Storage Workload Security

Cloud Insights

NetApp
March 09, 2023

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/cs_intro.html on March 09, 2023. Always check docs.netapp.com for the latest.

Table of Contents

Storage Workload Security . . . 1
- About Storage Workload Security . . . 1
- Getting Started . . . 1
- Alerts . . . 37
- Forensics . . . 43
- Automated Response Policies . . . 50
- Integration with ONTAP Autonomous Ransomware Protection . . . 52
- Blocking User Access . . . 54
- Workload Security: Simulating an Attack . . . 59
- Configuring Email Notifications for Alerts, Warnings, and Agent/Data Source Collector health . . . 63
- Workload Security API . . . 63

Storage Workload Security

About Storage Workload Security

Cloud Insights Storage Workload Security (formerly Cloud Secure) helps protect your data with actionable intelligence on insider threats. It provides centralized visibility and control of all corporate data access across hybrid cloud environments to ensure security and compliance goals are met.

Visibility

Gain centralized visibility and control of user access to your critical corporate data stored on-premise or in the cloud.

Replace tools and manual processes that fail to provide timely and accurate visibility into data access and control. Workload Security uniquely operates on both cloud and on-premise storage systems to give you real-time alerts of malicious user behavior.

Protection

Protect organizational data from being misused by malicious or compromised users through advanced machine learning and anomaly detection.

Alerts you to any abnormal data access through advanced machine learning and anomaly detection of user behavior.

Compliance

Ensure corporate compliance by auditing user data access to your critical corporate data stored on-premise or in the cloud.

Getting Started

Getting Started with Workload Security

There are configuration tasks that need to be completed before you can start using Workload Security to monitor user activity.

The Workload Security system uses an agent to collect access data from storage systems and user information from Directory Services servers.

You need to configure the following before you can start collecting data:

Task	Related information

Configure an Agent	Agent Requirements Add Agent **Video**: Agent Deployment
Configure a User Directory Connector	Add User Directory Connector **Video**: Active Directory Connection
Configure data collectors	Click **Admin > Data Collectors** Click the data collector you want to configure. See the Data Collector Vendor Reference section of the documentation. **Video**: ONTAP SVM Connection
Create Users Accounts	Manage User Accounts
Troubleshooting	**Video**: Troubleshooting

Workload Security can integrate with other tools as well. For example, see this guide on integration with Splunk.

Workload Security Agent Requirements

You must install an Agent in order to acquire information from your data collectors. Before you install the Agent, you should ensure that your environment meets operating system, CPU, memory, and disk space requirements.

Component	Linux Requirement
Operating system	A computer running a licensed version of one of the following: Red Hat Enterprise Linux 7.x, 8.x 64-bit CentOS 7.x 64-bit CentOS 8 Stream Ubuntu 20 through 22 64-bit Rocky 8.x 64-bit, Rocky 9.x 64-bit This computer should be running no other application-level software. A dedicated server is recommended. SE (Security Enhanced) Linux is not supported.
Commands	'unzip' is required for installation. Additionally, the 'sudo su –' command is required for installation, running scripts, and uninstall.
CPU	4 CPU cores
Memory	16 GB RAM

Component	Linux Requirement
Available disk space	Disk space should be allocated in this manner: /opt/netapp 35 GB (minimum) If /opt is a mounted folder from a NAS storage, make sure that local users have access to this folder. Agent or Data collector may fail to install if local users do not have permission to this folder. see the troubleshooting section for more details.
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).

Please note: The Workload Security agent can be installed in the same machine as a Cloud Insights acquisition unit and/or agent. However, it is a best practice to install these in separate machines. In the event that these are installed on the same machine, please allocate disk space as shown below:

Available disk space	50-55 GB For Linux, disk space should be allocated in this manner: /opt/netapp 25-30 GB /var/log/netapp 25 GB

Additional recommendations

- 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)**.

Cloud Network Access Rules

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

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

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 rules

Note that when adding *csuser*, that user requires SSH access to the ONTAP management LIF.

Protocol	Port	Destination	Direction	Description
TCP	389(LDAP) 636 (LDAPs / start-tls)	LDAP Server URL	Outbound	Connect to LDAP

Protocol	Port	Destination	Direction	Description
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/Outbound	Communication with ONTAP for Fpolicy events
TCP	7	SVM data LIF IP Addresses	Bidirectional	Bidirectional between ONTAP and Workload Security. Agent pings the SVM Lifs.

System Sizing

See the Event Rate Checker documentation for information about sizing.

Workload Security Agent Installation

Workload Security (formerly Cloud Secure) collects user activity data using one or more agents. Agents connect to devices in your environment and collect data that is sent to the Workload Security SaaS layer for analysis. See Agent Requirements to configure an agent VM.

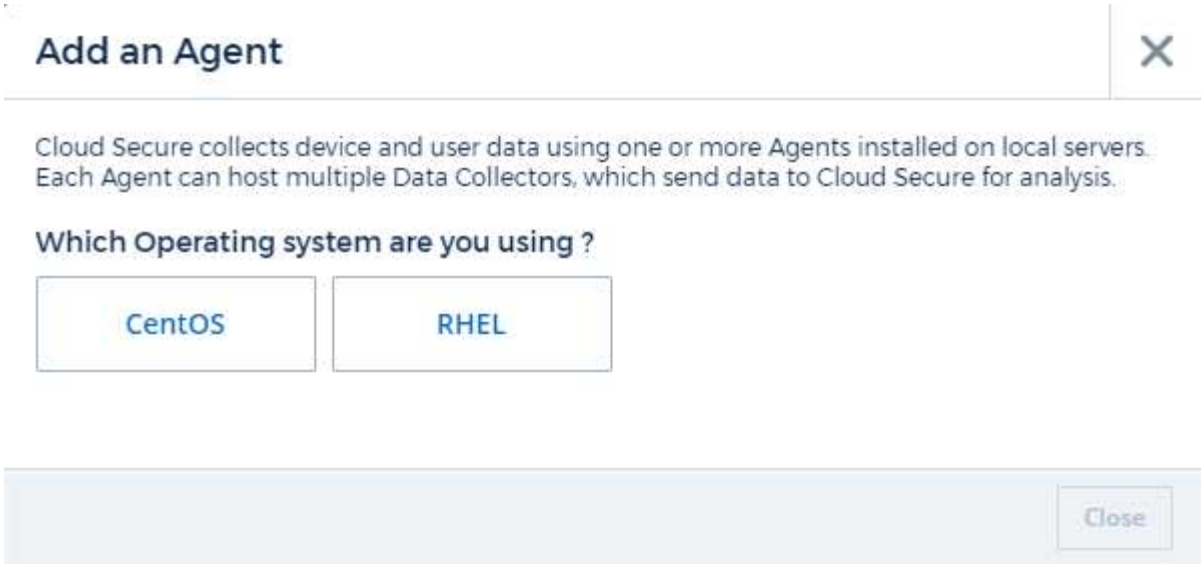
Before You Begin

- The sudo privilege is required for installation, running scripts, and uninstall.
- While installing the agent, a local user *cssys* and a local group *cssys* are created on the machine. If permission settings do not allow creation of a local user, and instead require Active Directory, a user with the username *cssys* must be created in the Active Directory server.

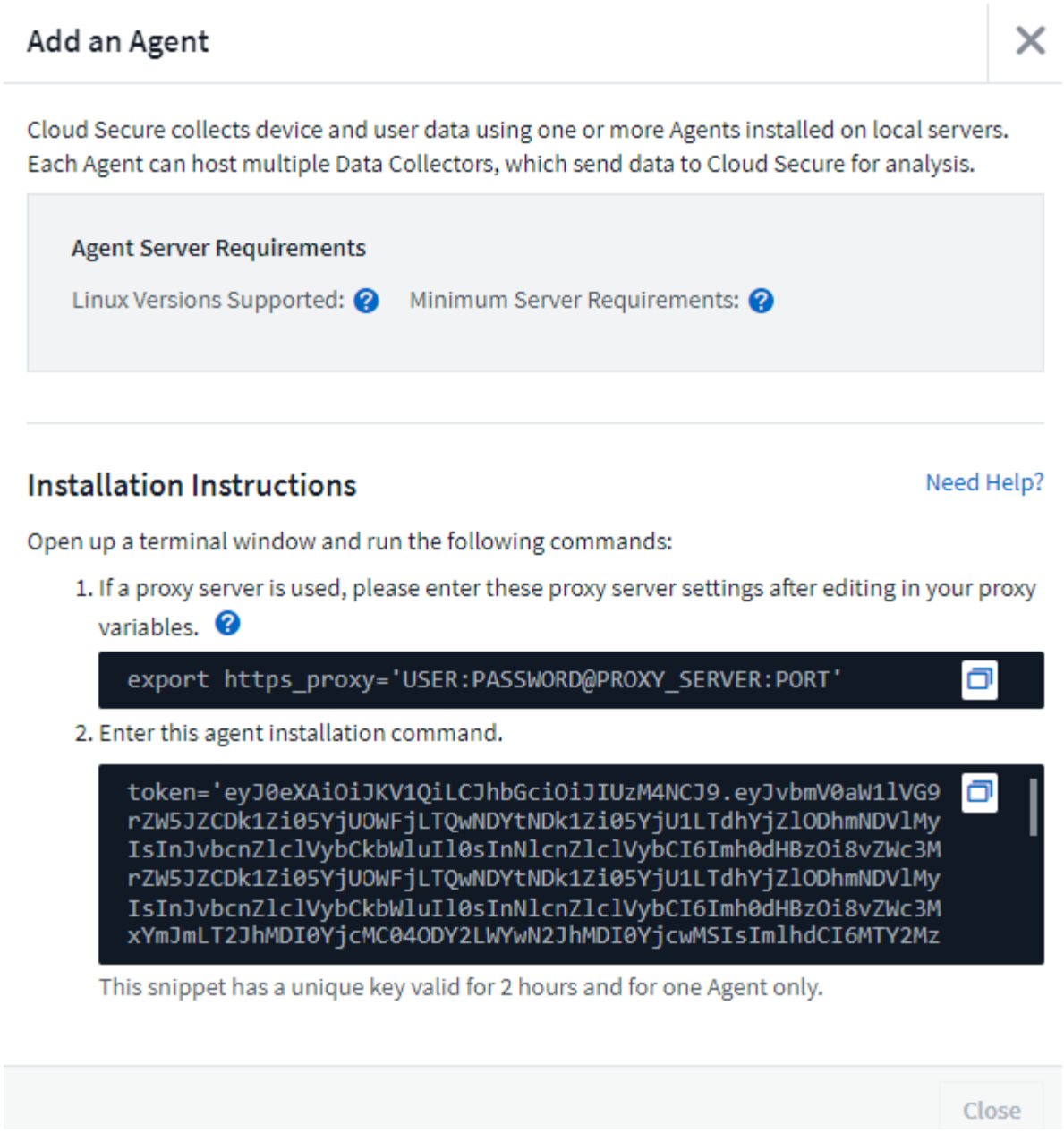
Steps to Install Agent

1. Log in as Administrator or Account Owner to your Workload Security environment.
2. Under the **Security** menu, select **Admin > Data Collectors > Agents > +Agent**

   The system displays the Add an Agent page:



3. Verify that the agent server meets the minimum system requirements.
4. To verify that the agent server is running a supported version of Linux, click *Versions Supported (i)*.
5. If your network is using proxy server, please set the proxy server details by following the instructions in the Proxy section.



6. Click the Copy to Clipboard icon to copy the installation command.
7. Run the installation command in a terminal window.
8. The system displays the following message when the installation completes successfully:

After You Finish

1. You need to configure a User Directory Collector .
2. You need to configure one or more Data Collectors.

Network Configuration

Run the following commands on the local system to open ports that will be used by Workload Security. If there is a security concern regarding the port range, you can use a lesser port range, for example *35000:35100*. Each SVM uses two ports.

Steps

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

Follow the next steps according to your platform:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Sample output:

```
-A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack -ctstate
NEW,UNTRACKED -j ACCEPT
```

CentOS 8.x / RHEL 8.x:

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000` (for CentOS 8)

Sample output:

```
35000-55000/tcp
```

Troubleshooting Agent Errors

Known problems and their resolutions are described in the following table.

Problem:	Resolution:
Agent installation fails to create the /opt/netapp/cloudsecure/agent/logs/agent.log folder and the install.log file provides no relevant information.	This error occurs during bootstrapping of the agent. The error is not logged in log files because it occurs before logger is initialized. The error is redirected to standard output, and is visible in the service log using the `journalctl -u cloudsecure-agent.service` command. This command can be used for troubleshooting the issue further.
Agent installation fails with 'This linux distribution is not supported. Exiting the installation'.	This error appears when you attempt to install the Agent on an unsupported system. See Agent Requirements.

Problem:	Resolution:
Agent Installation failed with the error: "-bash: unzip: command not found"	Install unzip and then run the installation command again. If Yum is installed on the machine, try “yum install unzip” to install unzip software. After that, re-copy the command from the Agent installation UI and paste it in the CLI to execute the installation again.

Agent was installed and was running. However agent has stopped suddenly.	SSH to the Agent machine. Check the status of the agent service via `sudo systemctl status cloudsecure-agent.service`.
	1. Check if the logs shows a message“Failed to start Workload Security daemon service” .
	2. Check if cssys user exists in the Agent machine or not. Execute the following commands one by one with root permission and check if the cssys user and group exists.
	`sudo id cssys`
	`sudo groups cssys`
	3. If none exists, then a centralized monitoring policy may have deleted the cssys user.
	4. Create cssys user and group manually by executing the following commands.
	`sudo useradd cssys`
	`sudo groupadd cssys`
	5. Restart the agent service after that by executing the following command:
	`sudo systemctl restart cloudsecure-agent.service`
	6. If it is still not running, please check the other troubleshooting options.

Unable to add more than 50 Data collectors to an Agent.	Only 50 Data collectors can be added to an Agent. This can be a combination of all the collector types, for example, Active Directory, SVM and other collectors.
UI shows Agent is in NOT_CONNECTED state.	Steps to restart the Agent. 1. SSH to the Agent machine. 2. Restart the agent service after that by executing the following command: `sudo systemctl restart cloudsecure-agent.service` 3. Check the status of the agent service via `sudo systemctl status cloudsecure-agent.service`. 4. Agent should go to CONNECTED state.
Agent VM is behind Zscaler proxy and the agent installation is failing. Because of Zscaler proxy’s SSL inspection, the Workload Security certificates are presented as it is signed by Zscaler CA so the agent is not trusting the communication.	Disable SSL inspection in the Zscaler proxy for the *.cloudinsights.netapp.com url. If Zscaler does SSL inspection and replaces the certificates, Workload Security will not work.

Problem:	Resolution:
While installing the agent, the installation hangs after unzipping.	“chmod 755 -Rf” command is failing. The command fails when the agent installation command is being run by a non-root sudo user that has files in the working directory, belonging to another user, and permissions of those files cannot be changed. Because of the failing chmod command, the rest of the installation does not execute. 1. Create a new directory named “cloudsecure”. 2. Go to that directory. 3. Copy and paste the full “token=…… … ./cloudsecure-agent-install.sh" installation command and press enter. 4. Installation should be able to proceed.
If the Agent is still not able to connect to Saas, please open a case with NetApp Support. Provide the Cloud Insights serial number to open a case, and attach logs to the case as noted.	To attach logs to the case: 1. Execute the following script with root permission and share the output file (cloudsecure-agent-symptoms.zip). a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Execute the following commands one by one with root permission and share the output. a. id cssys b. groups cssys c. cat /etc/os-release
The cloudsecure-agent-symptom-collector.sh script fails with the following error. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Collecting service log Collecting application logs Collecting agent configurations Taking service status snapshot Taking agent directory structure snapshot ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: line 52: zip: command not found ERROR: Failed to create /tmp/cloudsecure-agent-symptoms.zip	Zip tool is not installed.. Install the zip tool by running the command “yum install zip”. Then run the cloudsecure-agent-symptom-collector.sh again.

Problem:	Resolution:
Agent installation Fails with useradd: cannot create directory /home/cssys	This error can occur if user's login directory cannot be created under /home, due to lack of permissions. The workaround would be to create cssys user and add its login directory manually using the following command: *sudo useradd user_name -m -d HOME_DIR* -m :Create the user's home directory if it does not exist. -d : The new user is created using HOME_DIR as the value for the user's login directory. For instance, *sudo useradd cssys -m -d /cssys*, adds a user *cssys* and creates its login directory under root.
Agent is not running after installation. *Systemctl status cloudsecure-agent.service* shows the following: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: disabled) Active: activating (auto-restart) (Result: exit-code) since Tue 2021-08-03 21:12:26 PDT; 2s ago Process: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (code=exited status=126) Main PID: 25889 (code=exited, status=126), Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service: main process exited, code=exited, status=126/n/a Aug 03 21:12:26 demo systemd[1]: Unit cloudsecure-agent.service entered failed state. Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service failed.	This can be failing because *cssys* user may not have permission to install. If /opt/netapp is an NFS mount and if *cssys* user does not have access to this folder, installation will fail. *cssys* is a local user created by the Workload Security installer that may not have permission to access the mounted share. You can check this by attempting to access /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent using *cssys* user. If it returns "Permission denied", installation permission is not present. Instead of a mounted folder, install on a directory local to the machine.

Problem:	Resolution:
Agent was initially connected via a proxy server and the proxy was set during Agent installation. Now the proxy server has changed. How can the Agent's proxy configuration be changed?	You can edit the agent.properties to add the proxy details. Follow these steps: 1. Change to the folder containing the properties file: cd /opt/netapp/cloudsecure/conf 2. Using your favorite text editor, open the *agent.properties* file for editing. 3. Add or modify the following lines: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Save the file. 5. Restart the agent: sudo systemctl restart cloudsecure-agent.service

Deleting a Workload Security Agent

When you delete a Workload Security Agent, all the data collectors associated with the Agent must be deleted first.

Deleting an Agent

Deleting an Agent deletes all of the Data Collectors associated with the Agent. If you plan to configure the data collectors with a different agent you should create a backup of the Data Collector configurations before you delete the Agent.

Before you begin

1. Make sure all the data collectors associated with the agent are deleted from the Workload Security portal.

   Note: Ignore this step if all the associated collectors are in STOPPED state.

Steps to delete an Agent:

1. SSH into the agent VM and execute the following command. When prompted, enter "y" to continue.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Click **Admin > Data Collectors > Agents**

The system displays the list of configured Agents.

3. Click the options menu for the Agent you are deleting.
4. Click **Delete**.

   The system displays the **Delete Agent** page.

5. Click **Delete** to confirm the deletion.

Configuring an Active Directory (AD) User Directory Collector

Workload Security can be configured to collect user attributes from Active Directory servers.

Before you begin

- You must be a Cloud Insights Administrator or Account Owner to perform this task.
- You must have the IP address of the server hosting the Active Directory server.
- An Agent must be configured before you configure a User Directory connector.

Steps to Configure a User Directory Collector

1. In the Workload Security menu, click:
   Admin > Data Collectors > User Directory Collectors > + User Directory Collector and select **Active Directory**

   The system displays the Add User Directory screen.

Configure the User Directory Collector by entering the required data in the following tables:

Name	Description
Name	Unique name for the user directory. For example *GlobalADCollector*
Agent	Select a configured agent from the list
Server IP/Domain Name	IP address or Fully-Qualified Domain Name (FQDN) of server hosting the active directory

Forest Name	Forest level of the directory structure. Forest name allows both of the following formats: *x.y.z* ⇒ direct domain name as you have it on your SVM. [Example: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Relative distinguished names [Example: DC=hq,DC= companyname,DC=com] Or you can specify as the following: *OU=engineering,DC=hq,DC= companyname,DC=com* [to filter by specific OU engineering] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [to get only specific user with <username> from OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [to get all Acrobat Users within the Users in that organization] Trusted Active Directory domains are also supported.
Bind DN	User permitted to search the directory. For example: *username@companyname.com* or *username@domainname.com*
BIND password	Directory server password (i.e. password for username used in Bind DN)
Protocol	ldap, ldaps, ldap-start-tls
Ports	Select port

Add to table once link is provided:
For more details about forest names, please refer to this xref:./////

Enter the following Directory Server required attributes if the default attribute names have been modified in LDAP Directory Server. Most often these attributes names are *not* modified in LDAP Directory Server, in which case you can simply proceed with the default attribute name.

Attributes	Attribute name in Directory Server
Display Name	name
UNIXID	uidnumber
User Name	uid

Click Include Optional Attributes to add any of the following attributes:

Attributes	Attribute Name in Directory Server
Email Address	mail

Telephone Number	telephonenumber
Role	title
Country	co
State	state
Department	departmentnumber
Photo	photo
ManagerDN	manager
Groups	memberOf

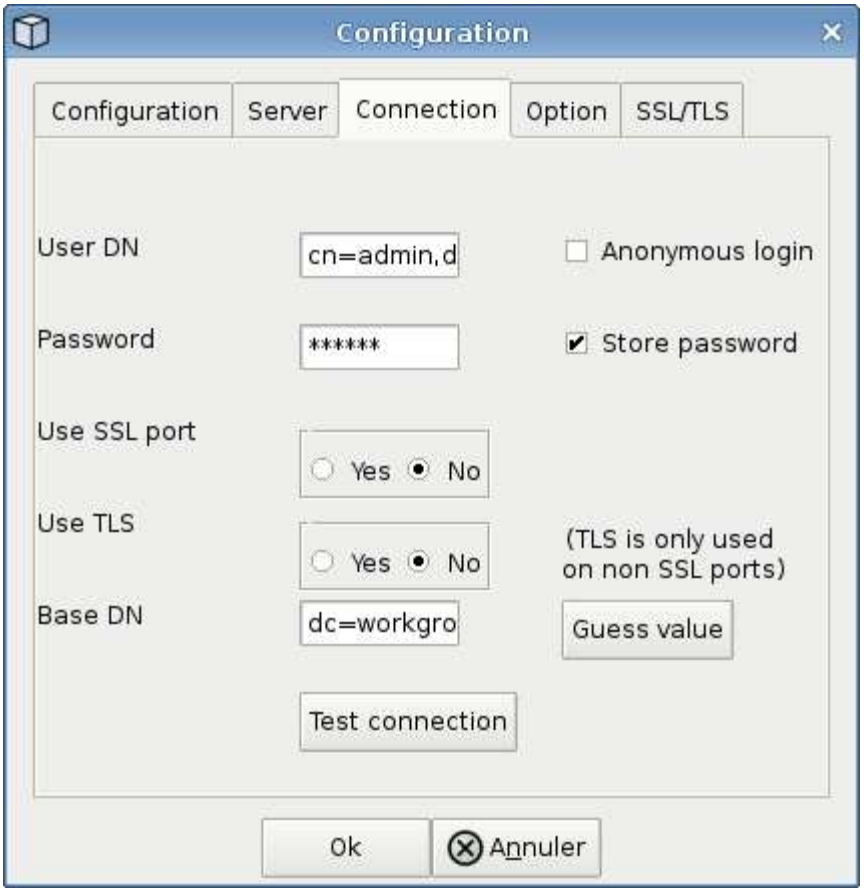
Testing Your User Directory Collector Configuration

You can validate LDAP User Permissions and Attribute Definitions using the following procedures:

- Use the following command to validate Workload Security LDAP user permission:

```
ldapsearch -D "uid=john ,cn=users,cn=accounts,dc=dorp,dc=company,dc=com"
-W -x -LLL -o ldif-wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
```

- Use LDAP Explorer to navigate an LDAP database, view object properties and attributes, view permissions, view an object's schema, execute sophisticated searches that you can save and re-execute.
  - Install LDAP Explorer (http://ldaptool.sourceforge.net/) or Java LDAP Explorer (http://jxplorer.org/) on any windows machine which can connect to the LDAP Server.
  - Connect to the LDAP server using the username/password of the LDAP directory server.



Troubleshooting LDAP Directory Collector Configuration Errors

The following table describes known problems and resolutions that can occur during collector configuration:

Problem:	Resolution:
Adding an LDAP Directory connector results in the ‘Error’ state. Error says, “Invalid credentials provided for LDAP server”.	Incorrect Bind DN or Bind Password or Search Base provided. Edit and provide the correct information.
Adding an LDAP Directory connector results in the ‘Error’ state. Error says, “Failed to get the object corresponding to DN=DC=hq,DC=domainname,DC=com provided as forest name.”	Incorrect Search Base provided. Edit and provide the correct forest name.
The optional attributes of domain user are not appearing in the Workload Security User Profile page.	This is likely due to a mismatch between the names of optional attributes added in CloudSecure and the actual attribute names in Active Directory. Fields are case sensitive. Edit and provide the correct optional attribute name(s).
Data collector in error state with "Failed to retrieve LDAP users. Reason for failure: Cannot connect on the server, the connection is null"	Restart the collector by clicking on the *Restart* button.

Problem:	Resolution:
Adding an LDAP Directory connector results in the ‘Error’ state.	Ensure you have provided valid values for the required fields (Server, forest-name, bind-DN, bind-Password). Ensure bind-DN input is always provided as uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com.
Adding an LDAP Directory connector results in the ‘RETRYING’ state. Shows error “Failed to determine the health of the collector hence retrying again”	Ensure correct Server IP and Search Base is provided ////
While adding LDAP directory the following error is shown: “Failed to determine the health of the collector within 2 retries, try restarting the collector again(Error Code: AGENT008)”	Ensure correct Server IP and Search Base is provided
Adding an LDAP Directory connector results in the ‘RETRYING’ state. Shows error “Unable to define state of the collector,reason Tcp command [Connect(localhost:35012,None,List(),Some(,seconds),true)] failed because of java.net.ConnectionException:Connection refused.”	Incorrect IP or FQDN provided for the AD Server. Edit and provide the correct IP address or FQDN. ////
Adding an LDAP Directory connector results in the ‘Error’ state. Error says, “Failed to establish LDAP connection”.	Incorrect IP or FQDN provided for the LDAP Server. Edit and provide the correct IP address or FQDN. Or Incorrect value for Port provided. Try using the default port values or the correct port number for the LDAP server.
Adding an LDAP Directory connector results in the ‘Error’ state. Error says, “Failed to load the settings. Reason: Datasource configuration has an error. Specific reason: /connector/conf/application.conf: 70: ldap.ldap-port has type STRING rather than NUMBER”	Incorrect value for Port provided. Try using the default port values or the correct port number for the AD server.
I started with the mandatory attributes, and it worked. After adding the optional ones, the optional attributes data is not getting fetched from AD.	This is likely due to a mismatch between the optional attributes added in CloudSecure and the actual attribute names in Active Directory. Edit and provide the correct mandatory or optional attribute name.
After restarting the collector, when will the LDAP sync happen?	LDAP sync will happen immediately after the collector restarts. It will take approximately 15 minutes to fetch user data of approximately 300K users, and is refreshed every 12 hours automatically.
User Data is synced from LDAP to CloudSecure. When will the data be deleted?	User data is retained for 13months in case of no refresh. If the tenant is deleted then the data will be deleted.

Problem:	Resolution:
LDAP Directory connector results in the ‘Error’ state. "Connector is in error state. Service name: usersLdap. Reason for failure: Failed to retrieve LDAP users. Reason for failure: 80090308: LdapErr: DSID-0C090453, comment: AcceptSecurityContext error, data 52e, v3839"	Incorrect forest name provided. See above on how to provide the correct forest name.
Telephone number is not getting populated in the user profile page.	This is most likely due to an attribute mapping problem with the Active Directory. 1. Edit the particular Active Directory collector which is fetching the user’s information from Active Directory. 2. Notice under optional attributes, there is a field name “Telephone Number” mapped to Active Directory attribute ‘telephonenumber’. 4. Now, please use the Active Directory Explorer tool as described above to browse the LDAP Directory server and see the correct attribute name. 3. Make sure that in LDAP Directory there is an attribute named ‘telephonenumber’ which has indeed the telephone number of the user. 5. Let us say in LDAP Directory it has been modified to ‘phonenumber’. 6. Then Edit the CloudSecure User Directory collector. In optional attribute section, replace ‘telephonenumber’ with ‘phonenumber’. 7. Save the Active Directory collector, the collector will restart and get the telephone number of the user and display the same in the user profile page.
If encryption certificate (SSL) is enabled on the Active Directory (AD) Server, the Workload Security User Directory Collector can not connect to the AD Server.	Disable AD Server encryption before Configuring a User Directory Collector. Once the user detail is fetched it will be there for 13 months. If the AD server gets disconnected after fetching the user details, the newly added users in AD won’t get fetched. To fetch again the user directory collector needs to be connected to AD.

Configuring the ONTAP SVM Data Collector

Workload Security uses data collectors to collect file and user access data from devices.

Before you begin

- This data collector is supported with the following:
  - Data ONTAP 9.2 and later versions. For best performance, use a Data ONTAP version where this issue is fixed.
  - SMB protocol version 3.1 and earlier. Note that Workload Security does not work with SMB configurations that use Flexcache. Starting with ONTAP9.7, Fpolicy is supported only in an NFS environment.

- NFS protocol version 4.0 and earlier
- Flexgroup is supported from ONTAP 9.4 and later versions
- ONTAP Select is supported

- Only data type SVMs are supported. SVMs with infinite volumes are not supported.
- SVM has several sub-types. Of these, only *default*, *sync_source*, and *sync_destination* are supported.
- An Agent must be configured before you can configure data collectors.
- Make sure that you have a properly configured User Directory Connector, otherwise events will show encoded user names and not the actual name of the user (as stored in Active Directory) in the “Activity Forensics” page.
- For optimal performance, you should configure the FPolicy server to be on the same subnet as the storage system.
- You must add an SVM using one of the following two methods:
  - By Using Cluster IP, SVM name, and Cluster Management Username and Password. ***This is the recommended method.***
    - SVM name must be exactly as is shown in ONTAP and is case-sensitive.
  - By Using SVM Vserver Management IP, Username, and Password
  - If you are not able or not willing to use the full Administrator Cluster/SVM Management Username and Password, you can create a custom user with lesser privileges as mentioned in the “A note about permissions” section below. This custom user can be created for either SVM or Cluster access.
    - o You can also use an AD user with a role that has at least the permissions of csrole as mentioned in “A note about permissions” section below. Also refer to the ONTAP documentation.
- Ensure the correct applications are set for the SVM by executing the following command:

```
clustershell::> security login show -vserver <vservername> -user-or
-group-name <username>
```

Example output:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Ensure that the SVM has a CIFS server configured:
  clustershell::> `vserver cifs show`

  The system returns the Vserver name, CIFS server name and additional fields.

- Set a password for the SVM vsadmin user. If using custom user or cluster admin user, skip this step.
  clustershell::> `security login password -username vsadmin -vserver svmname`

- Unlock the SVM vsadmin user for external access. If using custom user or cluster admin user, skip this step.
  clustershell::> `security login unlock -username vsadmin -vserver svmname`
- Ensure the firewall-policy of the data LIF is set to ‘mgmt’ (not ‘data’). Skip this step if using a dedicated management lif to add the SVM.
  clustershell::> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- When a firewall is enabled, you must have an exception defined to allow TCP traffic for the port using the Data ONTAP Data Collector.

  See Agent requirements for configuration information. This applies to on-premise Agents and Agents installed in the Cloud.

- When an Agent is installed in an AWS EC2 instance to monitor a Cloud ONTAP SVM, the Agent and Storage must be in the same VPC. If they are in separate VPCs, there must be a valid route between the VPC’s.

A Note About Permissions

Permissions when adding via Cluster Management IP:

If you cannot use the Cluster management administrator user to allow Workload Security to access the ONTAP SVM data collector, you can create a new user named “csuser” with the roles as shown in the commands below. Use the username “csuser” and password for “csuser” when configuring the Workload Security data collector to use Cluster Management IP.

To create the new user, log in to ONTAP with the Cluster management Administrator username/password, and execute the following commands on the ONTAP server:

```
security login role create -role csrole -cmddirname DEFAULT -access none
security login role create -role csrole -cmddirname "network interface"
-access readonly
security login role create -role csrole -cmddirname version -access
readonly
security login role create -role csrole -cmddirname volume -access
readonly
security login role create -role csrole -cmddirname vserver -access
readonly
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
```

Permissions when adding via Vserver Management IP:

If you cannot use the Cluster management administrator user to allow Workload Security to access the ONTAP SVM data collector, you can create a new user named “csuser” with the roles as shown in the commands below. Use the username “csuser” and password for “csuser” when configuring the Workload Security data collector to use Vserver Management IP.

To create the new user, log in to ONTAP with the Cluster management Administrator username/password, and execute the following commands on the ONTAP server. For ease, copy these commands to a text editor and replace the <vservername> with your Vserver name before and executing these commands on ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
```

Configure the data collector

Steps for Configuration

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

   The system displays the available Data Collectors.

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.

Configuration

Field	Description
Name	Unique name for the Data Collector
Agent	Select a configured agent from the list.
Connect via Management IP for:	Select either Cluster IP or SVM Management IP
Cluster / SVM Management IP Address	The IP address for the cluster or the SVM, depending on your selection above.
SVM Name	The Name of the SVM (this field is required when connecting via Cluster IP)

Username	User name to access the SVM/Cluster When adding via Cluster IP the options are: 1. Cluster-admin 2. ‘csuser’ 3. AD-user having similar role as csuser. When adding via SVM IP the options are: 4. vsadmin 5. ‘csuser’ 6. AD-username having similar role as csuser.
Password	Password for the above user name
Filter Shares/Volumes	Choose whether to include or exclude Shares / Volumes from event collection
Enter complete share names to exclude/include	Comma-separated list of shares to exclude or include (as appropriate) from event collection
Enter complete volume names to exclude/include	Comma-separated list of volumes to exclude or include (as appropriate) from event collection
Monitor Folder Access	When checked, enables events for folder access monitoring. Note that folder create/rename and delete will be monitored even without this option selected. Enabling this will increase the number of events monitored.
Set ONTAP Send Buffer size	Sets the ONTAP Fpolicy send buffer size. If an ONTAP version prior to 9.8p7 is used and performance issue is seen, then the ONTAP send buffer size can be altered to get improved ONTAP performance. Contact NetApp Support if you do not see this option and wish to explore it.

After you finish

- In the Installed Data Collectors page, use the options menu on the right of each collector to edit the data collector. You can restart the data collector or edit data collector configuration attributes.

Recommended Configuration for Metro Cluster

The following is recommended for Metro Cluster:

1. Connect two data collectors, one to the source SVM and another to the destination SVM.
2. The data collectors should be connected by *Cluster IP*.
3. At any moment of time, one data collector should be in running, another will be in error.

   The current ‘running’ SVM’s data collector will show as *Running*. The current ‘stopped’ SVM’s data collector will show as *Error*.

4. Whenever there is a switchover, the state of the data collector will change from ‘running’ to ‘error’ and vice versa.
5. It will take up to two minutes for the data collector to move from Error state to Running state.

Service Policy

If using service policy from ONTAP version 9.9.1, in order to connect to the Data Source Collector, the *data-fpolicy-client* service is required along with the data service *data-nfs*, and/or *data-cifs*.

Example:

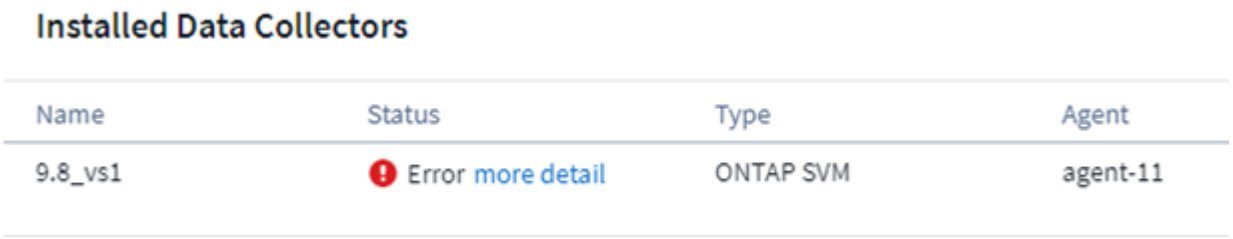
```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

In versions of ONTAP prior to 9.9.1, *data-fpolicy-client* need not be set.

Troubleshooting

Known problems and their resolutions are described in the following table.

In the case of an error, click on *more detail* in the *Status* column for detail about the error.



Problem:	Resolution:
Data Collector runs for some time and stops after a random time, failing with: "Error message: Connector is in error state. Service name: audit. Reason for failure: External fpolicy server overloaded."	The event rate from ONTAP was much higher than what the Agent box can handle. Hence the connection got terminated. Check the peak traffic in CloudSecure when the disconnection happened. This you can check from the **CloudSecure > Activity Forensics > All Activity** page. If the peak aggregated traffic is higher than what the Agent Box can handle, then please refer to the Event Rate Checker page on how to size for Collector deployment in an Agent Box. If the Agent was installed in the Agent box prior to 4 March 2021, run the following commands in the Agent box: echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf sysctl -p Restart the collector from the UI after resizing.

Problem:	Resolution:
Collector reports Error Message: “No local IP address found on the connector that can reach the data interfaces of the SVM”.	This is most likely due to a networking issue on the ONTAP side. Please follow these steps: 1. Ensure that there are no firewalls on the SVM data lif or the management lif which are blocking the connection from the SVM. 2. When adding an SVM via a cluster management IP, please ensure that the data lif and management lif of the SVM are pingable from the Agent VM. In case of issues, check the gateway, netmask and routes for the lif. You can also try logging in to the cluster via ssh using the cluster management IP, and ping the Agent IP. Make sure that the agent IP is pingable: *network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail* If not pingable, make sure the network settings in ONTAP are correct, so that the Agent machine is pingable. 3. If you have tried connecting via Cluster IP and it is not working, try connecting directly via SVM IP. Please see above for the steps to connect via SVM IP. 4. While adding the collector via SVM IP and vsadmin credentials, check if the SVM Lif has Data plus Mgmt role enabled. In this case ping to the SVM Lif will work, however SSH to the SVM Lif will not work. If yes, create an SVM Mgmt Only Lif and try connecting via this SVM management only Lif. 5. If it is still not working, create a new SVM Lif and try connecting through that Lif. Make sure that the subnet mask is correctly set. 6. Advanced Debugging: a) Start a packet trace in ONTAP. b) Try to connect a data collector to the SVM from CloudSecure UI. c) Wait till the error appears. Stop the packet trace in ONTAP. d) Open the packet trace from ONTAP. It is available at this location *https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/* e) Make sure there is a SYN from ONTAP to the Agent box. f) If there is no SYN from ONTAP then it is an issue

Problem:	Resolution:
Message: "Failed to determine ONTAP type for [hostname: <IP Address>. Reason: Connection error to Storage System <IP Address>: Host is unreachable (Host unreachable)"	1. Verify that the correct SVM IP Management address or Cluster Management IP has been provided. 2. SSH to the SVM or the Cluster to which you are intending to connect. Once you are connected ensure that the SVM or the Cluster name is correct.

Problem:	Resolution:
Error Message: "Connector is in error state. Service.name: audit. Reason for failure: External fpolicy server terminated."	1. It is most likely that a firewall is blocking the necessary ports in the agent machine. Verify the port range 35000-55000/tcp is opened for the agent machine to connect from the SVM. Also ensure that there are no firewalls enabled from the ONTAP side blocking communication to the agent machine. 2. Type the following command in the Agent box and ensure that the port range is open. *sudo iptables-save | grep 3500** Sample output should look like: *-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEW -j ACCEPT* 3. Login to SVM, enter the following commands and check that no firewall is set to block the communication with ONTAP. *system services firewall show* *system services firewall policy show* Check firewall commands on the ONTAP side. 4. SSH to the SVM/Cluster which you want to monitor. Ping the Agent box from the SVM data lif (with CIFS, NFS protocols support) and ensure that ping is working: *network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail* If not pingable, make sure the network settings in ONTAP are correct, so that the Agent machine is pingable. 5.If a single SVM is added twice added to a tenant via 2 data collectors, then this error will be shown. Delete one of the data collectors thru the UI. Then restart the other data collector thru the UI. Then the data collector will show “RUNNING” status and will start receiving events from SVM. Basically, in a tenant, 1 SVM should be added only once, via 1 data collector. 1 SVM should not added twice via 2 data collectors. 6. In instances where the same SVM was added in two different Workload Security environments (tenants), the last one will always succeed. The second collector will configure fpolicy with its own IP address and kick out the first one. So the collector in

Problem:	Resolution:
No events seen in activity page.	1. Check if ONTAP collector is in “RUNNING” state. If yes, then ensure that some cifs events are being generated on the cifs client VMs by opening some files. 2. If no activities are seen, please login to the SVM and enter the following command. *<SVM>event log show -source fpolicy* Please ensure that there are no errors related to fpolicy. 3. If no activities are seen, please login to the SVM. Enter the following command *<SVM>fpolicy show* Check if the fpolicy policy named with prefix “cloudsecure_” has been set and status is “on”. If not set, then most likely the Agent is unable to execute the commands in the SVM. Please ensure all the prerequisites as described in the beginning of the page have been followed.
SVM Data Collector is in error state and Errror message is “Agent failed to connect to the collector”	1. Most likely the Agent is overloaded and is unable to connect to the Data Source collectors. 2. Check how many Data Source collectors are connected to the Agent. 3. Also check the data flow rate in the “All Activity” page in the UI. 4. If the number of activities per second is significantly high, install another Agent and move some of the Data Source Collectors to the new Agent.
SVM Data Collector shows error message as "fpolicy.server.connectError: Node failed to establish a connection with the FPolicy server "12.195.15.146" (reason: "Select Timed out")"	Firewall is enabled in SVM/Cluster. So fpolicy engine is unable to connect to fpolicy server. CLIs in ONTAP which can be used to get more information are: event log show -source fpolicy which shows the error event log show -source fpolicy -fields event,action,description which shows more details. Check firewall commands on the ONTAP side.
Error Message: “Connector is in error state. Service name:audit. Reason for failure: No valid data interface (role: data,data protocols: NFS or CIFS or both, status: up) found on the SVM.”	Ensure there is an operational interface (having role as data and data protocol as CIFS/NFS.

Problem:	Resolution:
The data collector goes into Error state and then goes into RUNNING state after some time, then back to Error again. This cycle repeats.	This typically happens in the following scenario: 1. There are multiple data collectors added. 2. The data collectors which show this kind of behavior will have 1 SVM added to these data collectors. Meaning 2 or more data collectors are connected to 1 SVM. 3. Ensure 1 data collector connects to only 1 SVM. 4. Delete the other data collectors which are connected to the same SVM.
Connector is in error state. Service name: audit. Reason for failure: Failed to configure (policy on SVM svmname. Reason: Invalid value specified for 'shares-to-include' element within 'fpolicy.policy.scope-modify: "Federal'	The share names need to be given without any quotes. Edit the ONTAP SVM DSC configuration to correct the share names. *Include and exclude shares* is not intended for a long list of share names. Use filtering by volume instead if you have a large number of shares to include or exclude.
There are existing fpolicies in the Cluster which are unused. What should be done with those prior to installation of Workload Security?	It is recommended to delete all existing unused fpolicy settings even if they are in disconnected state. Workload Security will create fpolicy with the prefix "cloudsecure_". All other unused fpolicy configurations can be deleted. CLI command to show fpolicy list: *fpolicy show* Steps to delete fpolicy configurations: *fpolicy disable -vserver <svmname> -policy-name <policy_name>* *fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>* *fpolicy policy delete -vserver <svmname> -policy -name <policy_name>* *fpolicy policy event delete -vserver <svmname> -event-name <event_list>* *fpolicy policy external-engine delete -vserver <svmname> -engine-name <engine_name>*
After enabling Workload Security, ONTAP performance is impacted: Latency becomes sporadically high, IOPs become sporadically low.	Ensure that you are using a Data ONTAP version where this issue is fixed. The minimum version of ONTAP recommended is 9.8P7. If an ONTAP version prior to 9.8p7 is used and this performance issue is seen, then the ONTAP send buffer size can be altered to get improved ONTAP performance. Contact NetApp Support if you wish to explore this option and do not see this setting when adding a new data collector or editing an existing one.

Problem:	Resolution:
Data collector is in error, shows this error message. “Error: Connector is in error state. Service name: audit. Reason for failure: Failed to configure policy on SVM svm_test. Reason: Missing value for zapi field: events. “	Start with a new SVM with only NFS service configured. Add an ONTAP SVM data collector in Workload Security. CIFS is configured as an allowed protocol for the SVM while adding the ONTAP SVM Data Collector in Workload Security. Wait until the Data collector in Workload Security shows an error. Since the CIFS server is NOT configured on the SVM, this error as shown in the left is shown by Workload Security. Edit the ONTAP SVM data collector and un-check CIFs as allowed protocol. Save the data collector. It will start running with only NFS protocol enabled.
Data Collector shows the error message: “Error: Failed to determine the health of the collector within 2 retries, try restarting the collector again (Error Code: AGENT008)”.	1. On the Data Collectors page, scroll to the right of the data collector giving the error and click on the 3 dots menu. Select *Edit*. Enter the password of the data collector again. Save the data collector by pressing on the *Save* button. Data Collector will restart and the error should be resolved. 2. The Agent machine may not enough CPU or RAM headroom, that is why the DSCs are failing. Please check the number of Data Collectors which are added to the Agent in the machine. If it is more than 20, please increase the CPU and RAM capacity of the Agent machine. Once the CPU and RAM is increased, the DSCs will get into Initializing and then to Running state automatically. Look into the sizing guide on this page.

If you are still experiencing problems, reach out to the support links mentioned in the **Help > Support** page.

Configuring the Cloud Volumes ONTAP and Amazon FSx for NetApp ONTAP collector

Workload Security uses data collectors to collect file and user access data from devices.

Cloud Volumes ONTAP Storage Configuration

See the OnCommand Cloud Volumes ONTAP Documentation to configure a single-node / HA AWS instance to host the Workload Security Agent:
https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

After the configuration is complete, follow the steps to setup your SVM:
https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html

Supported Platforms

- Cloud Volumes ONTAP, supported in all the available cloud service providers wherever available. For example: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Agent Machine Configuration

The agent machine must be configured in the respective subnets of the cloud Service providers. Read more about network access in the [Agent Requirements].

Below are the steps for Agent installation in AWS. Equivalent steps, as applicable to the cloud service provider, can be followed in Azure or Google Cloud for the installation.

In AWS, use the following steps to configure the machine to be used as a Workload Security Agent:

Use the following steps to configure the machine to be used as a Workload Security Agent:

Steps

1. Log in to the AWS console and navigate to EC2-Instances page and select *Launch instance*.
2. Select a RHEL or CentOS AMI with the appropriate version as mentioned in this page: https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html
3. Select the VPC and Subnet that the Cloud ONTAP instance resides in.
4. Select *t2.xlarge* (4 vcpus and 16 GB RAM) as allocated resources.
    a. Create the EC2 instance.
5. Install the required Linux packages using the YUM package manager:
    a. Install *wget* and *unzip* native Linux packages.

Install the Workload Security Agent

1. Log in as Administrator or Account Owner to your Cloud Insights environment.
2. Navigate to Workload Security **Admin > Data Collectors** and click the **Agents** tab.
3. Click **+Agent** and specify RHEL as the target platform.
4. Copy the Agent Installation command.
5. Paste the Agent Installation command into the RHEL EC2 instance you are logged in to. This installs the Workload Security agent, providing all of the Agent Prerequisites are met.

For detailed steps please refer to this xref:./
https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Troubleshooting

Known problems and their resolutions are described in the following table.

Problem	Resolution

“Workload Security: Failed to determine ONTAP type for Amazon FxSN data collector” error is shown by the Data Collector. Customer is unable to add new Amazon FSxN data collector into Workload Security. Connection to FSxN cluster on port 443 from the agent is timing out. Firewall and AWS security groups have the required rules enabled to allow communication. An agent is already deployed and is in the same AWS account as well. This same agent is used to connect and monitor the remaining NetApp devices (and all of them are working).	Solve this issue by adding fsxadmin LIF network segment to agent’s security rule. Allowed all ports if you are not sure about the ports.

User Management

Workload Security user accounts are managed through Cloud Insights.

Cloud Insights provides four user account levels: Account Owner, Administrator, User, and Guest. Each account is assigned specific permission levels. A User account that has Administrator privileges can create or modify users, and assign each user one of the following Workload Security roles:

Role	Workload Security Access
Administrator	Can perform all Workload Security functions, including those for Alerts, Forensics, data collectors, automated response policies, and APIs for Workload Security. An Administrator can also invite other users but can only assign Workload Security roles.
User	Can view and manage Alerts and view Forensics. User role can change alert status, add a note, take snapshots manually, and restrict user access.
Guest	Can view Alerts and Forensics. Guest role cannot change alert status, add a note, take snapshots manually, or restrict user access.

Steps

1. Log into Workload Security
2. In the menu, click **Admin > User Management**

   You will be forwarded to Cloud Insights’s User Management page.

3. Select the desired role for each user.

While adding a new user, simply select the desired role (usually User or Guest).

More information on User accounts and roles can be found in the Cloud Insights User Role documentation.

SVM Event Rate Checker (Agent Sizing Guide)

The Event Rate Checker is used to check the NFS/SMB combined event rate in the SVM before installing an ONTAP SVM data collector, to see how many SVMs one Agent

machine will be able to monitor. Use the Event Rate Checker as a sizing guide to help plan your security environment.

An Agent can support up to 50 data collectors.

Requirements:

- Cluster IP
- Cluster admin username and password

> When running this script no ONTAP SVM Data Collector should be running for the SVM for which event rate is being determined.

Steps:

1. Install the Agent by following the instructions in CloudSecure.
2. Once the agent is installed, run the *server_data_rate_checker.sh* script as a sudo user:

```
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

3. This script requires *sshpass* to be installed in the linux machine. There are two ways to install it:
   a. Run the fiollowing command:

```
linux_prompt> yum install sshpass
```

   b. If that does not work, then download *sshpass* to the linux machine from the web and run the following command:

```
linux_prompt> rpm -i sshpass
```

4. Provide the correct values when prompted. See below for an example.
5. The script will take approximately 5 minutes to run.
6. After the run is complete, the script will print the event rate from the SVM. You can check Event rate per SVM in the console output:

```
“Svm svm_rate is generating 100 events/sec”.
```

Each Ontap SVM Data Collector can be associated with a single SVM, which means each data collector will be able to receive the number of events which a single SVM generates.

Keep the following in mind:

A) Use this table as a general sizing guide:

Agent Machine Configuration	Number of SVM Data Collectors	Max event Rate which the Agent Machine can handle
4 core, 16GB	10 data collectors	20K events/sec
4 core, 32GB	20 data collectors	20K events/sec

B) To calculate your total events, add the Events generated for all SVMs for that agent.

C) If the script is not run during peak hours or if peak traffic is difficult to predict, then keep an event rate buffer of 30%.

B + C Should be less than A, otherwise the Agent machine will fail to monitor.

In other words, the number of data collectors which can be added to a single agent machine should comply to the formula below:

```
Sum of all Event rate of all Data Source Collectors + Buffer Event rate of
30% < 20000 events/second
```

See the Agent Requirements page for additional pre-requisites and requirements.

Example

Let us say we have three SVMS generating event rates of 100, 200, and 300 events per second, respectively.

We apply the formula:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

Console output is available in the Agent machine in the file name *fpolicy_stat_<SVM Name>.log* in the present working directory.

The script may give erroneous results in the following cases:

- Incorrect credentials, IP, or SVM name are provided.
- An already-existing fpolicy with same name, sequence number, etc. will give error.
- The script is stopped abruptly while running.

An example script run is shown below:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

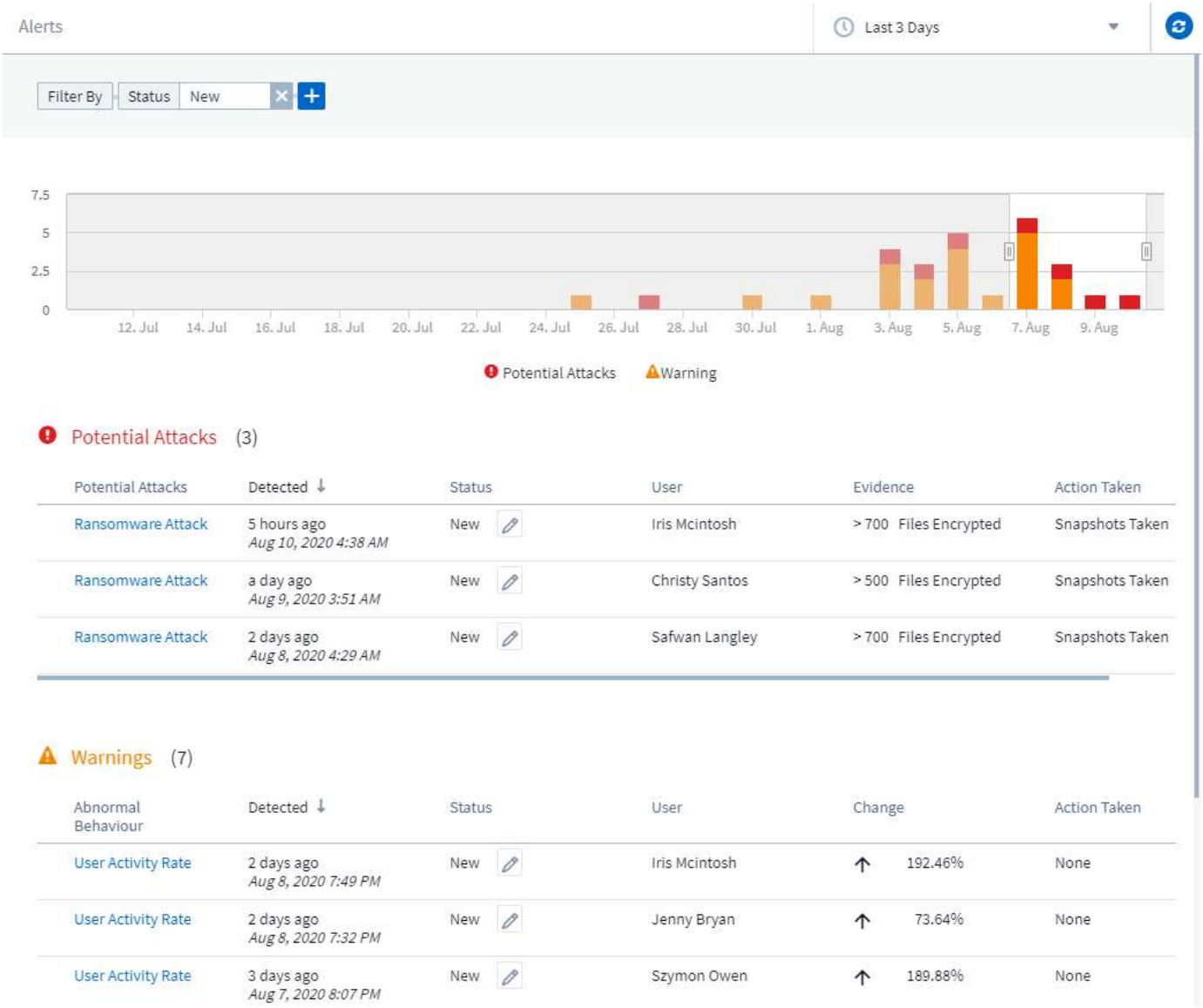
Troubleshooting

Question: If I run this script on an SVM that is already configured for Workload Security, does it just use the existing fpolicy config on the SVM or does it setup a temporary one and run the process?
Answer: The Event Rate Checker can run fine even for an SVM already configured for Workload Security. There should be no impact.

Question: Can I increase the number of SVMs on which the script can be run?
Answer: Yes. Simply edit the script and change the max number of SVMs from 5 to any desirable number.
Question: If I increase the number of SVMs, will it increase the time of running of the script?
Answer: No. The script will run for a max of 5 minutes, even if the number of SVMs is increased.
Question: Can I increase the number of SVMs on which the script can be run?
Answer: Yes. You need to edit the script and change the max number of SVMs from 5 to any desirable number.
Question: If I increase the number of SVMs, will it increase the time of running of the script?
Answer: No. The script will run for a max of 5mins, even if the number of SVMs are increased.

Alerts

The Workload Security Alerts page shows a timeline of recent attacks and/or warnings and allows you to view details for each issue.



Alert

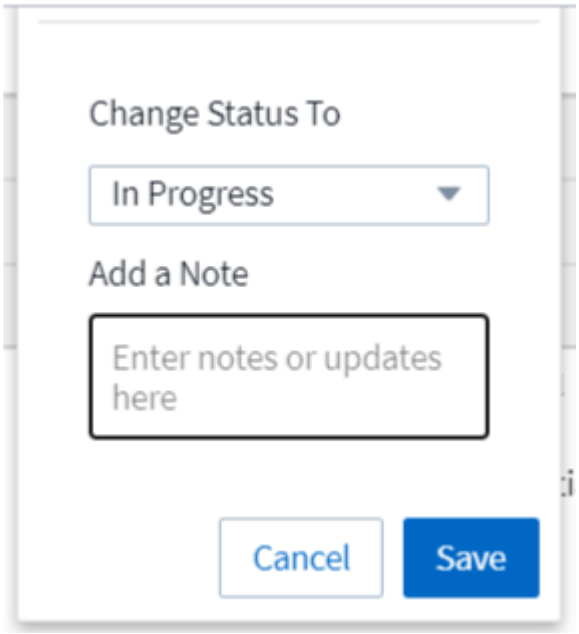
The Alert list displays a graph showing the total number of Potential Attacks and/or Warnings that have been raised in the selected time range, followed by a list of the attacks and/or warnings that occurred in that time range. You can change the time range by adjusting the start time and end time sliders in the graph.

The following is displayed for each alert:

Potential Attacks:

- The *Potential Attack* type (for example, Ransomware or Sabotage)
- The date and time the potential attack was *Detected*
- The *Status* of the alert:
  - **New**: This is the default for new alerts.
  - **In Progress**: The alert is under investigation by a team member or members.
  - **Resolved**: The alert has been marked as resolved by a team member.
  - **Dismissed**: The alert has been dismissed as false positive or expected behavior.

    An administrator can change the status of the alert and add a note to assist with investigation.



- The *User* whose behavior triggered the alert
- *Evidence* of the attack (for example, a large number of files was encrypted)
- The *Action Taken* (for example, a snapshot was taken)

Warnings:

- The *Abnormal Behavior* that triggered the warning
- The date and time the behavior was *Detected*
- The *Status* of the alert (New, In progress, etc.)
- The *User* whose behavior triggered the alert

- A description of the *Change* (for example, an abnormal increase in file access)
- The *Action Taken*

Filter Options

You can filter Alerts by the following:

- The *Status* of the alert
- Specific text in the *Note*
- The type of *Attacks/Warnings*
- The *User* whose actions triggered the alert/warning

The Alert Details page

You can click an alert link on the Alerts list page to open a detail page for the alert. Alert details may vary according to the type of attack or alert. For example, a Ransomware Attack detail page may show the following information:

Summary section:

- Attack type (Ransomware, Sabotage) and Alert ID (assigned by Workload Security)
- Date and Time the attack was detected
- Action Taken (for example, an automatic snapshot was taken. Time of snapshot is shown immediately below the summary section))
- Status (New, In Progress, etc.)

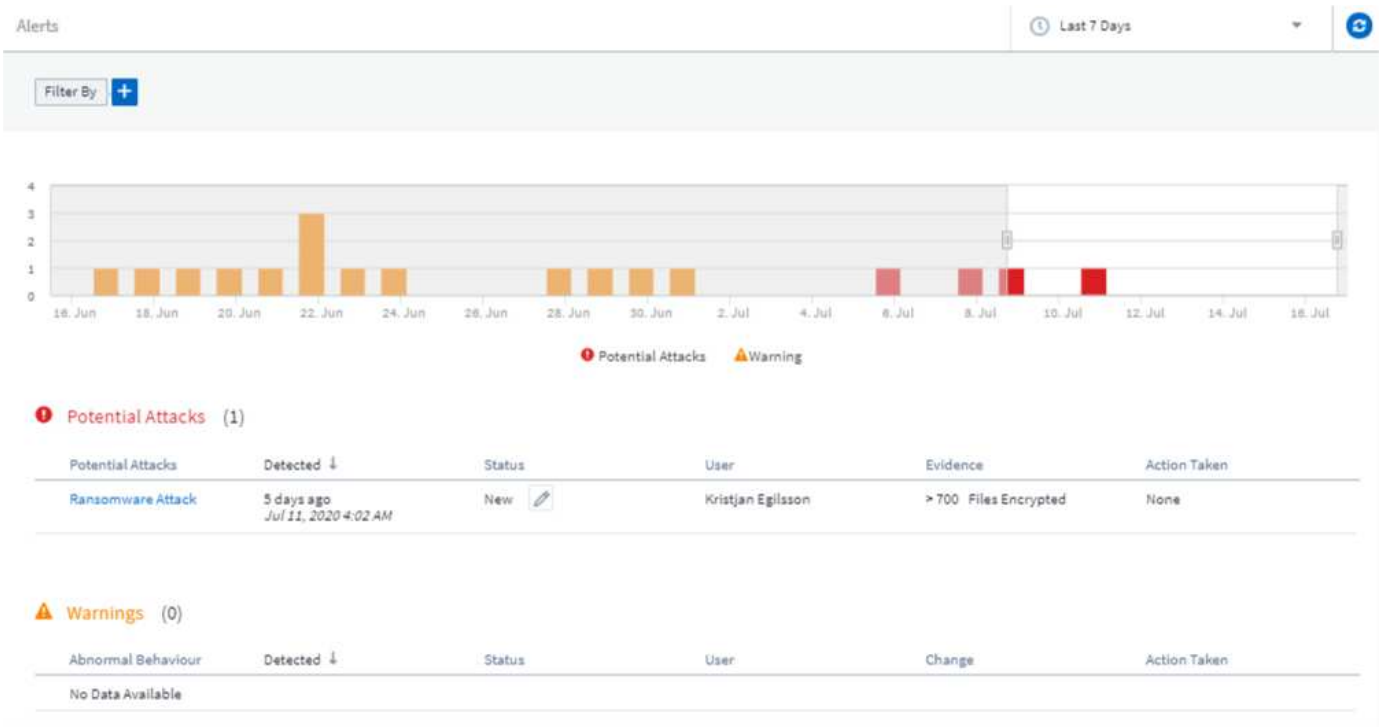
Attack Results section:

- Counts of Affected Volumes and Files
- An accompanying summary of the detection
- A graph showing file activity during the attack

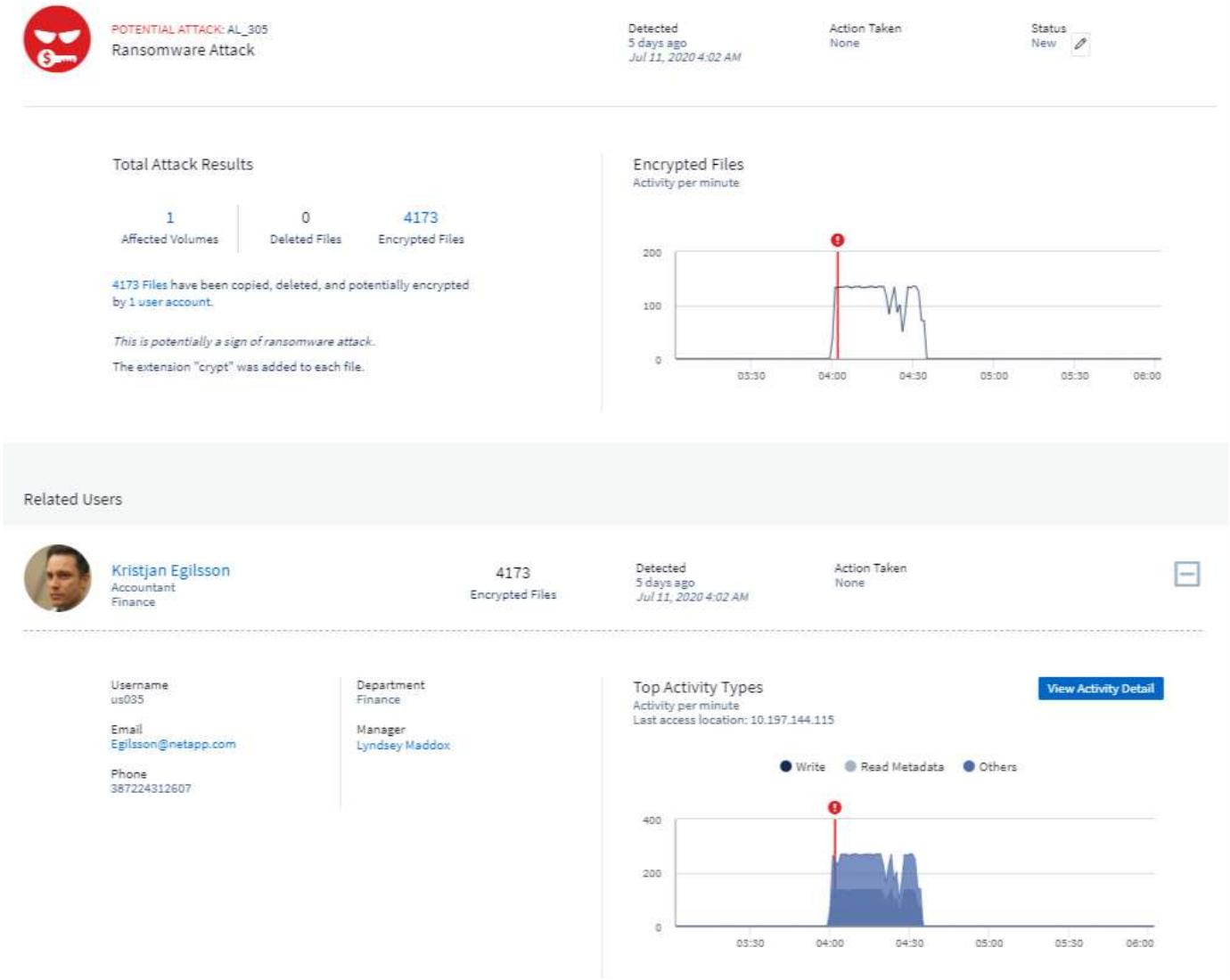
Related Users section:

This section shows details about the user involved in the potential attack, including a graph of Top Activity for the user.

Alerts page (this example shows a potential ransomware attack):



Detail page (this example shows a potential ransomware attack):

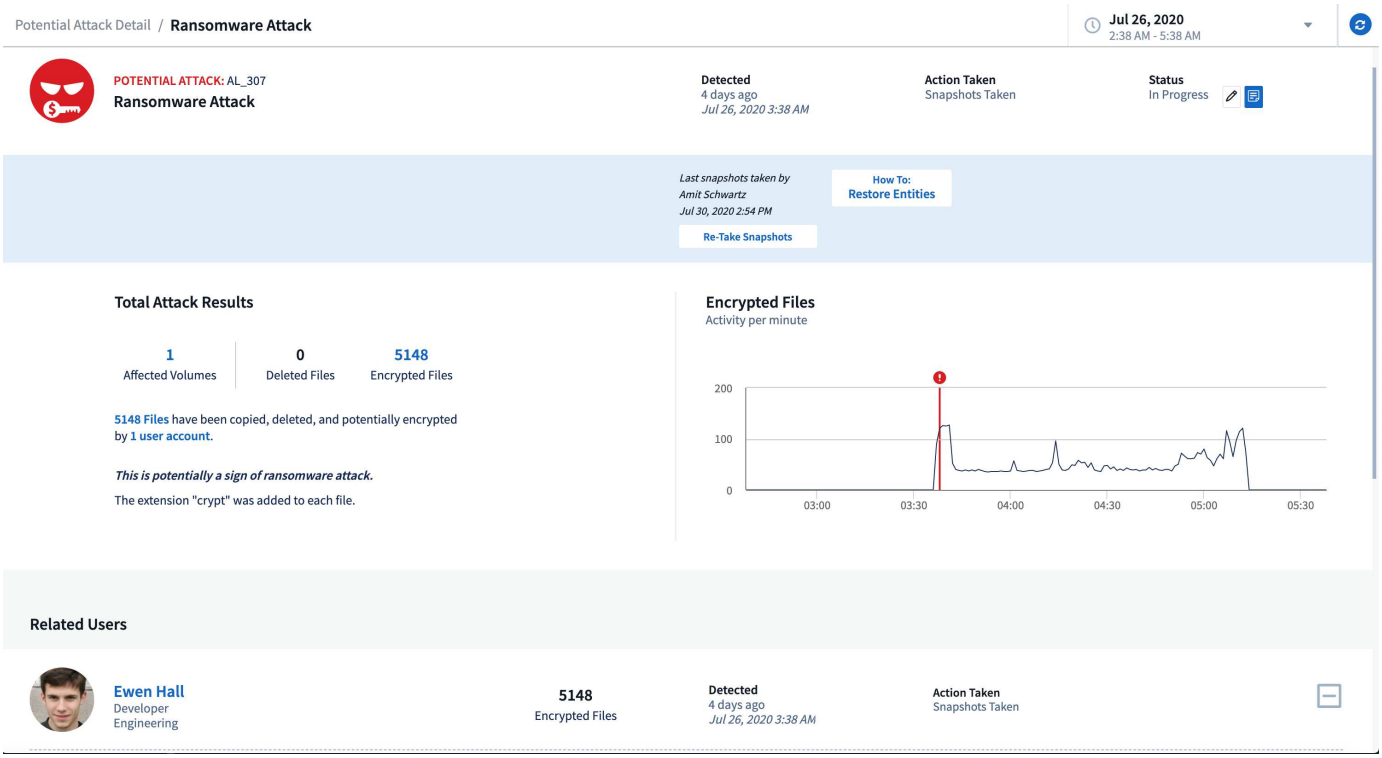


Take a Snapshot **Action**

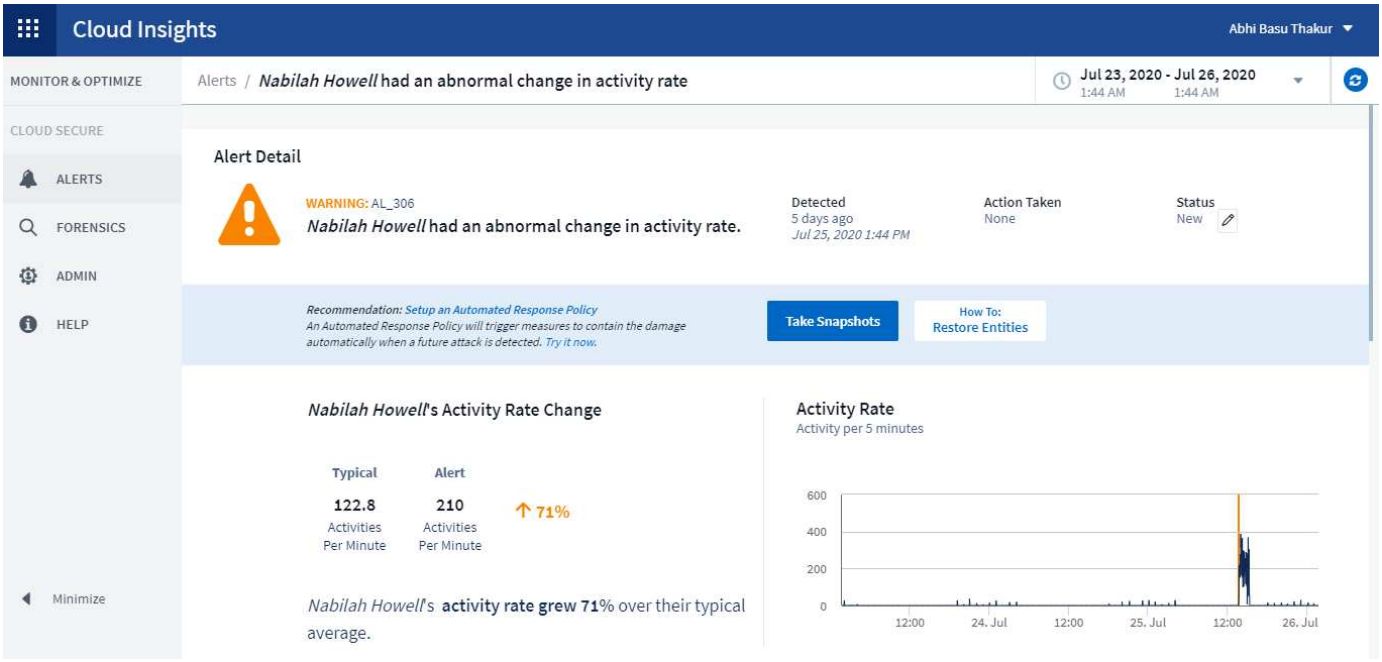
Workload Security protects your data by automatically taking a snapshot when malicious activity is detected, ensuring that your data is safely backed up.

You can define automated response policies that take a snapshot when ransomware attack or other abnormal user activity is detected.
You can also take a snapshot manually from the alert page.

Automatic Snapshot taken:



Manual Snapshot:



Alert Notifications

Email notifications of alerts are sent to an alert recipient list for every action on the alert. To configure alert recipients, click on **Admin > Notifications** and enter an email addresses for each recipient.

Retention Policy

Alerts and Warnings are retained for 13 months. Alerts and Warnings older than 13 months will be deleted. If the Workload Security environment is deleted, all data associated with the environment is also deleted.

Troubleshooting

Problem:	Try This:
For snapshots taken by Workload Security (CS), is there a purging/archiving period for CS snapshots?	No. There is no purging/archiving period set for CS snapshots. The user needs to define purging policy for CS snapshots. Please refer to the ONTAP documentation on how to setup the policies.
There is a situation where, ONTAP takes hourly snapshots per day. Will Workload Security (CS) snapshots affect it? Will CS snapshot take the hourly snapshot place? Will the default hourly snapshot get stopped?	Workload Security snapshots will not affect the hourly snapshots. CS snapshots will not take the hourly snapshot space and that should continue as before. The default hourly snapshot will not get stopped.
What will happen if the maximum snapshot count is reached in ONTAP?	If the maximum Snapshot count is reached, subsequent Snapshot taking will fail and Workload Security will show an error message noting that Snapshot is full. User needs to define Snapshot policies to delete the oldest snapshots, otherwise snapshots will not be taken. In ONTAP 9.3 and earlier, a volume can contain up to 255 Snapshot copies. In ONTAP 9.4 and later, a volume can contain up to 1023 Snapshot copies. See the ONTAP Documentation for information on setting Snapshot deletion policy.
Workload Security is unable to take snapshots at all.	Make sure that the role being used to create snapshots has xref:./ proper rights assigned. Make sure *csrole* is created with proper access rights for taking snapshots: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Snapshots are failing for older alerts on SVMs which were removed from Workload Security and subsequently added back again. For new alerts which occur after SVM is added again, snapshots are taken.	This is a rare scenario. In the event you experience this, log in to ONTAP and take the snapshots manually for the older alerts.
In the *Alert Details* page, the message “Last attempt failed” error is seen below the *Take Snapshot* button. Hovering over the error displays “Invoke API command has timed out for the data collector with id”.	This can happen when a data collector is added to Workload Security via SVM Management IP, if the LIF of the SVM is in *disabled* state in ONTAP. Enable the particular LIF in ONTAP and trigger *Take Snapshot manually* from Workload Security. The Snapshot action will then succeed.

Forensics

Forensics - All Activity

The All Activity page helps you understand the actions performed on entities in the

Workload Security environment.

Examining All Activity Data

Click **Forensics > Activity Forensics** and click the **All Activity** tab to access the All Activity page.
This page provides an overview of activities in your environment, highlighting the following information:

- A graph showing *Activity History* (accessed per minute/per 5 minutes/per 10 minutes based on selected global time range)

  You can zoom the graph by dragging out a rectangle in the graph. The entire page will be loaded to display the zoomed time range. When zoomed in, a button is displayed that lets the user zoom out.

- A chart of *Activity Types*. To obtain activity history data by activity type, click on corresponding x-axis label link.
- A chart of Activity on *Entity Types*. To obtain activity history data by entity type, click on corresponding x-axis label link.
- A list of the *All Activity* data

The **All Activity** table shows the following information. Note that not all of these columns are displayed by default. You can select columns to display by clicking on the "gear" icon .

- The **time** an entity was accessed including the year, month, day, and time of the last access.
- The **user** that accessed the entity with a link to the User information.
- The **activity** the user performed. Supported types are:
  - **Change Group Ownership** - Group Ownership is of file or folder is changed. For more details about group ownership please see this link.
  - **Change Owner** - Ownership of file or folder is changed to another user.
  - **Change Permission** - File or folder permission is changed.
  - **Create** - Create file or folder.
  - **Delete** - Delete file or folder. If a folder is deleted, *delete* events are obtained for all the files in that folder and subfolders.
  - **Read** - File is read.
  - **Read Metadata** - Only on enabling folder monitoring option. Will be generated on opening a folder on Windows or Running “ls” inside a folder in Linux.
  - **Rename** - Rename file or folder.
  - **Write** - Data is written to a file.
  - **Write Metadata** - File metadata is written, for example, permission changed.
  - **Other Change** - Any other event which are not described above. All unmapped events are mapped to “Other Change” activity type. Applicable to files and folders.
- The **Path** to the entity with a link to the Entity Detail Data
- The **Entity Type**, including entity (i.e. file) extension (.doc, .docx, .tmp, etc.)
- The **Device** where the entities reside
- The **Protocol** used to fetch events.

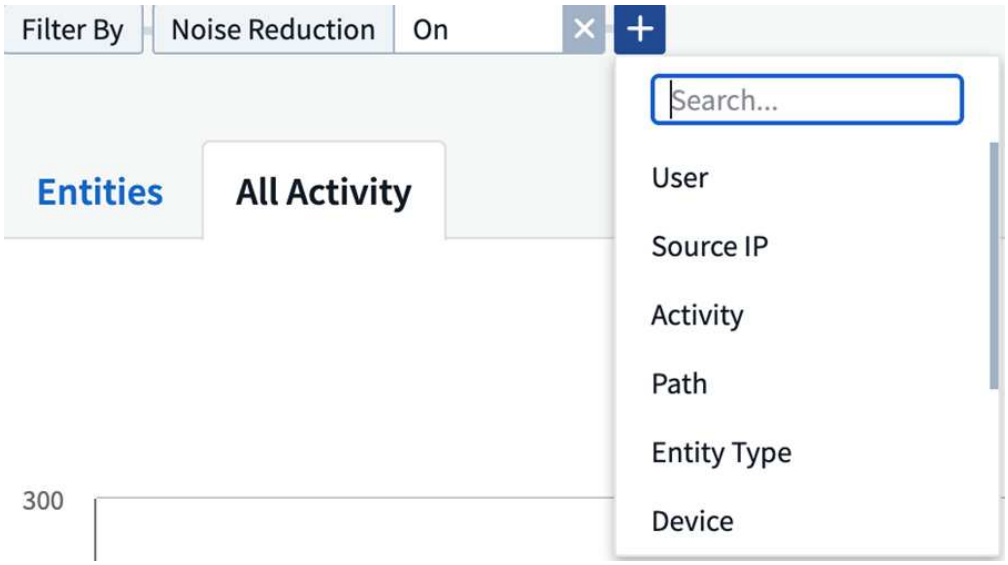
- The **Original Path** used for rename events when the original file was renamed. This column is not visible in the table by default. Use the column selector to add this column to the table.
- The **Volume** where the entities reside. This column is not visible in the table by default. Use the column selector to add this column to the table.

Filtering Forensic Activity History Data

There are two methods you can use to filter data.

1. Hover over the field in the table and click the filter icon that appears. The value is added to the appropriate filters in the top *Filter By* list.
2. Filter data by typing in the *Filter By* field:

   Select the appropriate filter from the top 'Filter By' widget by clicking the **[+]** button:



   Enter the search text

   Press Enter or click outside of the filter box to apply the filter.

You can filter Forensic Activity data by the following fields:

- The **Activity** type.
- **Source IP** from which the entity was accessed. You must provide a valid source IP address in double quotes, for example "10.1.1.1.". Incomplete IPs such as "10.1.1.**", "10.1.**.*", etc. will not work.
- **Protocol** to fetch protocol-specific activities.
- **Username** of the user performing the activity. You need to provide the exact Username to filter. Search with partial username, or partial username prefixed or suffixed with '*' will not work.
- **Noise Reduction** to filter files which are created in the last 2 hours by the user. It is also used to filter temporary files (for example, .tmp files) accessed by the user.

The following fields are subject to special filtering rules:

- **Entity Type**, using entity (file) extension

- **Path** of the entity
- **User** performing the activity
- **Device** (SVM) where entities reside
- **Volume** where entities reside
- The **Original Path** used for rename events when the original file was renamed.

The preceding fields are subject to the following when filtering:

- Exact value should be within quotes: Example: "searchtext"
- Wildcard strings must contain no quotes: Example: searchtext, *searchtext*, will filter for any strings containing ‘searchtext’.
- String with a prefix, Example: searchtext* , will search any strings which start with ‘searchtext’.

Sorting Forensic Activity History Data

You can sort activity history data by *Time, User, Source IP, Activity, Path* and *Entity Type*. By default, the table is sorted by descending *Time* order, meaning the latest data will be displayed first. Sorting is disabled for *Device* and *Protocol* fields.

Exporting All Activity

You can export the activity history to a .CSV file by clicking the *Export* button above the Activity History table. Note that only the top 10,000 records are exported.

Column Selection for All Activity

The *All activity* table shows select columns by default. To add, remove, or change the columns, click the gear icon on the right of the table and select from the list of available columns.

Activity History Retention

Activity history is retained for 13 months for active Workload Security environments.

Applicability of Filters in Forensics Page

Filter	What it does	Example	Applicable in Which Filters?	Not applicable for which filters	Result
* (Asterisk)	enables you to search for everything	Auto*03172022	User, PATH, Entity Type, Device Type, Volume, Original Path		returns all resources that start with “Auto" and end with “03172022”

? (question mark)	enables you to search for a specific number of characters	AutoSabotageUser1_03172022?	User, Entity Type, Device, Volume		returns AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225, and so on
OR	enables you to specify multiple entities	AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022	User, Domain, Username, PATH, Entity Type, Device, Original Path		returns any of AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022
NOT	allows you to exclude text from the search results	NOT AutoRansomUser4_03162022	User, Domain, Username, PATH, Entity Type, Original PATH, Volume	Device	returns everything that does not start with"AutoRansomUser4_03162022”
None	searches for NULL values in all fields	None	Domain		returns results where the target field is empty

Path / Original path Search

Search results with and without / will be different

/AutoDir1/AutoFile	Works
AutoDir1/AutoFile	Doesn’t work
/AutoDir1/AutoFile (Dir1)	Dir1 Partial substring doesn’t work
"/AutoDir1/AutoFile03242022"	Exact search works
Auto*03242022	Doesn’t work
AutoSabotageUser1_03172022?	Doesn’t work
/AutoDir1/AutoFile03242022 OR /AutoDir1/AutoFile03242022	Works
NOT /AutoDir1/AutoFile03242022	Works
NOT /AutoDir1	Works
NOT /AutoFile03242022	Doesn’t work
*	Shows all the entries

Troubleshooting

Problem	Try This

In the “All Activities” table, under the ‘User’ column, the user name is shown as: “ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” or "ldap:default:80038003”	Possible reasons could be: 1. No User Directory Collectors have been configured yet. To add one, go to **Admin > Data Collectors > User Directory Collectors** and click on **+User Directory Collector**. Choose *Active Directory* or *LDAP Directory Server*. 2. A User Directory Collector has been configured, however it has stopped or is in error state. Please go to **Admin > Data Collectors > User Directory Collectors** and check the status. Refer to the User Directory Collector troubleshooting section of the documentation for troubleshooting tips. After configuring properly, the name will get automatically resolved within 24 hours. If it still does not get resolved, check if you have added the correct User Data Collector. Make sure that the user is indeed part of the added Active Directory/LDAP Directory Server.
Some NFS events are not seen in UI.	Check the following: 1. A user directory collector for AD server with POSIX attributes set should be running with the unixid attribute enabled from UI. 2. Any user doing NFS access should be seen when searched in the user page from UI 3. Raw events (Events for whom the user is not yet discovered) are not supported for NFS 4. Anonymous access to the NFS export will not be monitored. 5. Make sure NFS version used in lesser than NFS4.1.

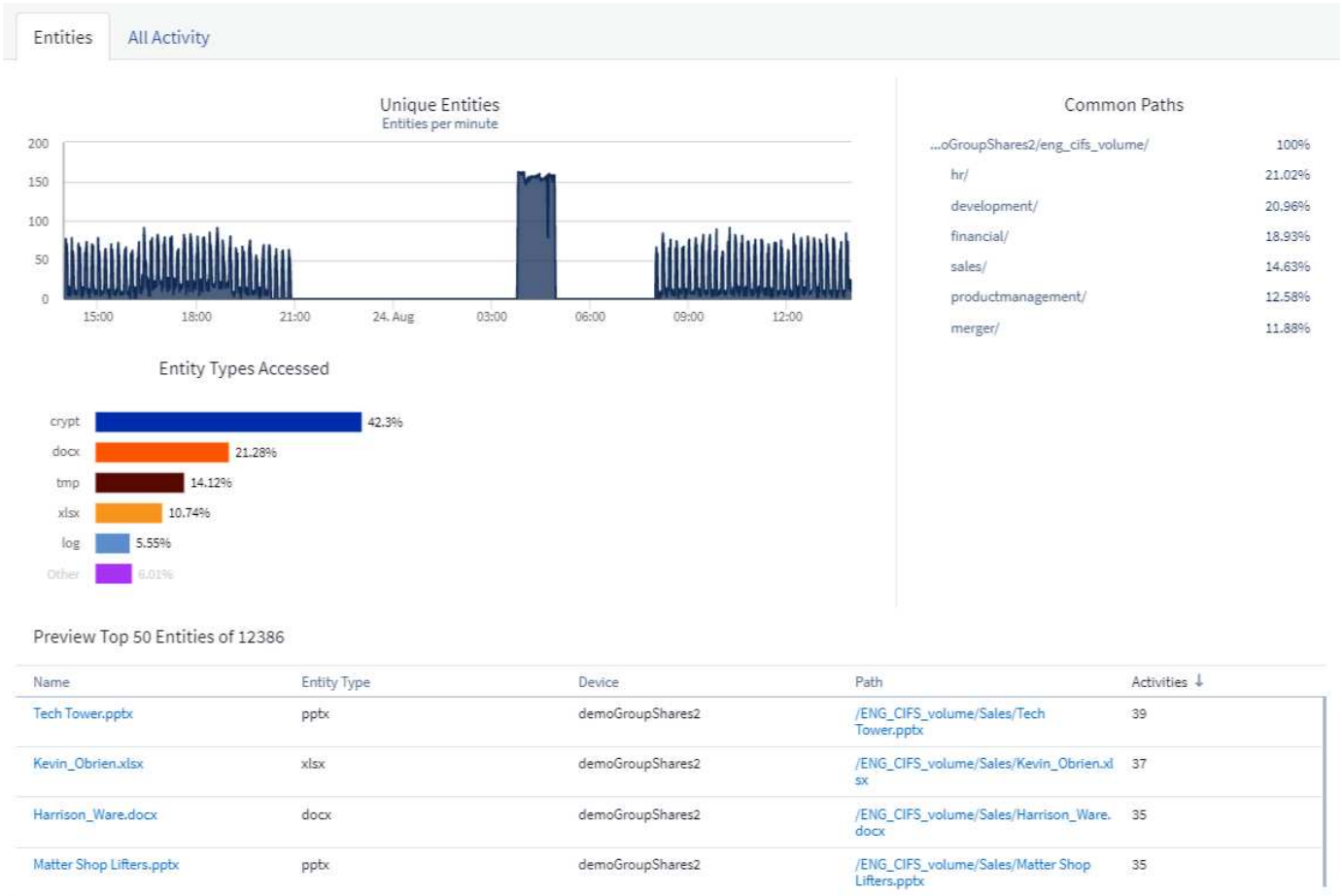
Forensic Entities Page

The Forensics Entities page provides detailed information about entity activity in your environment.

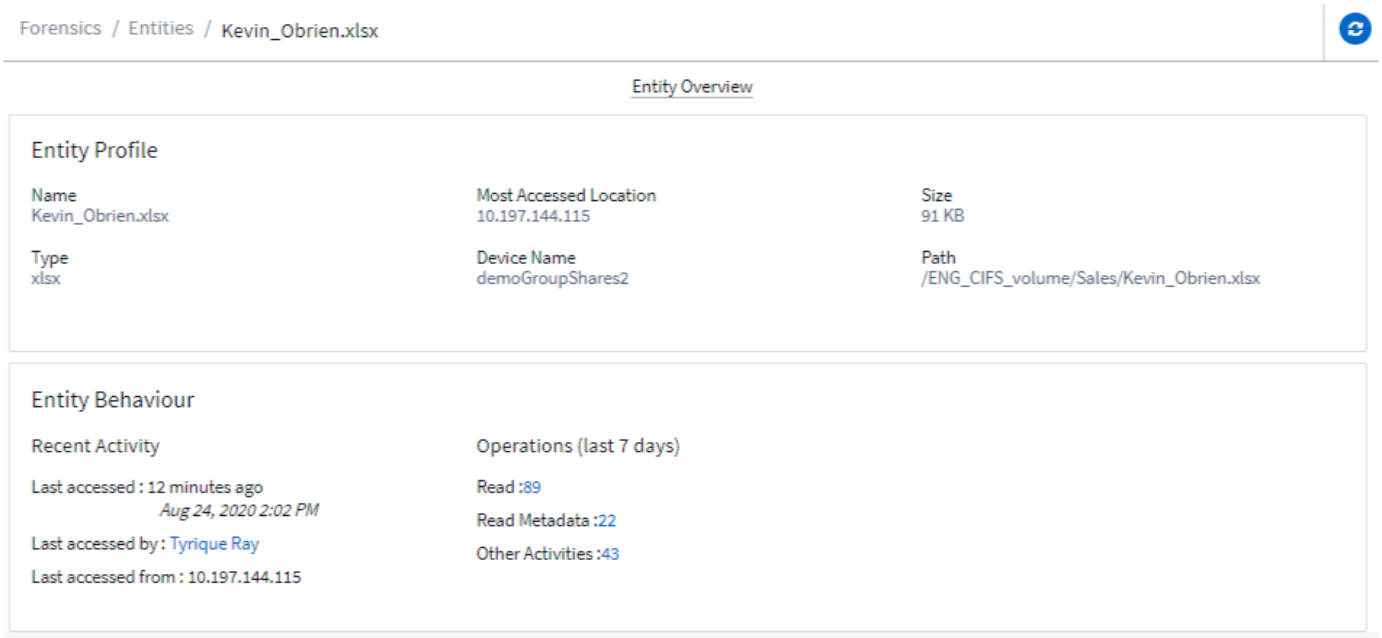
Examining Entity Information

Click **Forensics > Activity Forensics** and click the *Entities* tab to access the Entities page.

This page provides an overview of entity activity in your environment, highlighting the following information:
* A graph showing *Unique Entities* accessed per minute
* A chart of *Entity Types Accessed*
* A breakdown of the *Common Paths*
* A list of the *Top 50 Entities* out of the total number of entities



Clicking on an entity in the list opens an overview page for the entity, showing a profile of the entity with details like name, type, device name, most accessed location IP, and path, as well as the entity behavior such as the user, IP, and time the entity was last accessed.



Forensic User Overview

Information for each user is provided in the User Overview. Use these views to understand user characteristics, associated entities, and recent activities.

User Profile

User Profile information includes contact information and location of the user. The profile provides the following information:

- Name of the user
- Email address of the user
- User's Manager
- Phone contact for the user
- Location of the user

User Behavior

The user behavior information identifies recent activities and operations performed by the user. This information includes:

- Recent activity
  - Last access location
  - Activity graph
  - Alerts
- Operations for the last seven days
  - Number of operations

Refresh Interval

The User list is refreshed every 12 hours.

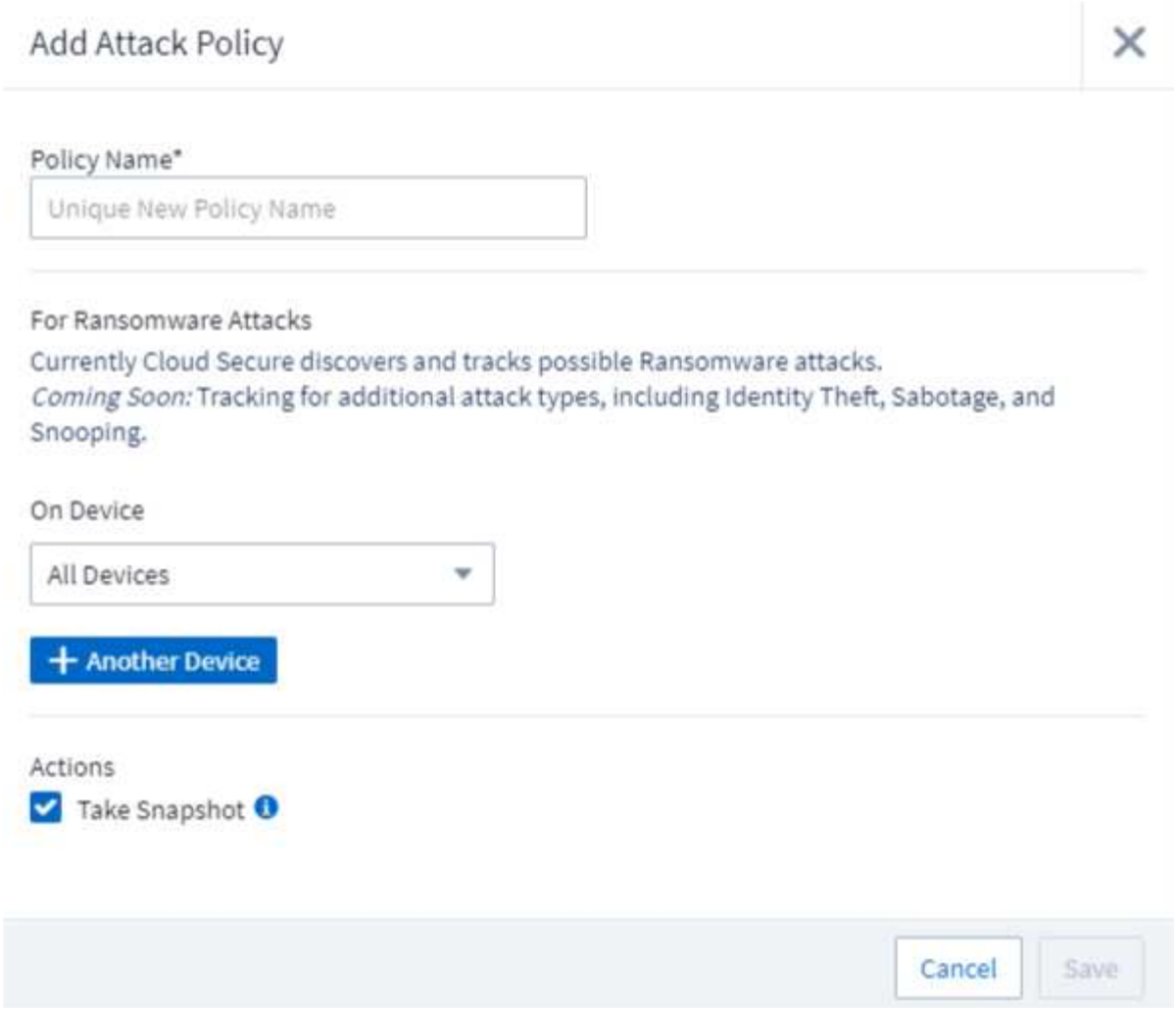
Retention Policy

If not refreshed again, the User list is retained for 13 months. After 13 months, the data will be deleted. If your Workload Security environment is deleted, all data associated with the environment is deleted.

Automated Response Policies

Response Policies trigger actions such as taking a snapshot or restricting user access in the event of an attack or abnormal user behavior.

You can set policies on specific devices or all devices. To set a response policy, select **Admin > Automated Response Policies** and click the appropriate *Policy button. You can create policies for Attacks or for Warnings.



You must save the policy with a unique name.

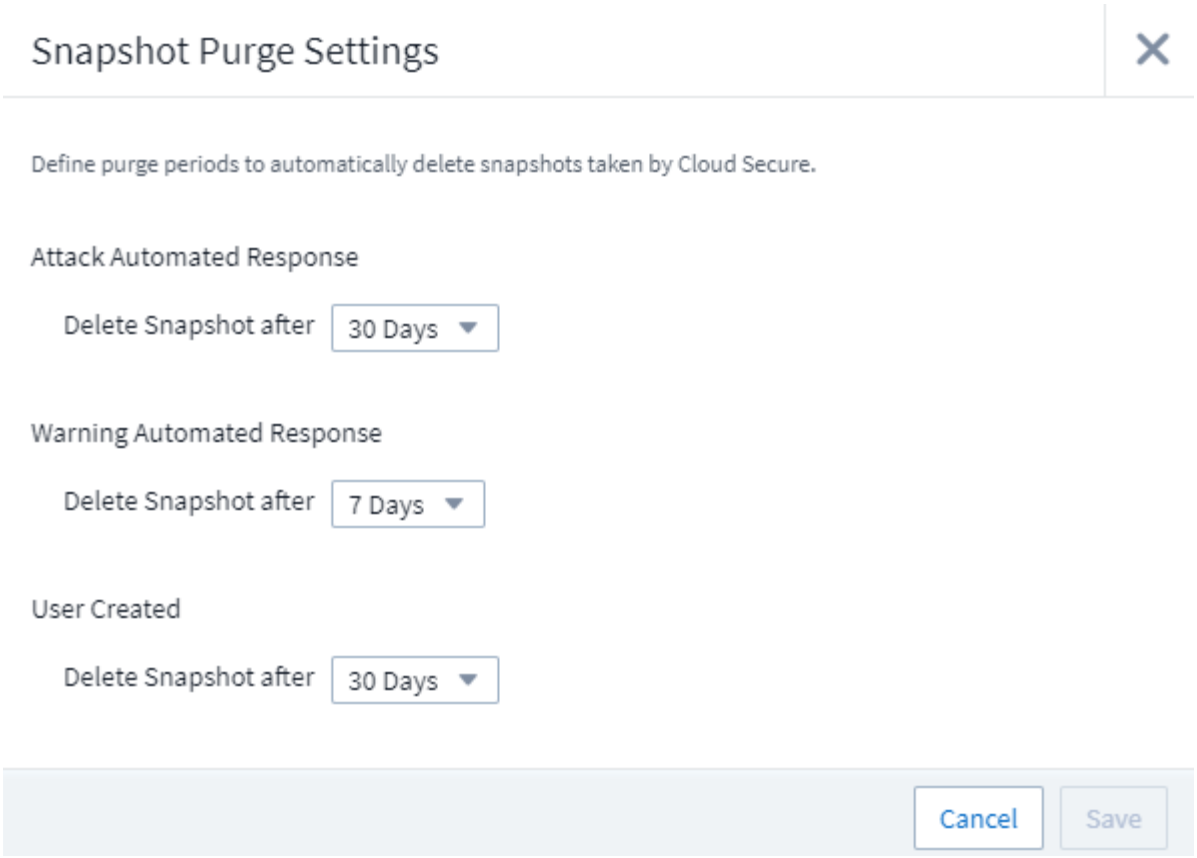
To disable an automated response action (for example, Take Snapshot), simply un-check the action and save the policy.

When an alert is triggered against the specified devices (or all devices, if selected), the automated response policy takes a snapshot of your data. You can see snapshot status on the Alert detail page.

See the Restrict User Access page for more details on restricting user access by IP.

You can modify or pause an Automated Response Policy by choosing the option in the policy's drop-down menu.

Workload Security will automatically delete snapshots once per day based on the Snapshot Purge settings.



Integration with ONTAP Autonomous Ransomware Protection

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.

Additional details and license requirements about ARP can be found here.

Workload Security integrates with ONTAP to receive ARP events and provide an additional analytics and automatic responses layer.

Workload Security receives the ARP events from ONTAP and takes the following actions:

1. Correlates volume encryption events with user activity to identify who is causing the damage.
2. Implements automatic response policies (if defined)
3. Provides forensics capabilities:
    - Allow customers to conduct data breach investigations.
    - Identify what files were affected, helping to recover faster and conduct data breach investigations.

Prerequisites

1. Minimum ONTAP version: 9.11.1
2. ARP enabled volumes. Details on enabling ARP can be found here. ARP must be enabled via

OnCommand System Manager. Workload Security cannot enable ARP.

3. Workload Security collector should be added via cluster IP.
4. Cluster level credentials are needed for this feature to work. In other words, cluster level credentials must be used when adding the SVM.

User permissions required

If you are using cluster administration credentials, no new permissions are needed.

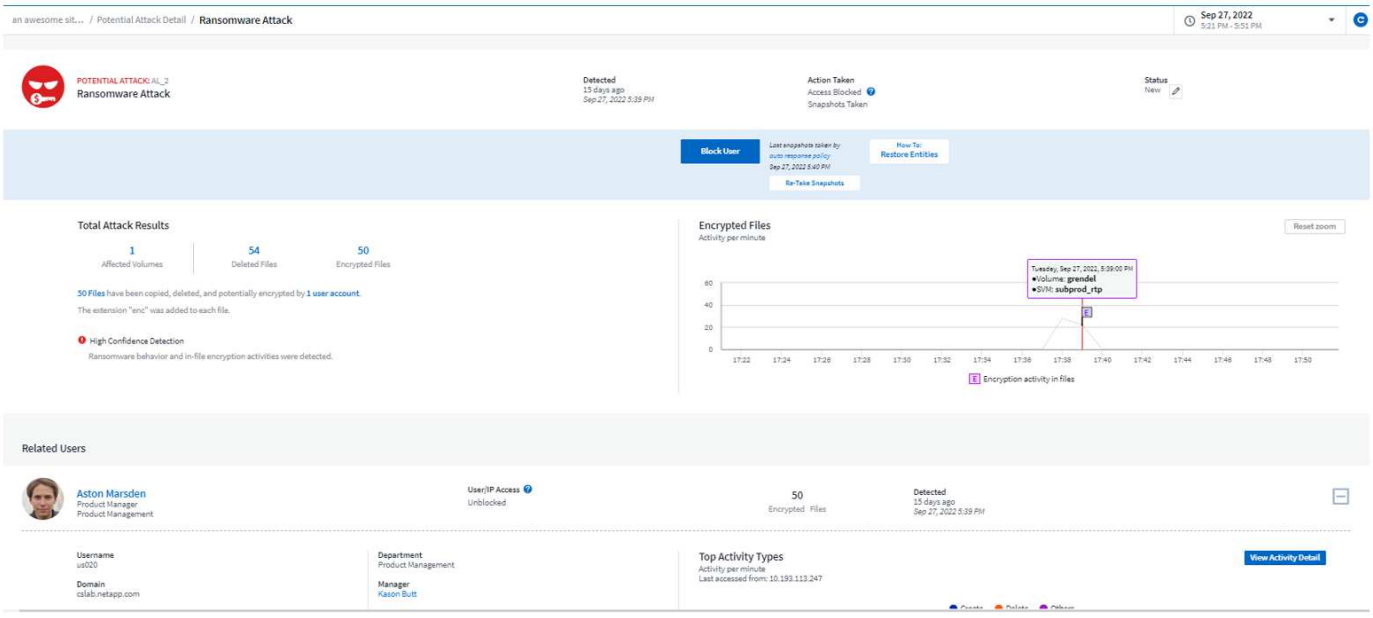
If you are using a custom user (for example, *csuser*) with permissions given to the user, then follow the steps below to give permissions to Workload Security to collect ARP related information from ONTAP.

For *csuser* with cluster credentials, do the following from the ONTAP command line:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Sample Alert

A sample alert generated due to ARP event is shown below:



A high confidence banner indicates the attack has shown ransomware behavior along with file encryption activities.
The encrypted files graph indicates the timestamp at which the volume encryption activity was detected by the ARP solution.

Limitations

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 and displayed by Workload Security. However, Forensic information related to the alert, as well as user mapping, will not be captured or shown.

Troubleshooting

Known problems and their resolutions are described in the following table.

Problem:	Resolution:
Email alerts are received 24 hrs after an attack is detected. In the UI, the alerts are shown 24 hrs before that when the emails are received by Cloud Insights Workload Security.	When ONTAP sends the *Ransomware Detected* Event to Cloud Insights Workload Security (i.e. Workload Security), the email is sent. The Event contains a list of attacks and its timestamps. The Workload Security UI displays the alert timestamp of the first file attacked. ONTAP sends the *Ransomware Detected* Event to Cloud Insights when a certain number of files are encoded. Therefore, there may be a difference between the time the alert is displayed in the UI and the time the email is sent.

Blocking User Access

Once an attack is detected, Workload Security can stop the attack by blocking user access to the file system. Access can be blocked automatically, using Automated Response Policies or manually from the alert or user details pages.

When blocking user access, you should define a blocking time period. After the selected time period ends, user access is automatically restored.
Access blocking is supported for both SMB and NFS protocols.

User is directly blocked for SMB and IP address of the host machines causing the attack will be blocked for NFS. Those machine IP addresses will be blocked from accessing any of the Storage Virtual Machines (SVMs) monitored by Workload Security.

For example, let's say Workload Security manages 10 SVMs and the Automatic Response Policy is configured for four of those SVMs. If the attack originates in one of the four SVMs, the user's access will be blocked in all 10 SVMs. A Snapshot is still taken on the originating SVM.

If there are four SVMs with one SVM configured for SMB, one configured for NFS, and the remaining two configured for both NFS and SMB, all the SVMs will be blocked if the attack originates in any of the four SVMs.

Prerequisites for User Access Blocking

Cluster level credentials are needed for this feature to work.

If you are using cluster administration credentials, no new permissions are needed.

If you are using a custom user (for example, *csuser*) with permissions given to the user, then follow the steps below to give permissions to Workload Security to block user.

For csuser with cluster credentials, do the following from the ONTAP command line:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

How to enable the feature?

- In Workload Security, navigate to **Admin > Automated Response Policies > Response Policy Settings > Block User Access**.
- Set “Enable Block User Access” to *enabled*.

How to set up Automatic user access blocking?

- Create a new Attack Policy or edit an existing Attack policy.
- Select the SVMs on which the attack policy should be monitored.
- Click on the checkbox “Block User File Access”. The feature will be enabled when this is selected.
- Under “Time Period” select the time until which the blocking should be applied.
- To test automatic user blocking,, you can simulate an attack via a simulated script.

How to know if there are blocked users in the system?

- In the alert lists page, a banner on the top of screen will be displayed in case any user is blocked.
- Clicking on the banner will take you to the “Users” page, where the list of blocked users can be seen.
- In the “Users” page, there in a column named “User/IP Access”. In that column, the current state of user blocking will be displayed.

Restrict and manage user access manually

- You can go to the alert details or user details screen and then manually block or restore a user from those screens.

User Access Limitation History

In the alert details and user details page, in the user panel, you can view an audit of the user’s access limitation history: Time, Action (Block, Unblock), duration, action taken by, manual/automatic, and affected IPs for NFS.

How to disable the feature?

At any time, you can disable the feature. If there are restricted users in the system, you must restore their access first.

- In Workload Security, navigate to **Admin > Automated Response Policies > Response Policy Settings > Block User Access**
- De-select “Enable Block User Access” to disable.

The feature will be hidden from all pages.

Manually Restore IPs for NFS

Use the following steps to manually restore any IPs from ONTAP if your Workload Security trial expires, or if the agent/collector is down.

1. List all export policies on an SVM.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Delete the rules across all policies on the SVM which have “cloudsecure_rule” as Client Match by specifying its respective RuleIndex. Workload Security rule will usually be at 1.

```
contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
```

3. Ensure Workload Security rule is deleted (optional step to confirm).

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Manually Restore Users for SMB

Use the following steps to manually restore any users from ONTAP if your Workload Security trial expires, or if the agent/collector is down.

You can get the list of users blocked in Workload Security from the users list page.

1. Login to the ONTAP cluster (where you want to unblock users) with cluster *admin* credentials. (For Amazon FSx, login with FSx credentials).
2. Run the following command to list all users blocked by Workload Security for SMB in all SVMs:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

In the above output, 2 users were blocked (US030, US040) with domain CSLAB.

1. Once we identify the position from the above output, run the following command to unblock the user:

```
vserver name-mapping delete -direction win-unix -position <position>
```

2. Confirm the users are unblocked by running the command:

```
vserver name-mapping show -direction win-unix -replacement " "
```

No entries should be displayed for the users previously blocked.

Troubleshooting

Problem	Try This
Some of the users are not getting restricted, though there is an attack.	1. Make sure that the Data Collector and Agent for the SVMs are in *Running* state. Workload Security won't be able to send commands if the Data Collector and Agent are stopped. 2. This is because the user may have accessed the storage from a machine with a new IP which has not been used before. Restricting happens via IP address of the host through which the user is accessing the storage. Check in the UI (Alert Details > Access Limitation History for This User > Affected IPs) for the list of IP addresses which are restricted. If the user is accessing storage from a host which has an IP different from the restricted IPs, then the user will still be able to access the storage through the non-restricted IP. If the user is trying to access from the hosts whose IPs are restricted, then the storage won't be accessible.
Manually clicking on Restrict Access gives "IP addresses of this user have already been restricted".	The IP to be restricted is already being restricted from another user.
Policy could not be modified. Reason: not authorized for that command.	Check if using csuser, permissions are given to the user as mentioned above.

Problem	Try This
User (IP Address) blocking for NFS works, but for SMB / CIFS, I see an error message: “SID to DomainName transformation failed. Reason timeout: socket is not established”	This can happen is *csuser* does not have permission to perform ssh. (Ensure connection at cluster level, then ensure user can perform ssh). *csuser* role requires these permissions. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking For *csuser* with cluster credentials, do the following from the ONTAP command line: security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all If *csuser* is not used and if admin user at cluster level is used, make sure that the admin user has ssh permission to ONTAP.

Workload Security: Simulating an Attack

You can use the instructions on this page to simulate an attack for testing or demonstrating Workload Security using the included Ransomware Simulation script.

Things to note before you begin

- The ransomware simulation script works on Linux only.
- The script is provided with the Workload Security agent installation files. It is available on any machine that has a Workload Security agent installed.
- You can run the script on the Workload Security agent machine itself; there is no need to prepare another Linux machine. However, if you prefer to run the script on another system, simply copy the script and run it there.

Have at least 1,000 sample files

This script should run on an SVM with a folder that has files to encrypt. We recommend having at least 1,000 files within that folder and any sub-folders. The files must not be empty.
Do not create the files and encrypt them using the same user. Workload Security considers this a low-risk activity and will therefore not generate an alert (i.e. the same user modifies files he/she/they just created).

See below for instructions to programmatically create non-empty files.

Guidelines before you run the simulator:

1. Make sure encrypted files are not empty.
2. Make sure you encrypt > 50 files. A small number of files will be ignored.
3. Do not run an attack with the same user multiple times. After a few times, CS will learn this user behavior and assume it is the user's normal behavior.
4. Do not encrypt files the same user has just created. Changing a file that was just created by a user is not considered a risky activity. Instead, use files created by another user OR wait for a few hours between creating the files and encrypting them.

Prepare the system

First, mount the target volume to machine. You can mount either an NFS mount or CIFs export.

To mount NFS export in Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Do not mount NFS version 4.1; it is not supported by Fpolicy.

To mount CIFs in Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

Next, set up a Data Collector:

1. Configure the Workload Security agent if not already done.
2. Configure SVM data collector if not already done.

Run the Ransomware Simulator script

1. Log in (ssh) to the Workload Security agent machine.
2. Navigate to: */opt/netapp/cloudsecure/agent/install*
3. Call the simulator script without parameters to see usage:

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

Encrypt your test files

To encrypt the files, run the following command:

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

Restore files

To decrypt, run the following command:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

Run the script multiple times

After generating a ransomware attack for a user, switch to another user in order to generate an additional attack.
Workload Security learns user behavior and will not alert on repeated ransomware attacks within a short

duration for the same user.

Create files programmatically

Before creating the files, you must first stop the data collector processing.
Perform the steps below before you add the data collector to the Agent. If you have already added the data collector, just edit the data collector, enter an invalid password, and save it. This will temporarily put the data collector in error state. NOTE: Be sure you note the original password!

Before running the simulation, you must first add files to be encrypted. You can either manually copy the files to be encrypted into the target folder, or use a script (see the example below) to programmatically create the files. Whichever method you use, copy at least 1,000 files.

If you choose to programmatically create the files, do the following:

1. Log into the Agent box.
2. Mount an NFS export from the SVM of the filer to the Agent machine. Cd to that folder.
3. In that folder create a file named createfiles.sh
4. Copy the following lines to that file.

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Save the file.
6. Ensure execute permission on the file:

```
chmod 777 ./createfiles.sh
```

7. Execute the script:

```
./createfiles.sh
```

   1000 files will be created in the current folder.

8. Re-enable the data collector

   If you disabled the data collector in step 1, edit the data collector, enter the correct password, and save. Make sure that the data collector is back in running state.

Configuring Email Notifications for Alerts, Warnings, and Agent/Data Source Collector health

To configure Workload Security alert recipients, click on **Admin > Notifications** and enter an email addresses in the appropriate section(s) for each recipient.

Potential Attack Alerts and Warnings

To send *Potential Attack* alert notifications, enter the recipients' email addresses in the *Send Potential Attack Alerts* section.
Email notifications are sent to the alert recipient list for every action on the alert.

To send *Warning* notifications, enter the recipients' email addresses in the *Send Warning Alerts* section.

Agent and Data Collector Health monitoring

You can monitor the health of Agents and Data Sources through notifications.

In order to receive notifications in the event that an Agent or Data Source collector is not functioning, enter the email addresses of the recipients in the *Data Collection Health Alerts* section.

Keep the following in mind:

- Health alerts will be sent only after the agent/collector stops reporting for at least one hour.
- Only one email notification is sent to the intended recipients in a given 24 hour period, even If the Agent or Data collector is disconnected for a longer duration.
- In case of an Agent failure, one alert will be sent (not one per collector). The email will include a list of all impacted SVMs.
- Active directory collection failure is reported as a warning; it does not impact Ransomware detection.
- The Getting Started setup list now includes a new *Configure email notifications* phase.

Workload Security API

The Workload Security API enables NetApp customers and independent software vendors (ISVs) to integrate Workload Security with other applications, such as CMDB’s or other ticketing systems.

Requirements for API Access:

- An API Access Token model is used to grant access.
- API Token management is performed by Workload Security users with the Administrator role.

API Documentation (Swagger)

The latest API information is found by logging in to Workload Security and navigating to **Admin > API Access**.
Click the **API Documentation** link.
The API Documentation is Swagger-based, which provides a brief description and usage information for the API and allows you to try it out in your environment.

API Access Tokens

Before using the Workload Security API, you must create one or more **API Access Tokens**. Access tokens grant read permissions. You can also set the expiration for each access token.

To create an Access Token:

- Click **Admin > API Access**
- Click **+API Access Token**
- Enter **Token Name**
- Specify **Token Expiration**

> Your token will only be available for copying to the clipboard and saving during the creation process. Tokens can not be retrieved after they are created, so it is highly recommended to copy the token and save it in a secure location. You will be prompted to click the Copy API Access Token button before you can close the token creation screen.

You can disable, enable, and revoke tokens. Tokens that are disabled can be enabled.

Tokens grant general purpose access to APIs from a customer perspective, managing access to APIs in the scope of their own environment.

The application receives an Access Token after a user successfully authenticates and authorizes access, then passes the Access Token as a credential when it calls the target API. The passed token informs the API that the bearer of the token has been authorized to access the API and perform specific actions based on the scope that was granted during authorization.

The HTTP header where the Access Token is passed is **X-CloudInsights-ApiKey:**

For example, use the following to retrieve storages assets:

```
curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
```

Where *<API_Access_Token>* is the token you saved during API access key creation.

Detailed information can be found in the *API Documentation* link under **Admin > API Access**.

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.