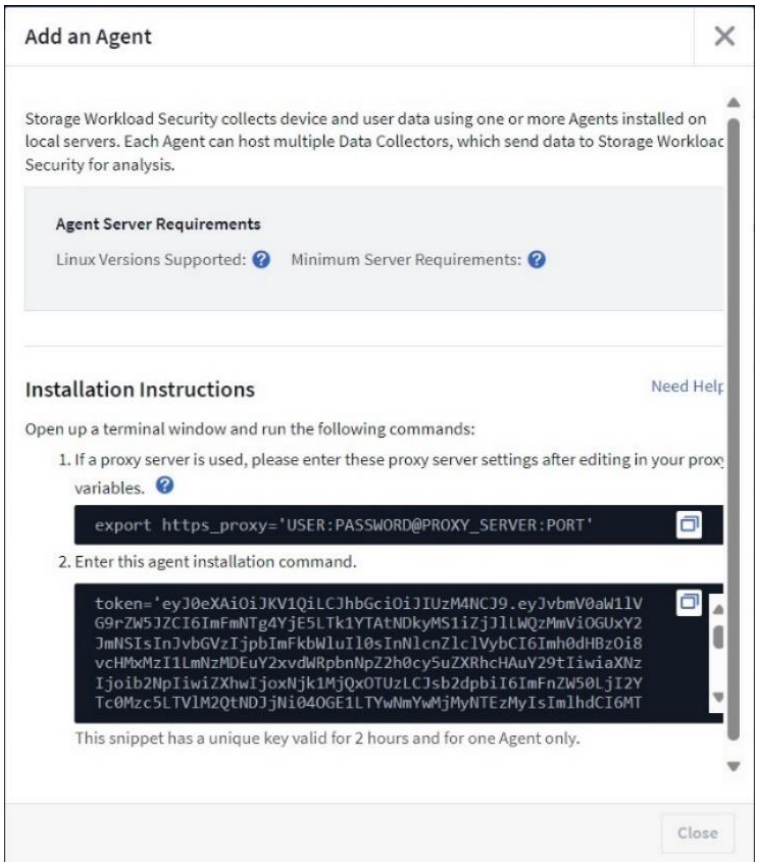
Steps to configure Workload Security agent

In the FlexPod lab setup, two Workload Security agents are configured on Centos 8 Stream based Linux VMs, one to monitor the ONTAP SVM data collector 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 Cloud 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 a pop-up message "New agent detected!".

The agent server console will start the service as shown in the following example.

```
Starting CloudSecure Agent services.
                    Welcome to CloudSecure (R) 1.531.0
                    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
[admin@fp-cloud-secure-1 ~]$
```

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

```
[admin@fp-cloud-secure-1 ~]$ sudo systemctl status cloudsecure-agent.service
[sudo] password for admin:
● cloudsecure-agent.service - Cloud Secure Agent Daemon Service
   Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled;
   Active: active (running) since Thu 2023-01-12 14:17:22 EST; 6 days ago
 Main PID: 1194 (java)
    Tasks: 77 (limit: 100910)
   Memory: 2.0G
   CGroup: /system.slice/cloudsecure-agent.service
           ├─ 1194 java -Dconfig.file=/opt/netapp/cloudsecure/agent/conf/applic
           └─96244 java -Dconfig.file=/opt/netapp/cloudsecure//data-collectors/

Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Warning:
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: The JKS keystore uses a proprieta
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Importing keystore /opt/netapp/cl
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: [Storing /opt/netapp/cloudsecure/
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Certificate was added to keystore
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: [Storing /opt/netapp/cloudsecure/
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: Certificate was added to keystore
Jan 17 21:53:34 fp-cloud-secure-1 bash[1194]: [Storing /opt/netapp/cloudsecure/
Jan 17 21:53:36 fp-cloud-secure-1 bash[1194]: Warning: Nashorn engine is planne
Jan 17 21:53:36 fp-cloud-secure-1 bash[1194]: Warning: Nashorn engine is planne

[admin@fp-cloud-secure-1 ~]$
```

8. Run the following commands on the prompt to open the ports that are used by Workload Security.

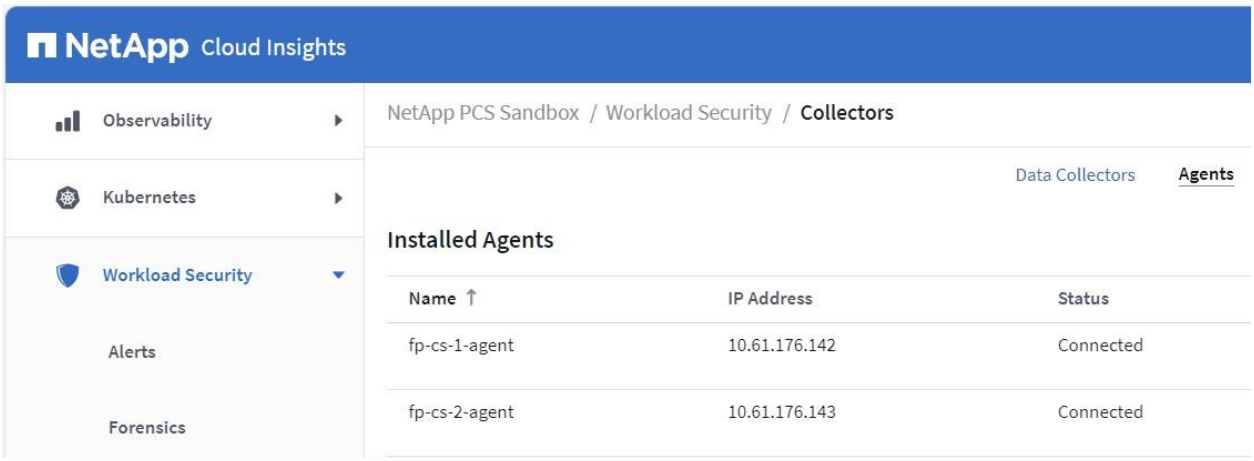
```
sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp

sudo firewall-cmd –reload
```

Note: Each SVM uses 2 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.

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

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

10. Repeat steps 2-6 to install additional agents as required.
11. You can check the status of the agent by clicking **Workload Security > Collectors** and choosing the **Agents** tab.



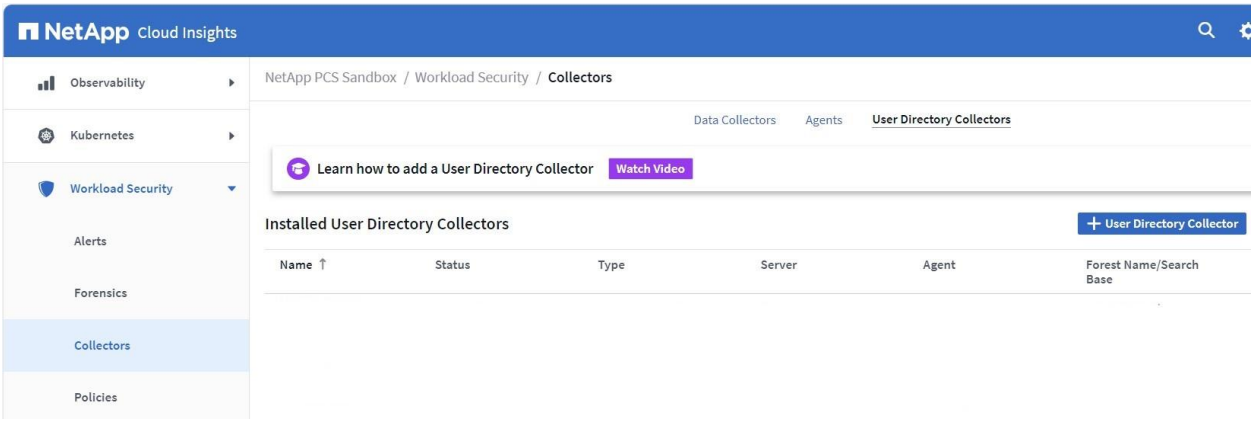
Configure a user directory collector

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 connector. The Workload Security agent must be configured before this step. This task can be performed by a Cloud Insights administrator or account owner.

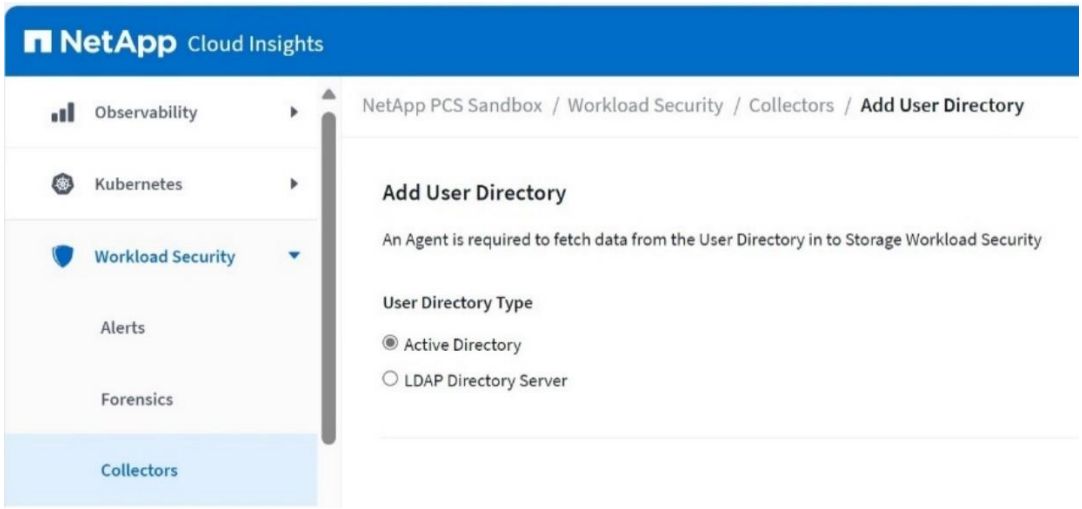
Steps to configure a user directory collector

Follow the procedure to configure a user directory collector.

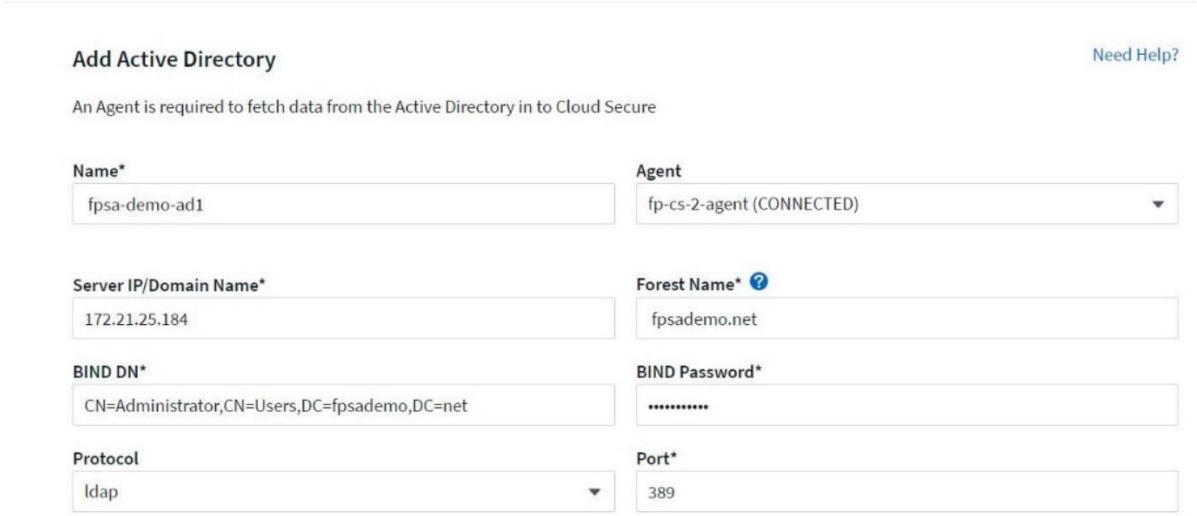
1. In the Cloud Insights menu, click: **Workload Security > Collectors > User Directory Collectors > + User Directory Collector**



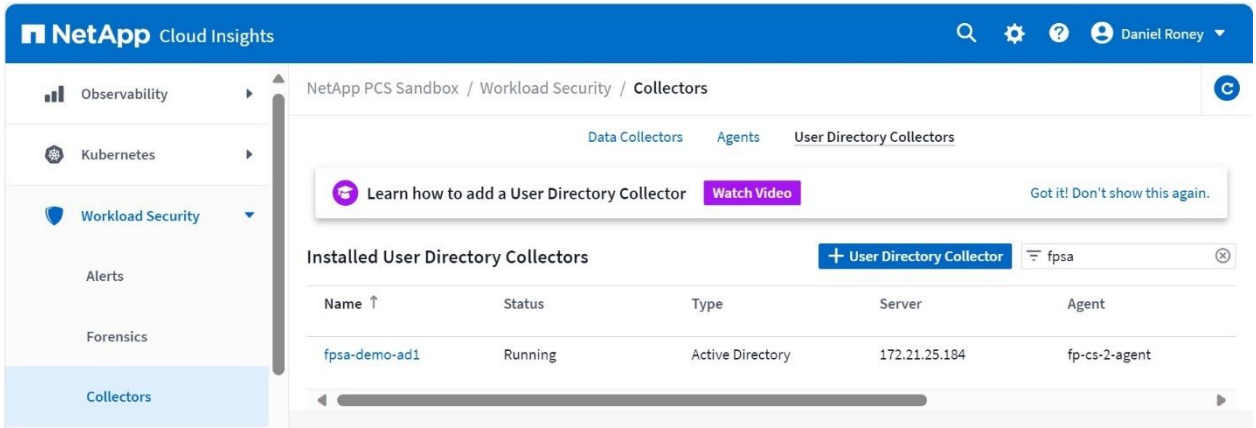
2. The system displays the **Add User Directory** screen. Choose **Active Directory** and click on **Continue.**



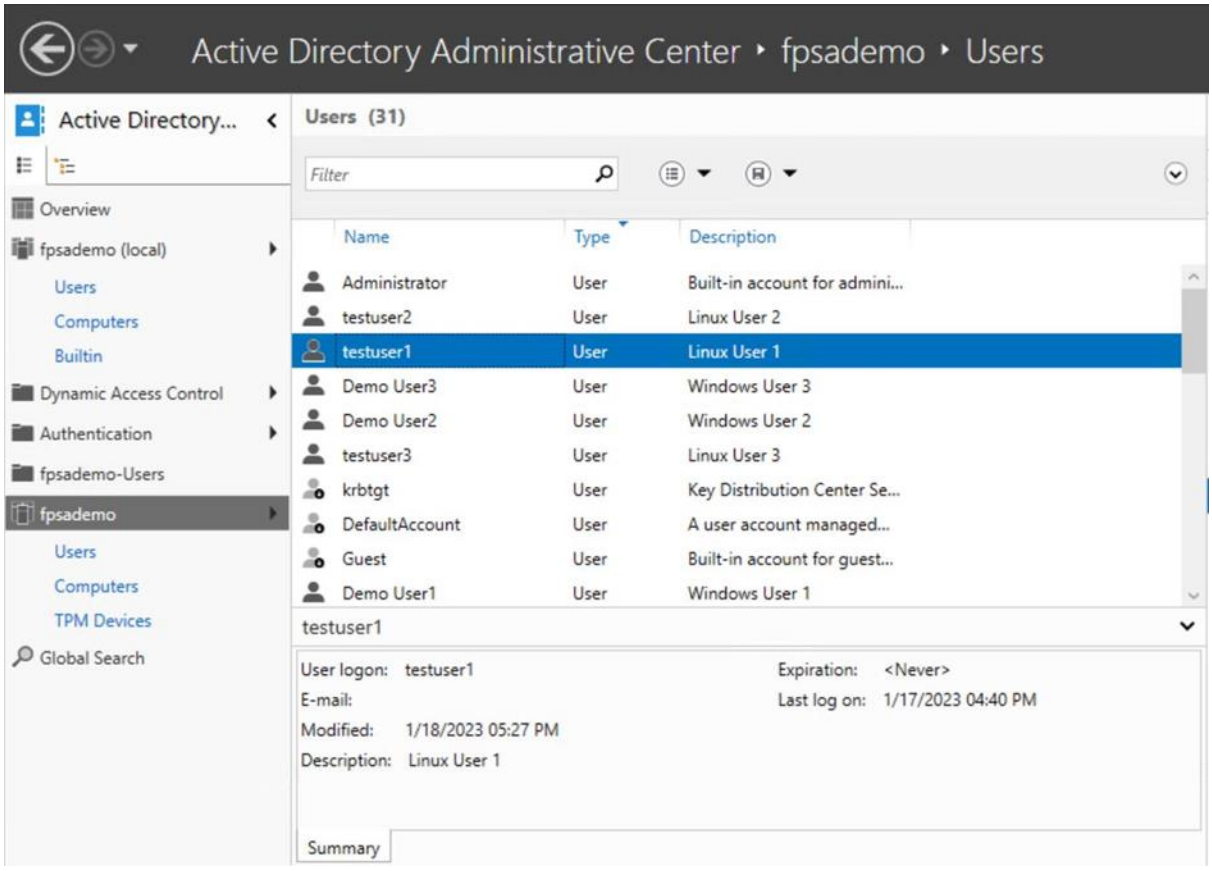
3. Select the agent that you installed previously and enter values in the remaining fields. You can leave the optional attributes with their default values. Click **Save** to add the user directory collector.



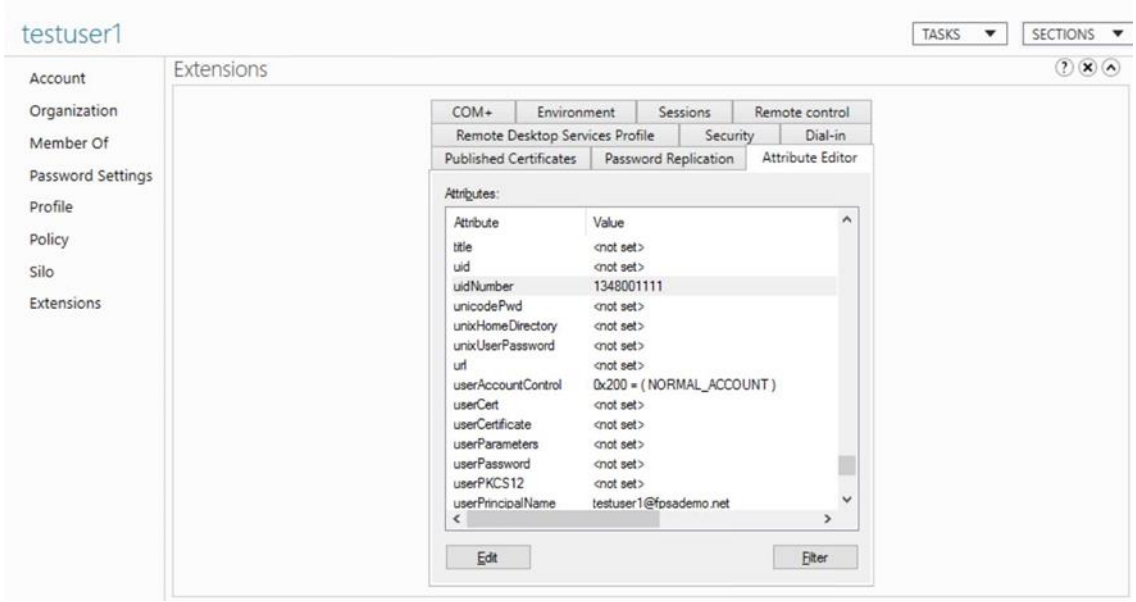
4. Verify that the collector is in the **Running** state.



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 Cloud 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

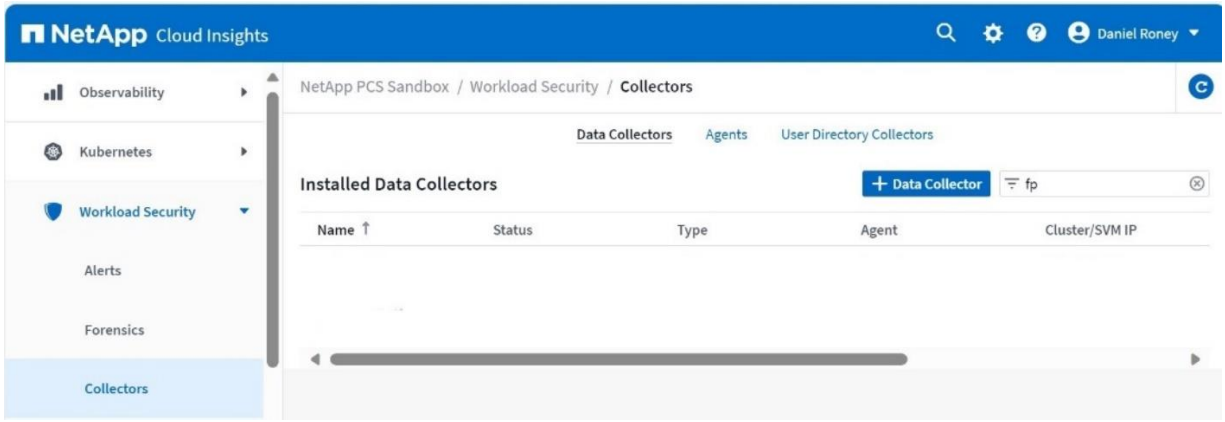
Workload Security currently supports three types of ONTAP data collectors: NetApp ONTAP SVM, NetApp Cloud Volumes ONTAP, and Amazon FSx for NetApp ONTAP. This document focuses on evaluating NetApp ONTAP SVM data collector.

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.

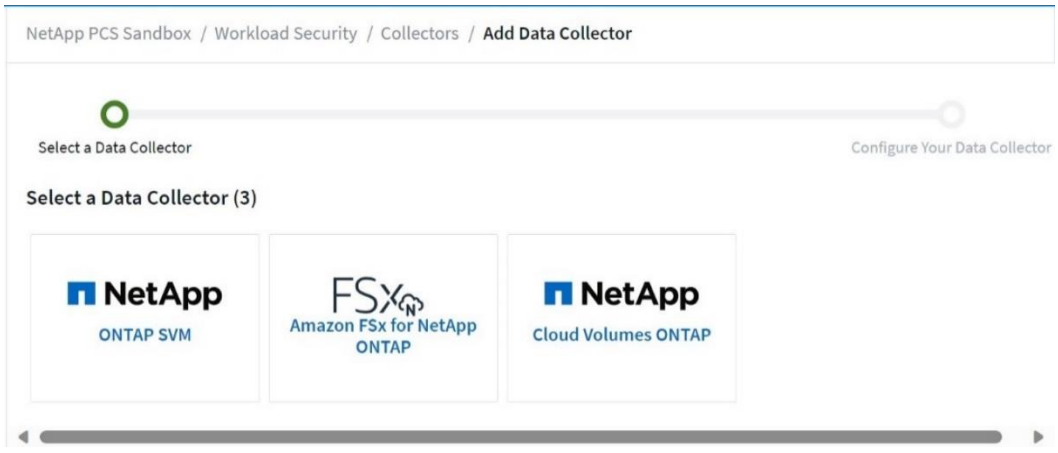
Steps to configure SVM data collector

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

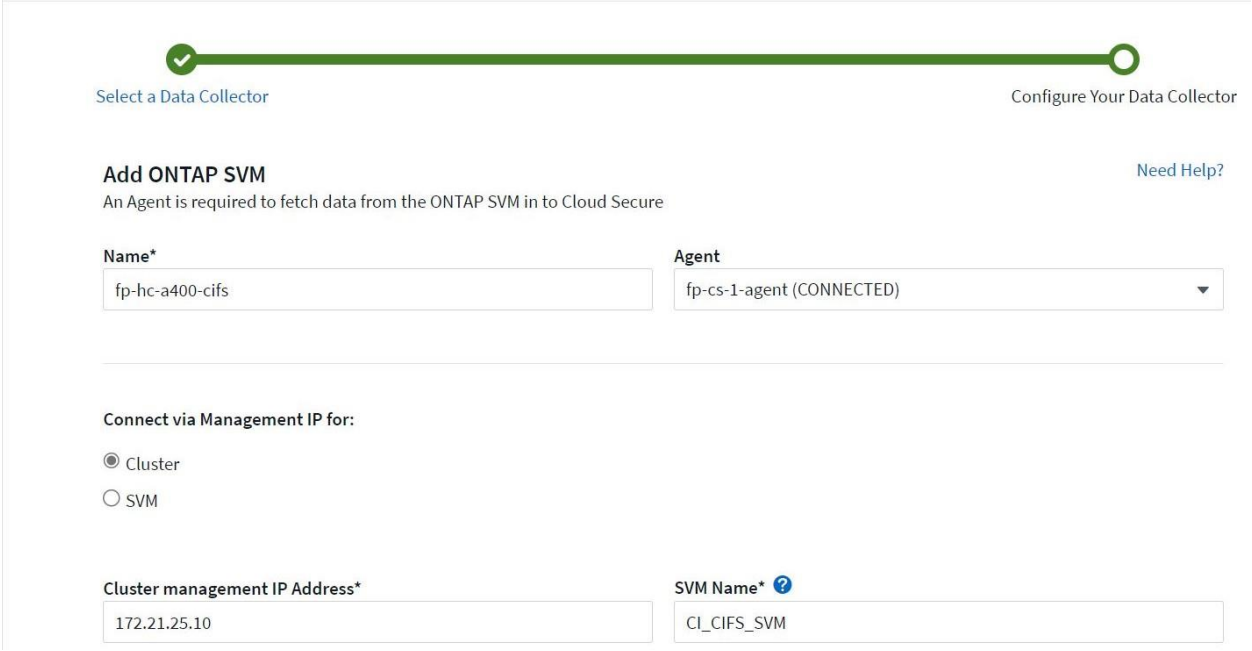
1. Log in as Administrator or Account Owner to your Cloud Insights environment.
2. Click **Workload Security > Collectors > Data Collectors > +Data Collector**



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

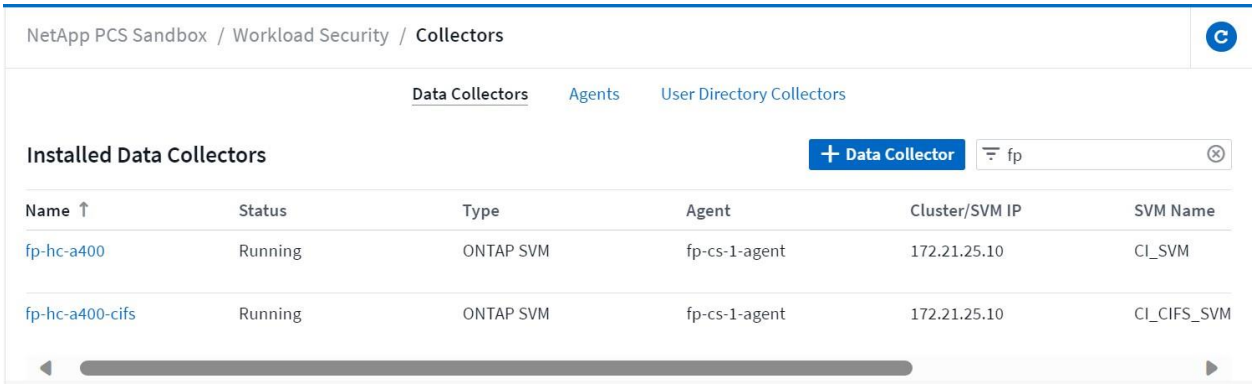


3. Hover over the NetApp SVM tile and click ***+Monitor.** The system displays the ONTAP SVM configuration page. Enter the required data for each field and click **Save**.



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

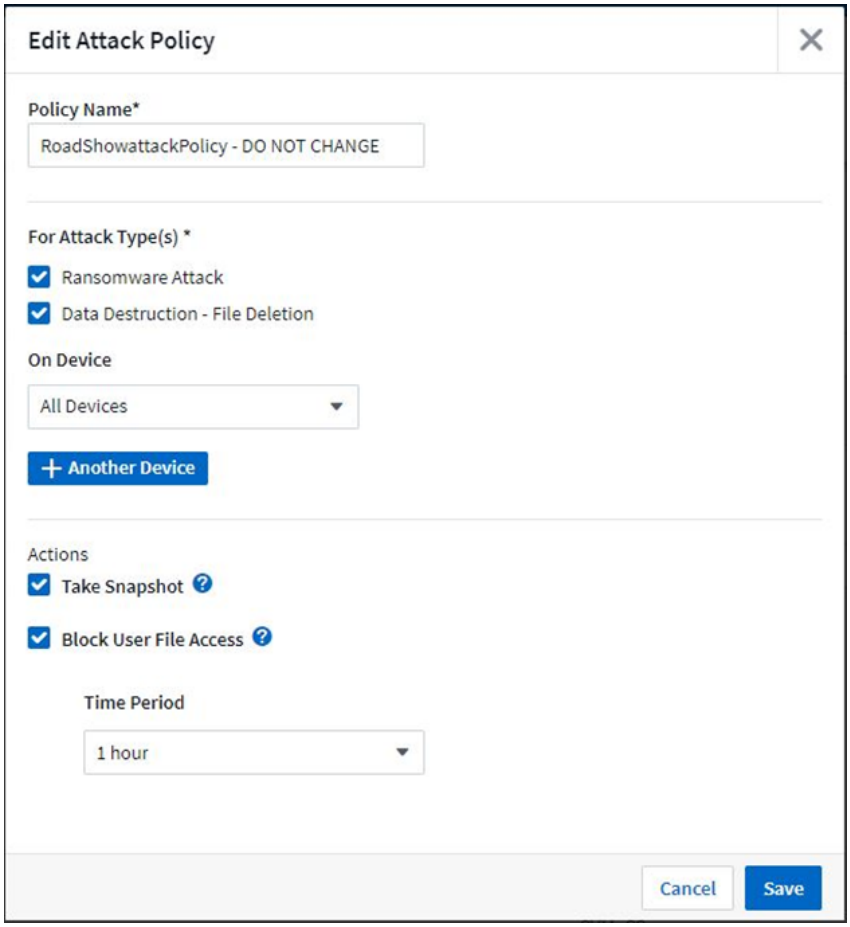
Response policies are used to trigger specific actions in the event of an attack or abnormal user behavior. You can create policies for attacks or warnings and apply them on specific devices or all devices.

Steps to configure automated response policy

Follow the procedure to configure attack and warning policies.

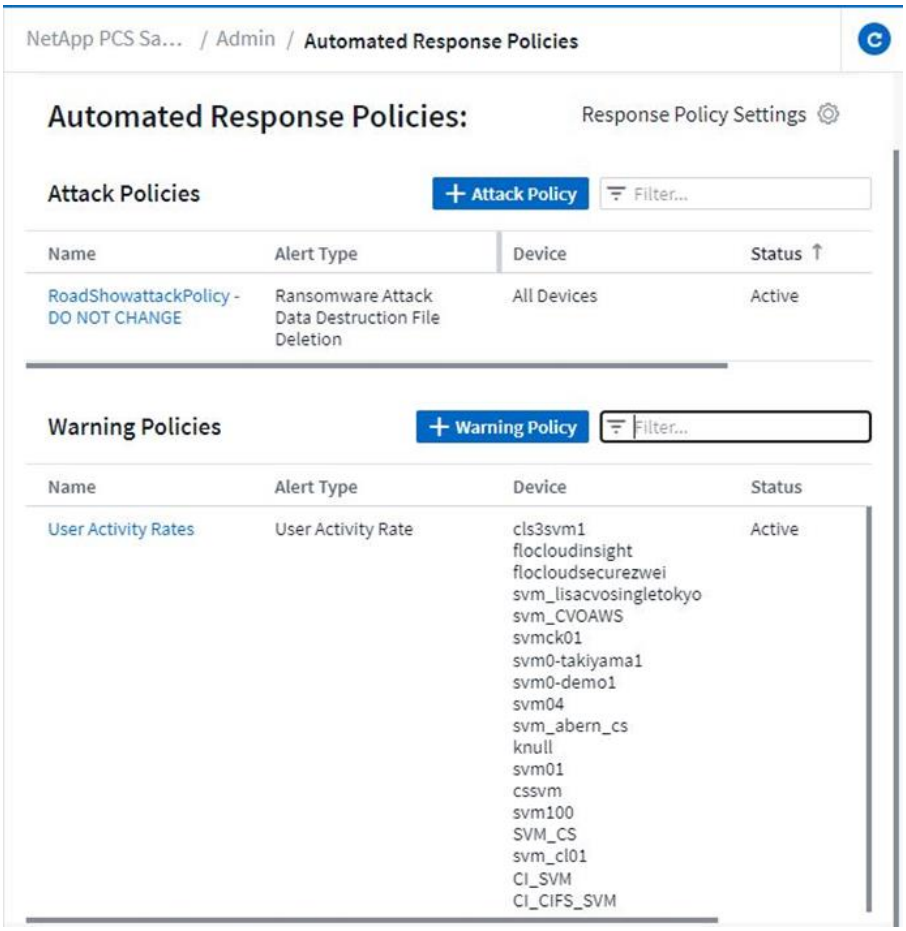
1. To Create an attack policy, go to **Workload Security > Policies > +Attack Policy**

   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.



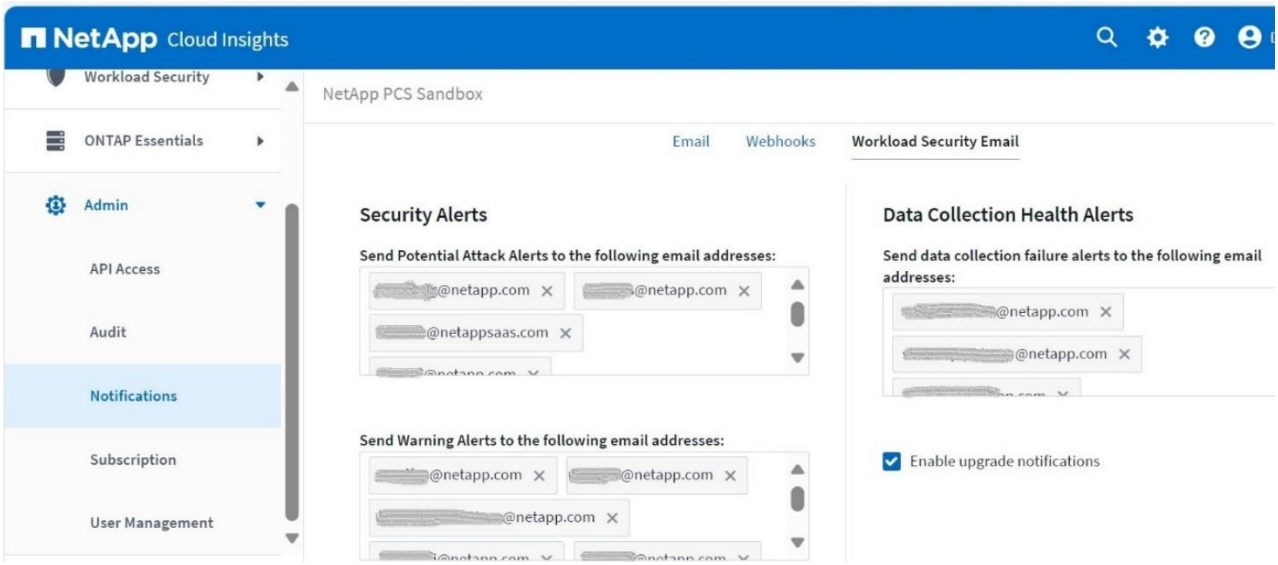
2. To Create a warning policy, go to **Workload Security > Policies > +Warning Policy**

   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 (NFS and SMB) environments to proactively detect and warn about abnormal in-file activity that might indicate a ransomware attack. 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 block user file access.
- Provides forensics capabilities:

✓ Allow customers to conduct data breach investigations.

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

ARP is a licensed feature. For more information on ARP licensing, refer to the following link.

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

Prerequisites

1. Latest ONTAP release and patch is recommended (currently ONTAP 9.13.1P2); minimum ONTAP release supported is 9.10.1.
2. ARP enabled volumes.
3. Workload Security collector should be added via cluster IP.
4. Cluster level credentials must be used when adding the SVM.

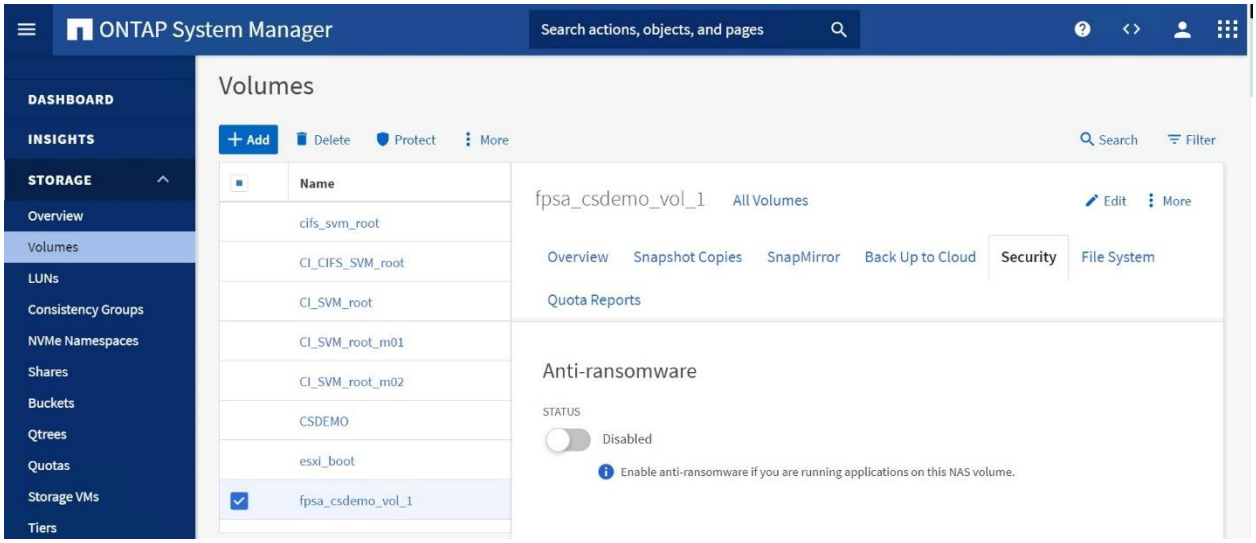
Enable Autonomous Ransomware Protection

ARP must be enabled via ONTAP System Manager or ONTAP CLI. Cloud Insights/Workload Security cannot enable ARP. When enabled, it will operate in the learning mode until it is switched to Active mode.

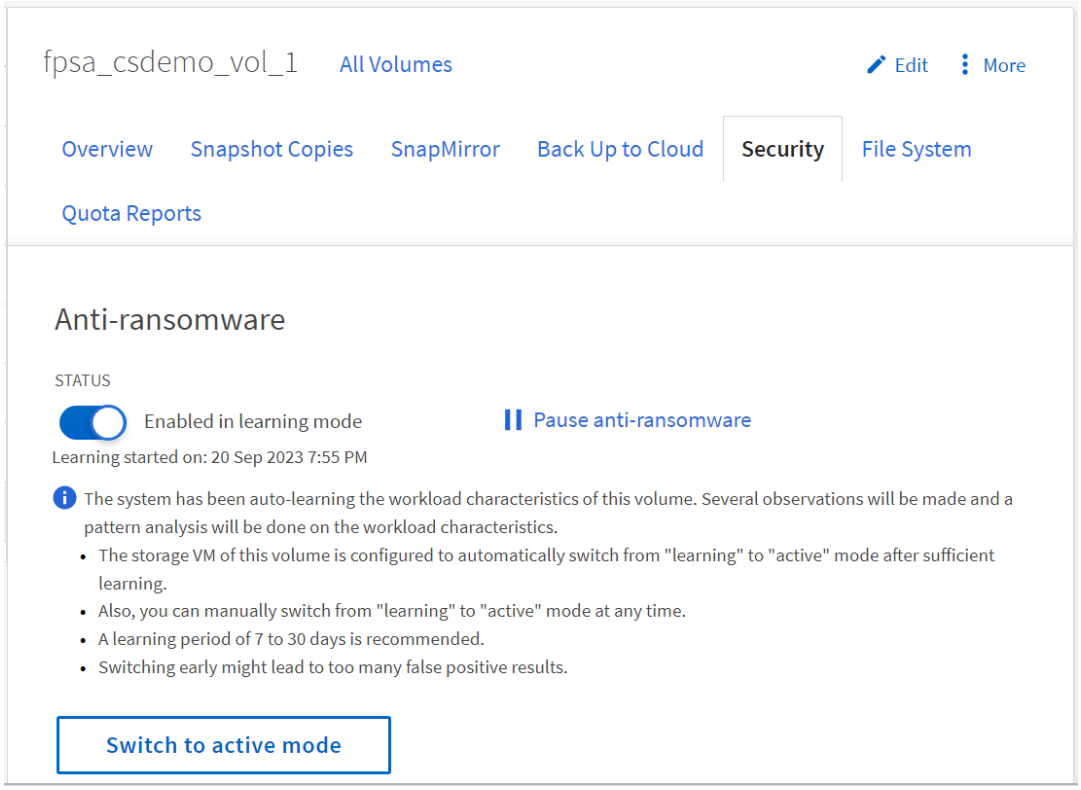
Steps:

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 in learning-mode in the Anti-ransomware box.
3. When the learning period is over, switch ARP to active mode.

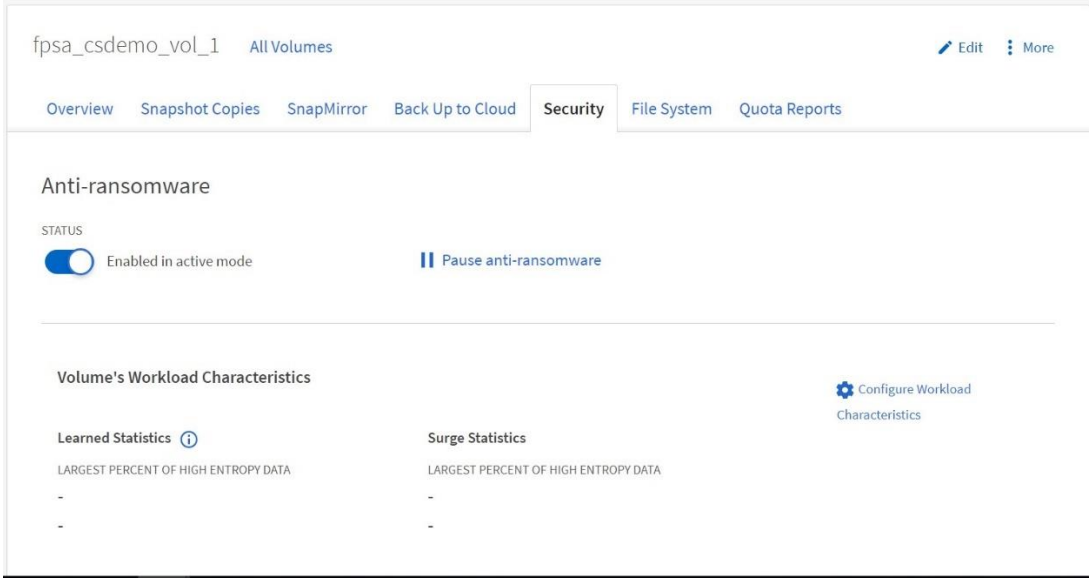
The following screenshots display ONTAP System Manager user interface to enable ARP.



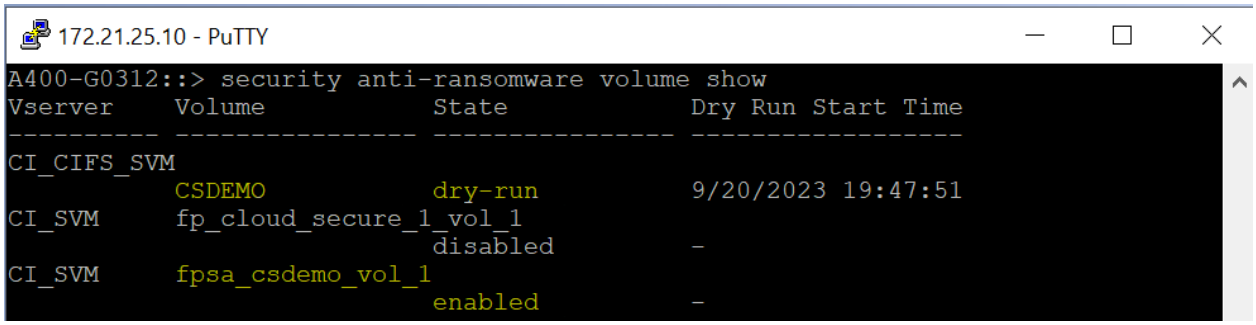
The following screenshot displays the status of ARP when it is enabled and running in learning mode. You can disable, pause or switch to active mode from this screen.



The following screen shows 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.

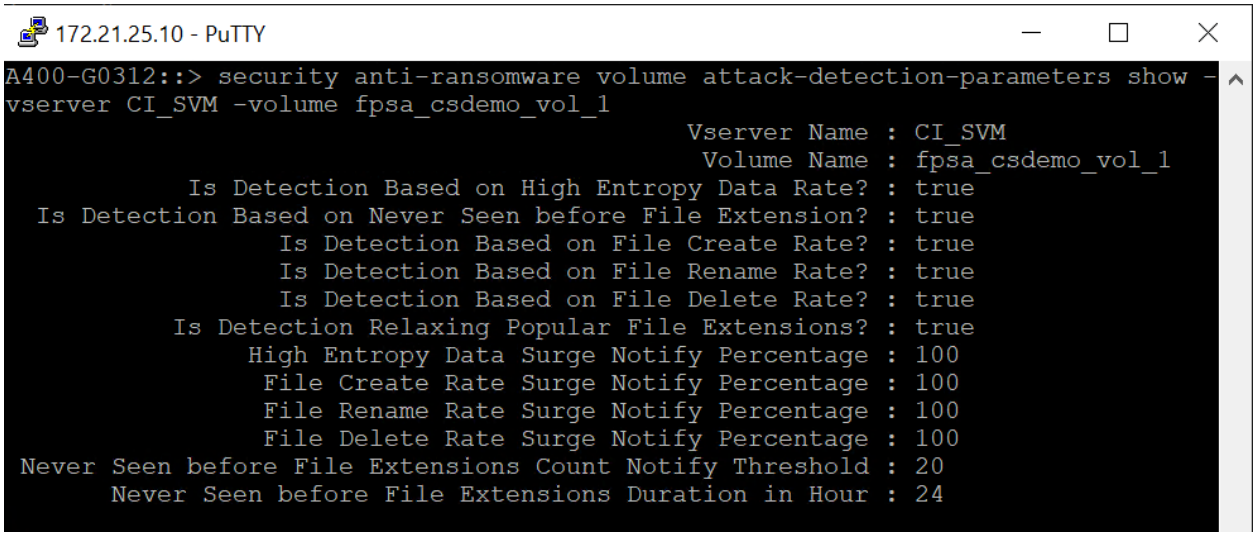
https://docs.netapp.com/us-en/ontap/anti-ransomware/enable-task.html

Fine tuning attack detection parameters

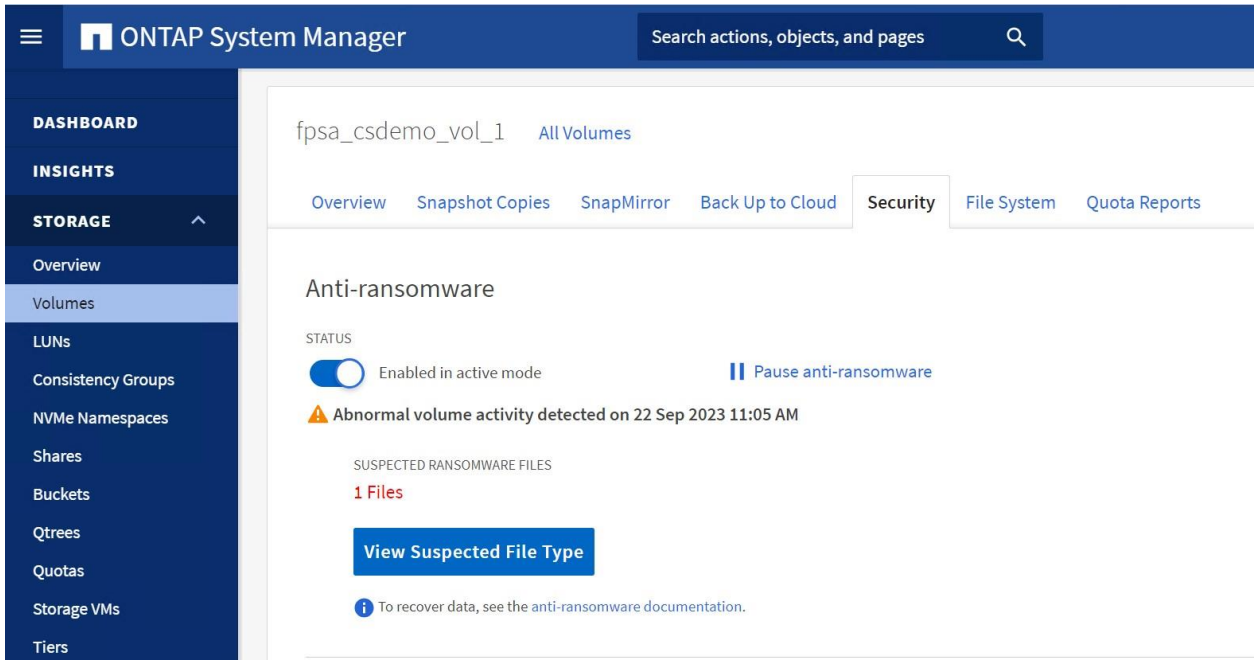
When Autonomous Ransomware Protection (ARP) is running in learning mode, it develops baseline values for file entropy, file extensions and IOPs for the specific ARP enabled volume. Entropy is an evaluation of the randomness of data in a file by ONTAP for use in determining suspicious file manipulation. 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.

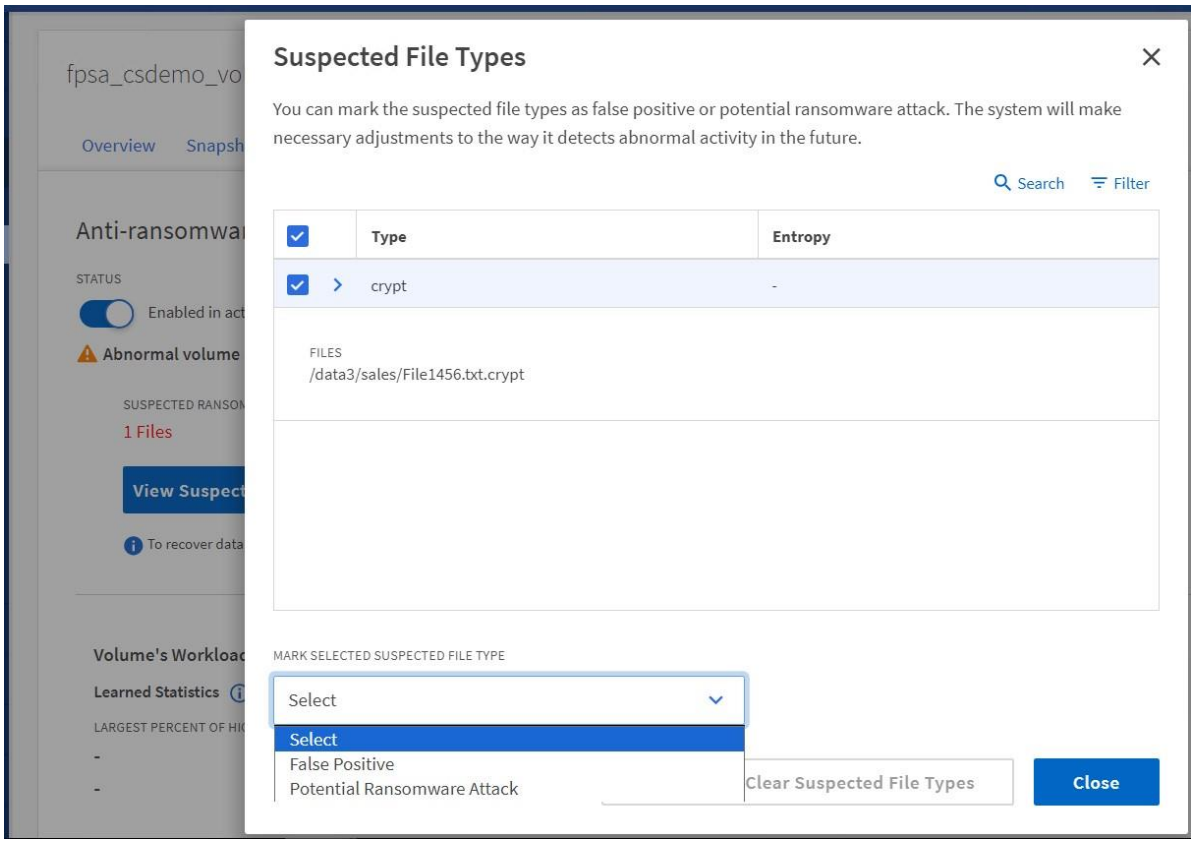
You can modify the attack detection parameters using "***security anti-ransomware volume attack-detection-parameters modify***" command. The following screenshot displays the default parameters that are enabled on ARP-enabled volume in the test environment. These parameters can be modified to suit the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



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.



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

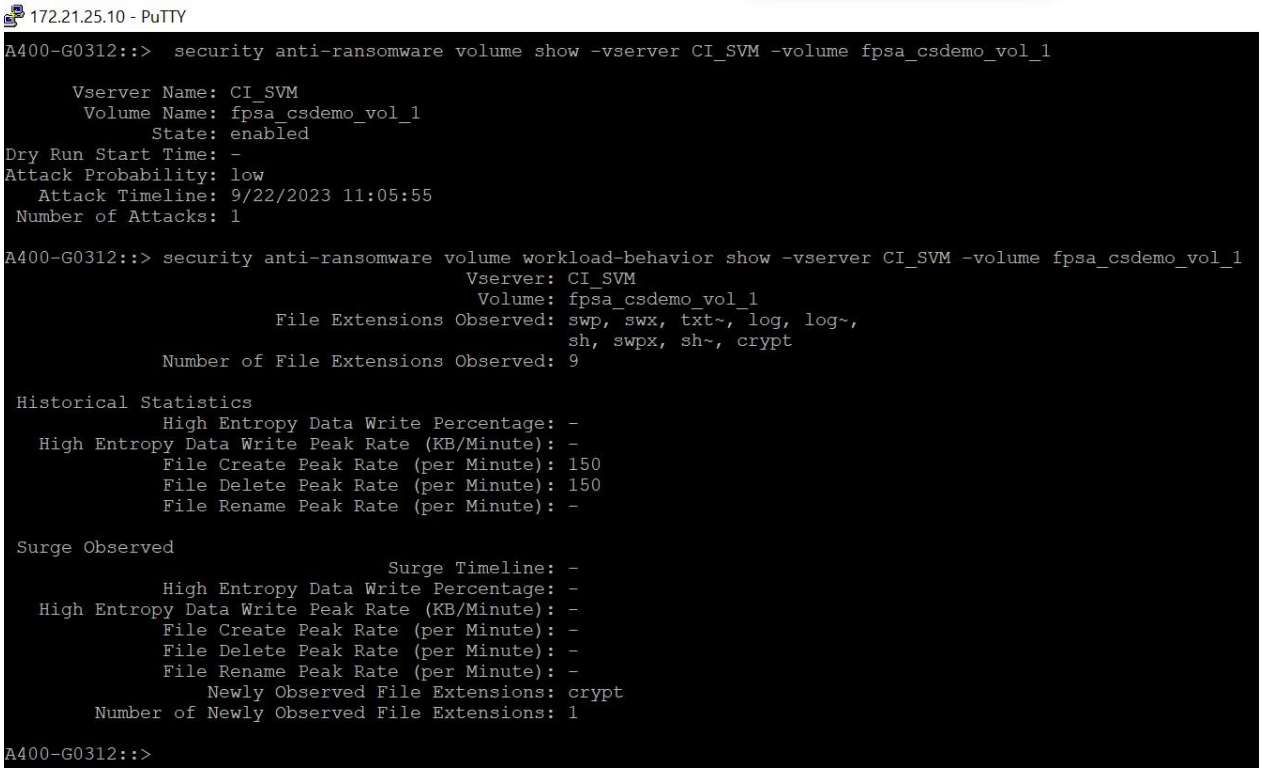
```
Cluster::> security anti-ransomware volume show -vserver <vserver name> -volume <volume name>
```

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

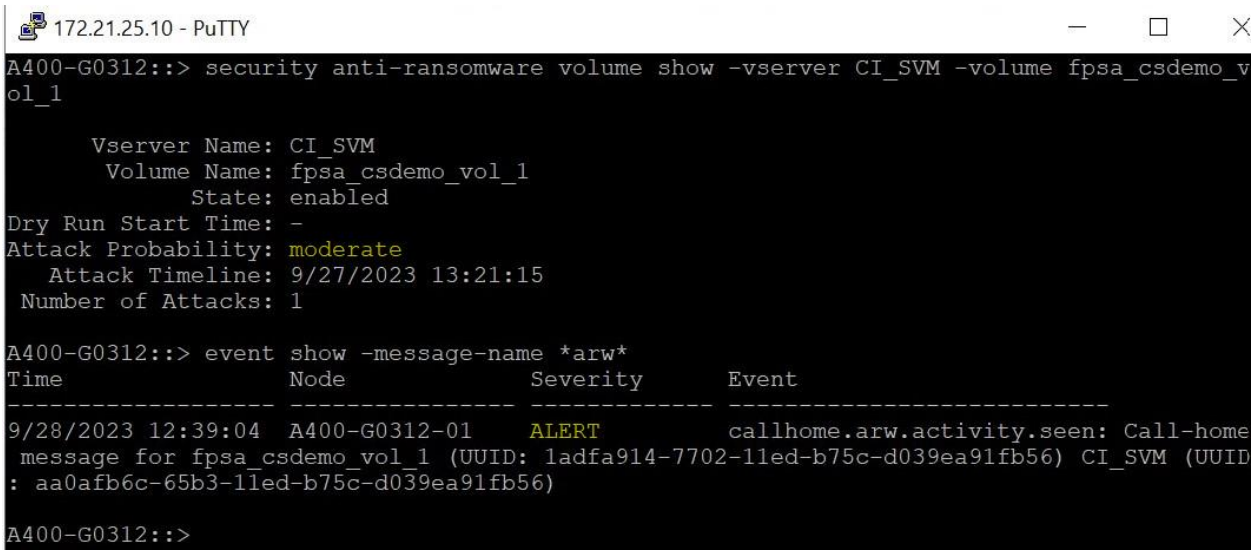
You may mark a suspected file type as false positive using the following command.

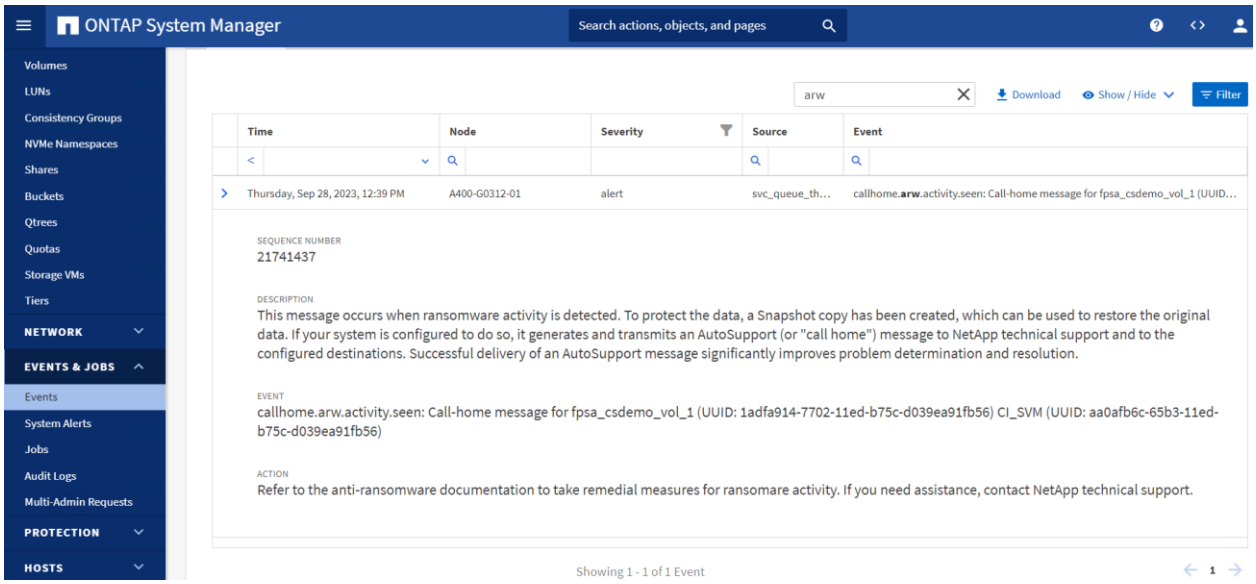
```
Cluster::> security anti-ransomware volume attack clear-suspect -vserver <vserver name> -volume <volume name> -extensions <extension name> -false-positive {true|false}
```

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



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.





Considerations and Limitations

1. ARP requires to function 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 switch from learning mode to active mode is done automatically. Note that Workload Security feature in Cloud Insights does not have a learning mode and is fully functional from day 1.
2. In the case where an SVM is not monitored by Workload Security, but there are ARP events generated by ONTAP, the events will still be received by Cloud Insights. However, Forensic information related to the alert, as well as user mapping, will not be captured or shown.
3. If you plan to use ARP in a VMDK on NFS configuration, there are limitations to ARP's protection. ARP and FPolicy can protect VMs on NFS from encryption at the VMDK level. If you have workloads with high-entropy files inside the VM, ARP is not recommended.
4. As of this writing, ARP is not supported on ONTAP S3 environments and SAN 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.

Case study

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

Accidental file deletion

Problem statement

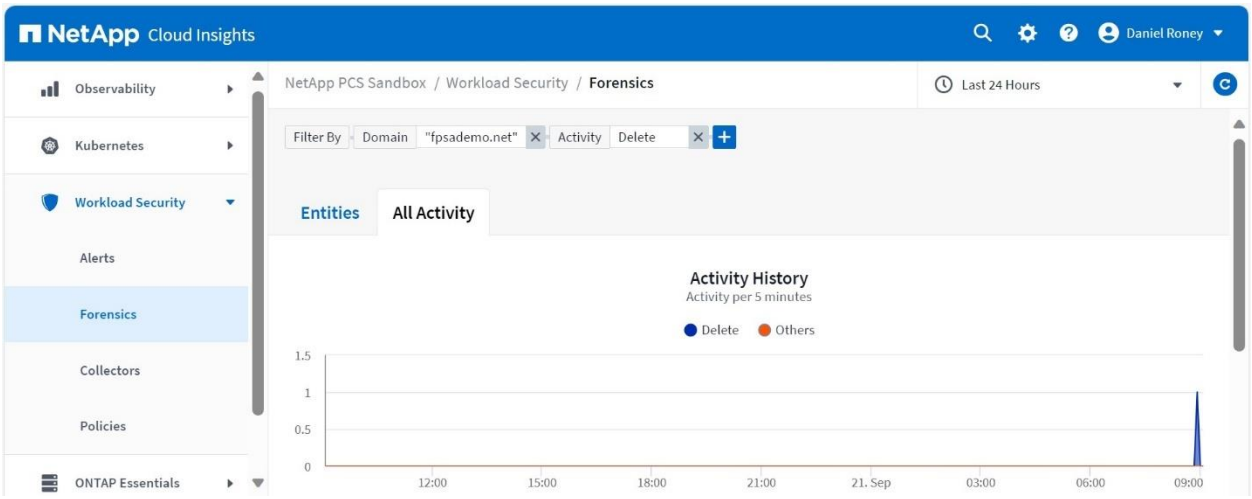
A user reported that “sales-data-Jan2023.docx” that he accessed the previous day is missing from an SMB share.

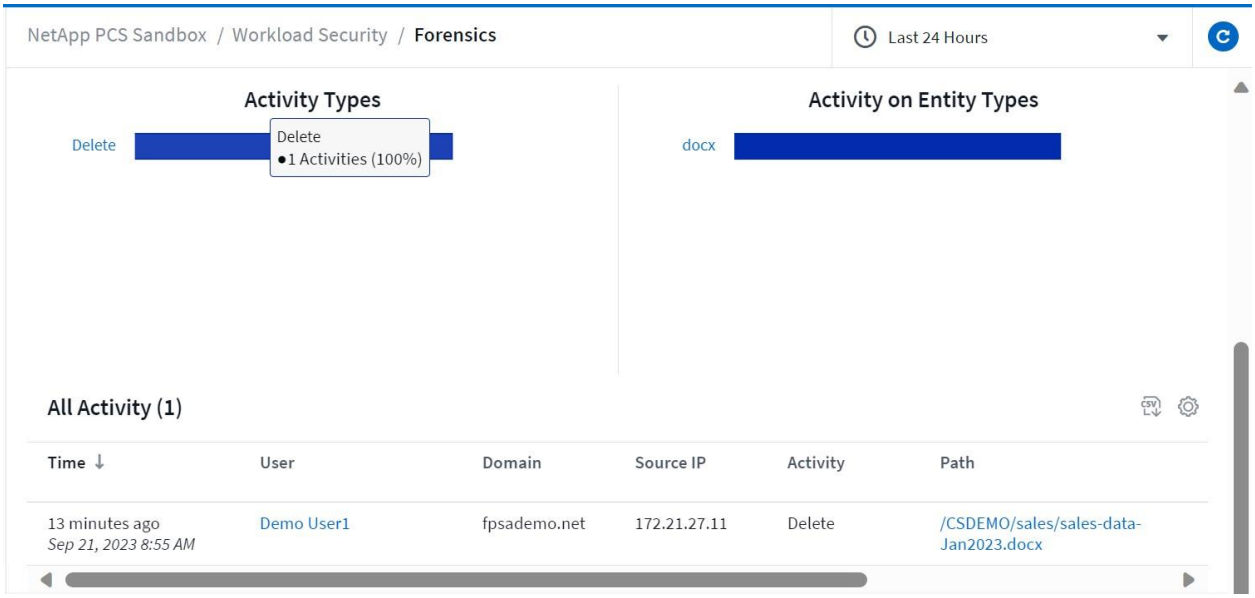
Analysis

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 24 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.

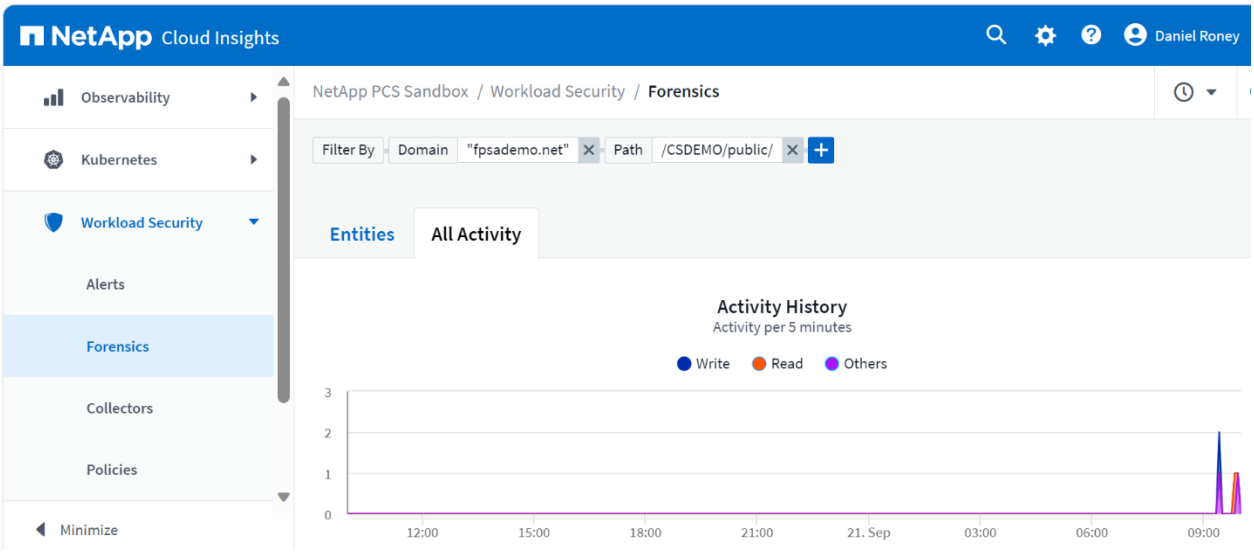
Problem statement

A HR employee has copied an offer letter to a public folder accidentally. The employee realized this mistake in 30 minutes and deleted the file, however he was not sure if someone else had copied or opened this file.

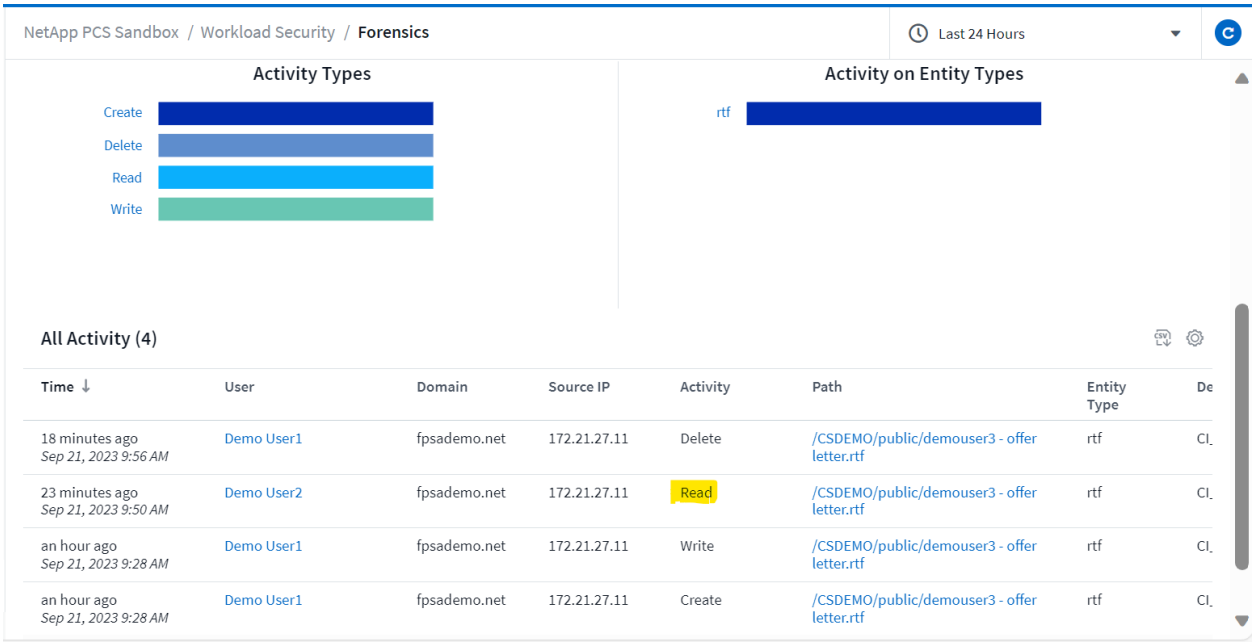
Analysis

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** has deleted the file from public folder. Workload Security tracked all file activities on the file that was deleted, 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.

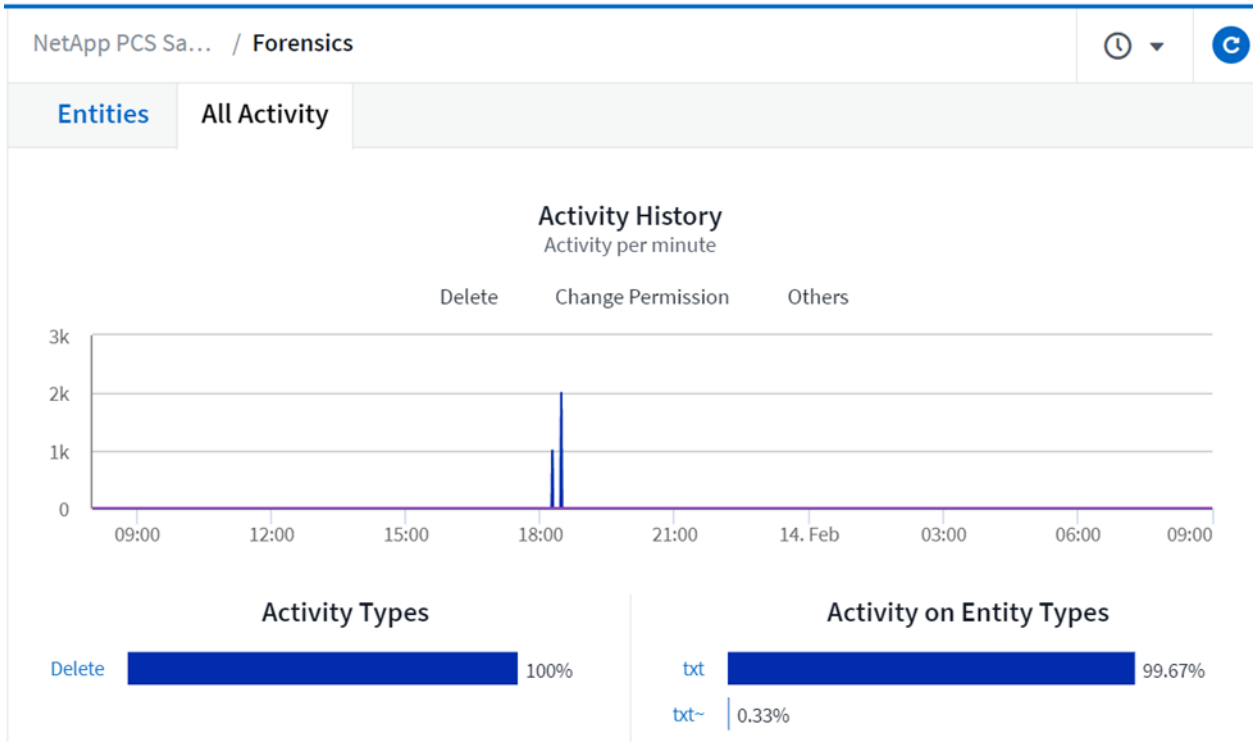
Bulk file deletion

Problem statement

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

Analysis

Cloud 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.



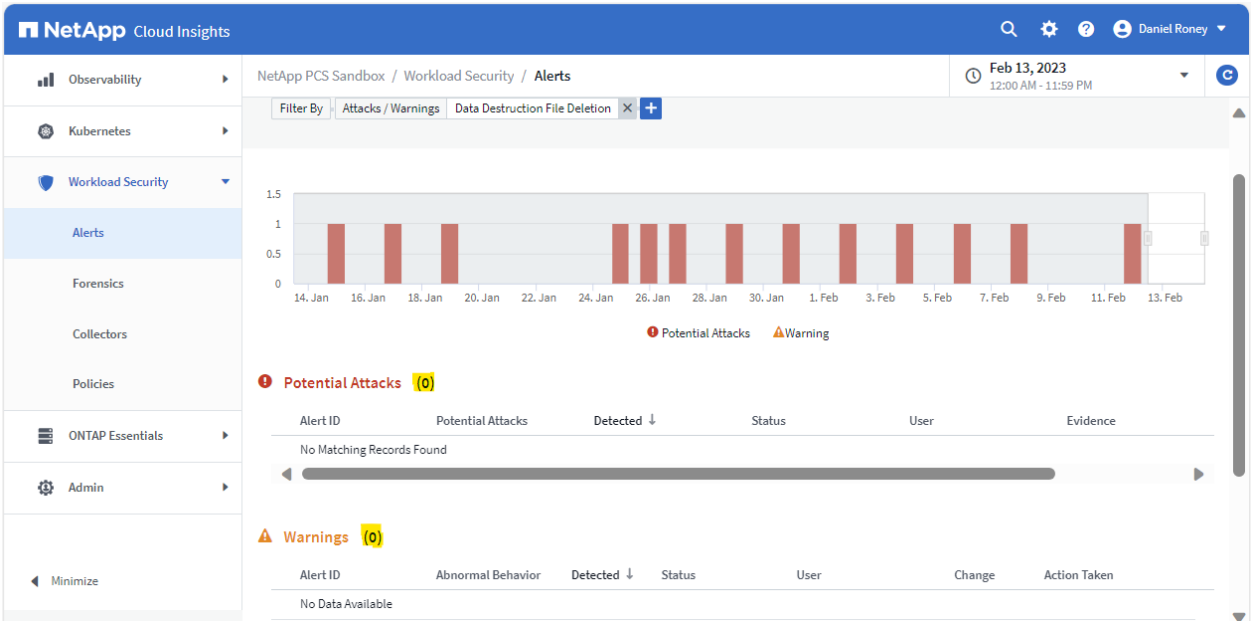
In this example, there were 2 bulk file deletion activities during that time, that involves over 3000 text files.

All Activity (3,015)

Time ↓	User	Domain	Source IP	Activity	Path	Entity Type	Device
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File2000.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1998.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1997.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1996.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1995.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:28 PM*	testuser2		172.21.27.13	Delete	/fpsa_csdemo_vol_1/data2/hr/File1994.txt	txt	CI_SVM

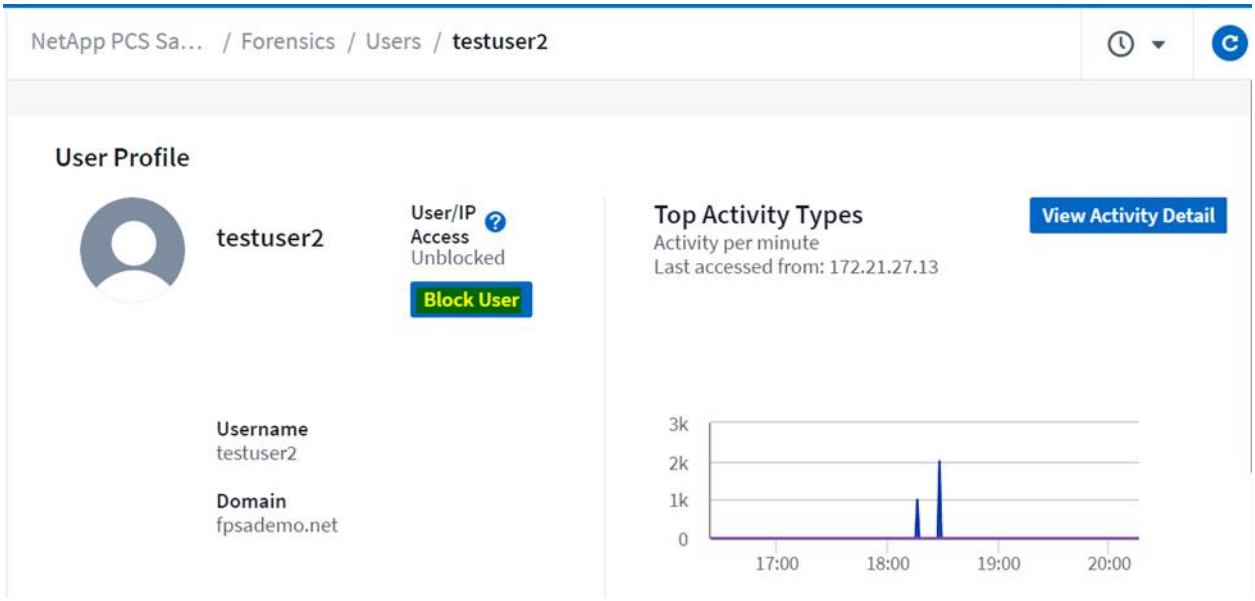
2 days ago *Feb 13, 2023 6:16 PM*	testuser2	172.21.27.13	Delete	/fpsa_csdemo_vol_1/data/File1524.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:16 PM*	testuser2	172.21.27.13	Delete	/fpsa_csdemo_vol_1/data/File1522.txt	txt	CI_SVM
2 days ago *Feb 13, 2023 6:16 PM*	testuser2	172.21.27.13	Delete	/fpsa_csdemo_vol_1/data/File1523.txt	txt	CI_SVM

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 Cloud Insights administrator can block this 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 "**testuser2**". Note that the administrator can block the user by clicking on **Block User** button.



Takeaway

Using Workload Security, the Cloud Insights administrator could provide the details of the bulk file deletion activity that affected over 3000 files in two folders. The Cloud 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, Cloud Insights does not require any training and is effective from day 1.

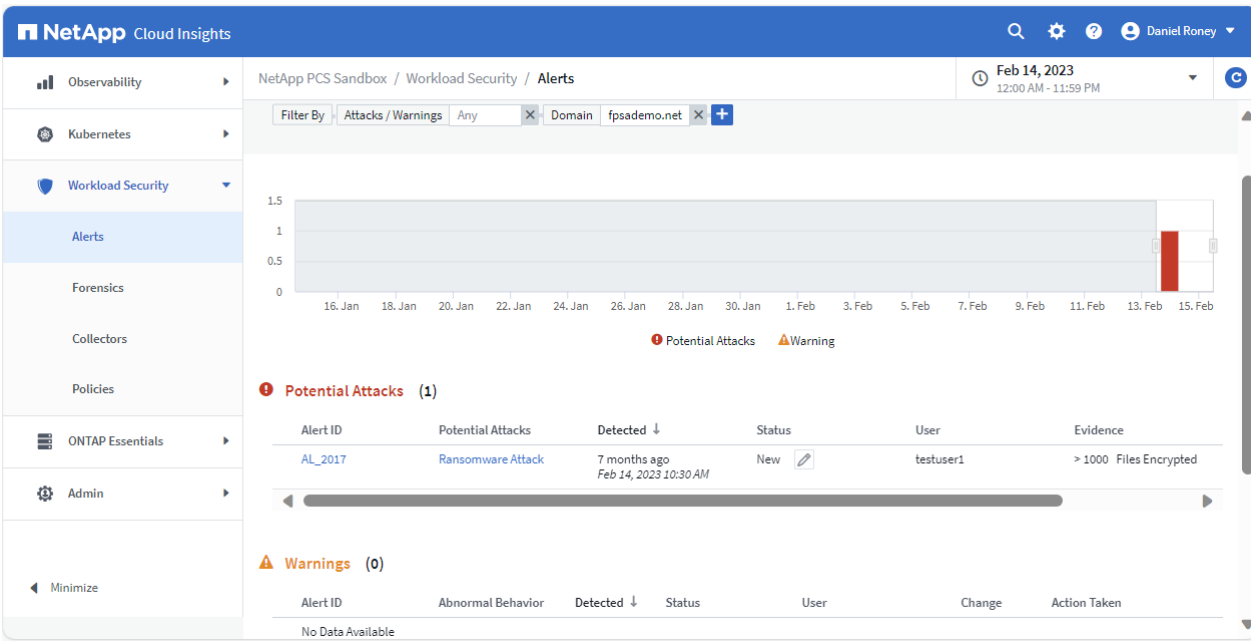
Ransomware attack simulation via Bulk File Encryption

Problem statement

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

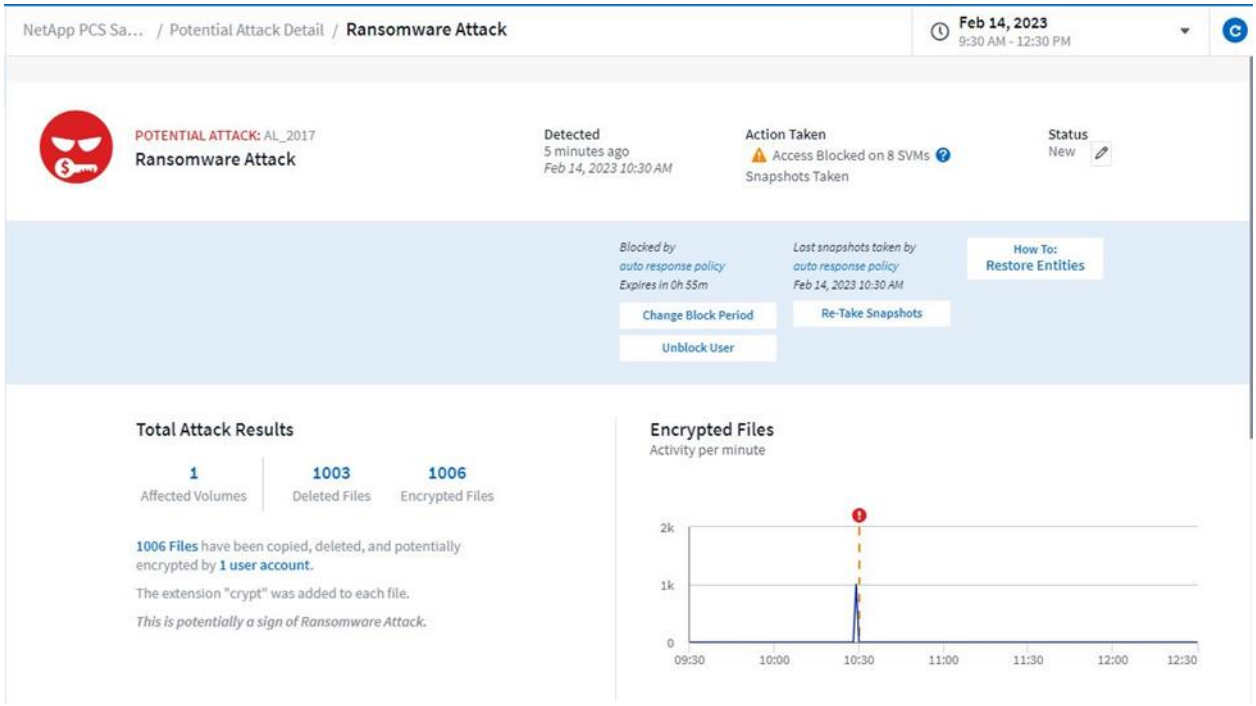
Analysis

Cloud Insights is launched to check on the alert. It reports that more than 1000 files are encrypted by **testuser1.**



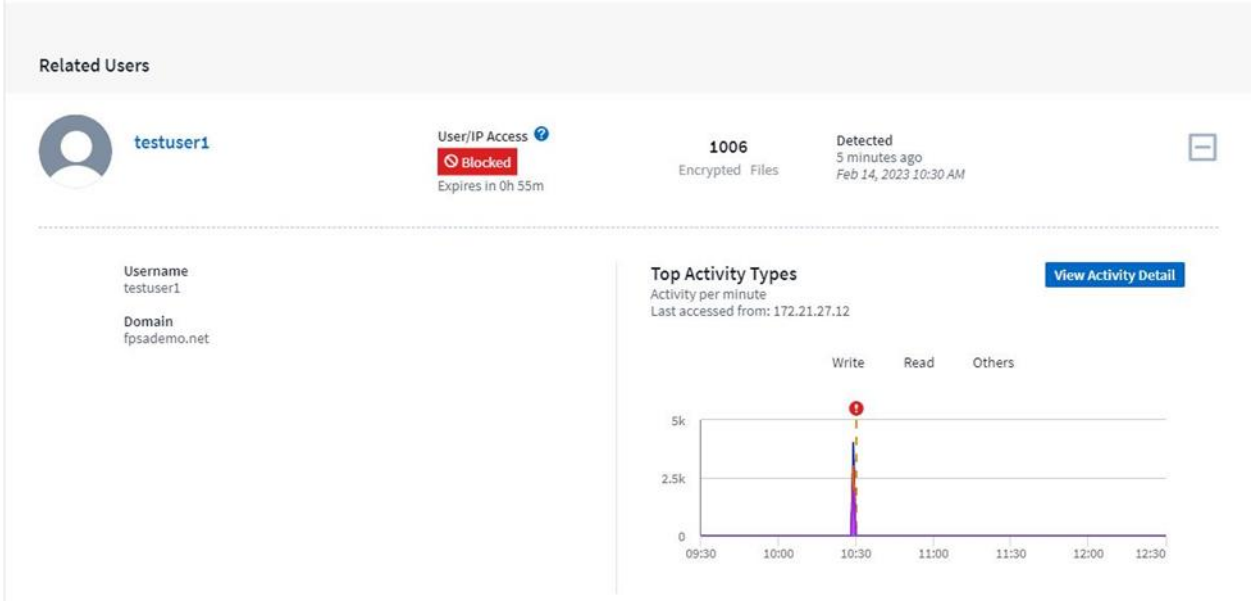
.

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. A Snapshot copy is also taken. 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.



Log in to the Linux host as testuser1 and try to access the NFS share. In this example access is denied for testuser1.

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 Cloud 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.

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 patch 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 Volume Snapshot restore feature of ONTAP as well as NetApp's SnapCenter® plug-ins that 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.

ONTAP Volume Snapshot Restore

In the ransomware attack simulation use case discussed earlier, we have seen that the auto response policy of Cloud Insight's Workload Security feature had triggered a volume snapshot as soon as the attack was detected. Although this snapshot may contain few encrypted files, it may be useful to restore the volume to a point in time as close to the attack with minimum encrypted files. Note that customers with core ONTAP could also get ransomware detection, alerting and snapshot capabilities through Autonomous Ransomware Protection (ARP). Unlike Cloud Insights, ARP does not provide forensics capabilities natively however, integrating it with Cloud Insights adds additional layer of forensics capabilities, user mapping and analytics data retention up to 13 months.

In the following screenshot, we see the affected device, 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_**" tag.

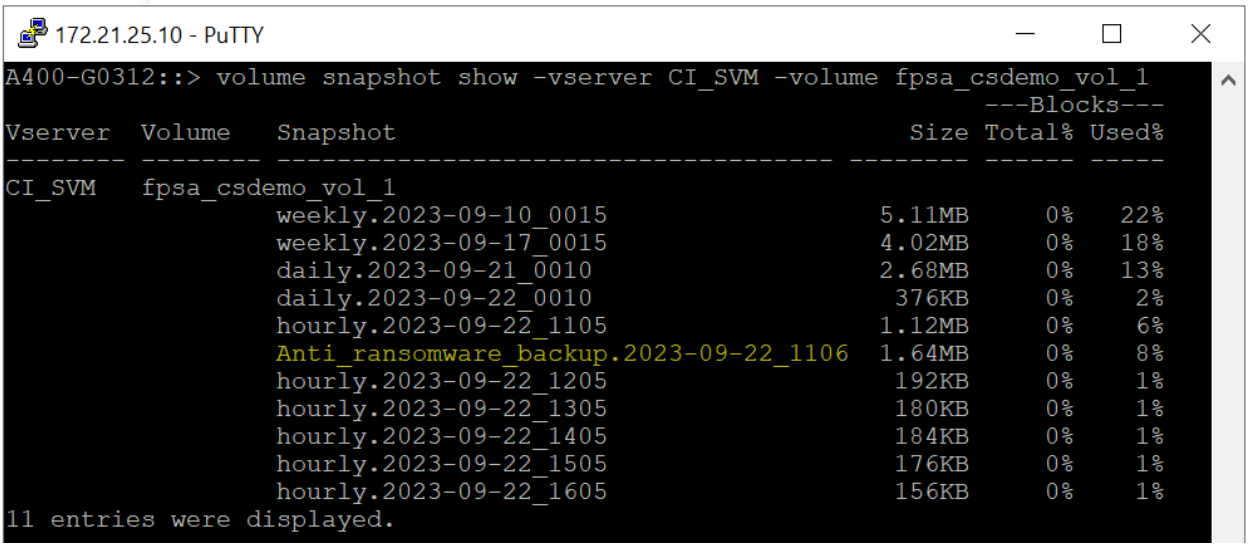
You may restore the volume to a snapshot using the following command.

```
Cluster::> volume snapshot restore -vserver <vserver name> -volume <volume name> -
snapshot <snapshot name>
```

```
A400-G0312::> volume snapshot restore -vserver CI_SVM -volume fpsa_csdemo_vol_1 -
snapshot cloudsecure_attack_auto_1676388648746
```

Note:

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.



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

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

SnapCenter Plug-in for VMware vSphere (SCV)

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 operations 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.

https://docs.netapp.com/us-en/sc-plugin-vmware-vsphere/scpivs44_deployment_workflow_for_new_users.html

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

https://docs.netapp.com/us-en/sc-plugin-vmware-vsphere/scpivs44_deployment_workflow_for_existing_users.html

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.

https://docs.netapp.com/us-en/sc-plugin-vmware-vsphere/scpivs44_download_the_ova_open_virtual_appliance.html

2. Deploy SnapCenter Plug-in for VMware vSphere.

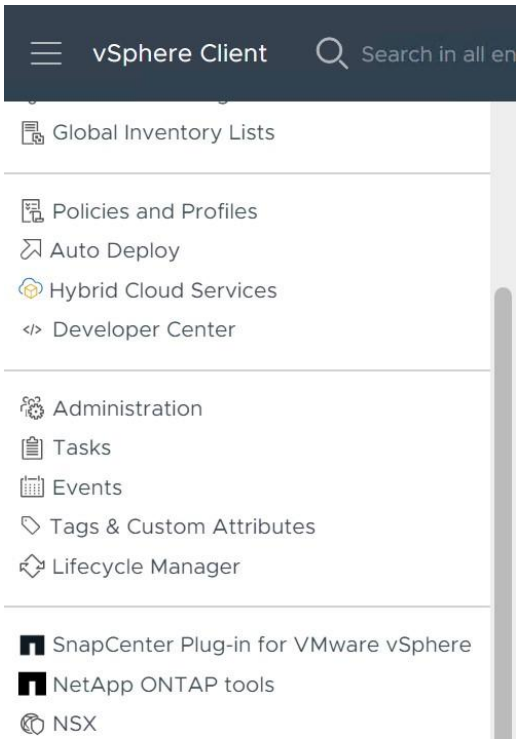
To use SnapCenter features to protect VMs, datastores, and application-consistent databases on virtualized machines, you must deploy SnapCenter Plug-in for VMware vSphere. SCV 4.9 is deployed in the validated environment. Refer to the following procedure for more details.

https://docs.netapp.com/us-en/sc-plugin-vmware-vsphere/scpivs44_deploy_snapcenter_plug-in_for_vmware_vsphere.html

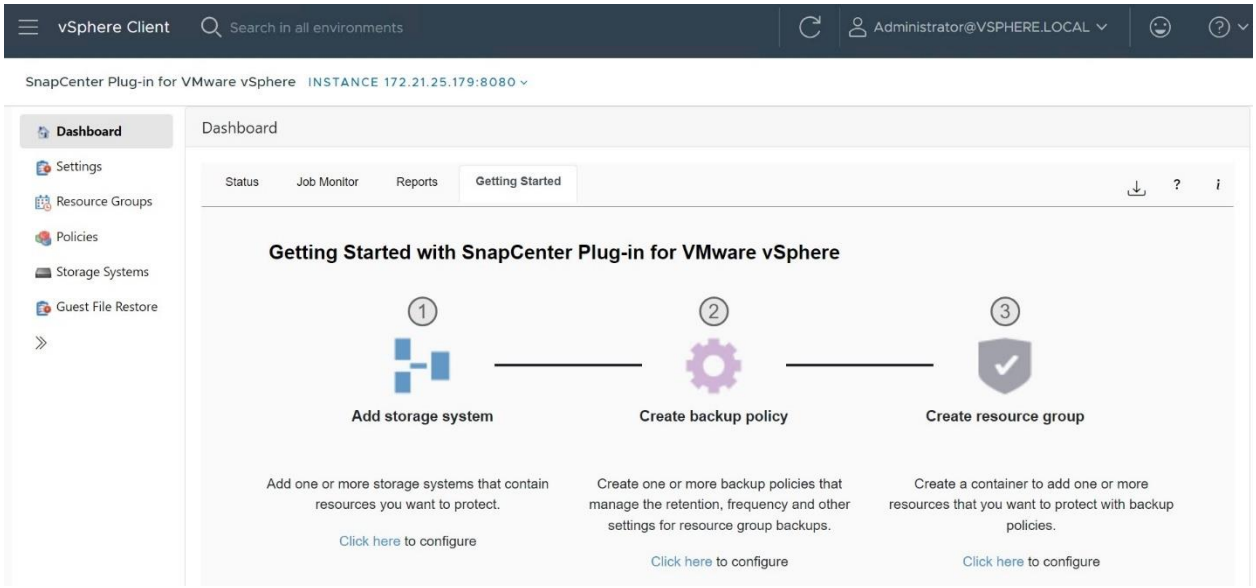
Backing up VMs and datastores

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.



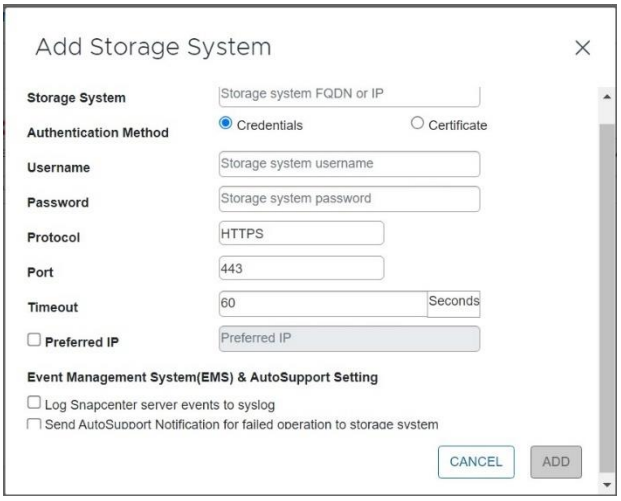
When SCV plug-in is opened, click on **Dashboard** on the left pane and select **Getting Started** tab on the right pane. This tab lists the steps to configure SCV plug-in for backing up VMs and datastores. You can click on the hyperlink under each step to open the wizard for the respective step. Alternatively, 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.



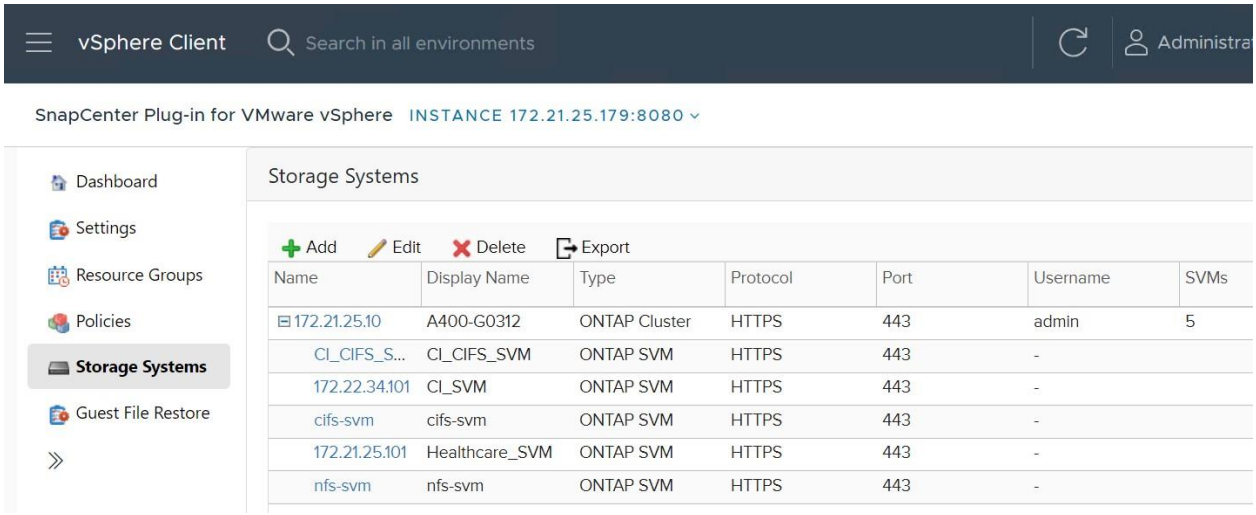
1. Add storage clusters and storage VMs.

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.



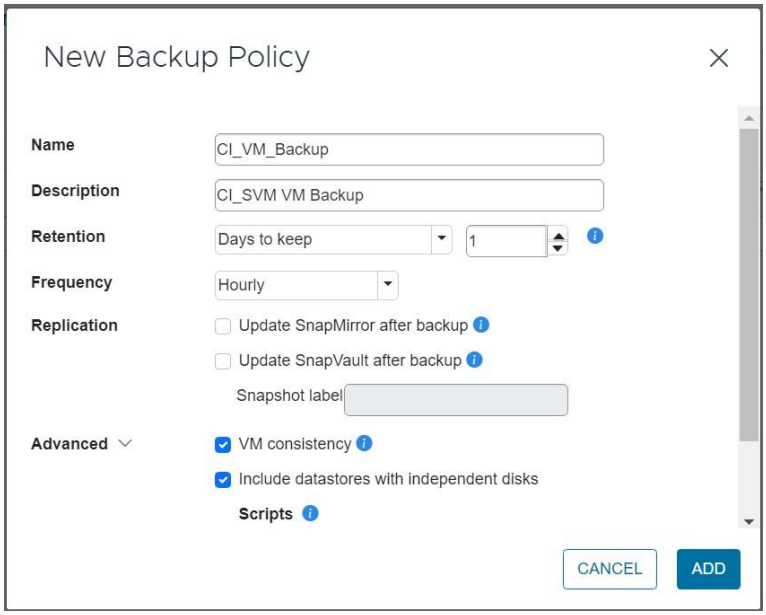
The following screenshot shows a storage cluster and SVMs that are added.



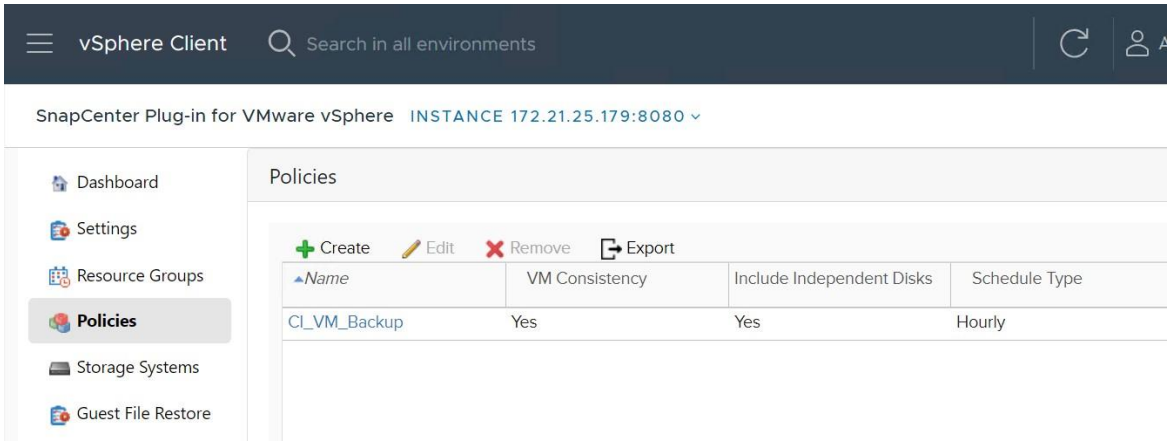
2. Create backup policies

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.

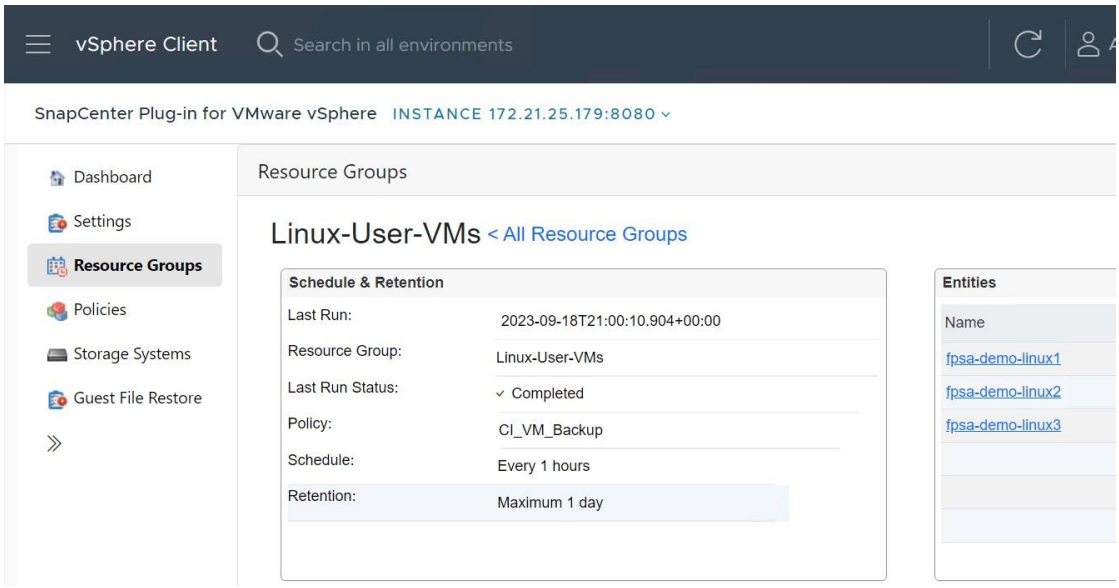


3. Create resource groups

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.

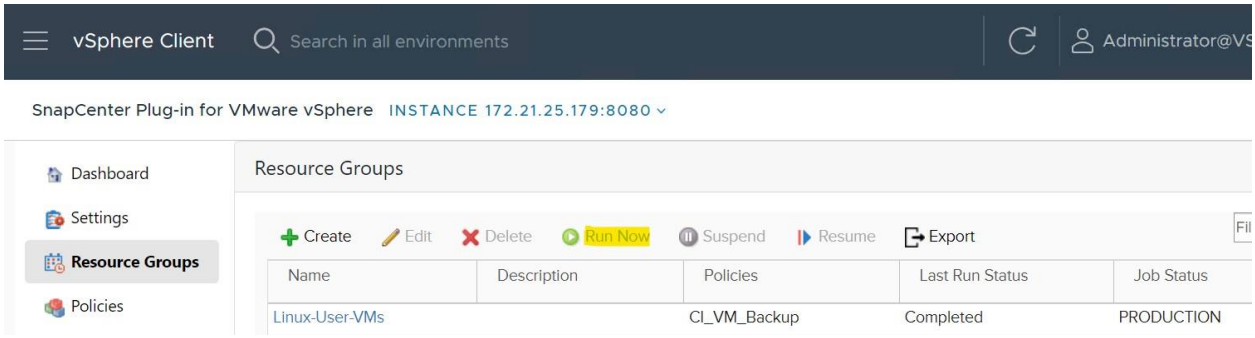
In this example, a resource group is created to backup 3 Linux VMs.



4. Performing Backup

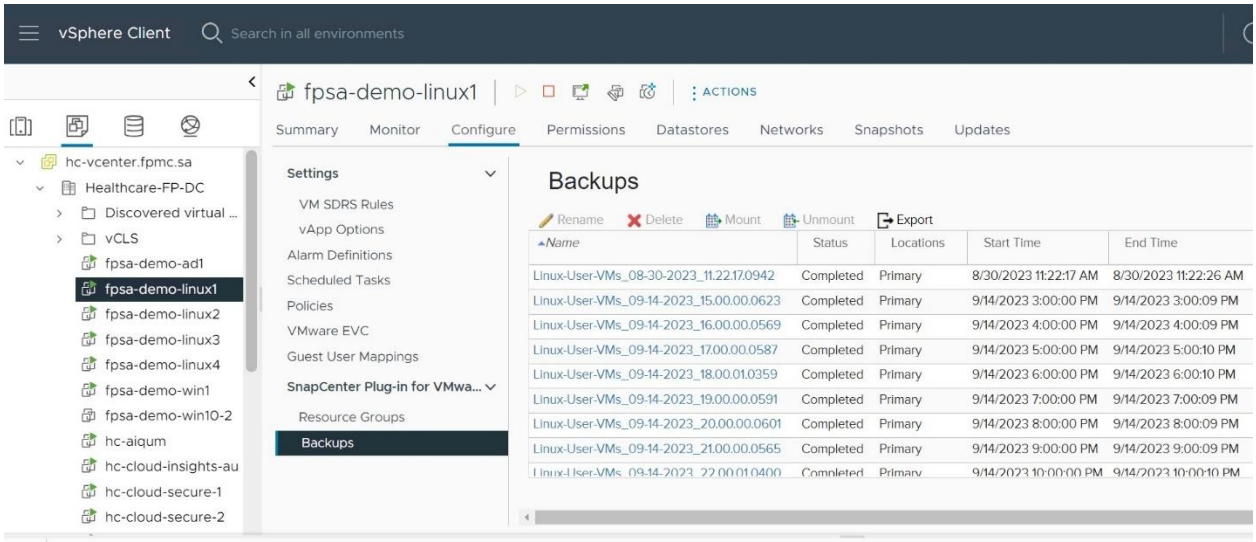
Backups are performed as specified in the backup policies that are configured for the resource group.

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



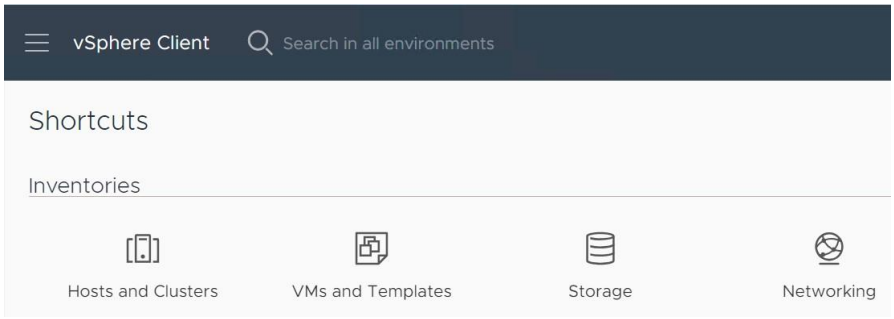
5. Viewing backups of a VM

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.

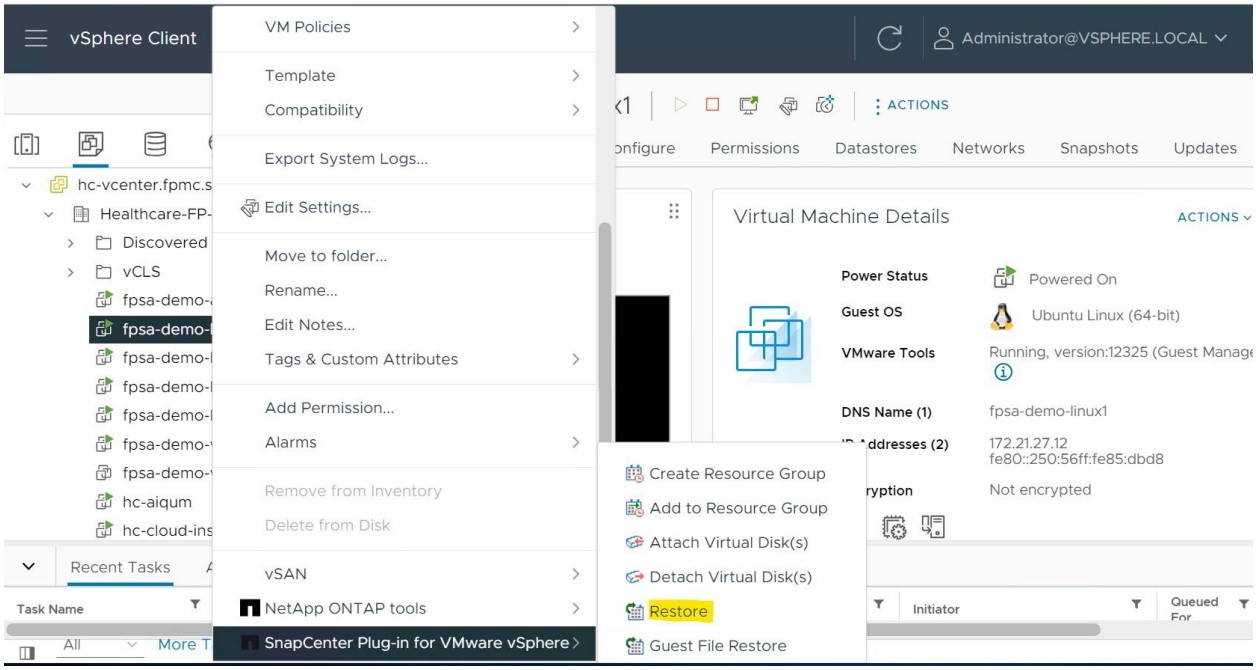


Restoring VMs from backup

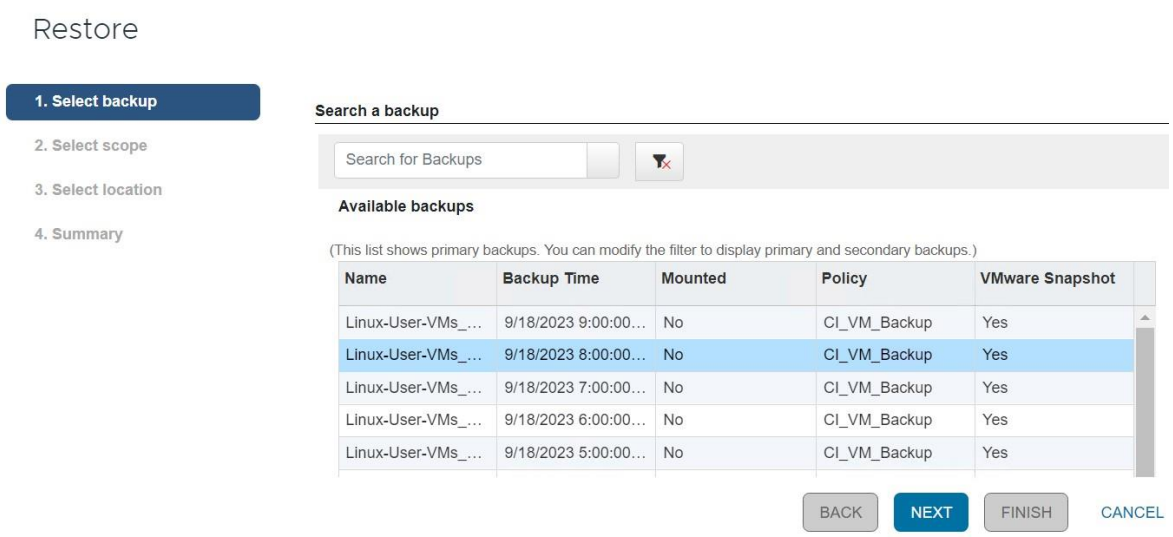
In the VMware vSphere client GUI, click Menu button on the top left corner and select shortcuts, and then select VMs and Templates from the inventory list.



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.



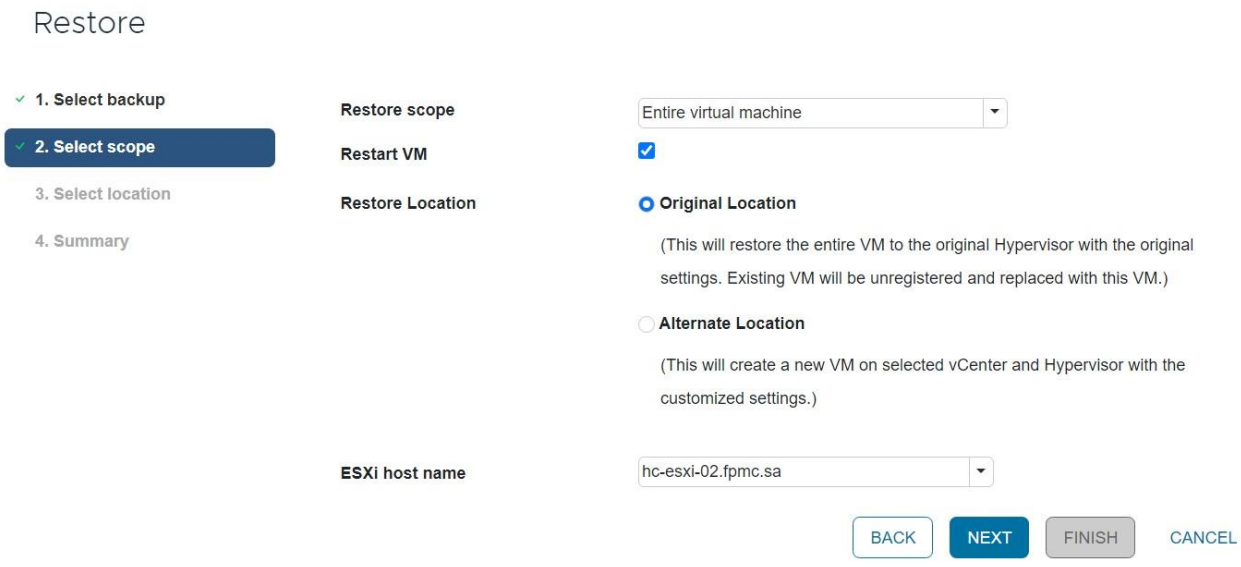
In the **Restore** wizard, on the **Select Backup** page, select the backup Snapshot copy that you want to restore from and click NEXT.



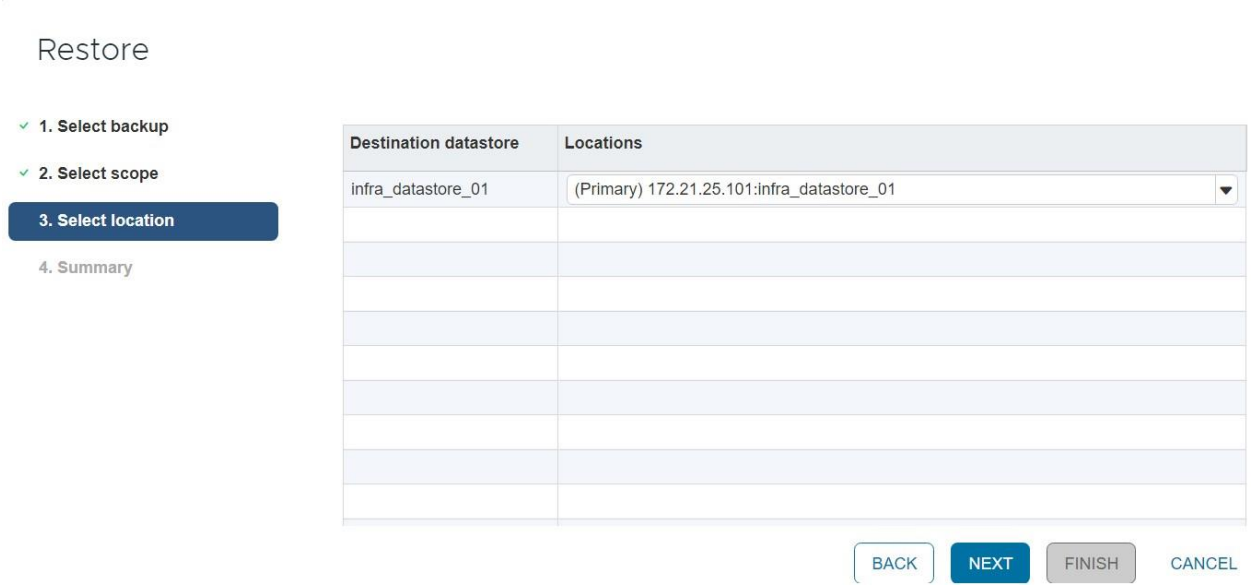
On the **Select Scope** page, select Entire virtual machine in the Restore scope field, then select the restore location, and then enter the destination information where the backup should be mounted. You may choose to restart the VM by clicking the check box.

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

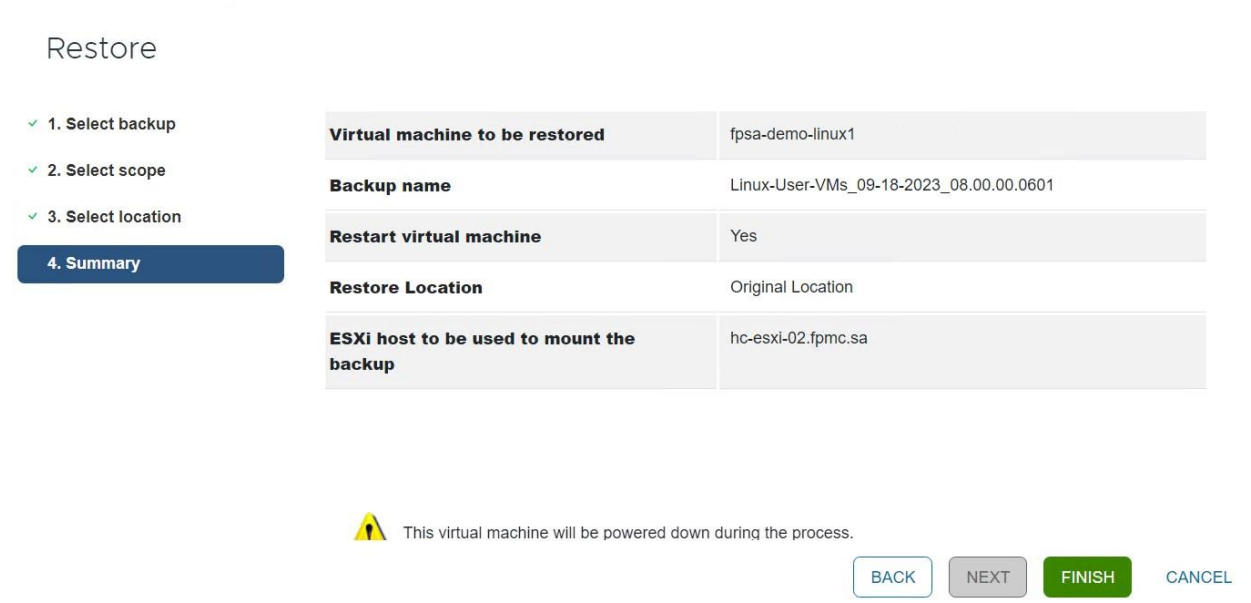
In this example, **Original Location** is chosen as restore location.



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.

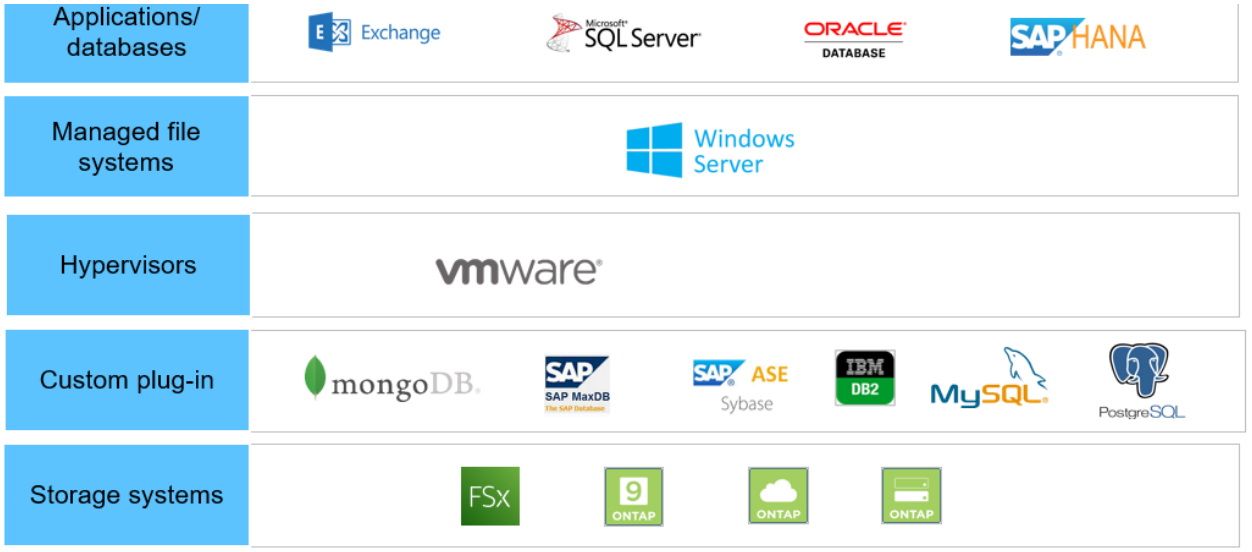
SnapCenter Plugins for application consistent backup and recovery

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 5).

Figure 5) 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

SnapCenter Plug-In for Microsoft SQL Server is part of the SnapCenter centralized multi-application/database framework for Snapshot data management and protection. It is comparable in functionality to the SnapManager® for Microsoft SQL Server product however the SnapCenter Plug-In has been completely rewritten to improve performance and scalability. SnapCenter supports Microsoft SQL Server version from 2012 to 2022. The SnapCenter Plug-In for Microsoft SQL Server license is part of the SnapCenter Standard license, so no additional license is required.

For information on SnapCenter SQL plug-in configuration and SQL database backup and restore, refer to the following CVD.

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_sql2022_xseries.html

Conclusion

As attackers find newer ways to generate and spread ransomware, newer techniques must be developed and adopted for ransomware detection and removal. The Workload Security feature of Cloud 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 Cloud 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.

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 Cloud 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.

Acknowledgement

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

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

Where to find additional information

- NetApp Cloud Insights Documentation
  https://docs.netapp.com/us-en/cloudinsights/index.html
- 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/
- TR-4802: FlexPod, The Solution to Ransomware
  https://docs.netapp.com/us-en/flexpod/security/security-ransomware_what_is_ransomware.html#how-does-ransomware-work
- TR-4868: NetApp Cloud Insights for FlexPod
  https://docs.netapp.com/us-en/flexpod/hybrid-cloud/cloud-insights_netapp_cloud_insights_for_flexpod.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	March 2023	Initial version.
Version 2.0	Sept 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.

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.

Copyright information

Trademark information

NetApp