

Acronis

Acronis Storage 2.4

Backup Gateway Quick Start Guide

July 18, 2018

Copyright Statement

Acronis International GmbH, 2002-2016. All rights reserved.

"Acronis" and "Acronis Secure Zone" are registered trademarks of Acronis International GmbH.

"Acronis Compute with Confidence", "Acronis Startup Recovery Manager", "Acronis Active Restore",

"Acronis Instant Restore" and the Acronis logo are trademarks of Acronis International GmbH.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <http://kb.acronis.com/content/7696>

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121 and patent pending applications.

Contents

- 1. Introduction 1**
 - 1.1 About This Guide 1
 - 1.2 Hardware Requirements for ABGW-only Installations 1

- 2. Installing Acronis Storage 3**

- 3. Creating the Storage Cluster 6**

- 4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway 8**
 - 4.1 Connecting to the Local Storage Cluster via Acronis Backup Gateway 9
 - 4.2 Connecting to External NFS Shares via Acronis Backup Gateway 13
 - 4.3 Connecting to Public Cloud Storage via Acronis Backup Gateway 17

- 5. Migrating Backups from Older Solutions 21**
 - 5.1 Migrating Backups from Acronis Storage 1.5 22
 - 5.2 Migrating Backups from Acronis Storage Gateway 1.6 and 1.7 (NFS) 26

- 6. Monitoring Acronis Backup Gateway 30**

- 7. Releasing Nodes from Acronis Backup Gateway 32**

CHAPTER 1

Introduction

1.1 About This Guide

This guide describes how to deploy Acronis Storage with the sole purpose of creating Acronis Backup Gateway (ABGW) endpoints.

1.2 Hardware Requirements for ABGW-only Installations

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

- Use a virtual machine (VM) with at least two virtual HDDs (three are recommended). In this case, only one HDD will be used for data storage and you must 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 are recommended). Have in mind that you will need to use more disks for storage to enable data redundancy. For more details on how to plan your server configuration, see the [Installation Guide](#).

Other minimal requirements are:

- 150 GB or higher capacity of each HDD/SSD.

Note: If you plan to use Acronis 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, see the [Administrator's Guide](#).

- A dual-core CPU.
- 4GB RAM.
- 1Gbps network interface. It is recommended to use static IP addresses. You can also use the same network interface for both internal and external traffic (but you are advised to configure secure networking later).

CHAPTER 2

Installing Acronis Storage

To install Acronis Storage, do the following:

1. Prepare 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).
2. Boot the server from the chosen media.
3. On the welcome screen, choose **Install Acronis Storage**. After the installation program loads, you will see the **Installation Summary** screen.
4. Open the **INSTALLATION DESTINATION** screen and select a device in the **Device Selection** section. Configure other options if required.
5. Open the **ACRONIS STORAGE** screen, in the **Component Installation** section, choose **Management Panel and Storage**.

Component Installation

- Management Panel.** The web user interface for adding and managing storage nodes.
- Storage.** Choose this option only if the Management Panel is already installed.
- Management Panel and Storage.** Both components at once.

Important: Only one management panel is required, so choose this option for the first node only!

Management network

eno16777736 - 10.30.26.129 ▼

The Management Network is used by the management node to configure and manage storage nodes. It can also be used by storage administrators for accessing storage nodes directly via SSH. This network should be protected and inaccessible over WAN. It can be the same as the private Storage Network used for communication between storage nodes.

Management Panel network

eno16777736 - 10.30.26.129 ▼

The Management Control Panel Network is used by storage administrators to access the web control panel of Storage. In most cases, it can be the same as the Management Network. If, however, the Management Network is only accessible by storage nodes, choose another network for the control panel, one that can be accessed by storage administrators. For security reasons, the web control panel should not be accessible from public/WAN networks.

Create a password for the Management Panel

Confirm the password

6. Make sure that the appropriate network interface is selected in both **Management Panel network** and **Management network** drop-down lists.
7. Create a password for the superadmin account of the management panel. Click **Done**.
8. Click **Begin Installation**. While Acronis Storage is installing, create a password for the root account. Installation will not finish until the password is created.

Once the installation is complete, the node will reboot automatically and you will see a welcome prompt with the address of the management panel. For example:

```
Use the following hostname and IP address to connect to this server:
localhost.localdomain
(IP: 10.94.15.104)

Web Control Panel is available on the following addresses:
http://10.94.15.104:8888
```

Log in to the management panel using the default user name shown on the login screen and password created during installation.

Note: If prompted, add the security certificate to browser's exceptions.

CHAPTER 3

Creating the Storage Cluster

To create the storage cluster, do the following:

1. Open the **NODES** screen and click the 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 dashes ("-").

× New cluster

Cluster

cluster1

Storage interface

eth0 - 10.100.6.105

Encryption

New cluster Advanced configuration

4. Click the cogwheel icon next to the **Storage interface** drop-down list.
5. On the **Network Configuration** screen, select a network interface and click **Choose role**.
6. Select the network roles as pictured below and click **Done**.

✕ Choose roles

- Internal
 - Management
 - Storage
 - Object Storage private
 - ABGW private
- Public
 - iSCSI
 - S3 public
 - ABGW public
 - Web CP
 - SSH
 - NFS
- Custom [\(configure\)](#)

7. Close the roles tab and, back on the **New cluster** tab, click **New Cluster** to create the cluster.

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

CHAPTER 4

Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

Note: If you are going to migrate your Acronis Storage Gateway, skip the steps described in this chapter and proceed to *Migrating Backups from Older Solutions* on page 21.

The Acronis 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-premise storage for their clients’ backed-up data.

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

Acronis Backup Gateway supports the following storage backends:

- Acronis 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

4.1. Connecting to the Local Storage Cluster via Acronis Backup Gateway

and other overhead, which reduces overall performance.

Note:

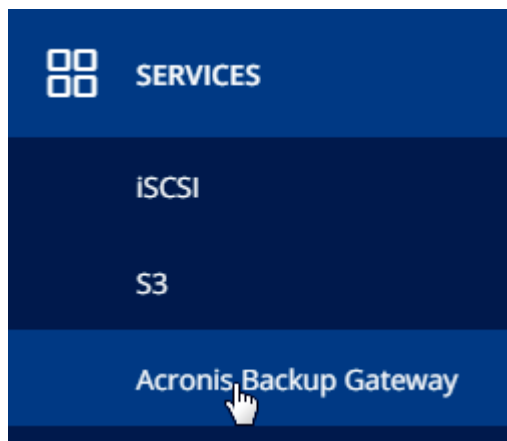
1. When configuring Acronis Backup Gateway, you will need to provide the credentials of your administrator account in the Acronis backup software.
2. In cases when not local but external storage (e.g., NFS) is used with Acronis Backup Gateway, redundancy has to be provided by said external storage. Acronis Backup Gateway does not provide data redundancy or perform data deduplication itself.

4.1 Connecting to the Local Storage Cluster via Acronis Backup Gateway

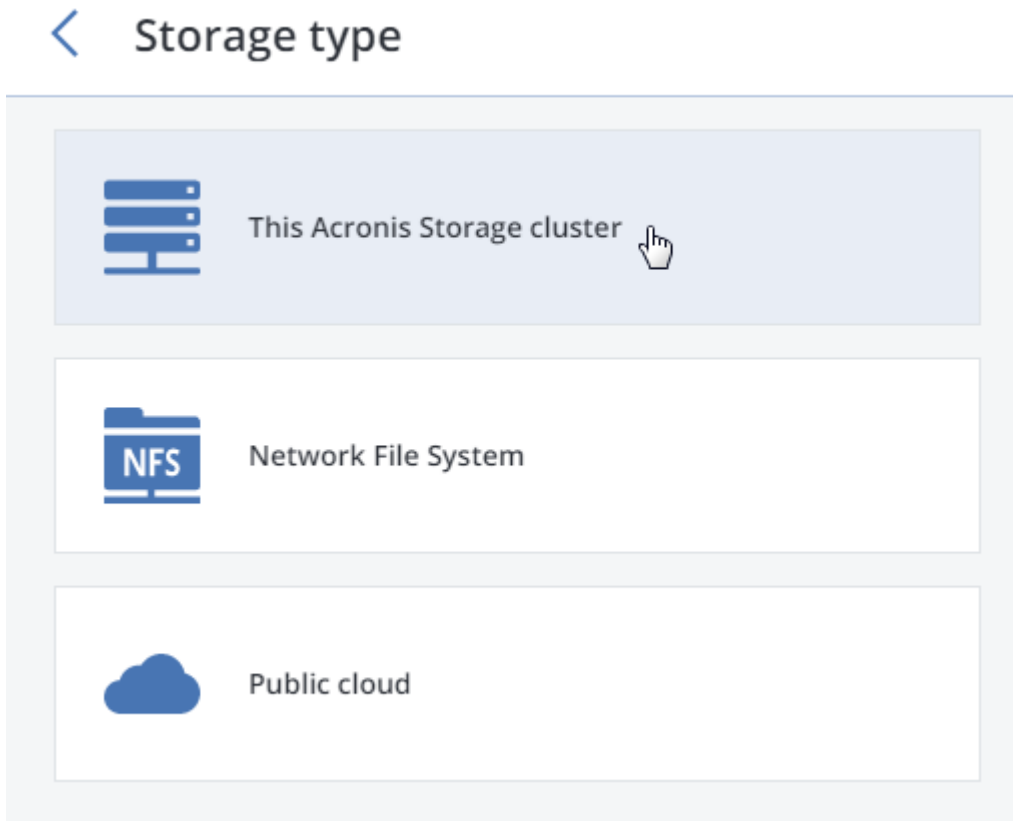
Before you proceed, make sure that the destination storage has enough space for backups.

To set up Acronis Backup Gateway, do the following:

1. In the left menu, click **SERVICES > Acronis Backup Gateway**.



2. Select the only available node and click **Create gateway** in the right menu.
3. Select **This Acronis Storage cluster** as storage type.



4. Make sure a network interface with the **ABGW private** role is selected in the drop-down list. The corresponding interfaces with the **ABGW public** role will be selected automatically. Click **NEXT**.

Note: If necessary, click the cogwheel icon and assign the required role(s) to network interfaces on the **Network Configuration** screen.



5. On the **Volume Parameters** tab, select the desired tier, failure domain, and data redundancy mode.

< Volume parameters

Tier:

Tier 0

Data redundancy:

Erasure coding

Failure-domain:

Disk

Encoding 1+0	0% overhead	
Encoding 1+2	200% overhead	
Encoding 3+2	67% overhead	
Encoding 5+2	40% overhead	i
Encoding 7+2	29% overhead	i
Encoding 17+3	18% overhead	i

PROCEED

Note:

1. Redundancy by replication is not supported for Acronis Backup Gateway.
2. You can later change the erasure coding mode on the **Acronis Backup Gateway > Parameters** panel.

6. 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.

← DNS Configuration

DNS name

This would probably require to change the configuration of the DNS server. The DNS configuration may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com.
root.nfs.backup.example.com. (
    2017060813 ; serial
    1h ; refresh
    30m ; retry
    7d ; expiration
    1h ) ; minimum

; primary name server
NS ns1.myhoster.com.

; secondary name server
NS ns2.myhoster.com.

A 10.250.14.12
```

PROCEED

Important:

1. Configure your DNS server according to the example suggested in the management panel.

4.2. Connecting to External NFS Shares via Acronis Backup Gateway

2. Each time you changes nodes in the Acronis Backup Gateway cluster, adjust the DNS settings accordingly.

Click **NEXT**.

7. On the **Registration** pane, specify the following, depending on your Acronis backup software:
 - In **Account Server Name**, 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 **Acronis 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**.

4.2 Connecting to External NFS Shares via Acronis Backup Gateway

Note:

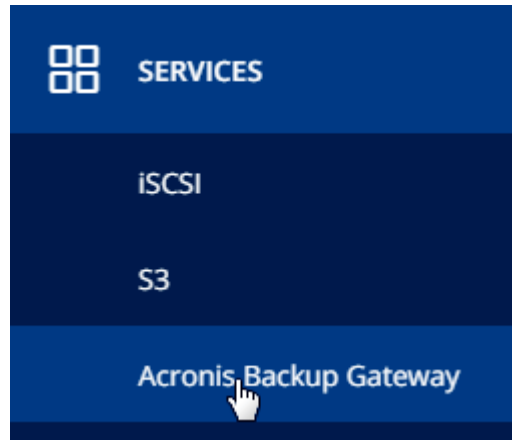
1. Acronis Storage does not provide data redundancy on top of NFS volumes. Depending on the implementation, NFS shares may use their own hardware or software redundancy.
2. In the current version of Acronis Storage, only one cluster node may store backups on an NFS volume.

Before you proceed, make sure that:

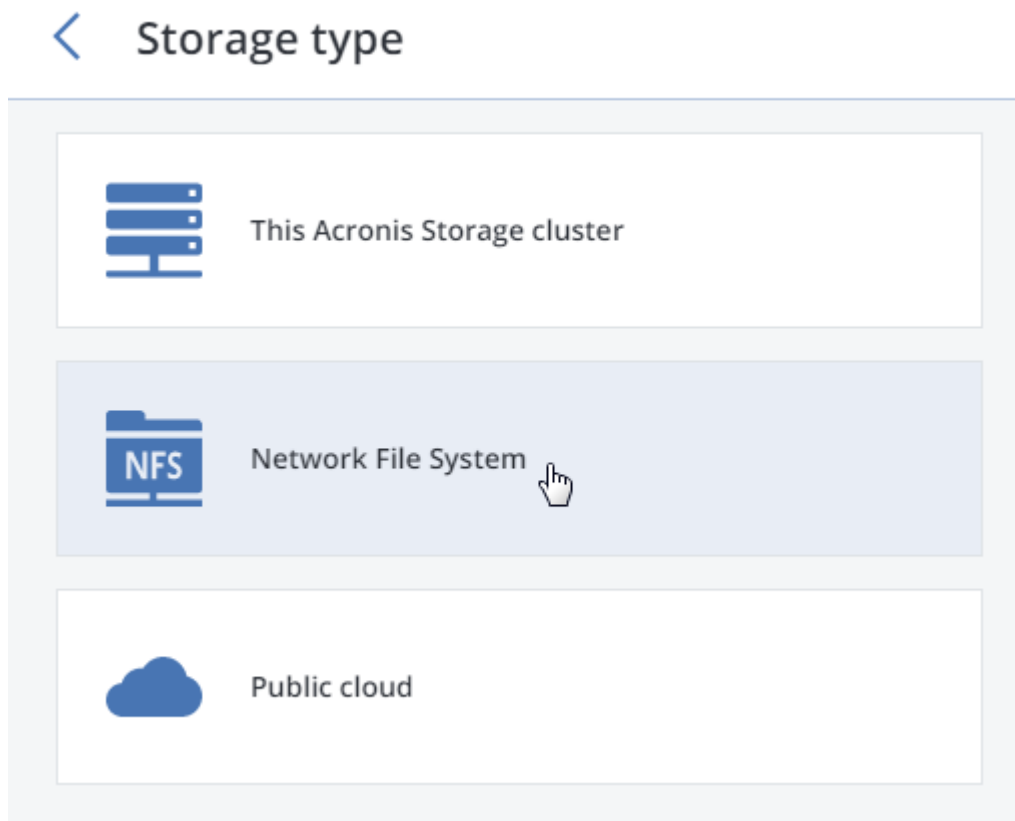
1. The NFS share has enough space for backups;
2. Each NFS export is used by only one gateway. In particular, do not configure two Acronis Storage installations to use the same NFS export for backup storage.

To set up Acronis Backup Gateway, do the following:

1. In the left menu, click **SERVICES > Acronis Backup Gateway**.



2. Select the only available node and click **Create gateway** in the right menu.
3. Select **Network File System** as storage type.



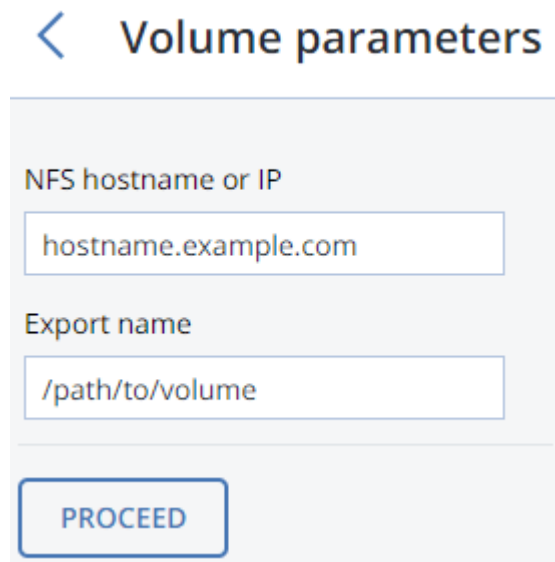
4. Make sure a network interface with the **ABGW private** role is selected in the drop-down list. The corresponding interfaces with the **ABGW public** role will be selected automatically. Click **NEXT**.

4.2. Connecting to External NFS Shares via Acronis Backup Gateway

Note: If necessary, click the cogwheel icon and assign the required role(s) to network interfaces on the **Network Configuration** screen.



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



6. 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.

< DNS Configuration

DNS name

This would probably require to change the configuration of the DNS server. The DNS configuration may look as follows:

```
$TTL 1h

@   IN  SOA  ns1.myhoster.com.
      root.nfs.backup.example.com. (
        2017060813   ; serial
        1h   ; refresh
        30m   ; retry
        7d   ; expiration
        1h ) ; minimum

; primary name server
NS ns1.myhoster.com.

; secondary name server
NS ns2.myhoster.com.

A 10.250.14.12
```

PROCEED

Important:

1. Configure your DNS server according to the example suggested in the management panel.
2. Each time you changes nodes in the Acronis Backup Gateway cluster, adjust the DNS settings accordingly.

Click **NEXT**.

4.3. Connecting to Public Cloud Storage via Acronis Backup Gateway

7. On the **Registration** pane, specify the following, depending on your Acronis backup software:
 - In **Account Server Name**, 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 **Acronis 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**.

4.3 Connecting to Public Cloud Storage via Acronis Backup Gateway

With Acronis Backup Gateway, you can have Acronis Backup Cloud or Acronis Backup Advanced store backups in a number of public clouds: Amazon S3, IBM Cloud, Alibaba Cloud, I1J, Cleversafe, Microsoft Azure, Swift object storage, Softlayer (Swift), Google Cloud Platform, as well as solutions using S3 with the older AuthV2-compatible authentication methods. However, compared to the local Acronis 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 Acronis 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.

Important:

1. When working with public clouds, Acronis 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 Acronis Backup Gateway on multiple cluster nodes and select a good redundancy mode. If Acronis Storage 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 Storage with the gateway is deployed in a virtual machine, make sure it is made redundant by the virtualization solution it runs on.

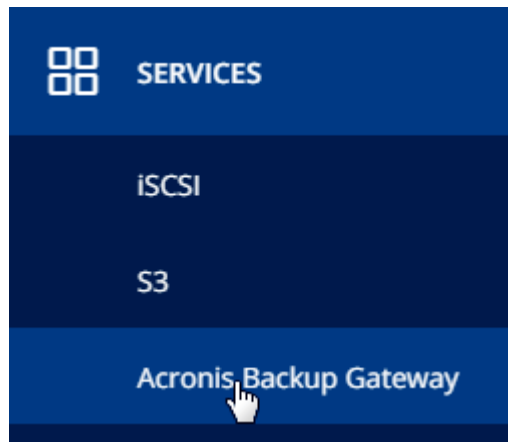
2. Make sure the local storage cluster has plenty of logical space for staging. For example, if you perform backup daily, provide enough space for at least 1.5 days' worth of backups. If the daily backup total is 2TB, provide at least 3TB of logical space. The corresponding raw storage required will vary depending on the encoding mode: 9TB (3TB per node) in the mode 1+2, 5TB (1TB per node) in the mode 3+2, etc.
3. You must update Acronis Backup Agents to version 12.0.4492 (Windows/Mac) or 12.0.4470 (Linux). Otherwise agents' attempts to place backups in the new storage backend will result in "Backup failed" errors.
4. If you are to store backups in an Amazon S3 cloud, keep in mind that Acronis 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. Acronis Backup Gateway detects such delays and protects backup integrity by blocking access until the cloud updates.

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

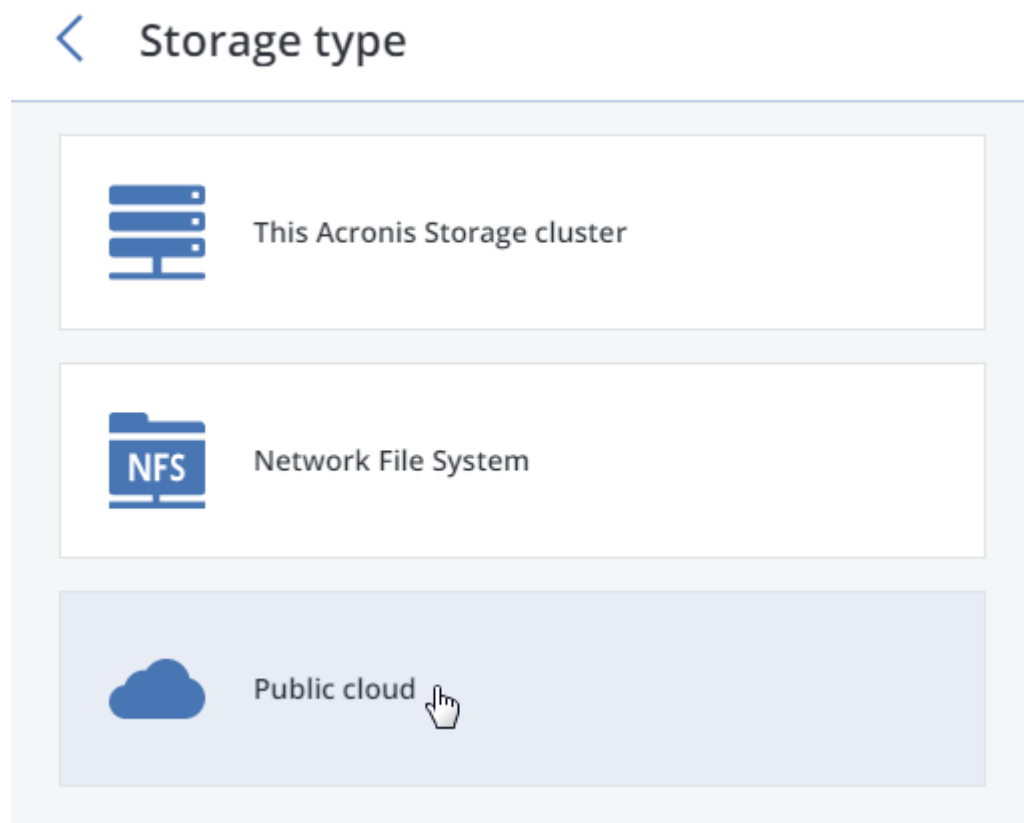
To set up Acronis Backup Gateway, do the following:

1. In the left menu, click **SERVICES > Acronis Backup Gateway**.

4.3. Connecting to Public Cloud Storage via Acronis Backup Gateway



2. Select the only available node and click **Create gateway** in the right menu.
3. Select **Public Cloud** as storage type.



4. Make sure a network interface with the **ABGW private** role is selected in the drop-down list. The corresponding interfaces with the **ABGW public** role will be selected automatically. Click **NEXT**.

Note: If necessary, click the cogwheel icon and assign the required role(s) to network interfaces on the **Network Configuration** screen.



5. On the **Public cloud parameters** pane, do the following:
 - 5.1. Select a public cloud provider. If your provider is S3-compatible but not in the list, try **AuthV2 compatible**.
 - 5.2. Depending on the provider, specify **Region**, **Authentication (keystone) URL**, or **Endpoint URL**.
 - 5.3. In case of Swift object storage, specify the authentication protocol version and attributes required by it.
 - 5.4. Specify user credentials. In case of Google Cloud, select a JSON file with keys to upload.
 - 5.5. Specify the folder (bucket, container) to store backups in. The folder must be writeable.Click **NEXT**.
6. On the **Registration** pane, specify the following, depending on your Acronis backup software:
 - In **Account Server Name**, 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 **Acronis Account**, specify the credentials of a partner account in the cloud or of an organization administrator on the local management server..
7. Finally, click **DONE**.

CHAPTER 5

Migrating Backups from Older Solutions

By means of Acronis Backup Gateway, you can migrate backups from Acronis Storage 1.5 and Acronis Storage Gateway 1.6 and 1.7 to a storage backend of your choice: local storage cluster, external NFS, or public cloud.

Important:

1. Before you proceed, make sure that the destination storage backend has enough space for both existing and new backups.
2. Migration to NFS backends is not available if multiple nodes are selected as Backup Gateway.

The migration procedure can be described as follows:

1. Root credentials for SSH access to the chosen source storage are provided to Acronis Backup Gateway.
2. Acronis Backup Gateway sets up a proxy on the source storage that starts redirecting requests incoming from Acronis Backup Agents from the source storage to Acronis Backup Gateway.
3. Acronis Backup Gateway starts relocating backups to the chosen storage backend. The data that remains to be migrated is shown in the **Migration Backlog** section on the Acronis Backup Gateway **Overview** screen. When the backlog empties, all data has been migrated.

After the migration has started, the data of new and incremental backups is stored on the destination storage. Backups from the source storage are pulled in the background. The entire process is transparent to backup agents, which continue working uninterrupted.

4. To be able to dispose of the source storage after migration completes, requests from Acronis Backup

Agents are directed straight to Acronis Backup Gateway, bypassing the proxy on the source storage. Steps that you need to take depend on how the source storage is registered in Acronis Backup Cloud: under the IP address or DNS name.

- If the source storage is already registered under the DNS name, you need to change the IP address behind it to those of the Acronis Backup Gateway nodes.
- If the source storage is registered under the IP address, it is strongly recommended to re-register Acronis Backup Gateway in Acronis Backup Cloud under a DNS name that resolves into the IP addresses of Acronis Backup Gateway nodes. Using a DNS name will provide a smoother transition and you will not need to reconfigure Acronis Backup Cloud even if you change nodes in the Acronis Backup Gateway (you will still need to adjust the IP addresses behind the DNS name accordingly).

Alternatively, if you do not want to use a DNS name, you need to wait for the migration to complete, shut down both the source and destination machines, and reconfigure your network so that the public interface of the destination machine gets the IP address of the source machine.

The concrete steps that you need to perform in the management panel to initiate backup migration are described in the next subsections.

5.1 Migrating Backups from Acronis Storage

1.5

1. Update all Acronis Storage 1.5 nodes to version 1.5.65655 or newer as earlier versions are not eligible for migration. To do this, log in to the Acronis Storage web console, proceed to **SETTINGS > Software Update**, upload the [latest ISO image](#), and click **Update**.
2. Log in to the new Acronis Storage cluster and on the **SERVICES > Acronis Backup Gateway > Nodes** screen, select one or more nodes and click **Migrate**.
3. Select **Acronis Storage 1.5** and click **NEXT**.
4. Specify the DNS name of the source storage registered in Acronis Backup Cloud and click **NEXT**.

< Enter source storage DNS (2/9)

Specify the DNS name of the source storage registered in Acronis Backup Cloud.

DNS name

BACK

NEXT

5. Provide the credentials for the cloud management portal of the Acronis Backup Cloud installation that the source storage is registered in and click **NEXT**.
6. Enable SSH access on all FES nodes of Acronis Storage 1.5 as instructed and click **NEXT**.
7. Map the public IP addresses of FES nodes accessible via SSH to their private IP addresses and click **NEXT**. This step is required to access FES nodes via SSH through tunnels.

< Set up IP mapping for FES nodes (5/9)

Listed below are public IP addresses of the FES nodes in the source storage. For each FES node, specify its private IP address open for SSH connections.

Public IP address (FES)

Private IP address (SSH)

10.28.74.3

10.28.74.9

BACK

NEXT

8. Choose a destination storage type to create a gateway to:
 - local Acronis Storage cluster,

- external NFS, or
 - public cloud.
9. Make sure a network interface with the **ABGW private** role is selected in the drop-down list. The corresponding interfaces with the **ABGW public** role will be selected automatically. Click **NEXT**.

Note: If necessary, click the cogwheel icon and assign the required role(s) to network interfaces on the **Network Configuration** screen.

10. Configure the destination storage backend:

- For a storage cluster, select the desired tier, failure domain, and redundancy mode.
- For NFS, specify a hostname or IP address, an export name and path, and choose the NFS version.

< Volume parameters

NFS hostname or IP

nfs.example.com

Export name

/path/to/export

NFS3 (no clustering)

NFS4

- For public cloud, select a public cloud provider, specify credentials, and the name of the folder (bucket, container).

Important: You must update Acronis Backup Agents to version 12.0.4492 (Windows/Mac) or 12.0.4470 (Linux). Otherwise agents' attempts to place backups in the new storage backend will result in "Backup failed" errors.

< Public cloud parameters

Select the object storage type

Amazon S3 ▼

Region

us-east-1 ▼

Access key ID

Secret Access key

Bucket

acronis-us-west-gateway-files

Click **NEXT**.

11. Review the source and destination storages and click **PROCEED**.
12. On the next panel, follow the instructions to point the source storage DNS name to the IP addresses of your new Acronis Storage cluster. Having updated the DNS configuration, click **START MIGRATION**. If all the backup agents have been rerouted to the new Acronis Storage cluster, the migration will start. Otherwise you will need to wait until all backup agents have cached the new IP addresses.

Reconfigure DNS

Before migration can start, all traffic between backup agents and source storage must be rerouted via a TCP proxy that has been set up in this cluster. For this, you will need to reconfigure your DNS server as suggested below to map source storage's DNS name `source.example.com` to this storage cluster's IP address(es). After that, all backup agents must cache the new IP address(es), which may take about a day.

Suggested DNS configuration

[Copy to clipboard](#)

```
$TTL 1h

@      IN      SOA     ns1.myhoster.com. source.example.com (
      2018042013  ; serial
      1h       ; refresh
      30m      ; retry
      7d       ; expiration
      1h      ; minimum

; primary name server
NS ns1.myhoster.com.

; secondary name server
NS ns2.myhoster.com.

A 10.248.64.99
```

✖ [Cancel migration and reset settings](#)

START MIGRATION

Depending on data size, migration may take as long as several days.

5.2 Migrating Backups from Acronis Storage Gateway 1.6 and 1.7 (NFS)

1. Disable the firewall or explicitly open TCP port 44446 on the source Acronis Storage Gateway.
 - To disable the firewall, run

5.2. Migrating Backups from Acronis Storage Gateway 1.6 and 1.7 (NFS)

```
# systemctl stop firewalld
```

- To open TCP port 44446 in the firewall, do the following:

- 1.1. Find out the zone where port 44445 is open:

```
# firewall-cmd --list-all-zones | grep active  
mix_eth0 (active)
```

- 1.2. Add the required port to the same zone:

```
# firewall-cmd --zone=mix_eth0 --permanent --add-port=44446/tcp  
# firewall-cmd --reload
```

2. In the management panel of the ABGW node, proceed to **SERVICES > Acronis Backup Gateway > Nodes**, select the only available node to run the gateway services on, and click **Migrate**.
3. Select the source storage version and click **NEXT**.
4. Specify the connection details for the source storage and click **NEXT**.

< Connect to source (2/7)

Specify the address of the source storage (as registered in Backup Cloud) and the root password to that machine.

Hostname or IP address

Password

Make sure the SSH service is running and port 22 is open for incoming connections.

5. Provide the credentials for the cloud management portal of the Acronis Backup Cloud installation that the source storage is registered in and click **NEXT**.
6. If the source storage is registered in Acronis Backup Cloud under an IP address, you will see the DNS configuration screen. On it, click **RE-REGISTER WITH DNS** and specify the source storage DNS name (recommended, see above). Or, if you want to keep using the IP address, click **PROCEED WITH IP**.

Important:

1. If you specified a DNS name, configure your DNS server according to the suggested example.
2. Each time you change nodes in the Acronis Backup Gateway, adjust the DNS settings accordingly.

7. Choose a destination storage type to create a gateway to:

- local Acronis Storage cluster,
- external NFS, or
- public cloud.

8. Make sure a network interface with the **ABGW private** role is selected in the drop-down list. The corresponding interfaces with the **ABGW public** role will be selected automatically. Click **NEXT**.

Note: If necessary, click the cogwheel icon and assign the required role(s) to network interfaces on the **Network Configuration** screen.

9. Configure the destination storage backend:

- For a storage cluster, select the desired tier, failure domain, and redundancy mode.
- For NFS, specify a hostname or IP address, an export name and path, and choose the NFS version.

< Volume parameters

NFS hostname or IP

Export name

NFS3 (no clustering)

NFS4

- For public cloud, select a public cloud provider, specify credentials, and the name of the folder

5.2. Migrating Backups from Acronis Storage Gateway 1.6 and 1.7 (NFS)

(bucket, container).

Important: You must update Acronis Backup Agents to version 12.0.4492 (Windows/Mac) or 12.0.4470 (Linux). Otherwise agents' attempts to place backups in the new storage backend will result in "Backup failed" errors.

< Public cloud parameters

Select the object storage type

Amazon S3 ▼

Region

us-east-1 ▼

Access key ID

Secret Access key

Bucket

acronis-us-west-gateway-files

Click **NEXT**.

10. Review the source and destination storages and click **START MIGRATION**.

Depending on data size, migration may take as long as several days.

CHAPTER 6

Monitoring Acronis Backup Gateway

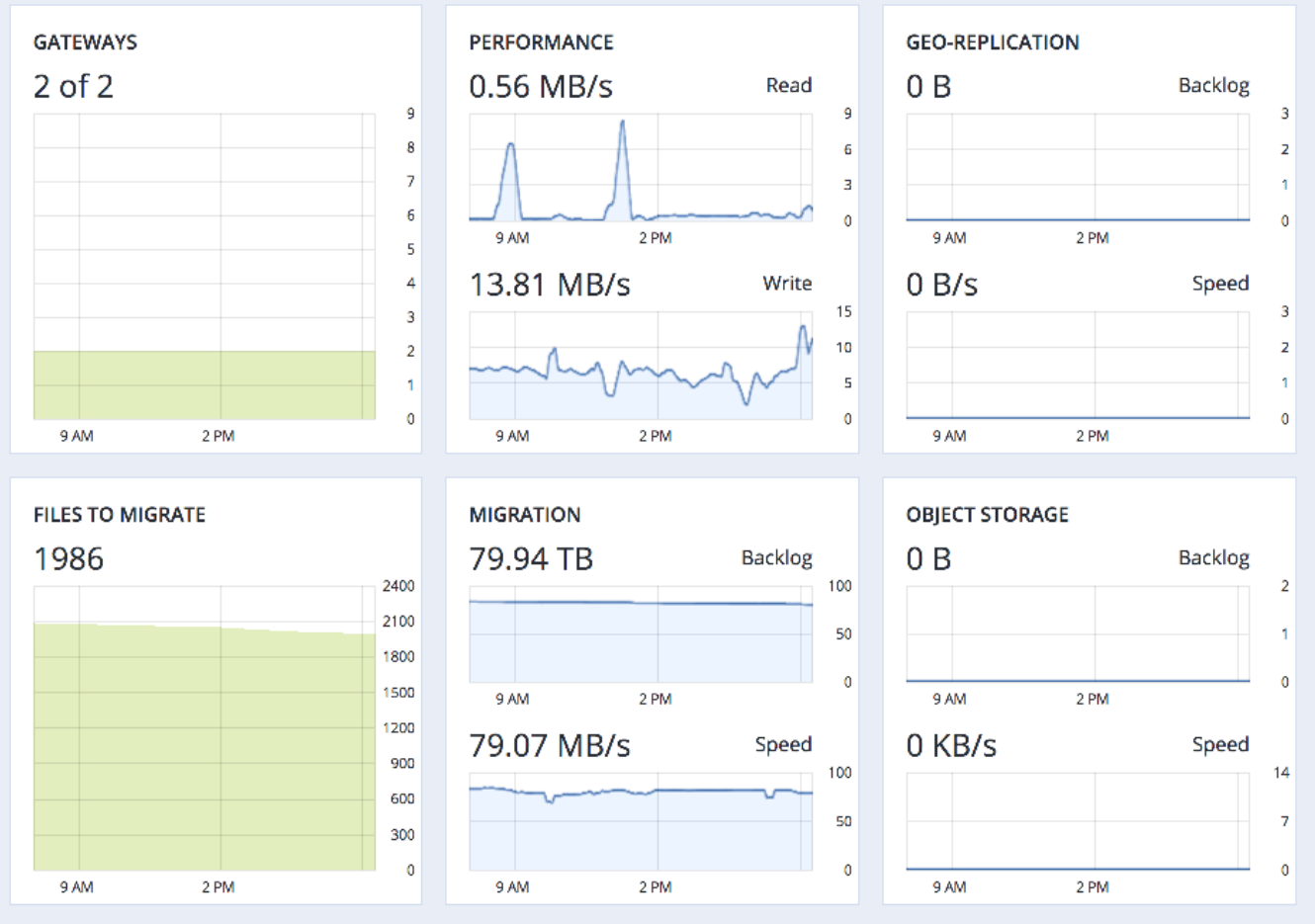
After you create an Acronis Backup Gateway, you can monitor it on the **SERVICES > Acronis Backup Gateway > OVERVIEW** screen. The charts show the following information:

- the performance of Acronis Backup Gateway services,
- the geo-replication speed and backlog (the amount of data waiting to be replicated),
- migration speed and backlog (the amount of data waiting to be migrated),
- object storage speed and backlog (the amount of data waiting to be uploaded to public cloud),
- how many files are left in migration queue.

If backlogs do not decrease over time, it means the data cannot be replicated, migrated, or uploaded fast enough. The reason may be insufficient network transfer speed, and you may need to check or upgrade your network.

Acronis Backup Gateway

OVERVIEW **NODES** GEO-REPLICATION



CHAPTER 7

Releasing Nodes from Acronis Backup Gateway

Acronis Backup Gateway is meant to provide access to one specific storage backend. If you need to switch the backend, e.g., from a public cloud to a local Acronis Storage cluster or one public cloud bucket to another, you need to delete the Acronis Backup Gateway by releasing all its nodes and create a new one.

Note: When the Acronis Backup Gateway is deleted, it is also unregistered from your Acronis backup software, which loses access to the storage backend.

Do the following to release the only node in the gateway:

1. On the **SERVICES > Acronis Backup Gateway > NODES** screen, select the node and click **Release**.
2. On the **Unregister Acronis Backup Gateway** panel, choose one of the following:
 - **Graceful release** (recommended, see note below). Releases the node, deletes the Acronis Backup Gateway and unregisters it from your Acronis backup software.
 - **Force release**. Releases the node, deletes the Acronis Backup Gateway but does not unregister it from your Acronis backup software.

Important: Choose this option only if you are sure that the gateway has already been unregistered from your Acronis backup software. Otherwise, you will need to register a new gateway in your Acronis backup software and for that you will need to delete and recreate not just the Acronis Backup Gateway but also the entire Acronis Storage cluster.

✕ Unregister from Acronis Backup Cloud

Graceful release

Force release

To unregister this Acronis Backup Gateway cluster from Acronis Backup Cloud, provide the credentials of your administrator account in Acronis Backup Cloud

Administrator account

User

Password

3. Specify the credentials of your administrator account in your Acronis backup software and click **NEXT**. In case the release is forced, simply click **NEXT**.