



Configuring NetApp Data Collectors

Cloud Insights

NetApp

April 23, 2020

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html on April 23, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Configuring NetApp Data Collectors 1
 - Configuring the ONTAP SVM Data Collector 1
 - Configuring the Cloud Volumes ONTAP Data Collector..... 3

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

Name	Field
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

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 vsserver_name
security login show -vserver vsserver_name
network interface modify -vserver vsserver_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 SVM data collector.
2. Configure the data collector
 - a. Provide a name
 - b. Agent name is the agent configured in the cloud
 - c. SVM management IP Address
 - d. Username
 - e. Password
 - f. Click **Add Collector**
3. Verify the Agent Server is running using the `docker ps` command and a `docker logs <docker_image_id>` file.

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

Copyright Information

Copyright © 2019–2020 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.