Table of contents

About this guide .................................................................................................................. 3
Requirements .................................................................................................................... 4
Configuring networks ......................................................................................................... 5
Creating virtual machines ................................................................................................. 8
Deploying Acronis Cyber Infrastructure in virtual machines ............................................ 12
  Deploying the management node .................................................................................... 13
  Deploying secondary nodes ........................................................................................... 14
Adding space to Acronis Cyber Infrastructure .................................................................... 16
Adding locations to Acronis Cyber Protect or Acronis Cyber Protect Cloud ..................... 18
  Connecting to the local storage cluster via Backup Gateway ....................................... 19
  Connecting to external NFS shares via Backup Gateway ............................................. 21
  Connecting to public cloud storage via Backup Gateway ........................................... 24
About this guide

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

Briefly, you will need to do the following:

2. Create virtual machines for Acronis Cyber Infrastructure.
3. Deploy Acronis Cyber Infrastructure in the virtual machines.
4. Set up Backup Gateway.

To configure Acronis Cyber Infrastructure for your scenario, refer to the Administrator Guide.
Requirements

To be able to run the Acronis Cyber Infrastructure on VMware vSphere, make sure the following requirements are met:

- VMware vSphere version: 6.7 and newer
- VM version: 14 and newer
- The host should have enough memory. At least 8 GB of RAM is required for a node with one storage disk running Backup Gateway.
- The vSphere datastore should have 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. The maximum recommended size for one virtual disk is 16 TB.

**Important**

Plan the size of virtual disks beforehand and reserve enough space for the expected data growth. The disks cannot be resized later, though you might add new ones.

- For the backup gateway scenario, Acronis Cyber Infrastructure can be deployed in a single virtual machine. For the general-purpose deployment, however, it is recommended to create three or five virtual machines to enable load balancing and high availability.

**Note**

The complete hardware requirements for the backup gateway scenario are described in "System requirements" in the Administrator Guide.
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 "Network requirements and recommendations" in the Administrator Guide.

*To create a virtual switch*

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

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Private port group</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>0</td>
</tr>
<tr>
<td>Virtual switch</td>
<td>Private network switch</td>
</tr>
</tbody>
</table>

[Add] [Cancel]
Creating virtual machines

First, you need to upload the Acronis Cyber Infrastructure image to the VMware vSphere datastore, and then proceed to creating virtual machines.

To upload the Acronis Cyber Infrastructure image
1. Obtain the Acronis Cyber Infrastructure image here and unpack 2 VMDK files.
2. In the Navigator panel, click the required datastore. Click Datastore browser on its toolbar.
3. In the Datastore browser window, create a directory named after your virtual machine.
4. Upload the Acronis Cyber Infrastructure image (two VMDK files) to this directory.

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 (refer to "Requirements" (p. 4)).
Deploying Acronis Cyber Infrastructure in virtual machines

When the virtual machine is started, do the following:

1. Log in as **storage-user** by using the default password (which is **password**). You will be prompted to change the password at once. For example:

```
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user storage-user.
Changing password for storage-user.
(currect) UNIX password:
New password:
Retype new password:
pwd: all authentication tokens updated successfully.
```

In (current) UNIX password type **password**; in New password and Retype new password type a new password. The password will be changed both for **storage-user** and the root user.

2. Log in as **storage-user** again by using the new password, and then switch to the root user:

```
$ sudo su
```

3. 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.

4. Verify that the IP address has been assigned, and the interface is up, for example, by using `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.
Deploying the management node

To deploy the management node in a virtual machine, you need to configure the management node, and then create the storage cluster on it.

To configure the management node

1. Register the management node and initialize its admin panel:
   a. On the node, run the following command as the root user to configure the admin panel component:
      ```
      echo <password> | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh -i <private_iface> -x <public_iface>
      ```
      where
      - `<password>` is the desired administrator password
      - `<private_iface>` is the name of the private network interface
      - `<public_iface>` is the name of the public network interface
   b. Start the admin panel service on the node:
      ```
      # systemctl start vstorage-ui-backend
      ```
   c. Register the node in the admin panel:
      ```
      # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -x <public_iface>
      ```
      where
      - `<MN_IP_address>` is the IP address of the node's private network interface
      - `<public_iface>` is the name of the public network interface

2. Reboot the virtual machine. The admin panel IP address will be shown in the 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 on the Infrastructure > Nodes screen. Its status will be Unassigned.

3. On the Infrastructure > Networks screen, click the pencil icon next to the Compute API traffic type available for the public network, and then click Save.

4. Add the Compute API traffic type to your public network:
   a. On the Infrastructure > Networks screen, click the pencil icon next to the Compute API traffic type.
   b. Add this traffic type to your public network by selecting its radio button.
   c. Click the check mark to apply the changes.

To create the storage cluster
1. Open the **Infrastructure > Nodes** screen, and then click **Create storage cluster**.
2. [Optional] To configure the disk roles or node location, click the cogwheel icon.
3. Enter a name for the cluster. It may only contain Latin letters (a-z, A-Z), numbers (0-9), and hyphens (“-”).
4. Enable encryption, if required.
5. Click **Create**.

You can monitor cluster creation on the **Infrastructure > Nodes** screen. The creation might take some time, depending on the number of disks to be configured. Once the configuration is complete, the cluster is created.

You can now proceed to deploying secondary nodes if required by your scenario. If you need a only single node for Backup Gateway, proceed to "Adding locations to Acronis Cyber Protect or Acronis Cyber Protect Cloud" (p. 18).

## Deploying secondary nodes

To deploy a secondary node in a virtual machine, you need to configure it, and then add it to the storage cluster.

### To configure a secondary node

1. Obtain the token and management node address in the admin panel:
   a. Log in to the admin panel on port 8888. The panel's IP address is shown in the console after deploying the primary node. Use the default user name shown on the login screen and the primary node's root password.
      If prompted, add the security certificate to the browser's exceptions.
   b. In the admin panel, open **Infrastructure > Nodes**, and then click **Connect node** to invoke a screen with the management node address and the token.
2. Open the virtual machine terminal and register the secondary node with the admin panel by running:

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

   where
   - `<MN_IP_address>` is the IP address of the private network interface on the node with the admin panel
   - `<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. Its status will be **Unassigned**.

### To add the secondary node to the storage cluster

1. On the **Infrastructure > Nodes** screen, click an unassigned node.
2. On the node right pane, click **Join to cluster**.

© Acronis International GmbH, 2003-2022
3. Click **Join** to assign the roles to disks automatically and add the node to the default location. Alternatively, click the cogwheel icon to configure the disk roles or node location.

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 Administrator Guide.
Adding space to Acronis Cyber Infrastructure

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

- 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 "How logical space is calculated" in the Administrator Guide.
- 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. Therefore, you will need to 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.

**To configure the new disk in the admin panel**

1. On the Infrastructure > Nodes screen, click the name of the node with the created disk. Go to the Disks tab to see all the node disks.
2. Click the disk without a role that you created earlier.
3. On the disk right pane, click Assign role.
4. In the Assign role window, select the Storage role, a storage tier, and enable checksumming, if
required. For more info, refer to "Configuring new disks manually" in the Administrator Guide.

### Assign role

Select the role to assign to the disk "sdc"

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage</strong></td>
<td>Use the disk to store data.</td>
</tr>
<tr>
<td><strong>Cache</strong></td>
<td>Use the disk to store write cache. This disk does not add capacity to the cluster but improves its performance.</td>
</tr>
<tr>
<td><strong>Metadata</strong></td>
<td>Use the disk to store cluster metadata.</td>
</tr>
<tr>
<td><strong>Metadata + Cache</strong></td>
<td>Use the disk to store both cluster metadata and write cache.</td>
</tr>
</tbody>
</table>

**Storage tier**

- Tier 0

**Caching and checksumming**

- Enable checksumming

**Buttons**

- Cancel
- Assign
Adding locations to Acronis Cyber Protect or Acronis Cyber Protect Cloud

Backup storage uses Backup Gateway as a storage access point. It is intended for service providers who use Acronis Cyber Protect and/or Acronis Cyber Protect Cloud and want to store their clients’ backed-up data in the local cluster, in the cloud (like Google Cloud, Microsoft Azure, and AWS S3), or on NAS (via the NFS protocol).

Backup storage enables a service provider to easily configure storage for the proprietary deduplication-friendly data format used by Acronis. In addition, the backup storage data can be georeplicated.

Backup storage supports the following backup destinations:

- Acronis Cyber Infrastructure storage clusters with erasure coding providing for data redundancy
- 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 the scenario and requirements, it is recommended to keep Acronis backup data in the Acronis Cyber Infrastructure 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. Besides, with external backup destinations, redundancy has to be provided by the external storage. Backup storage does not provide data redundancy or perform data deduplication itself.

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

Limitations

- Two-factor authentication (2FA) is not supported for Backup Gateway registration in Acronis Cyber Protect Cloud. To register Backup Gateway, mark a user as a service account, as described in the Acronis Cyber Cloud documentation, and specify the user credentials during the registration.

Prerequisites

- If you have enabled login control for the Acronis Cyber Protect Cloud web interface, ensure that the public IP address of your backup storage cluster is specified among the allowed IP addresses, as instructed in the Acronis Cyber Cloud documentation.
Connecting to the local storage cluster via Backup Gateway

Limitations

- Redundancy by replication is not supported for backup storage.

Prerequisites

- The storage cluster has at least one disk with the Storage role.
- The destination storage has enough space for both existing and new backups.
- Ensure that each node to join the backup storage cluster has the TCP port 44445 open for outgoing Internet connections, as well as for incoming connections from Acronis backup software.

To select the local cluster as the backup destination

1. On the Infrastructure > Networks screen, make sure that the Backup (ABGW) private and Backup (ABGW) public traffic types are added to the networks you intend to use.
2. Open the Storage services > Backup storage screen, and then click Create backup storage.
3. On the Backup destination step, select Acronis Cyber Infrastructure cluster.
4. On the Nodes step, select nodes to add to the backup storage cluster, and then click Next.
5. On the Storage policy step, select the desired tier, failure domain, and data redundancy mode. For more information, refer to "Storage policies" in the Administrator Guide. Then, click Next.
6. On the DNS step, specify an external DNS name for backup storage, for example, backupstorage.example.com. Backup agents will use this DNS name and the TCP port 44445 to upload backup data. Then, click Next.
Important
- Configure your DNS server according to the example suggested in the admin panel.
- Each time you change the network configuration of nodes in the backup storage cluster, adjust the DNS records accordingly.

```plaintext
Domain name (not IP address)
backupstorage.example.com

This may require changing the DNS server configuration, which may look as follows:

$TTL 1h

@   IN   SOA   ns1.myhoster.com. root.backupstorage.example.com. (  
  2021011213 ; serial  
  1h ; refresh  
  30m ; retry  
  7d ; expiration

Note
For complex environments, HAProxy might be used to build a scalable and redundant load balancing platform, which can be easily moved or migrated and is independent from Acronis Cyber Infrastructure. For more information, refer to https://kb.acronis.com/content/64787.

7. On the Acronis account step, specify the following information for your Acronis product:
   - The URL of the cloud management portal (for example, https://cloud.acronis.com/) or the hostname/IP address and port of the local management server (for example, http://192.168.1.2:9877)
   - The credentials of a partner account in the cloud or of an organization administrator on the local management server
8. On the **Summary** step, review the configuration, and then click **Create**.

## Connecting to external NFS shares via Backup Gateway

### 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.
- Only one cluster node may store backups on an NFS share.
- Each NFS export is used by only one gateway. In particular, do not connect two Acronis Cyber Infrastructure installations to the same NFS export for backup storage.
- Multiple full backups stored on an NFS share may consume additional storage space due to the delay of automatic compaction, which is performed for one backup at a time.

### Prerequisites

- The storage cluster has at least one disk with the **Storage** role.
- The destination storage has enough space for both existing and new backups.
- Ensure that each node to join the backup storage cluster has the TCP port 44445 open for outgoing Internet connections, as well as for incoming connections from Acronis backup software.
- Ensure that the node to join the backup storage has access to external NFS storage.
To select an external NFS share as the backup destination

1. On the Infrastructure > Networks screen, make sure that the Backup (ABGW) private and Backup (ABGW) public traffic types are added to the networks you intend to use.
2. Open the Storage services > Backup storage screen, and then click Create backup storage.
4. On the Nodes step, select one node to add to the backup storage cluster, and then click Next.
5. On the NFS share step, specify the hostname or IP address of the NFS share, the export name, and select the NFS version. Then, click Next.

Note
NFS version 4 is recommended, as it provides better scalability and performance compared to NFS version 3, which has limitations in the protocol.

- **NFS share hostname or IP address**
  10.16.136.140

- **Export name**
  /share1

- **NFS version**
  - NFSv4 (recommended)
  - NFSv3

6. On the DNS step, specify an external DNS name for backup storage, for example, backupstorage.example.com. Backup agents will use this DNS name and the TCP port 44445 to upload backup data. Then, click Next.
Important

- Configure your DNS server according to the example suggested in the admin panel.
- Each time you change the network configuration of nodes in the backup storage cluster, adjust the DNS records accordingly.

This may require changing the DNS server configuration, which may look as follows:

```plaintext
$TTL 1h

@ IN SOA ns1.myhoster.com. root.backupstorage.example.com. (2021011213 ; serial
1h ; refresh
30m ; retry
7d ; expiration

```

7. On the **Acronis account** step, specify the following information for your Acronis product:
   - The URL of the cloud management portal (for example, https://cloud.acronis.com/) or the hostname/IP address and port of the local management server (for example, http://192.168.1.2:9877)
   - The credentials of a partner account in the cloud or of an organization administrator on the local management server
8. On the **Summary** step, review the configuration, and then click **Create**.

**Connecting to public cloud storage via Backup Gateway**

With Backup Gateway, you can have Acronis Cyber Protect Cloud or Acronis Cyber Protect 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
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 the storage backend.

Backups are cold data with a specific access pattern: the data is not accessed frequently but is expected to be available immediately when accessed. For this use case, it is cost-efficient to choose storage classes intended for long-term storage with 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

Archive storage classes like Amazon S3 Glacier, Azure Archive Blob, or Google Archive cannot be used for backup because they do not provide instant access to data. High access latency (several hours) makes it technically impossible to browse archives, restore data fast, and create incremental backups. Even though the archive storage is usually very cost-efficient, keep in mind that there are a number of different cost factors. In fact, the total cost of public cloud storage consists of payments for storing data, operations, traffic, data retrieval, early deletion, and so on. For example, an archive storage service can charge six months’ storage payment for just one data recall operation. If the storage data is expected to be accessed more frequently, the added costs increase significantly the total cost of data storage. In order to avoid the low data retrieval rate and to cut expenses, we recommend using Acronis Cyber Cloud for storing backup data.

**Limitations**

- 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. Using temporary disks may result in data loss.
- If you plan 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.
- 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 2 TB, provide at least 3 TB of logical space. The required raw storage will vary depending on the encoding mode: 9 TB (3 TB per node) in the 1+2 mode, 5 TB (1 TB per node) in the 3+2 mode, etc.
- A separate object container is required for each backup storage cluster.
- Redundancy by replication is not supported for backup storage.

**Prerequisites**
• The storage cluster has at least one disk with the **Storage** role.
• The destination storage has enough space for both existing and new backups.
• Ensure that each node to join the backup storage cluster has the TCP port 44445 open for outgoing Internet connections, as well as for incoming connections from Acronis backup software.

**To select a public cloud as the backup destination**

1. On the **Infrastructure > Networks** screen, make sure that the **Backup (ABGW) private** and **Backup (ABGW) public** traffic types are added to the networks you intend to use.
2. Open the **Storage services > Backup storage** screen, and then click **Create backup storage**.
3. On the **Backup destination** step, select **Public cloud**.
4. On the **Nodes** step, select nodes to add to the backup storage cluster, and then click **Next**.
5. On the **Public cloud** step, specify information relevant for your public cloud provider:
   a. Select a public cloud provider. If your provider is S3 compatible but not in the list, try **AuthV2 compatible (S3)** or **AuthV4 compatible (S3)**.
   b. Depending on the provider, specify **Region**, **Authentication (keystone) URL**, or **Endpoint URL**.
   c. In the case of **Swift object storage**, specify the authentication protocol version and attributes required by it.
   d. Specify user credentials. In the case of **Google Cloud**, select a JSON file with keys to upload.
   e. Specify the folder (bucket, container) to store backups in. The folder must be writeable.
      A separate object container should be used for each backup storage cluster.
   f. Click **Next**.
6. On the **Storage policy** step, select the desired tier, failure domain, and data redundancy mode. Redundancy by replication is not supported for Backup Gateway. For more information, refer to "Storage policies" in the Administrator Guide. Then, click **Next**.

7. On the **DNS** step, specify an external DNS name for backup storage, for example, **backupstorage.example.com**. Backup agents will use this DNS name and the TCP port 44445 to upload backup data. Then, click **Next**.
Important

- Configure your DNS server according to the example suggested in the admin panel.
- Each time you change the network configuration of nodes in the backup storage cluster, adjust the DNS records accordingly.

```
Domain name (not IP address)
backupstorage.example.com
```

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backupstorage.example.com. (2021011213 ; serial
 1h ; refresh
 30m ; retry
 7d ; expiration)
```

Note

For complex environments, HAProxy might be used to build a scalable and redundant load balancing platform, which can be easily moved or migrated and is independent from Acronis Cyber Infrastructure. For more information, refer to https://kb.acronis.com/content/64787.

8. On the Acronis account step, specify the following information for your Acronis product:

- The URL of the cloud management portal (for example, https://cloud.acronis.com/) or the hostname/IP address and port of the local management server (for example, http://192.168.1.2:9877)
- The credentials of a partner account in the cloud or of an organization administrator on the local management server
9. On the Summary step, review the configuration, and then click Create.