Acronis Storage 2.4

Backup Gateway Quick Start Guide

April 12, 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 Acronis Storage Cluster **6**

4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway **9**

4.1 Connecting to the Acronis Storage Cluster via Acronis Backup Gateway 10

4.2 Connecting to External NFS Shares via Acronis Backup Gateway 14

4.3 Connecting to Public Cloud Storage via Acronis Backup Gateway 18

5. Migrating Backups from Acronis Storage Gateway **21**

6. Monitoring Acronis Backup Gateway **27**

7. Releasing Nodes from Acronis Backup Gateway **29**

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 Acronis Storage Installation Guide.

Other minimal requirements are:

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

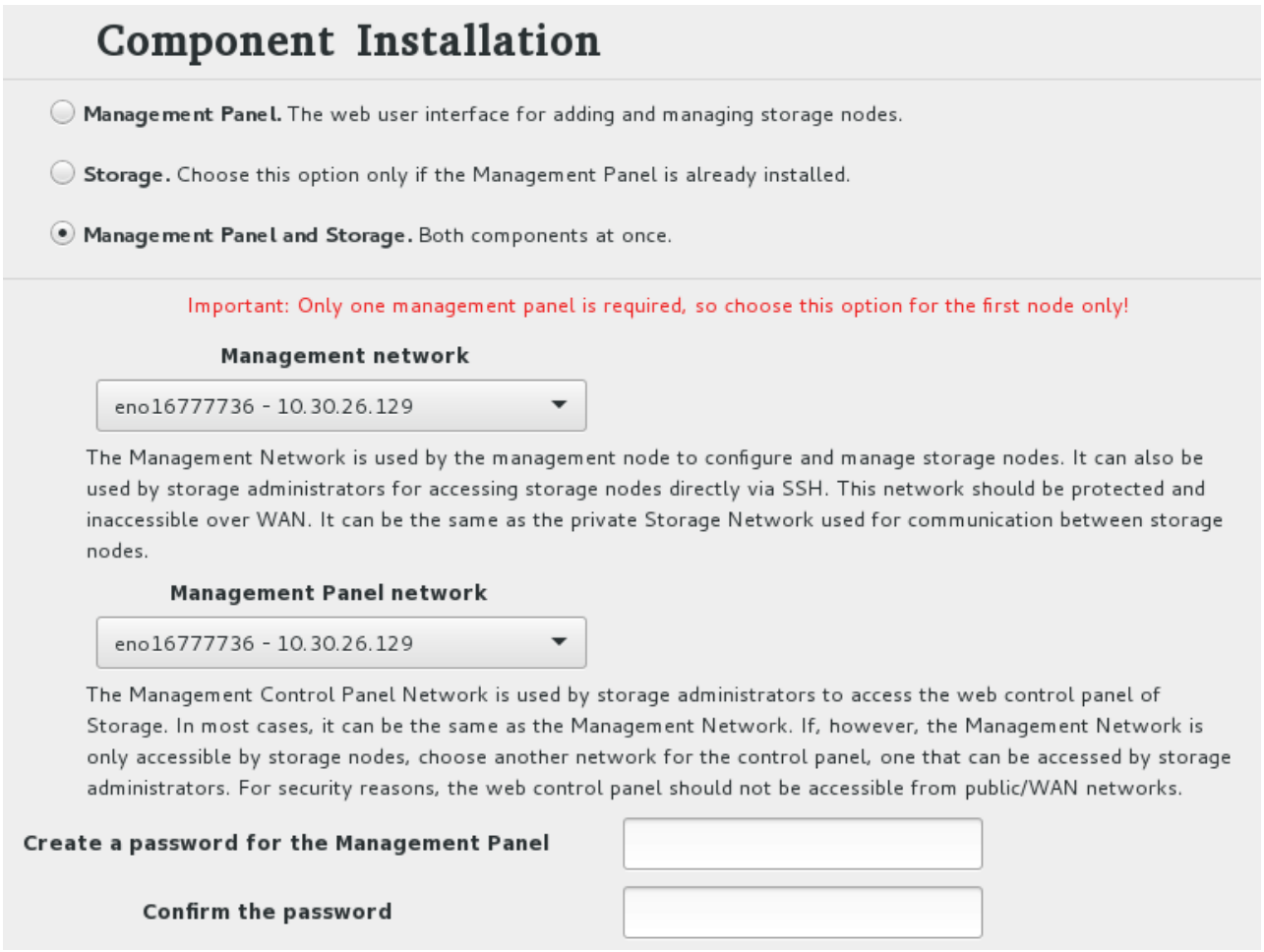
- a dual-core CPU,
- 4GB RAM,
- 1Gbps network interface. It is recommended to use static IP addresses. You can also use the same network interface for both internal and external traffic (but you are advised to configure secure networking later).

CHAPTER 2

Installing Acronis Storage

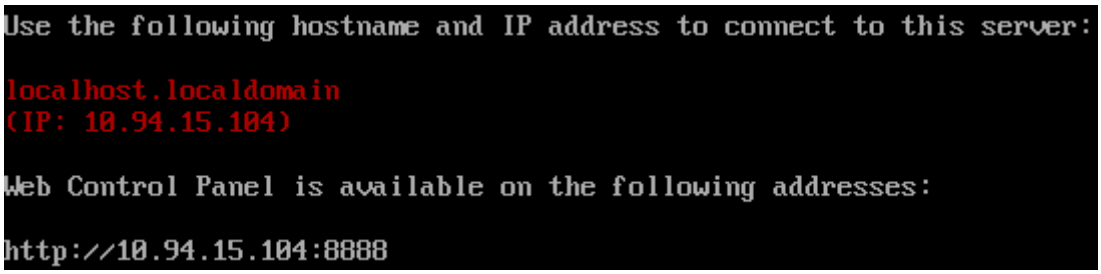
To install Acronis Storage, do the following:

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**.



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 a superadmin account of the management panel, confirm it in the corresponding field, and memorize it.
8. Click **Done** and **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 at which you can log in to the Acronis Storage management panel. For example:



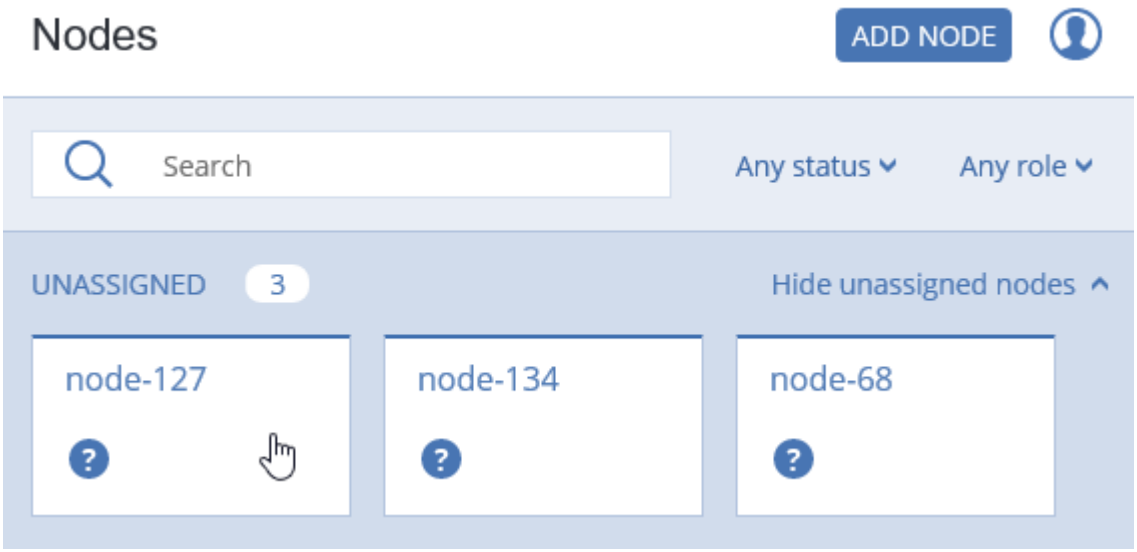
Note: If prompted, add the security certificate to browser's exceptions.

CHAPTER 3

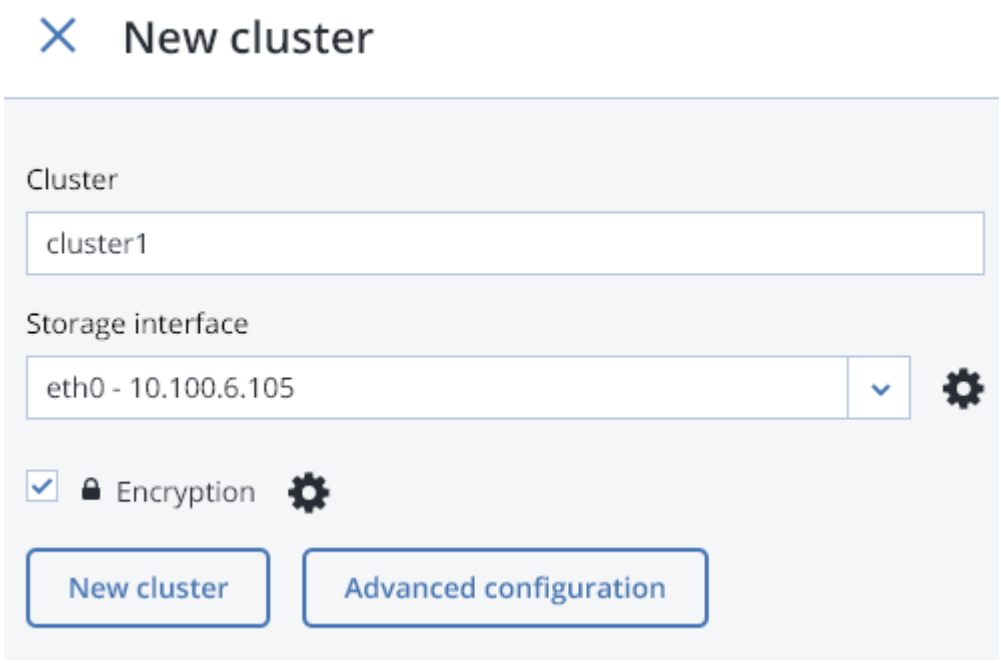
Creating the Acronis Storage Cluster

To create the Acronis Storage cluster, do the following:

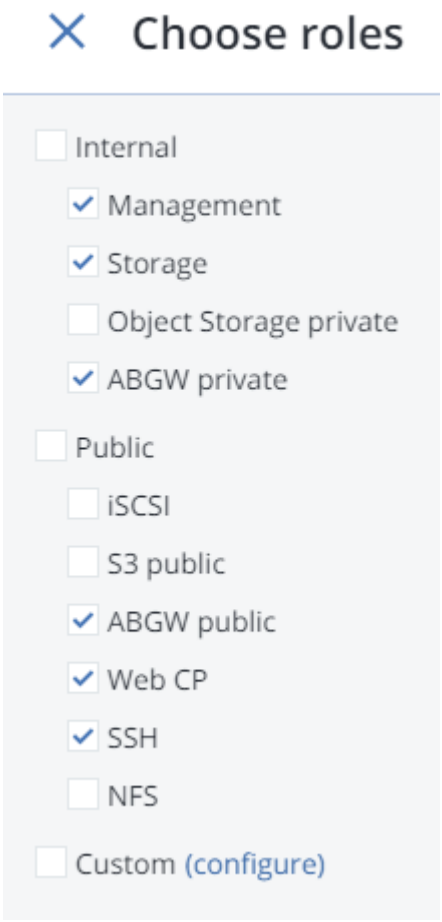
1. In the management panel, open the **NODES** screen and click the node in the **UNASSIGNED** list.



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 ("-").



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**.



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 **NODES** screen.

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 Acronis Storage Gateway* on page 21.

You can use Acronis Backup Gateway to keep Acronis Backup Cloud and Acronis Backup Advanced data on the following storage backends:

- Acronis Storage clusters,
- NFS shares,
- public clouds, including a number of S3 solutions as well as Microsoft Azure and OpenStack Swift.

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, redun-

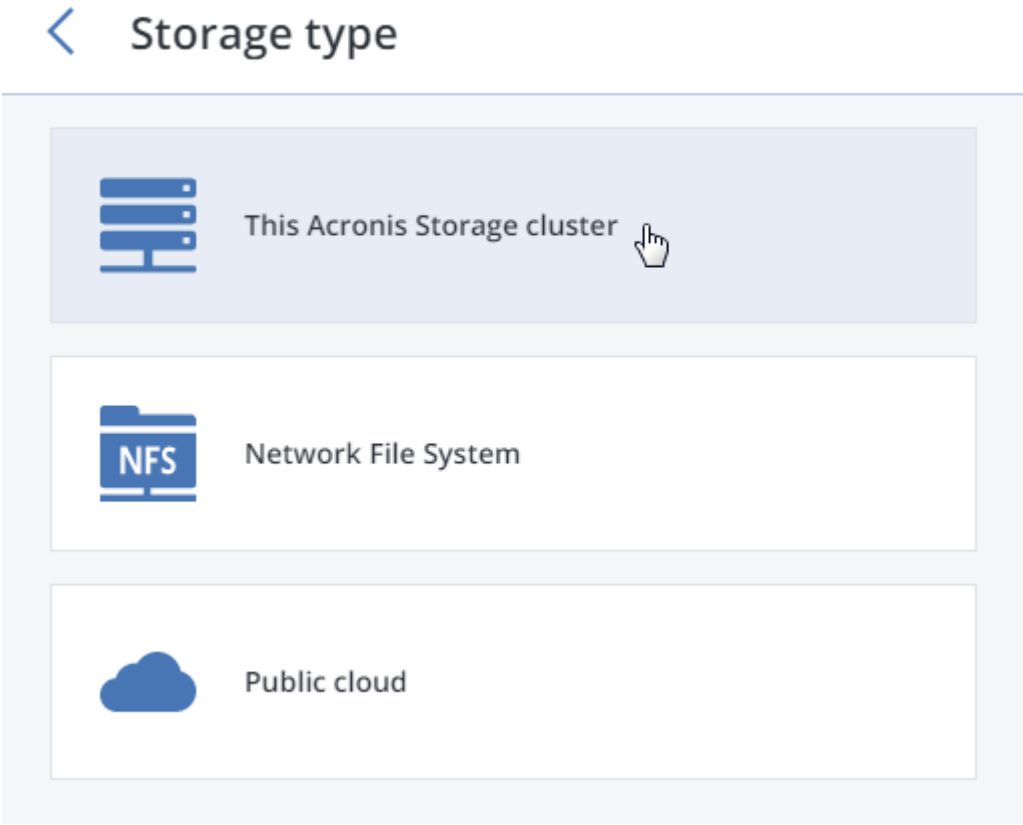
dancy has to be provided by said external storage. Acronis Backup Gateway does not provide data redundancy or perform data deduplication itself.

4.1 Connecting to the Acronis Storage Cluster via Acronis Backup Gateway

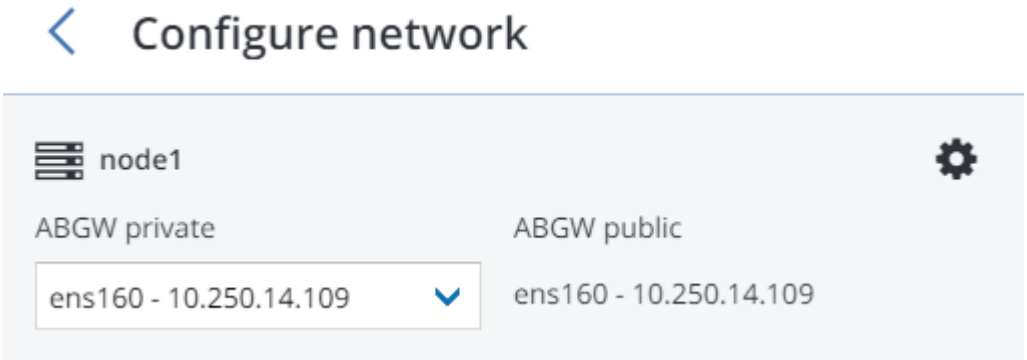
Before you proceed, make sure that the Acronis Storage cluster has enough space for backups.

To connect Acronis Backup Cloud or Acronis Backup Advanced to the local Acronis Storage cluster via Acronis Backup Gateway, do the following:

1. Make sure that the Acronis Backup Gateway network is configured on each node that will run the gateway service.
2. On the **SERVICES** > **Acronis Backup Gateway** > **Nodes** screen, select the checkbox next to the only node in the cluster.
3. Click **Create Gateway** then **This Acronis Storage cluster**.

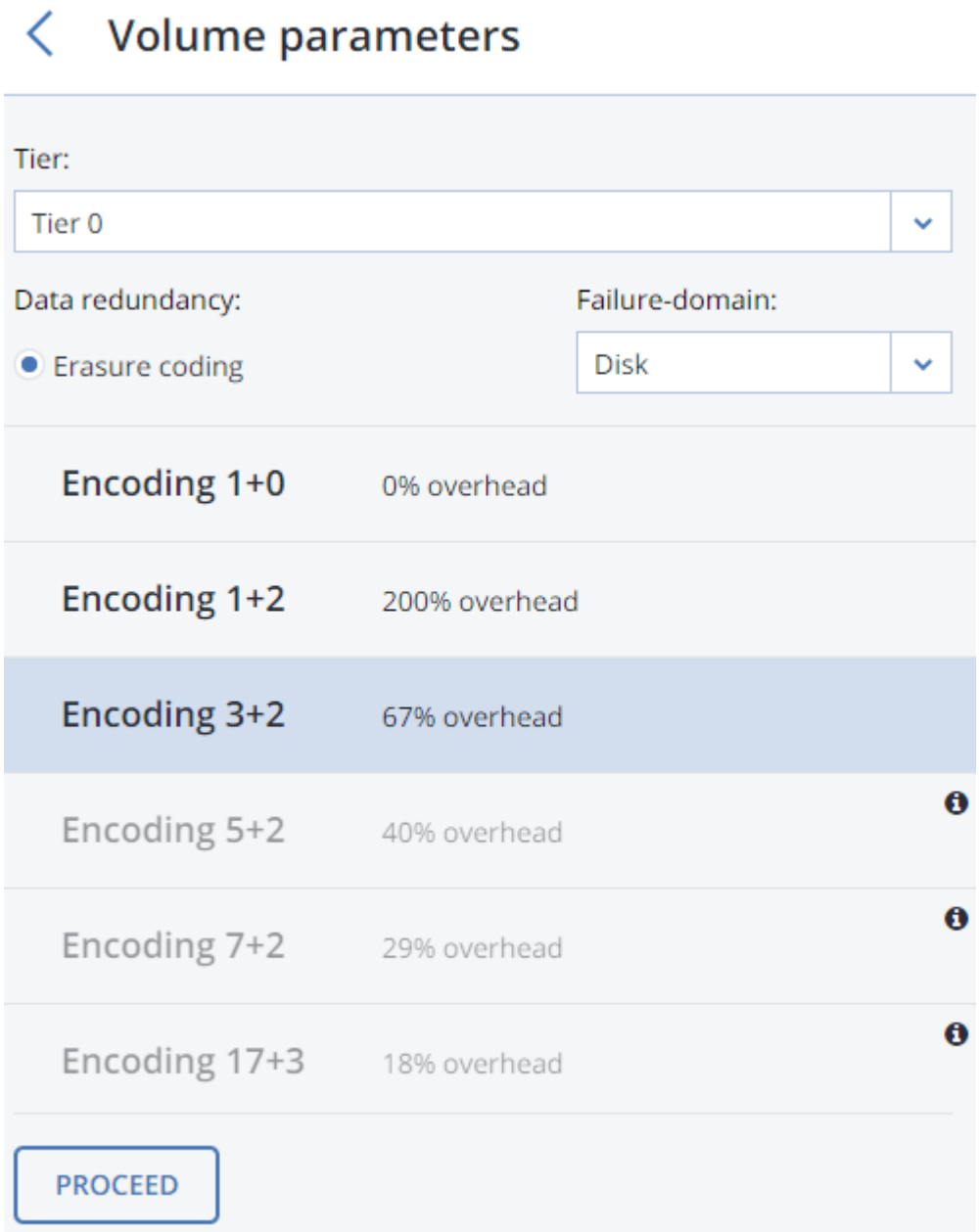


4. Select the network interface on the node to which the Acronis Backup Gateway network role is assigned. The gateway service will listen on the IP address assigned to this interface.



5. Click **NEXT**.

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

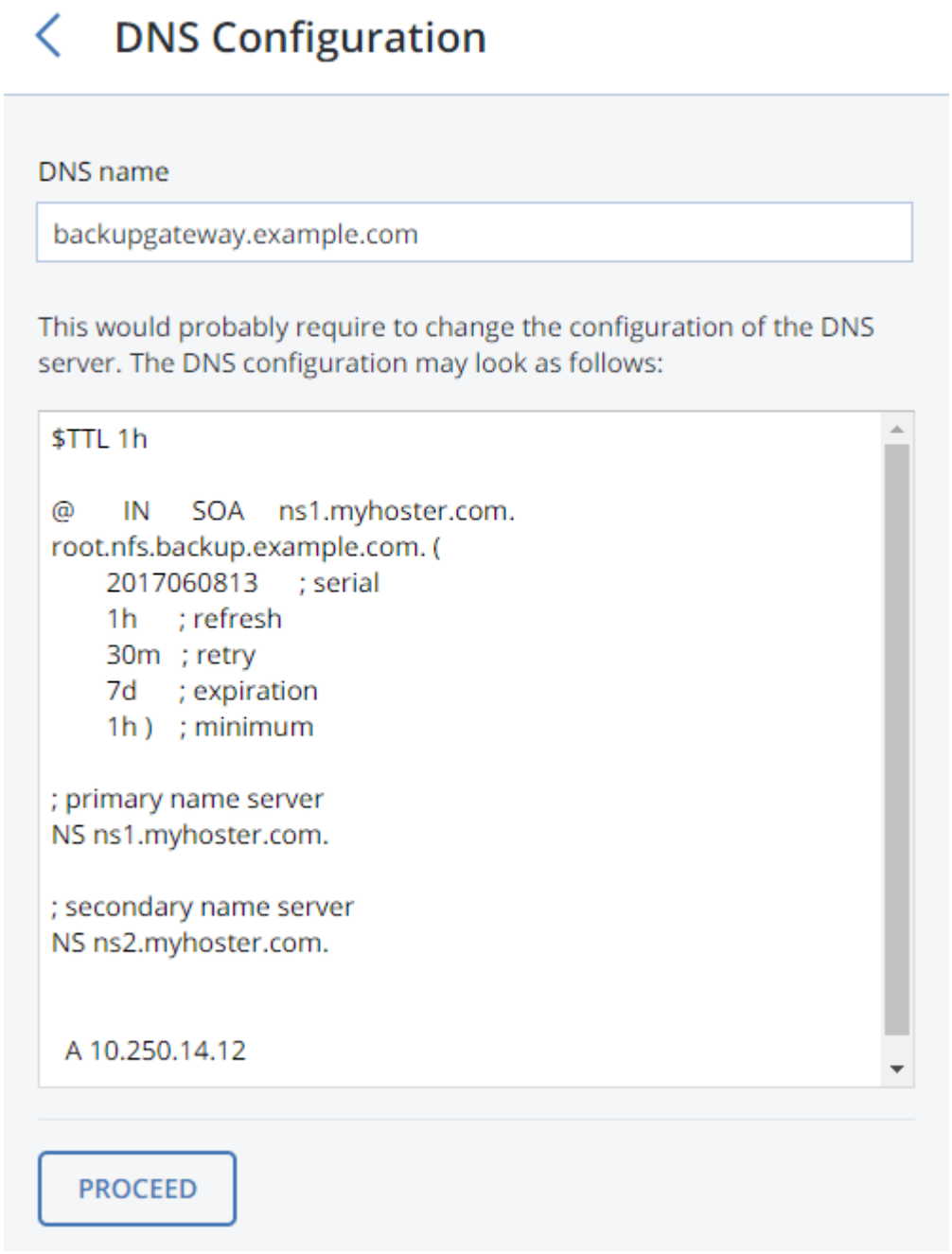


Note:

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.

7. Click **NEXT**.

8. 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 backed-up data.



Important:

1. Configure your DNS server according to the example suggested in the management panel.
2. Each time you add or remove a node to or from the Acronis Backup Gateway cluster, adjust the DNS settings accordingly.

9. Click **NEXT**.
10. Depending on the Acronis product you use, specify the following on the **Registration** tab:
    - 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 the Acronis Backup Cloud or Acronis Backup Advanced administrator account.
11. 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.

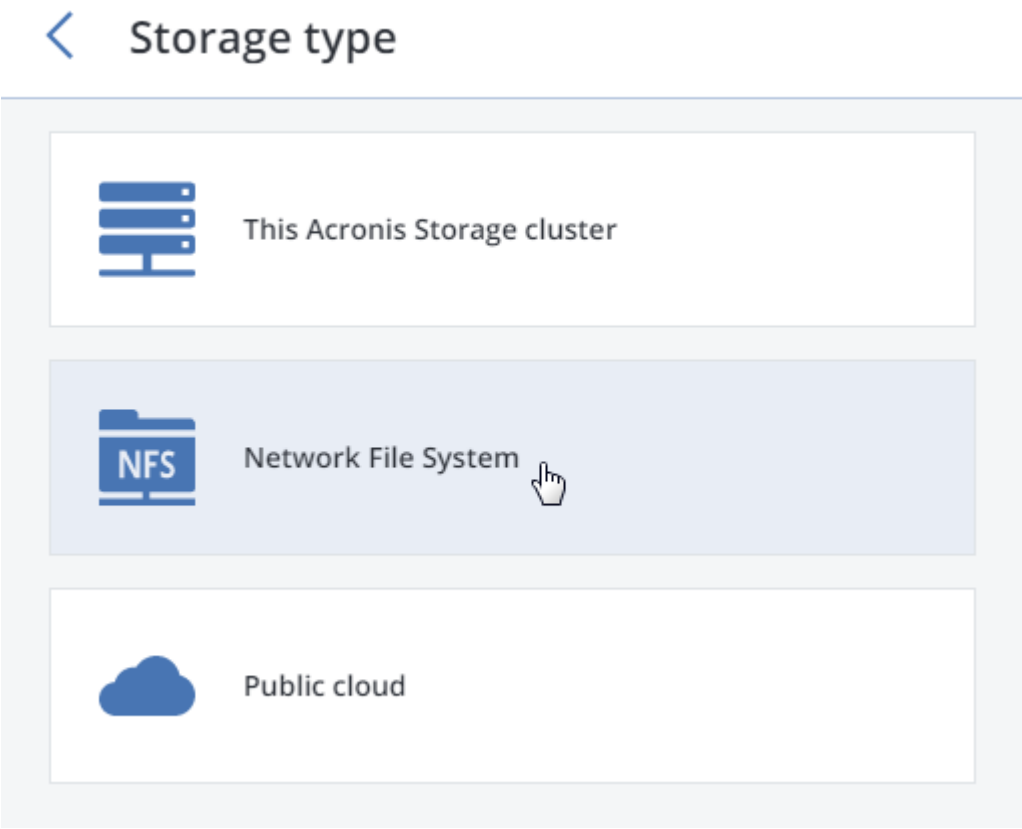
Before you proceed, make sure that:

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.

4.2. Connecting to External NFS Shares via Acronis Backup Gateway

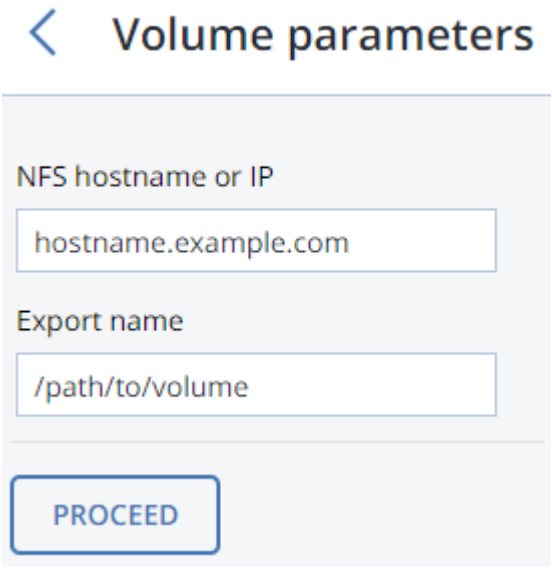
To connect Acronis Backup Cloud or Acronis Backup Advanced to an external NFS share via Acronis Backup Gateway, do the following:

1. Make sure that the Acronis Backup Gateway network role is assigned on the node that will run the gateway service.
2. On the **SERVICES** > **Acronis Backup Gateway** > **Nodes** screen, select the checkbox next to the only node in the cluster.
3. Click **Create Gateway** and **Network File System**.



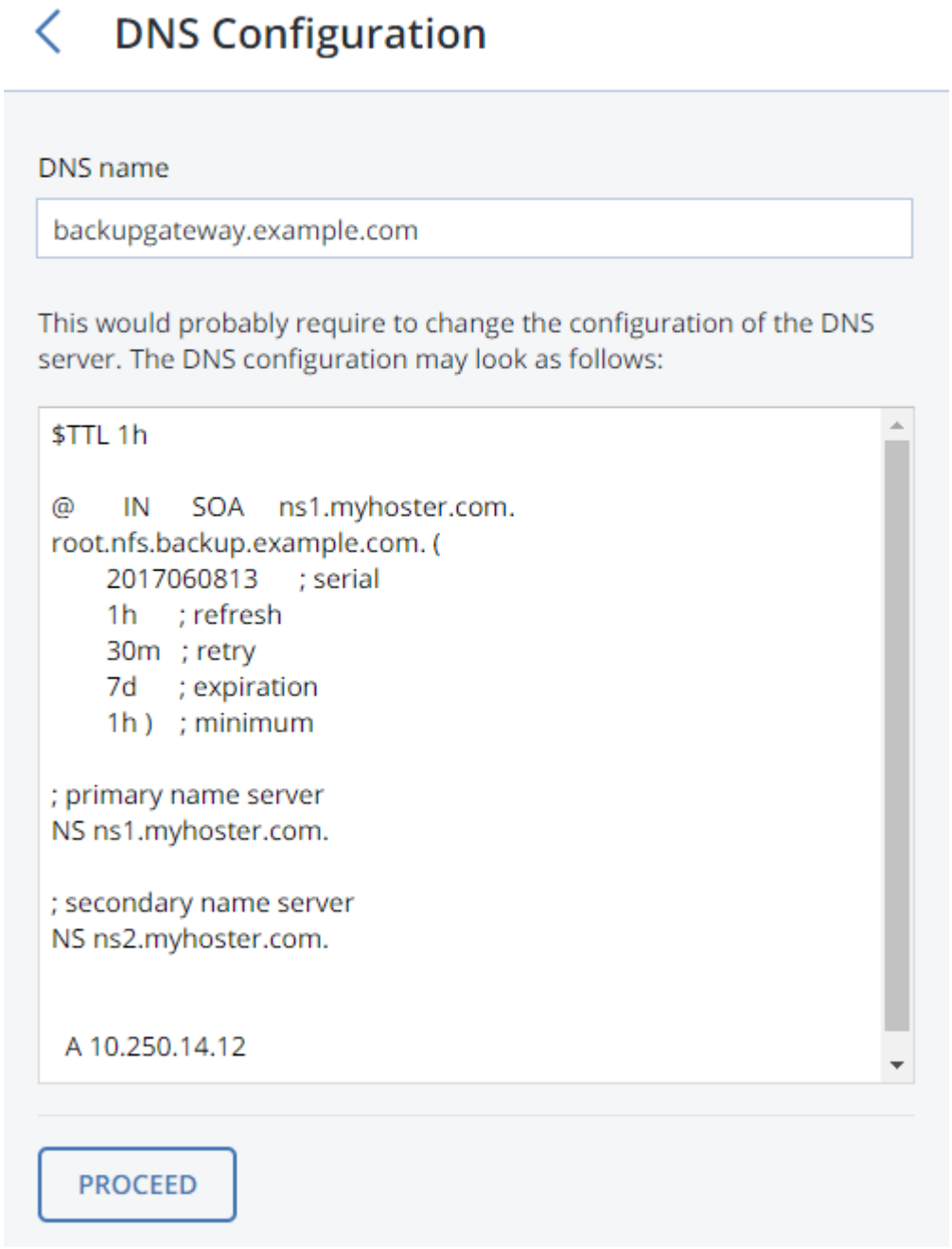
4. Make sure the network interface with the assigned Acronis Backup Gateway network role is selected. The gateway service will listen on the IP address assigned to this interface. Click **NEXT**.

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 backed-up data.

4.2. Connecting to External NFS Shares via Acronis Backup Gateway



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.

7. Click **NEXT**.
8. Depending on the Acronis product you use, specify the following on the **Registration** tab:
   - 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 the Acronis Backup Cloud or Acronis Backup Advanced administrator account.
9. 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, IIJ, Cleversafe, Microsoft Azure, Swift object storage, Softlayer (Swift) 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.

Important:

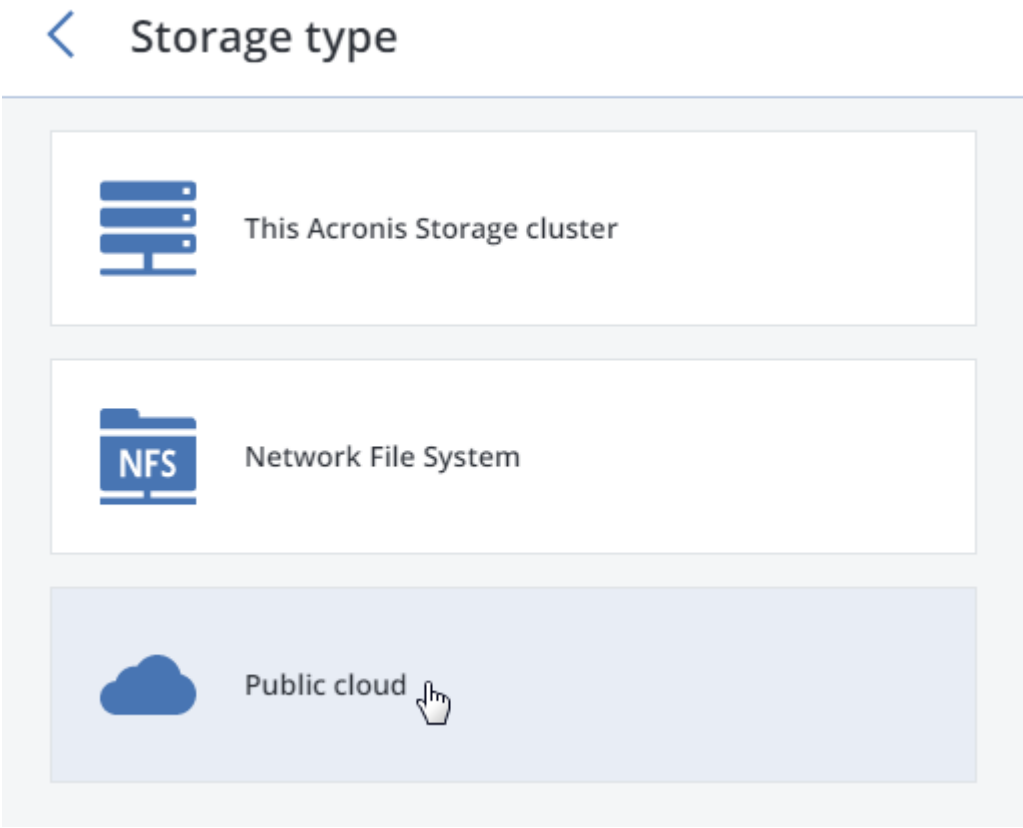
1. When working with public clouds, Acronis Backup Gateway uses the local storage as the staging area as well as to keep service information. It means that the data to be uploaded to a public cloud is first stored locally and only then sent to the destination. For this reason, it is vital that the local 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. You must update Acronis Backup Agents to version 4492 (Windows/Mac) or 4470 (Linux). Otherwise

agents' attempts to place backups in the new storage backend will result in "Backup failed" errors.

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

To connect your Acronis backup software to a public cloud folder via Acronis Backup Gateway, do the following:

1. On the **SERVICES** > **Acronis Backup Gateway** > **Nodes** screen, select the checkbox next to the only node in the cluster.
2. Click **Create Gateway** then **Public Cloud**.



3. Make sure the network interface with the assigned Acronis Backup Gateway network role is selected. The gateway service will listen on the IP address assigned to this interface. Click **NEXT**.

4. On the **Public cloud parameters** tab, do the following:
   4.1. Select a public cloud provider. If your provider is S3-compatible but not in the list, try **AuthV2 compatible**.
   4.2. Depending on the provider, specify **Region**, **Authentication (keystone) URL**, or **Endpoint URL**.
   4.3. In case of Swift object storage, specify the authentication protocol version and attributes required by it.
   4.4. Specify user credentials.
   4.5. Specify the folder (bucket, container) to store backups in. The folder must be writeable.
5. Click **NEXT**.
6. Depending on the Acronis product you use, specify the following on the **Registration** tab:
   - 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 the Acronis Backup Cloud or Acronis Backup Advanced administrator account.
7. Click **DONE**.

CHAPTER 5

Migrating Backups from Acronis Storage Gateway

Acronis Backup Gateway allows you to migrate backups from Acronis Storage Gateway 1.7 to a storage backend of your choice: your Acronis Storage cluster, external NFS, or public cloud.

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

The migration procedure can be described as follows:

1. Root credentials for SSH access to the Acronis Storage Gateway (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 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 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 as follows:

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

     ```
     # systemctl stop firewalld
     ```

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

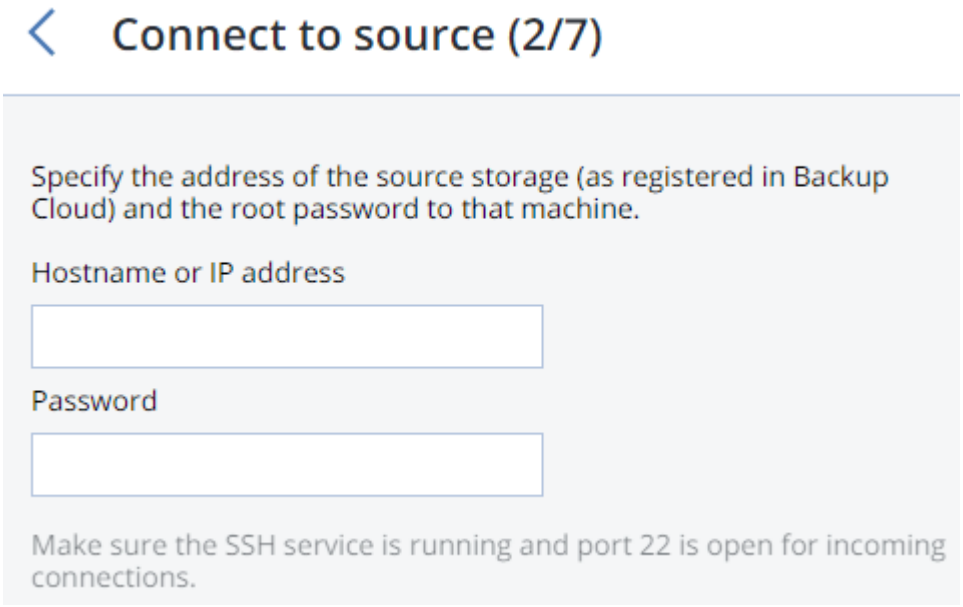
     1.1. Find out the zone where port 44445 is open:

     ```
     # 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 WebCP of the ABGW node, proceed to **SERVICES** > **Acronis Backup Gateway** > **Nodes**, select the checkbox next to the only node in the cluster, and click **Migrate**.
3. Select the source storage version and click **NEXT**.
4. Specify the connection details for the source storage and click **NEXT**.

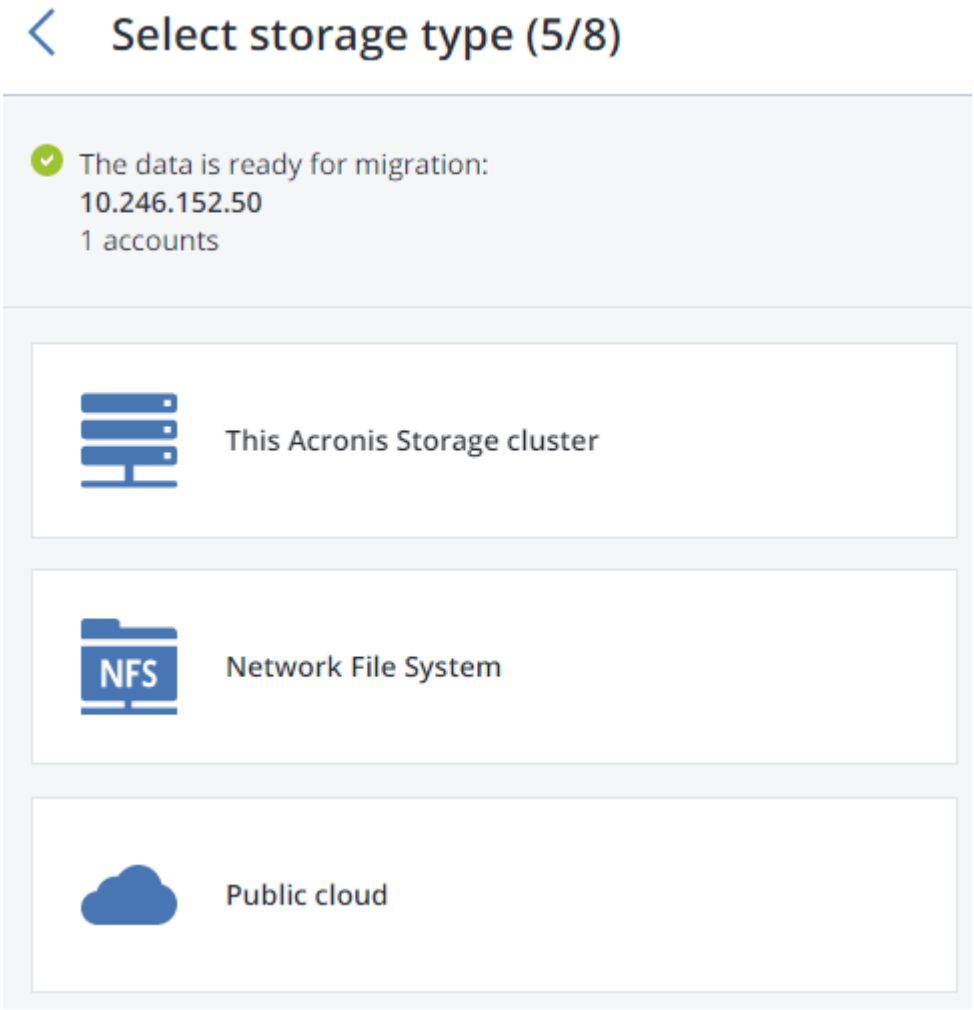


5. Provide the credentials for the cloud management portal of the Acronis Backup Cloud installation that the source storage is registered in and click **NEXT**.
6. If the source storage is registered in Acronis Backup Cloud under an IP address, you will see the DNS configuration screen. On it, click **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.



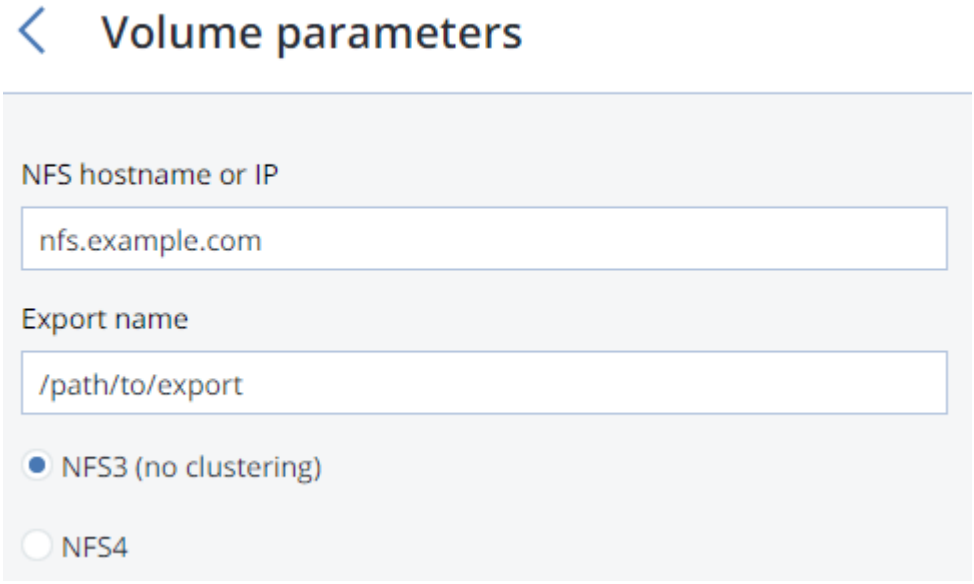
8. Make sure a network interface with the **ABGW private** role is selected in the drop-down list. The corresponding interfaces with the **ABGW public** role will be selected automatically.

   Note: If necessary, click the cogwheel icon and assign Acronis Backup Gateway roles on the **Network Configuration** screen.

9. Click **NEXT**.

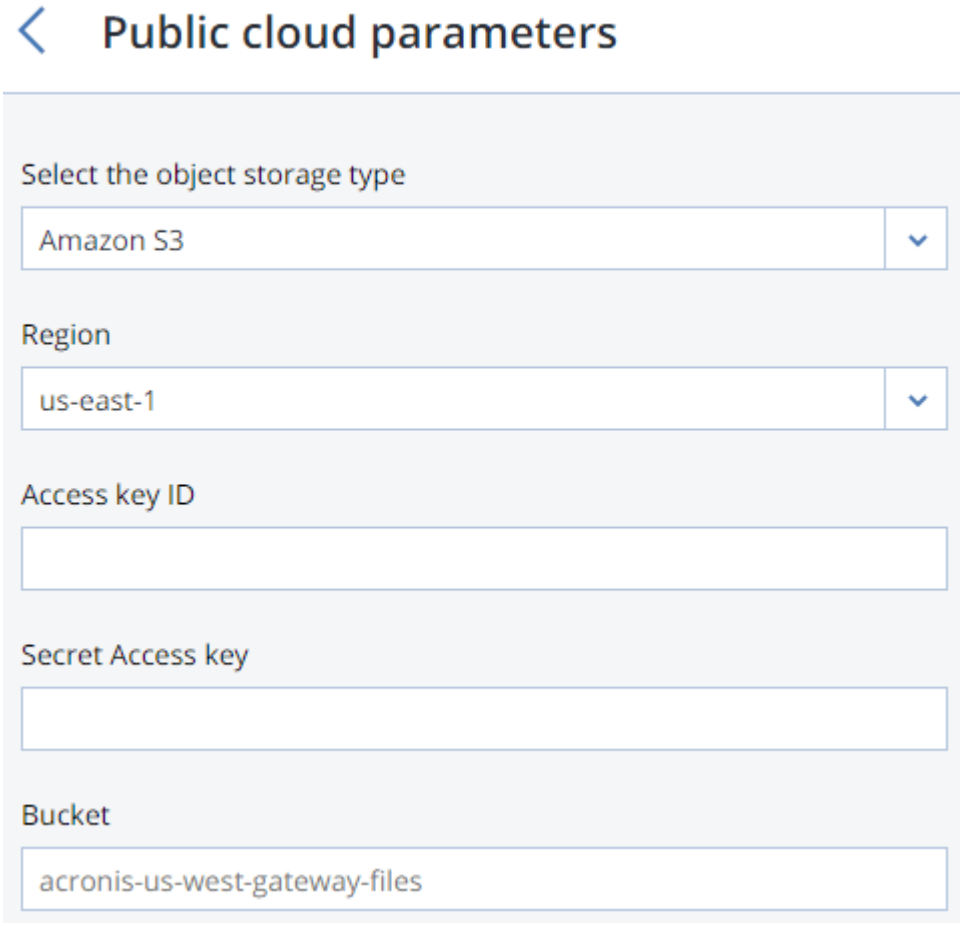
10. Depending on the destination storage type you selected, configure the backup storage backend:

    - For an Acronis 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.



- 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 4492 (Windows/Mac) or 4470 (Linux). Otherwise agents' attempts to place backups in the new storage backend will result in "Backup failed" errors.



11. Click **NEXT**.
12. On the **Finalize migration** panel, click **START MIGRATION**.

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

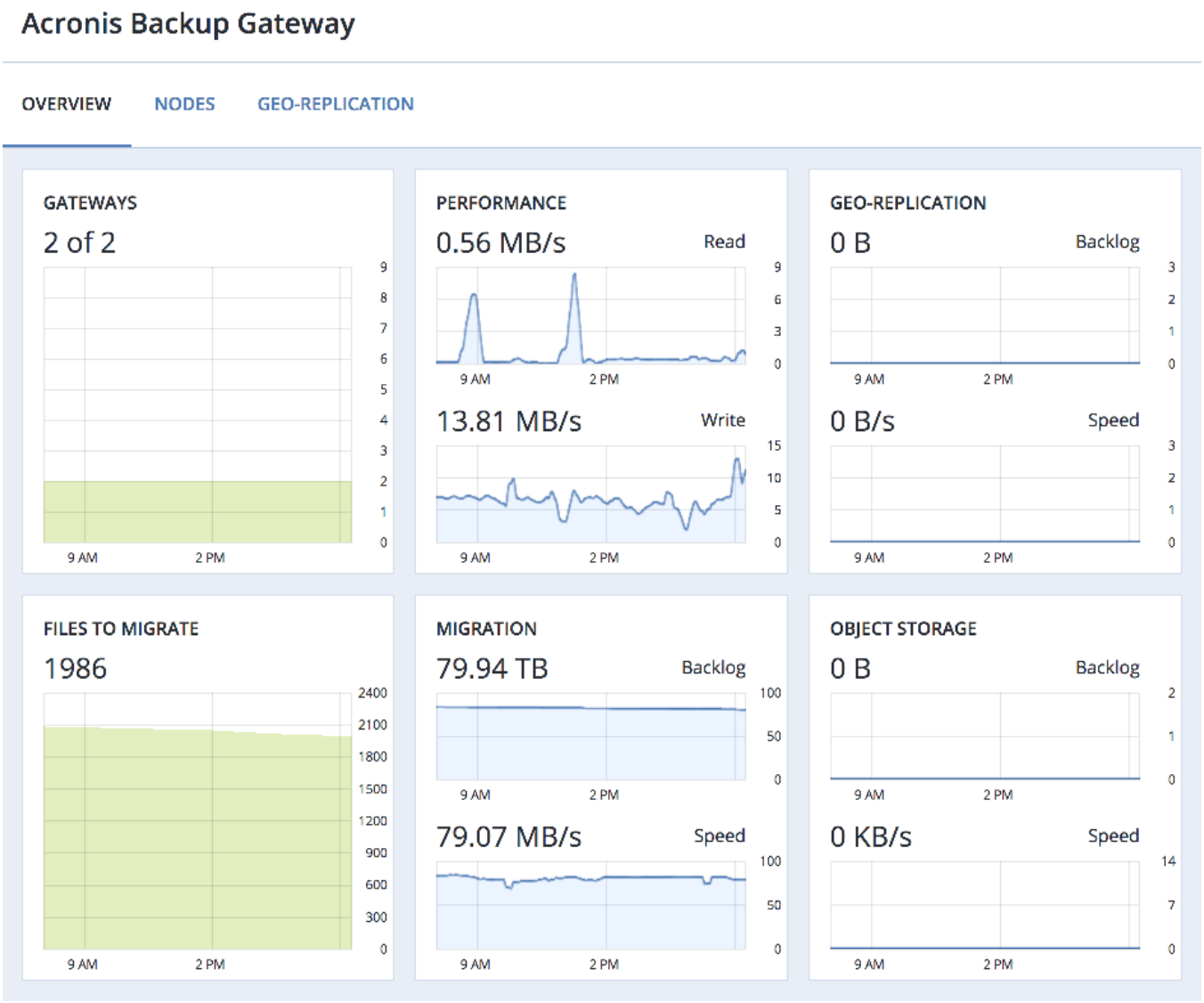
CHAPTER 6

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
GATEWAYS
2 of 2
9 AM
2 PM
PERFORMANCE
0.56 MB/s
Read
13.81 MB/s
Write
GEO-REPLICATION
0 B
Backlog
0 B/s
Speed
FILES TO MIGRATE
1986
MIGRATION
79.94 TB
Backlog
79.07 MB/s
Speed
OBJECT STORAGE
0 B
Backlog
0 KB/s
Speed

CHAPTER 7

Releasing Nodes from Acronis Backup Gateway

An 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, you need to delete the Acronis Backup Gateway by releasing all its nodes and create a new one.

> **Note:** If you delete the Acronis Backup Gateway, your Acronis backup software will lose access to the specified storage backend.

To release one or more nodes from the Acronis Backup Gateway, select them on the **SERVICES** > **Acronis Backup Gateway** > **NODES** screen and click **Release**. The Acronis Backup Gateway will remain operational until there is at least one node in it.

Releasing the last node is different as it deletes the Acronis Backup Gateway and unregisteres it from your Acronis backup software, which loses access to the storage backend.

Do the following to release the last node:

1. On the **SERVICES** > **Acronis Backup Gateway** > **NODES** screen, select the last node and click **Release**.
2. On the **Unregister Acronis Backup Gateway** panel, choose one of the following:
   2.1. **Graceful release** (recommended, see note below). Releases the last node, deletes the Acronis Backup Gateway and unregisters it from your Acronis backup software.
   2.2. **Force release**. Releases the last 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.

3. Specify the credentials of your administrator account in Acronis Backup Cloud or Acronis Backup Advanced and click **NEXT**. In case the release is forced, simply click **NEXT**.