



# **Cloud Secure Agent Installation**

## **Cloud Insights**

Tony Lavoie, Dave Grace  
September 13, 2021

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 October 26, 2021. Always check docs.netapp.com for the latest.

# Table of Contents

- Cloud Secure Agent Installation . . . . . 1
  - Before You Begin . . . . . 1
  - Steps to Install Agent . . . . . 1
  - Network Configuration . . . . . 2
  - Troubleshooting Agent Errors. . . . . 3

# 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.

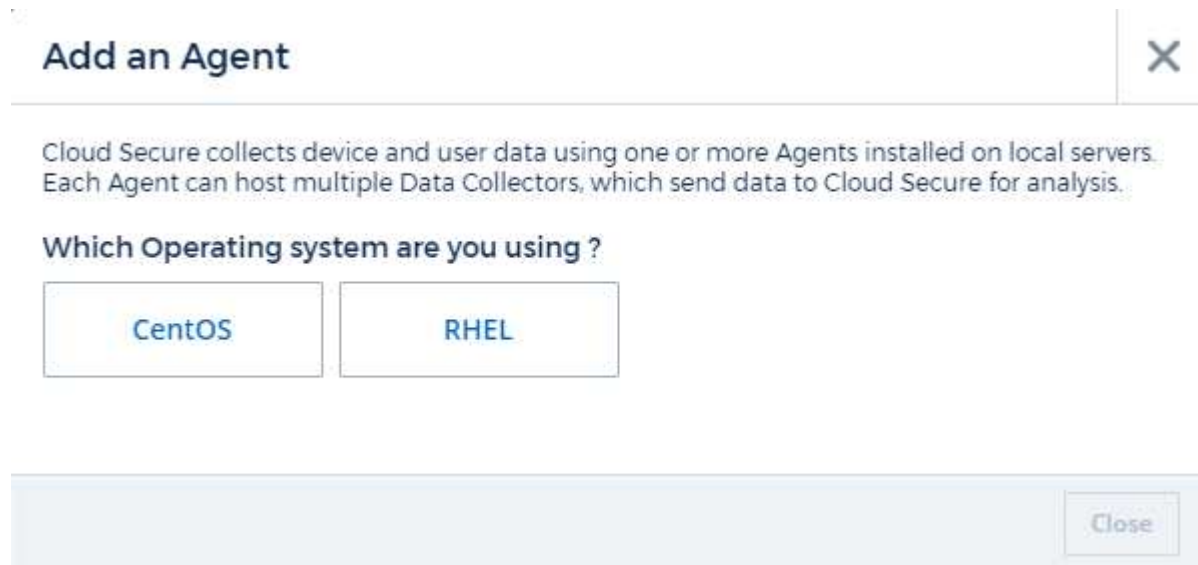
## Before You Begin

- 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:



**Add an Agent** X

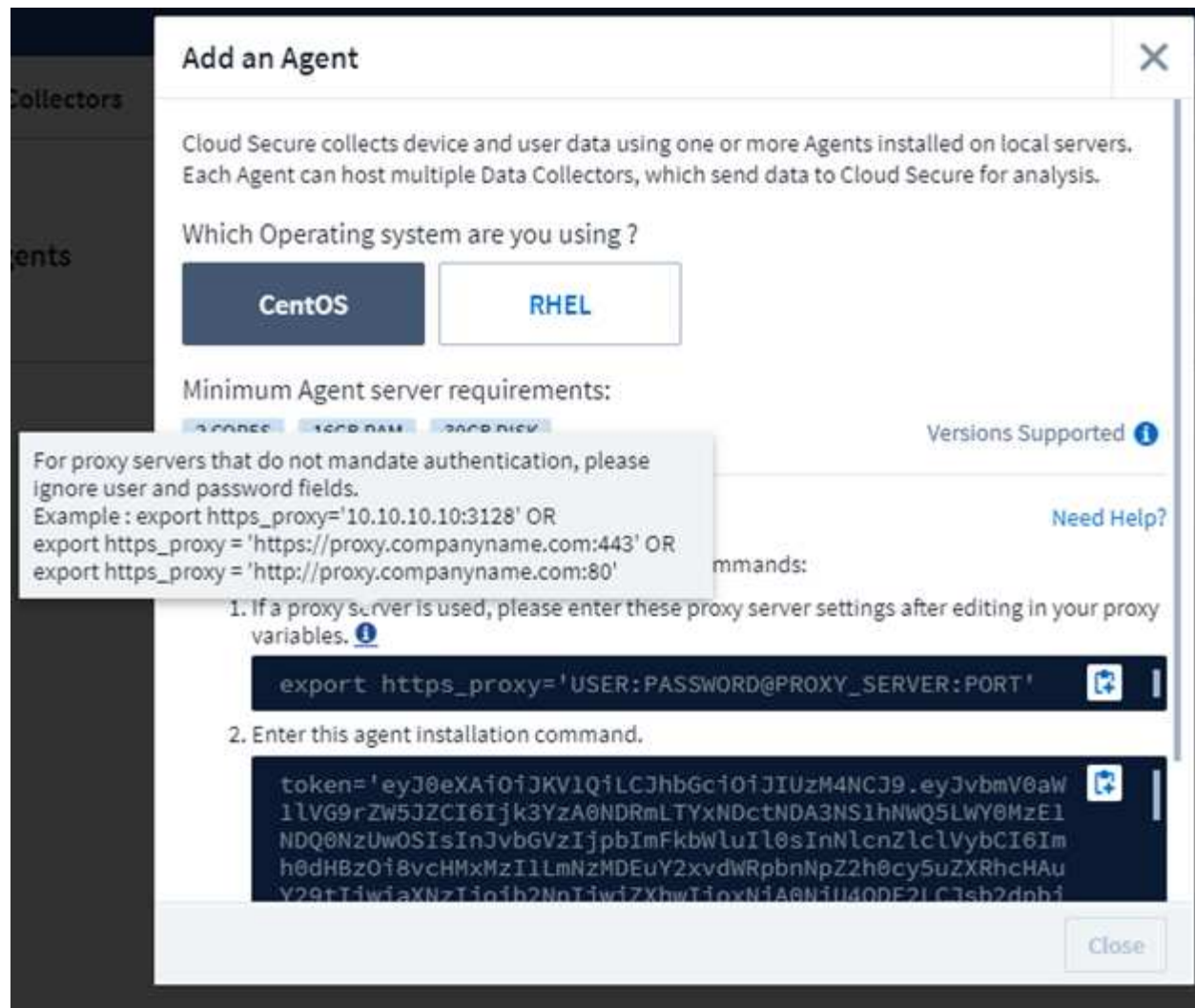
Cloud Secure collects device and user data using one or more Agents installed on local servers. Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

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)*.
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 <code>journalctl -u cloudsecure-agent.service</code> 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.   | <p>SSH to the Agent machine. Check the status of the agent service via <code>sudo systemctl status cloudsecure-agent.service</code>.</p> <ol style="list-style-type: none"> <li>1. Check if the logs shows a message "Failed to start Cloud Secure daemon service" .</li> <li>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.</li> </ol> <pre>sudo id cssys sudo groups cssys</pre> <ol style="list-style-type: none"> <li>3. If none exists, then a centralized monitoring policy may have deleted the cssys user.</li> <li>4. Create cssys user and group manually by executing the following commands.</li> </ol> <pre>sudo useradd cssys sudo groupadd cssys</pre> <ol style="list-style-type: none"> <li>5. Restart the agent service after that by executing the following command:</li> </ol> <pre>sudo systemctl restart cloudsecure-agent.service</pre> <ol style="list-style-type: none"> <li>6. If it is still not running, please check the other troubleshooting options.</li> </ol> |
| Unable to add more than 20 Data collectors to an Agent.  | Only 20 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.  | <p>Steps to restart the Agent.</p> <ol style="list-style-type: none"> <li>1. SSH to the Agent machine.</li> <li>2. Restart the agent service after that by executing the following command:</li> </ol> <pre>sudo systemctl restart cloudsecure-agent.service</pre> <ol style="list-style-type: none"> <li>3. Check the status of the agent service via <code>sudo systemctl status cloudsecure-agent.service</code>.</li> <li>4. Agent should go to CONNECTED state.</li> </ol>   |
| Agent VM is behind Zscaler proxy and the agent installation is failing. Because of Zscaler proxy's SSL inspection, the Cloud Secure 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, Cloud Secure will not work.   |

| Problem:   | Resolution:  |
|--|--|
| <p>While installing the agent, the installation hangs after unzipping.</p>   | <p>“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.</p> <ol style="list-style-type: none"> <li>1. Create a new directory named “cloudsecure”.</li> <li>2. Go to that directory.</li> <li>3. Copy and paste the full “token=.....<br/>./cloudsecure-agent-install.sh” installation command and press enter.</li> <li>4. Installation should be able to proceed.</li> </ol> |
| <p>If the Agent is still not able to connect to Saas, please open a case with NetApp Support. Provide the Cloud Insights serial number to open a case, and attach logs to the case as noted.</p> | <p>To attach logs to the case:</p> <ol style="list-style-type: none"> <li>1. Execute the following script with root permission and share the output file (cloudsecure-agent-symptoms.zip). <ol style="list-style-type: none"> <li>a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh</li> </ol> </li> <li>2. Execute the following commands one by one with root permission and share the output. <ol style="list-style-type: none"> <li>a. id cssys</li> <li>b. groups cssys</li> <li>c. cat /etc/os-release</li> </ol> </li> </ol>  |

## Copyright Information

Copyright © 2021 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.