Acronis Cyber Infrastructure 3.5

Backup Gateway Quick Start Guide for VMware vSphere

March 30, 2020

Contents

CHAPTER 1

About This Guide

This guide explains how to deploy Acronis Cyber Infrastructure and configure Backup Gateway on VMware vSphere 6.5 and newer.

Briefly, you will need to do the following:

1. Configure networks.
2. Create virtual machines for Acronis Cyber Infrastructure.
3. Deploy Acronis Cyber Infrastructure in the virtual machines.

All these steps are described in detail in the following chapters.

Having deployed Acronis Cyber Infrastructure, you will need to configure it for your scenario. Steps to set up a backup gateway are provided in *Connecting Acronis Backup Software to Storage Backends via Backup Gateway* (page 17). Other instructions are available in the Acronis Cyber Infrastructure *Administrator's Guide*.

1.1 Requirements

- For the backup gateway scenario, Acronis Cyber Infrastructure can be deployed in a single virtual machine. For general-purpose deployment, however, it is recommended to create three or five virtual machines to enable load balancing and high availability.
- Make sure the vSphere datastore has enough free storage space. Each virtual machine occupies at least 425 GB (two 200 GB storage disks and a 25 GB system disk). The Acronis Cyber Infrastructure template also takes up about 35 GB.
- Make sure the host has enough memory. 4 GB of RAM is the minimum for a one-node setup. Otherwise at least 8 GB of RAM is required for the management node, and at least 4 GB of RAM is taken by each

secondary node.

- Use a separate object container for each Backup Gateway cluster.

Note: The complete hardware requirements for the backup gateway scenario are described in the section “Hardware Requirements for Backup Gateway” of the Acronis Cyber Infrastructure *Installation Guide*.

CHAPTER 2

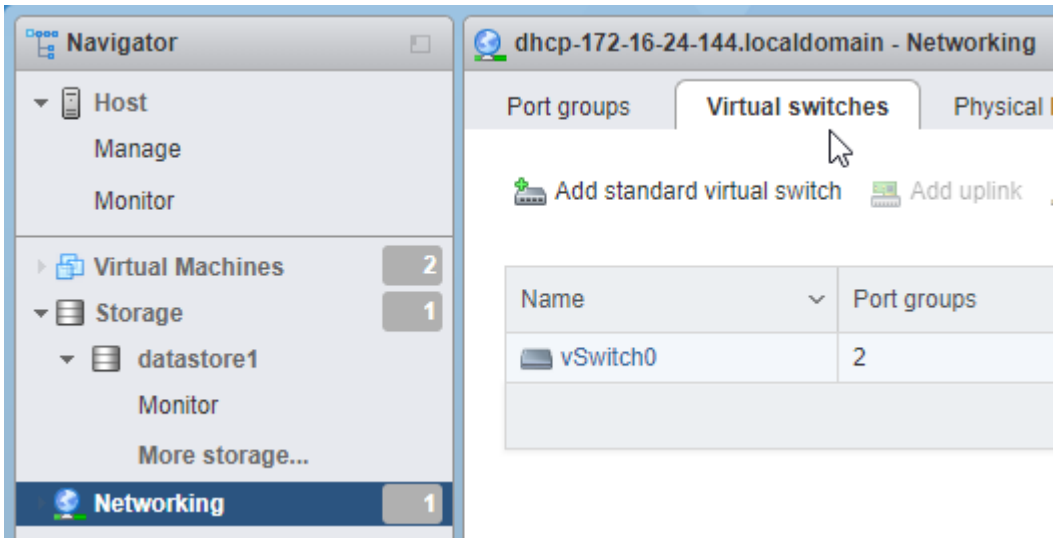
Configuring Networks

Acronis Cyber Infrastructure typically requires two networks: public for outside connectivity and private for data exchange between virtual machines. While a public network may already be set up, it is recommended to create a dedicated private network even if one exists. To create a private network, you will need a virtual switch with custom security parameters and a port group.

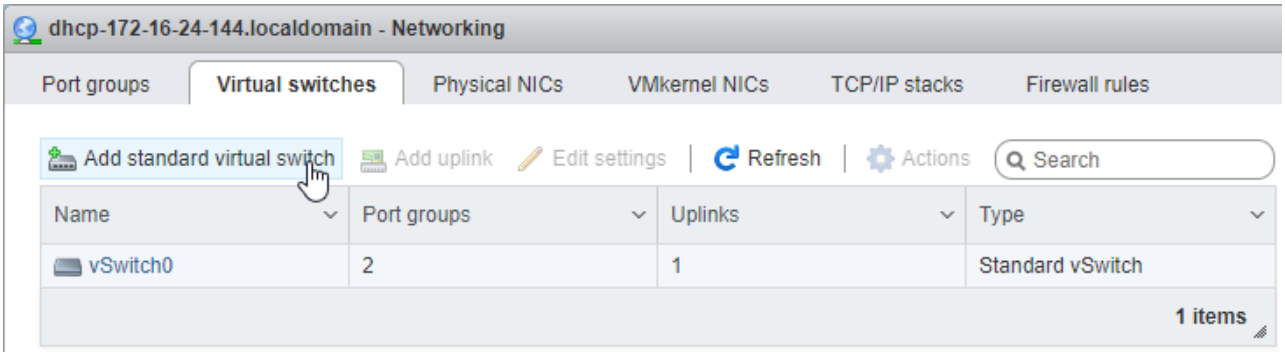
Note: The complete network requirements are provided in the section “Planning Network” of the Acronis Cyber Infrastructure *Installation Guide*.

To create a virtual switch, follow these steps:

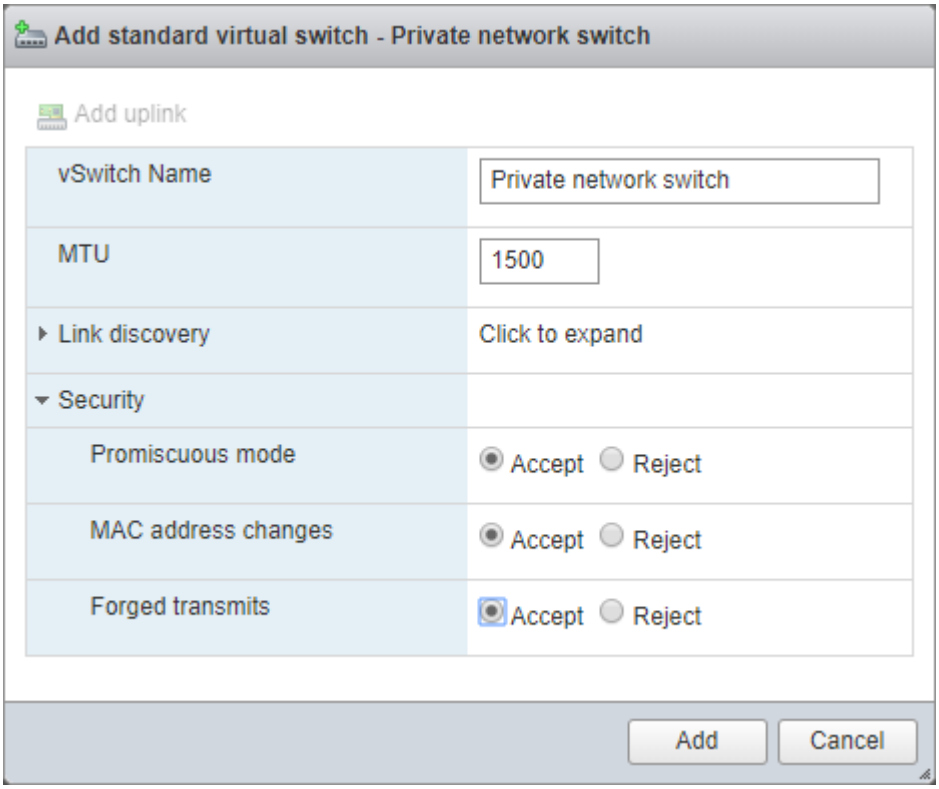
1. In the Host Client, click **Networking** in the left menu. Open the **Virtual switches** tab.



2. Click **Add standard virtual switch** on the toolbar.

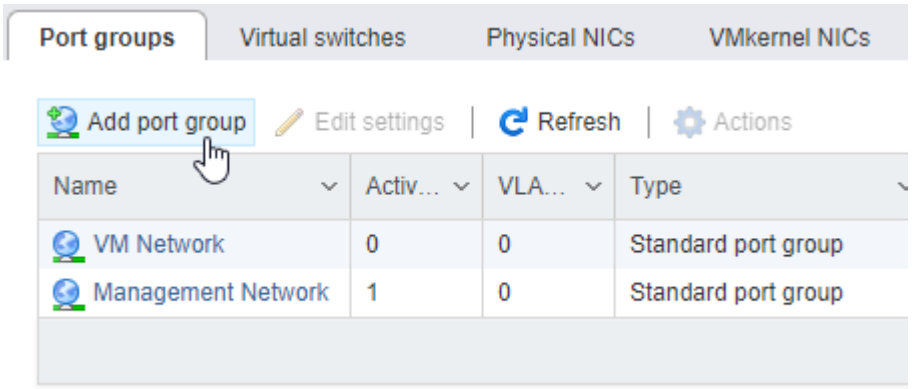


3. Enter the switch name and expand **Security**. Select **Accept** for **Promiscuous mode**, **MAC address changes**, and **Forged transmits**.

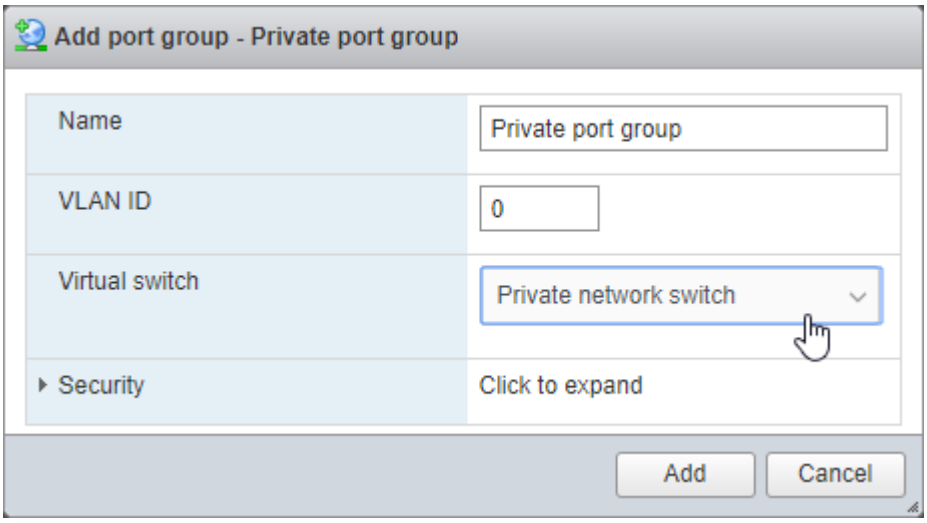


To create a port group, follow these steps:

1. Open the **Port groups** tab and click **Add port group** on the toolbar.



2. Enter the port group name. Select the virtual switch you created earlier.



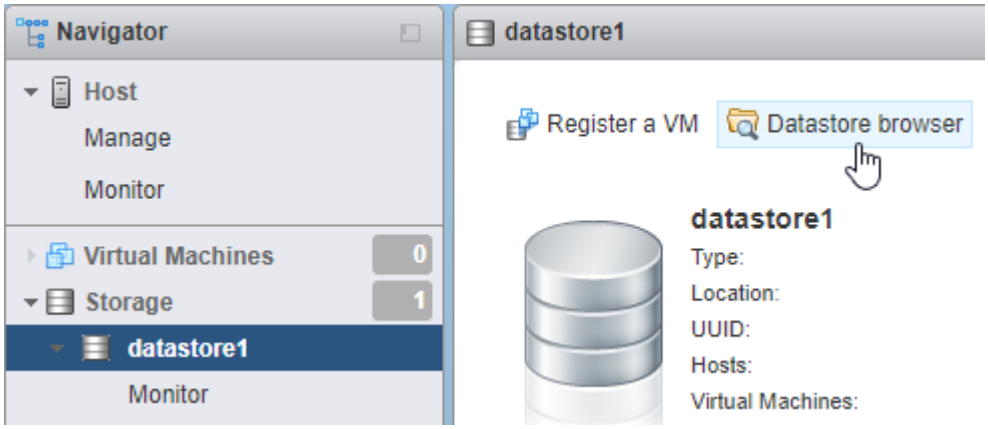
CHAPTER 3

Creating Virtual Machines

First, obtain the Acronis Cyber Infrastructure image (2 VMDK files). To do this, visit the product page and submit a request.

Next, upload the 2 VMDK files to the VMware vSphere datastore:

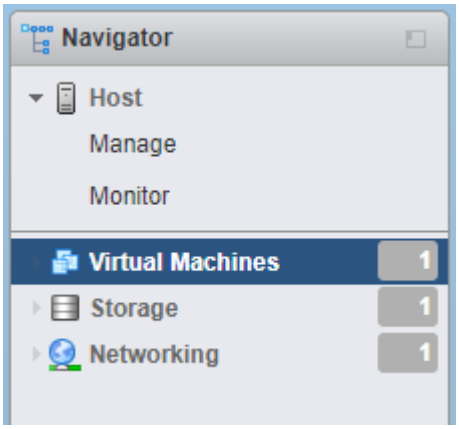
1. In the **Navigator** panel, click the required datastore. Click **Datastore browser** on its toolbar.
2. In the **Datastore browser** window, create a directory named after your virtual machine.



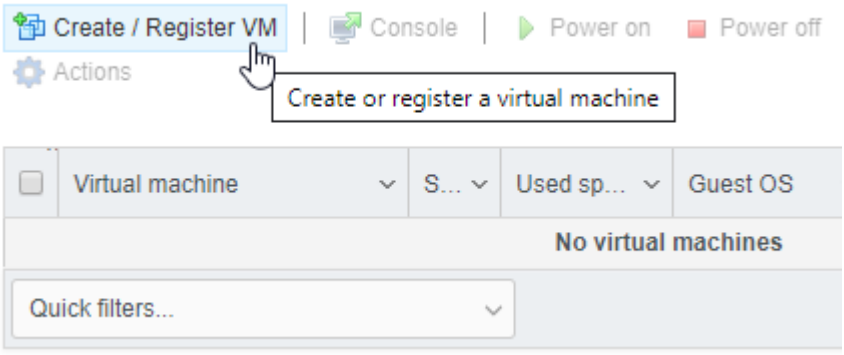
3. Upload the Acronis Cyber Infrastructure image (two VMDK files) to this directory.

Follow these steps to create a virtual machine for Acronis Cyber Infrastructure:

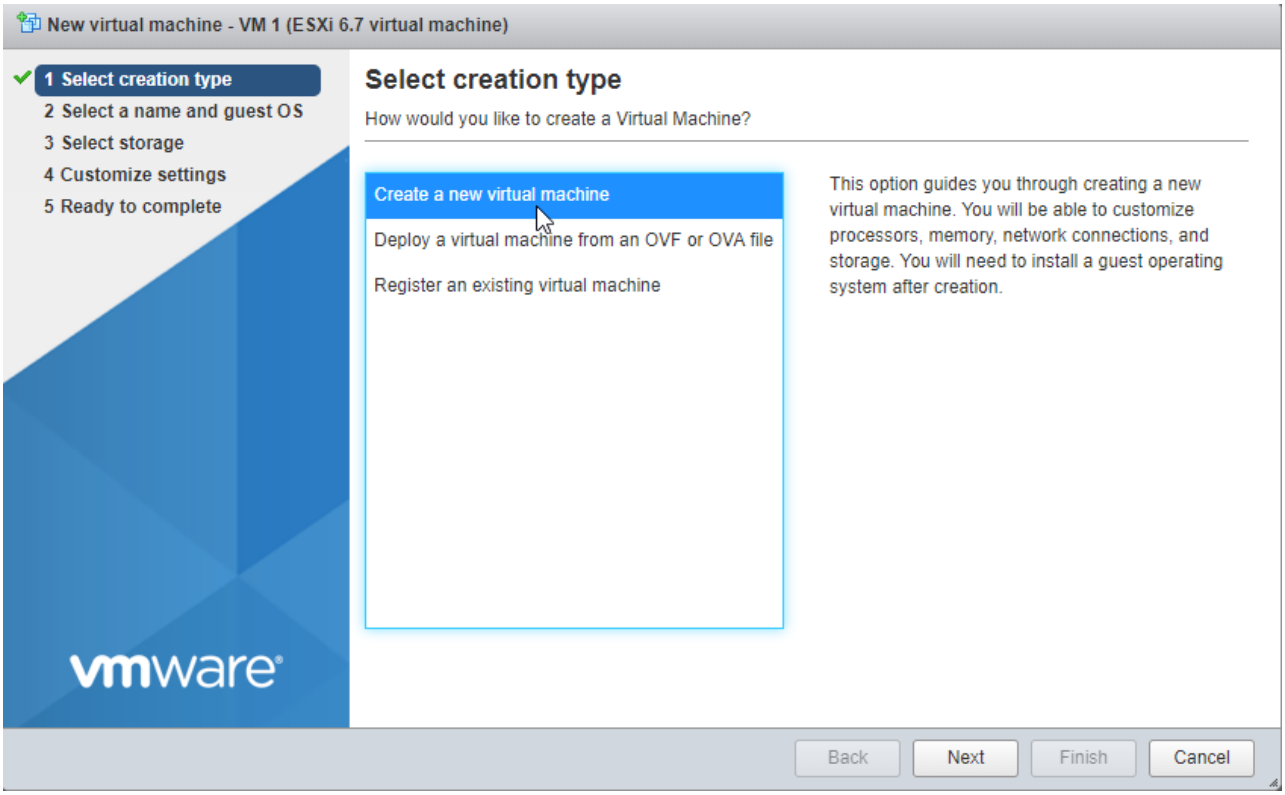
1. In the Host Client, click **Virtual Machines** in the left menu.



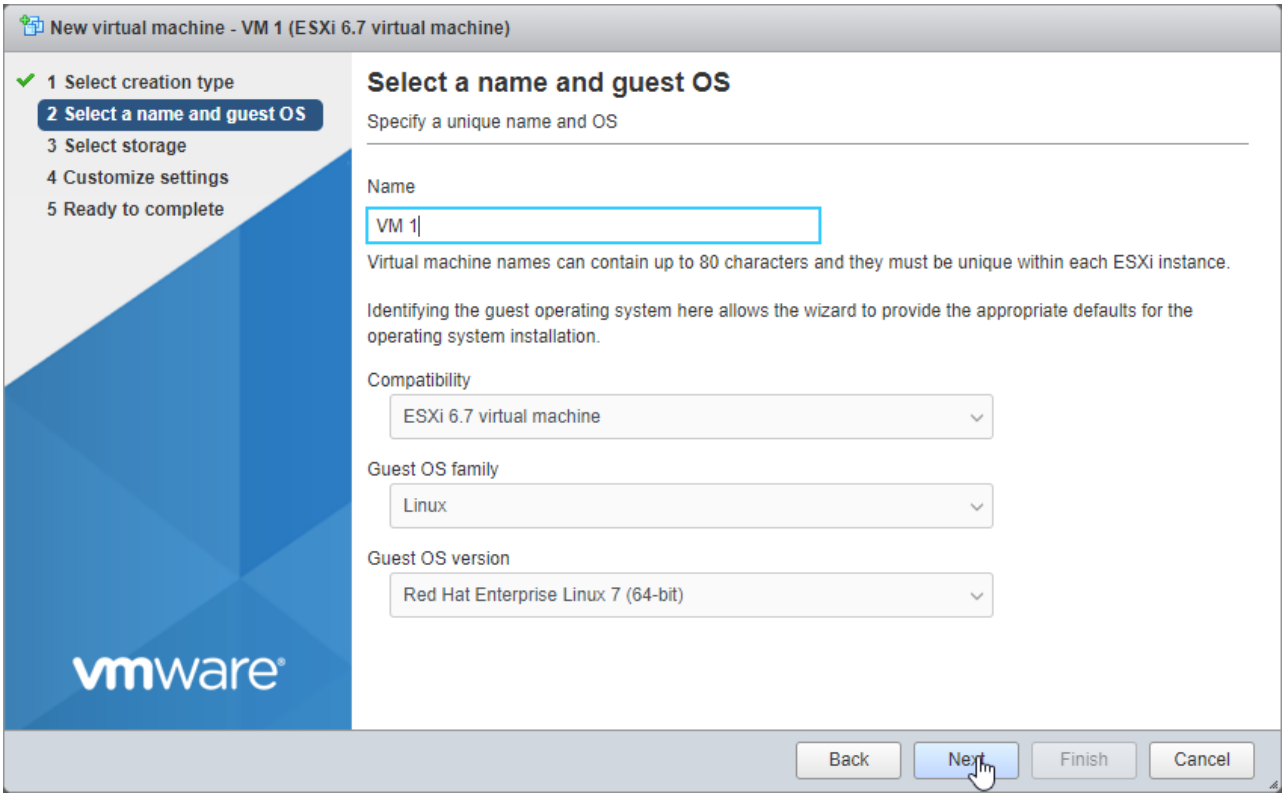
2. Click **Create / Register VM** on the toolbar.



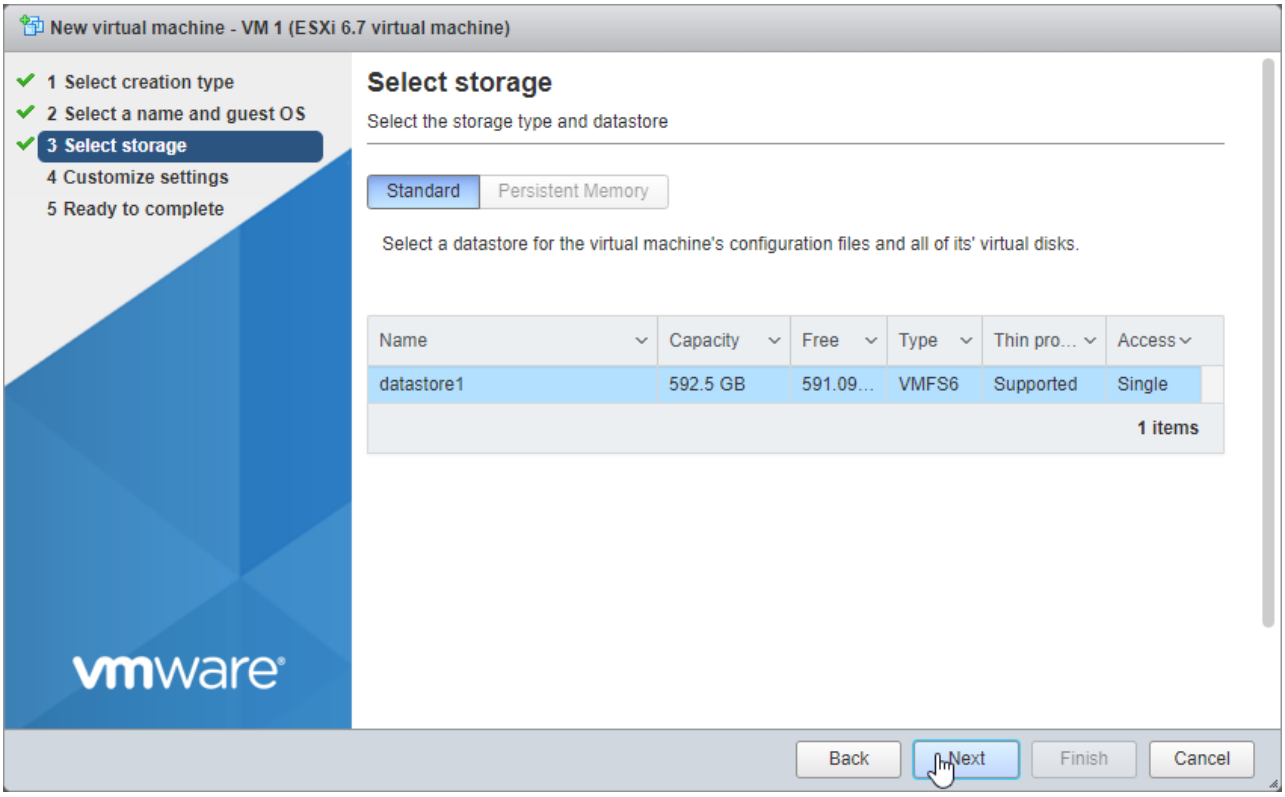
3. In the **New virtual machine** wizard, on step 1 select **Create a new virtual machine**. Click **Next**.



4. On step 2, enter a name for the virtual machine and select the guest OS. Click **Next**.

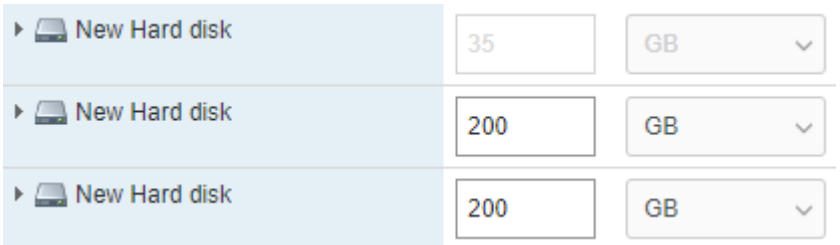


5. On step 3, select the storage type and datastore. Make sure the datastore has enough free space.

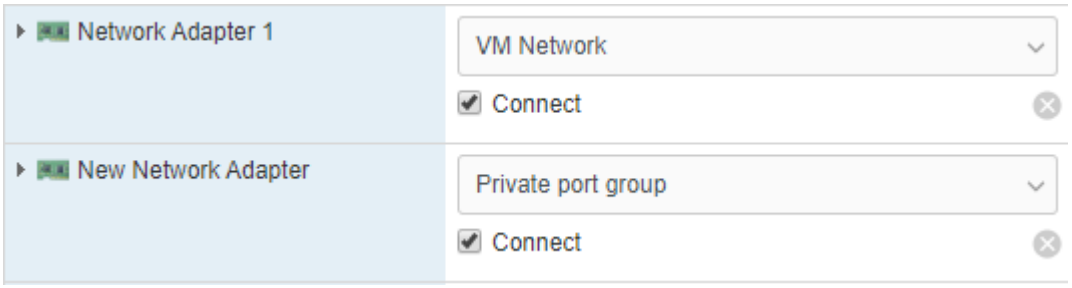


6. On step 4, remove the existing hard disk and click **Add hard disk** on the toolbar. Select **Existing hard disk** and browse to the image you uploaded to the datastore earlier. Click **Select**.

7. Click **Add hard disk** on the toolbar again. Select **New standard hard disk**. Set its size to 200 GB. Repeat this step to add one more hard disk of 200 GB. All in all, you should have three hard disks: 35 GB, 200 GB, and 200 GB.



8. On the **Customize settings** window, click the **Add network adapter** on the toolbar. Make sure one adapter is connected to the public network, while the other is connected to the private port group you have created.



9. On step 5, check the configuration and click **Finish**.
10. Select the virtual machine in the **Navigator** menu and start it.

Repeat these steps to create as many virtual machines as you need based on the desired scenario (see *Requirements* (page 1)).

CHAPTER 4

Deploying Acronis Cyber Infrastructure in Virtual Machines

When the virtual machine is started, login as `storage-user` using the default password (which is `password`). You will be prompted to change the password at once.

Switch to the root user and configure and enable the `eth1` network interface:

```
# cat > /etc/sysconfig/network-scripts/ifcfg-eth1 << EOF
ARPCHECK="no"
BOOTPROTO="static"
IPADDR=192.168.1.<node>
NETMASK=255.255.255.0
DEVICE="eth1"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
NAME="eth1"
ONBOOT="yes"
EOF
# ifup eth1
```

Where `<node>` is the node number: 2 for the management node, 3 for the first secondary node, and so on.

Check that the IP address has been assigned, and the interface is up, e.g., with `ip -4 a show eth1`.

Further configuration varies depending on the node role. You will need to deploy a single management node and may also want to deploy two or four secondary nodes.

4.1 Deploying the Management Node

1. To register the management node and initialize its admin panel, run as the root user:

   ```
   # echo '<passwd>' | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh \
   -i <int_net> -x <ext_net>
   # systemctl start vstorage-ui-backend
   # systemctl start vstorage-ui-agent
   # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_IP>
   ```

   Where `<passwd>` is the desired administrator password; `<int_net>` is the internal (private) network interface; `<ext_net>` is the external (public) network interface; and `<mn_IP>` is the management node IP address.

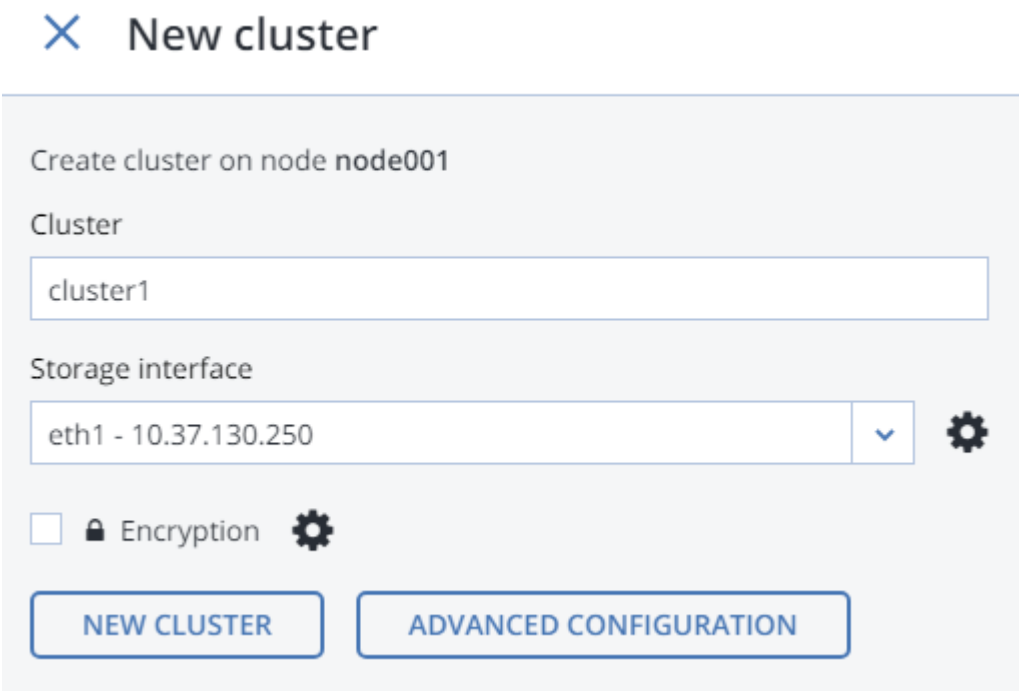
2. Reboot the virtual machine. The admin panel IP address will be shown in terminal's welcome prompt. Now you can log in to the admin panel on port 8888. Use the `admin` user name and the management node's root password that you provided in the previous step.

   In the admin panel, you will see the node you have deployed in the **UNASSIGNED** list on the **INFRASTRUCTURE** > **Nodes** screen.

3. On the **INFRASTRUCTURE** > **Networks** screen, click **Edit**. Make the **Compute API** traffic type available for the public network and click **Save**.

Now you need to create the storage cluster. Do the following:

1. Open the **INFRASTRUCTURE** > **Nodes** screen and click a node in the **UNASSIGNED** list.
2. On the node overview screen, click **Create cluster**.
3. In the **Cluster** field, type a name for the cluster. The name may only contain Latin letters (a-z, A-Z), numbers (0-9), underscores ("_") and hyphens ("-").



4. Click **NEW CLUSTER**.

The storage cluster is ready. You can now proceed to deploying secondary nodes if required by your scenario. If you only need a single node for the backup gateway, proceed to *Connecting Acronis Backup Software to Storage Backends via Backup Gateway* (page 17).

4.2 Deploying Secondary Nodes

To deploy a secondary node in a virtual machine, do the following:

1. Obtain the management node IP address and token from the admin panel. Open **INFRASTRUCTURE** > **Nodes**. Click **ADD NODE** to invoke a screen with the management node IP address and the token.
2. Open the virtual machine terminal and register the secondary node with the admin panel as follows:

   ```
   # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_addr> -t <token>
   ```

   Where `<mn_addr>` is the management node IP address; and `<token>` is the token obtained in the admin panel.

   In the admin panel, the newly registered secondary node will appear on the **INFRASTRUCTURE** > **Nodes** screen in the **UNASSIGNED** list.

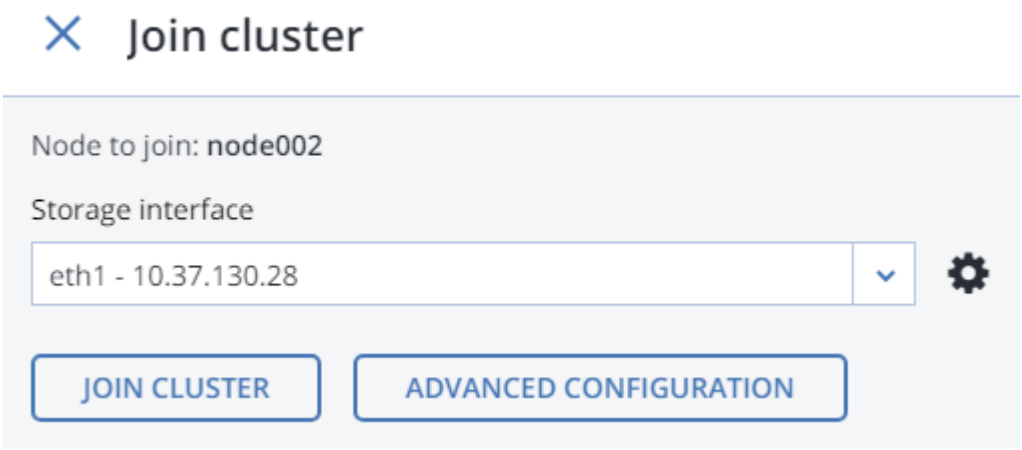
3. Add the secondary node to the storage cluster:

    1. On the **INFRASTRUCTURE** > **Nodes** screen, click an unassigned node.

    2. On the node overview screen, click **Join cluster**.

    3. Make sure the network interface that is connected to a network with the traffic type **Storage** is selected from the **Storage interface** drop-down list.

        If node network interfaces are not configured, click the cogwheel icon and assign a network with the traffic type **Storage** to a node's network interface.



    4. Click **Join cluster** to have Acronis Cyber Infrastructure assign the roles to disks automatically and add the node to the current cluster. Alternatively, click **Advanced configuration** to assign the roles to each drive manually.

Repeat these steps for each secondary node. After all of them are in the storage cluster, you can enable high availability for the management node on the **SETTINGS** > **Management node** > **MANAGEMENT HIGH AVAILABILITY** screen.

Now you can proceed to set up Acronis Cyber Infrastructure for the desired scenario. Instructions on performing various configuration tasks are provided in the Acronis Cyber Infrastructure *Administrator's Guide*.

CHAPTER 5

Adding Space to Acronis Cyber Infrastructure

Before you create new disks, consider the following recommendations for their sizing:

1. If you have a cluster of several nodes, the nodes should be the same size for redundancy reasons. Then, the data will be spread more evenly among them. For more information, refer to "Understanding Allocatable Disk Space" in the *Administrator's Command Line Guide*.
2. Having the same-size disks helps distribute the loads more evenly. Inside a cluster, the disk usage is proportional to the disk size. For example, if you have a disk of 10 TB and a disk of 2 TB, a 50% cluster load will use 5 TB and 1 TB respectively.

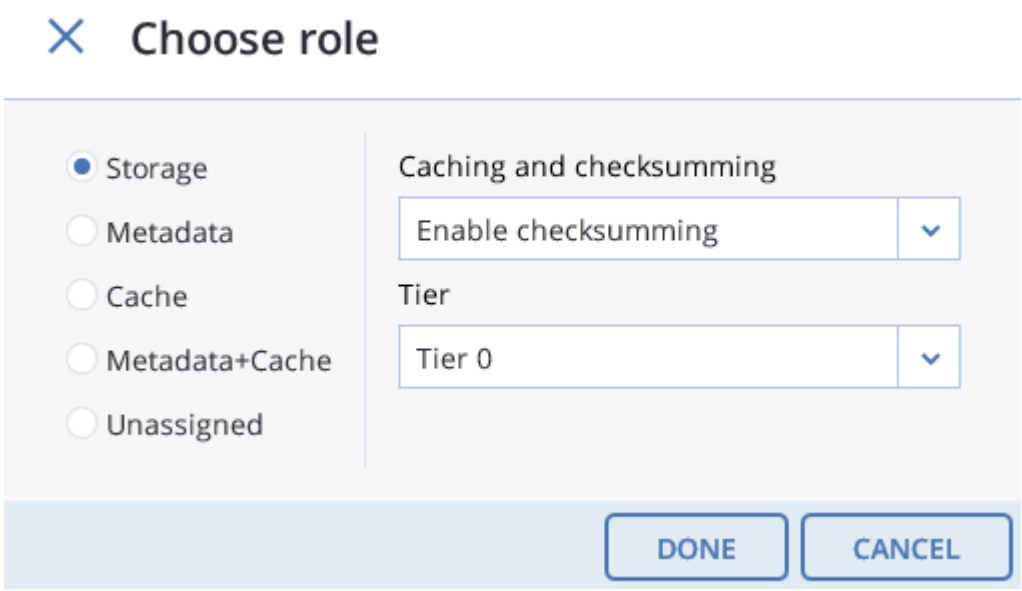
If you want to increase physical space in your storage cluster, you can add new virtual disks to your nodes. Do not use the **extend disk** option of the VMware vSphere on your Acronis Cyber Infrastructure virtual machine, as the file system will not be resized correspondingly. So please create a new virtual disk and add it to your virtual machine as described below.

Add a new virtual disk to your virtual machine as outlined in Add a New Hard Disk to a Virtual Machine. After that, it will be listed in the node's disks in the admin panel of Acronis Cyber Infrastructure.

In the admin panel, follow these steps to configure the new disk:

1. On the **INFRASTRUCTURE** > **Nodes** screen, click the node with the created disk. Click the **DISKS>** section to see all the node disks.
2. The disk with the **Unassigned** role is the one that you created earlier. Select it and click **Assign** on the right.
3. On the **Choose role** screen, select the **Storage** role, a tier, and enable checksumming if required. For

more info, see “Assigning Disk Roles Manually” in the *Administrator’s Guide*.



CHAPTER 6

Connecting Acronis Backup Software to Storage Backends via Backup Gateway

The Backup Gateway storage access point (also called “gateway”) is intended for service providers who use Acronis Backup Cloud and/or Acronis Backup Advanced and want to organize an on-premises storage for their clients’ backed-up data.

Backup Gateway enables a service provider to easily configure storage for the proprietary deduplication-friendly data format used by Acronis.

Backup Gateway supports the following storage backends:

- storage clusters with software redundancy by means of erasure coding
- NFS shares
- public clouds, including a number of S3 solutions as well as Microsoft Azure, OpenStack Swift, and Google Cloud Platform

While your choice should depend on scenario and requirements, it is recommended to keep Acronis backup data in the local storage cluster. In this case, you can have the best performance due to WAN optimizations and data locality. Keeping backups in an NFS share or a public cloud implies the unavoidable data transfer and other overhead, which reduces overall performance.

Take note of the following:

- When configuring Backup Gateway, you will need to provide the credentials of your administrator account in the Acronis backup software.

- In cases when not local but external storage (e.g., NFS) is used with Backup Gateway, redundancy has to be provided by the said external storage. Backup Gateway does not provide data redundancy or perform data deduplication itself.

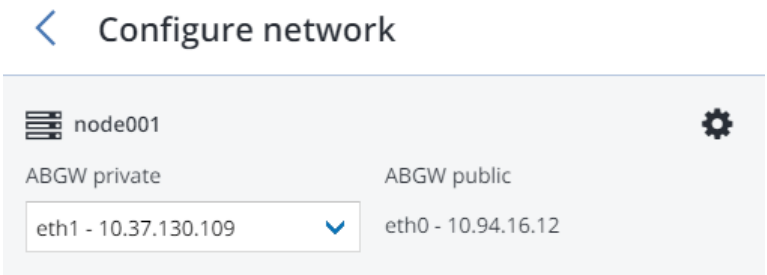
6.1 Connecting to the Local Storage Cluster via Backup Gateway

Before you proceed, make sure that the destination storage has enough space for both existing and new backups.

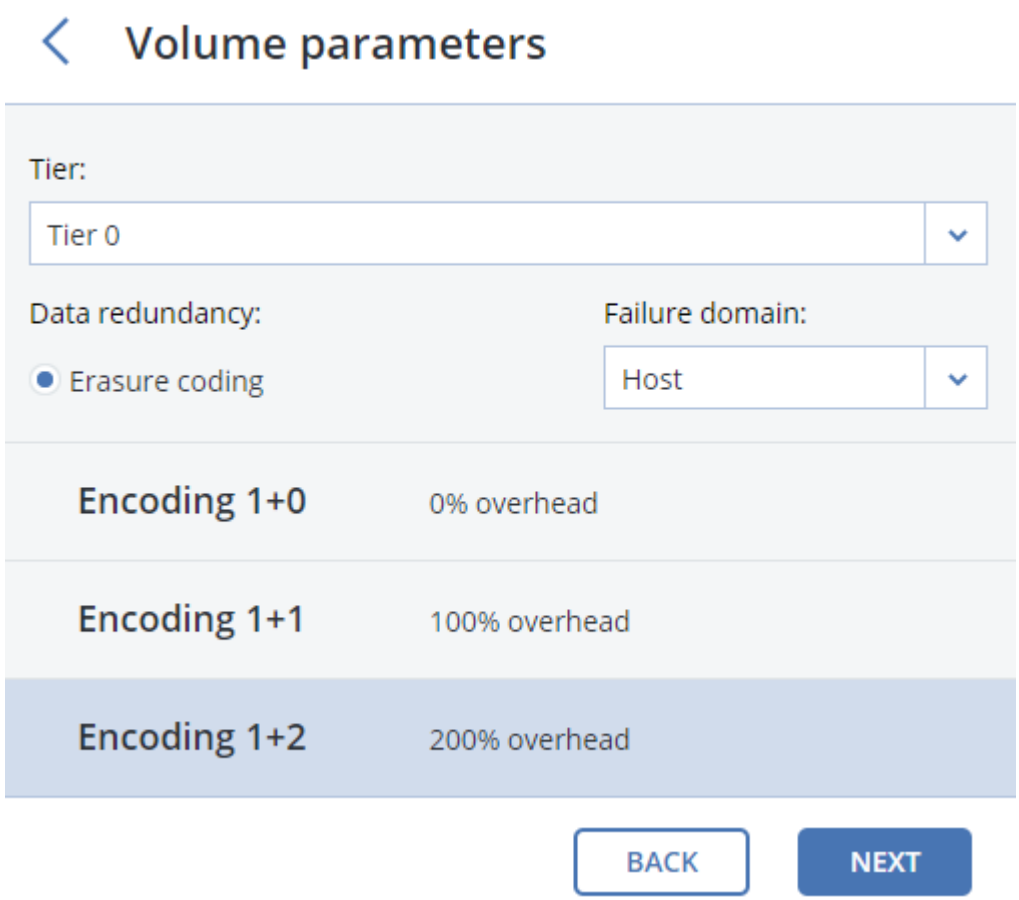
To set up Backup Gateway, do the following:

1. On the **INFRASTRUCTURE** > **Networks** screen, make sure that the **ABGW private** and **ABGW public** traffic types are added to your networks.
2. In the left menu, click **STORAGE SERVICES** > **Backup storage**.
3. Select the node(s) to run the gateway services on and click **Create gateway** in the right menu.
4. Select **This Acronis cluster** as storage type.
5. Make sure the correct network interface is selected in the drop-down list. Click **NEXT**.

   If necessary, click the cogwheel icon and configure node's network interfaces on the **Network Configuration** screen.



6. On the **Volume Parameters** tab, select the desired tier, failure domain, and data redundancy mode. For more information, refer to the sections "Understanding Storage Tiers", "Understanding Failure Domains", and "Understanding Data Redundancy" in the *Installation Guide*.



Redundancy by replication is not supported for Backup Gateway. For erasure coding, changing redundancy scheme is disabled, because it may decrease cluster performance. The reason is that re-encoding demands a significant amount of cluster resources for a long period of time. If you still want to change the redundancy scheme, please contact the technical support.

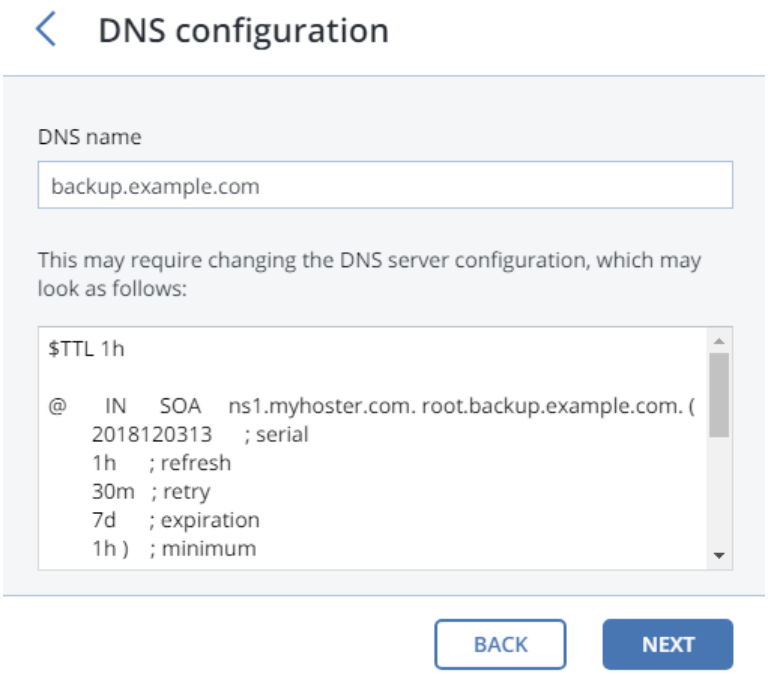
Click **NEXT**.

7. On the **DNS Configuration** tab, specify the external DNS name for this gateway, e.g, `backupgateway.example.com`. Make sure that each node running the gateway service has a port open for outgoing Internet connections and incoming connections from your Acronis backup software. Backup agents will use this address and port to upload the backup data.

Important: Configure your DNS server according to the example suggested in the admin panel.

Important: Each time you change nodes in the Backup Gateway cluster, adjust the DNS settings

accordingly.



Click **Next**.

8. On the **Register in backup software** pane, specify the following information for your Acronis product:
   - In **Address**, specify the address of the Acronis Backup Cloud management portal (e.g., https://cloud.acronis.com/) or the hostname/IP address and port of the Acronis Backup Advanced management server (e.g., http://192.168.1.2:9877).
   - In **Account**, specify the credentials of a partner account in the cloud or of an organization administrator on the local management server.
9. Finally, click **DONE**.

6.2 Connecting to External NFS Shares via Backup Gateway

Take note of these limitations:

- Acronis Cyber Infrastructure does not provide data redundancy on top of NFS volumes. Depending on

the implementation, NFS shares may use their own hardware or software redundancy.

- In the current version of Acronis Cyber Infrastructure, only one cluster node may store backups on an NFS volume.

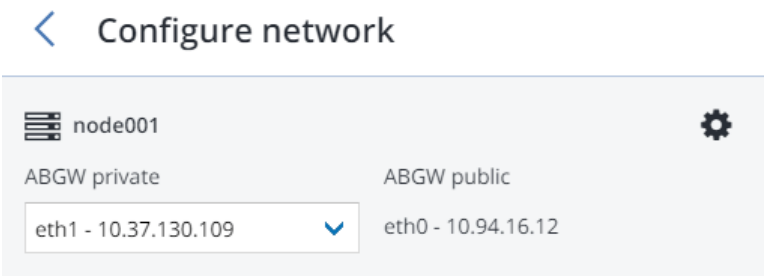
Before you proceed, make sure that:

1. The NFS share has enough space for backups.
2. Each NFS export is used by only one gateway. In particular, do not configure two Acronis Cyber Infrastructure installations to use the same NFS export for backup storage.

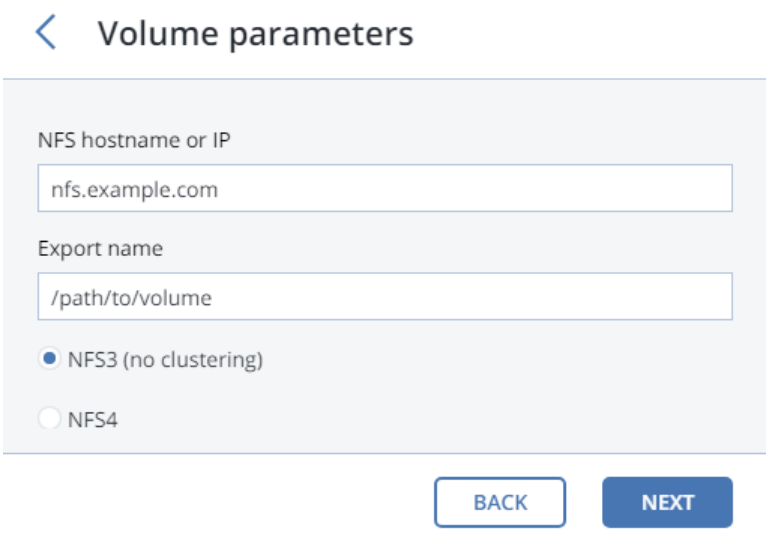
To set up Backup Gateway, do the following:

1. On the **INFRASTRUCTURE** > **Networks** screen, make sure that the **ABGW private** and **ABGW public** traffic types are added to your networks.
2. In the left menu, click **STORAGE SERVICES** > **Backup storage**.
3. Select the node(s) to run the gateway services on and click **Create gateway** in the right menu.
4. Select **Network File System** as storage type.
5. Make sure the correct network interface is selected in the drop-down list. Click **NEXT**.

   If necessary, click the cogwheel icon and configure node's network interfaces on the **Network Configuration** screen.



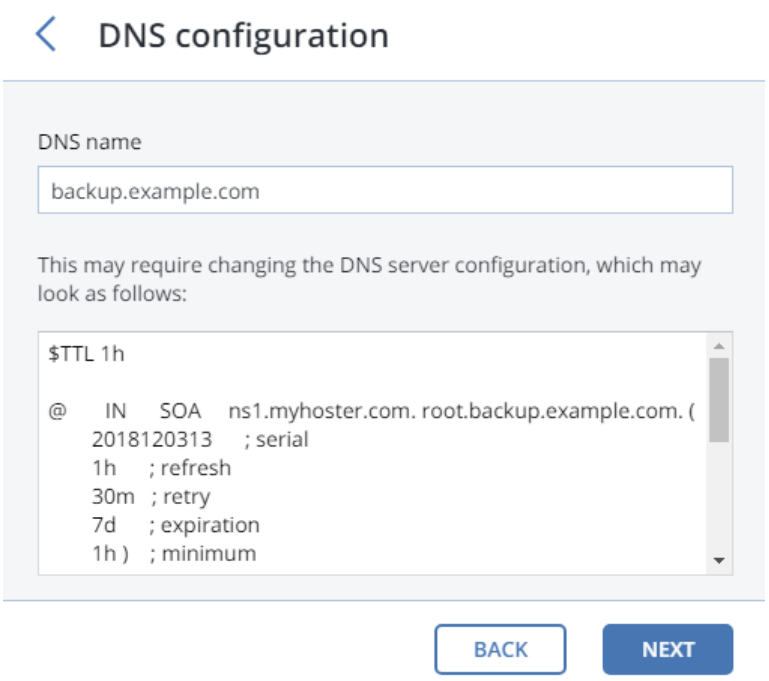
6. On the **Volume Parameters** tab, specify the hostname or IP address of the NFS share as well as the export name. Click **NEXT**.



7. On the **DNS Configuration** tab, specify the external DNS name for this gateway, e.g, `backupgateway.example.com`. Make sure that each node running the gateway service has a port open for outgoing Internet connections and incoming connections from your Acronis backup software. Backup agents will use this address and port to upload the backup data.

Important: Configure your DNS server according to the example suggested in the admin panel.

Important: Each time you change nodes in the Backup Gateway cluster, adjust the DNS settings accordingly.



Click **Next**.

8. On the **Register in backup software** pane, specify the following information for your Acronis product:
   - In **Address**, specify the address of the Acronis Backup Cloud management portal (e.g., https://cloud.acronis.com/) or the hostname/IP address and port of the Acronis Backup Advanced management server (e.g., http://192.168.1.2:9877).
   - In **Account**, specify the credentials of a partner account in the cloud or of an organization administrator on the local management server.
9. Finally, click **DONE**.

6.3 Connecting to Public Cloud Storage via Backup Gateway

With Backup Gateway, you can have Acronis Backup Cloud or Acronis Backup Advanced store backups in a number of public clouds and on-premises object storage solutions:

- Amazon S3
- IBM Cloud

- Alibaba Cloud
- IIJ
- Cleversafe
- Cloudian
- Microsoft Azure
- Swift object storage
- Softlayer (Swift)
- Google Cloud Platform
- Wasabi
- Other solutions using S3 with the older AuthV2-compatible authentication methods

However, compared to the local storage cluster, storing backup data in a public cloud increases the latency of all I/O requests to backups and reduces performance. For this reason, it is recommended to use the local storage cluster as storage backend.

Since backups are cold data with specific access rights, it is cost-efficient to use storage classes that are intended for long-term storage of infrequently accessed data. The recommended storage classes include the following:

- Infrequent Access for Amazon S3
- Cool Blob Storage for Microsoft Azure
- Nearline and Coldline Storage for Google Cloud Platform

Note that real data storage costs may be 10-20% higher due to additional fees for operations like data retrieval and early deletion.

6.3.1 Important Requirements and Restrictions

1. When working with public clouds, Backup Gateway uses the local storage as the staging area as well as to keep service information. It means that the data to be uploaded to a public cloud is first stored locally and only then sent to the destination. For this reason, it is vital that the local storage is persistent and redundant so the data does not get lost. There are multiple ways to ensure the persistence and redundancy of local storage. You can deploy Backup Gateway on multiple cluster nodes and select a

good redundancy mode. If Acronis Cyber Infrastructure with the gateway is deployed on a single physical node, you can make the local storage redundant by replicating it among local disks. If Acronis Cyber Infrastructure with the gateway is deployed in a virtual machine, make sure it is made redundant by the virtualization solution it runs on.

2. Make sure the local storage cluster has plenty of logical space for staging. For example, if you perform backup daily, provide enough space for at least 1.5 days' worth of backups. If the daily backup total is 2TB, provide at least 3TB of logical space. The required raw storage will vary depending on the encoding mode: 9TB (3TB per node) in the 1+2 mode, 5TB (1TB per node) in the 3+2 mode, etc.
3. If you are to store backups in an Amazon S3 cloud, keep in mind that Backup Gateway may sometimes block access to such backups due to the eventual consistency of Amazon S3. It means that Amazon S3 may occasionally return stale data as it needs time to render the most recent version of the data accessible. Backup Gateway detects such delays and protects backup integrity by blocking access until the cloud updates.
4. Use a separate object container for each Backup Gateway cluster.

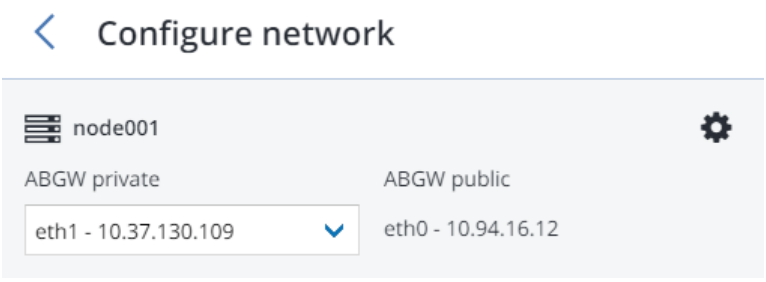
6.3.2 Setting Up Backup Gateway

Before you proceed, make sure that the destination storage has enough space for backups.

To set up Backup Gateway, do the following:

1. On the **INFRASTRUCTURE** > **Networks** screen, make sure that the **ABGW private** and **ABGW public** traffic types are added to your networks.
2. In the left menu, click **STORAGE SERVICES** > **Backup storage**.
3. Select the node(s) to run the gateway services on and click **Create gateway** in the right menu.
4. Select **Public Cloud** as storage type.
5. Make sure the correct network interface is selected in the drop-down list. Click **NEXT**.

   If necessary, click the cogwheel icon and configure node's network interfaces on the **Network Configuration** screen.



6. On the **Public cloud parameters** pane, do the following:

    1. Select a public cloud provider. If your provider is S3-compatible but not in the list, try **AuthV2 compatible**.
    2. Depending on the provider, specify **Region**, **Authentication (keystone) URL**, or **Endpoint URL**.
    3. In case of Swift object storage, specify the authentication protocol version and attributes required by it.
    4. Specify user credentials. In case of Google Cloud, select a JSON file with keys to upload.
    5. Specify the folder (bucket, container) to store backups in. The folder must be writeable.

        Use a separate object container for each Backup Gateway cluster.

    Click **NEXT**.

7. On the **Register in backup software** pane, specify the following information for your Acronis product:

    - In **Address**, specify the address of the Acronis Backup Cloud management portal (e.g., https://cloud.acronis.com/) or the hostname/IP address and port of the Acronis Backup Advanced management server (e.g., http://192.168.1.2:9877).
    - In **Account**, specify the credentials of a partner account in the cloud or of an organization administrator on the local management server.

8. Finally, click **DONE**.