# Table of contents

Introduction .................................................................................................................................................. 3
Hardware requirements for installations with Backup Gateway ......................................................... 4
Installing Acronis Cyber Infrastructure ................................................................................................. 5
Creating the storage cluster .................................................................................................................. 6
Adding locations to Acronis Cyber Protect or Acronis Cyber Protect Cloud ..................................... 7
  Connecting to the local storage cluster via Backup Gateway ............................................................. 8
  Connecting to external NFS shares via Backup Gateway ................................................................. 10
  Connecting to public cloud storage via Backup Gateway ............................................................... 13
Adding nodes to Backup Gateway .......................................................................................................... 19
Updating the certificate for Backup Gateway .......................................................................................... 20
Re-registering Backup Gateway in a new Acronis Cyber Protect instance ........................................ 21
Changing the redundancy scheme for Backup Gateway ........................................................................... 22
Migrating backups from older Acronis solutions .................................................................................... 24
Monitoring Backup Gateway .................................................................................................................. 25
Releasing nodes from Backup Gateway .................................................................................................. 27
Introduction

Acronis Cyber Infrastructure represents a new generation of hyperconverged infrastructures targeted at both service providers and end customers. It is a scale-out, cost-efficient, and multi-purpose solution that combines universal storage and high-performance virtualization.

Acronis Cyber Infrastructure works seamlessly with the Acronis Cyber Cloud suite of products, Acronis Cyber Protect. It minimizes the number of technologies needed in datacenters and provides for additional performance improvements.

This guide describes how to deploy Acronis Cyber Infrastructure on a single node with the sole purpose of creating Backup Gateway endpoints.
Hardware requirements for installations with Backup Gateway

Normally, Acronis Cyber Infrastructure is installed on at least five nodes to fully utilize its built-in high availability and data redundancy capabilities. However, if you only want to use the Backup Gateway, you can deploy a very basic installation on a single virtual or physical node. Although in this case you may need to provide data redundancy by other means or risk losing user data. You can do the following:

- Use a virtual machine (VM) with at least two virtual HDDs (three disks are recommended). In this case, only one HDD will be used for data storage and you may need to make sure that the VM is made redundant by the virtualization solution it runs on.
- Use a physical server with at least two disks (three disks are recommended). Have in mind that you will need to use more disks for storage to enable data redundancy. For more details on hardware requirements, refer to "System requirements" in the Administrator Guide.

The following table lists the minimal hardware requirements for a node with Backup Gateway:

<table>
<thead>
<tr>
<th>Type</th>
<th>Management node with storage and Backup Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>64-bit x86 processors with AMD-V or Intel VT hardware virtualization extensions enabled.</td>
</tr>
<tr>
<td></td>
<td>4 cores(^1)</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>1 disk: system + metadata, 120 GB SATA HDD</td>
</tr>
<tr>
<td></td>
<td>1 disk: storage, SATA HDD, size as required(^2)</td>
</tr>
<tr>
<td>Network</td>
<td>10 GbE for storage traffic</td>
</tr>
<tr>
<td></td>
<td>1 GbE for other traffic</td>
</tr>
</tbody>
</table>

\(^1\) A CPU core can be a physical core in a multicore processor if you deploy on a physical server, or a virtual core in case you deploy in a VM.

\(^2\) If you plan to use Backup Gateway to store backups in the cloud, make sure the local storage cluster has plenty of logical space for staging (keeping backups locally before sending them to the cloud). For example, if you perform backups daily, provide enough space for at least 1.5 days’ worth of backups. For more details, refer to "Creating backup storage in a public cloud" in the Administrator Guide.
Installing Acronis Cyber Infrastructure

To install Acronis Cyber Infrastructure, do the following:

1. Obtain the distribution ISO image. To do that, visit the product page and submit a request for the trial version. You can also download the ISO from Acronis Cyber Cloud:
   a. Go to the management portal and select SETTINGS > Locations in the left menu.
   b. Click Add backup storage and click the Download ISO button in the open window.
2. Prepare the bootable media using the distribution ISO image (mount it to an IPMI virtual drive, create a bootable USB drive, or set up a PXE server).
3. Boot the server from the chosen media.
4. On the Welcome screen, choose Install Acronis Cyber Infrastructure.
5. On step 1, carefully read the End-User License Agreement. Accept it by selecting the I accept the End-User License Agreement check box, and then click Next.
6. On step 2, configure a static IP address for the network interface and provide a host name: either a fully qualified domain name (<hostname>,<domainname>) or a short name (<hostname>). A dynamic IP is not recommended as it might cause issues with reaching the nodes. Check that the network settings are correct.
7. On step 3, choose your time zone. Date and time will be set via NTP. You will need an Internet connection for synchronization to complete.
8. On step 4, specify what type of node you are installing. First, deploy one primary node. Then, deploy as many secondary nodes as you need.
   - If you chose to deploy the primary node, select two network interfaces: for internal management and configuration and for access to the admin panel. Also create and confirm a password for the superadmin account of the admin panel. This node will be the management node.
   - If you chose to deploy a secondary node, provide the IP address of the management node and the token. Both are obtained from the admin panel. Log in to the admin panel on port 8888. The panel's IP address is shown in the console after deploying the primary node. Enter the default username admin and the superadmin account password. In the admin panel, open Infrastructure > Nodes, and then click Connect node, to invoke a screen with the management node address and the token.
     The node may appear on the Infrastructure > Nodes screen with the Unassigned status as soon as the token is validated. However, you will be able to join it to the storage cluster only after the installation is complete.
9. On step 5, choose a disk for the operating system. This disk will have the supplementary role System, although you will still be able to set it up for data storage in the admin panel. You can also create software RAID1 for the system disk, to ensure its high performance and availability.
10. On step 6, enter and confirm the password for the root account, and then click Start installation.

Once the installation is complete, the node will reboot automatically. The admin panel IP address will be shown in the welcome prompt.
Creating the storage cluster

To create the storage cluster, do the following:

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.
Adding locations to Acronis Cyber Protect or Acronis Cyber Protect Cloud

**Note**
Migration from Acronis Storage versions 1.5-1.7 is no longer supported. Use Acronis Cyber Infrastructure 4.0 to migrate backups, and then upgrade to the latest version. For details, refer to "Migrating backups from older Acronis solutions" (p. 24).

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 geo-replicated.

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.

```
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
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**.
3. On the **Backup destination** step, select **Network File System (NFS) share**.
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.

```
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
```

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.

```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.

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**.
Adding nodes to Backup Gateway

You can add more nodes that will serve as targets for backups from Acronis Cyber Protect and/or Acronis Cyber Protect Cloud for high availability and scalability of your backup storage.

To add nodes to backup storage

1. Go to the Storage services > Backup storage > Nodes screen.
2. Click Add node.
3. Select nodes to join the backup storage cluster and click Add.

The nodes will be added to your backup storage and will run Backup Gateway.
Updating the certificate for Backup Gateway

When you register a Backup Gateway in Acronis Cyber Protect Cloud or Acronis Cyber Protect, they exchange certificates that are valid for three years. One and a half months before expiration, you will be alerted about the expiring certificate in the admin panel.

**Prerequisites**

- Ensure that two-factor authentication (2FA) is disabled for your partner account. You can also disable it for a specific user within a 2FA-enabled tenant, as described in the Acronis Cyber Cloud documentation, and specify the user credentials.
- 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.

**To update the certificate**

1. On the Storage services > Backup storage screen, go to the Settings tab, and then click Certificate.
2. Specify the credentials of a partner account in the cloud or of an organization administrator on the local management server.
3. Click Update.

The new certificate will be automatically loaded in five minutes.
Re-registering Backup Gateway in a new Acronis Cyber Protect instance

To switch configured backup storage to a different Acronis Cyber Protect instance, you need to re-register the gateway with that instance.

**To re-register backup storage**

1. On the Storage services > Backup storage screen, go to the Settings tab, and then click Re-registration.
2. Specify the hostname/IP address of the target management server and the port 9877 (for example, http://192.168.1.2:9877), and then enter your credentials for the management server.

   **Note**
   The address must be provided by using the HTTP protocol, not HTTPS.

3. Click Save.
Changing the redundancy scheme for Backup Gateway

You can update the redundancy scheme used for backup storage by changing the storage policy. Such a configurable redundancy scheme ensures high scalability and maximum efficiency of backup storage.

During the re-encoding process, data is partially stored with a new redundancy scheme, and the other part is stored with an old scheme. However, the system uses the storage policy with the least redundancy. For example, if you are switching from the 1+0 encoding mode to 1+2, the system will use the 1+0 encoding mode. In this case, it is critical not to turn off any storage node or disk until the process is complete.

**Important**
If you changed the encoding scheme for your backup storage cluster with the help of the technical support team, re-apply your redundancy settings in the admin panel to ensure that all data was encoded.

**Limitations**
- Redundancy by replication is not supported for backup storage.

**To change the storage policy**

1. On the Storage services > Backup storage screen, go to the Settings tab, and then click Storage policy.
2. Select the desired storage tier, failure domain, or data redundancy mode. For more information, refer to "Storage policies" in the Administrator Guide.
3. Click Save.
When the re-encoding process starts, its progress and the estimated time of completion will be shown on the screen. During this process, you can select another redundancy scheme. In this case, the current re-encoding process will be stopped and the new redundancy scheme will be applied.
**Migrating backups from older Acronis solutions**

Migration from Acronis Storage versions 1.5-1.7 is no longer supported. You can use Acronis Cyber Infrastructure 4.0 to migrate backups, and then upgrade to the latest version.

**To migrate backups from Acronis Storage 1.5-1.7**

1. Install Acronis Cyber Infrastructure version 4.0. To obtain the distribution ISO image, refer to [https://kb.acronis.com/content/63431](https://kb.acronis.com/content/63431).
2. Migrate your backups from Acronis Storage 1.5-1.7 to version 4.0 by following the instructions in "Migrating backups from older Acronis solutions" in the Acronis Cyber Infrastructure 4.0 Administrator Guide.
3. Wait until the migration is complete, and then update your cluster to the latest version, as described in "Installing updates" in the Acronis Cyber Infrastructure 4.0 Administrator Guide.

---

**Warning!**
An update process may interrupt data migration, which will lead to partial data unavailability.
Monitoring Backup Gateway

After you create backup storage, you can monitor it on the Storage services > Backup storage > Overview screen. The charts show the following information:

- **Nodes.** The chart shows the number and availability of nodes in the backup storage cluster.
- **Performance.** The chart shows the read and write activity of backup storage services over time.
- **Geo-replication.** The chart shows the geo-replication speed and backlog, which is the amount of data waiting to be replicated. If the geo-replication backlog does not decrease over time, it means the data cannot be replicated fast enough. The reason may be insufficient network transfer speed, and you may need to check or upgrade your network.
- **Append latency.** The chart shows the time spent on processing requests from backup agents to the storage.
- **Append throttle.** If the chart is not empty, it means the underlying storage lacks free space and the backup storage is throttling user requests to slow down the data flow.

Two thresholds, soft and hard, are set on the percentage of used storage space. When the soft threshold is reached, backup storage starts to throttle write operations. Throttling intensity depends on consumed space and increases until the hard threshold is reached. When the used space passes the hard threshold, throttling works with maximum intensity. The thresholds depend on the backup destination and the number of nodes in the backup storage cluster:

<table>
<thead>
<tr>
<th>Backup destination</th>
<th>Number of backup nodes</th>
<th>Soft threshold</th>
<th>Hard threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local cluster</td>
<td>1</td>
<td>93%</td>
<td>95%</td>
</tr>
<tr>
<td></td>
<td>2+</td>
<td>90%</td>
<td>92%</td>
</tr>
<tr>
<td>NFS</td>
<td>1</td>
<td>93%</td>
<td>95%</td>
</tr>
<tr>
<td>Public cloud</td>
<td>1</td>
<td>88%</td>
<td>90%</td>
</tr>
<tr>
<td></td>
<td>2+</td>
<td>85%</td>
<td>87%</td>
</tr>
</tbody>
</table>

- **Object storage.** The chart shows the object storage speed and backlog, which is the amount of data waiting to be uploaded to public cloud. If the object storage backlog does not decrease over time, it means the data cannot be uploaded fast enough. The reason may be insufficient network transfer speed, and you may need to check or upgrade your network.

You can also monitor backups storage nodes. To do this, go to Storage services > Backup storage > Nodes and click the required node. On the right pane, the Overview tab displays the performance statistics:

- **CPU/RAM:** CPU usage in percent over time, and RAM usage, in GiB over time
- **Successful/Failed request rate:** the number of successful and failed append requests per second
- **Egress/Ingress request rate:** the number of read and write requests per second
• **Throughput**: the amount of data read from or written to the backup storage per second
• **Request latency**: the time spent on processing requests
Releasing nodes from Backup Gateway

Backup storage is connected to one specific backup destination. If you need to switch the destination, for example, from a public cloud to a local storage cluster or one public cloud bucket to another, you need to delete the backup storage by releasing all of its nodes from the backup storage cluster and create a new one.

When the backup storage is deleted, it is also unregistered from your Acronis backup software, which loses access to the backup destination.

Limitations

- If you choose a forcible release and keep Backup Gateway registered in your Acronis backup software, next time you will need to register another gateway in your Acronis backup software. For that, you will have to delete and recreate not just the backup storage but also the entire storage cluster.

To release a node from backup storage

1. Go to the Storage services > Backup storage > Nodes screen.
2. Click a node to release, and then on the node right pane, click Release.
3. Click Release in the confirmation window.

The backup storage will remain operational until there is at least one node in it.

To release all nodes from backup storage

1. Go to the Storage services > Backup storage > Nodes screen.
2. Select all of the backup nodes or click the only node in the backup storage cluster, and then click Release.
3. In the Release nodes window:
   - Select (Recommended) Gracefully to delete Backup Gateway from the node and unregister it from your Acronis backup software.
   - Select Forcibly to delete Backup Gateway from the node but do not unregister it from your Acronis backup software.

   **Important**
   Select this option only if you are sure that the gateway is already unregistered from your Acronis backup software.

4. If you chose a graceful release, specify the credentials of your administrator account in your Acronis backup software.
5. Click Release.