NetApp SnapLock

This page provides a guide to configuring a NetApp SnapLock storage as a Storage Target in Verba.

SnapLock is an alternative to the traditional optical "write once, read many" (WORM) data. SnapLock is used for the storage of read-only WORM data. SnapLock is a license-based, disk-based, open-protocol feature that works with application software to administer non-rewritable storage of data. The primary objective of this Data ONTAP feature is to provide storage-enforced WORM and retention functionality by using open file protocols such as CIFS. SnapLock can be deployed for protecting data in strict regulatory environments in such a way that even the storage administrator is considered an untrusted party. SnapLock provides special purpose volumes in which files can be stored and committed to a nonerasable, non-rewritable state either forever or for a designated retention period. SnapLock allows this retention to be performed at the granularity of individual files through standard open file protocols such as CIFS.

For a general description of storage targets, please refer to Storage and export targets.

Please refer to the official NetApp SnapLock guide to deploy and configure the NetApp system.

Verba uses the NetApp Manageability SDK to access the WORM specific features of the Data ONTAP API.

NetApp SnapLock permissions

The system uses standard SMB protocol for file operations. The following permissions must be enabled:

- read,
- write,
- delete,
- list.

The system requires permission for the following Data ONTAP API calls:

- Cluster mode (NetApp v9.x or later with cluster mode enabled):
  - snaplock-get-node-compliance-clock
  - snaplock-set-file-retention
  - snaplock-get-file-retention
- 7-mode (NetApp v8.x or earlier):
  - snaplock-get-system-compliance-clock
  - file-set-snaplock-retention-time
  - file-get-snaplock-retention-time

Configuring the DATA ONTAP API permissions on NetApp v9.x or later (cluster mode)

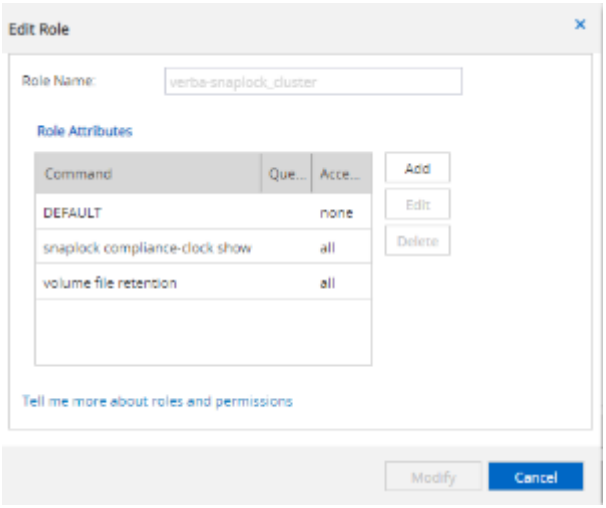
Follow the steps below to create a user account on NetApp with the necessary permissions:

Step 1 - Login to the cluster **OnCommand System Manager**

Step 2 - Navigate to **Settings** by pressing the gear icon on the top right

Step 3 - Create a new cluster-level role. Click on the **Roles** link on the right panel under the **Management** section, press **Add**. In the new window define the **Role Name** and add the **Role Attributes** by clicking on the **Add** button as follows:

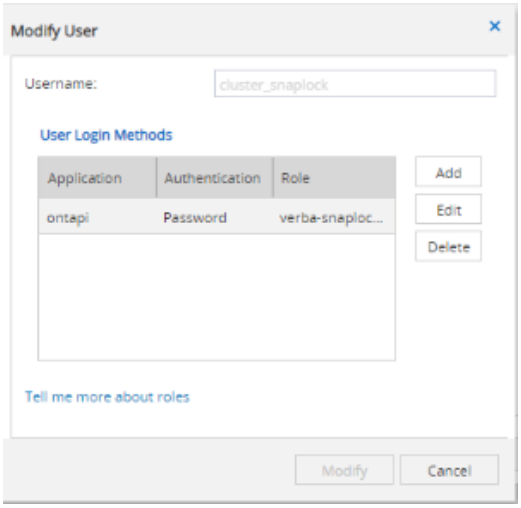
Command	Query	Access Level
snaplock compliance-clock show		All
volume file retention		All



Step 4 - Press **Add** to save the new role

Step 5 - Create a new cluster-level user. Click on the **Users** link on the right panel under the **Management** section, press **Add**. In the new window define the **Username**, **Password** and add the **User Login Method** by clicking on the **Add** button as follows:

Application	Authentication	Role
ontapi	Password	The name of the previously create cluster-level role



Step 6 - Press **Add** to save the new user

Configuring the DATA ONTAP API permissions on NetApp v8.x or earlier (7-mode)

Follow the steps below to create a user account on NetApp with the necessary permissions:

Step 1 - Login to the NetApp server via SSH

Step 2 - Run the following commands to create a new role with the required permissions:

```
useradmin role add your_new_verba_role_name -a login-http-admin,api-
snaplock-get-system-compliance-clock,api-file-set-snaplock-retention-
time,api-file-get-snaplock-retention-time
```

Step 3 - Run the following commands to create a new group and assign the new role to the group:

```
useradmin group add your_new_verba_group_name -r your_new_verba_role_name
```

Step 4 - Run the following commands to create a new user and add the user to the new group:

```
useradmin domainuser add your_new_user_name -g your_new_verba_group_name
```

NetApp SnapLock compliance clock

When Verba uploads / moves media files to a NetApp SnapLock storage target, setting the retention period with auto-delete it takes the clock drift of SnapLock into account at the point of the file move. If the storage goes down at any time during the retention period (between the upload / move and the date of auto-deletion) Verba will not be able to retrieve that information, thus will try to delete the files in question earlier than SnapLock would allow it. As a result, auto-deletion by Verba policies might fail.

Creating a NetApp SnapLock target

Follow the steps below to create a new Verba Storage target for NetApp SnapLock:

Step 1 - Open the Verba Web interface then select **Data Management > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select NetApp SnapLock
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)

Volume Path	Specify the NetApp specific volume path. Run the following command to find out the volume path:
	
	volume show
	
	Example:
	
	`verba::> volume show`
	`Vserver Volume Aggregate State Type Size Available Used%`
	`--------- ------------ ------------ ---------- ---- ---------- ---------- -----`
	`verba-01 vol0 aggr0_verba_01 online RW 3.16 GB 2.05GB 31%`
	`vs1.verbatest.local test_volume vfs online RW 342.5MB 50.46 MB 84%`
	`vs1.verbatest.local svm_root vmd online RW 20MB 17.48 MB 7%`
	
	The Volume Path value is:
	
	`/vol/test_volume`

Host Name or IP Address	The connection string used by the application to connect to the NetApp SnapLock Data ONTAP API. Depending on the version of the NetApp SnapLock system, 7-mode or cluster mode can be configured.

For 7-mode NetApp SnapLock systems:

- **7-mode system with a connection to the NetApp server**: de
  ne the FQDN or IP address of the NetApp server without defining the protocol (it will be HTTPS by default)

```
netapp_server_address
```

- **7-mode system with a connection to the vFiler**: define the hostname or IP address of the NetApp vFiler, HTTP protocol must be defined

```
http://netapp_vfiler_address
```

- **7-mode system with vFiler tunneling to allow HTTPS connections**: define the hostname or IP address of the NetApp server and the instance name of the vFiler after a comma (,) or semicolon (;), without defining the protocol (it will be HTTPS by default)

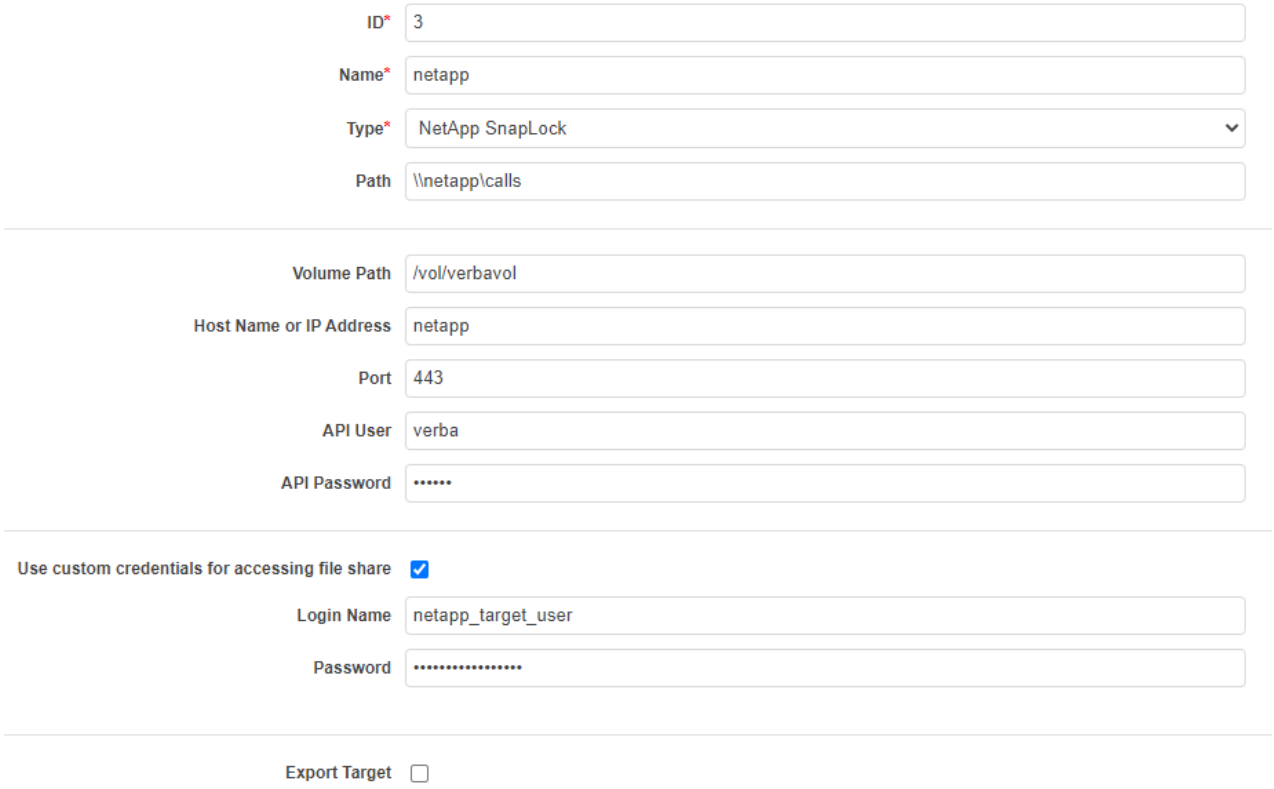
```
netapp_server_address;
instancename
```

	For **cluster mode,** further parameters are needed which can be advertised in the Host Name or IP Address field:
	
	• cluster FQDN or IP address
	• cluster_mode=1, which enables cluster mode in the API
	• vserver=, the name of the vServer hosting the storage folder
	• node=node hosting the vserver
	
	The parameters should be concatenated either with ; or ,
	
	`netapp_server_address;`
	`cluster_mode=1,`
	`vserver=vserver_name,`
	`node=node_name`
	
	The parameters can be determined from NetApp console with the following commands:
	
	• *vserver show*
	• *node show*
	
	Example:
	
	The IP address of the server is 10.2.1.13
	
	`verbalabs::> vserver show`
	`Admin Operational Root`
	`Vserver Type Subtype State`
	`State Volume Aggregate`
	`test data default running`
	`running test_root test_root`
	`verbalabs admin - - - - -`
	`verbalabs-01`
	`node - - - - -`
	
	`verbalabs::> node show`
	`Node Health Eligibility`
	`Uptime Model Owner Location`
	`verbalabs-01 true true 1`
	`days 15:54 SIMBOX`
	
	Then hostname field value is:
	
	`10.2.1.13;cluster_mode=1;`
	`vserver=test;node=verbalabs-`
	`01`

Port	The access port of the NetApp SnapLock Data ONTAP API (443 by default)
API User	User name of the API user configured for Verba access in NetApp SnapLock

API Password	Password of the API user configured for Verba access in NetApp SnapLock
Use custom credentials for accessing the file share	It is possible to use credentials other than the service user for each NetApp SnapLock storage. Provide the username and password credentials for accessing the storage through SMB.

Step 4 - Click **Save** to save the settings



After this point, the Storage target is available for use by other Verba components (e.g. Data management policies).

Configuring SSL certificates for the SnapLock Data ONTAP API connection

NetApp SnapLock can be configured to accept SSL connections from trusted sources only. You can configure the trusted and signed certificates used by the Verba system on the servers directly. If you intend to use multiple NetApp SnapLock systems for Verba, you need to use the same certificates for all, because it is a server-side setting in the Verba system. By default, Verba uses its own self-signed certificates for the SSL connection.

Follow the steps below to configure the certificates.

Step 1 - Copy the X.509 certificate and key files to the Verba server

Step 2 - Navigate to the **Configuration / Servers**

Step 3 - Click on the Verba server you would like to configure

Step 4 - Click on the **Change Configuration Settings** tab

Step 5 - Open the **Storage Management / Upload Targets / NetApp SnapLock** tree on a Verba Recording Server or the **Storage Management / Storage Targets / NetApp SnapLock** tree on a Verba Media Repository server or on a Verba Media Repository and Recording Server

Step 6 - Configure a trusted custom X.509 certificate for the connection

Step 7 - Click the **Save** icon and follow the instructions on the page to apply the configuration on the server

Step 8 - Repeat the steps above on all Verba servers where you move files to NetApp SnapLock