Cloud Secure Agent Installation

Cloud Insights

Tony Lavoie, Dave Grace
April 16, 2020

NetApp®

Table of Contents

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:
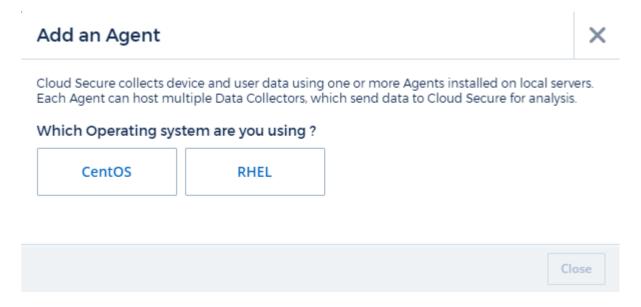`sudo java -` (or) `sudo rpm -qa | grep -I java`
If the command returns information similar to 'IBM J9 VM (build 2.9.x)' you need to remove the package:

```
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:

   ## Add an Agent   ✕

   Cloud Secure collects device and user data using one or more Agents installed on local servers.
   Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

   Which Operating system are you using ?

CentOS	RHEL

   Close

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)*.

Add an Agent

Cloud Secure collects device and user data using one or more Agents installed on local servers. Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

Which Operating system are you using ?

CentOS **RHEL**

Minimum Agent server requirements:

4 CORES   16GB RAM   40GB DISK   Versions Supported ⓘ

Installation Instructions

Open up a terminal window and run the following command:

```
sudo curl -X GET -H 'Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIU
zM4NCJ9.eyJvbmV0aW1lVG9rZW5JZCI6IjlkNWUwZGE1LWEzYTctNGM3My05ODhjLTM0MWNi
NzU3ZmIzZSIsImRvY2tlclJlcG9zaXRvcnkiOiJodHRwczovL29jaSlyZWdpc3RyeS5vY2ku
Y2xvdWQubmFuZS5vcGVuZW5nbGFiLm5ldGFwcC5jb206NTAwMCIsInJvbGVzIjpbImFkbWlu
Il0sInNlcnZlclVybCI6Imh0dHBzOi8vMTY0ZDcwYWItZDI0OC00YWQ1LWEzNWUtYWY2Mzg3
NGEyNThlLmRldi5jbG91ZHNlY3VyZS5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjox
NTQ4NzEzMjM2LCJsb2dpbiI6ImFnZW50LjI4OTUzMWFlLTIxZjYtNDM5Ni05ZmQyLTA1M2Fi
NDJmM2FkYYSIsImlhdCI6MTU0ODDcwNjAzNiwidXVpZCI6IjI4OTUzMWFlLTIxZjYtNDM5Ni05
ZmQyLTA1M2FiNDJmM2FkYYSIsInRlbmFudCI6IjE2NGQ3MGFiLWQyNDgtNGFkNS1hMzVlLWFm
NjM4NzRhMjU4ZSIsImFnZW50TG9naW5VcmwiOiJodHRwczovL2FnZW50bG9naW4uZGV2LmNs
b3Vkc2VjdXJlLm5ldGFwcC5jb20ifQ.OS8645HmX8LGrw0ZDAgAmx6cUdNaKzvisNr05Rx4b
CiiN--n5BoxbZlkG593wwWw' -o cloudsecure-linux-agent-installer-1.0.zip ht
tps://164d70ab-d248-4ad5-a35e-af63874a258e.dev.cloudsecure.netapp.com/re
st/v1/agents/installers/linux/1.0 && sudo unzip cloudsecure-linux-agent-
installer-1.0.zip -d . && sudo chmod 755 -Rf . && sudo -- /bin/bash -c
'TOKEN=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJvbmV0aW1lVG9rZW5JZCI6Ijl
kNWUwZGE1LWEzYTctNGM3My05ODhjLTM0MWNiNzU3ZmIzZSIsImRvY2tlclJlcG9zaXRvcnk
iOiJodHRwczovL29jaSlyZWdpc3RyeS5vY2kuY2xvdWQubmFuZS5vcGVuZW5nbGFiLm5ldGF
wcC5jb206NTAwMCIsInJvbGVzIjpbImFkbWluIl0sInNlcnZlclVybCI6Imh0dHBzOi8vMTY
```

Close

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:

✓ New agent detected!

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.