CLEONDRIS

Cleondris Technical Implementation Note | TIN-96

Cleondris Permissions on Data ONTAP

(Working Copy, 2023-10-21)

Cleondris GmbH, Switzerland

October 2023

IMPORTANT

The information given in this technical implementation note represents current internal planning for Cleondris and can be subject to further changes without further notice. As such, this document is subject to change and may be changed by Cleondris at any time without notice. The information is not intended to be binding upon Cleondris to any particular course of business, product strategy and/or development.

Table of Contents

1 Cleondris and ONTAP Communication Overview

For management purposes, Cleondris software communicates with NetApp Data ONTAP using the ONTAPI (ZAPI), REST API, NDMP and SnapDiff protocols.

Both the ONTAPI (ZAPI) and REST API are proprietary NetApp management interfaces, which are invoked by Cleondris software via a HTTPS endpoint on port 443 running on the NetApp Data ONTAP cluster management server or on a data SVM. The ONTAPI (ZAPI) and REST API access is mandatory for Cleondris software.

NDMP (Network Data Management Protocol) is an open protocol. NDMP is optionally used by Cleondris to implement file copy/restore and to optionally speed up volume indexing and analysis.

SnapDiff is another proprietary NetApp protocol, which is used by Cleondris to index and analyze volumes. SnapDiff access is mandatory for volume indexing (CDM/IDX products) and volume analysis (SnapGuard product).

This document describes the necessary steps to create a restricted login and optionally a NDMP user on NetApp Data ONTAP for use by Cleondris.

2 ONTAPI (ZAPI) and REST API Access

For historical reasons, the NetApp documentation refers to the ONTAPI (ZAPI) application programming interface sometimes simply as "ONTAPI" or "ZAPI" and in newer documentation "ONTAPI (ZAPI)".

The ONTAPI interface has been part of ONTAP for many years. With the release of ONTAP 9.6, NetApp has also added a REST interface. Initially, the REST interface only supported a subset of management capabilities available in ONTAPI, but with recent releases (ONTAP 9.10.1) the coverage is almost on par.

From a technical perspective, the two APIs are very similar. They both use a HTTPS over port 443, with the important difference that ONTAPI uses XML messages, while the REST API is JSON based.

Cleondris can connect to NetApp Data ONTAP using these protocols in two ways:

1. Via the cluster management server. This is a special SVM that allows Cleondris to work with all data SVMs on the cluster.
2. Via (one or more) data SVMs. This allows to display and control only the directly connected data SVMs in Cleondris.

Most customers will choose to connect via the cluster management server. However, if you don't own the cluster and only have access to one or more data SVMs, then you need to choose the second method.

Traditionally, Cleondris has used ONTAPI to manage NetApp ONTAP systems, and even with ONTAP 9.6+ did not use the REST API, due to lack of functionality. However, since NetApp added new functionality sometimes only in the REST API (e.g., SnapDiff V3 and SnapMirror Cloud starting with ONTAP 9.8), Cleondris had to use both APIs simultaneously.

Originally, NetApp planned to remove support for ONTAPI in NetApp ONTAP release 9.13.1, but as of February 2023, these plans have changed, current public NetApp documentation (CPC-00410) mentions that ONTAPI will only be removed in ONTAP release 9.18.1.

Please note:

- On ONTAP versions **7.x, 8.x and 9.1 – 9.7**, Cleondris only uses ONTAPI (ZAPI).
- On ONTAP versions **9.8 – 9.9.1**, Cleondris uses ZAPI and optionally REST for SnapMirror Cloud management.
- On ONTAP versions **9.10.1 – 9.13.1**, Cleondris uses ZAPI. For features not available in ZAPI (SnapMirror Cloud and SnapDiff V3 management), or to work around certain bugs, REST is being used.
- On ONTAP versions **9.14.1+** Cleondris will only use REST. A Cleondris release compatible with ONTAP 9.14.1+ is planned for Q1 2024.

2.1 Accessing NetApp Data ONTAP via the Cluster Management Server

Typically, in a demo lab for quick tests, Cleondris is connected via the cluster admin user "admin" (which has full ZAPI access) and no restricted user needs to be setup.

However, in production environments, a more documented and restricted setup is needed:

There are two steps involved in creating a restricted login:

1. A dedicated, restricted role needs to be created.
2. A dedicated user needs to be created that is assigned the above role.

To create a restricted role for use by Cleondris, you need administrative SSH access to the cluster management server of the respective Data ONTAP cluster. Then, enter the commands from the following sections.

NOTE: Depending on the used ONTAP versions, the commands may vary:

2.1.1 Commands for ONTAP versions 9.1 – 9.9.1:

Step 1: Please login to ONTAP using SSH and an admin user, then enter the following commands (you need to replace the text "*CLUSTER*" with the name of the cluster – the name is shown on the SSH prompt):

```
security login role create -vserver CLUSTER -role cln_role -cmddirname "cluster" -access all
security login role create -vserver CLUSTER -role cln_role -cmddirname "vserver" -access all
security login role create -vserver CLUSTER -role cln_role -cmddirname "system" -access readonly
security login role create -vserver CLUSTER -role cln_role -cmddirname "storage" -access readonly
security login role create -vserver CLUSTER -role cln_role -cmddirname "snapmirror" -access all
security login role create -vserver CLUSTER -role cln_role -cmddirname "volume" -access all
security login role create -vserver CLUSTER -role cln_role -cmddirname "network" -access readonly
security login role create -vserver CLUSTER -role cln_role -cmddirname "lun" -access all
security login role create -vserver CLUSTER -role cln_role -cmddirname "version" -access readonly
security login role create -vserver CLUSTER -role cln_role -cmddirname "job" -access readonly
security login role create -vserver CLUSTER -role cln_role -cmddirname "timezone" -access all
security login role create -vserver CLUSTER -role cln_role -cmddirname "metrocluster" -access readonly
```

Please note: the access type for the command directory "*timezone*" needs to be "*all*". This is due to a limitation in Data ONTAP (the timezone and current clock cannot be read with "readonly" access).

Step 2: To create a restricted user (called "***cln***" in the following example) that is using the above created role, enter the following command (please replace the text "*CLUSTER*" with the name of the cluster):

```
security login create -username cln -application ontapi -authmethod password -role
cln_role -vserver CLUSTER -comment "Cleondris"
```

When executing the above command, ONTAP will ask for a password for this new user.

2.1.2 Commands for ONTAP versions 9.10.1, 9.11.1, 9.12.1 and 9.13.1:

*Please ensure that you are using at least ONTAP **9.10.1P9**, **9.11.1P1** or **9.12.1**, otherwise you might run into ONTAP bug 1388040. If you are affected by the bug, please contact Cleondris support for a workaround.*

Step 1: Please login to ONTAP using SSH and an admin user, then enter the following commands (you need to replace the text "*CLUSTER*" with the name of the cluster – the name is shown on the SSH prompt):

```
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/cluster -access all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/svm -access all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/cloud -access all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/name-services -access
all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/storage -access
readonly
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/storage/volumes -
access all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/storage/luns -access
all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/storage/file -access
all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/storage/snapshot-
policies -access all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/snapmirror -access
all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/network -access
readonly
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/protocols -access all
security login rest-role create -vserver CLUSTER -role cln_role_rest -api /api/private -access all
```

Step 2: To create a restricted user (called "***cln***" in the following example) that is using the above created role, enter the following command (again, please replace the text "*CLUSTER*" with the name of the cluster):

```
security login create -username cln -application http -authmethod password -role
cln_role_rest -vserver CLUSTER -comment "Cleondris"
```

When executing the above command, ONTAP will ask for a password for this new user.

Step 3: The user needs also access ONTAPI (ZAPI), this is why you also need to enter the following command (again, please replace the text "*CLUSTER*" with the name of the cluster):

```
security login create -username cln -application ontapi -authmethod password -role
cln_role_rest -vserver CLUSTER -comment "Cleondris"
```

2.1.3 Adding the cluster in the Cleondris setup screen

When adding this cluster in the Cleondris setup, you need to the enter the following:

- Hostname: IP address or hostname of a cluster management interface
- Username: "cln"
- Password: The above entered password.

To list the available IP addresses of the cluster management server, enter the following in a NetApp Data ONTAP SSH session:

```
network interface show -role cluster-mgmt
```

2.2 Accessing NetApp Data ONTAP via a Data SVM

This is typically needed if you don't have access to the cluster management interface.

You can connect Cleondris directly to one or more data SVMs on a cluster, however, in this case you must not connect Cleondris to the same cluster via the cluster management server.

For each data SVM that you want to access from Cleondris, there are two steps involved:

1. A dedicated user needs to be created that is assigned the default "vsadmin" role
2. You must ensure that the SVM has at least one management network interface

To create a user (called "**cln**" in the following example) that is using the "vsadmin" role, enter the following command (please replace the text "SVM" with the name of the data SVM):

2.2.1 Commands for ONTAP versions 9.1 – 9.9.1:

```
security login create -username cln -application ontapi -authmethod password -role vsadmin -
vserver SVM -comment "Cleondris"
```

When executing the above command, ONTAP will ask for a password for the new user (please replace the text "*SVM*" with the name of the SVM).

2.2.2 Commands for ONTAP versions 9.10.1, 9.11.1, 9.12.1 and 9.13.1:

```
security login create -username cln -application http -authmethod password -role vsadmin -
vserver SVM -comment "Cleondris"
```

When executing the above command, ONTAP will ask for a password for the new user (please replace the text "*SVM*" with the name of the SVM).

The user needs also access to the ZAPI, this is why you also need to enter the following command (again, please replace the text "*SVM*" with the name of the SVM):

```
security login create -username cln -application ontapi -authmethod password -role vsadmin -
vserver SVM -comment "Cleondris"
```

2.2.3 Adding the SVM in the Cleondris setup screen

When adding this data SVM in the Cleondris setup, you need to the enter the following:

- Hostname: IP address or hostname of a management interface of the data SVM
- Username: "cln"
- Password: The above entered password.

Even though this is just a data SVM, it needs to be added in Cleondris as an ordinary cluster. In the inventory, Cleondris will display this as a "single-SVM" cluster, the hardware model will be shown as "SVM". Cluster level information, e.g., aggregates or node details, won't be available, ONTAP does not make this information available via data SVMs.

To list the available IP addresses of the data SVM, enter the following in a NetApp Data ONTAP SSH session (replace "SVM" with the actual name):

```
# network interface show -vserver SVM -fields lif,services,address
```

Please note: both API/REST only works on data SVM network interfaces that are configured with the "*management-https*" service and the "*mgmt*" firewall policy. If needed, add another data interface (exclusive for management purposes) and configure it with the "*default-*

management" service-policy (which includes the "*management-https*" service) and the "*mgmt*" firewall policy.

2.3 Upgrading from ONTAP 9.9.1 or earlier to ONTAP 9.10.1+

If you are already using Cleondris and are updating your ONTAP clusters to 9.10.1 (or newer), then the permissions for the existing, dedicated Cleondris user needs to be updated, otherwise support for SnapDiff V3 and SnapMirror Cloud is not possible.

The straightforward way is to remove the existing user and the assigned legacy role, then create the "rest-role" and re-create the user with the commands from the previous section.

Step 1: Inspect current roles and assigned users (replace "CLUSTER" with the name of the cluster):

```
security login show -vserver CLUSTER
security login role show -vserver CLUSTER
security login rest-role show -vserver CLUSTER
```

Note: the "role show" commands may also show legacy role entries that are automatically created when defining a "rest-role". These entries disappear when the corresponding "rest-role" is deleted.

Step 2: Remove any existing Cleondris users and roles:

```
security login delete -user-or-group-name cln -application * -authentication-method *^
security login role delete -role cln_role -cmddirname *
security login rest-role delete -role cln_role_rest -api *
```

Step 3: Re-create the role and user according to the instructions in the previous sections.

3 Optional NDMP Access

Cleondris software can optionally use the NDMP interface of Data ONTAP to implement file copy/restore and to speed up the analysis of volumes (by default, SnapDiff is used, which is not very fast when performing a baseline scan of a snapshot). Cleondris implements the NetApp specific "CAB" (Cluster-Aware-Backup) extension for NDMP and is fully compatible with the advanced NDMP implementation of NetApp Data ONTAP.

On the NetApp Data ONTAP cluster, NDMP only needs to be enabled on the cluster admin SVM. Using the NDMP CAB extension, Cleondris software can inspect all volumes of the cluster, no matter to which SVM they belong.

3.1 Checking NDMP Status on the Cluster

Enter the following commands to check NDMP on the cluster:

```
system services ndmp node-scope-mode status
```

→ The output should be "*NDMP node-scope-mode is disabled.*" (this is the default).

```
vserver ndmpd show
```

→ The line for the cluster admin SVM must indicate that NDMP is enabled ("true") and the authentication type must be "challenge". The status of non-admin vservers is not important for NDMP access from Cleondris software products.

3.2 Enabling NDMP for the Cluster Admin SVM

In case NDMP is not enabled yet on the cluster admin SVM, proceed as follows:

- **In case node-scope mode is enabled, please check with your backup team**. This is an indication that the backup team is using a legacy tape backup solution and you should not change NDMP to vserver-scoped mode. For backwards-compatibility, Cleondris software fully supports node-scoped mode.
- **To enable NDMP on the cluster admin SVM, enter the following command**:
  `vserver services ndmp modify –vserver <svm_name> -enable true`
  (please replace the text `<svm_name>` with the name of the svm)

3.3 Creating a NDMP Password Hash

NDMP users do not have their own distinct password, rather they access the system using a hash of the password of a local user that has the ***necessary backup privileges***. To use the "admin" user, enter the following command (again, please replace the text "CLUSTER" with the name of the cluster):

```
vserver ndmpd generate-password -vserver CLUSTER -user admin
```

The shown username and hash (e.g., "admin" / "K5oDDoeGGapYH4kL") can then be used to configure an optional NDMP user in Cleondris software. **In case you later change the**

password of the underlying ONTAP user, you must re-execute the "generate-password" command again to retrieve the new hash (as long as the password is not changed, re-executing this command will always yield the same hash result).

If you want to use another user, then please check the respective documentation for the Data ONTAP release of your cluster. However, please note that there are no privileges that can be removed from an NDMP user – either the user has full NDMP access or none.

4 Optional SnapDiff Access

SnapDiff is proprietary NetApp protocol and only available to selected NetApp implementation partners. Cleondris uses SnapDiff to index (CDM/IDX products) and analyze (SnapGuard product) volumes on ONTAP. If the SnapDiff endpoint cannot be accessed by Cleondris, then the above-mentioned features are not available.

4.1 How Cleondris uses SnapDiff

Depending on the ONTAP release, Cleondris either uses SnapDiff V1 or V3.

- For ONTAP versions **7.x, 8.x and 9.1 – 9.13.1** Cleondris can use SnapDiff V1 which is part of the ZAPI interface. **Therefore, no specific configuration is needed, since Cleondris simply uses the ZAPI interface to access SnapDiff V1 functionality on ONTAP.**
- For ONTAP versions **9.10.1** and following**,** Cleondris by default tries to use the newer SnapDiff V3. **SnapDiff V3 is much more performant than SnapDiff V1, but also requires a slightly more complex network setup and REST access.**

4.2 Why SnapDiff V3 should be used on ONTAP 9.10.1+

NetApp has announced that the support for SnapDiff V1/V2 is eventually going to be removed and all customers must eventually use SnapDiff V3.

Initial plans removed the support in ONTAP 9.10.1GA, but NetApp has re-added SnapDiff V1, since too many customers still rely on it.

Nevertheless, officially SnapDiff V1/V2 is deprecated with ONTAP 9.10.1 and customers should switch as early as possible to SnapDiff V3. At the present, it is unclear whether ONTAP 9.14.1 is going to support SnapDiff V1/V2.

Cleondris can use SnapDiff V3 out of the box, but unfortunately you must adjust some ONTAP settings and your network setup first, so that the access with SnapDiff V3 is possible at all.

Please note: this change does not only affect Cleondris, but all partner applications that access SnapDiff.

References:

CPC-00352: Deprecation of SnapDiff v1 and v2 APIs and the impact on third-party data protection applications supporting SnapDiff

https://mysupport.netapp.com/info/communications/ECMLP2876788.html

FAQ: SnapDiff Support in ONTAP

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapDiff/FAQ%3A_SnapDiff_Support_in_ONTAP

4.3 What has changed with SnapDiff V3

The way partner applications (like Cleondris) need to communicate with ONTAP to perform SnapDiff operations has changed with SnapDiff V3:

- SnapDiff V1 is part of the ZAPI interface.
- SnapDiff V3 requires two communication channels: sessions are initiated via the REST interface and session data is retrieved using an RPC protocol (similar to NFS) via TCP port 2049 on SVM data LIFs.

4.4 Checklist for SnapDiff V3 Access

To ensure that Cleondris can access SnapDiff V3 functionality on ONTAP 9.10.1+, please check the requirements in the following sections.

4.4.1 Data LIF Requirements

For each SVM where volumes need to be processed with SnapDiff V3, ensure that at least one data interface is present that uses a service-policy which contains the "*data-nfs*" service.

Important: the NFS service does **not** need to be enabled on the SVM, only the "*data-nfs*" entry must be present in the services for at least one data interface. Typically, one uses the "*default-data-files*" service-policy which already contains the "*data-nfs*" service.

```
network interface show -vserver SVM -fields lif, service-policy, services

vserver lif service-policy services

------- --- -------------- --------

SVM  test_lif_001  default-data-files  data-core,data-nfs,data-cifs,data-
flexcache,data-fpolicy-client,data-dns-server

SVM  test_lif_002  custom-data-7854  data-core,management-ssh,management-
https,data-fpolicy-client,data-dns-server,management-http,backup-ndmp-
control,management-snmp-server
```

4.4.2 Network / Firewall / Routing Requirements

You need to ensure that routing/firewalling between the Cleondris appliance and the data interfaces of the SVM (which contains the volume to be inspected via SnapDiff) is not too restrictive. When establishing the SnapDiff V3 RPC connection, Cleondris automatically chooses a data interface that has the required "*data-nfs*" entry in its service list.

Cleondris needs to be able to establish TCP connections to port 2049 of the selected data LIF of the SVM. On current ONTAP versions the SnapDiff V3 RPC endpoint is **only** available on data LIFs of the respective SVM.

4.4.3 Login Requirements

To start a SnapDiff V3 session, Cleondris needs to execute REST calls. Please ensure that you have followed the instructions in section 2 to ensure that the account used by Cleondris has access to the REST features.

4.4.4 SnapDiff RPC server

Cleondris versions 8.0.2211 (and newer) can automatically enable the so-called SnapDiff RPC server feature on ONTAP when using SnapDiff V3 on an SVM. No special precautions are needed. However, when using earlier Cleondris versions, the SnapDiff RPC server needs to be enabled manually on each SVM where SnapDiff shall be used:

https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-cmpr-900%2FTOC__vserver__snapdiff-rpc-server.html

4.5 How to use SnapDiff V1 on ONTAP 9.10.1+

By default, Cleondris uses SnapDiff V3 on ONTAP 9.10.1 and newer. To change the default behavior and force the use of SnapDiff V3 please use the following instructions.

Procedure:

- Ensure that you are using Cleondris release 8.0.2304 or newer.
- In the "Setup > NetApp" screen, edit the details of the respective cluster and change the value in the SnapDiff version selection dropdown from "Automatic" to "SnapDiff V1".

.

Cleondris GmbH
Buckhauserstrasse 17
CH-8048 Zürich