# Getting Started

## Data Infrastructure Insights

NetApp
January 17, 2025

# Table of Contents

# 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<br><br>Add Agent<br><br>**Video**: Agent Deployment |
| Configure a User Directory Connector | Add User Directory Connector<br><br>**Video**: Active Directory Connection |
| Configure data collectors | Click **Workload Security > Collectors**<br><br>Click the data collector you want to configure.<br><br>See the Data Collector Vendor Reference section of the documentation.<br><br>**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:<br><br>* CentOS 8 Stream (64-bit), CentOS 9 Stream, SELinux<br>* OpenSUSE Leap 15.3 through 15.5 (64-bit)<br>* Oracle Linux 8.6 - 8.8, 9.1 through 9.4 (64-bit)<br>* Red Hat Enterprise Linux 8.6 through 8.8, 9.1 through 9.4 (64-bit), SELinux<br>* Rocky 9.2 - 9.4 (64-bit), SELinux<br>* SUSE Linux Enterprise Server 15 SP3 through 15 SP5 (64-bit)<br>* Ubuntu 20.04 LTS, 22.04 LTS, and 24,04 LTS (64-bit)<br>* Debian 10 and 11 (64-bit)<br>* AlmaLinux 9.3 and 9,4 (64-bit)<br><br>This computer should be running no other application-level software. A dedicated server is recommended. |
| 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 |
| Available disk space | Disk space should be allocated in this manner:<br>/opt/netapp 36 GB (minimum 35 GB free space after filesystem creation)<br><br>Note: It is recommended to allocate a little extra disk space to allow for the creation of the filesystem. Ensure that there is at least 35 GB free space in the filesystem.<br><br>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 Data Infrastructure 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<br>For Linux, disk space should be allocated in this manner:<br>/opt/netapp 25-30 GB<br>/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 | Source | Destination | Description |
|---|---|---|---|---|
| TCP | 443 | Workload Security Agent | <site_name>.cs01.cloudinsights.netapp.com<br><site_name>.c01.cloudinsights.netapp.com<br><site_name>.c02.cloudinsights.netapp.com | Access to Data Infrastructure Insights |
| TCP | 443 | Workload Security Agent | gateway.c01.cloudinsights.netapp.com<br>agentlogin.cs01.cloudinsights.netapp.com | Access to authentication services |

For **Europe-based** Workload Security environments:

| Protocol | Port | Source | Destination | Description |
|---|---|---|---|---|
| TCP | 443 | Workload Security Agent | <site_name>.cs01-eu-1.cloudinsights.netapp.com<br><site_name>.c01-eu-1.cloudinsights.netapp.com<br><site_name>.c02-eu-1.cloudinsights.netapp.com | Access to Data Infrastructure Insights |
| TCP | 443 | Workload Security Agent | gateway.c01.cloudinsights.netapp.com<br>agentlogin.cs01-eu-1.cloudinsights.netapp.com | Access to authentication services |

For **APAC-based** Workload Security environments:

| Protocol | Port | Source | Destination | Description |
|---|---|---|---|---|
| TCP | 443 | Workload Security Agent | <site_name>.cs01-ap-1.cloudinsights.netapp.com<br><site_name>.c01-ap-1.cloudinsights.netapp.com<br><site_name>.c02-ap-1.cloudinsights.netapp.com | Access to Data Infrastructure Insights |
| TCP | 443 | Workload Security Agent | gateway.c01.cloudinsights.netapp.com<br>agentlogin.cs01-ap-1.cloudinsights.netapp.com | Access to authentication services |

## In-network rules

| Protocol | Port | Source | Destination | Description |
|---|---|---|---|---|
| TCP | 389(LDAP)<br>636 (LDAPs / start-tls) | Workload Security Agent | LDAP Server URL | Connect to LDAP |
| TCP | 443 | Workload Security Agent | Cluster or SVM Management IP Address (depending on SVM collector configuration) | API communication with ONTAP |

| Protocol | Port | Source | Destination | Description |
|---|---|---|---|---|
| TCP | 35000 - 55000 | SVM data LIF IP Addresses | Workload Security Agent | Communication from ONTAP to the Workload Security Agent for Fpolicy events. These ports must be opened towards the Workload Security Agent in order for ONTAP to send events to it, including any firewall on the Workload Security Agent itself (if present).<br><br>NOTE that you do not need to reserve **all** of these ports, but the ports you reserve for this must be within this range. It is recommended to start by reserving ~100 ports, and increasing if necessary. |
| TCP | 7 | Workload Security Agent | SVM data LIF IP Addresses | Echo from Agent to SVM Data LIFs |
| SSH | 22 | Workload Security Agent | Cluster management | Needed for CIFS/SMB user blocking. |

### 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 on your tenant 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

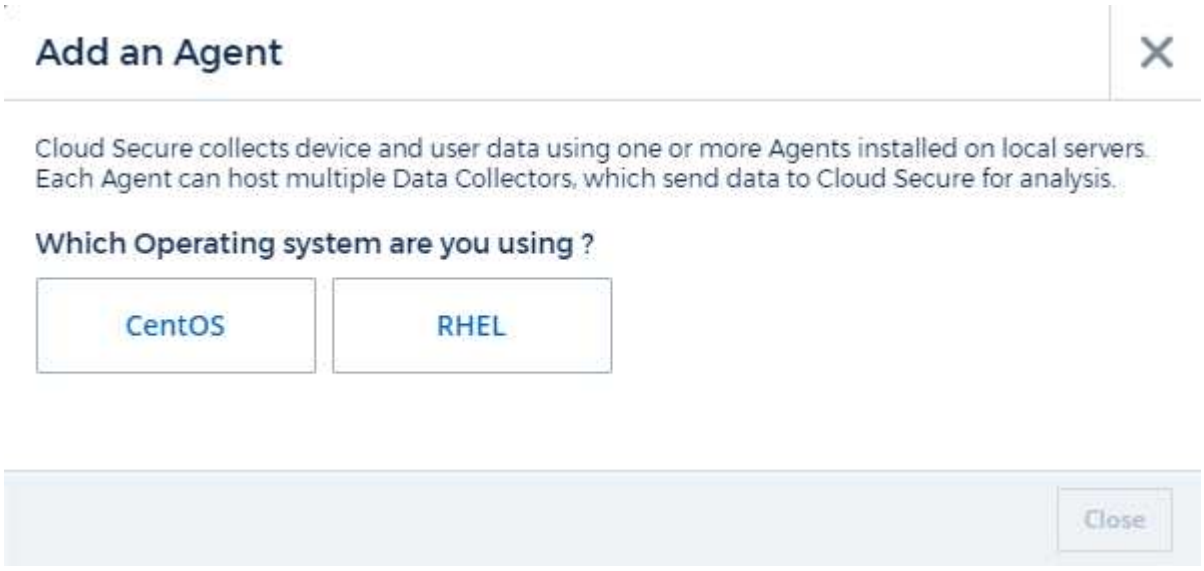
permission settings do not allow creation of a local user, and instead require Active Directory, a user with the username *cssys* must be created in the Active Directory server.

- You can read about Data Infrastructure Insights security here.

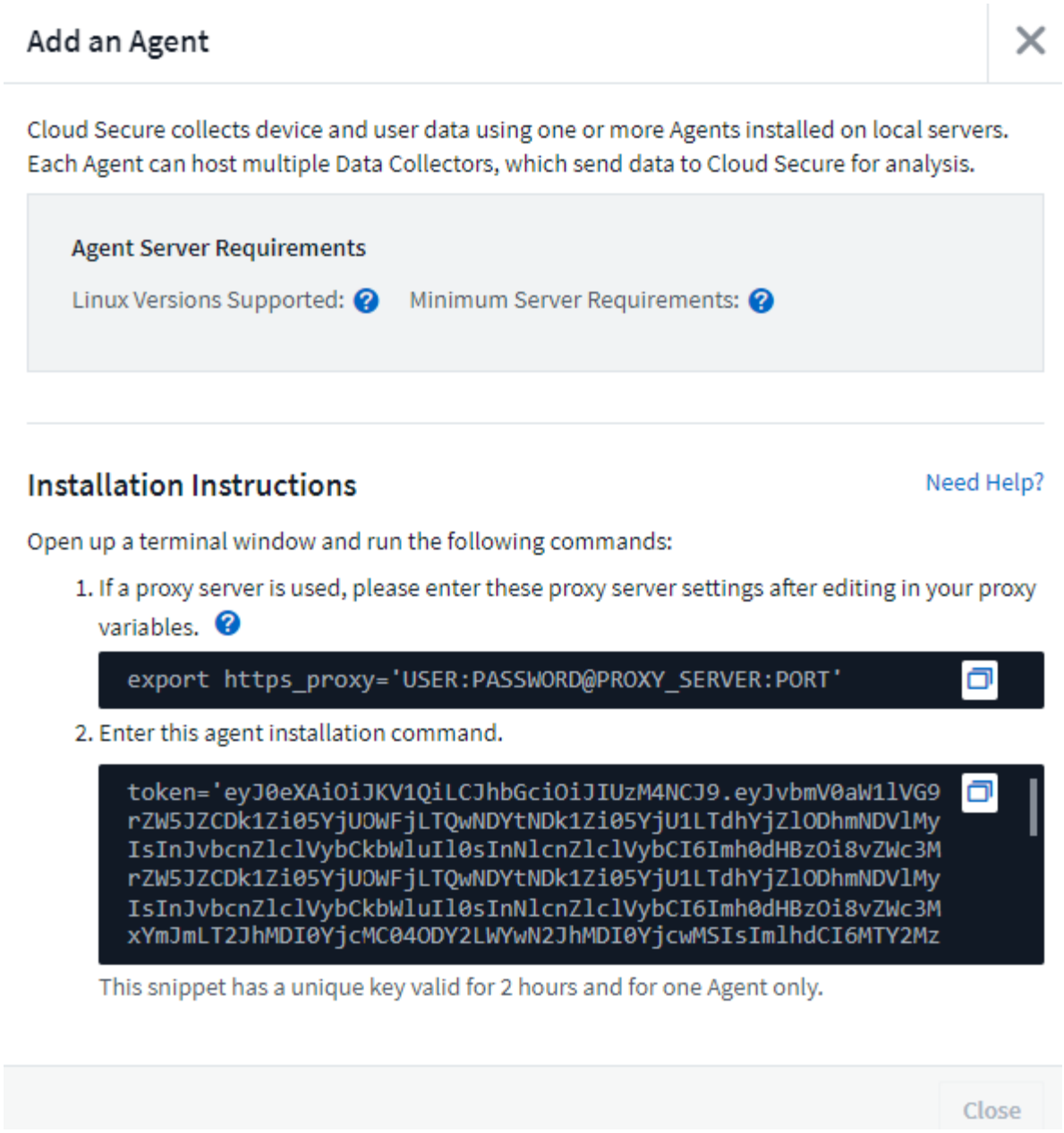
## Steps to Install Agent

1. Log in as Administrator or Account Owner to your Workload Security environment.
2. Select **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
```

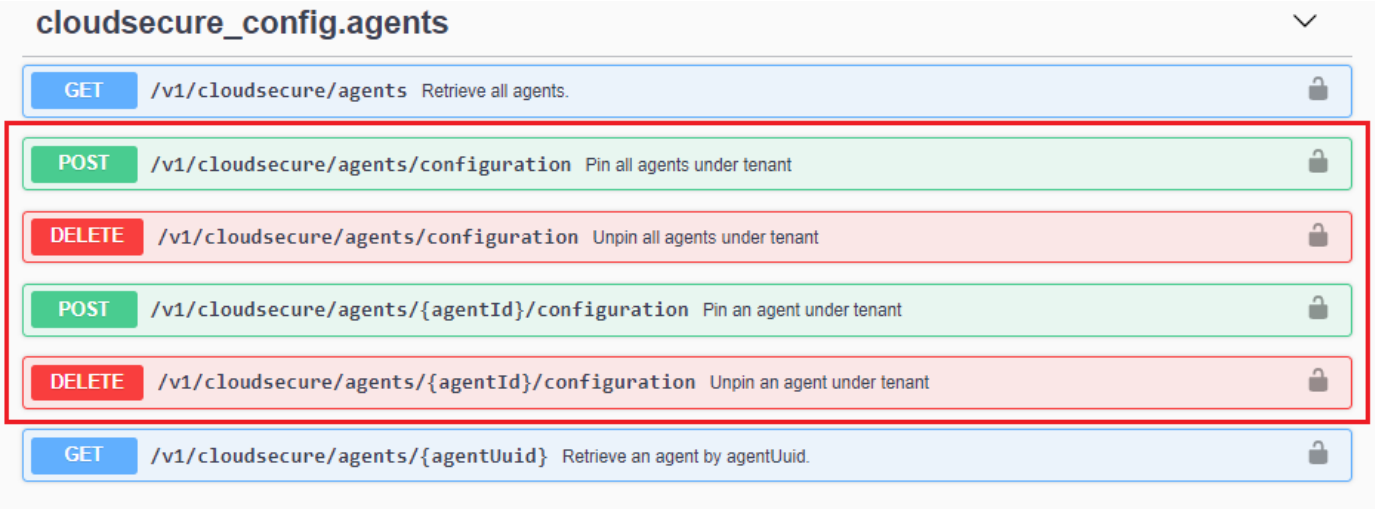
## "Pinning" an Agent at the current version

By default, Data Infrastructure Insights Workload Security updates agents automatically. Some customers may wish to pause automatic updating, which leaves an Agent at its current version until one of the following occurs:

- The customer resumes automatic Agent updates.
- 30 days have passed. Note that the 30 days starts on the day of the most recent Agent update, not at the day the Agent is paused.

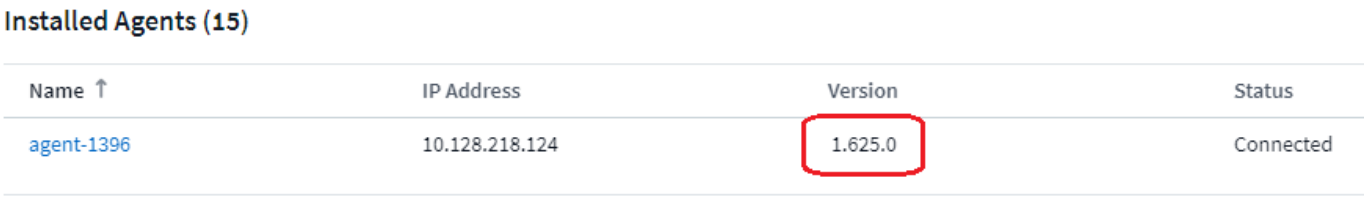
In each of these cases, the agent will be updated at the next Workload Security refresh.

To pause or resume automatic agent updates, use the *cloudsecure_config.agents* APIs:




Note that it may take up to five minutes for the pause or resume action to take effect.

You can view your current Agent versions on the **Workload Security > Collectors** page, in the **Agents** tab.




## 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.<br>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.<br>est |
| 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. |
| 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.<br>After that, re-copy the command from the Agent installation UI and paste it in the CLI to execute the installation again. |

| Problem: | Resolution: |
| --- | --- |
| 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`.<br>1. Check if the logs shows a message“Failed to start Workload Security daemon service” .<br>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.<br>`sudo id cssys`<br>`sudo groups cssys`<br>3. If none exists, then a centralized monitoring policy may have deleted the cssys user.<br>4. Create cssys user and group manually by executing the following commands.<br>`sudo useradd cssys`<br>`sudo groupadd cssys`<br>5. Restart the agent service after that by executing the following command:<br>`sudo systemctl restart cloudsecure-agent.service`<br>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.<br>1. SSH to the Agent machine.<br>2. Restart the agent service after that by executing the following command:<br>`sudo systemctl restart cloudsecure-agent.service`<br>3. Check the status of the agent service via `sudo systemctl status cloudsecure-agent.service`.<br>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.<br>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.<br><br>1. Create a new directory named “cloudsecure”.<br>2. Go to that directory.<br>3. Copy and paste the full “token=…… … ./cloudsecure-agent-install.sh" installation command and press enter.<br>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 Data Infrastructure Insights serial number to open a case, and attach logs to the case as noted. | To attach logs to the case:<br>1. Execute the following script with root permission and share the output file (cloudsecure-agent-symptoms.zip).<br>a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh<br>2. Execute the following commands one by one with root permission and share the output.<br>a. id cssys<br>b. groups cssys<br>c. cat /etc/os-release |
| The cloudsecure-agent-symptom-collector.sh script fails with the following error.<br><br>[root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh<br>Collecting service log<br>Collecting application logs<br>Collecting agent configurations<br>Taking service status snapshot<br>Taking agent directory structure snapshot<br>…….<br>…….<br>/opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: line 52: zip: command not found<br>ERROR: Failed to create /tmp/cloudsecure-agent-symptoms.zip | Zip tool is not installed..<br>Install the zip tool by running the command “yum install zip”.<br>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.<br><br>The workaround would be to create cssys user and add its login directory manually using the following command:<br><br>*sudo useradd user_name -m -d HOME_DIR*<br><br>-m :Create the user's home directory if it does not exist.<br>-d : The new user is created using HOME_DIR as the value for the user's login directory.<br><br>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.<br>*Systemctl status cloudsecure-agent.service* shows the following:<br><br>[root@demo ~]# systemctl status cloudsecure-agent.service<br>agent.service – Workload Security Agent Daemon Service<br>Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: disabled)<br>Active: activating (auto-restart) (Result: exit-code) since Tue 2021-08-03 21:12:26 PDT; 2s ago<br>Process: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (code=exited status=126)<br>Main PID: 25889 (code=exited, status=126),<br><br>Aug 03 21:12:26 demo systemd[1]: cloudsecure-agent.service: main process exited, code=exited, status=126/n/a<br>Aug 03 21:12:26 demo systemd[1]: Unit cloudsecure-agent.service entered failed state.<br>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.<br><br>If /opt/netapp is an NFS mount and if *cssys* user does not have access to this folder, installation will fail.<br>*cssys* is a local user created by the Workload Security installer that may not have permission to access the mounted share.<br><br>You can check this by attempting to access /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent using *cssys* user.<br>If it returns "Permission denied", installation permission is not present.<br><br>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:<br><br>1. Change to the folder containing the properties file:<br><br>cd /opt/netapp/cloudsecure/conf<br><br>2. Using your favorite text editor, open the *agent.properties* file for editing.<br><br>3. Add or modify the following lines:<br><br>AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com<br>AGENT_PROXY_PORT=80<br>AGENT_PROXY_USER=pxuser<br>AGENT_PROXY_PASSWORD=pass1234<br><br>4. Save the file.<br><br>5. Restart the agent:<br><br>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 **Workload Security > 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 Data Infrastructure 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:
   **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.<br>Forest name allows both of the following formats:<br><br>*x.y.z* ⇒ direct domain name as you have it on your SVM. [Example: hq.companyname.com]<br><br>*DC=x,DC=y,DC=z* ⇒ Relative distinguished names [Example: DC=hq,DC= companyname,DC=com]<br><br>Or you can specify as the following:<br><br>*OU=engineering,DC=hq,DC= companyname,DC=com* [to filter by specific OU engineering]<br><br>*CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [to get only specific user with <username> from OU <engineering>]<br><br>*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]<br><br>Trusted Active Directory domains are also supported. |
| Bind DN | User permitted to search the directory. For example: *username@companyname.com* or *username@domainname.com*<br>In addition, Domain Read Only permission is required. User must be a member of the Security group *Read-only Domain Controllers*. |
| 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 |

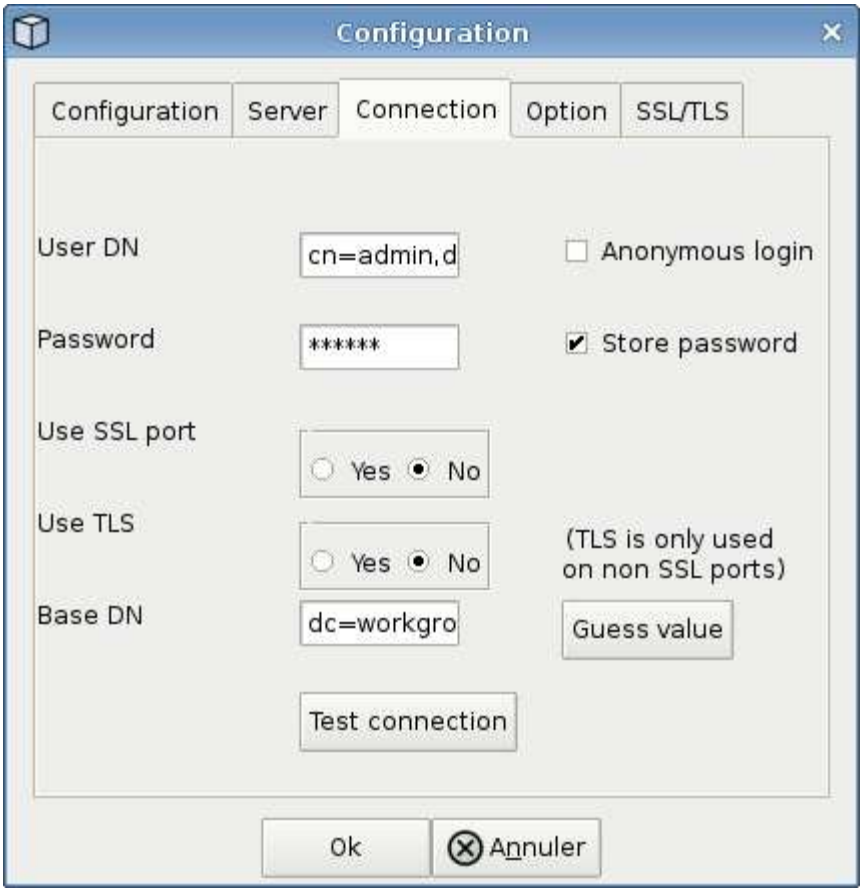
## Testing Your User Directory Collector Configuration

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).<br>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<br><br>//// |
| While adding LDAP directory the following error is shown:<br>“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.<br>//// |
| 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.<br>Or<br>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.<br><br>1. Edit the particular Active Directory collector which is fetching the user’s information from Active Directory.<br>2. Notice under optional attributes, there is a field name “Telephone Number” mapped to Active Directory attribute ‘telephonenumber’.<br>4. Now, please use the Active Directory Explorer tool as described above to browse the LDAP Directory server and see the correct attribute name.<br>3. Make sure that in LDAP Directory there is an attribute named ‘telephonenumber’ which has indeed the telephone number of the user.<br>5. Let us say in LDAP Directory it has been modified to ‘phonenumber’.<br>6. Then Edit the CloudSecure User Directory collector. In optional attribute section, replace ‘telephonenumber’ with ‘phonenumber’.<br>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.<br>Once the user detail is fetched it will be there for 13 months.<br>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 greater than 9.13.1.
  - SMB protocol version 3.1 and earlier.
  - NFS versions up to and including NFS 4.1 with ONTAP 9.15.1 or later.

- 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.
- • ONTAP Persistent Store is supported from 9.14.1.
- 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.

## Prerequisites for User Access Blocking

Keep the following in mind 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
```

## 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
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
security login create -user-or-group-name csuser -application http
-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>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

**Protobuf Mode**

Workload Security will configure the FPolicy engine in protobuf mode when this option is enabled in the collector's *Advanced Configuration* settings. Protobuf mode is supported in ONTAP version 9.15 and later.

More details on this feature can be found in the ONTAP documentation.

Specific permissions are required for protobuf (some or all of these may already exist):

Cluster mode:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Vserver mode:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

**Permissions for ONTAP Autonomous Ransomware Protection and ONTAP Access Denied**

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 more information, read about Integration with ONTAP Access Denied

and Integration with ONTAP Autonomous Ransomware Protection

## Configure the data collector

**Steps for Configuration**

1. Log in as Administrator or Account Owner to your Data Infrastructure Insights environment.
2. Click **Workload Security > 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<br>When adding via Cluster IP the options are:<br>1. Cluster-admin<br>2. ‘csuser’<br>3. AD-user having similar role as csuser.<br>When adding via SVM IP the options are:<br>4. vsadmin<br>5. ‘csuser’<br>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 MetroCluster

The following is recommended for MetroCluster:

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 with ONTAP **version 9.9.1 or newer**, 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.

## Play-Pause Data  Collector

2 new operations are now shown on kebab menu of collector (PAUSE and RESUME).

If the Data Collector is in *Running* state, you can Pause collection. Open the "three dots" menu for the collector and select PAUSE. While the collector is paused, no data is gathered from ONTAP, and no data is sent from the collector to ONTAP. This means no Fpolicy events will flow from ONTAP to the data collector, and from there to Data Infrastructure Insights.

Note that if any new volumes, etc. are created on ONTAP while the collector is Paused, Workload Security won’t gather the data and those volumes, etc. will not be reflected in dashboards or tables.

Keep the following in mind:

- Snapshot purge won’t happen as per the settings configured on a paused collector.
- EMS events (like ONTAP ARP) won’t be processed on a paused collector. This means if ONTAP identifies a ransomware attack, Data Infrastructure Insights Workload Security won’t be able to acquire that event.
- Health notifications emails will NOT be sent for a paused collector.
- Manual or Automatic actions (such as Snapshot or User Blocking) will not be supported on a paused collector.
- On agent or collector upgrades, agent VM restarts/reboots, or agent service restart, a paused collector will remain in *Paused* state.
- If the data collector is in *Error* state, the collector cannot be changed to *Paused* state. The Pause button will be enabled only if the state of the collector is *Running*.
- If the agent is disconnected, the collector cannot be changed to *Paused* state. The collector will go into *Stopped* state and the Pause button will be disabled.

## Persistent Store

Persistent store is supported with ONTAP 9.14.1 and later. Note that volume name instructions vary from ONTAP 9.14 to 9.15.

Persistent Store can be enabled by selecting the checkbox in the collector edit/add page. After selecting the checkbox, a text field is displayed for accepting volume name. Volume name is a mandatory field for enabling Persistent Store.

- For ONTAP 9.14.1, you must create the volume prior to enabling the feature, and provide the same name in the *Volume Name* field. The recommended volume size is 16GB.
- For ONTAP 9.15.1, the volume will be created automatically with 16GB size by the collector, using the name provided in in the *Volume Name* field.

Specific permissions are required for Persistent Store (some or all of these may already exist):

Cluster mode:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

Vserver mode:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

### Troubleshooting

See the Troubleshooting the SVM Collector page for troubleshooting tips.

# 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 Data Infrastructure Insights environment.
2. Navigate to Workload Security **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.<br>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.<br>Allowed all ports if you are not sure about the ports. |

# User Management

Workload Security user accounts are managed through Data Infrastructure Insights.

Data Infrastructure 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 Data Infrastructure 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 Data Infrastructure 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 a maximum of 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 following 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. You can increase the number of cores and/or memory to increase the number of data collectors supported, up to a maximum of 50 data collectors:

| 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 | Answer |
| --- | --- |

| | |
|---|---|
| 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? | The Event Rate Checker can run fine even for an SVM already configured for Workload Security. There should be no impact. |
| Can I increase the number of SVMs on which the script can be run? | Yes. Simply edit the script and change the max number of SVMs from 5 to any desirable number. |
| If I increase the number of SVMs, will it increase the time of running of the script? | No. The script will run for a max of 5 minutes, even if the number of SVMs is increased. |
| Can I increase the number of SVMs on which the script can be run? | Yes. You need to edit the script and change the max number of SVMs from 5 to any desirable number. |
| If I increase the number of SVMs, will it increase the time of running of the script? | No. The script will run for a max of 5mins, even if the number of SVMs are increased. |
| What happens if I run the Event Rate Checker with an existing agent? | Running the Event Rate Checker against an already-existing agent may cause an increase in latency on the SVM. This increase will be temporary in nature while the Event rate Checker is running. |

## Copyright information



## Trademark information