



# Cloud Secure Agent Installation

## Cloud Insights

Tony Lavoie, Dave Grace

April 16, 2020

This PDF was generated from [https://docs.netapp.com/us-en/cloudinsights/task\\_cs\\_add\\_agent.html](https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html) on May 07, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

- Cloud Secure Agent Installation ..... 1
  - Before You Begin..... 1
  - Steps to Install Docker..... 1
  - Docker Installation Reference..... 2
  - Steps to Install Docker on a VM Without Full Access to the Internet..... 2
  - Java Requirement..... 2
  - Steps to Install Agent..... 3
  - Files Created During Installation..... 5
  - Network Configuration..... 5
  - Troubleshooting Agent Installation Errors..... 5

# 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzU4NCJ9.eyJvbmV0aWw1VG9rZW5JZCI6IjlkNWUwZGE1LWEzYTctNGM3My05ODhjLTM0MWNiNzU3ZmIzZSI6ImRvY2t1c2lJcG9zaXRvcnk0IjodHRwczovL29jaSlyZWdpc3RyeS5vY2kuY2xvdWQubmFuZS5vcGVuZW5nbGF1Lm5ldGFwcC5jb206NTAwMCIsInJvbGVzIjpbImFkbWluIl0sInNlcnZ1c2lVbCI6Imh0dHBz0i8vMTY0ZDcwYWI0ZDI0C00YwQ1LWEzNWU0Y2Y2Mzg3NGEYNTllLmRldi5jbG91ZHNLY3VyZS5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiaXhwIjoxNTQ4NzEzZmJmM2LCJsb2dpbiI6ImFnZW50LjI4OTUzMWFLLTlxZjYtNDM5Ni05ZmQyLTAlM2FiNDJmM2FkYSIsImh0dCI6MTU0ODcwNjAzNiwiZHVpZCI6IjI4OTUzMWFLLTlxZjYtNDM5Ni05ZmQyLTAlM2FiNDJmM2FkYSIsInRlbnMfudCI6IjE2NGQ3MGFiLWQyNDgtNGFkNS1hMzVlLWFMNjM4NzRhMjU4ZSI6ImFnZW50TG9naW5VcmwiOiJodHRwczovL2FnZW50bG9naW4uZGV2LmNsY3Vkc2VjdXJlLm5ldGFwcC5jb20ifQ.OS8645HmX8LGrw0ZDagAmx6cUdNaKzvisNr05Rx4bCiIn--n5BoxbZlkG593www' -o cloudsecure-linux-agent-installer-1.0.zip https://164d70ab-d248-4ad5-a35e-af63874a258e.dev.cloudsecure.netapp.com/rest/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=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzU4NCJ9.eyJvbmV0aWw1VG9rZW5JZCI6IjlkNWUwZGE1LWEzYTctNGM3My05ODhjLTM0MWNiNzU3ZmIzZSI6ImRvY2t1c2lJcG9zaXRvcnk0IjodHRwczovL29jaSlyZWdpc3RyeS5vY2kuY2xvdWQubmFuZS5vcGVuZW5nbGF1Lm5ldGFwcC5jb206NTAwMCIsInJvbGVzIjpbImFkbWluIl0sInNlcnZ1c2lVbCI6Imh0dHBz0i8vMTY0ZDcwYWI0ZDI0C00YwQ1LWEzNWU0Y2Y2Mzg3NGEYNTllLmRldi5jbG91ZHNLY3VyZS5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiaXhwIjoxNTQ4NzEzZmJmM2LCJsb2dpbiI6ImFnZW50LjI4OTUzMWFLLTlxZjYtNDM5Ni05ZmQyLTAlM2FiNDJmM2FkYSIsImh0dCI6MTU0ODcwNjAzNiwiZHVpZCI6IjI4OTUzMWFLLTlxZjYtNDM5Ni05ZmQyLTAlM2FiNDJmM2FkYSIsInRlbnMfudCI6IjE2NGQ3MGFiLWQyNDgtNGFkNS1hMzVlLWFMNjM4NzRhMjU4ZSI6ImFnZW50TG9naW5VcmwiOiJodHRwczovL2FnZW50bG9naW4uZGV2LmNsY3Vkc2VjdXJlLm5ldGFwcC5jb20ifQ.OS8645HmX8LGrw0ZDagAmx6cUdNaKzvisNr05Rx4bCiIn--n5BoxbZlkG593www'
```



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" error	To correct this error use the sh shell to run the command.

Problem:	Resolution:
<p>Agent installation fails to create the ~/agent/logs folder and the install.log file provides no relevant information.</p>	<p>This error occurs during bootstrapping of the agent. The error is not logged in log files because it occurs before logger is initialized.</p> <p>The error is redirected to standard output, and is visible in the service log using the <code>journalctl -u cloudsecure-agent.service</code> command. This command can be used for troubleshooting the issue further.</p>
<p>Agent installation fails with ‘This linux distribution is not supported. Exiting the installation’.</p>	<p>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.</p>



## Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

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