Acronis Cyber Infrastructure 3.0

Storage User's Guide

November 20, 2019

Copyright Statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Contents

CHAPTER 1

Supported Storage Types

Your service provider can configure Acronis Cyber Infrastructure to keep your data in three storage types:

- S3 object storage for storing an unlimited number of objects (files).
- iSCSI block storage for virtualization, databases, and other needs.
- NFS shares for storing an unlimited number of files via a distributed filesystem.

The following sections describe the ways to access data in Acronis Cyber Infrastructure in detail.

CHAPTER 2

Accessing S3 Buckets

To access S3 buckets, get the following information (credentials) from your system administrator:

- user panel IP address
- DNS name of the S3 endpoint
- access key ID
- secret access key

Acronis Cyber Infrastructure allows you to access your S3 data in several ways:

- via the Acronis Cyber Infrastructure user panel
- via a third-party S3 application like Cyberduck, Mountain Duck, Backup Exec, etc.

2.1 Managing Buckets via the Acronis Cyber Infrastructure User Panel

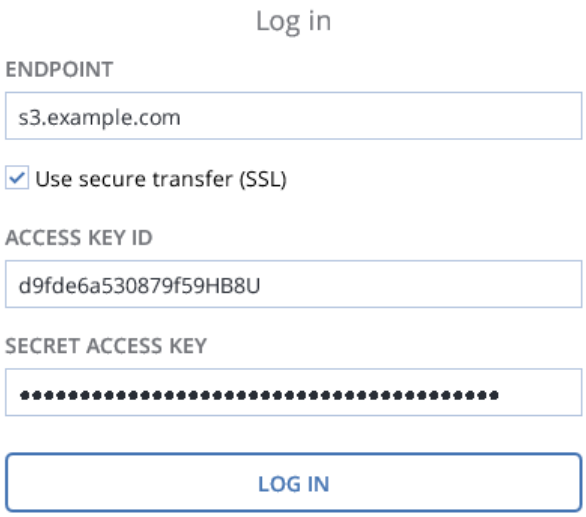
This section describes how to manage buckets and their contents from the Acronis Cyber Infrastructure user panel.

2.1.1 Logging in to User Panel

To log in to the Acronis Cyber Infrastructure user panel, do the following:

1. On any computer with access to the web interface, in a web browser visit

`http://<user_panel_IP_address>:8888/s3/`.



2. On the login screen, enter your credentials and click **LOG IN**.

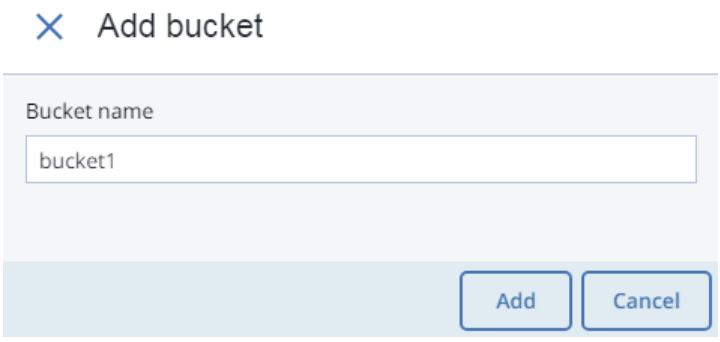
Once you log in to the web interface, you will see the **Buckets** screen with the list of your buckets. From here, you can manage buckets as well as folders and files stored inside the buckets.

To log out, click the user icon in the upper right corner of any screen and click **Log out**.

2.1.2 Adding, Deleting, and Listing S3 Buckets

On the **Buckets** screen:

- To add a new bucket, click **Add bucket**, specify a name, and click **Add**.



  Use bucket names that comply with DNS naming conventions. For more information on bucket naming, see *S3 Bucket and Key Naming Policies* (page 13).

- To delete a bucket, select it and click **Delete**.

- To list bucket contents, click a bucket name in the list.

2.1.2.1 Listing S3 Bucket Contents in a Browser

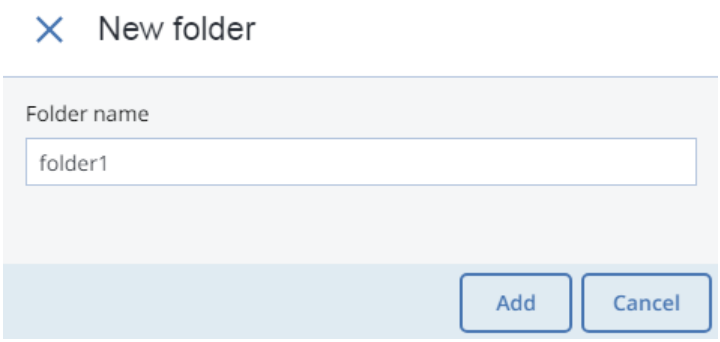
You can list bucket contents with a web browser. To do this, visit the URL that consists of the external DNS name for the S3 endpoint that you specified when creating the S3 cluster and the bucket name. For example, `mys3storage.example.com/mybucket`.

Note: You can also copy the link to bucket contents by right-clicking it in CyberDuck, and then selecting **Copy URL**.

2.1.3 Creating, Deleting, and Listing Folders

On the bucket contents screen:

- To create a folder, click **New folder**, specify folder name in the **New folder** window, and click **Add**.

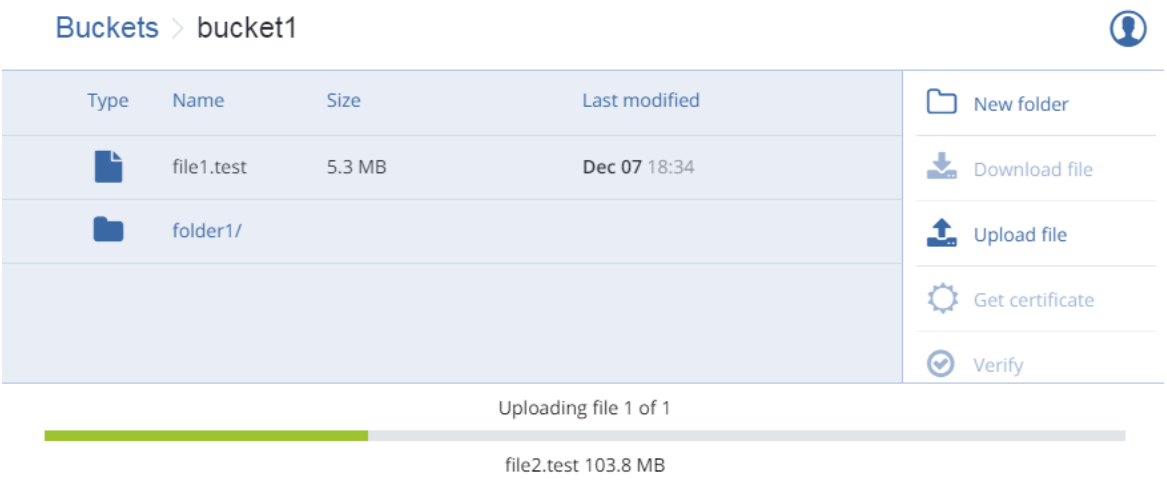


- To delete a folder, select it and click **Delete**.
- To list folder contents, click a folder name.

2.1.4 Uploading and Downloading Files

On the bucket or folder contents screen:

- To upload files to S3, click **Upload** and choose files to upload.



- To download files, select them and click **Download**.

2.1.5 Obtaining and Validating File Certificates

Acronis Cyber Infrastructure offers integration with the Acronis Notary service to leverage blockchain notarization and ensure the immutability of data saved in S3 buckets.

To certify files stored in your buckets, ask your system administrator to enable the Acronis Notary service for the buckets.

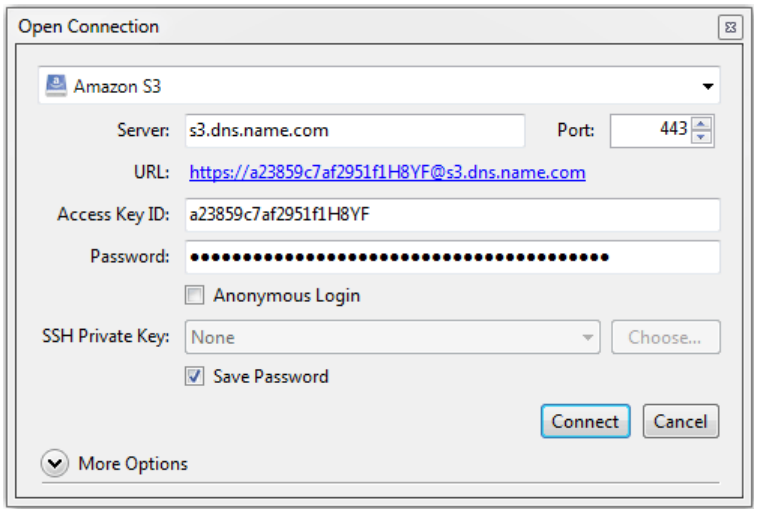
After that, you will be able to do the following:

- To get a notarization certificate for a file, select it and click **Get Certificate**.
- To check the validity of a file's certificate, click **Verify**.

2.2 Accessing S3 Storage with CyberDuck

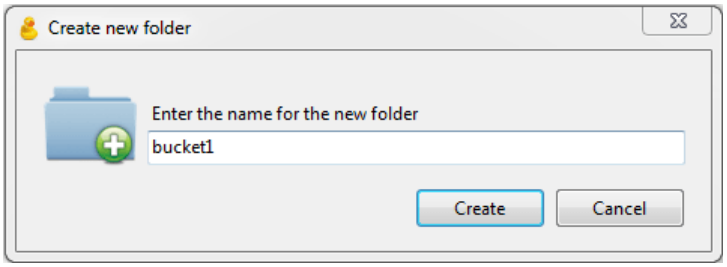
To access Acronis Cyber Infrastructure with CyberDuck, do the following:

1. In CyberDuck, click **Open Connection**.
2. Specify your credentials:
    - The DNS name of the S3 endpoint.
    - The **Access Key ID** and the **Password**, the secret access key of an object storage user.



By default, the connection is established over HTTPS. To use CyberDuck over HTTP, you must install a special S3 profile.

3. Once the connection is established, click **File** > **New Folder** to create a bucket.



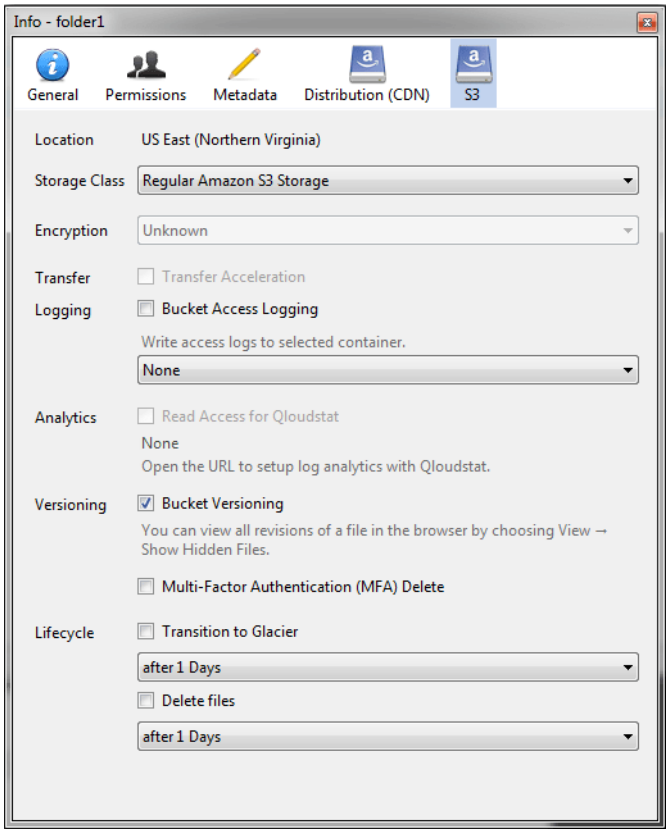
4. Specify a name for the new bucket, and then click **Create**. Use bucket names that comply with DNS naming conventions. For more information on bucket naming, see *S3 Bucket and Key Naming Policies* (page 13).

The new bucket will appear in CyberDuck. You can manage it and its contents.

2.2.1 Managing S3 Bucket Versions

Versioning is a way of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. For more information about bucket versioning, refer to the Amazon documentation.

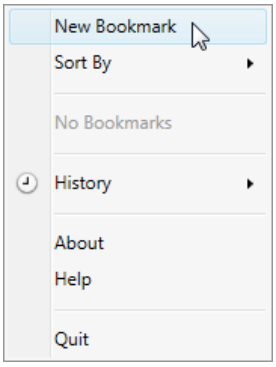
Bucket versioning is turned off by default. In CyberDuck, you can enable it in bucket properties. For example:



2.3 Mounting S3 Storage with Mountain Duck

Mountain Duck enables you to mount and access Acronis Cyber Infrastructure S3 storage as a regular disk drive. Do the following:

1. If your service provider has provided you with an SSL certificate, install it.
2. In Mountain Duck, click **New Bookmark**.

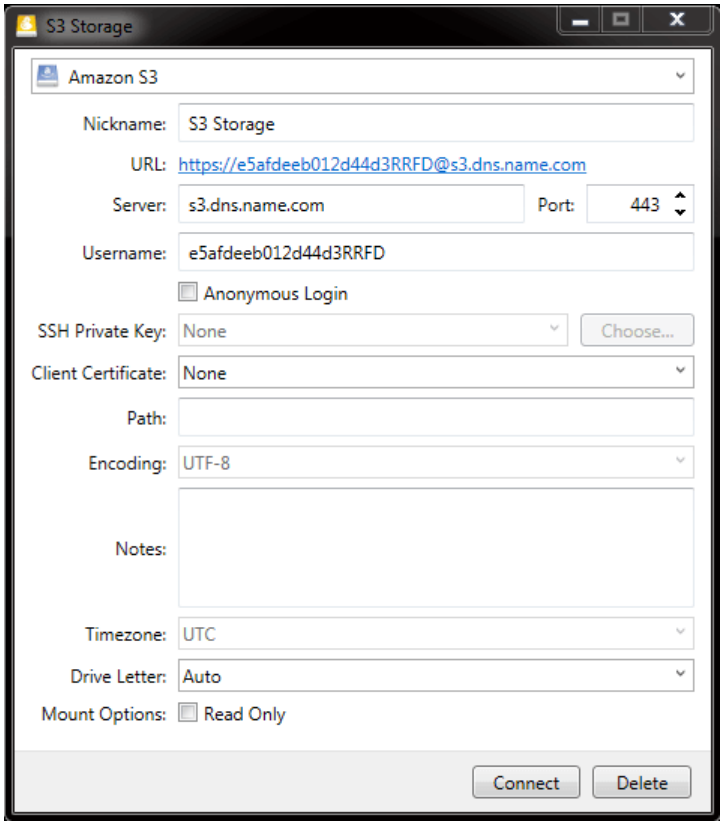


3. In the properties window, select **Amazon S3** profile from the first drop-down list and specify the

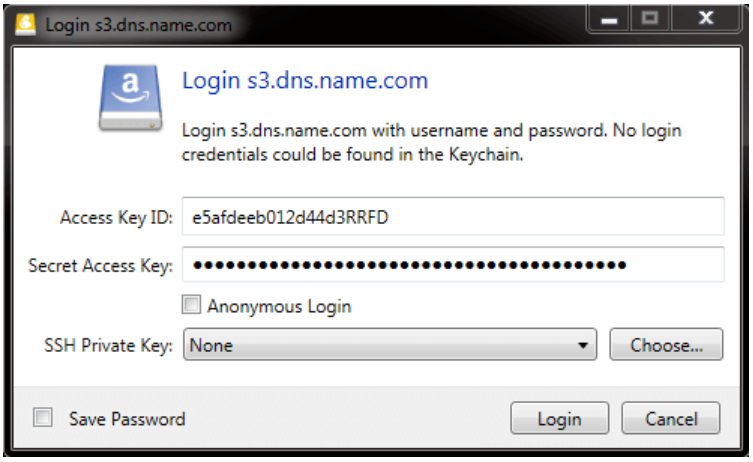
following parameters:

- **Nickname** of the disk drive
- endpoint DNS name in the **Server** field
- access key ID in the **Username** field

Click **Connect**.



4. In the login window, specify **Secret Access Key** and click **Login**.



Mountain Duck will mount the S3 storage as a disk drive. On the disk, you can manage buckets and store files in them.

2.3.1 Creating S3 Buckets on Mounted S3 Storage

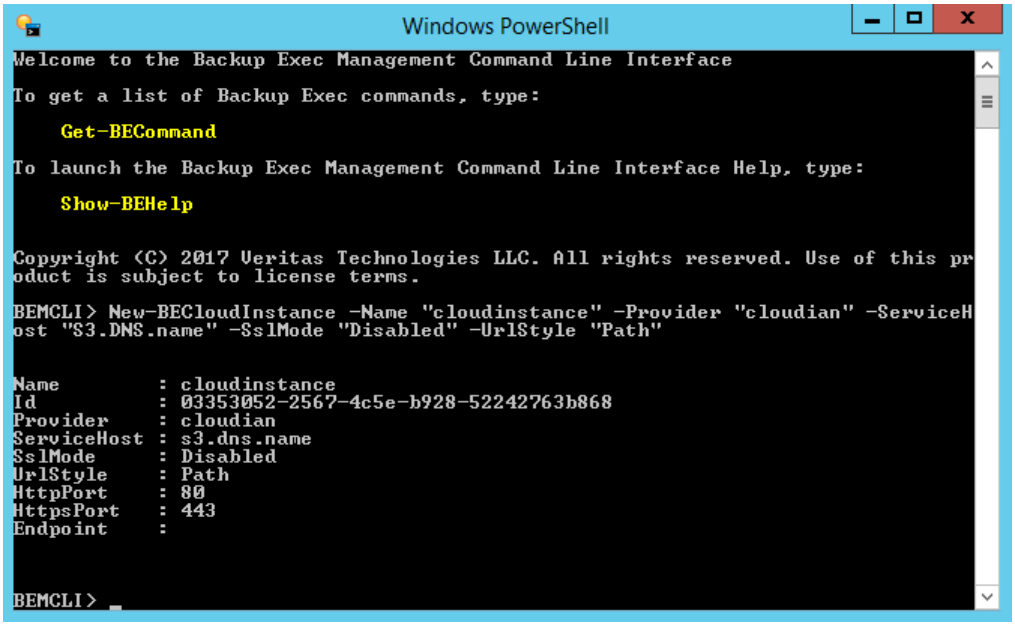
Windows and Mac OS X, operating systems supported by Mountain Duck, treat buckets as folders in case the S3 storage is mounted as a disk drive. In both operating systems, the default folder name contains spaces. This violates bucket naming conventions (see *S3 Bucket and Key Naming Policies* (page 13)), therefore you cannot create a new bucket directly on the mounted S3 storage. To create a bucket on a mounted S3 storage, create a folder with a name complying with DNS naming conventions elsewhere and copy it to the root of the mounted S3 storage.

2.4 Configuring Backup Exec to Keep Backups in S3 Storage

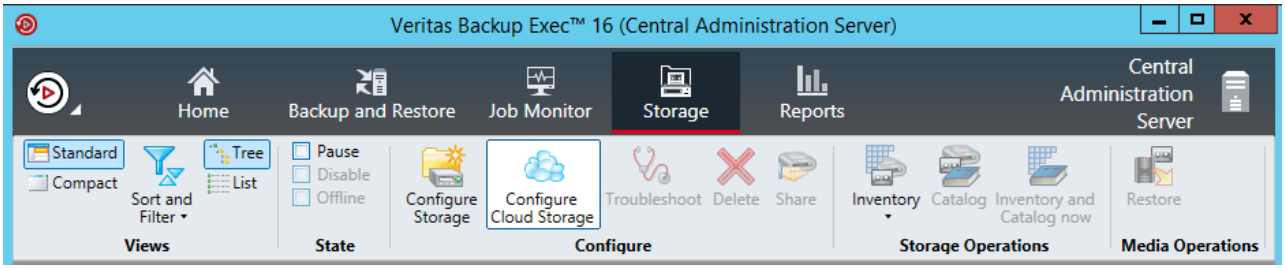
To store Backup Exec backups in S3 storage, do the following:

1. Create a bucket to store backups either using the Acronis Cyber Infrastructure user panel or another application.
2. Install Backup Exec. During installation, make sure so select all the components of Backup Exec and check all the updates.
3. Run `CLILauncher` located in `C:\Program Files\Veritas\Backup Exec`.
4. In the Backup Exec command-line prompt, run the following command:

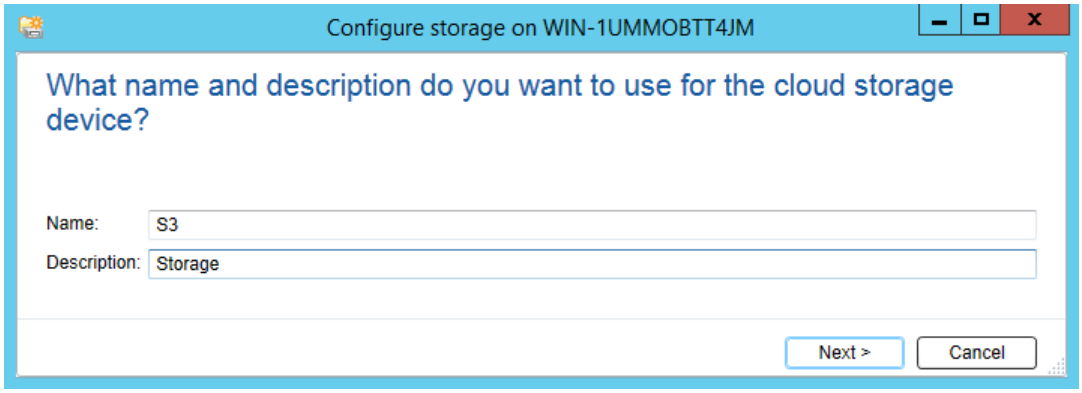
```
# New-BECloudInstance -Name "cloudinstance" -Provider "cloudian" \
-ServiceHost "<S3_DNS_name>" -SslMode "Disabled" -UrlStyle "Path"
```



5. In Backup Exec, click **Configure Cloud Storage** on the **Storage** tab.

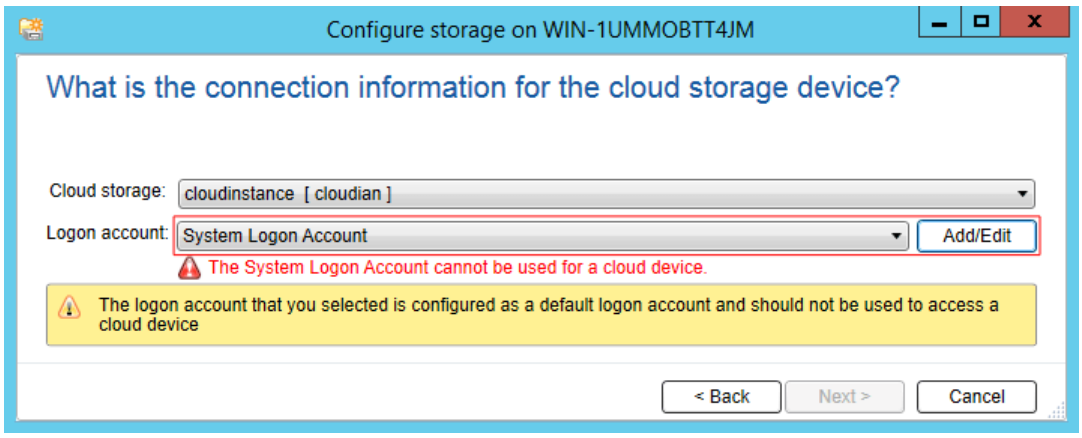


6. In the **Configure storage...** window, specify a name for the S3 storage and click **NEXT**.



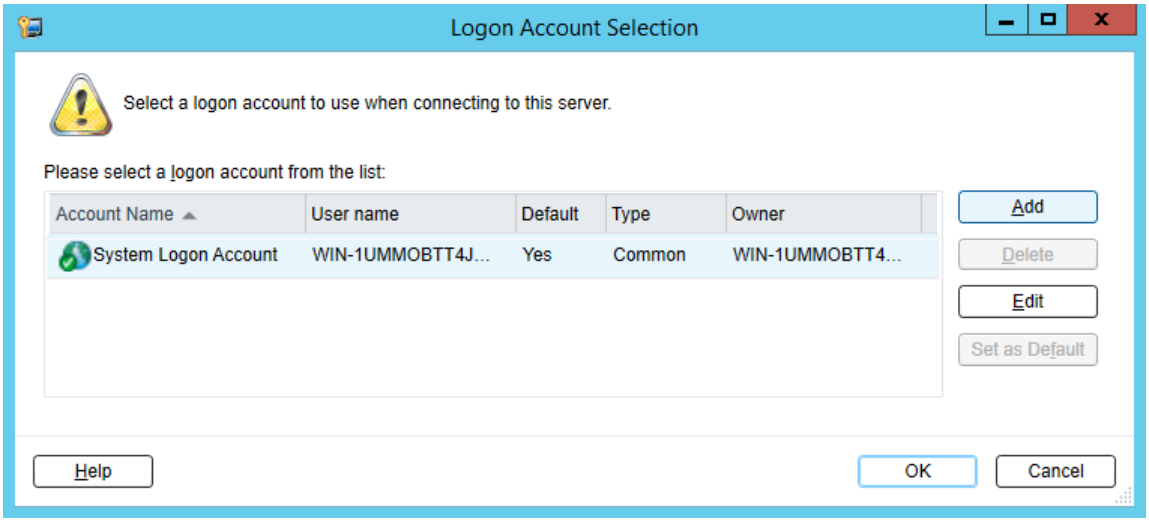
7. Select the **S3** device and click **NEXT**.

8. Select **cloudinstance [cloudian]** from the **Cloud storage** drop-down list.



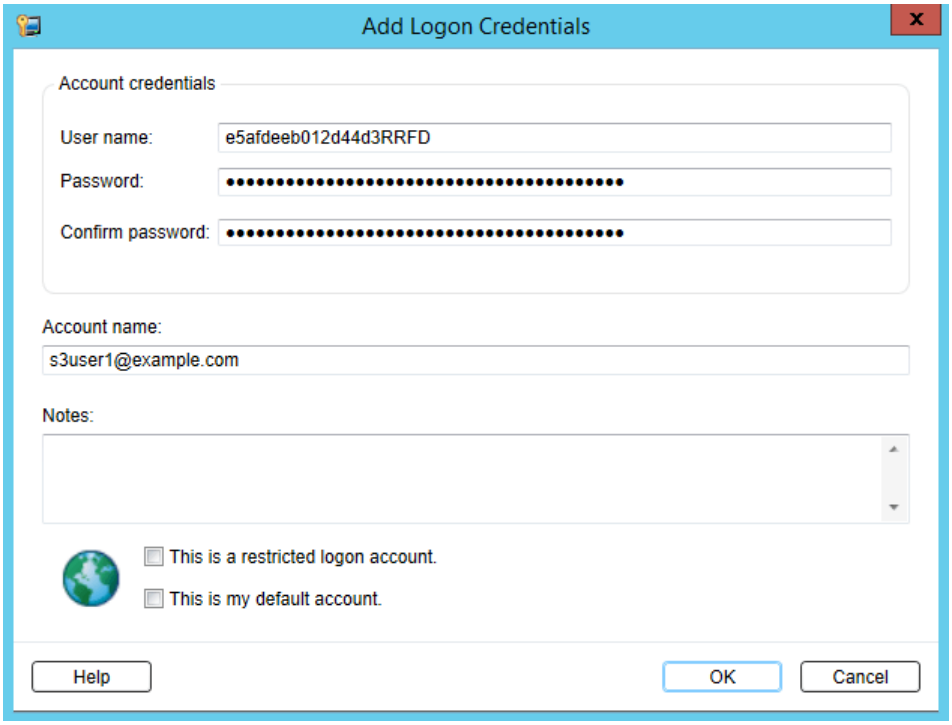
9. Click **Add/Edit** next to the **Logon account** drop-down list.

10. In the **Logon Account Selection** window, click **Add**.



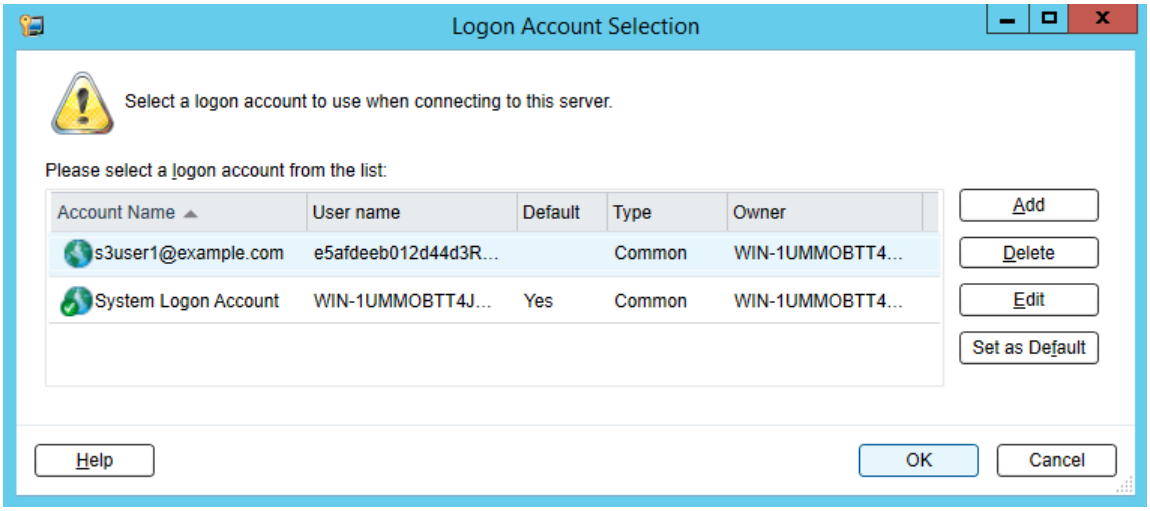
11. In the **Account credentials** section, specify your credentials:

    1. S3 access key ID in the **User name** field.
    2. S3 secure access key in the **Password** field and confirm it.
    3. The username of your account in the **Account name** field.



12. Clear all the checkboxes and click **OK**.
13. Back in the **Logon Account Selection** window, make sure the newly added user account is selected and

click **OK**.



14. Back in the **Configure storage...** window, click **NEXT**.
15. Select a bucket and click **NEXT** twice.
16. On the summary screen, click **Finish**, **OK**, and **Yes**.

Once the Backup Exec services are restarted, the S3 storage will appear in the list on the **Storage** tab. Now you can create backup jobs and specify the S3 storage as destination.

2.5 S3 Bucket and Key Naming Policies

It is recommended to use bucket names that comply with DNS naming conventions:

- can be from 3 to 63 characters long,
- must start and end with a lowercase letter or number,
- can contain lowercase letters, numbers, periods (.), hyphens (-), and underscores (_),
- can be a series of valid name parts (described previously) separated by periods.

An object key can be a string of any UTF-8 encoded characters up to 1024 bytes long.

CHAPTER 3

Accessing iSCSI Targets

This section describes ways to attach iSCSI targets to operating systems and third-party virtualization solutions that support the explicit ALUA mode.

3.1 Accessing iSCSI Targets from VMware ESXi

Before using Acronis Cyber Infrastructure volumes with VMware ESXi, you need to configure it to properly work with ALUA Active/Passive storage arrays. It is recommended to switch to the `VMW_PSP_RR` path selection policy (PSP) to avoid any issues. For example, on VMware ESXi 6.5:

- to set the default PSP for all devices, run

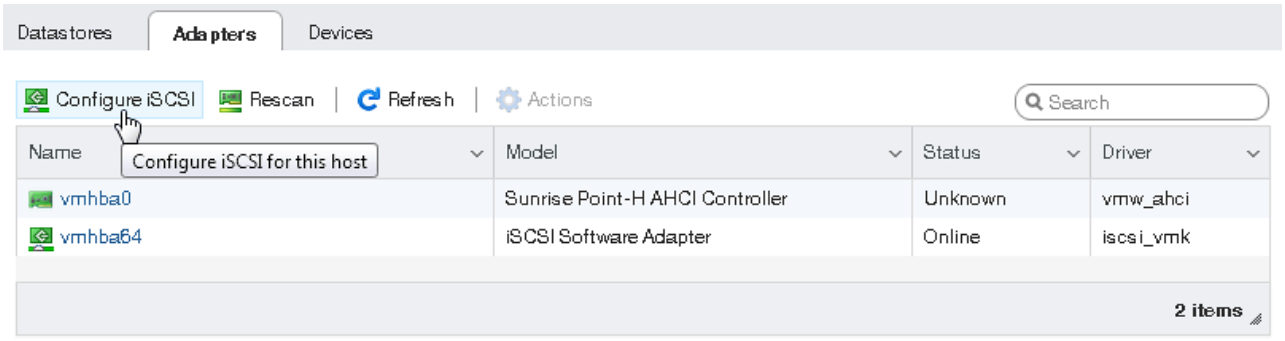
```
# esxcli storage nmp satp rule add --satp VMW_SATP_ALUA --vendor VSTORAGE \
--model VSTOR-DISK --psp VMW_PSP_RR -c tpgs_on
```

- to set the PSP for a specific device, run

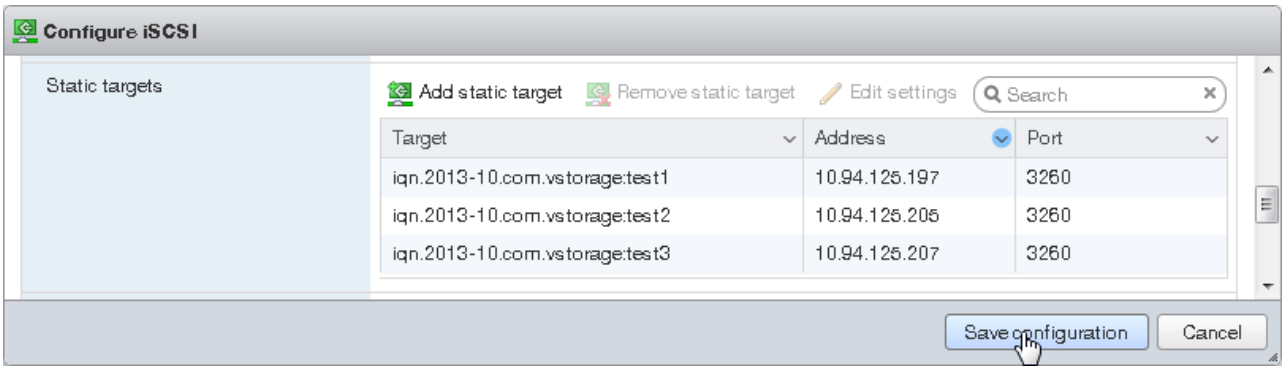
```
# esxcli storage core claimrule load
```

Now you can proceed to create datastores from Acronis Cyber Infrastructure volumes exported via iSCSI. Log in to the VMware ESXi web panel and do the following:

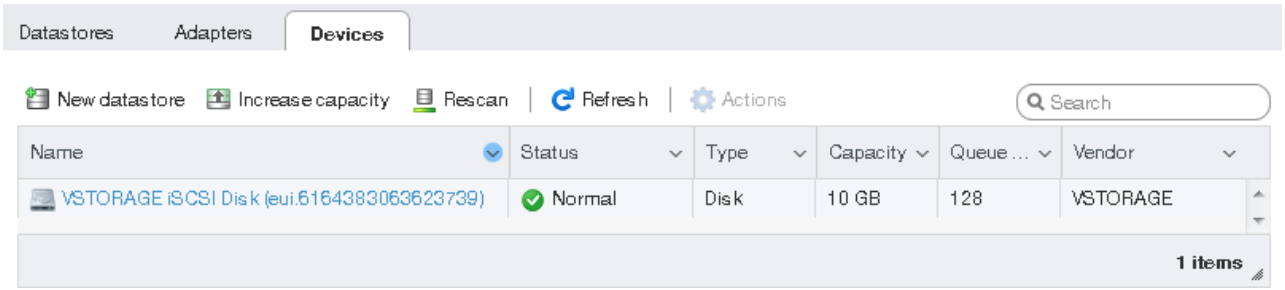
1. In the Navigator, go to the **Storage** > **Adapters** tab and click **Configure iSCSI**.



2. In the **Configure iSCSI** window, click **Add static target** in the **Static targets** section, fill out target IQNs, IP addresses, and ports. Click **Save configuration**.



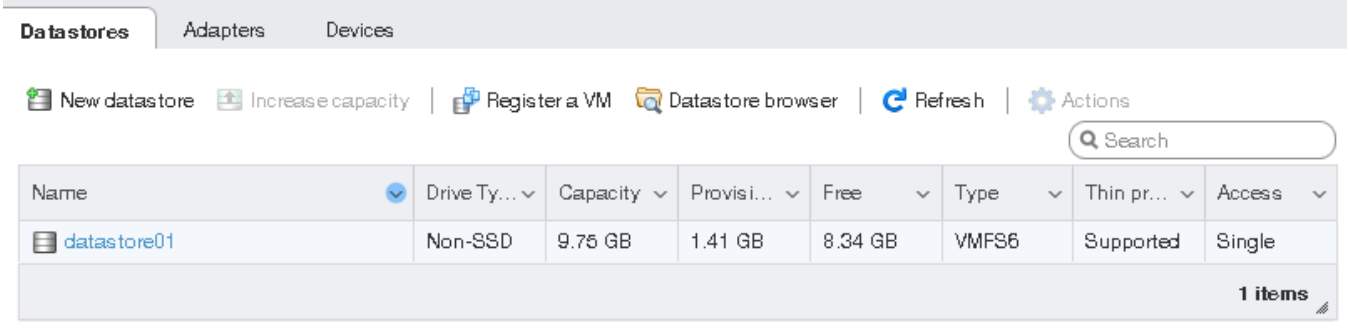
3. Proceed to the **Devices** tab and click **Refresh**. The newly added disk will appear in the list of devices.



4. Select the disk and click **New datastore**. In the wizard that appears, enter a name for the datastore and select partitioning options. Click **Finish** to actually partition the disk.

> **Warning:** Partitioning the disk will erase all data from it.

The ready-to-use disk will appear in the list of datastores. You can now view its contents it with the datastore browser and provision it to VMs.



Note: If your ESXi host loses connectivity to VMFS3 or VMFS5 datastores, follow the instructions in KB article #2113956.

3.2 Accessing iSCSI Targets from Linux

To connect a Linux-based iSCSI initiator to iSCSI targets of Acronis Cyber Infrastructure working in the ALUA mode, do as follows:

1. Make sure the required packages are installed.

   - On RPM-based systems (CentOS and other), run:

     ```
     # yum install iscsi-initiator-utils device-mapper-multipath
     ```

   - On DEB-based systems (Debian and Ubuntu), run:

     ```
     # apt-get install open-iscsi multipath-tools
     ```

2. Create and edit the configuration file `/etc/multipath.conf` as follows:

   ```
   ...
   defaults {
            user_friendly_names no
            path_grouping_policy group_by_prio
            failback immediate
            flush_on_last_del yes
   }
   devices {
        device {
            vendor "VSTORAGE"
            features "3 queue_if_no_path pg_init_retries 50"
            hardware_handler "1 alua"
            path_grouping_policy group_by_name
            path_selector "queue-length 0"
   ```

```
        failback followover
        path_checker tur
        prio alua
    }
}
...
```

3. Load the kernel module and launch the multipathing service.

```
# modprobe dm-multipath
# systemctl start multipathd; systemctl enable multipathd
```

4. If necessary, enable CHAP parameters `node.session.auth.*` and `discovery.sendtargets.auth.*` in `/etc/iscsi/iscsid.conf`.

5. Launch the iSCSI services:

```
# systemctl start iscsi iscsid
# systemctl enable iscsi iscsid
```

6. Discover all targets by their IP addresses. For example:

```
# iscsiadm -m discovery -t st -p 10.94.91.49 10.94.91.49 3260,1 \
iqn.2014-06.com.vstorage:target1
# iscsiadm -m discovery -t st -p 10.94.91.54 10.94.91.54:3260,1 \
iqn.2014-06.com.vstorage:target2
# iscsiadm -m discovery -t st -p 10.94.91.55 10.94.91.55:3260,1 \
iqn.2014-06.com.vstorage:target3
```

7. Log in to the discovered targets. For example:

```
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target1 -l
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target2 -l
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target3 -l
```

8. Find out the multipath device ID. For example:

```
# multipath -ll
360000000000000000000b50326ea44e3 dm-10 VSTORAGE,VSTOR-DISK
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1 alua' wp=rw
|-+- policy='queue-length 0' prio=50 status=active
| `- 6:0:0:1 sdf 8:80  active ready running
|-+- policy='queue-length 0' prio=1 status=enabled
| `- 8:0:0:1 sdj 8:144 active ghost running
`-+- policy='queue-length 0' prio=1 status=enabled
  `- 7:0:0:1 sdh 8:112 active ghost running
# fdisk -l | grep 360000000000000000000b50326ea44e3
Disk /dev/mapper/360000000000000000000b50326ea44e3: 10.7 GB, 10737418240 bytes, \
20971520 sectors
```

You can also find out the multipath device ID by adding `360000000000000000000` to the last six bytes of

the volume ID. In the example above, `360000000000000000000b50326ea44e3` is the multipath device ID mapped from the volume ID `61c9d567-4666-4c16-8030-b50326ea44e3`.

Now you can create partitions on the iSCSI device (`/dev/mapper/360000000000000000000b50326ea44e3` in this example) as well as format and mount it to your initiator node using standard Linux tools.

When you no longer need the external iSCSI device, you can remove it from the initiator node as follows:

1. Make sure the iSCSI device is not in use.
2. Disable multipathing to the device. For example:

```
# multipath -f /dev/mapper/360000000000000000000b50326ea44e3
```

3. Log out of the iSCSI targets. For example:

```
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target1 -p 10.94.91.49:3260 -u
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target2 -p 10.94.91.54:3260 -u
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target3 -p 10.94.91.55:3260 -u
```

4. Delete the iSCSI targets. For example:

```
# iscsiadm -m node -o delete -T iqn.2014-06.com.vstorage:target1 -p 10.94.91.49:3260
# iscsiadm -m node -o delete -T iqn.2014-06.com.vstorage:target2 -p 10.94.91.54:3260
# iscsiadm -m node -o delete -T iqn.2014-06.com.vstorage:target3 -p 10.94.91.55:3260
```

3.3 Accessing iSCSI Targets from Microsoft Hyper-V

Before connecting an iSCSI initiator of Microsoft Hyper-V to iSCSI targets working in the ALUA mode, you need to install and configure Multipath I/O (MPIO). This feature can be used starting from Windows Server 2008 R2. To connect the initiator, for example, on Microsoft Hyper-V Server 2016, do the following:

1. Run Windows PowerShell with administrator privileges and install MPIO.

```
> Enable-WindowsOptionalFeature  Online  FeatureName MultiPathIO
```

   Your server will automatically reboot to finalize the installation.

2. In the Windows PowerShell console, configure MPIO as follows:
   1. Enable support for iSCSI disks:

```
> Enable-MSDSMAutomaticClaim -BusType iSCSI
```

2. Set the failover policy to Fail Over Only. The policy uses a single active path for sending all I/O, and all other paths are standby. If the active path fails, one of the standby paths is used. When the path recovers, it becomes active again.

```
> Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy FOO
```

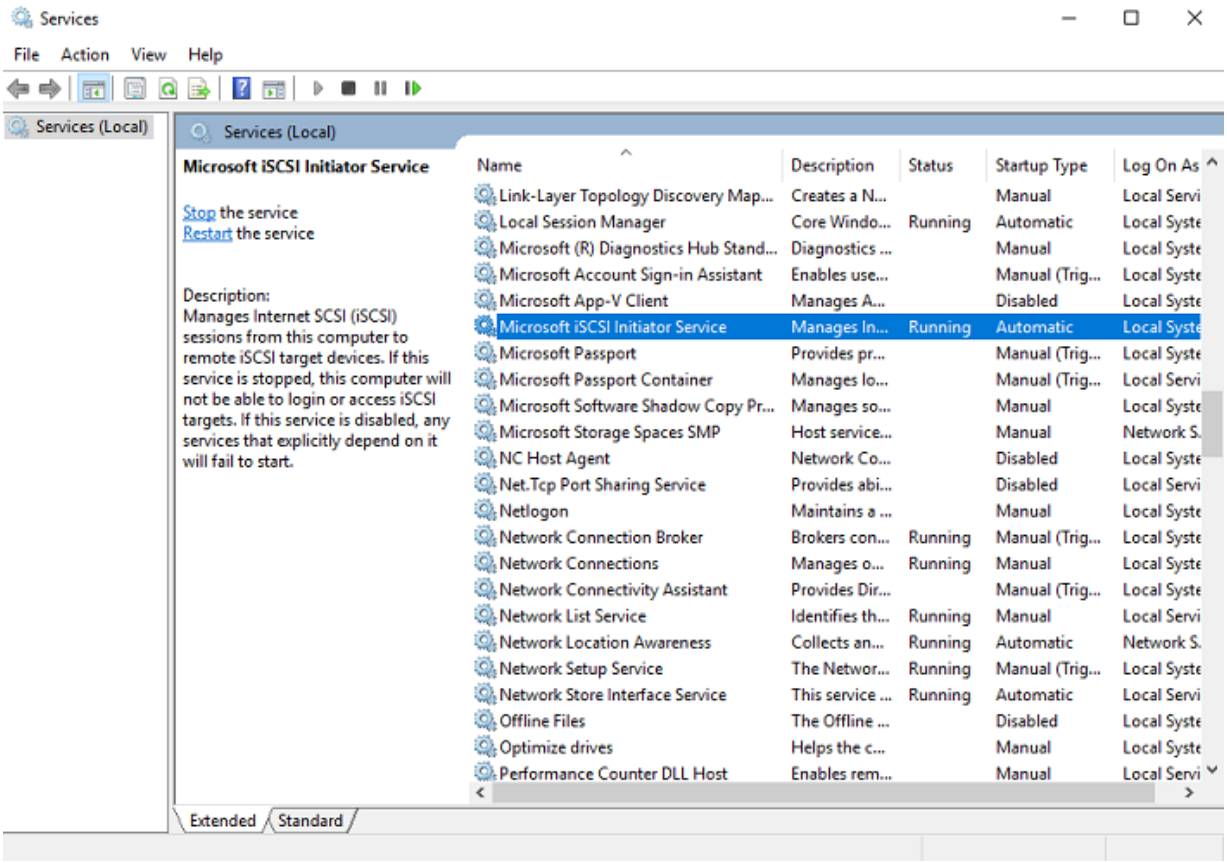
3. Enable path verification. By default, the initiator will verify each path every 30 seconds.

```
> Set-MPIOSetting -NewPathVerificationState Enabled
```

4. Reboot the server.

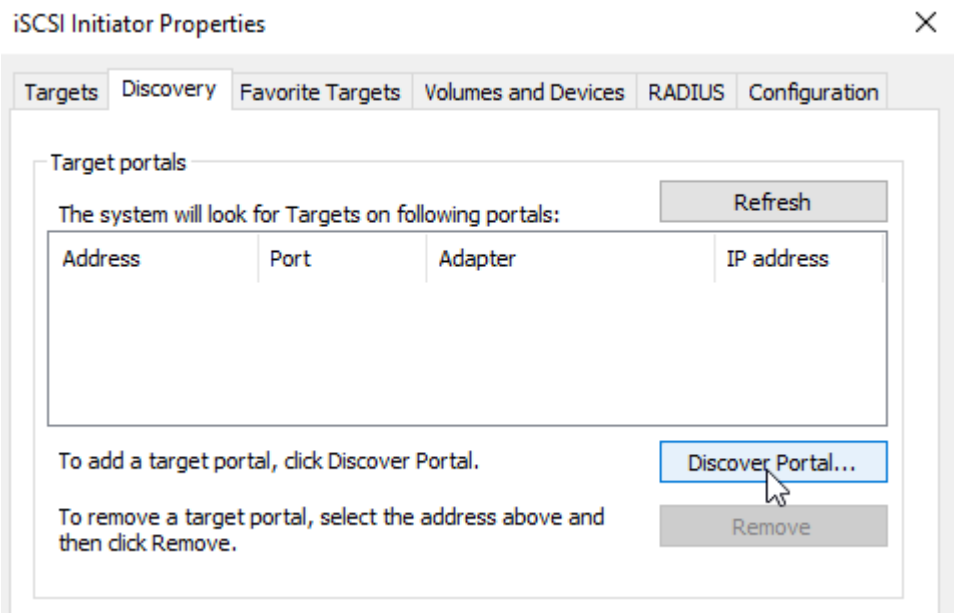
3. Connect your targets to the iSCSI initiator as follows:

1. In the **Control Panel** > **System and Security** > **Administrative Tools** > **Services** window, make sure that **Microsoft iSCSI Initiator Service** is running and its startup type is set to **Automatic**.

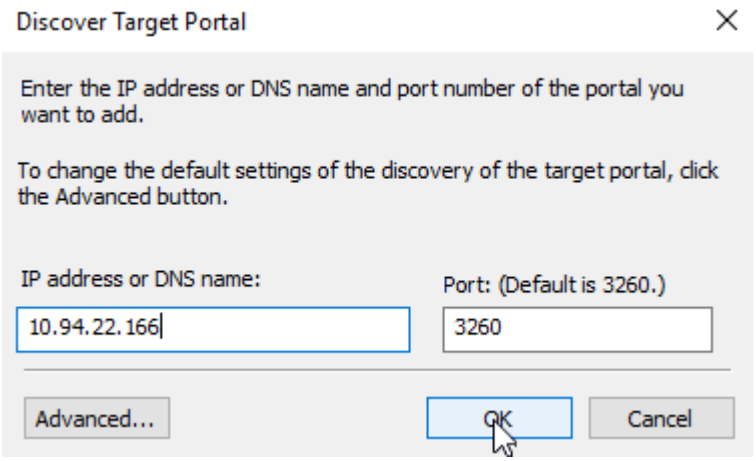


2. Launch **iSCSI Initiator**.

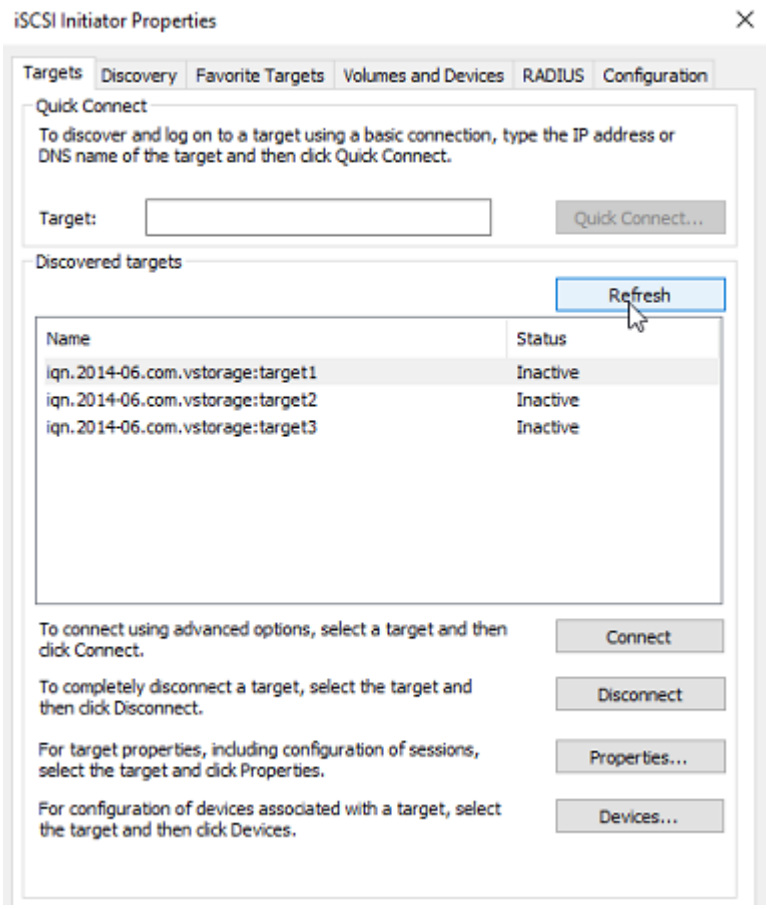
3. In the **iSCSI Initiator Properties** window, open the **Discovery** tab and click **Discover Portal**.



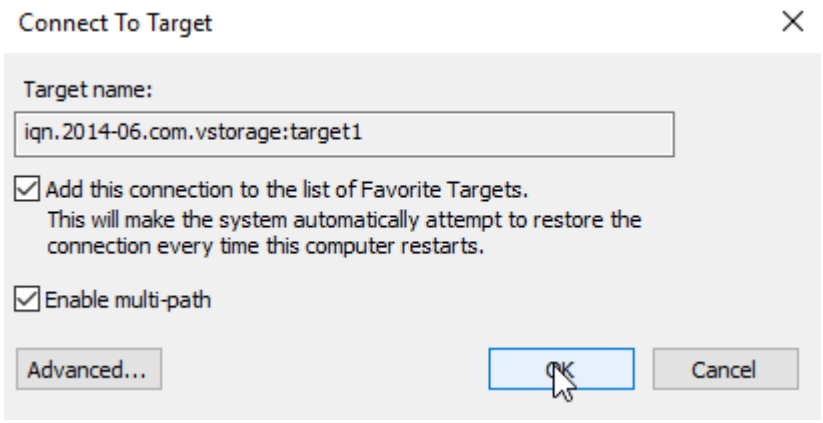
4. In the **Discover Target Portal** window, enter the target IP address and click **OK**. Repeat this step for each target from the target group.



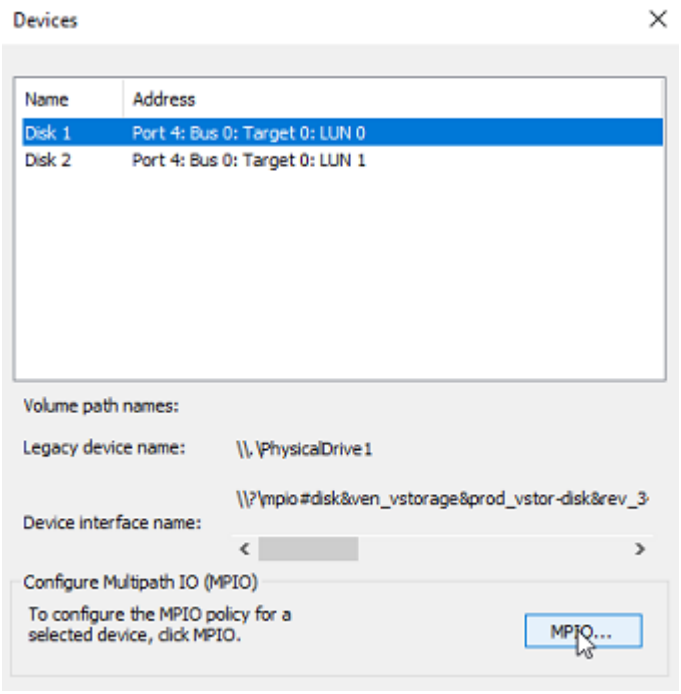
5. On the **Targets** tab, click **Refresh** to discover the added targets.



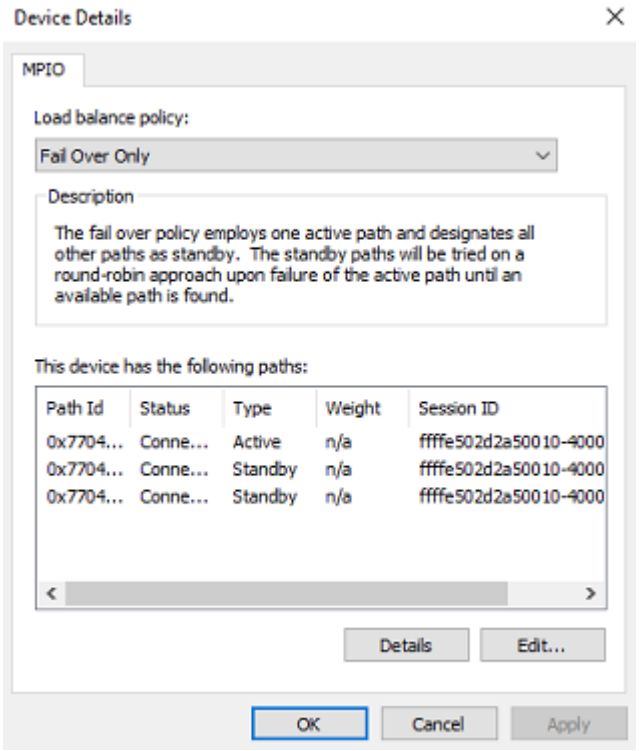
6. Click **Connect** for each target to connect it to the initiator. In the **Connect To Target** window, select the **Enable multi-path** checkbox and click **OK**.



7. On the **Targets** tab, click **Devices..**, select the connected LUN, and click **MPIO..**.

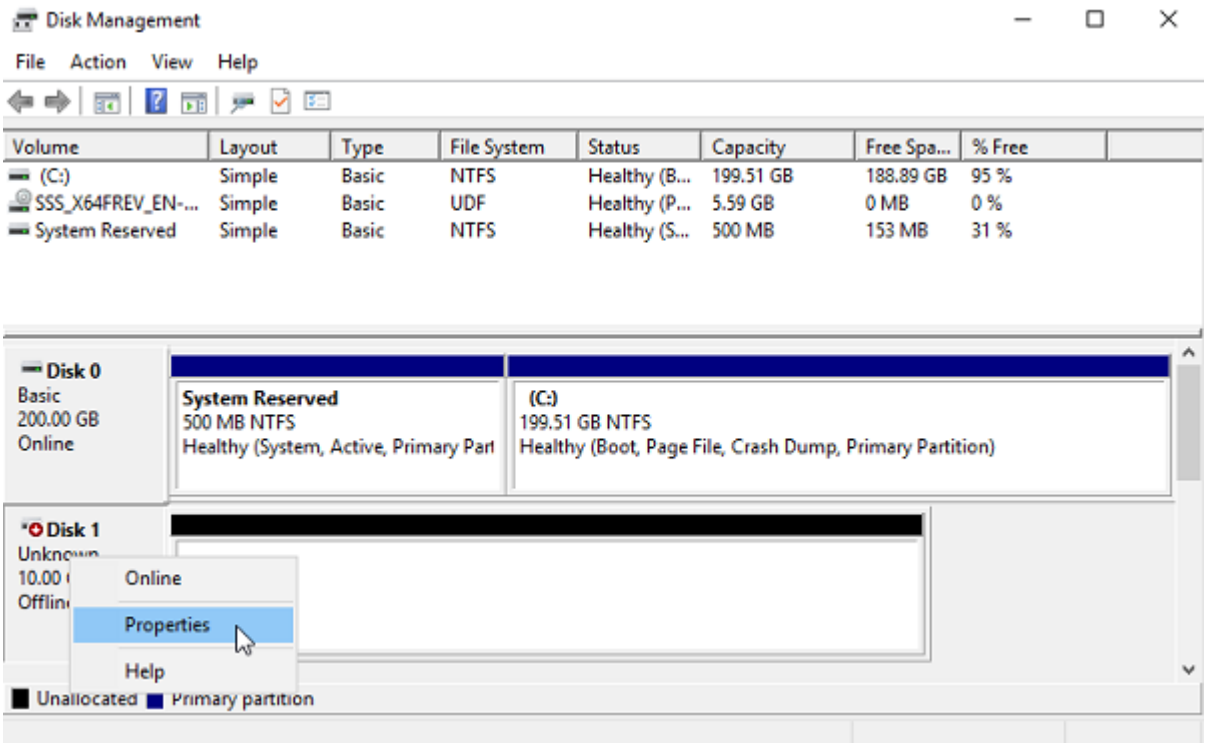


8. Make sure the connected LUN has several paths.

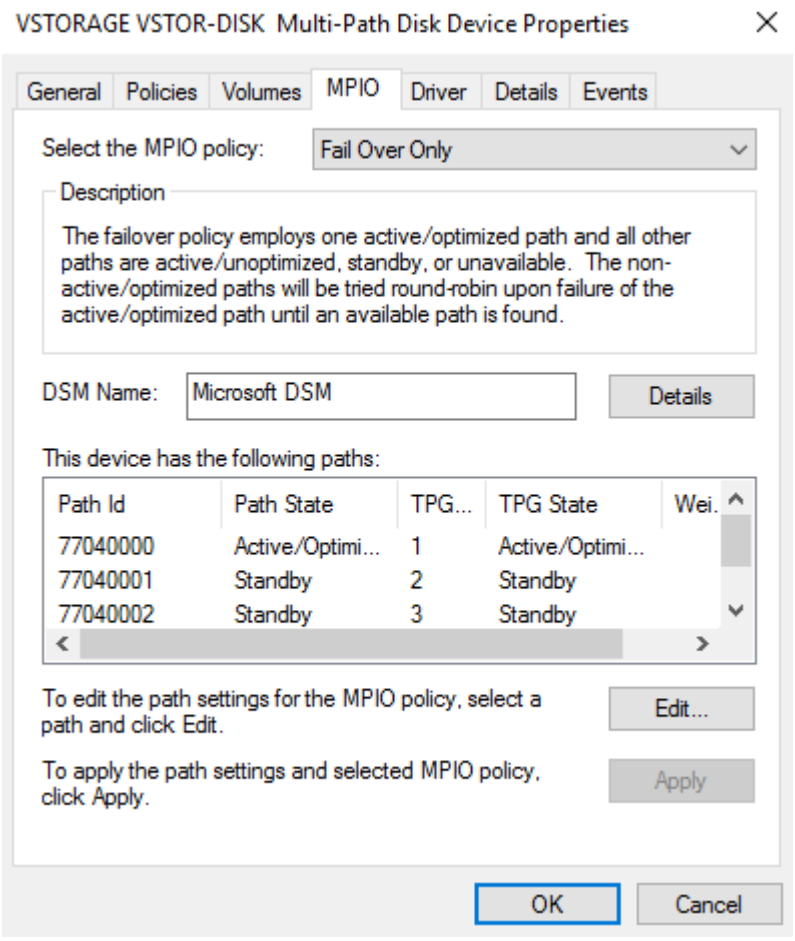


You can now initialize the newly added disk for use in Microsoft Hyper-V. Do the following:

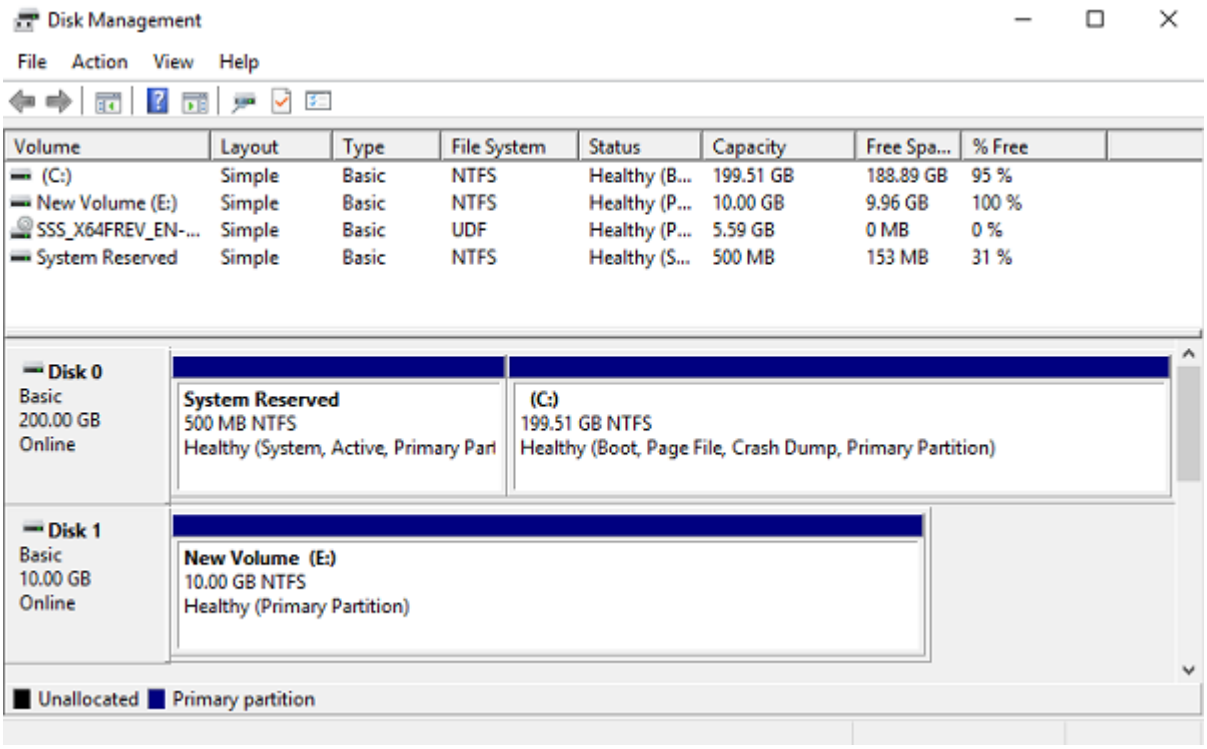
1. Open **Disk Management**, right-click the added disk, and choose **Properties** from the drop-down menu.



2. Check the settings on the **MPIO** tab. The first connected target becomes **Active/Optimized** and the preferred path.



3. Partition and format the disk as usual.


Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (B... 199.51 GB 188.89 GB 95 %
New Volume (E:) Simple Basic NTFS Healthy (P... 10.00 GB 9.96 GB 100 %
SSS_X64FREV_EN-... Simple Basic UDF Healthy (P... 5.59 GB 0 MB 0 %
System Reserved Simple Basic NTFS Healthy (S... 500 MB 153 MB 31 %
Disk 0
Basic
200.00 GB
Online
System Reserved
500 MB NTFS
Healthy (System, Active, Primary Part
(C:)
199.51 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)
Disk 1
Basic
10.00 GB
Online
New Volume (E:)
10.00 GB NTFS
Healthy (Primary Partition)
Unallocated
Primary partition

CHAPTER 4

Accessing NFS Shares

This section describes ways to mount Acronis Cyber Infrastructure NFS shares on Linux and MacOS.

Note: Acronis Cyber Infrastructure currently does not support the Windows built-in NFS client.

4.1 Mounting NFS Exports on Linux

You can mount an NFS export created in Acronis Cyber Infrastructure like any other directory exported via NFS. You will need the share IP address (or hostname) and the volume identifier.

In console, run a command like the following:

```
# mount -t nfs -o vers=4.0 192.168.0.51:/<share_name>/ /mnt/nfs
```

where:

- `-o vers=4.0` is the NFS version to use.

  To use pNFS, change `-o vers=4.0` to `-o vers=4.1`. In all other cases, make sure to always specify NFS version 4.0 or newer.

- `192.168.0.51` is the share IP address. You can also use the share hostname.

- `/<share_name>/` is the root export path. For user exports, specify their full path, for example: `/<share_name>/export1`.

- `/mnt/nfs` is an existing local directory to mount the export to.

4.2 Mounting NFS Exports on MacOS

You can mount an NFS export created in Acronis Cyber Infrastructure like any other directory exported via NFS. You will need the share IP address (or hostname) and the volume identifier.

You can use the command-line prompt or Finder:

- In console, run a command like the following:

  ```
  # mount -t nfs -o vers=4.0 192.168.0.51:/<share_name>/ /mnt/nfs
  ```

  where:

  - `-o vers=4.0` is the NFS version to use.
  - `192.168.0.51` is the share IP address. You can also use the share hostname.
  - `/<share_name>/` is the root export path. For user exports, specify their full path, for example: `/<share_name>/export1`.
  - `/mnt/nfs` is an existing local directory to mount the export to.

- In Finder, do the following:

  1. Set the NFS version to 4.0. To do this, add the `nfs.client.mount.options = vers=4.0` line to the `/etc/nfs.conf` file.
  2. In the **Finder** > **Go** > **Connect to server** window, specify `nfs://192.168.0.51:/<share_name>/`

     where:

     - `192.168.0.51` is the share IP address. You can also use the share hostname.
     - `/<share_name>/` is the root export path. For user exports, specify their full path, for example: `/<share_name>/export1`.
  3. Click **Connect**.

     The Finder will mount the export to `/Volumes/<share_name>/`.