



Configuring the ONTAP SVM Data Collector

Cloud Insights

Tony Lavoie
September 01, 2021

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html on October 26, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Configuring the ONTAP SVM Data Collector 1

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 with the following:
 - Data ONTAP 9.2 and later versions. For best performance, use a Data ONTAP version where [this issue](#) is fixed.
 - SMB protocol version 3.1 and earlier
 - NFS protocol version 4.0 and earlier
- Only data type SVMs are supported. SVMs with infinite/flexgroup volumes are not supported
- SVM has several sub-types. Of these, only *default* and *sync_source* are supported.
- An Agent [must be configured](#) before you can configure data collectors.
- Make sure that you have a properly configured User Directory Connector, otherwise events will show encoded user names and not the actual name of the user (as stored in Active Directory) in the “Activity Forensics” page.
- For optimal performance, you should configure the FPolicy server to be on the same subnet as the storage system.
- You must add an SVM using one of the following two methods:
 - By Using Cluster IP, SVM name, and Cluster Management Username and Password. *This is the recommended method.*
 - SVM name must be exactly as is shown in ONTAP and is case-sensitive.
 - By Using SVM Vserver Management IP, Username, and Password
 - If you are not able or not willing to use the full Administrator Cluster/SVM Management Username and Password, you can create a custom user with lesser privileges as mentioned in the “[A note about permissions](#)” section below. This custom user can be created for either SVM or Cluster access.
 - You can also use an AD user with a role that has at least the permissions of csrole as mentioned in “A note about permissions” section below. Also refer to the [ONTAP documentation](#).
- Ensure the correct applications are set for the SVM by executing the following command:

```
clustershell::> security login show -vserver <vservename> -user-or  
-group-name <username>
```

Example output:

```
Vserver: svmname
```

User/Group Name	Application	Authentication Method	Role Name	Acct Locked	Second Authentication Method
vsadmin	http	password	vsadmin	no	none
vsadmin	ontapi	password	vsadmin	no	none
vsadmin	ssh	password	vsadmin	no	none

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 vsadmin user. If using custom user or cluster admin user, skip this step.
clustershell::> security login password -username vsadmin -vserver svmname
- Unlock the SVM vsadmin user for external access. If using custom user or cluster admin user, skip this step.
clustershell::> security login unlock -username vsadmin -vserver svmname
- Ensure the firewall-policy of the data LIF is set to 'mgmt' (not 'data'). Skip this step if using a dedicated management lif to add the SVM.
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.

A Note About Permissions

Permissions when adding via Cluster Management IP:

If you cannot use the Cluster management administrator user to allow Cloud Secure to access the ONTAP SVM data collector, you can create a new user named "csuser" with the roles as shown in the commands below. Use the username "csuser" and password for "csuser" when configuring the Cloud Secure data collector to use Cluster Management IP.

To create the new user, log in to ONTAP with the Cluster management Administrator username/password, and execute the following commands on the ONTAP server:

```

security login role create -role csrole -cmddirname DEFAULT -access none
security login role create -role csrole -cmddirname "network interface"
-access readonly
security login role create -role csrole -cmddirname version -access
readonly
security login role create -role csrole -cmddirname volume -access
readonly
security login role create -role csrole -cmddirname vserver -access
readonly
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole

```

Permissions when adding via Vserver Management IP:

If you cannot use the Cluster management administrator user to allow Cloud Secure to access the ONTAP SVM data collector, you can create a new user named “csuser” with the roles as shown in the commands below. Use the username “csuser” and password for “csuser” when configuring the Cloud Secure data collector to use Vserver Management IP.

To create the new user, log in to ONTAP with the Cluster management Administrator username/password, and execute the following commands on the ONTAP server. For ease, copy these commands to a text editor and replace the <vservename> with your Vserver name before and executing these commands on ONTAP:

```

security login role create -vserver <vservname> -role csrole -cmddirname
DEFAULT -access none
security login role create -vserver <vservname> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservname> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservname> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservname> -role csrole -cmddirname
vserver -access readonly
security login role create -vserver <vservname> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservname> -role csrole -cmddirname
"volume snapshot" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservname>

```

Configure the data collector

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. Hover over the **NetApp SVM** tile and click ***+Monitor**.

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.
Connect via Management IP for:	Select either Cluster IP or SVM Management IP
Cluster / SVM Management IP Address	The IP address for the cluster or the SVM, depending on your selection above.
SVM Name	The Name of the SVM (this field is required when connecting via Cluster IP)

Username	User name to access the SVM/Cluster When adding via Cluster IP the options are: 1. Cluster-admin 2. 'csuser' 3. AD-user having similar role as csuser. When adding via SVM IP the options are: 4. vsadmin 5. 'csuser' 6. AD-username having similar role as csuser.
Password	Password for the above user name
Filter Shares/Volumes	Choose whether to include or exclude Shares / Volumes from event collection
Enter complete share names to exclude/include	Comma-separated list of shares to exclude or include (as appropriate) from event collection
Enter complete volume names to exclude/include	Comma-separated list of volumes to exclude or include (as appropriate) from event collection
Monitor Folder Access	When checked, enables events for folder access monitoring. Note that folder create/rename and delete will be monitored even without this option selected. Enabling this will increase the number of events monitored.

After you finish


- In the Installed Data Collectors page, use the options menu on the right of each collector to edit the data collector. You can restart the data collector or edit data collector configuration attributes.

Troubleshooting

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

In the case of an error, click on *more detail* in the *Status* column for detail about the error.

Installed Data Collectors

Name	Status	Type	Agent
9.8_vs1	 Error more detail	ONTAP SVM	agent-11

Problem:	Resolution:
<p>Data Collector runs for some time and stops after a random time, failing with: "Error message: Connector is in error state. Service name: audit. Reason for failure: External fpolicy server overloaded."</p>	<p>The event rate from ONTAP was much higher than what the Agent box can handle. Hence the connection got terminated.</p> <p>Check the peak traffic in CloudSecure when the disconnection happened. This you can check from the CloudSecure > Activity Forensics > All Activity page.</p> <p>If the peak aggregated traffic is higher than what the Agent Box can handle, then please refer to the Event Rate Checker page on how to size for Collector deployment in an Agent Box.</p> <p>If the Agent was installed in the Agent box prior to 4 March 2021, run the following commands in the Agent box:</p> <pre>echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf sysctl -p</pre> <p>Restart the collector from the UI after resizing.</p>

Problem:	Resolution:
<p>Collector reports Error Message: “No local IP address found on the connector that can reach the data interfaces of the SVM”.</p>	<p>This is most likely due to a networking issue on the ONTAP side. Please follow these steps:</p> <ol style="list-style-type: none"> 1. Ensure that there are no firewalls on the SVM data lif or the management lif which are blocking the connection from the SVM. 2. When adding an SVM via a cluster management IP, please ensure that the data lif and management lif of the SVM are pingable from the Agent VM. In case of issues, check the gateway, netmask and routes for the lif. <p>You can also try logging in to the cluster via ssh using the cluster management IP, and ping the Agent IP. Make sure that the agent IP is pingable:</p> <pre><i>network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail</i></pre> <p>If not pingable, make sure the network settings in ONTAP are correct, so that the Agent machine is pingable.</p> <ol style="list-style-type: none"> 3. If you have tried connecting via Cluster IP and it is not working, try connecting directly via SVM IP. Please see above for the steps to connect via SVM IP. 4. While adding the collector via SVM IP and vsadmin credentials, check if the SVM Lif has Data plus Mgmt role enabled. In this case ping to the SVM Lif will work, however SSH to the SVM Lif will not work. If yes, create an SVM Mgmt Only Lif and try connecting via this SVM management only Lif. 5. If it is still not working, create a new SVM Lif and try connecting through that Lif. Make sure that the subnet mask is correctly set. 6. Advanced Debugging: <ol style="list-style-type: none"> a) Start a packet trace in ONTAP. b) Try to connect a data collector to the SVM from CloudSecure UI. c) Wait till the error appears. Stop the packet trace in ONTAP. d) Open the packet trace from ONTAP. It is available at this location <pre><i>https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/</i></pre> <ol style="list-style-type: none"> e) Make sure there is a SYN from ONTAP to the Agent box. f) If there is no SYN from ONTAP then it is an issue

Problem:	Resolution:
<p>Message: "Failed to determine ONTAP type for [hostname: <IP Address>. Reason: Connection error to Storage System <IP Address>: Host is unreachable (Host unreachable)"</p>	<ol style="list-style-type: none"> 1. Verify that the correct SVM IP Management address or Cluster Management IP has been provided. 2. SSH to the SVM or the Cluster to which you are intending to connect. Once you are connected ensure that the SVM or the Cluster name is correct.

Problem:	Resolution:
<p>Error Message: "Connector is in error state. Service.name: audit. Reason for failure: External fpolicy server terminated."</p>	<ol style="list-style-type: none"> 1. It is most likely that a firewall is blocking the necessary ports in the agent machine. Verify the port range 35000-55000/tcp is opened for the agent machine to connect from the SVM. Also ensure that there are no firewalls enabled from the ONTAP side blocking communication to the agent machine. 2. Type the following command in the Agent box and ensure that the port range is open. <pre>sudo iptables-save grep 3500*</pre> <p>Sample output should look like:</p> <pre>-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEW -j ACCEPT</pre> 3. Login to SVM, enter the following commands and check that no firewall is set to block the communication with ONTAP. <pre>system services firewall show system services firewall policy show</pre> <p>Check firewall commands on the ONTAP side.</p> 4. SSH to the SVM/Cluster which you want to monitor. Ping the Agent box from the SVM management lif (with CIFS, NFS protocols support) and ensure that ping is working: <pre>network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail</pre> <p>If not pingable, make sure the network settings in ONTAP are correct, so that the Agent machine is pingable.</p> 5.If a single SVM is added twice added to a tenant via 2 data collectors, then this error will be shown. Delete one of the data collectors thru the UI. Then restart the other data collector thru the UI. Then the data collector will show "RUNNING" status and will start receiving events from SVM. <p>Basically, in a tenant, 1 SVM should be added only once, via 1 data collector. 1 SVM should not added twice via 2 data collectors.</p> 6. In instances where the same SVM was added in two different Cloud Secure environments (tenants), the last one will always succeed. The second collector will configure fpolicy with its own IP address and kick out the first one. So the collector in the first one will

Problem:	Resolution:
No events seen in activity page.	<p>1. Check if ONTAP collector is in “RUNNING” state. If yes, then ensure that some cifs events are being generated on the cifs client VMs by opening some files.</p> <p>2. If no activities are seen, please login to the SVM and enter the following command. <code><SVM>event log show -source fpolicy</code> Please ensure that there are no errors related to fpolicy.</p> <p>3. If no activities are seen, please login to the SVM. Enter the following command <code><SVM>fpolicy show</code> Please check if the fpolicy policy named with prefix “metadata_service” has been set and status is “on”. If not set, then most likely the Agent is unable to execute the commands in the SVM. Please ensure all the prerequisites as described in the beginning of the page have been followed.</p>
SVM Data Collector is in error state and Error message is “Agent failed to connect to the collector”	<p>1. Most likely the Agent is overloaded and is unable to connect to the Data Source collectors.</p> <p>2. Check how many Data Source collectors are connected to the Agent.</p> <p>3. Also check the data flow rate in the “All Activity” page in the UI.</p> <p>4. If the number of activities per second is significantly high, install another Agent and move some of the Data Source Collectors to the new Agent.</p>
SVM Data Collector shows error message as "fpolicy.server.connectError: Node failed to establish a connection with the FPolicy server "12.195.15.146" (reason: "Select Timed out")"	<p>Firewall is enabled in SVM/Cluster. So fpolicy engine is unable to connect to fpolicy server. CLIs in ONTAP which can be used to get more information are:</p> <p>event log show -source fpolicy which shows the error event log show -source fpolicy -fields event,action,description which shows more details.</p> <p>Check firewall commands on the ONTAP side.</p>
Error Message: “Connector is in error state. Service name:audit. Reason for failure: No valid data interface (role: data,data protocols: NFS or CIFS or both, status: up) found on the SVM.”	Ensure there is an operational interface (having role as data and data protocol as CIFS/NFS).

Problem:	Resolution:
The data collector goes into Error state and then goes into RUNNING state after some time, then back to Error again. This cycle repeats.	<p>This typically happens in the following scenario:</p> <ol style="list-style-type: none"> 1. There are multiple data collectors added. 2. The data collectors which show this kind of behavior will have 1 SVM added to these data collectors. Meaning 2 or more data collectors are connected to 1 SVM. 3. Ensure 1 data collector connects to only 1 SVM. 4. Delete the other data collectors which are connected to the same SVM.
Connector is in error state. Service name: audit. Reason for failure: Failed to configure (policy on SVM svmname. Reason: Invalid value specified for 'shares-to-include' element within 'fpolicy.policy.scope-modify: "Federal"	<p>The share names need to be given without any quotes. Edit the ONTAP SVM DSC configuration to correct the share names.</p> <p><i>Include and exclude shares</i> is not intended for a long list of share names. Use filtering by volume instead if you have a large number of shares to include or exclude.</p>
There are existing fpolicies in the Cluster which are unused. What should be done with those prior to installation of Cloud Secure?	<p>It is recommended to delete all existing unused fpolicy settings even if they are in disconnected state. Cloud Secure will create fpolicy with the prefix "cloudsecure_". All other unused fpolicy configurations can be deleted.</p> <p>CLI command to show fpolicy list:</p> <p><i>fpolicy show</i></p> <p>Steps to delete fpolicy configurations:</p> <p><i>fpolicy disable -vserver <svmname> -policy-name <policy_name></i> <i>fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name></i> <i>fpolicy policy delete -vserver <svmname> -policy-name <policy_name></i> <i>fpolicy policy event delete -vserver <svmname> -event-name <event_list></i> <i>fpolicy policy external-engine delete -vserver <svmname> -engine-name <engine_name></i></p>
After enabling Cloud Secure, ONTAP performance is impacted: Latency becomes sporadically high, IOPs become sporadically low.	Ensure that you are using a Data ONTAP version where this issue is fixed.

If you are still experiencing problems, reach out to the support links mentioned in the **Help > Support** page.

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.