Getting Started

Cloud Insights

NetApp
April 20, 2021

Table of Contents

Getting Started

Getting Started with Cloud Secure

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

The Cloud Secure 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

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 7.2 64-bit Red Hat Enterprise Linux 7.2 64-bit KVM Red Hat Enterprise Linux 7.5 64-bit Red Hat Enterprise Linux 7.5 64-bit KVM Red Hat Enterprise Linux 7.8 64-bit Red Hat Enterprise Linux 7.8 64-bit KVM CentOS 7.2 64-bit CentOS 7.2 64-bit KVM CentOS 7.5 64-bit CentOS 7.5 64-bit KVM CentOS 7.8 64-bit CentOS 7.8 64-bit KVM This computer should be running no other application-level software. A dedicated server is recommended.
Commands	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: /opt/netapp 25 GB
Network	100 Mbps to 1 Gbps Ethernet connection, static IP address, IP connectivity to all devices, and a required port to the Cloud Secure instance (80 or 443).

Please note: Cloud Insights agent and Cloud Secure agent can be installed in the same machine. However, it is a best practice to install them in separate machines. In the event that both agents are installed on the same machine, please allocate disk space as shown below:

Available disk space	50 GB For Linux, disk space should be allocated in this manner: /opt/netapp 25 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** Cloud Secure 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** Cloud Secure 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

In-network rules

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

Related:

See the Event Rate Checker documentation for information about sizing.

Cloud Secure Agent Installation

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 Cloud Secure SaaS layer for analysis. See Agent Requirements to configure an agent VM.

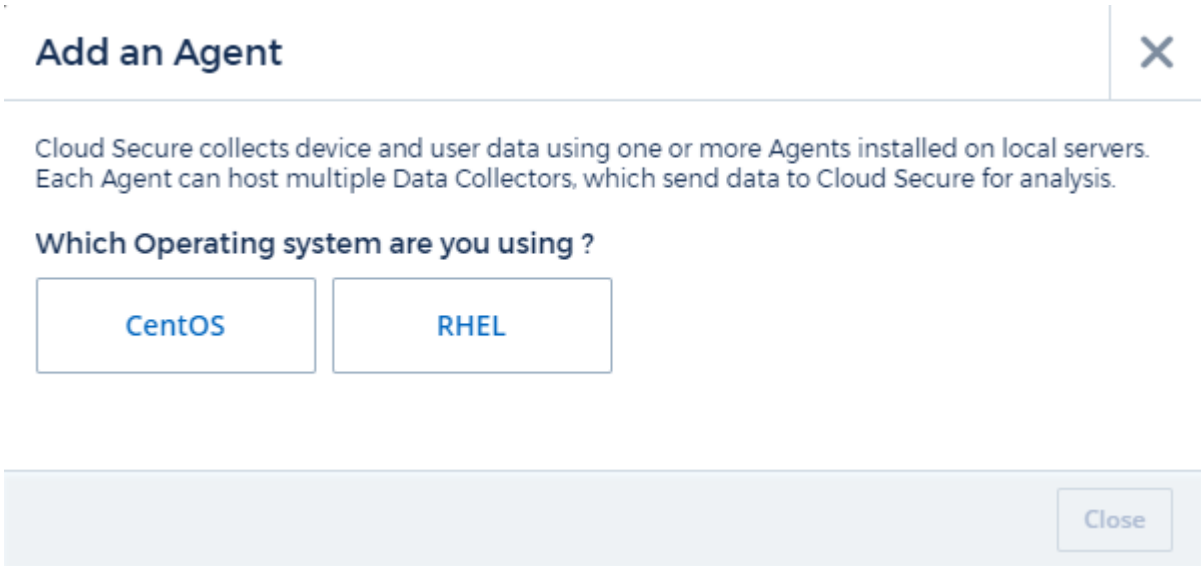
Before You Begin

- The sudo privilege is required for installation, running scripts, and uninstall.

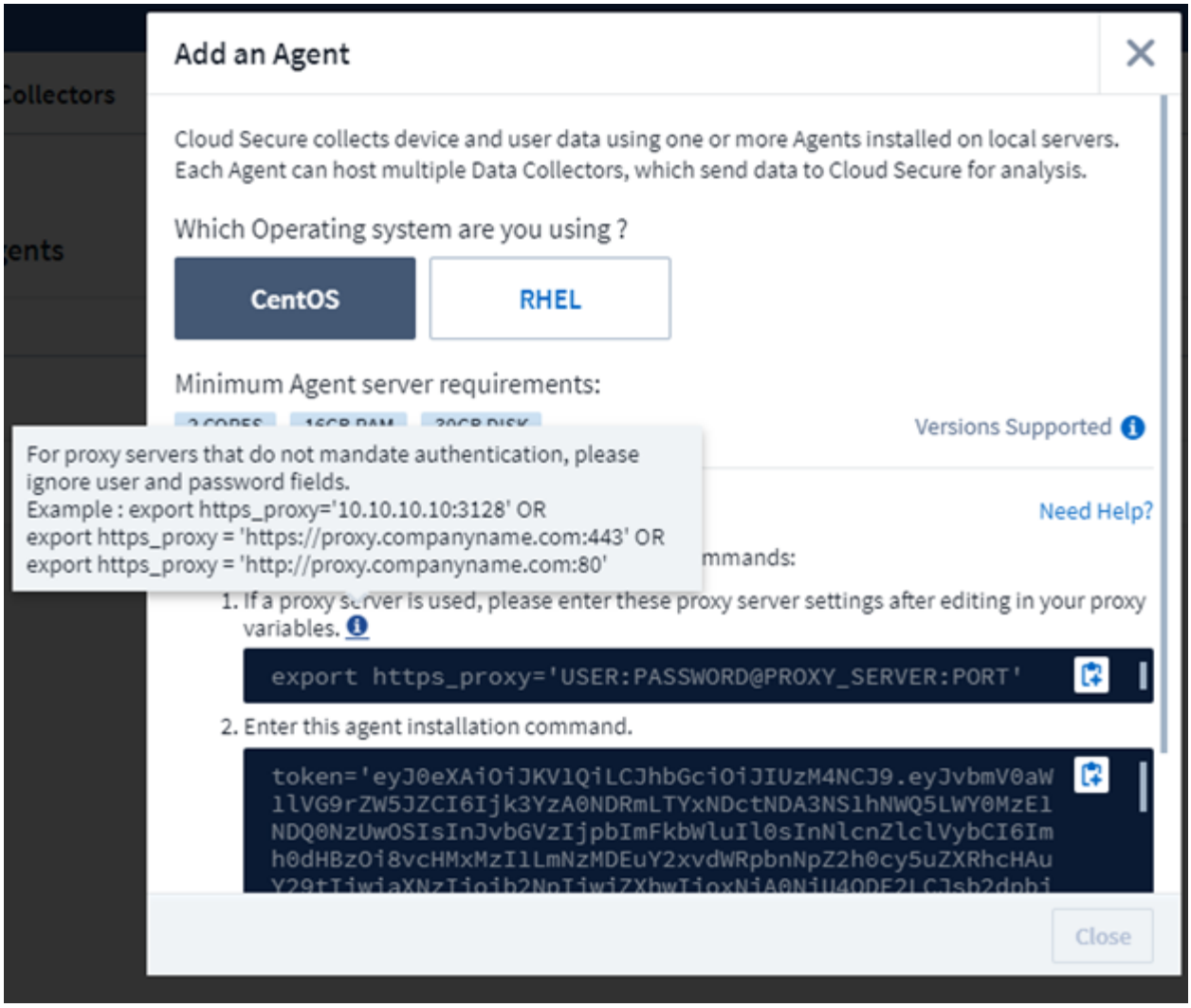
Steps to Install Agent

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

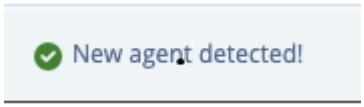
   The system displays the Add an Agent page:



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



7. Click the Copy to Clipboard icon to copy the installation command.
8. Run the installation command in a terminal window.
9. 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 Cloud Secure.

Steps

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

3. `sudo iptables-save | grep 35000`

   sample output:
   -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEW -j ACCEPT

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'.	The supported platforms for Cloud Secure 1.0.0 are RHEL 7.x / CentOS 7.x. Ensure that you are not installing the agent on a RHEL 6.x or CentOS 6.x system.
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.

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`.
	1. Check if the logs shows a message“Failed to start Cloud Secure 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 10 Data collectors to an Agent.	Only 10 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.

Deleting a Cloud Secure Agent

When you delete a Cloud Secure 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 Cloud Secure 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

Cloud Secure 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 Cloud Secure 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]
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

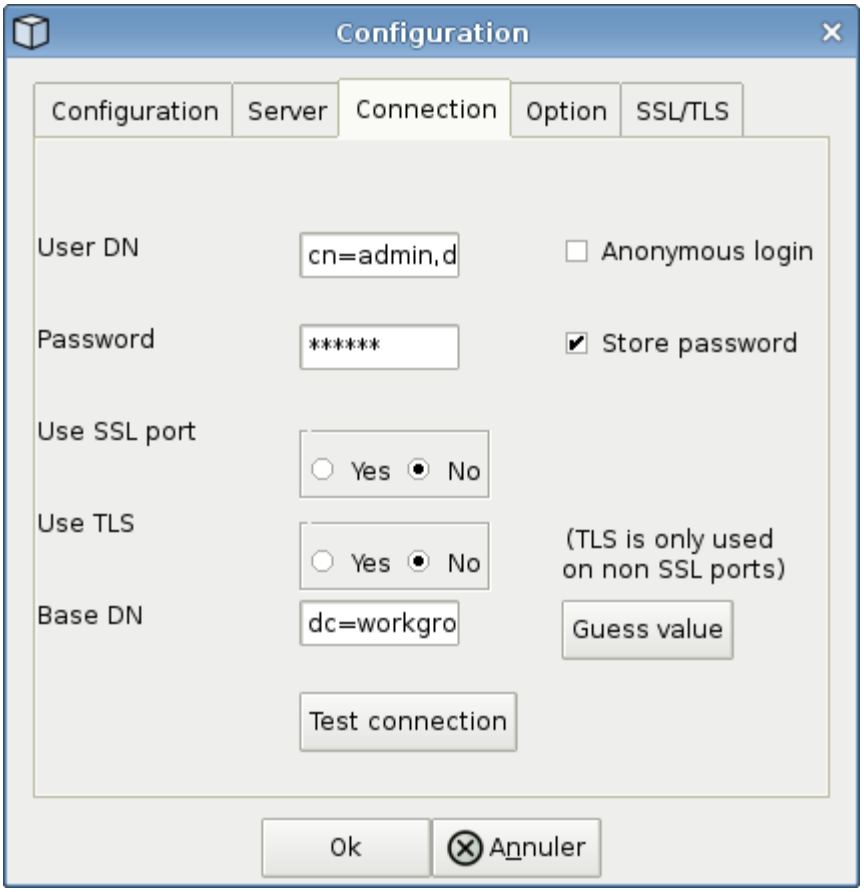
Testing Your User Directory Collector Configuration

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

- Use the following command to validate Cloud Secure 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 Cloud Secure 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 Cloud Secure 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

Cloud Secure 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
  - SMB protocol version 3.1 and earlier
  - NFS protocol version 4.0 and earlier
- Only data type SVMs are supported. SVMs with infinite/flexgroup volumes are not supported

- SVM has several sub-types. Of these, only *default* and *sync_source* 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
    - 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 Cloud Secure 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 Cloud Secure 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
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 Cloud Secure 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 Cloud Secure 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.

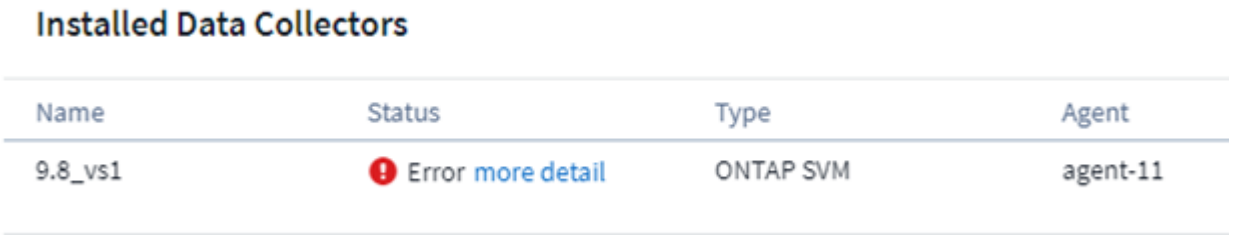
After you finish

- 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.

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:
Error message: "Connection to the FPolicy server <IP> is broken. (reason: "FPolicy server is removed from external engine.")"	SVM is unable to reach the Fpolicy Server. 1. Make sure there is route available from SVM to the Fpolicy Server/Agent machine IP. Login to the cluster/SVM and ping the Fpolicy Server IP address using the following command: *net ping -lif <data_lif> -destination <agent IP> -vserver <svmname> -show-detail* 2. In instances where the same SVM was added in two different Cloud Secure 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 the first one will stop receiving events and its "audit" service will enter into error state. To prevent this, configure each SVM on a single environment.
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.
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 management 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.

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* Please check if the fpolicy policy named with prefix “metadata_service” 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.

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

Configuring the Cloud Volumes ONTAP Data Collector

Cloud Secure uses data collectors to collect file and user access data from devices.

Cloud Volumes ONTAP Storage Configuration

See the OnCommand Cloud Manager Documentation to configure a single-node / HA AWS instance to host the Cloud Secure Agent:
https://docs.netapp.com/us-en/occm/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

Agent Machine Configuration

Use the following steps to configure the machine to be used as a Cloud Secure 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 Cloud Secure Agent

1. Log in as Administrator or Account Owner to your Cloud Insights environment.
2. Navigate to Cloud Secure **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 Cloud Secure 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

User Management

Cloud Secure user accounts are managed through Cloud Insights.

Cloud Insights provides four user accounts: Account Owner, Administrator, User, and Guest. Each account is assigned specific permission levels. A User account that has Administrator privileges can access Cloud Secure and can create or modify users.

Steps

1. Log into Cloud Secure
2. In the menu, click **Admin > User Management**

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

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

SVM Event Rate Checker

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.

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. Provide the correct values when prompted. See below for an example.
4. The script will take approximately 5 minutes to run.
5. 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”.
```

1. 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) A single Agent machine can handle upto 7000 events per second and maximum of 10 data collectors.

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% < 7000 events/second
```

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 < 7000 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): QA_SVM
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...
Running check for svm QA_SVM...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
Stopping sample QA_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 shails3 is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm shails3 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 Cloud Secure, 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 Cloud Secure. There should be no impact.