Cloud Secure

Cloud Insights

NetApp
May 21, 2020

Table of Contents

Cloud Secure

About Cloud Secure

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

Visibility

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

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

Protection

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

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

Compliance

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

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
Configure a User Directory Connector	Add User Directory Connector
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.
Create Users Accounts	Manage User Accounts

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 CentOS 7.2 64-bit CentOS 7.2 64-bit KVM CentOS 7.5 64-bit CentOS 7.5 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.

Component	Linux Requirement
Docker	The Docker CE package must be installed on the VM hosting the agent. The agent systems should always have the Docker CE package installed. Users should not install the Docker-client-xx or Docker-common-xx native RHEL Docker packages since these do not support the 'docker run' CLI format that Cloud Secure supports.
CPU	2 CPU cores
Memory	16 GB RAM
Available disk space	Disk space should be allocated in this manner: 50 GB available for the root partition /opt/netapp 5 GB /var/log/netapp 5 GB
Network	100 Mbps 1 Gbps Ethernet connection, static IP address, IP connectivity to all devices, and a required port to the Cloud Secure instance (80 or 443).
Agent outbound URLs (port 433)	https://<Site ID>.cs01.cloudinsights.netapp.com You can use a broader range to specify the tenant ID: https://*.cs01.cloudinsights.netapp.com/ https://gateway.c01.cloudinsights.netapp.com https://agentlogin.cs01.cloudinsights.netapp.com

Cloud Network Access Rules

Protocol	Port	Destination	Direction	Description
TCP	443	<tenant id>.cs01.cloudinsights.netapp.com <tenant id>.c01.cloudinsights.netapp.com <tenant id>.c02.cloudinsights.netapp.com	Outbound	Access to Cloud Insights

Protocol	Port	Destination	Direction	Description
TCP	443	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.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

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.

Before You Begin

- The sudo privilege is required for installation, running scripts, and uninstall.
- The Docker CE package must be installed on the VM hosting the agent.

  To determine if the Docker CE package is installed, use the following command:
  `sudo rpm -qa |grep -i docker-ce`
  If the package is installed, the command returns the package name, for example:
  docker-ce-18.03.1.ce-1.el7.centos.x86_64

- The Docker-client-xx or Docker-common-xx native RHEL Docker packages are not supported. These packages do not support the `docker run cli` format that Cloud Secure supports.

  Use the following commands to determine if these packages are installed:
  `sudo rpm -qa | grep -i docker-client`
  `sudo rpm -qa |grep -i docker-common`

Steps to Install Docker

1. Install the required dependencies:
   `sudo yum install yum-utils device-mapper-persistent-data lvm2`
2. Add docker stable repository to your system:
   `sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo`
3. To use the latest version of Docker CE, enable repositories that are disabled by default:
   `sudo yum-config-manager --enable docker-ce-edge`
4. Install the latest version of Docker CE using the following command:
   `sudo yum install docker-ce`
   (Version must be higher than 17.06)
5. Start Docker
   `sudo systemctl start docker`
6. Use the following command to automatically start Docker on system reboot:
   `sudo systemctl enable docker`

Docker Installation Reference

For additional installation information, see:
* https://docs.docker.com/install/linux/docker-ce/centos/
* https://getstart.blog/2018/03/24/docker-ce-installation-on-red-hat-7/

Steps to Install Docker on a VM Without Full Access to the Internet

Steps

1. Uninstall existing docker installation:

   ```
   sudo rpm -qa | grep docker
   sudo rpm -e <rpms>
   ```

2. Install Docker-ce
   a. Download all required rpms and copy them to the VM on which the agent is to be installed.

```
https://download.docker.com/linux/centos/docker-ce.repo
sudo yum-config-manager --add-repo <repo_file>
https://download.docker.com/linux/centos/7/x86_64/stable/Packages/docker-ce-
18.09.0-3.el7.x86_64.rpm
https://download.docker.com/linux/centos/7/x86_64/stable/Packages/docker-ce-cli-
18.09.0-3.el7.x86_64.rpm
https://download.docker.com/linux/centos/7/x86_64/stable/Packages/containerd.io-
1.2.6-3.3.el7.x86_64.rpm
sudo rpm -i <rpms>
sudo systemctl enable docker
sudo systemctl start docker
```

Java Requirement

OpenJDK Java is required. Use the following command to determine if OpenJDK Java is installed:
`sudo rpm -qa|grep -i openjdk`

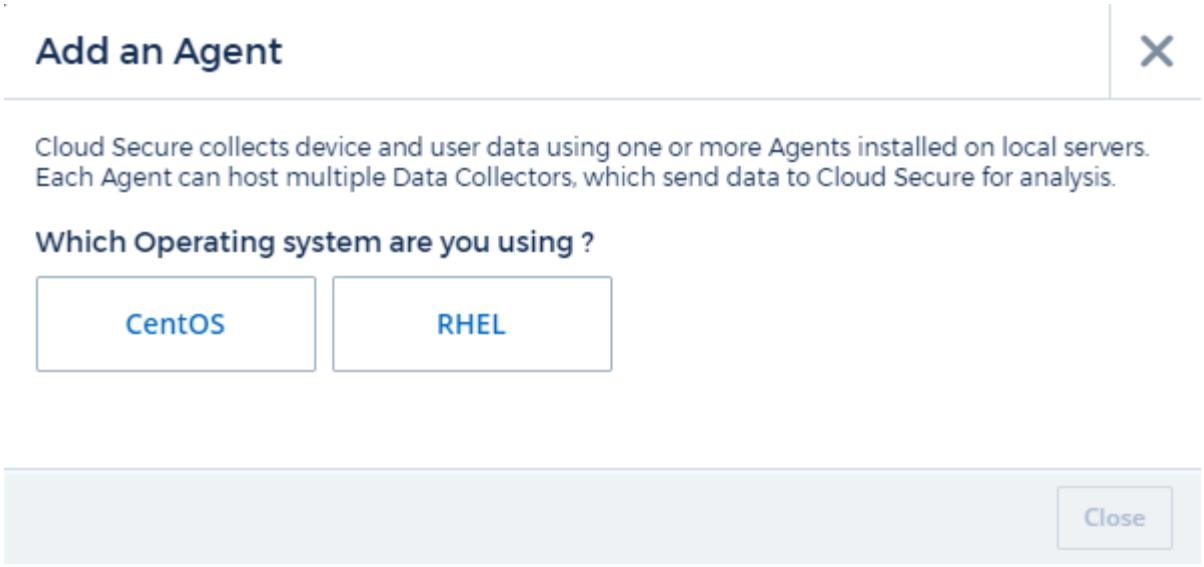
Install OpenJDK Java using the following command:
`sudo yum install -y java-1.8.0-openjdk`

The IBM Java package, found in some RHEL versions, must be uninstalled. Use the following command to verify the Java version:
`sudo java -` (or) `sudo rpm -qa | grep -I java`
If the command returns information similar to 'IBM J9 VM (build 2.9.x)' you need to remove the package:
`sudo update-alternatives --remove java /usr/lib/jvm/jdk[version]/bin/java`

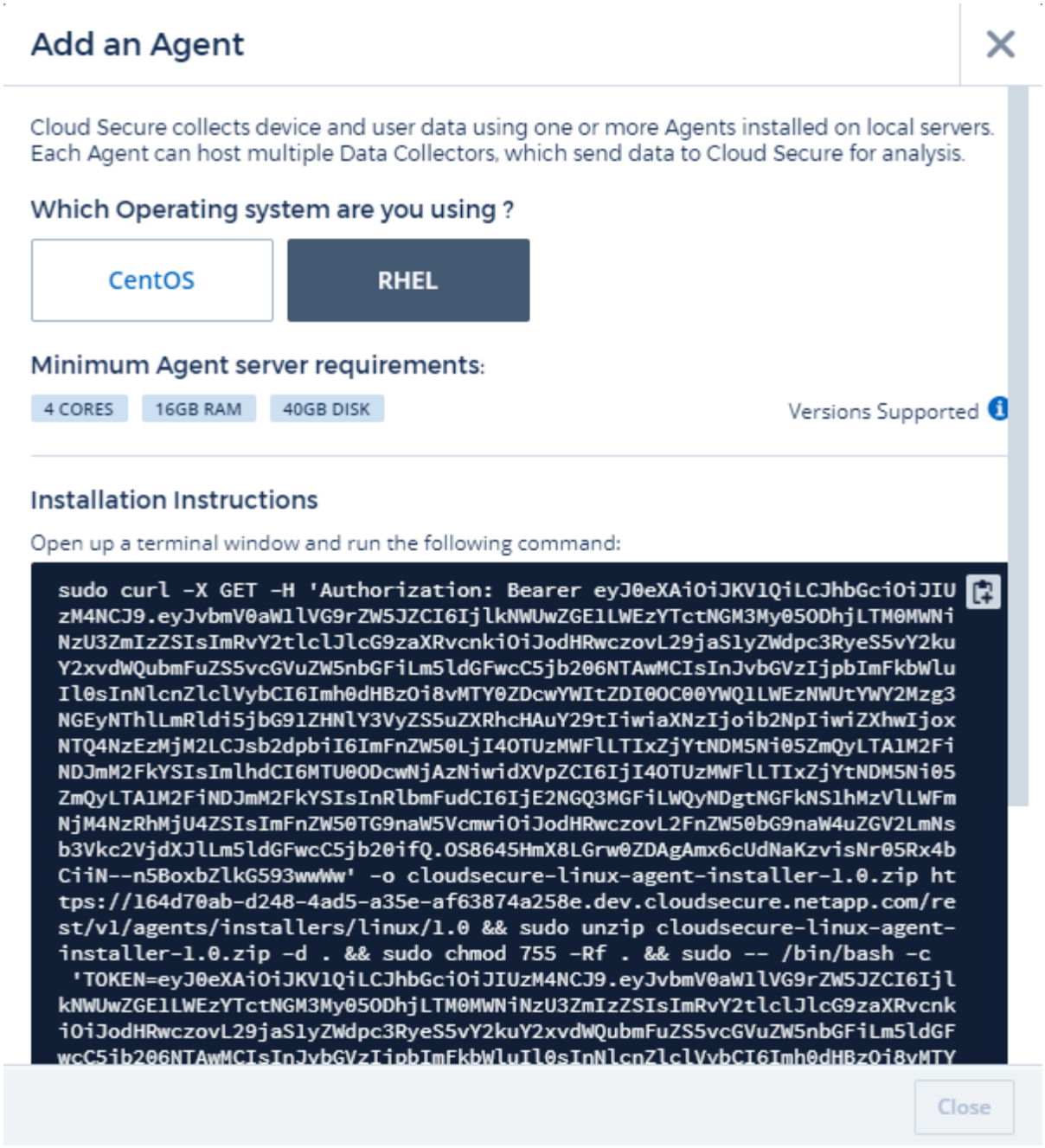
Steps to Install Agent

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

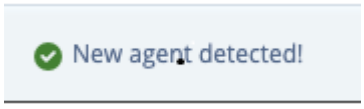
   The system displays the Add an Agent page:



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. 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.

Files Created During Installation

- Installation directory:

  /opt/netapp/cloudsecure/agent

- Installation logs:

  /var/log/netapp/cloudsecure/install
  /opt/netapp/cloud-secure/logs

- Agent Logs:
- You can use the following command to verify the agent installed correctly:
  `sudo grep -irn register /opt/netapp/cloudsecure/agent/logs/agent.log`
- Use the following script to uninstall the agent:
  `sudo cloudsecure-agent-uninstall.sh`

Network Configuration

Use the following commands to open ports to be used by Cloud Secure.

Steps

1. `sudo firewall-cmd --permanent --zone=public --add-port=35001-35100/tcp`
2. `sudo firewall-cmd --reload`
3. `sudo iptables-save | grep 35001`

   sample output:

4. -A IN_public_allow -p tcp -m tcp --dport 35001 -m conntrack -ctstate NEW -j ACCEPT

Troubleshooting Agent Installation Errors

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

Problem:	Resolution:
Agent installation fails with "File name too long" errror	To correct this error use the sh shell to run the command.

Problem:	Resolution:
Agent installation fails to create the ~/agent/logs 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.

Deleting a Cloud Secure Agent

When you delete a Cloud Secure Agent, all of the data collectors associated with the Agent are deleted.

Deleting an Agent

Deleting an Agant 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.

Steps to delete an Agent:

1. `sudo cloudsecure-agent-uninstall.sh`
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**.

Configuring a User Directory Collector

You configure Cloud Secure 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**

   The system displays the Add User Directory screen.

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

Name	Description
User Directory Name	Unique name for the user directory
Agent	Select a configured agent from the list
Server	IP address of server hosting the active directory
Forest Name	Forest level of the directory structure
Bind DN	User permitted to search the directory
BIND password	Directory server password
Protocol	ldap, ldaps, ldap-start-tls
Ports	Select port

Enter the following Directory Server required attributes:

Attributes	Attribute name in Directory Server
Display Name	name
SID	objectsid
User Name	sAMAccountName

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	department
Photo	thumbnailphoto
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 -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p 389 -D Administrator@netapp.com -W
  ```

- Use AD Explorer to navigate an AD database, view object properties and attributes, view permissions, view an object's schema, execute sophisticated searches that you can save and re-execute.
  - Install AD Explorer
  - Connect to the AD server using the username/password of the AD directory server.

Troubleshooting User Directory Collector Configuration Errors

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

Problem:	Resolution:
Adding a User 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 'Administrator@<domain_forest_name>' or as a user account with domain admin privileges.
The optional attributes of domain user are not appearing in the Cloud Secure User Profile page.	Ensure you have used the AD domain user 'Attribute Editor' to enter the optional attributes.

Configuring NetApp Data Collectors

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 on Data ONTAP 9.1 and later versions.
- An Agent must be configured before you can configure data collectors.
- A separate subnet must be used for FPolicy traffic.
- You need the SVM management IP address.
- You need a username and password to access the SVM.
- Ensure the correct protocols are set for the SVM.

```
security login show -vserver svmname
Vserver: svmname
Authentication Acct Is-Nsswitch
User/Group Name Application Method Role Name Locked Group
vsadmin http password vsadmin yes no
vsadmin ontapi password vsadmin yes no
vsadmin ssh password vsadmin yes no
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

  clustershell::> `security login password -username vsadmin -vserver svmname`

- Unlock the SVM for external access:

  clustershell::> `security login unlock -username vsadmin -vserver svmname`

- Verify that the ONTAP FPolicy framework can connect to the External FPolicy server engine that the Agent system hosts:

  clustershell::> `vserver fpolicy show-engine -vserver svmname`

  The agent IP address state should be "Connected".

- Ensure the firewall-policy of the data LIF is set to ‘mgmt’ (not ‘data’).

  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.

If you cannot use the "vsadmin" user, create the following roles for the data collector using the "causer" user:

```
security login show -vserver svmname
```

```
security login role create -vserver svmname -role carole -cmddirname DEFAULT -access none
security login role create -vserver svmname -role carole -cmddirname "network interface" -access
readonly
security login role create -vserver svmname -role carole -cmddirname version -access readonly
security login role create -vserver svmname -role carole -cmddirname volume -access readonly
security login role create -vserver svmname -role carole -cmddirname vserver -access readonly
security login role create -vserver svmname -role carole -cmddirname "vserver fpolicy" -access all
security login create -user-or-group-name causer -application ontapi -authmethod password -role
carole -vserver svmname
```

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. Click the **NetApp** tile.

   Select ONTAP SVM

   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 or click **Add Agent** to configure an Agent. See Agent requirements and Agent Installation for configuration information.
SVM Management IP Address	Management IP Address
Username	User name to access the SVM
Password	SVM Password
Enter complete share names to exclude	Comma-separated list of shares to exclude from event collection
Enter complete volume names to exclude	Comma-separated list of volumes to exclude from event collection

After you finish

- Click **Test Configuration** to check the status of the collector you configured.
- In the Installed Data Collectors page, use the options menu on the right of each collector to edit the data collector. You can start, stop, and edit data collector configuration attributes.

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, open an SSH session to the Cloud ONTAP cluster and enter the following commands using the Cluster Management interface:

```
system services firewall modify -node nodename -enabled false
security login password -SVM admin username vsadmin -vserver vserver_name
security login show -vserver vserver_name
network interface modify -vserver vserver_name -lif lif1_name -firewall-policy mgmt
```

Client Configuration

Use the following steps to configure the client (AWS EC2 RHEL or CentOS 7.2/7.5 instance) 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 RHEL7.2/7.5 or CentOS 7.2/7.5 AMI.
3. Select the VPC and Subnet that the Cloud ONTAP instance resides in.
4. Select t2_xlarge (8 vcpus and 32 GB RAM) as allocated resources.
    a. Create the EC2 instance.
5. Install the required Linux packages using the YUM package manager:
6. Install wget, install unzip native Linux packages.
7. Install selinux (dependency package for the docker-ce):

    ```
    wget          http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.68-1.el7.noarch.rpm

    yum install -y container-selinux-2.68-1.el7.noarch.rpm
    ```

8. Install the docker-ce (not the native docker) package using https://download.docker.com/linux/centos/7/x86_64/stable/Packages/ (use a version higher than 17.03).
9. Install JRE:

    ```
    yum install -y java-1.8.0-openjdk##
    ```

10. SSH to the Redhat EC2 VM

```
ssh -i "your_new_pem.pem" <ec2_hostname_or_IP>

sudo su -
```

11. Perform a docker login after installing the required AWS CLI package:

```
curl "https://s3.amazonaws.com/aws-cli/awscli-bundle.zip" -o "awscli-bundle.zip"

unzip awscli-bundle.zip

sudo ./awscli-bundle/install -i /usr/local/aws -b /usr/local/bin/aws

/usr/local/bin/aws --version

aws configure --profile collector_readonly

aws ecr get-login --no-include-email --region us-east-1 --profile collector_readonly

docker login -u AWS -p <token_generated_above> <ECR_hostname>
```

12. Use the following command to verify the steps completed successfully and the cs-ontap-dsc image can be successfully pulled:

```
docker pull 376015418222.dkr.ecr.us-east-1.amazonaws.com/cs-ontap-dsc:1.25.0
```

Install the Cloud Secure Agent

1. Log in as Administrator or Account Owner to your Cloud Insights environment.
2. Click **Admin**>**Data Collectors**>**Agents**> +**Agent** and specify RHEL as the target platform.
3. Copy the Agent Installation command.
4. 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.

Add a NetApp ONTAP data collector

1. Click **Admin** > **Data Collectors** > **Data Collectors** > +**Data Collector** and specify the NetApp ONTAP Cloud Volumes data collector. Enter the required information in the fields.

Configuration

Field	Description
Name	Unique name for the Data Collector
Agent	Select a configured agent from the list or click **Add Agent** to configure an Agent. See Agent requirements and Agent Installation for configuration information.
SVM Management IP Address	Management IP Address

Username	User name to access the SVM
Password	SVM Password
Enter complete share names to exclude	Comma-separated list of shares to exclude from event collection
Enter complete volume names to exclude	Comma-separated list of volumes to exclude from event collection

a. Click **Add Collector**

1. Verify the Agent Server is running using the `docker ps` command and a `docker logs <docker_image_id>` file.

   All of the data collector's service status should be in the 'running' state.