

Acronis

Acronis Storage 2.4

Administrator's 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 Acronis Storage	1
2. Managing Acronis Storage	2
2.1 Configuring Node Network Interfaces	2
2.1.1 Setting Up Network Bonding	7
2.1.2 Setting Up VLAN Interfaces	10
2.2 Creating the Acronis Storage Cluster	11
2.2.1 Creating the Cluster on the First Node	12
2.2.2 Adding Nodes to Cluster	14
2.2.3 Assigning Disk Roles Manually	16
2.3 Releasing Nodes from Cluster	19
2.4 Removing Nodes from the Unassigned List	20
2.5 Managing Tier Encryption	21
2.6 Managing Acronis Storage Users	22
2.6.1 Creating User Accounts	22
2.6.2 Managing User Accounts	24
2.6.3 Adding LDAP or Active Directory Users	25
2.7 Managing Acronis Storage Updates	28
2.8 Allowing root Access to Cluster Nodes Over SSH	29
2.9 Backing Up and Restoring Management Database	30
2.9.1 Restoring Management Database from Backup	31
2.10 Enabling Management Panel High Availability	32
2.11 Accessing the Management Panel via SSL	35
2.12 Managing Acronis Storage Licenses	36
2.12.1 Installing License Keys	36

2.12.2	Installing SPLA Licenses	38
2.13	Connecting Remote iSCSI Devices to Storage Cluster Nodes	39
2.13.1	Assigning Disk Roles To Remote iSCSI Devices	40
3.	Monitoring Acronis Storage Clusters	41
3.1	Monitoring Cluster Status	41
3.2	Monitoring Cluster Storage Space	41
3.2.1	Physical Space Chart	42
3.2.2	Logical Space Chart	42
3.2.2.1	Understanding Logical Space	43
3.2.3	Monitoring Chunk Status and Replication	43
3.2.4	Monitoring Cluster Services	44
3.2.5	Monitoring Cluster I/O Activity	45
3.3	Monitoring Acronis Cluster Objects via SNMP	46
3.3.1	Enabling SNMP Access	47
3.3.2	Accessing Acronis Objects via SNMP	48
3.3.2.1	Listening to SNMP Traps	49
3.3.3	Monitoring Clusters with Zabbix	49
3.3.4	Description of Cluster Objects and Traps	53
4.	Monitoring Acronis Storage Nodes	56
4.1	Node Statuses	56
4.2	Monitoring Node Performance	56
4.2.1	Monitoring Node Disks	58
4.2.1.1	Monitoring the S.M.A.R.T. Status of Node Disks	59
4.3	Monitoring Node Network	59
5.	Viewing Acronis Storage Alerts, Audit Log, and Sending E-mail Notifications	60
5.1	Viewing Alerts	60
5.2	Viewing Audit Log	61
5.3	Sending E-mail Notifications	62
6.	Exporting Acronis Storage Cluster Data	65
6.1	Exporting Data via iSCSI	65
6.1.1	Creating Acronis Storage iSCSI Targets	66
6.1.1.1	Performance Tips	68
6.1.2	Listing, Stopping, and Deleting Acronis Storage iSCSI Targets	68

6.1.3	Configuring Acronis Storage iSCSI Targets	68
6.1.3.1	Listing LUNs	70
6.1.3.2	Adding LUNs	70
6.1.3.3	Configuring LUNs	72
6.1.3.4	Deleting LUNs	72
6.1.4	Managing iSCSI Users	72
6.1.4.1	Creating CHAP Accounts for Acronis Storage iSCSI Targets	72
6.1.4.2	Creating Acronis Storage iSCSI Targets Bound to CHAP Accounts	73
6.1.4.3	Changing CHAP Account Passwords	74
6.2	Exporting Data via S3	75
6.2.1	Object Storage Infrastructure Overview	76
6.2.2	Planning the S3 Cluster	77
6.2.3	Sample Object Storage	78
6.2.4	Creating the S3 Cluster	80
6.2.5	Managing Object Storage Users	84
6.2.5.1	Adding S3 users	85
6.2.5.2	Managing S3 Access Key Pairs	86
6.2.6	Managing Object Storage Buckets	88
6.2.6.1	Listing Bucket Contents	88
6.2.6.2	Managing Acronis Notary in Buckets	89
6.2.7	Best Practices for Using S3 in Acronis Storage	90
6.2.7.1	Bucket and Key Naming Policies	90
6.2.7.2	Improving Performance of PUT Operations	91
6.2.8	Replicating Data Between Geographically Distributed Datacenters with S3 Clusters	91
6.2.9	Monitoring S3 Access Points	93
6.2.10	Releasing Nodes from S3 Clusters	93
6.2.11	Supported Amazon S3 Features	94
6.2.11.1	Supported Amazon S3 REST Operations	94
6.2.11.2	Supported Amazon Request Headers	96
6.2.11.3	Supported Amazon Response Headers	96
6.2.11.4	Supported Amazon Error Response Headers	97
6.2.11.5	Supported Authentication Scheme and Methods	98
6.3	Exporting Data via NFS	98
6.3.1	Setting Up an NFS Cluster	99
6.3.2	Creating NFS Shares	99

6.3.3	Creating NFS Exports	100
6.3.4	Setting Up User Authentication and Authorization	101
6.3.4.1	Authenticating NFS Share Users with Kerberos	101
6.3.4.2	Authorizing NFS Export Users with LDAP	102
6.4	Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway	102
6.4.1	Understanding the Infrastructure	103
6.4.2	Connecting to the Acronis Storage Cluster via Acronis Backup Gateway	104
6.4.3	Connecting to External NFS Shares via Acronis Backup Gateway	109
6.4.4	Connecting to Public Cloud Storage via Acronis Backup Gateway	113
6.4.5	Migrating Backups from Acronis Storage Gateways	116
6.4.6	Monitoring the Acronis Backup Gateway Cluster	121
6.4.7	Releasing Nodes from the Acronis Backup Gateway Cluster	122

CHAPTER 1

Introduction

To support the growing demand for both high performance and high data availability, modern data centers need a fast, flexible storage solution. Existing solutions, however, are often difficult to manage and maintain, or not flexible enough (e.g., local RAID arrays), or too expensive (e.g., storage area networks).

Acronis Storage is designed to solve these issues. It can run on commodity hardware, so no significant infrastructure investments are needed. It is also easy to set up and grow on demand.

1.1 About Acronis Storage

Acronis Storage is a software-defined storage solution that allows you to quickly and easily transform low-cost commodity hardware and network equipment into protected enterprise-grade storage like storage area networks (SAN) or network-attached storage (NAS).

Acronis Storage is optimized for storing large amounts of data and provides data redundancy (replication and erasure coding), high availability, self-healing, and storage sharing.

In Acronis Storage, user data is stored on organized clusters of servers in the form of fixed-size chunks. These chunks are automatically replicated and distributed across available servers in the cluster to ensure high availability of user data.

Cluster storage space can be exported through access points like iSCSI, S3, NFS, or Acronis Backup Gateway.

CHAPTER 2

Managing Acronis Storage

To start managing Acronis Storage, log in to the management panel as admin (or superadmin) and make sure that storage nodes are shown on the **NODES** screen.

The first step to perform, before you can create the cluster, is to create the internal and public networks required by Acronis Storage. You can do that by configuring the network interfaces of all nodes. Having created the networks, you can proceed to creating Acronis Storage clusters.

2.1 Configuring Node Network Interfaces

As described in **Planning Network** in the *Acronis Storage Installation Guide*, Acronis Storage requires one internal network for node traffic and one public network for exporting the storage space. You need to create these networks by assigning correct network roles to network interfaces on each node.

Important: To be able to create a cluster, you will need to assign a storage role to a node's network interface.

To assign a network role to a network interface, do the following:

1. On the **NODES** screen, click the node to configure the network interface(s) of.

2.1. Configuring Node Network Interfaces

The screenshot shows the 'Nodes' management page. At the top, there is a search bar and filters for 'Any status' and 'Any role'. Below this, a section titled 'UNASSIGNED' shows a count of 4 nodes. A button 'Hide unassigned nodes' is visible. Four node cards are displayed: node-127, node-121, node-125, and node-134. Each card has a question mark icon, indicating they are not yet configured.

2. On the node overview screen, click **NETWORK**.

Nodes > node-125 **HEALTHY**





The screenshot shows the node overview for 'node-125', which is in a 'HEALTHY' state. The interface is divided into several sections:

- CPU CORES:** 20
- RAM:** 125.64 GB
- CPU USAGE:** 2.24 % (with a line graph showing usage over time from 1 PM to 10 PM)
- DISKS:** 37 hdd (34 unused), 1 ssd
- READ:** 0 MB (with a bar chart showing read activity)
- 0 Ops:** (with a bar chart showing operations)
- NETWORK:** This tab is selected and highlighted with a hand cursor. It shows two network interfaces: 10.90.100.118 (disabled, indicated by a grey dot) and 10.90.100.125 (enabled, indicated by a green checkmark). The total capacity is 10 GB.
- TX:** 15 B/s (with a line graph showing transmission activity)

3. Select a network interface and click **Configure**.

Nodes > node-125 > Network ADD NODE 

DISKS NETWORK

Name	Status ↓	IPs	Speed		 Details
ens6f0	 OK	10.90.100.125/24	10 Gb / 10 Gb	Mar	 Performance
eno2	 DISABLE...	10.90.100.118/24	0 b / 10 Gb		 Down
eno1	 DISABLE...		0 b / 10 Gb		 Configure
eno3	 DISABLE...		0 b / 10 Gb		 Delete
eno4	 DISABLE...		0 b / 10 Gb		 Create bonding

4. On the **Configure** screen, do one of the following:

- To obtain the IP address, DNS, and routing settings from the DHCP server, select **Automatically (DHCP)**.
- To obtain just the IP address from the DHCP server, select **Automatically (DHCP address only)**.
- To specify the IP address manually, select **Manual** and add the IP address.

Warning: Dynamic IP address allocation will cause network issues as soon as the IP addresses of cluster nodes will change. Configure static IP addresses from the start or as soon as possible.

2.1. Configuring Node Network Interfaces

× **Configure**

☒ Automatically (DHCP)
☐ Automatically (DHCP address only)
☐ Manual

10.211.55.44/24

+ Add

− Remove

Gateway

10.211.55.1

DNS Server

10.211.55.1

MTU

1500

Done

5. If necessary, set up a gateway and a DNS server.
6. If you have set a custom maximum transmission unit (MTU) on the network hardware, set the same value in the corresponding field.

Warning: Setting a custom MTU in management panel prior to configuring it on the network hardware will result in network failure on the node and require manual resetting. Setting an MTU that differs from the one configured on the network hardware may result in network outage or poor performance.

7. Click **Done** to return to the list of network interfaces, do not change the selection, and click **Choose role**.

8. On the **Choose roles** panel, select roles to assign to the network interface (for details, see **Network Interface Roles** in the *Acronis Storage Installation Guide*).

×

Choose roles

☒ Internal

- ☒ Management
- ☒ Storage
- ☒ Object Storage private
- ☒ ABGW private


☒ Public

- ☒ iSCSI
- ☒ S3 public
- ☒ ABGW public
- ☒ Web CP
- ☒ SSH
- ☒ NFS

☐ Custom [\(configure\)](#)



DONE

9. If you need to open specific ports on a network interface with public roles, do the following:
 - 9.1. Click **Configure**.

 **Configure custom role**

Here you can manage allowed ports for custom role.

	Name	Port
<input checked="" type="checkbox"/>	FTP cmd	<input type="text" value="21"/>
<input type="checkbox"/>	FTP data	20

 Add  Remove

9.2. On the **Configure custom role** panel, create custom roles: click **Add** and specify role names and ports. Custom roles can later be assigned to any network interface in a cluster.

To remove a custom role, make sure it is not assigned to any interface, select it, and click **Remove**.

9.3. Click **Done** to return to the **Choose roles** panel.

11. Select the required roles and click **Done** to assign them.

2.1.1 Setting Up Network Bonding



Bonding multiple network interfaces is optional but provides the following benefits:

- High network availability. If one of the interfaces fails, the traffic will be automatically routed through the working interface(s).
- Higher network performance. For example, two bonded Gigabit interfaces will deliver the throughput of about 1.7 Gbit/s or up to 200 MB/s. For a storage node, the required number of network interfaces to bond may depend on the number of disks. For example, an HDD can deliver data at speeds of up to 1


Gbps.

To create a bond, do the following:

1. On the **NODES** screen, click the node to bond the network interfaces on.
2. On the node overview screen, click **NETWORK**.
3. In the **NETWORK** list, check network interfaces to bond, and click **Create bonding** in the menu to the right.

DISKS		NETWORK	
<input type="checkbox"/>	Name	Status	
<input checked="" type="checkbox"/>	ens6f0		OK
<input checked="" type="checkbox"/>	eno2		OK

4. On the **Configure Bonding** panel, select the bonding type from the drop-down list. The balance-xor type is selected by default and recommended for both fault tolerance and good performance.

 **Configure Bonding**

Type


balance-xor


☒ Automatically (DHCP)

☐ Automatically (DHCP address only)

☐ Manual

There are no items to show in this view.

 Add

 Remove

Gateway

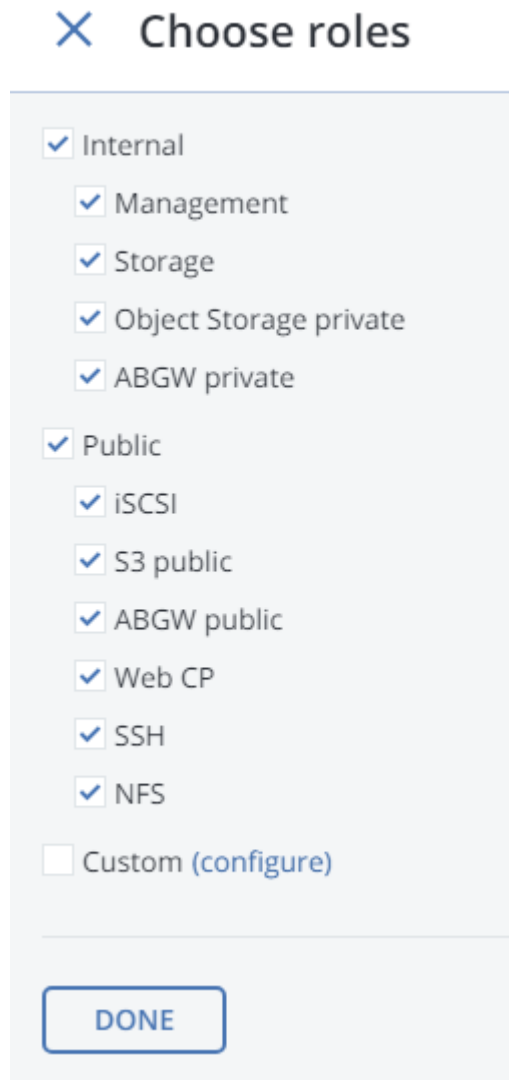
DNS Server

MTU

auto

PROCEED

- Set up network parameters as described in step 4 in *Configuring Node Network Interfaces* on page 2 and click **PROCEED**.
- On the **Choose roles** panel, select roles to assign to the bonding network interface (for details, see **Network Interface Roles** in the *Acronis Storage Installation Guide*).



The screenshot shows a modal window titled "Choose roles" with a blue 'X' icon in the top left corner. The window has a light gray background and contains a list of roles with checkboxes. The roles are grouped into two main sections: "Internal" and "Public". Under "Internal", there are five roles: "Management", "Storage", "Object Storage private", and "ABGW private", all of which are checked. Under "Public", there are seven roles: "iSCSI", "S3 public", "ABGW public", "Web CP", "SSH", and "NFS", all of which are checked. At the bottom of the list is an unchecked checkbox for "Custom (configure)". A blue "DONE" button is located at the bottom right of the dialog.

Choose roles

- ☒ Internal
 - ☒ Management
 - ☒ Storage
 - ☒ Object Storage private
 - ☒ ABGW private
- ☒ Public
 - ☒ iSCSI
 - ☒ S3 public
 - ☒ ABGW public
 - ☒ Web CP
 - ☒ SSH
 - ☒ NFS
- ☐ Custom (configure)

DONE

7. Click **Done**.

2.1.2 Setting Up VLAN Interfaces

To set up a VLAN network interface, do the following:

1. On the **NODES** screen, click the node on which to configure VLAN.
2. On the node overview screen, click **NETWORK**.
3. Select a network interface and click **Create VLAN**.
4. On the **Configure VLAN** panel, specify a number for VLAN, add an IP address, and, if necessary, set up a

2.2. Creating the Acronis Storage Cluster

gateway and a DNS server.

× **Configure VLAN**

VLAN #

☒ Automatically (DHCP)
☐ Automatically (DHCP address only)
☐ Manual

There are no items to show in this view.

+ Add − Remove

Gateway

DNS Server

MTU

Proceed

5. Click **Proceed** to create a VLAN interface.

2.2 Creating the Acronis Storage Cluster

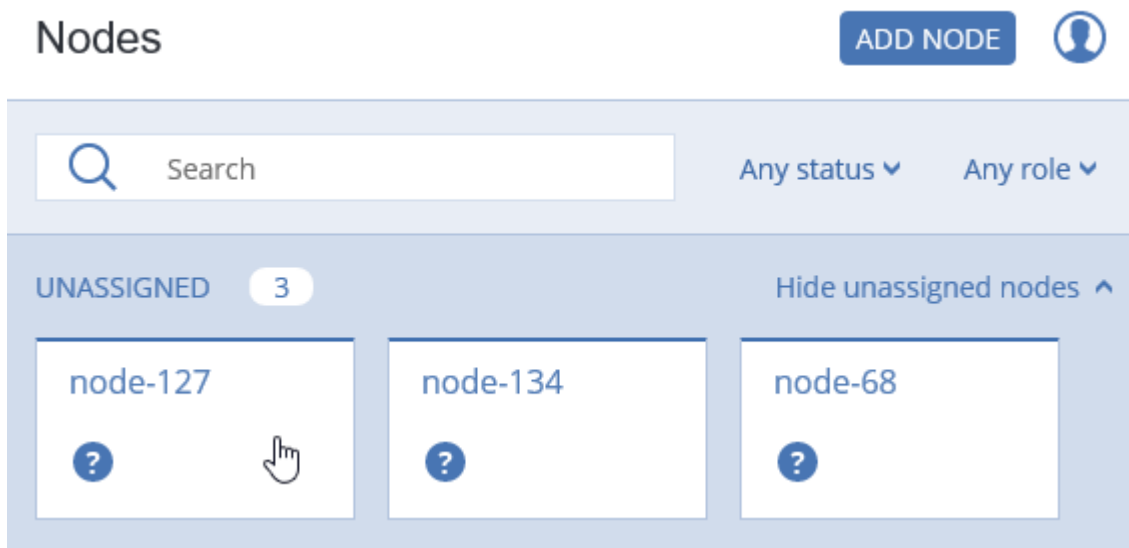
To create the Acronis Storage cluster means to create the cluster on one (first) node, then populate it with more nodes.

Important: To be able to create the cluster, you will need to assign a storage role to a node's network interface.

If you have remote iSCSI devices you wish to connect to cluster nodes, you can configure them prior to cluster creation as described in *Connecting Remote iSCSI Devices to Storage Cluster Nodes* on page 39.


2.2.1 Creating the Cluster on the First Node

1. Open the **NODES** screen and click a node in the **UNASSIGNED** list.



2. On the node overview screen, click **Create cluster**.
3. In the **Cluster** field, type a name for the cluster. The name may only contain Latin letters (a-z, A-Z), numbers (0-9), underscores ("_") and dashes ("-").

2.2. Creating the Acronis Storage Cluster

 **New cluster**


Cluster



cluster1

Storage interface

eth0 - 10.100.6.105

▼



☒  Encryption 

New cluster

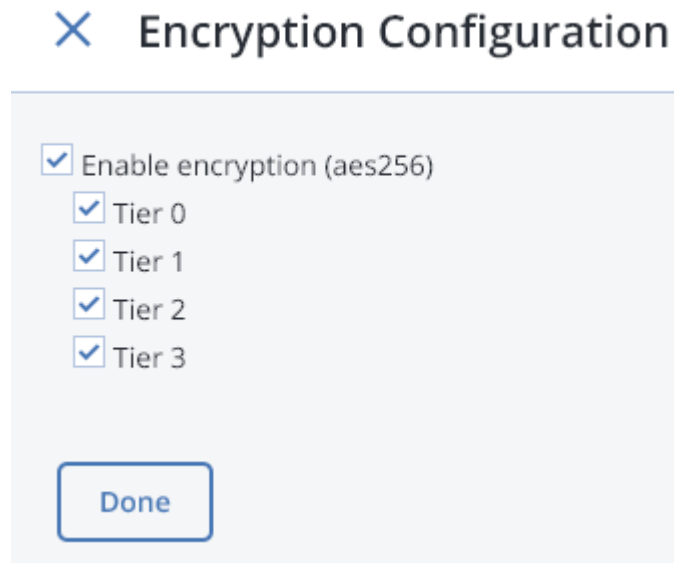
Advanced configuration

4. Make sure a configured network interface with a storage role is selected from the **Storage interface** drop-down list.

Note: If the network was not previously configured, click the cogwheel icon and, on the **Network Configuration** screen, configure a storage role for a network interface.

5. If required, enable data encryption. To do this, check the **Encryption** box (see [Managing Tier Encryption](#) on page 21) and proceed to create the cluster. Encryption will be enabled for all tiers by default.

To enable encryption for particular tiers, click the cogwheel icon to open the **Encryption Configuration** panel, select tiers to encrypt, and click **Done**.



Note: You can later disable encryption for new chunk services (CS) on the **SETTINGS > Advanced settings** panel.

6. Click **New cluster** to have Acronis Storage assign the roles to disks automatically. Alternatively, click **Advanced configuration** to assign the roles to each drive manually and tweak other settings.

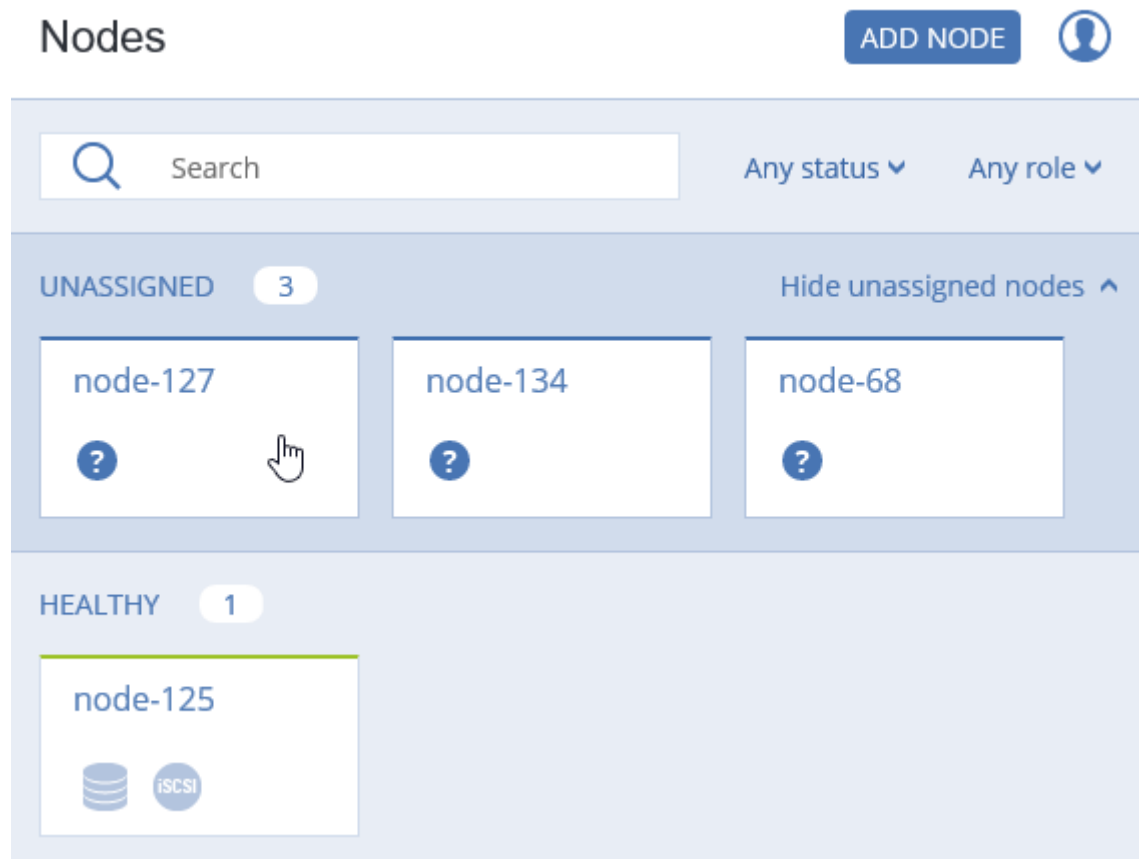
You can monitor cluster creation progress in the **HEALTHY** list of the **NODES** screen. The creation might take some time depending on the number of disks to be configured. Once the automatic configuration is complete, the cluster is created.

2.2.2 Adding Nodes to Cluster

To add an unassigned node to a cluster, do the following:


1. On the **NODES** screen, click an unassigned node.

2.2. Creating the Acronis Storage Cluster





2. On the node overview screen, click **Join cluster**.
3. Make sure a configured network interface with a storage role is selected from the **Storage interface** drop-down list.

Note: If the network was not previously configured, click the cogwheel icon and, on the **Network Configuration** screen, configure a storage role for a network interface.

 **Join cluster**

Storage interface

eno2 - 10.90.100.140 



Join cluster


Advanced configuration

5. Click **Join cluster** to have Acronis Storage assign the roles to disks automatically and add the node to the current cluster. Alternatively, click **Advanced configuration** to assign the roles to each drive manually (see *Assigning Disk Roles Manually* on page 16).

2.2.3 Assigning Disk Roles Manually

If you clicked **Advanced configuration** while creating a cluster or adding nodes to it, you will be taken to the list of drives on the node where you can manually assign roles to these drives. Do the following:

1. On the **Join cluster** or **New cluster** panel, select a drive or check multiple drives in the list and click **Configure**.
2. On the **Choose role** screen, select one of the following roles for the disk:

 **Choose role**

☒ Storage


☐ Metadata

☐ Cache


☐ Metadata + Cache

☐ Unassigned

Caching and checksumming

Enable checksumming 

Tier

Tier 0 (Encrypted) 

Done

Cancel

2.2. Creating the Acronis Storage Cluster

- **Storage.** Use the disk to store chunks and run a chunk service on the node. From the **Caching and checksumming** drop-down list, select one of the following:
 - **Use SSD for caching and checksumming.** Available and recommended only for nodes with SSDs.
 - **Enable checksumming** (default). Recommended for cold data as it provides better reliability.
 - **Disable checksumming.** Recommended for hot data as it provides better performance.

Data caching improves cluster performance by placing the frequently accessed data on an SSD.

Data checksumming generates checksums each time some data in the cluster is modified. When this data is then read, a new checksum is computed and compared with the old checksum. If the two are not identical, a read operation is performed again, thus providing better data reliability and integrity.

If a node has an SSD, it will be automatically configured to keep checksums when you add a node to a cluster. This is the recommended setup. However, if a node does not have an SSD drive, checksums will be stored on a rotational disk by default. It means that this disk will have to handle double the I/O, because for each data read/write operation there will be a corresponding checksum read/write operation. For this reason, you may want to disable checksumming on nodes without SSDs to gain performance at the expense of checksums. This can be especially useful for hot data storage.

Note: To add an SSD to a node that is already in the cluster (or replace a broken SSD), you will need to release the node from the cluster, attach the SSD, choose to join the node to the cluster again, and, while doing so, select **Use SSD for caching and checksumming** for each disk with the role **Storage**.

With this role, you can also select a tier from the **Tier** drop-down list. To make better use of data redundancy, do not assign all the disks on a node to the same tier. Instead, make sure that each tier is evenly distributed across the cluster with only one disk per node assigned to it. For more information, see **Understanding Storage Tiers** in the *Acronis Storage Installation Guide*.

Note: If the disk contains old data that was not placed there by Acronis Storage, the disk will not be considered suitable for use in Acronis Storage.

- **Metadata.** Use the disk to store metadata and run a metadata service on the node.


- **Cache.** Use the disk to store write cache. This role is only for SSDs. To cache a specific storage tier, select it from the drop-down list. Otherwise, all tiers will be cached.
- **Metadata+Cache.** A combination of two roles described above.
- **Unassigned.** Remove the roles from the disk.




Note:



1. If a physical server has a system disk with the capacity greater than 100GB, that disk can be additionally assigned the Metadata or Storage role. In this case, a physical server can have at least 2 disks.
2. It is recommended to assign the System+Metadata role to an SSD. Assigning both these roles to an HDD will result in mediocre performance suitable only for cold data (e.g., archiving).
3. The System role cannot be combined with the Cache and Metadata+Cache roles. The reason is that is I/O generated by the operating system and applications would contend with I/O generated by journaling, negating its performance benefits.

3. Click **Done**.
4. Repeat steps 1 to 3 for every disk you want to be used in the Acronis Storage cluster.
5. Click **NEW CLUSTER** or **JOIN CLUSTER**. On the **Configuration summary** screen, check the number of disks per each configuration category.

✕ Configuration summary

METADATA SERVICE				
	Metadata	1		

STORAGE SERVICE	SSD cache	Same disk cache	No cache	
	Tier 0	1	0	0
	Tier 1	3	0	0
	Tier 2	0	1	0

SSD CACHE		
	Tier 0	1
	Tier 1	1

PROCEED

CANCEL

6. Click **PROCEED**. You can monitor disk configuration progress in the **HEALTHY** list of the **NODES** screen.

2.3 Releasing Nodes from Cluster

To release a node means to remove it from the cluster (e.g., for maintenance). As the node may be running services needed by the cluster, do the following prior to releasing it to avoid cluster degradation:

1. If the node runs one of the five required metadata services, add a metadata role to another node. You need to make sure that the cluster has at least five metadata services running at any time.

2. If the node has any access points, make sure that the same access points are configured on other nodes in the cluster as well.
3. If the node has iSCSI targets, move them to a different node.
4. If the node has an S3 gateway or ABGW, reconfigure DNS for S3 and ABGW access points to remove the node from DNS records. Next, release the node from S3 and ABGW in the corresponded sections of the **SERVICES** screen.
5. Make sure the cluster has enough storage space to accommodate the data from the released node.

Once you initiate the release, the cluster will start replicating data chunks that were stored on the released node and distributing them among other storage nodes in the cluster. Depending on the amount of data to replicate, the process may take as much as several hours.

If necessary, you can also release a node forcibly, that is, without replication.

Warning: Releasing nodes forcibly may result in data loss.

To release a node from a cluster, do the following:

1. On the **NODES** screen, click the node to release.
2. On the node overview screen, click **Release**.
3. If necessary, in the **Release** node window, check force to release the node forcibly (highly not recommended).
4. Click **Yes**. The released node will return to the **UNASSIGNED** list on the **NODES** screen.

2.4 Removing Nodes from the Unassigned List

Nodes in the **UNASSIGNED** list can be completely removed from Acronis Storage.

Do the following: on the **NODES** screen, select the node in the **UNASSIGNED** list and click **Remove (forget)**.

Nodes completely removed from Acronis Storage can be re-added to the **UNASSIGNED** list in two ways:

- By logging in to the node via SSH and running `/usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m MN_ADDRESS -t TOKEN` in the node's console (MN_ADDRESS is the management node IP address

2.5. Managing Tier Encryption

and TOKEN is the token obtained in the management panel).

- By reinstalling Acronis Storage on the node from scratch.

2.5 Managing Tier Encryption

Acronis Storage can encrypt data stored on disks with the AES-256 standard, so if a disk gets lost or stolen the data will be safe. Acronis Storage stores disk encryption keys in cluster's metadata (MDS).

Encryption can be enabled or disabled only for the newly created chunk services (CS). Once tier encryption is enabled, you can decrypt disks (CSs) by manually releasing them from encrypted tiers. Correspondingly, simply enabling encryption on the disk's tier will not encrypt its data (CS). To encrypt a disk, you must assign it to an encrypted tier.

Note:

1. Acronis Storage does not encrypt data transmitted over the internal network.
2. Enabled encryption slightly decreases performance.

Advanced

ENCRYPTION

☒ Enable encryption (aes256)

☒ Tier 0☒ Tier 1☒ Tier 2☒ Tier 3

SAVE

To enable or disable tier encryption, on the **SETTINGS > Advanced settings** panel, select or deselect tiers and click **SAVE**.

2.6 Managing Acronis Storage Users

During the management panel installation on the first node, Acronis Storage creates the default unique administrator account, superadmin. The user name for this account is **admin** and the password is specified during installation. This account cannot be deleted and its privileges cannot be changed. Other than that, superadmin does not differ from a user account assigned the **Administrator** role (i.e. an admin).

An admin can create user accounts and assign to them one or more roles listed below:

- **Administrator**, can fully manage cluster and users.
- **Network**, can modify network settings and roles.
- **Cluster**, can create cluster, join nodes to cluster, and manage (assign and release) disks.
- **ABGW**, can create and manage Acronis Backup Gateway instances.
- **iSCSI**, can create and manage iSCSI targets and LUNs.
- **NFS**, can create and manage NFS shares and exports.
- **S3**, can create and manage S3 cluster.
- **SSH**, can add and remove SSH keys for cluster nodes access.
- **Updates**, can install Acronis Storage updates.

User accounts to which no roles are assigned are guest accounts. Guests can monitor Acronis Storage performance and parameters but cannot change any settings.

Note: All users can change their own passwords (see [Managing User Accounts](#) on page 24).

2.6.1 Creating User Accounts

To create a user account in the web-based user interface, do the following:

1. Log in to the management panel as admin.

2.6. Managing Acronis Storage Users

2. Open the **SETTINGS > Users** screen and click **ADD USER**.
3. On the **Add user** panel, specify the user name, password, and, if required, a user description in the corresponding fields.

✕ Add user

Name
 ☒ Enabled

Password

Description

SELECT ROLES

☐ **Administrator**
Can perform all management operations.

☒ **ABGW**
Can create and manage Acronis Backup Gateway.

☒ **NFS**
Can create and manage NFS.

☐ **Cluster**
Can create cluster, join nodes to cluster, and manage (assign and release) disks.

☒ **iSCSI**
Can create and manage iSCSI targets and LUNs.

☐ **Updates**
Can install updates.

☒ **Network**
Can modify network settings and roles.

☒ **S3**
Can create and manage S3 cluster.

☐ **SSH**
Can add and remove SSH keys for cluster nodes access.

ADD

4. Check the roles to assign to the account and click **Done**.

2.6.2 Managing User Accounts

Any user can change their account password by clicking the user icon in the top right corner of the management panel and then clicking **Change password**.

An admin can create/delete other users' accounts, add/remove roles from them, change their descriptions and passwords (although superadmin's password can only be changed by superadmin), as well as enable/disable user accounts (i.e. allow/prohibit user login). To manage a user account, login as an admin, open the **Settings** -> **Users** screen, select a user from the list, and click **Configure** or **Delete** depending on what you need to do.

✕ **Configure user**

Name

user1

Enabled

☒

Password

[change](#)

Description

SELECT ROLES

☐ **Administrator**
Can perform all management operations.

☒ **ABGW**
Can create and manage Acronis Backup Gateway.

☐ **NFS**
Can create and manage NFS.

☐ **Cluster**
Can create cluster, join nodes to cluster, and manage (assign and release) disks.

☐ **iSCSI**
Can create and manage iSCSI targets and LUNs.

☐ **Updates**
Can install updates.

☒ **Network**
Can modify network settings and roles.

☐ **S3**
Can create and manage S3 cluster.

☐ **SSH**
Can add and remove SSH keys for cluster nodes access.

DONE

2.6.3 Adding LDAP or Active Directory Users

You can add users and user groups to Acronis Storage from an external LDAP-compliant database or Microsoft Active Directory. These users will be able to log in using their respective user names and passwords. The set of actions these users will be able to perform in Acronis Storage will be defined by the roles you assign in Storage (listed in *Managing Acronis Storage Users* on page 22).

To add an LDAP (or AD) user or group to Acronis Storage, do the following:


1. On the **SETTINGS > Advanced settings** screen, open the **LDAP/AD** tab.









The screenshot shows the 'Advanced' settings interface. At the top, there's a header 'Advanced' with a user icon. Below it are four tabs: 'LDAP/AD', 'ENCRYPTION', 'SNMP', and 'MANAGEMENT NODE HA'. The 'LDAP/AD' tab is selected. The form contains the following fields:

- Type:** A dropdown menu showing 'Microsoft Active Directory'.
- Address:** A text input field containing '10.250.35.97'.
- Port:** A text input field containing '389'.
- Login:** A text input field containing 'cn=admin, cn=Users, dc=ya, dc=skol, dc=ko'.
- Password:** An empty text input field.
- Search Base DN:** A text input field containing 'dc=ya, dc=skol, dc=ko'.
- Advanced:** An unchecked checkbox.
- SAVE:** A blue button at the bottom left.

2. Select LDAP or Microsoft Active Directory from the **Type** drop-down list.
3. Specify the following parameters:
 - IP **Address** of an LDAP server or AD domain controller;
 - (optional) LDAP **Port**;

- **Bind DN** (a distinguished name of an LDAP authentication database user) or **Login** (AD);
 - **Bind Password** (LDAP) or **Password** (AD);
 - **Search Base DN**, a distinguished name of a search starting point;
 - (optional) **Advanced** LDAP or AD parameters.
4. Click **Save** to authenticate in Active Directory or LDAP server.
 5. On the **SETTINGS > Users** screen, click **ADD LDAP USER**.
 6. On the **Add LDAP users** panel, select users or user groups to add to Acronis Storage and click **Add**.

 **Add LDAP users**


<input type="checkbox"/>	Type	Name ↓	Description	
<input type="checkbox"/>		WinRMRemoteWMIUse...	Members of this gr...	
<input checked="" type="checkbox"/>		Administrators	Administrators hav...	
<input type="checkbox"/>		Users	Users are prevente...	
<input type="checkbox"/>		Guests	Guests have the sa...	
<input type="checkbox"/>		Print Operators	Members can admi...	
<input type="checkbox"/>		Backup Operators	Backup Operators c...	
<input type="checkbox"/>		Replicator	Supports file replica...	

ADD

2.6. Managing Acronis Storage Users

7. On the **Roles** panel, select the roles to assign to selected users or user groups.

Note: If a role is assigned to a group, every user in it is granted the corresponding privileges.

 **Roles**

☐ **Network**
Can modify network settings and roles.

☐ **NFS**
Can create and manage NFS.

☐ **Updates**
Can install updates.

☐ **SSH**
Can add and remove SSH keys for cluster nodes access.

☐ **Administrator**
Can perform all management operations.

☐ **S3**
Can create and manage S3 cluster.

☐ **iSCSI**
Can create and manage iSCSI targets and LUNs.

☐ **ABGW**
Can create and manage Acronis Backup Gateway.

☐ **Cluster**
Can create cluster, join nodes to cluster, and manage (assign and release) disks.

ADD

8. Click **Add** to add users to Acronis Storage.

Users

ADD USER

ADD LDAP USER

Search

Type	Name ↓	Description	
	user1	Guest user	Guest
	admin		Superadmin
LDAP	LDAPuser1	OpenLDAP	Network, Guest, SS...
LDAP	Administrators	Administrators hav...	Administrator
LDAP	Administrator	Built-in account for...	Administrator
LDAP	AD User Group	Active Directory	S3, Guest

Configure

Delete

2.7 Managing Acronis Storage Updates

You can update your Acronis Storage infrastructure using the web-based user interface.


Important: To check for and download updates, the cluster must be healthy and each node in the infrastructure must be able to open outgoing Internet connections.

To update Acronis Storage, do the following:

1. Open the **SETTINGS > Updates** screen and click **CHECK FOR UPDATES**. The script will run `yum update` on each node. If updates are available for a node, said node's status will change to `Update available`.


2.8. Allowing root Access to Cluster Nodes Over SSH

Updates



No updates available

CHECK FOR UPDATES

Node	Status	
10.90.100.99	Update available	
10.90.100.129	Update available	

2. To apply all available updates, click **UPDATE NOW**.

While updates are being applied, some of the Acronis Storage services might be unavailable for a short period of time.

2.8 Allowing root Access to Cluster Nodes Over SSH

In certain situations, you or the technical support team may need root access to cluster nodes via SSH. To allow root access to all nodes in the cluster, do the following:

1. Obtain an SSH public key from the technical support team.
2. Open the **SETTINGS > SSH** screen, click **ADD KEY**, paste the key, and click **Add key**.

✕ Add Public Key

Key

```
ssh-rsa
AAAAB3NzaC1yc2EARRABIwAAAEQEAkIOUpkDHrfHY17SbrmTIpNLTG
K9Tjom/BWDSU
GPI+nafzIHDTYW7hdi4yZ5ew18JH4JW9jbhUFrviQzM7xIELEVf4h9IFX5
QVkbPppSwg0cda3
Pbv7kOdJ/MTyRRWXFCR+HAo3FXRitBqxiX1nYUXpHAZsMciLq8V6Rjs
NAQwdsdMFvSIVK/7XA
t3FaoJoAsncM1Q9x5+3V0Ww68/eIFmb1zuUFIjQJKprX88XypNDvjYN
by6vw/Pb0rwert/En
mZ+AW4OZPnTPI89ZPmVMLuayrD2cE86Z/il8b+gw3r3+1nKatmlkjn2
so1d01QraTIMqVSsbx
NrRFi9wrf+M7Q== user@localdomain.local
```

Add key

To delete the key after root access is no longer required, select the key and click **Delete**.

2.9 Backing Up and Restoring Management Database

Acronis Storage stores node information, statistics, and configuration in a database on the node with the management panel. Database backups are created automatically every day.


Warning: Do not rename the backup file! Otherwise you will not be able to restore the management database from it.


To back up the database manually, open the **SETTINGS > Backup** screen and click **BACKUP NOW**.


Backup OK

System stores node information, statistics and configuration in a database. Its backups are created automatically.

[How to recover?](#)

 Last backup
Mar 09, 2017, 11:32 AM

 Backup period
Daily

 Backup location
/mnt/vstorage/webcp/backup/

BACKUP NOW

Once backup is completed, the **Last backup** date will be refreshed.

2.9.1 Restoring Management Database from Backup

You can restore a management node database from backup on the following nodes:

- the same management node or any node assigned to a cluster,
- a new node outside the cluster. In this case, Acronis Storage will restore the database and install only the management panel component on the node.

To restore to the same management node or a cluster node, run the following script:

```
# /usr/libexec/vstorage-ui-backend/bin/restore-management-node.sh \  
-x <public_network_interface> -i <internal_network_interface>
```

where `<public_network_interface>` and `<internal_network_interface>` are interfaces with already assigned public and internal roles. They will be assigned the **Web CP** and **Management** roles, respectively.

Note: You can specify the same network interface in both parameters.

To restore the database to a new node, do the following:

1. Copy the backup file `/mnt/vstorage/webcp/backup/backup-<timestamp>.tar` from the initial management node to the same directory on the target node.
2. Run the following script on the target node:

```
# /usr/libexec/vstorage-ui-backend/bin/restore-management-node.sh \  
-x <public_network_interface> -i <internal_network_interface> \  
-f <path-to-backup-file>
```

where `<public_network_interface>` and `<internal_network_interface>` are interfaces to be assigned the **Web CP** and **Management** roles, respectively.

2.10 Enabling Management Panel High Availability

Acronis Storage can provide high availability of the management panel by hosting its standby (inactive) instances on multiple nodes and continuously updating them. If the management node fails or becomes unreachable over the network, a management panel instance on another node will take over the panel's service and keep its dedicated IP address. The relocation of the service can take several minutes.

To enable management panel high availability, dedicate at least 3 nodes to host management panel instances and do the following:

1. Make sure to assign the WebCP role to network interfaces on each node that will host management panel instances.
2. On the **SETTINGS > Management node** screen, open the **MANAGEMENT NODE HA CONFIGURATION** tab.

2.10. Enabling Management Panel High Availability

Advanced

MANAGEMENT NODE HA CONFIGURATION

SSL ACCESS

AVAILABLE NODES



5

Hide available nodes ^

Create HA



10.250.14.113

☒


10.250.14.12

☒



10.250.14.120

☐






10.250.14.15

☐










localhost


☒

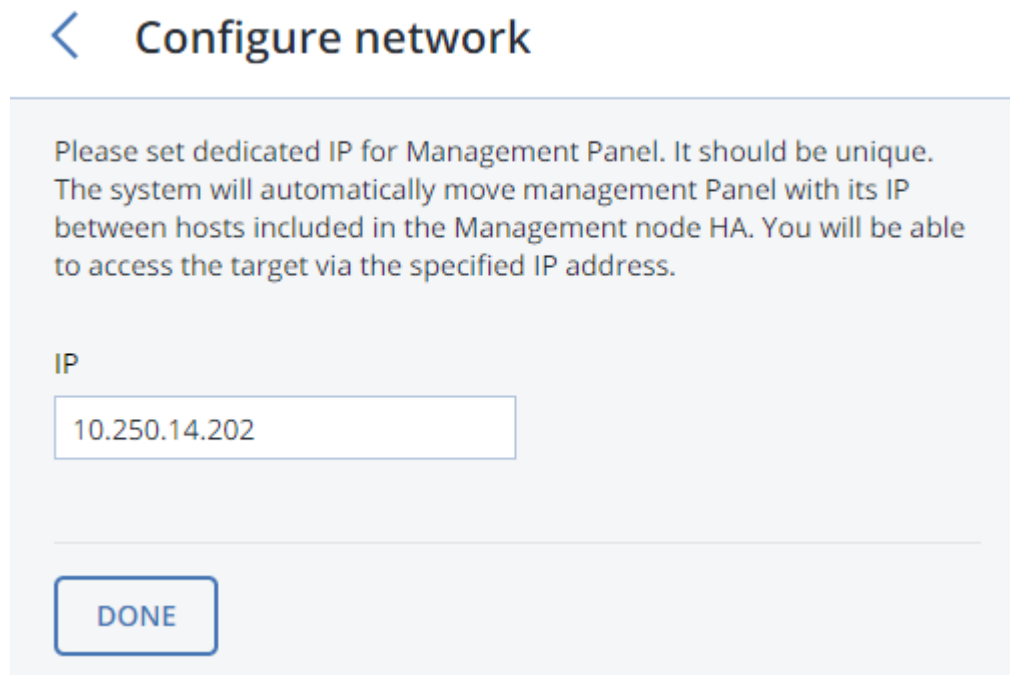
3. Select at least 3 nodes to host management panel instances and click **Create HA**.
4. Make sure a configured network interface with an internal management role is selected from the **Management private** interface drop-down list of each node.

✕ Configure network

 10.250.14.113 	
Management private	WebCP public
<input type="text" value="ens160 - 10.250.14.113"/> 	ens160 - 10.250.14.113
<hr/>	
 10.250.14.12 	
Management private	WebCP public
<input type="text" value="ens160 - 10.250.14.12"/> 	ens160 - 10.250.14.12
<hr/>	
 localhost 	
Management private	WebCP public
<input type="text" value="ens160 - 10.250.14.16"/> 	ens160 - 10.250.14.16

PROCEED

- On the **Configure network** screen, set a static IP address dedicated for the HA management panel. It must be different from the IP addresses of any node in the cluster and accessible from the public network. Click **DONE**.



< **Configure network**

Please set dedicated IP for Management Panel. It should be unique. The system will automatically move management Panel with its IP between hosts included in the Management node HA. You will be able to access the target via the specified IP address.

IP

10.250.14.202

DONE

Once the management panel high availability is enabled, you can log in to the panel only at https://<HA_management_panel_IP>:8888.

To remove management panel instances from the nodes, select them from the HA list on the **MANAGEMENT NODE HA** tab and click **Release nodes**.

2.11 Accessing the Management Panel via SSL

When configuring various Acronis Storage features, you may need to enter sensitive information like credentials for user and e-mail accounts, S3 services, and such. To secure communication with the management panel, you can switch to the HTTPS protocol as follows:

1. On the **SETTINGS > Management node > SSL ACCESS** tab, click **UPLOAD**.
2. Upload an SSL certificate from a trusted certificate authority.
3. Click **SAVE**.

The uploaded certificate will be added to the configuration of the web server hosting the management panel and you will be able to access it over HTTPS.

You can also generate a self-signed certificate, although it will not be trusted and you will have to manually accept it in your browser.

2.12 Managing Acronis Storage Licenses

Acronis Storage comes with a trial license that allows you to evaluate its features. The trial license has no expiration date but limits the storage capacity to 1TB.

To start using Acronis Storage in a production environment, it is recommended to install a commercial license. The following licensing models are supported:

- License key. Implementing the provisioning model, keys are time-limited (subscription) or perpetual and grant a certain storage capacity. If a commercial license is already installed, a key augments its expiration date or storage limit (not both).
- Services provider license agreement (SPLA). SPLA implements the pay-as-you-go model: it grants unlimited storage capacity and customers are charged for the actual usage of cluster space. With SPLA, Acronis Storage automatically sends reports to Acronis Data Cloud once every four hours. If no reports have been received for two weeks, the license expires.

You can switch the licensing model at any time:

- Switching from a license key to SPLA terminates the key even if it has not yet expired. Terminated keys cannot be used anymore.
- Switching from SPLA to a license key changes the licensing model to subscription or perpetual. After doing so, ask your service provider to terminate your SPLA by either disabling the Storage application for your account or deleting the account.

Note: If a license expires, all write operations to the Acronis Storage cluster stop until a valid license is installed.

2.12.1 Installing License Keys

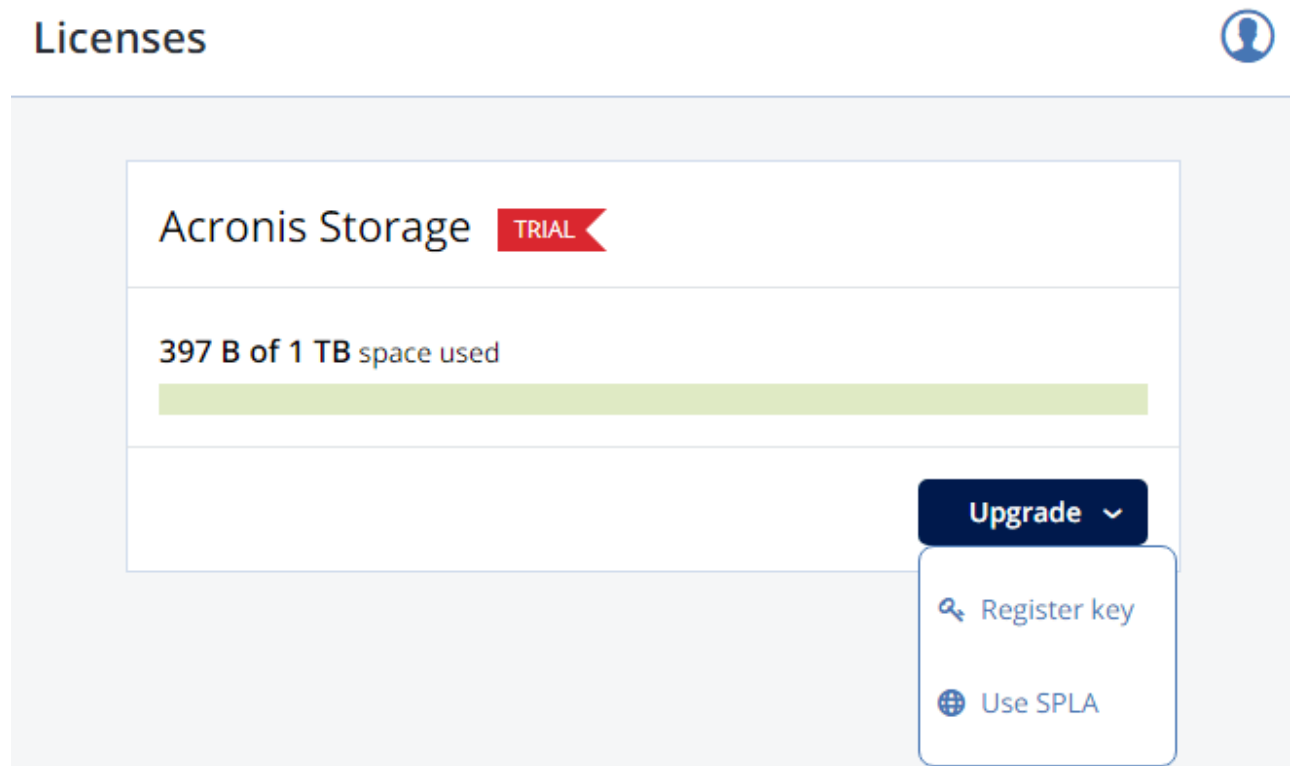
To install an Acronis Storage license key, do the following:

1. If you are switching from SPLA, ask your service provider to terminate the agreement by either disabling

2.12. Managing Acronis Storage Licenses

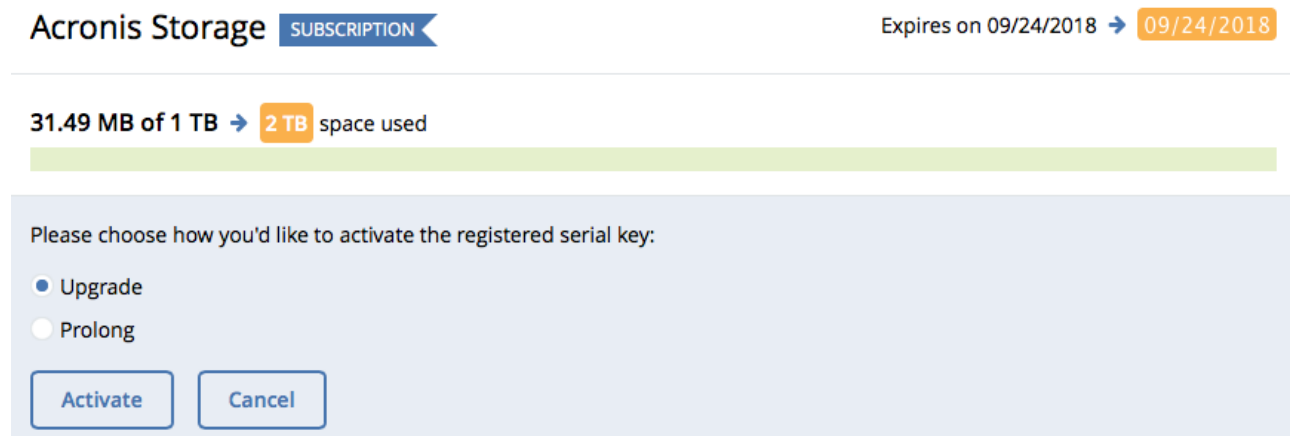
the Storage application for your account or deleting the account.

2. On the **LICENSES** screen, click **Upgrade** and **Register key**.



The screenshot shows the 'Licenses' page header with a user profile icon. Below it is a card for 'Acronis Storage' with a red 'TRIAL' badge. It indicates '397 B of 1 TB space used' with a green progress bar. An 'Upgrade' button with a dropdown arrow is visible, and its menu is open, showing 'Register key' (with a key icon) and 'Use SPLA' (with a globe icon).

3. Paste the license key, click **REGISTER**, and choose one of the following:



The screenshot shows the 'Acronis Storage' page with a blue 'SUBSCRIPTION' badge. It displays 'Expires on 09/24/2018' and '09/24/2018' in an orange box. Below, it shows '31.49 MB of 1 TB' and '2 TB space used' with a green progress bar. A section titled 'Please choose how you'd like to activate the registered serial key:' contains two radio buttons: 'Upgrade' (selected) and 'Prolong'. At the bottom are 'Activate' and 'Cancel' buttons.

- **Upgrade**, to add storage capacity.
- **Prolong**, to prolong the license.

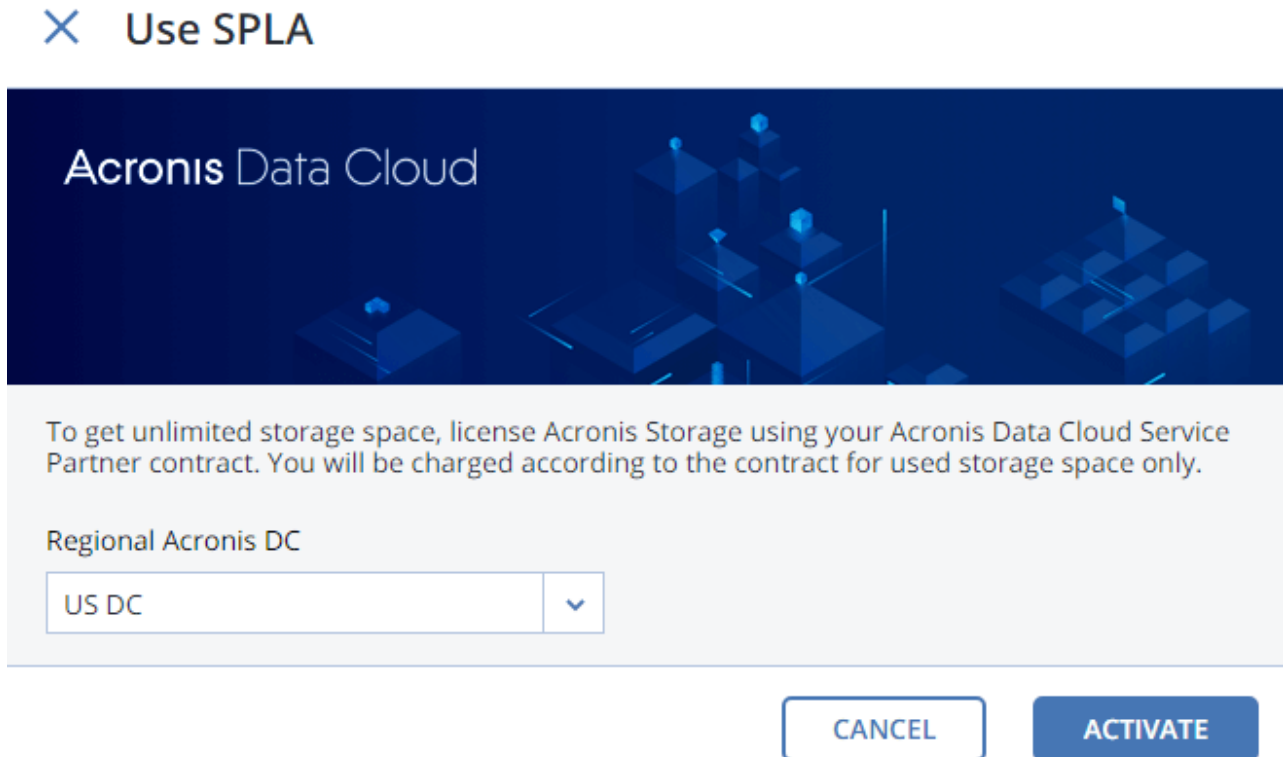
4. Click **Activate**.

The expiration date or storage capacity will change according to what the key grants.

2.12.2 Installing SPLA Licenses

To install a SPLA license, do the following:

1. On the **LICENSES** screen, click **Upgrade** and **Use SPLA**.



2. In the **Use SPLA** window, select a region from the drop-down list and click **Activate**. You will be redirected to a log in page of Acronis Data Cloud.
3. Log in to Acronis Data Cloud.
4. In the **Register cluster** window, accept the license agreement.
5. In the registration confirmation window, click **Done**.


The registered cluster will show up in Acronis Data Cloud. You will be able to monitor its resource usage and download reports.

2.13 Connecting Remote iSCSI Devices to Storage Cluster Nodes

Acronis Storage allows you to connect remote iSCSI devices to nodes and perceives their LUNs as storage disks. You can connect iSCSI devices to nodes at any time.

To connect a remote iSCSI device to a node, do the following:

1. On the **NODES** screen, select a node, open its **DISKS** tab, and click **iSCSI target**.

 **Remote iSCSI Target**

Target IQN

iqn.2014-06.com.vstorage:target1

IP address: Port

+ Add portal

10.94.129.123

10.94.129.124

☒ CHAP authentication (optional)

Login

user1

Password

.....

CANCEL

CONNECT

2. In the **Remote iSCSI Target** window, do the following:
 - 2.1. Specify the IQN of the target.
 - 2.2. In the **Portal** and **Port** fields, specify the target's IP address and port (optional) and click the corresponding check icon.
 - 2.3. (Optional) If the target has multiple paths, click **Add portal** and configure it as in the previous step.
 - 2.4. (Optional) If necessary, check **CHAP authentication** and specify the credentials.
 - 2.5. Click **Connect**.

Acronis Storage will connect the target (i.e. all its LUNs) and initiate it; corresponding entries with the **iSCSI** type will appear in the node's **DISKS** list.

To remove the iSCSI target, click **iSCSI Target**, **DELETE CONNECTION**, and **DELETE**.

2.13.1 Assigning Disk Roles To Remote iSCSI Devices

If the node was already in the cluster before you connected the iSCSI device to it, assign disk roles to all its LUNs. To do this:

1. Select a disk with the **iSCSI** type and click **Assign**.
2. In the **Choose role** window, select **Storage** and click **Done**.
3. Repeat the above steps for every disk with the **iSCSI** type.

Note: You can assign metadata or cache roles to these disks but it is recommended only for single-node installations with SAN-provided redundancy that host Acronis Backup Gateways. For more information on disk roles, see the roles description in [Assigning Disk Roles Manually](#) on page 16.

CHAPTER 3

Monitoring Acronis Storage Clusters

From the management panel, you can monitor the performance of both the whole cluster and its parts.

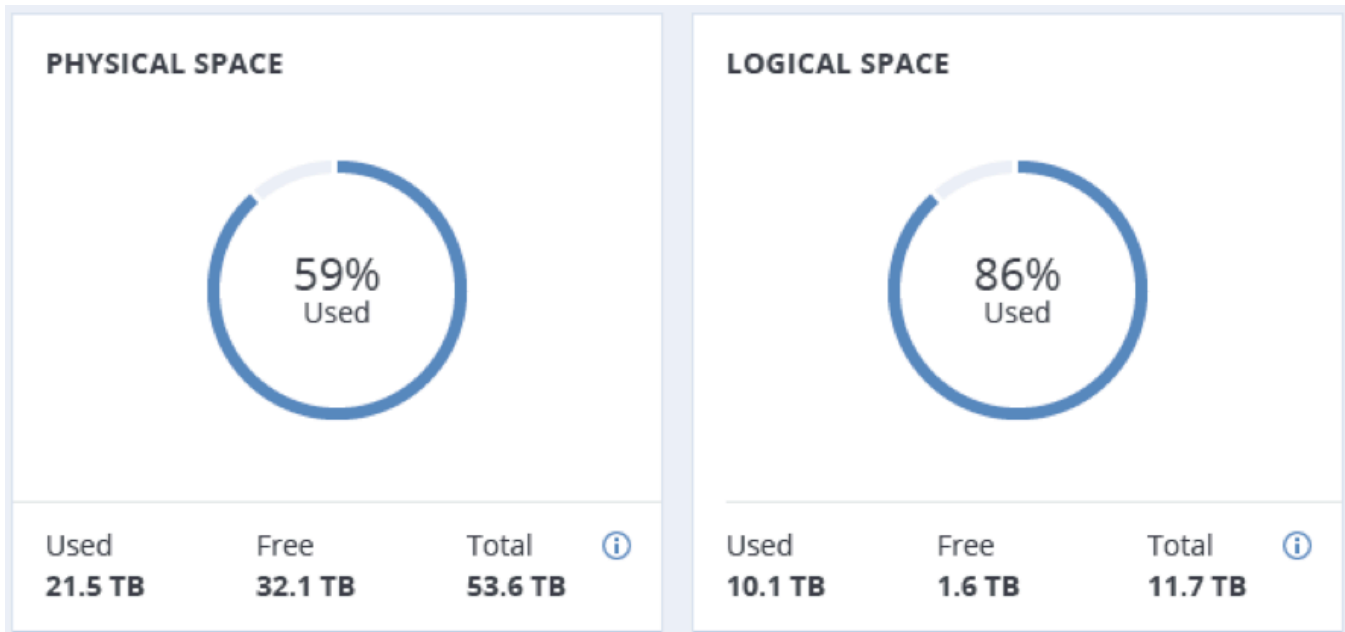
3.1 Monitoring Cluster Status

The overall cluster statistics are available on the cluster **OVERVIEW** screen. Pay attention to the cluster status that can be one of the following:

- **HEALTHY.** All cluster components are active and operate normally.
- **UNKNOWN.** Not enough information about the cluster state (e.g., because the cluster is inaccessible).
- **DEGRADED.** Some of the cluster components are inactive or inaccessible. The cluster is trying to heal itself, data replication is scheduled or in progress.
- **FAILURE.** The cluster has too many inactive services, automatic replication is disabled. If the cluster enters this state, troubleshoot the nodes or contact the support team.

3.2 Monitoring Cluster Storage Space

You can monitor cluster storage space on the cluster **OVERVIEW** screen. Typical statistics may look like this:



The two charts that provide information on how storage space is used are **PHYSICAL SPACE** and **LOGICAL SPACE**. They are described in the following sections in more detail.

3.2.1 Physical Space Chart

The **PHYSICAL SPACE** chart shows the combined space of all disks available to the cluster. The following statistics are available:

- **Used space.** The space occupied by all data chunks and their replicas plus the space occupied by any other data stored on cluster nodes' disks.
- **Free space.** The unused space on all cluster nodes' disks.
- **Total space.** The total space on all cluster nodes' disks.

3.2.2 Logical Space Chart

The **LOGICAL SPACE** chart represents all the space that can be allocated and used by the cluster for storing user data. This space includes the following:

- **Total space.** The maximum disk space available as defined by license.
- **Used space.** The space occupied exclusively by user data. Replicas and erasure coding metadata are not

3.2. Monitoring Cluster Storage Space

taken into account.

- **Free space.** The difference between the two above.

3.2.2.1 Understanding Logical Space

When monitoring disk space information in the cluster, keep in mind that logical space is the amount of free disk space that can be used for storing user data in the form of data chunks and all their replicas. Once this space runs out, no data can be written to the cluster.

To better understand how logical disk space is calculated, consider the following example:

- The cluster has three disks with the storage role. The first disk has 200 GB of space, the second one has 500 GB, and the third one has 1 TB.
- If the redundancy mode is set to three replicas, each data chunk must be stored as three replicas on three different disks with the storage role.

In this example, the available logical disk space will be 200 GB, that is, equal to the capacity of the smallest disk with the storage role. The reason is that each replica must be stored on a different disk. So once the space on the smallest disk (i.e. 200 GB) runs out, no new chunk replicas can be created unless a new disk with the storage role is added or the redundancy mode is changed to two replicas.

With the two replicas redundancy mode, the available logical disk space would be 700 GB, because the two smallest disks combined can hold 700 GB of data.

3.2.3 Monitoring Chunk Status and Replication

You can monitor the state of all chunks in the cluster in the **CHUNKS** section of the cluster **OVERVIEW** screen.

The table below lists all possible states a chunk can have.

State	Description
healthy	Percentage of chunks that have enough active replicas. The normal state of chunks.
offline	Percentage of chunks all replicas of which are offline. Such chunks are completely inaccessible for the cluster and cannot be replicated, read from or written to. All requests to an offline chunk are frozen until a CS that stores that chunk's replica goes online. Get offline cluster nodes back online as soon as possible to avoid data loss.

State	Description
blocked	Percentage of chunks which have fewer active replicas than the set minimal amount. Write requests to a blocked chunk are frozen until it has at least the set minimum amount of replicas. Read requests to blocked chunks are allowed, however, as they still have some active replicas left. Blocked chunks have higher replication priority than degraded chunks. Having blocked chunks in the cluster increases the risk of losing data, so postpone any maintenance on working cluster nodes and get offline chunk servers back online as fast as possible.
degraded	Percentage of chunks with the number of active replicas lower than normal but equal to or higher than the set minimum. Such chunks can be read from and written to.

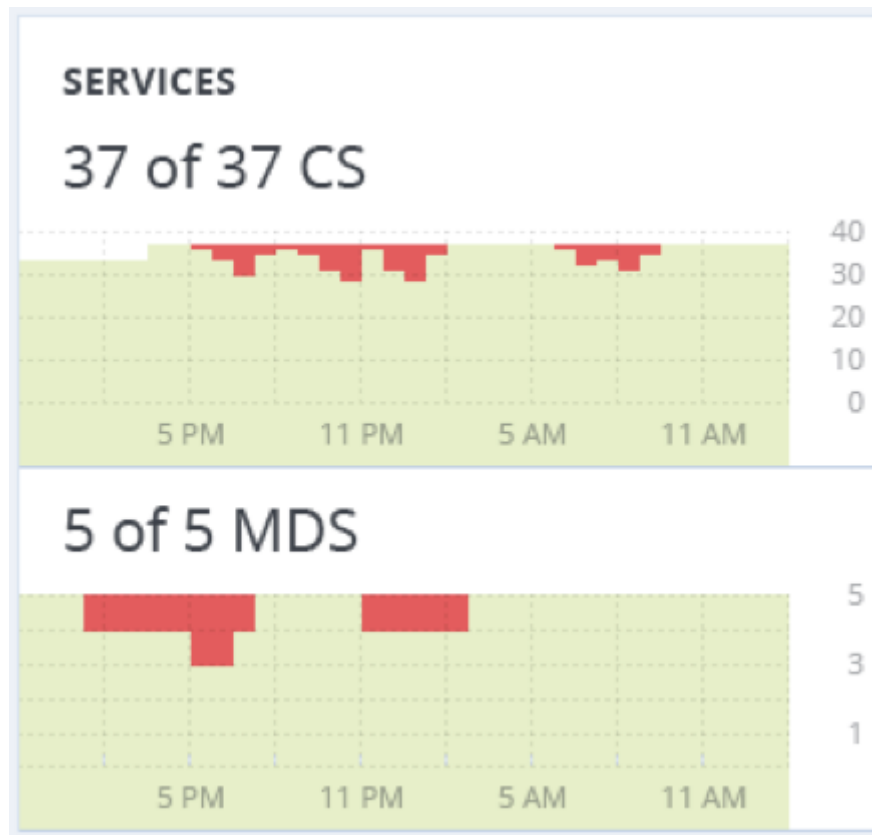
3.2.4 Monitoring Cluster Services

You can monitor two types of services in the **SERVICES** section on the cluster **OVERVIEW** screen:

- MDS, metadata services. Ensure that five are running at all times.
- CS, chunk services. With this chart, you can also keep track of all disks with the storage role.

Typical statistics may look like this:

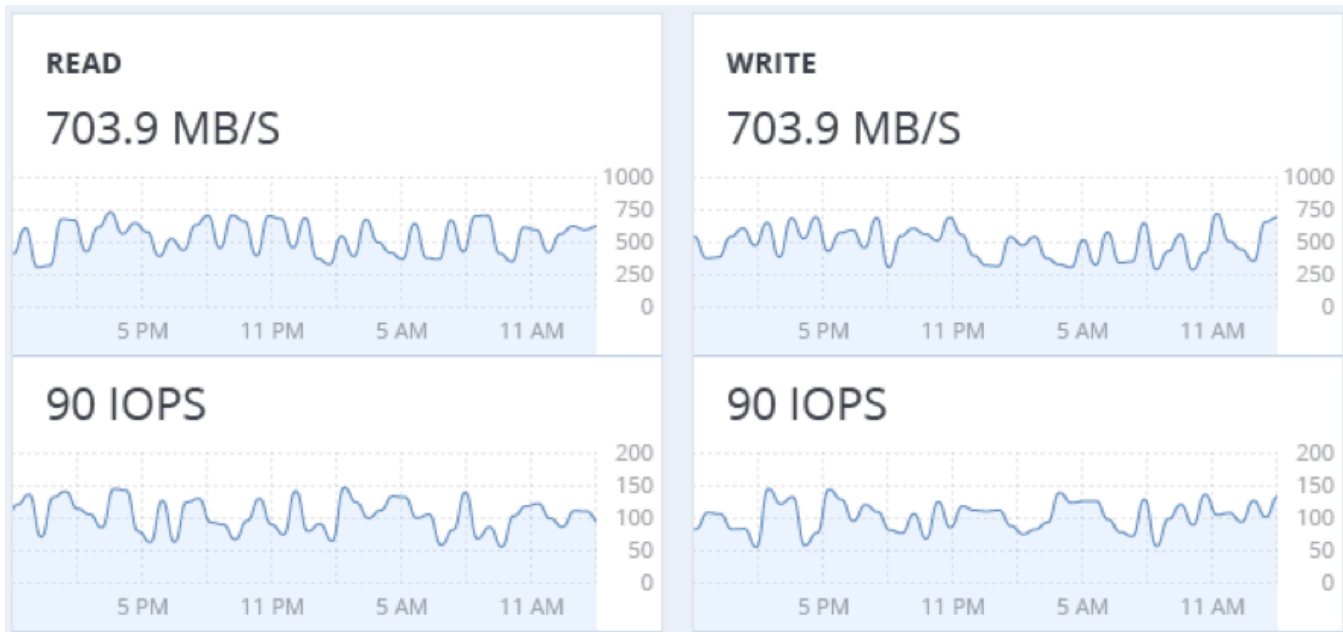
3.2. Monitoring Cluster Storage Space



If some of the services were not in the healthy state for some time, these time periods will be highlighted in red on the charts.

3.2.5 Monitoring Cluster I/O Activity

You can monitor the history of the cluster I/O activity on the **READ** and **WRITE** charts on the cluster **OVERVIEW** screen. Typical statistics may look like this:



The current cluster I/O activity averaged for the last 10 seconds is shown as:

- the speed of read and write I/O operations, in megabytes per second (MB/s).
- the number of read and write I/O operations per second (IOPS).

3.3 Monitoring Acronis Cluster Objects via SNMP

You can monitor cluster objects via the Simple Network Management Protocol (SNMP). The implementation conforms to the same Structure of Management Information (SMI) rules as the data in the standard SNMP context: all objects are organized in a tree; each object identifier (OID) is a series of integers corresponding to tree nodes and separated by dots.

General information:

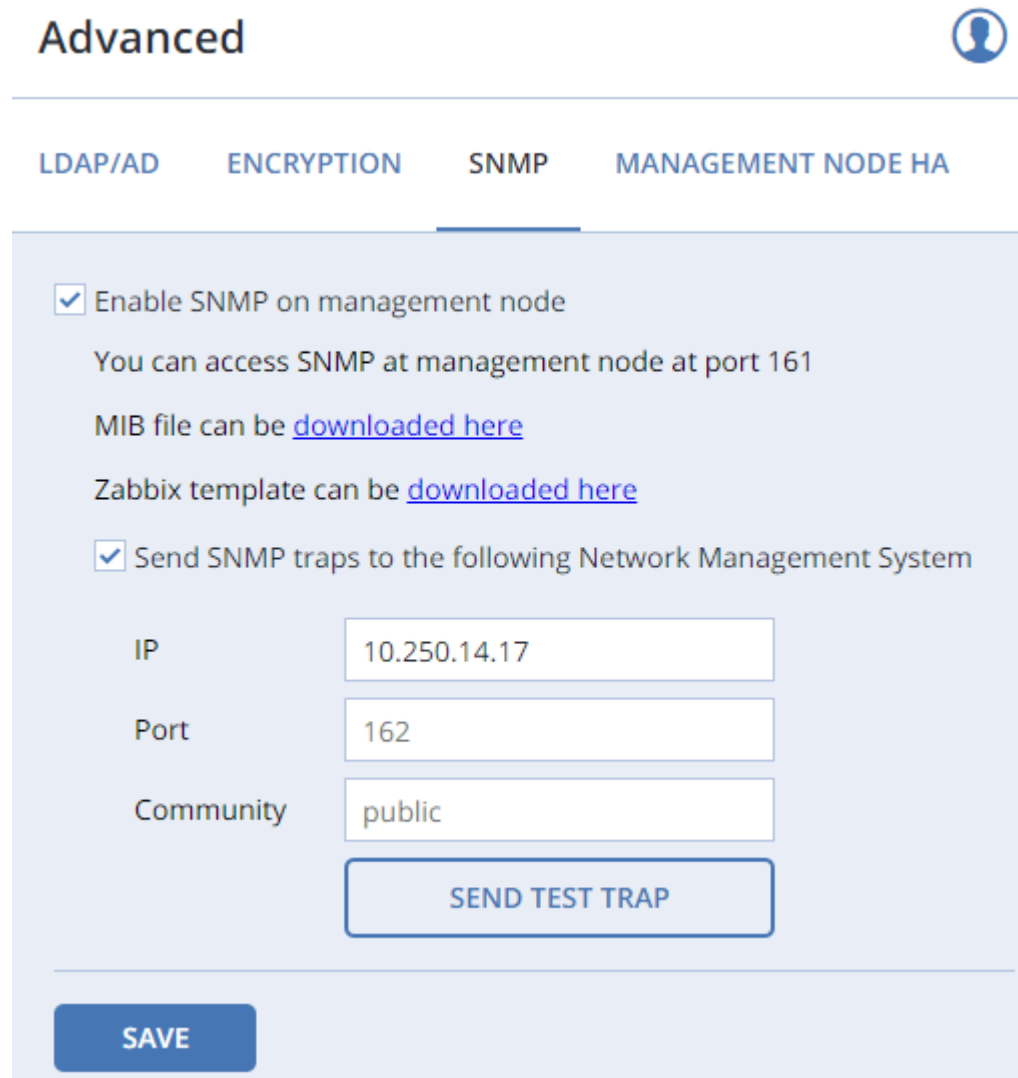
- The OID of the root subtree with all the objects you can monitor is 1.3.6.1.4.1.8072.161.1.
- The VSTORAGE-MIB.txt information base file is required to monitor the objects. You can download the file at http://<management_panel_IP>:8888/api/v2/snmp/mibs/VSTORAGE-MIB.txt.


The following subsections describe ways to enable and use SNMP to monitor cluster objects.

3.3.1 Enabling SNMP Access

To monitor cluster objects, enable the SNMP access on the node. Do the following in the management panel:

1. On the **SETTINGS > Advanced settings > SNMP** tab, check **Enable SNMP on management node**. Doing so lets your network management system (SNMP monitor) access the cluster via the SNMP protocol on the management node's port 161.



Advanced 

LDAP/AD **ENCRYPTION** **SNMP** **MANAGEMENT NODE HA**

☒ **Enable SNMP on management node**

You can access SNMP at management node at port 161

MIB file can be [downloaded here](#)

Zabbix template can be [downloaded here](#)

☒ **Send SNMP traps to the following Network Management System**

IP	<input type="text" value="10.250.14.17"/>
Port	<input type="text" value="162"/>
Community	<input type="text" value="public"/>

SEND TEST TRAP

SAVE

2. Click the corresponding link to download the MIB file and set it up in your SNMP monitor.
3. If required, have Acronis Storage send SNMP traps to your SNMP monitor. Do the following:
 - 3.1. Check **Send SNMP traps to Network Management System**.

- 3.2. Specify the **IP** of the system, and, if required, change the default **Port** and **Community**.
- 3.3. If required, click **SEND TEST TRAP** to test the service.
4. Click **SAVE** to apply changes.

3.3.2 Accessing Acronis Objects via SNMP

You can access Acronis objects with SNMP tools of your choice, e.g., the free Net-SNMP suite for Linux.

To display cluster information on the node with management panel, place the MIB file to `/usr/share/snmp/mibs` and run the `snmpwalk` command. For example:

```
# snmpwalk -M /usr/share/snmp/mibs -m VSTORAGE-MIB -v 2c -c public \  
localhost:161 VSTORAGE-MIB:cluster
```

Typical output may be the following:

```
VSTORAGE-MIB::clusterName.0 = STRING: "cluster1"  
VSTORAGE-MIB::healthStatus.0 = STRING: "healthy"  
VSTORAGE-MIB::usedSpace.0 = Counter64: 173732322  
VSTORAGE-MIB::totalSpace.0 = Counter64: 1337665179648  
VSTORAGE-MIB::freeSpace.0 = Counter64: 1318963253248  
VSTORAGE-MIB::licenseStatus.0 = STRING: "unknown"  
VSTORAGE-MIB::licenseCapacity.0 = Counter64: 1099511627776  
VSTORAGE-MIB::licenseExpirationStatus.0 = STRING: "None"  
VSTORAGE-MIB::ioReadOpS.0 = Counter64: 0  
VSTORAGE-MIB::ioWriteOpS.0 = Counter64: 0  
VSTORAGE-MIB::ioReads.0 = Counter64: 0  
VSTORAGE-MIB::ioWrites.0 = Counter64: 0  
VSTORAGE-MIB::csActive.0 = Counter64: 11  
VSTORAGE-MIB::csTotal.0 = Counter64: 11  
VSTORAGE-MIB::mdsAvail.0 = Counter64: 4  
VSTORAGE-MIB::mdsTotal.0 = Counter64: 4  
<...>
```

3.3. Monitoring Acronis Cluster Objects via SNMP

3.3.2.1 Listening to SNMP Traps

To start listening to SNMP traps, do the following:

1. Configure the `snmptrapd` daemon to log SNMP traps, allow them to trigger executable actions, and resend data to the network. To do this, add the following public community string to the `/etc/snmp/snmptrapd.conf` file:

```
authCommunity log,execute,net public
```

2. Start the daemon and specify the MIB file:

```
# snmptrapd -M /usr/share/snmp/mibs -m VSTORAGE-MIB -n -f -Lf /tmp/traps.log
```

3. Send a test trap from the **SETTINGS > Advanced settings > SNMP** tab in the management panel.
4. View the log file:

```
# tail -f /tmp/traps.log
2017-04-23 02:48:18 UDP: [127.0.0.1]:58266->[127.0.0.1]:162 [UDP: \
[127.0.0.1]:58266->[127.0.0.1]:162]:
SNMPv2-SMI::mib-2.1.3.0 = Timeticks: (1687405) 4:41:14.05      \
SNMPv2-SMI::snmpModules.1.1.4.1.0 = OID: VSTORAGE-MIB::generalAlert      \
VSTORAGE-MIB::trapType = STRING: Test Case      VSTORAGE-MIB::trapMsg = \
STRING: This Is Text Message to end-user      \
VSTORAGE-MIB::trapPriority = Counter64: 1
```

The test trap is considered a `generalAlert`.

3.3.3 Monitoring Clusters with Zabbix

To configure cluster monitoring in Zabbix, do the following:

1. On the **SETTINGS > Advanced settings > SNMP** tab, click the corresponding link to download a template for Zabbix.

Note: The template is compatible with Zabbix 3.x.

2. In Zabbix, click **Configuration > Templates > Import** and **Browse**.

Import file vstorage.xml

Rules	Update existing	Create new	Delete missing
Groups		<input checked="" type="checkbox"/>	
Hosts	<input type="checkbox"/>	<input type="checkbox"/>	
Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Template screens	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Template linkage		<input checked="" type="checkbox"/>	
Applications		<input checked="" type="checkbox"/>	<input type="checkbox"/>
Items	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Discovery rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Triggers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Graphs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Web scenarios	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Screens	<input type="checkbox"/>	<input type="checkbox"/>	
Maps	<input type="checkbox"/>	<input type="checkbox"/>	
Images	<input type="checkbox"/>	<input type="checkbox"/>	
Value mappings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

3. Navigate to the template, select it, and click **Import**.
4. Click **Configuration > Hosts > Create host**.

3.3. Monitoring Acronis Cluster Objects via SNMP

Host name

Visible name

Groups

In groups

Other groups

Discovered hosts
Hypervisors
Linux servers
Templates
Virtual machines
Zabbix servers

New group

Agent interfaces

IP address DNS name Connect to Port Default

[Add](#)

SNMP interfaces

IP DNS [Remove](#)

☒ Use bulk requests

[Add](#)

JMX interfaces

[Add](#)

IPMI interfaces

[Add](#)

Description

Monitored by proxy

Enabled ☒

[Add](#) [Cancel](#)

5. On the **Host** tab, do the following:

5.1. Specify the **Host name** of the management node and its **Visible name** in Zabbix.

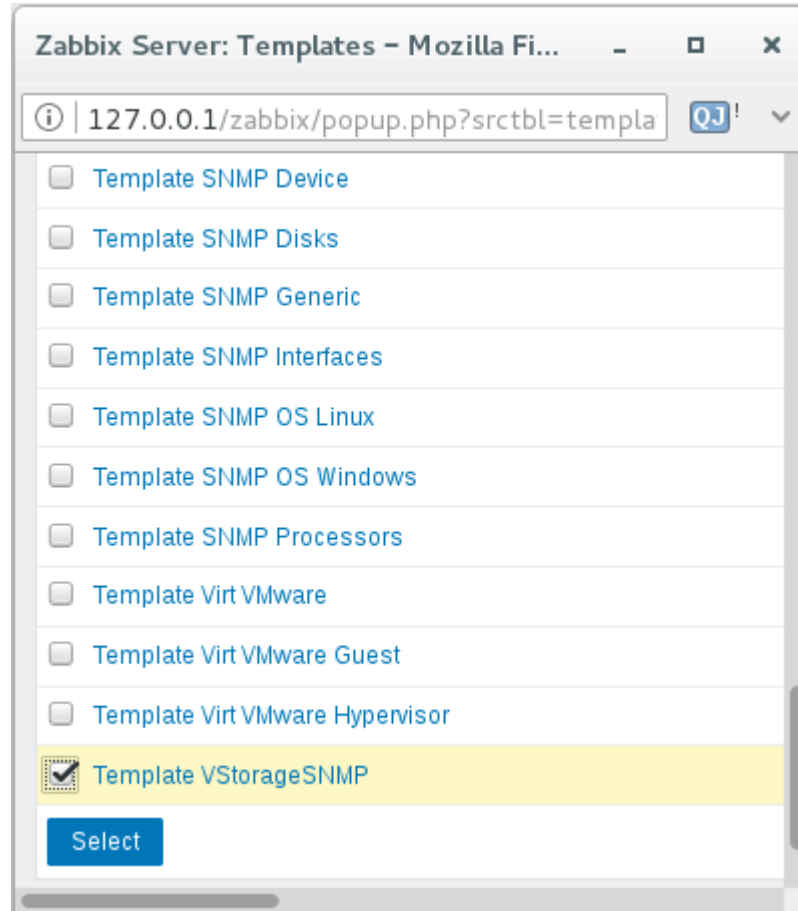
5.2. Specify **vstorage** in the **New group** field.

5.3. **Remove** the **Agent Interfaces** section.

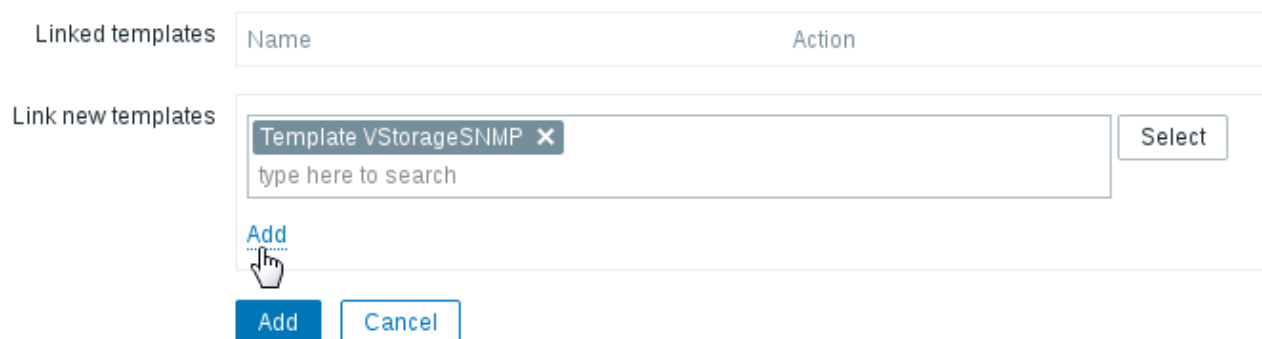
5.4. **Add** an **SNMP interfaces** section and specify the IP of the management node in the corresponding field.

6. On the **Templates** tab, click **Select** next to the **Link new templates** field.

7. In the **Zabbix Server: Templates** window, check the **Template VStorageSNMP** template and click **Select**.



8. Back on the **Templates** tab, click the **Add** link in the **Link new templates** section. The VStorageSNMP template will appear in the **Linked templates** group.



9. Having configured the host and added its template, click the **Add** button.

3.3. Monitoring Acronis Cluster Objects via SNMP

Linked templates

Name	Action
Template VStorageSNMP	Unlink

Link new templates

Select

[Add](#)

Add

Cancel

In a few minutes, the cluster's **SNMP** label in the **Availability** column on the **Configuration > Hosts** screen will turn green.

<input type="checkbox"/>	Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info		
<input type="checkbox"/>	Cluster	Applications 2	Items 32	Triggers 7	Graphs 3	Discovery 2	Web	10.250.14.15: 161	VStorageSNMP	Enabled	ZBX	SNMP	JMX	IPMI	NONE

To monitor cluster's parameters, open the **Monitoring > Latest data** screen, set the filter's **Host groups** to **vstorage** and click **Apply**.

You can create performance charts on the **Configuration > Hosts > <cluster> > Graphs** tab and a workplace for them on the **Monitoring > Screens** tab.

3.3.4 Description of Cluster Objects and Traps

The table below describes cluster-related objects you can monitor:

Object	Description
VSTORAGE-MIB:cluster	General cluster information.
VSTORAGE-MIB:csStatTable	Chunk server statistics table.
VSTORAGE-MIB:mdsStatTable	Metadata server statistics table.
VSTORAGE-MIB::clusterName	Cluster name.
VSTORAGE-MIB::healthStatus	Cluster health status.
VSTORAGE-MIB::usedSpace	The space occupied by all data chunks and their replicas plus the space occupied by any other data stored on cluster nodes' disks.
VSTORAGE-MIB::totalSpace	The total space on all cluster nodes' disks.
VSTORAGE-MIB::freeSpace	The unused space on all cluster nodes' disks.
VSTORAGE-MIB::licenseStatus	License status.
VSTORAGE-MIB::licenseCapacity	The maximum disk space available as defined by license.

Object	Description
VSTORAGE-MIB::licenseExpirationStatus	License expiration status.
VSTORAGE-MIB::ioReadOpS	Current read speed in operations per second.
VSTORAGE-MIB::ioWriteOpS	Current write speed in operations per second.
VSTORAGE-MIB::ioReads	Current read speed in bytes per second.
VSTORAGE-MIB::ioWrites	Current read write in bytes per second.
VSTORAGE-MIB::csActive	The number of active chunk servers.
VSTORAGE-MIB::csTotal	The total number of chunk servers.
VSTORAGE-MIB::mdsAvail	The number of running metadata servers.
VSTORAGE-MIB::mdsTotal	The total number of metadata servers.
VSTORAGE-MIB::s3OsAvail	The number of running S3 object servers.
VSTORAGE-MIB::s3OsTotal	The total number of S3 object servers.
VSTORAGE-MIB::s3NsAvail	The number of running S3 name servers.
VSTORAGE-MIB::s3NsTotal	The total number of S3 name servers.
VSTORAGE-MIB::s3GwAvail	The number of running S3 gateways.
VSTORAGE-MIB::s3GwTotal	The total number of S3 gateways.

The table below describes the CS-related objects you can monitor:

Object	Description
VSTORAGE-MIB::csId	Chunk server identifier.
VSTORAGE-MIB::csStatus	Current chunk server status.
VSTORAGE-MIB::csIoReadOpS	Current read speed of a chunk server in operations per second.
VSTORAGE-MIB::csIoWriteOpS	Current write speed of a chunk server in operations per second.
VSTORAGE-MIB::csIoWait	The percentage of time spent waiting for I/O operations. Includes time spent waiting for synchronization.
VSTORAGE-MIB::csIoReadS	Current read speed of a chunk server in bytes per second.
VSTORAGE-MIB::csIoWriteS	Current write speed of a chunk server in bytes per second.

The table below describes MDS-related objects you can monitor:

Object	Description
VSTORAGE-MIB::mdsId	Metadata server identifier.
VSTORAGE-MIB::mdsStatus	Current metadata server status.

3.3. Monitoring Acronis Cluster Objects via SNMP

Object	Description
VSTORAGE-MIB::mdsMemUsage	The amount of memory used by a metadata server.
VSTORAGE-MIB::mdsCpuUsage	The percentage of the CPU's capacity used by a metadata server.
VSTORAGE-MIB::mdsUpTime	Time since the startup of a metadata server.

The table below describes SNMP traps triggered by the specified alerts:

Trap	Alert
licenseExpired	The license has expired.
tooFewClusterFreeLogicalSpace	Too few free space is left.
tooFewClusterFreePhysicalSpace	Too few physical space is left.
tooFewNodes	Too few nodes are left.
tooFewMdses	Too few MDSs are left.
generalAlert	Other.

CHAPTER 4

Monitoring Acronis Storage Nodes

Nodes added to the Acronis Storage infrastructure are listed on the **NODES** screen, grouped by their statuses. If there are no clusters in Acronis Storage, you will only see a list of the **UNASSIGNED** nodes. If there are clusters, you can select one in the drop-down list on the left. The cluster nodes will be listed on the screen alongside the unassigned nodes.

4.1 Node Statuses

A node can have one of the following statuses:

- **HEALTHY.** All the storage services on the node are running.
- **OFFLINE.** The node cannot be reached from the management panel, although it may still be up and its services may be running.
- **FAILED.** One or more storage services on the node have failed.
- **UNASSIGNED.** The node is not assigned to a cluster.

4.2 Monitoring Node Performance

To monitor the performance of a cluster node, open the NODES screen and click the node. On the node overview screen, you will see performance statistics described below.

4.2. Monitoring Node Performance

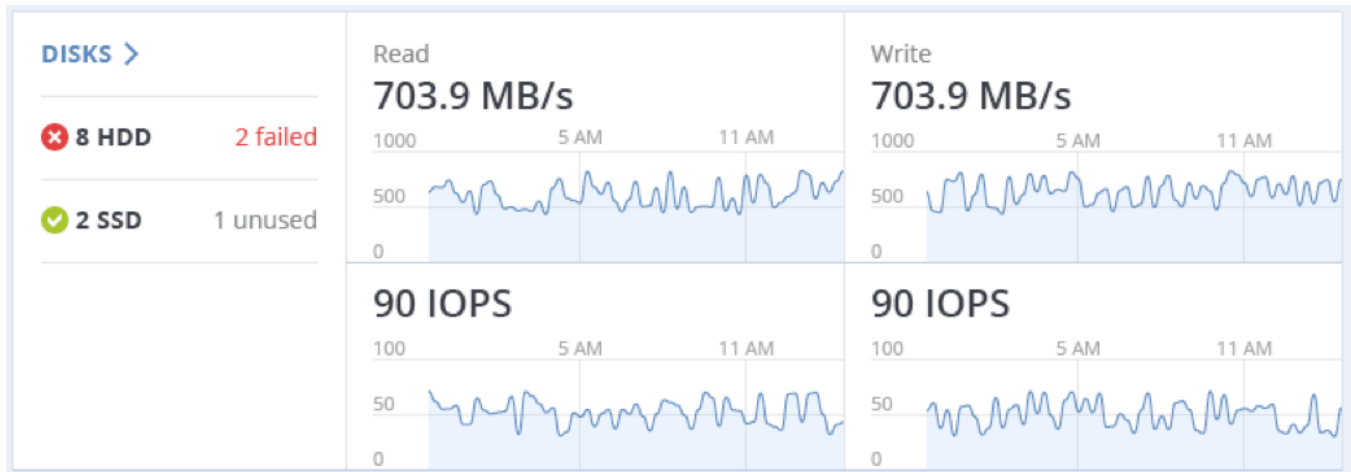
The overall statistics include:

- the number of CPUs and the amount of RAM,
- CPU usage, in percent over time,
- RAM usage, in percent over time.



The **DISKS** section shows:

- the number of HDD and SSD drives and their statuses,
- node I/O activity over time on the read and write charts.



The **NETWORK** section shows:

- the list of network interfaces and their statuses,
- the amount of transmitted (TX) and received (RX) traffic over time.



The following sections provide more information on disk and network usage.

4.2.1 Monitoring Node Disks

To monitor the usage and status of node disks, click the **DISKS** link on the node overview screen. You will see a list of all disks on the node and their status icons.

A disk status icon shows the combined status of S.M.A.R.T. and the service corresponding to the disk role. It can be one of the following:

- **Ok.** The disk and service are healthy.
- **Failed.** The service has failed or S.M.A.R.T. reported an error.
- **Releasing.** The service is being released. When the process finishes, the disk status will change to **Ok**.

On this screen, you can:

- monitor the details and performance of each disk,
- manage disk roles,
- have the disk blink its activity LED. Works only for LSI and PERC controllers.

To monitor performance of a particular disk, select it and click **Performance**. The **Drive performance** panel will display the I/O activity of the disk.

To view information about the disk, including its S.M.A.R.T. status, click **Details**.

To have the disk blink its activity LED, select the disk, and click **Blink**. To have the disk stop blinking, click **Unblink**.

4.3. Monitoring Node Network

4.2.1.1 Monitoring the S.M.A.R.T. Status of Node Disks

The S.M.A.R.T. status of all disks is monitored by a tool installed along with Acronis Storage. Run every 10 minutes, the tool polls all disks attached to nodes, including journaling SSDs and system disks, and reports the results to the management node.

Note: For the tool to work, make sure the S.M.A.R.T. functionality is enabled in node's BIOS.

If a S.M.A.R.T. warning message is shown in the node status, one of that node's disks is in pre-failure condition and should be replaced. If you continue using the disk, keep in mind that it may fail or cause performance issues.

Pre-failure condition means that at least one of these S.M.A.R.T. counters is not zero:

- Reallocated Sector Count
- Reallocated Event Count
- Current Pending Sector Count
- Offline Uncorrectable

4.3 Monitoring Node Network

To monitor the node's network usage, click **NETWORK** on the node overview screen.

To display the performance charts of a specific network interface, select it in the list and click **Performance**. When monitoring network performance, keep in mind that if the **TX DROPS** and/or **RX DROPS** charts are not empty, the network is experiencing issues and requires attention.

To display the details of a network interface, click **Details**. The **Network details** panel shows the interface state, bandwidth, MTU, MAC address, and all IP addresses.

CHAPTER 5

Viewing Acronis Storage Alerts, Audit Log, and Sending E-mail Notifications

This chapter describes Acronis Storage alerts and audit log and e-mail notifications settings.


5.1 Viewing Alerts




The **ALERTS** tab lists all the alerts logged by Acronis Storage. An alert is generated and logged each time one of the following conditions is met or events happen:



- a critical issue has happened with a cluster, its components (CS, MDS), disks, nodes, or services;
- cluster requires configuration or more resources to build or restore its health;
- network requires configuration or is experiencing issues that may affect performance;
- license is about to expire or has expired;
- cluster is about to or has run out of available space.

5.2. Viewing Audit Log

Alerts



<input type="checkbox"/>	Type	Message	Date and time	Resource	
<input checked="" type="checkbox"/>		The license isn't loaded	May 09, 2017, 3:18 AM	cluster	
<input type="checkbox"/>		Node 10.250.14.16 is offline	Jun 01, 2017, 3:55 PM	cluster	

 Details
 Ignore

To view an alert details, select an alert on the **ALERTS** tab and click **Details**.

Alerts can be ignored (deleted from the alerts list) or postponed for several hours. Postponed alerts reappear in the list after some time.

To ignore or postpone an alert, select it and click the corresponding button.

5.2 Viewing Audit Log

The **AUDIT LOG** tab lists all management operations performed by users and their activity events.

Audit log



<input type="text" value="Search"/>		Show extended details	
Date and time ↓	User	Activity	
May 16, 2017, 3:17 PM	admin	Login user	Login user "admin"
May 16, 2017, 3:13 PM	admin	Login user	Login user "admin"
May 16, 2017, 3:13 PM	admin	Login user	Login user "admin"
May 16, 2017, 3:02 PM	admin	Login user	Login user "admin"
May 15, 2017, 4:04 PM	admin	Login user	Login user "admin"
May 15, 2017, 4:04 PM	admin	Login user	Login user "admin"
May 05, 2017, 4:37 PM	admin	Assign node	Assign node "10.250...."
May 03, 2017, 4:13 PM	admin	Release node	Release node 10.250...
May 02, 2017, 6:23 PM	admin	Assign nodes to object ...	Assign node "10.250...."
May 02, 2017, 6:22 PM	admin	Assign node	Assign node "10.250...."
May 02, 2017, 12:47 PM	admin	Release node	Release node 10.250...

To view detailed information on a log entry, select it and click **Show extended details**.

5.3 Sending E-mail Notifications

Acronis Storage can send automatic e-mail notifications about errors, warnings, and alerts.

To set up e-mail notifications, do the following:

1. On the **SETTINGS > Advanced settings > EMAIL NOTIFICATIONS** tab, specify the following information:

5.3. Sending E-mail Notifications





- 1.1. In the **From** and **Sender name** fields, the notification sender's e-mail and name.
- 1.2. In the **To** field, one or more notification recipient e-mails, one per line.
- 1.3. In the **User account** fields, the credentials of the notification sender registered on the SMTP server.
- 1.4. In the **Outgoing SMTP server** field, the DNS name of the SMTP server, either public (e.g., `smtp.gmail.com`) or the one in your organization.

Note: The management node must be able to access the SMTP server.

- 1.5. If required, a custom **SMTP port** the server uses.
- 1.6. In the **Security** field, the security protocol of the SMTP server.

Advanced

LDAP/AD ENCRYPTION SNMP EMAIL NOTIFICATIONS

From <input type="text" value="user@gmail.com"/>	To <input type="text" value="user@gmail.com"/>
Sender name <input type="text" value="Acronis Storage"/>	<input type="button" value="TEST"/>
User account <input type="text" value="user"/> <input type="text" value="....."/>	Send notifications about <input checked="" type="checkbox"/>  Errors <input checked="" type="checkbox"/>  Warnings <input checked="" type="checkbox"/>  Information
Outgoing SMTP server <input type="text" value="smtp.gmail.com"/>	
SMTP port <input type="text" value="465"/>	Security <input type="text" value="SSL"/> 

2. Tick the checkboxes for alerts you want to get notified about.
3. Click **SAVE**.

To send a test e-mail, specify your e-mail registered on the SMTP server in both the **From** and **To** fields and click **TEST**.

CHAPTER 6

Exporting Acronis Storage Cluster Data

Acronis Storage allows you to export storage space as:

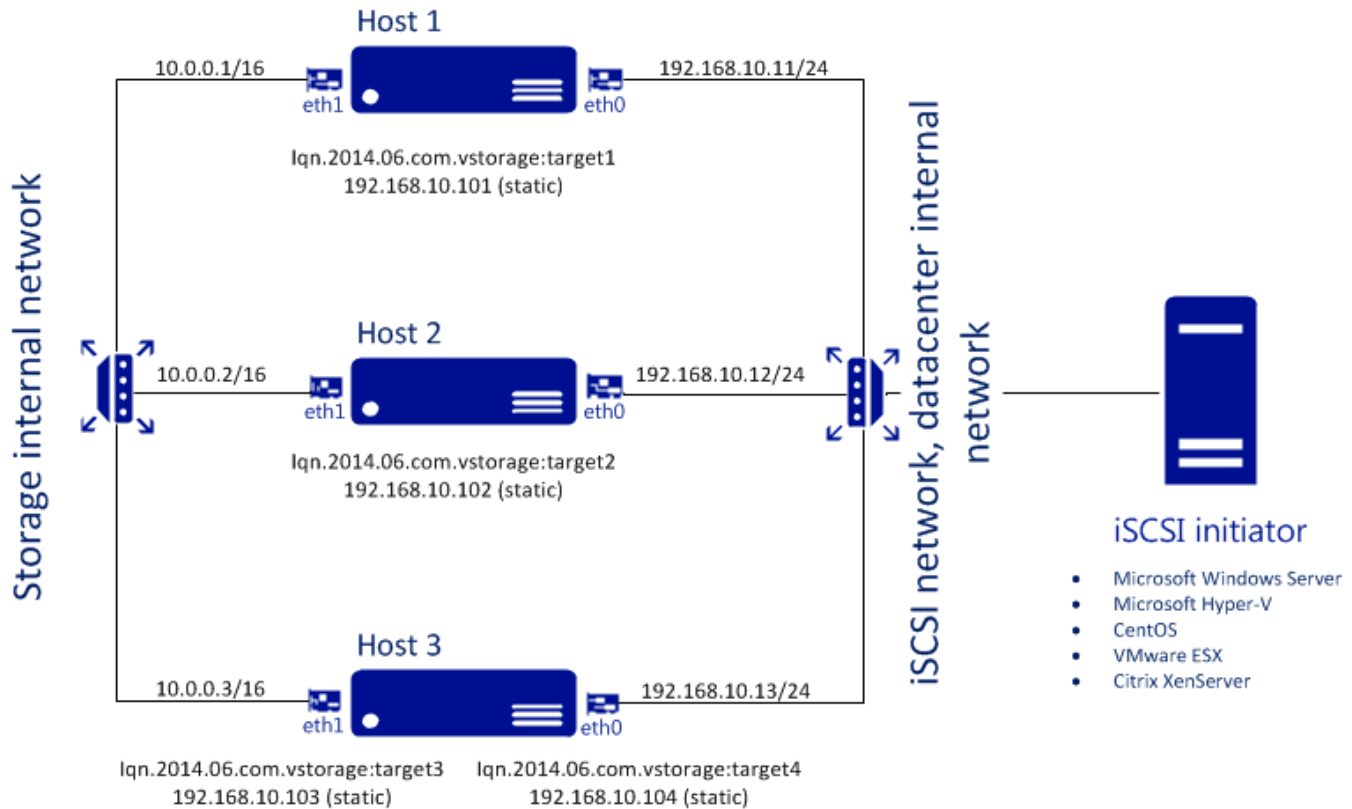
- Block storage via iSCSI for virtualization, databases and other needs.
- Object storage for storing unlimited number of files via an Amazon S3 compatible protocol. You can store data like media files, backups, Open Xchange files and access the storage using Dropbox-like applications. You can build your own Amazon S3 compatible object storage services as a part of your cloud offering or for internal needs.
- A back-end for Acronis Backup Cloud and Acronis Backup Advanced backups.
- NFS exports.

6.1 Exporting Data via iSCSI

Acronis Storage allows you to export cluster disk space to external operating systems in the form of LUN block devices over iSCSI in a SAN-like manner.

In Acronis Storage, you can create and run multiple iSCSI targets per Acronis Storage cluster node. In turn, each iSCSI target can have multiple LUNs (virtual disks). At any given moment, each iSCSI target runs on a single node. If a node fails, iSCSI targets hosted on it are moved to and re-launched on a healthy node.

The figure below shows a typical network configured for exporting Acronis Storage disk space over iSCSI.



In this example there are three hardware nodes working in an Acronis Storage cluster. Two nodes host one iSCSI target each, while the third hosts two iSCSI targets. Each node has two network connections: one internal for cluster communication and one external for iSCSI exporting. Each iSCSI target has its own static IP address assigned from the datacenter network. The iSCSI network must be properly configured to run iSCSI targets. Each iSCSI target has a unique IP address from the iSCSI subnetwork different from the host IP address. So make sure you have a range of unused IP addresses for iSCSI targets.

6.1.1 Creating Acronis Storage iSCSI Targets

Note:

1. Each iSCSI target must be assigned at least one unique IP address from DC network's static pool.
2. The name of each iSCSI target must be unique in the Acronis Storage cluster.
3. Acronis Storage iSCSI targets support persistent reservations to allow iSCSI initiators obtain exclusive access to the specified target's LUNs.

6.1. Exporting Data via iSCSI

To create and start a target, do the following:

1. On the **SERVICES > iSCSI > Targets** screen, click **ADD TARGET**.
2. On the **Add target** panel, type a name for the new target in the **Name** field.

× **Add target**

Name

target1

Node

abr-126983-wr-210

▼

☐ Enable CHAP

▼

Target portal IP address

☐ 10.250.14.150

+ Add − Remove

☒ Enable limits

IOPS:

−

100

+

Bandwidth (MB/s):

−

100

+

DONE

3. In the node drop-down list, select a node on which the target will be located. The node should have an iSCSI role assigned to one of its network interfaces to appear in the list.

4. If necessary, check the **Enable CHAP** box and select an iSCSI user in the corresponding drop-down list (For more information on CHAP users, see *Managing iSCSI Users* on page 72).
5. Click **Add** to specify one or more IP addresses for the target.
6. If necessary, enable and specify IOPS and bandwidth limits for the target. If both limits are set, the first one that is hit is applied. Setting a limit value to zero disables the limit.
7. Click **Done** to create the target.

The iSCSI target will be automatically started after creation and the initiators will be able to access the target via the specified IP address.

6.1.1.1 Performance Tips

- Spread iSCSI targets evenly across nodes in the cluster. For example, ten nodes with one iSCSI target per each will perform better than a single node with ten iSCSI targets on it.
- Fewer LUNs per more iSCSI targets will perform better than more LUNs per fewer iSCSI targets.

6.1.2 Listing, Stopping, and Deleting Acronis Storage iSCSI Targets


On the iSCSI targets screen, you can list and manage all iSCSI targets and their LUNs, and display detailed information about specific iSCSI targets registered on a node.

To stop or delete an iSCSI target, select it on the iSCSI targets screen and click **Stop** or **Delete**, respectively. Doing so will disconnect the iSCSI initiator from the target. However, breaking the connection in such a way may result in I/O errors on the iSCSI initiator's side.

6.1.3 Configuring Acronis Storage iSCSI Targets

To configure an iSCSI target, do the following:


1. On the **SERVICES > iSCSI > Targets** screen, select the necessary target and click **Configure**.
2. On the **Configure** target screen, specify the necessary parameters.

 **Configure target**



IQN

Node

☐ Enable CHAP





Target portal IP address



 Add  Remove

☒ Enable limits

IOPS:

Bandwidth (MB/s):

DONE

3. Click **Done**.

6.1.3.1 Listing LUNs

In Acronis Storage, each iSCSI target can have multiple LUNs (virtual disks or volumes). You can list the LUNs of a target and iSCSI initiators that are currently connected.

To list the LUNs, open the **SERVICES > iSCSI > Targets** screen, select a target and click a link in the **LUNs** column.

To list the initiators that are currently connected to iSCSI targets, open the **INITIATORS** tab on the same screen.

6.1.3.2 Adding LUNs

To add a LUN to an iSCSI target, do the following:

- 1. On the **SERVICES > iSCSI > Targets** screen, select the necessary target and click a link in the **LUNs** column.

ISCSI targets

<div><div></div><div>Search</div></div>				
IQN	State	LUNs	Initiators	
iqn.2014.06.com.vstorage:tar...	running	1	0	10.90.100.118

- 2. To add a new LUN to the list, click **ADD LUN**.

×

Add LUN

LUN

1

▼

LUN size

−

20

+

GB

Tier 0

▼

☒

Data redundancy:

☒ Erasure coding

☐ Replication

Failure domain:

Disk

▼

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

3. On the **Add LUN** screen, select the LUN's number from the drop-down list.
4. In the **LUN Size** field, specify the size of the LUN in GB; select a tier from the drop-down list to the right.
For more information on tiers, see **Understanding Storage Tiers** in the *Acronis Storage Installation Guide*.
5. From the **Failure domain** drop-down list, choose a placement policy for replicas. For more details, see **Understanding Failure Domains** in the *Acronis Storage Installation Guide*.

6. Choose a data redundancy mode. For more details, see **Understanding Data Redundancy** in the *Acronis Storage Installation Guide*.
7. Click **Done**.

6.1.3.3 Configuring LUNs

To configure a LUN of an iSCSI target, do the following:

1. On the **SERVICES > iSCSI > Targets** screen, stop the target to which the LUN belongs.
2. Click a link in the target's **LUNs** column.
3. On the **Configure LUN** screen, specify the LUN size in the corresponding field.
4. Click **Done**.

6.1.3.4 Deleting LUNs

To delete a LUN, do the following:

1. On the **SERVICES > iSCSI > Targets** screen, select the necessary target and click a link in the **LUNs** column.
2. Select the necessary LUN in the list and click **Delete**.

6.1.4 Managing iSCSI Users

6.1.4.1 Creating CHAP Accounts for Acronis Storage iSCSI Targets

To create a CHAP account, do the following:

1. On the **SERVICES > iSCSI Users** screen, click **Add user**.
2. Specify login, password, and, if necessary, a description for the account. The password should be 12 to 16 characters long for Windows clients to be able to establish connections.

✕ Add user

Login
user1

Password
••••••

Description
A new CHAP user.

☒ Enabled

Done

3. Click **Done**.

The newly created CHAP user account will be listed on the **iSCSI Users** screen.

6.1.4.2 Creating Acronis Storage iSCSI Targets Bound to CHAP Accounts

To create an Acronis Storage iSCSI target bound to a CHAP account, do the following:

1. On the **SERVICES > iSCSI > Targets** screen, select an iSCSI target and click **Configure**.
2. On the **Configure** target screen, check **Enable CHAP** and/or **Enable mutual CHAP** and select users in the corresponding drop-down lists. If you enable CHAP, the target will authenticate the initiator. If you enable mutual CHAP, the initiator will authenticate the target. These options can be enabled in any combination.

× **Configure target**

IQN

Node

☒ **Enable CHAP**

▼

user1

user2

+ Add

− Remove

DONE

3. Click **Done**.

6.1.4.3 Changing CHAP Account Passwords

To change the password of a CHAP account, do the following:

1. On the **SERVICES > iSCSI Users** screen, select a user and click **Configure**.
2. In the **Password** section on the **Configure** user screen, click change.

✕ Configure user

Login
user1

Password
[change](#)

Description
A new CHAP user.

☒ Enabled

Done

3. Type a new password in the corresponding field and click **Done**. The password should be 12 to 16 characters long for Windows clients to be able to establish connection.

The new password will become active after target reboot.

6.2 Exporting Data via S3

Acronis Storage allows you to export cluster disk space to customers in the form of an S3-like object-based storage.

Acronis Storage is implemented as an Amazon S3-like API, which is one of the most common object storage APIs. End users can work with Acronis Storage as they work with Amazon S3. You can use the usual applications for S3 and continue working with it after the data migration from Amazon S3 to Acronis Storage.

Object storage is a storage architecture that enables managing data as objects (like in a key-value storage) as opposed to files on file systems or blocks in a block storage. Except for the data, each object has metadata

that describes it as well as a unique identifier that allows finding the object in the storage. Object storage is optimized for storing billions of objects, in particular for application storage, static web content hosting, online storage services, big data, and backups. All of these uses are enabled by object storage thanks to a combination of very high scalability and data availability and consistency.

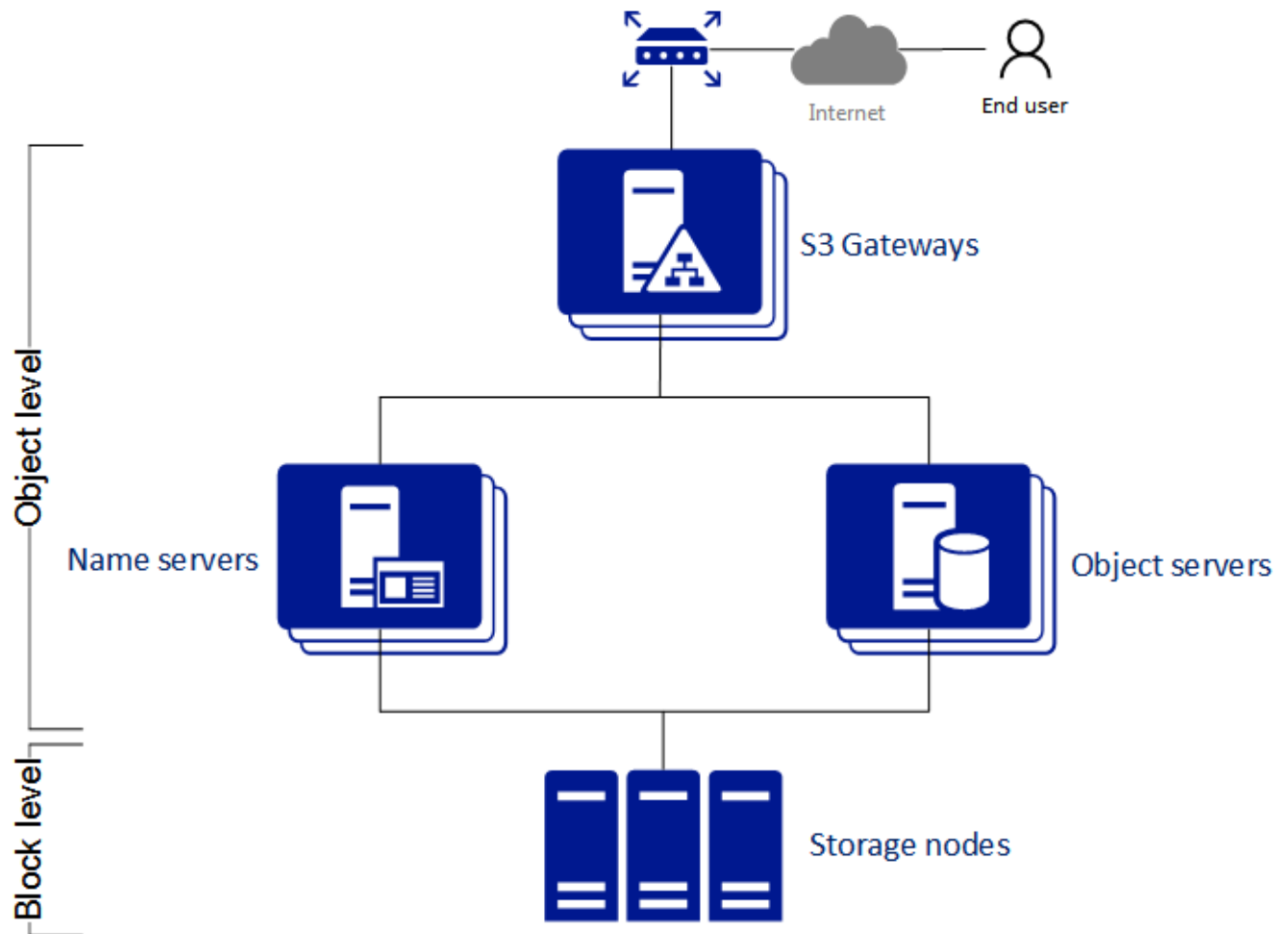
Compared to other types of storage, the key difference of object storage is that parts of an object cannot be modified, so if the object changes a new version of it is spawned instead. This approach is extremely important for maintaining data availability and consistency. First of all, changing an object as a whole eliminates the issue of conflicts. That is, the object with the latest timestamp is considered to be the current version and that is it. As a result, objects are always consistent, i.e. their state is relevant and appropriate.

Another feature of object storage is eventual consistency. Eventual consistency does not guarantee that reads are to return the new state after the write has been completed. Readers can observe the old state for an undefined period of time until the write is propagated to all the replicas (copies). This is very important for storage availability as geographically distant data centers may not be able to perform data update synchronously (e.g., due to network issues) and the update itself may also be slow as awaiting acknowledges from all the data replicas over long distances can take hundreds of milliseconds. So eventual consistency helps hide communication latencies on writes at the cost of the probable old state observed by readers. However, many use cases can easily tolerate it.

6.2.1 Object Storage Infrastructure Overview

The infrastructure of the object storage consists of the following entities: object servers (OS), name servers (NS), and the S3 gateways (GW).

These entities run as services on the Acronis Storage nodes. Each service should be deployed on multiple Acronis Storage nodes for high availability.



- An object server stores actual object data received from S3 gateway, packed into special containers to achieve high performance. The containers are redundant, you can specify the redundancy mode while configuring object storage.
- A name server stores information about objects (metadata) received from the S3 gateway. Metadata includes object name, size, ACL, location, owner, and such.
- S3 gateway is a data proxy between object servers and users. It receives and handles Amazon S3 protocol requests and uses nginx web server for external connections. S3 gateway handles S3 user authentication and ACL checks. It has no data of its own (i.e. is stateless).

6.2.2 Planning the S3 Cluster

Before creating an S3 cluster, do the following:

1. Define which nodes of the Acronis Storage cluster will run the S3 storage access point services. It is recommended to have all nodes available in Acronis Storage run these services.
2. Configure the network so that the following is achieved:
 - All components of the S3 cluster communicate with each other via the S3 private network. All nodes of an S3 cluster must be connected to the S3 private network. Acronis Storage internal network can be used for this purpose.
 - The nodes running S3 gateways must have access to the public network.
 - The public network for the S3 gateways must be balanced by an external DNS load balancer.

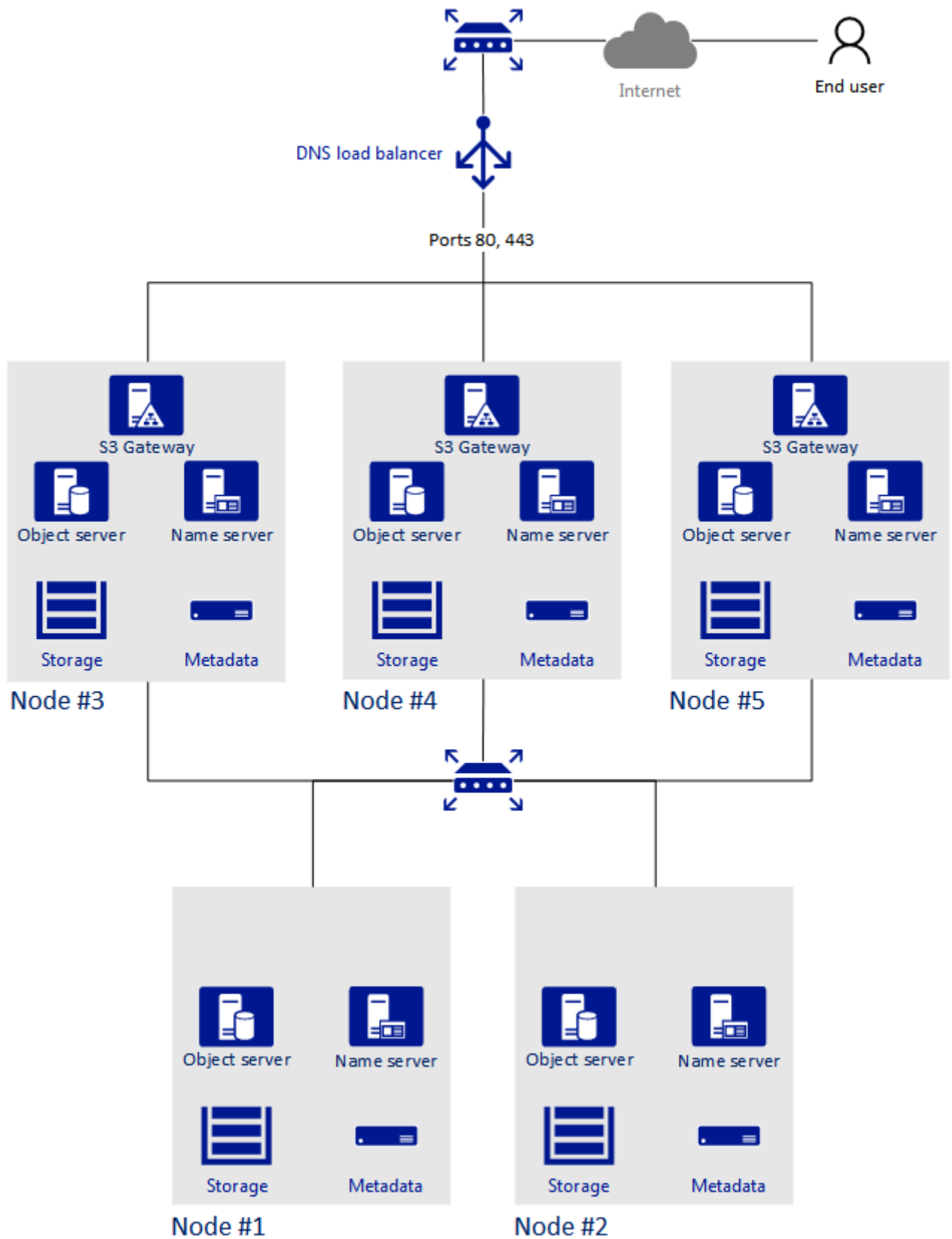
For more details on network configuration, refer to **Planning Network** in the *Acronis Storage Installation Guide*.

3. All components of the S3 cluster should run on multiple nodes for high-availability. Name server and object server components in the S3 cluster are automatically balanced and migrated between S3 nodes. S3 gateways are not automatically migrated; their high availability is based on DNS records. You should maintain the DNS records manually when adding or removing the S3 gateways.

6.2.3 Sample Object Storage

This section shows a sample object storage deployed on top of an Acronis Storage cluster of five nodes that run various services. The final setup is shown on the figure below.

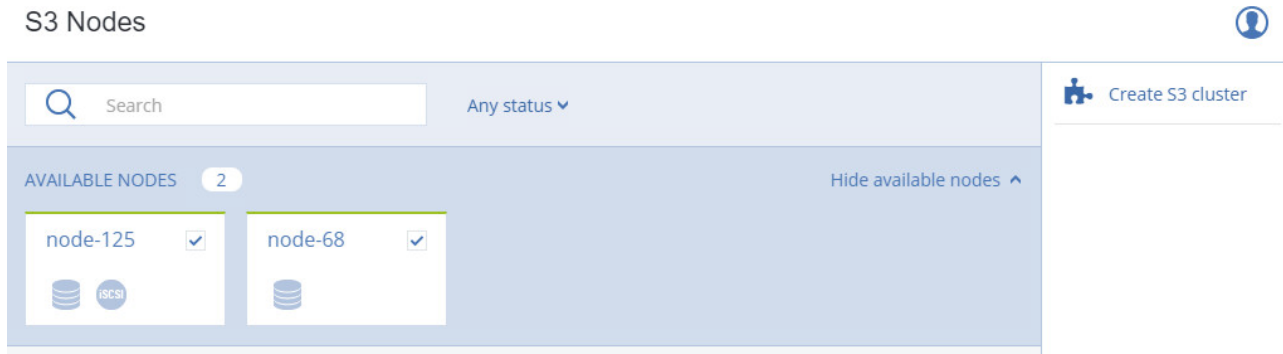
6.2. Exporting Data via S3



6.2.4 Creating the S3 Cluster

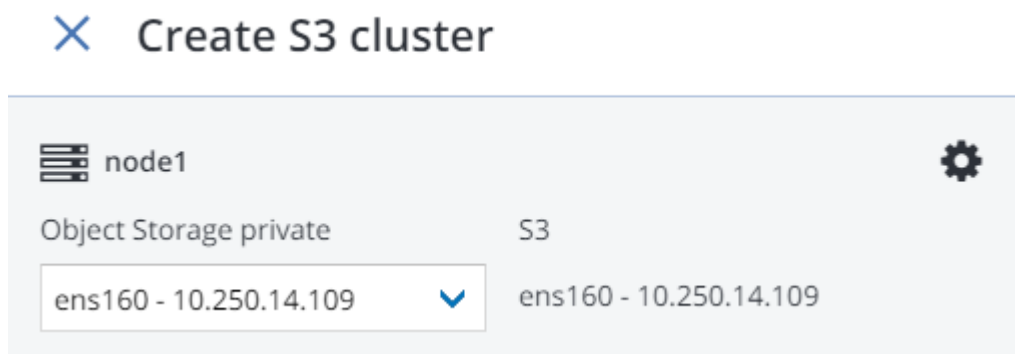
To set up object storage services on a cluster node, do the following:

1. Make sure that S3 private network is configured on each node that will run object storage services.
2. On the **SERVICES > Nodes** screen, check the box of each cluster node where object storage services will run.



3. Click **Create S3 cluster**.
4. Make sure a network interface with an **Object Storage private** role is selected in the drop-down list. The corresponding interfaces with S3 public roles will be selected automatically.

Note: If necessary, click the cogwheel icon and, on the **Network Configuration** screen, configure S3 roles.



5. Click **Proceed**.
6. In **Tier**, select the storage tier that will be used for the object storage. For information about storage

6.2. Exporting Data via S3

tiers, consult **Understanding Storage Tiers** in the *Acronis Storage Installation Guide*.

7. In **Failure domain**, choose a placement policy for replicas. For more details, see **Understanding Failure Domains** in the *Acronis Storage Installation Guide*.
8. In **Data redundancy**, select the redundancy mode that the object storage will use. For more details, see **Understanding Data Redundancy** in the *Acronis Storage Installation Guide*.

✕ Volume parameters


Tier:	
<div>Tier 0</div>	
Data redundancy:	Failure-domain:
<input checked="" type="radio"/> Erasure coding	<div>Disk</div>
Encoding 1+0	0% overhead
Encoding 1+2	200% overhead
Encoding 3+2	67% overhead
Encoding 5+2	40% overhead
Encoding 7+2	29% overhead
Encoding 17+3	18% overhead
<div>Done</div>	

Note: You can later change the redundancy mode on the **S3 > Settings** panel.


9. Click **Proceed**.
10. Specify the external (publicly resolvable) DNS name for the S3 endpoint that will be used by the end users to access the object storage. For example, `mys3storage.example.com`. Click **Proceed**.

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

11. From the drop-down list, select an S3 endpoint protocol: HTTP, HTTPS or both.

 **Protocols**


S3 endpoint protocols:

HTTPS and HTTP 

Endpoint URLs:

`http://s3com.ru/bucketname/objectname`

`https://s3com.ru/bucketname/objectname`

 It is not recommended to use HTTP for production deployments

☐ Generate self-signed certificate

SSL certificate:

Upload new

Valid

DONE

6.2. Exporting Data via S3

Note: It is recommended to use only HTTPS for production deployments.

If you have selected HTTPS, do one of the following:

- Check **Generate self-signed certificate** to get a self-signed certificate for HTTPS evaluation purposes.

Note:

1. S3 geo-replication requires a certificate from a trusted authority. It does not work with self-signed certificates.
2. To access the data in the S3 cluster via a browser, add the self-signed certificate to browser's exceptions.

- Acquire a key and a trusted wildcard SSL certificate for endpoint's bottom-level domain. For example, the endpoint `s3.storage.example.com` would need a wildcard certificate for `*.s3.storage.example.com` with the subject alternative name `s3.storage.example.com`.

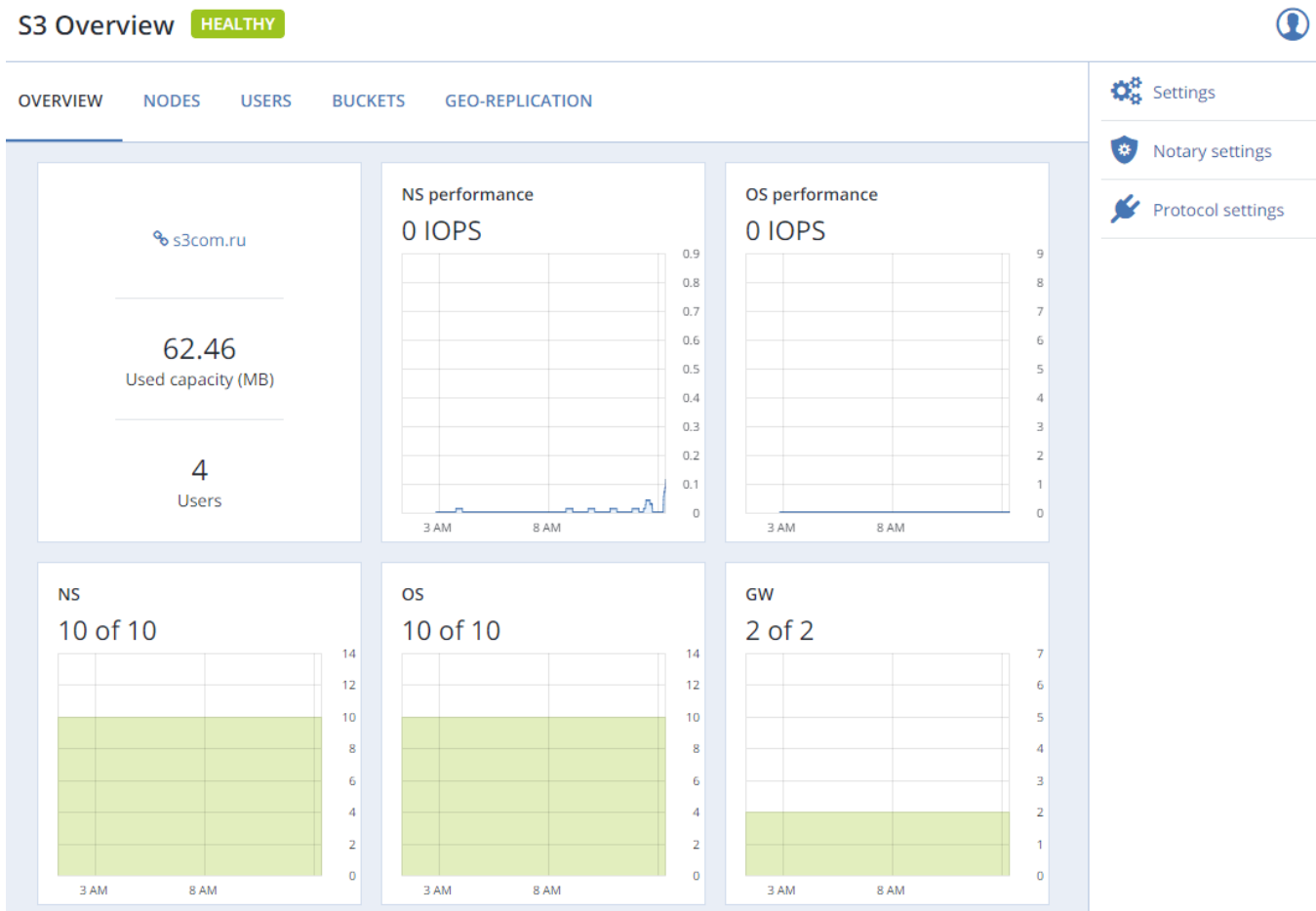
Upload the certificate, and, depending on the certificate type, do one of the following:

- in case the certificate is contained in a PKCS#12 file, specify the passphrase;
- upload the SSL key.

12. If required, click **Configure Acronis Notary** and specify **Notary DNS name** and **Notary user key**. For more information on Acronis Notary, see **Managing Acronis Notary in Buckets**.

13. Click **Done** to create an S3 cluster.

After the cluster is created, on the **S3 Overview** screen, you can view cluster status, hostname, used disk capacity, the number of users, I/O activity, and the state of S3 services.



To check if the S3 cluster is successfully deployed and can be accessed by users, visit https://<S3_DNS_name> or http://<S3_DNS_name> in your browser. You should receive the following XML response:

```
<Error>
<Code>AccessDenied</Code>
<Message/>
</Error>
```

To start using the S3 storage, you will also need to create at least one S3 user.

6.2.5 Managing Object Storage Users

The concept of S3 user is one of the base concepts of object storage along with those of object and bucket (container for storing objects). The Amazon S3 protocol uses a permission model based on access control lists (ACLs) where each bucket and each object is assigned an ACL that lists all users with access to the given resource and the type of this access (read, write, read ACL, write ACL). The list of users includes the entity

6.2. Exporting Data via S3

owner assigned to every object and bucket at creation. The entity owner has extra rights compared to other users. For example, the bucket owner is the only one who can delete that bucket.

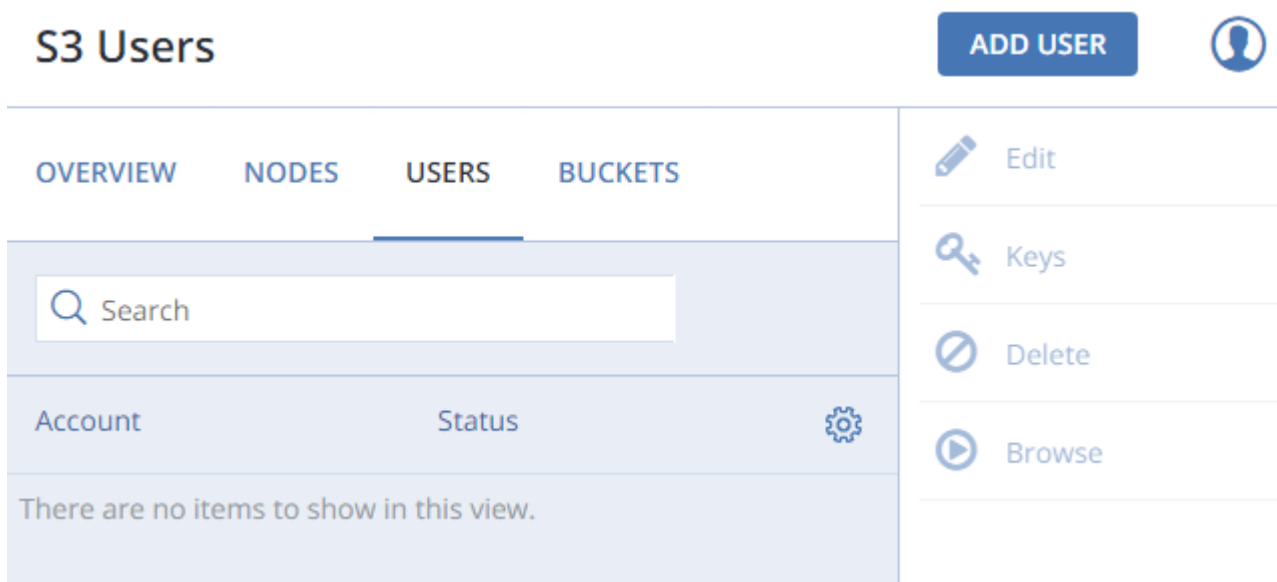
User model and access policies implemented in Acronis Storage comply with the Amazon S3 user model and access policies.

User management scenarios in Acronis Storage are largely based on the Amazon Web Services user management and include the following operations: create, query, and delete users as well as generate and revoke user access key pairs.

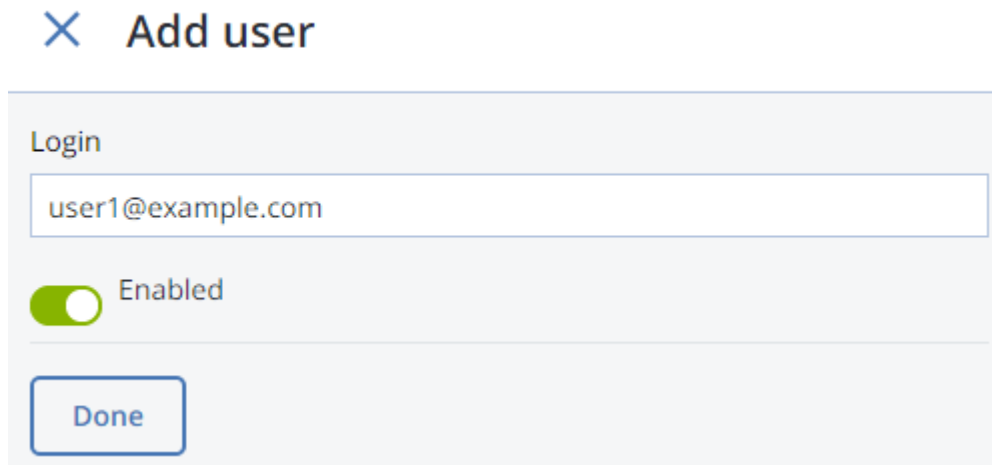
6.2.5.1 Adding S3 users

To add an S3 user, do the following:

1. On the **SERVICES > S3 Users** screen, click **Add user**.



2. Specify a valid email address as login for the user and click **Done**.



×

Add user

Login

user1@example.com

☒ Enabled

Done

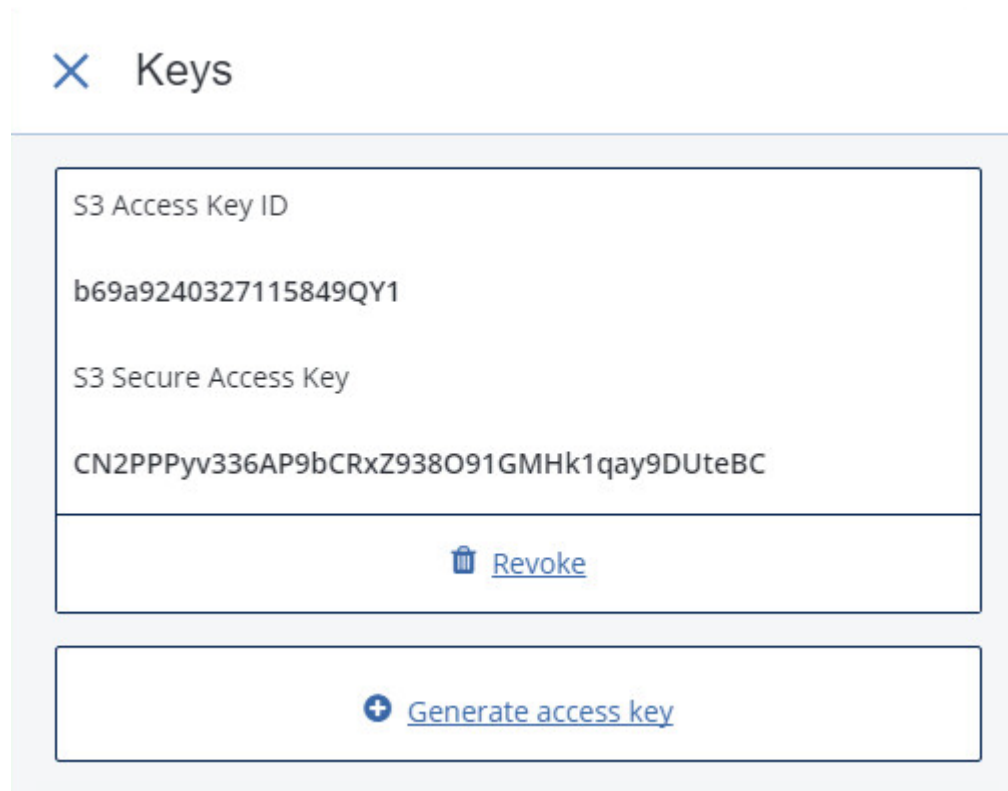
6.2.5.2 Managing S3 Access Key Pairs

Each S3 user has one or two key pairs (access key and secret key) for accessing the S3 cloud. You can think of the access key as login and the secret key as password. (For more information about S3 key pairs, refer to <http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSGettingStartedGuide/AWSCredentials.html>.) The access keys are generated and stored locally in the Acronis Storage cluster on S3 name servers. Each user can have up to two key pairs. It is recommended to periodically revoke old and generate new access key pairs.

To view, add, or revoke the S3 access key pairs for an S3 user, do the following:

1. Select a user in the list and click **Keys**.

6.2. Exporting Data via S3



2. The existing keys will be shown on the **Keys** panel.

- To revoke a key, click **Revoke**.
- To add a new key, click **Generate access key**.

To access a bucket, a user will need the following information:

- management panel IP address,
- DNS name of the S3 cluster specified during configuration,
- S3 access key ID,
- S3 secret access key,
- SSL certificate if the HTTPS protocol was chosen during configuration.

Note: The certificate file can be found in the `/etc/nginx/ssl/` directory on any node hosting the S3 gateway service.

To automatically log in to S3 with user credentials using the generated keys, select a user and click **Browse**.

Note: To **Browse** using an SSL certificate, make sure it is valid or, in case of a self-signed one, add it to browser's exceptions.

6.2.6 Managing Object Storage Buckets

All objects in Amazon S3-like storage are stored in containers called buckets. Buckets are addressed by names that are unique in the given object storage, so an S3 user of that object storage cannot create a bucket that has the same name as a different bucket in the same object storage. Buckets are used to:

- group and isolate objects from those in other buckets,
- provide ACL management mechanisms for objects in them,
- set per-bucket access policies, for example, versioning in the bucket.

In the current version of Acronis Storage, you can enable and disable Acronis Notary for object storage buckets and monitor the space used by them on the **SERVICES > S3 > Buckets** screen. You cannot create and manage object storage buckets from Acronis Storage management panel. However, you can do it via the Acronis Storage user panel or by using a third-party application. For example, the applications listed below allow you to perform the following actions:

- CyberDuck: create and manage buckets and their contents.
- MountainDuck: mount object storage as a disk drive and manage buckets and their contents.
- Backup Exec: store backups in the object storage.

6.2.6.1 Listing Bucket Contents

You can list bucket contents with a web browser. To do this, visit the URL that consists of the external DNS name for the S3 endpoint that you specified when creating the S3 cluster and the bucket name. For example, `mys3storage.example.com/mybucket`.

Note: You can also copy the link to bucket contents by right-clicking it in CyberDuck, and then selecting Copy URL.

6.2. Exporting Data via S3

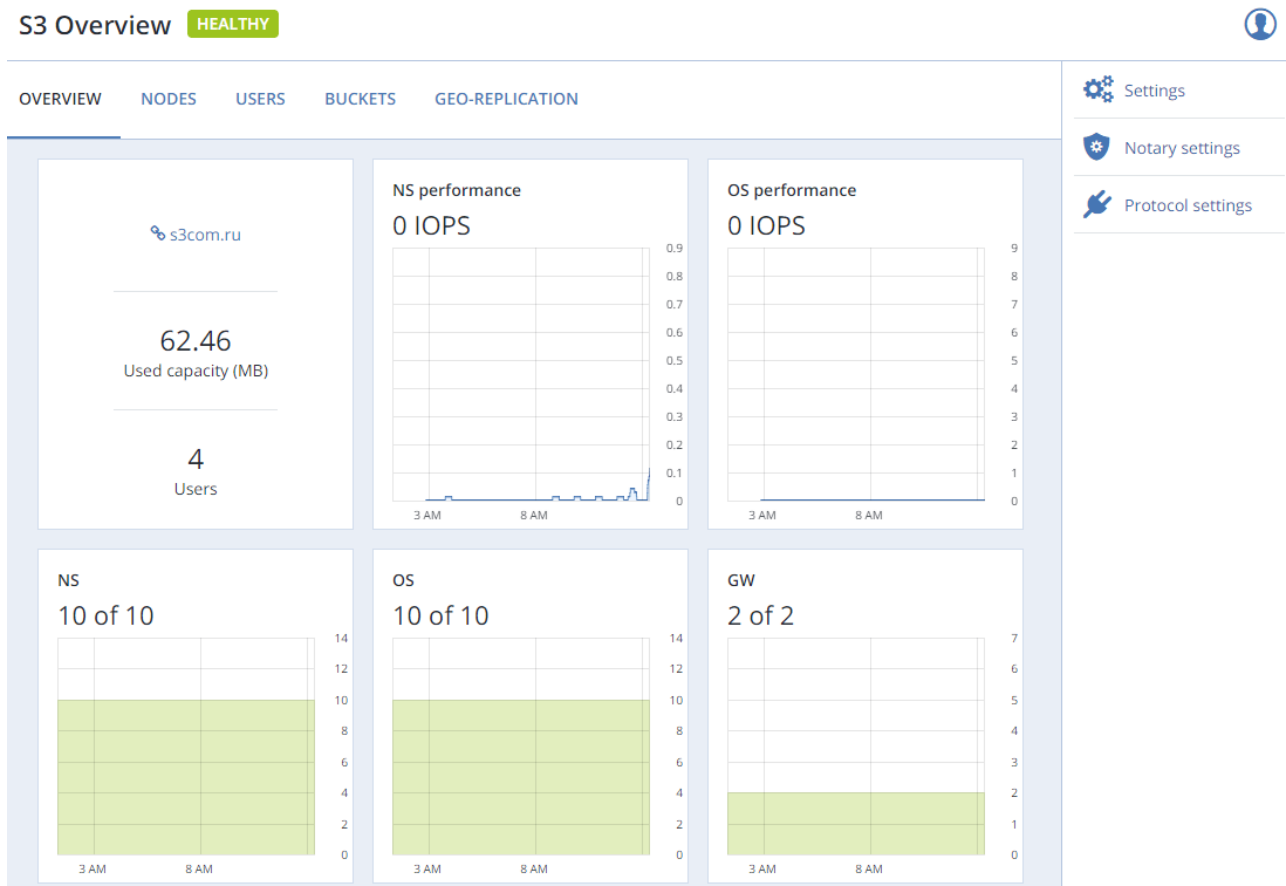
6.2.6.2 Managing Acronis Notary in Buckets

Acronis Storage offers integration with the Acronis Notary service to leverage blockchain notarization and ensure the immutability of data saved in object storage clusters. To use Acronis Notary in user buckets, you need to set it up in the S3 cluster and enable it for said buckets.


Setting Up Acronis Notary

To set up Acronis Notary, do the following:

1. Get the DNS name and the user key for the notary service from your Acronis sales contact.
2. On the **SERVICES > S3** screen, click **Notary settings**.



3. On the **Notary Settings** screen, specify the DNS name and user key in the respective fields and click **Done**.

 **Notary Settings**

Notary DNS name

Notary User Key

Done

Enabling and Disabling Acronis Notary

To enable or disable blockchain notarization for a bucket, select a bucket on the **SERVICES > S3 > Buckets** screen and click **Enable Notary** or **Disable Notary**, respectively.

Notarization is disabled for new buckets by default.

Note: Once you enable notarization for a bucket, certificates are created automatically only for the newly uploaded files. The previously uploaded files are left unnotarized. Once a file was notarized, it will remain notarized even if you disable notarization later.

6.2.7 Best Practices for Using S3 in Acronis Storage

This section offers recommendations on how to best use the S3 feature of Acronis Storage.

6.2.7.1 Bucket and Key Naming Policies

It is recommended to use bucket names that comply with DNS naming conventions:

- can be from 3 to 63 characters long,
- must start and end with a lowercase letter or number,

6.2. Exporting Data via S3

- can contain lowercase letters, numbers, periods (.), hyphens (-), and underscores (_),
- can be a series of valid name parts (described previously) separated by periods.

An object key can be a string of any UTF-8 encoded characters up to 1024 bytes long.

6.2.7.2 Improving Performance of PUT Operations

Object storage supports uploading of objects as large as 5 GB in size with a single PUT request, or 5 TB in size with multipart upload. Upload performance can be improved, however, by splitting large objects into pieces and uploading them concurrently with multipart upload API. This approach will divide the load between multiple OS services.

It is recommended to use multipart uploads for objects larger than 5 MB.

6.2.8 Replicating Data Between Geographically Distributed Datacenters with S3 Clusters

Acronis Storage can store replicas of S3 cluster data and keep them up-to-date in multiple geographically distributed datacenters with S3 clusters based on Acronis Storage. Geo-replication reduces the response time for local S3 users accessing the data in a remote S3 cluster or remote S3 users accessing the data in a local S3 cluster as they do not need to have an Internet connection.

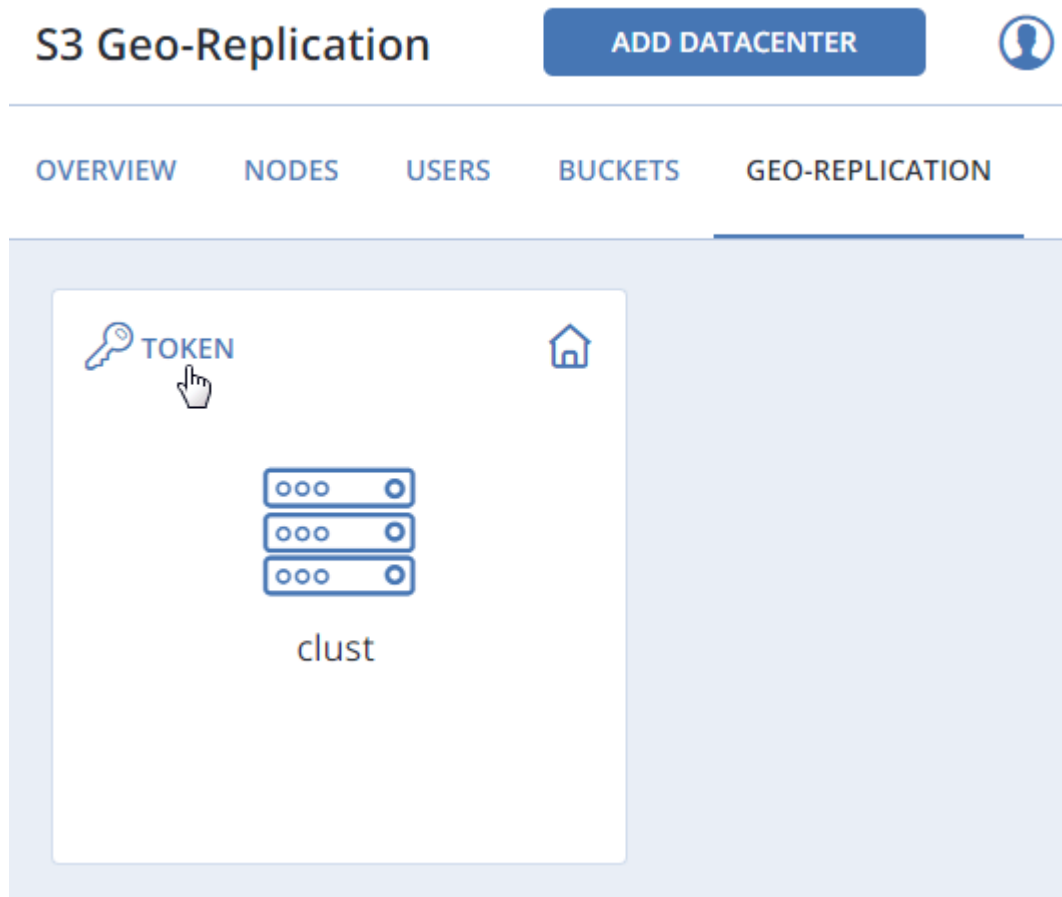
Geo-replication schedules the update of the replicas as soon as any data is modified. Geo-replication performance depends on the speed of Internet connection, the redundancy mode, and cluster performance.

If you have multiple datacenters with enough free space, it is recommended to set up geo-replication between S3 clusters residing in these datacenters.


Important: Each cluster must have its own SSL certificate signed by a global certificate authority.

To set up geo-replication between S3 clusters, exchange tokens between datacenters as follows:

1. In the management panel of a remote datacenter, open the **SERVICES > S3 > GEO-REPLICATION** screen.



2. In the section of the home S3 cluster, click **TOKEN** and, on the **Get token** panel, copy the token.
3. In the management panel of the local datacenter, open the **SERVICES > S3 > GEO-REPLICATION** screen and click **ADD DATACENTER**.

 **Add datacenter**

Insert here the token received at another datacenter to make replication between them:

Token

`eyJ1c2VyX3NIY3JldF9rZXkiOiAiaUN2YUt0SzR2MkIjFbUN2cUxIRE0yRnNZVm53UmlsZFB1clU0S2hhUCIsICJ1aWQiOiAiMzY0MTc1MjFjMmJmZDNiZCIsICJpc19zZWxmljogdHJ1ZSwgInVyYbCl6ICJodHRwczovL3MzY29tLnJ1OjQ0MyIsICJ1c2VyX2tleV9pZCI6ICJiM2NhMjFjMjU3Yjk2Y2U5VlhVNCl6ICJyZWZkYWJsZV9uYW1lIjogIm15X2NsdXN0In0=`

ADD

4. Enter the copied token and click **Done**.
5. Configure the remote Acronis Storage S3 cluster the same way.

6.2.9 Monitoring S3 Access Points

The S3 monitoring screen enables you to inspect the availability of each S3 component as well as the performance of NS and OS services (which are highly available).

If you see that some of the NS or OS services are offline, it means that the S3 access point does not function properly, and you should contact support consult the CLI guide for low-level troubleshooting. S3 gateways are not highly available, but DNS load balancing should be enough to avoid downtime if the gateway fails.

The performance charts represent the number of operations that the OS/NS services are performing.

6.2.10 Releasing Nodes from S3 Clusters

Before releasing a node, make sure that the cluster has enough nodes running the Name Server, Object Server, and S3 Gateway services left.

Warning: When the last node in the S3 cluster is removed, the cluster is destroyed, and all the data is deleted.

To release a node from an S3 cluster, do the following:

1. On the **SERVICES > S3 Nodes** screen, check the box of the node to release.
2. Click **Release**.

6.2.11 Supported Amazon S3 Features

This section lists Amazon S3 operations, headers, and authentication schemes supported by the Acronis Storage implementation of the Amazon S3 protocol.

6.2.11.1 Supported Amazon S3 REST Operations

The following Amazon S3 REST operations are currently supported by the Acronis Storage implementation of the Amazon S3 protocol:

Supported service operations:

- GET Service

Bucket operations:

Operation	Supported
DELETE/HEAD/PUT Bucket	Yes
GET Bucket (List Objects)	Yes (only version 1)
GET/PUT Bucket acl	Yes
GET Bucket location	Yes (returns US East)
GET Bucket Object versions	Yes
GET/PUT Bucket versioning	Yes
List Multipart Uploads	Yes
DELETE/GET/PUT Bucket analytics	No
DELETE/GET/PUT Bucket cors	No
DELETE/GET/PUT Bucket inventory	No
DELETE/GET/PUT Bucket lifecycle	No

6.2. Exporting Data via S3

Operation	Supported
DELETE/GET/PUT Bucket metrics	No
DELETE/GET/PUT Bucket policy	No
DELETE/GET/PUT Bucket replication	No
DELETE/GET/PUT Bucket tagging	No
DELETE/GET/PUT Bucket website	No
GET/PUT Bucket accelerate	No
GET/PUT Bucket logging	No
GET/PUT Bucket notification	No
GET/PUT Bucket requestPayment	No
List Bucket Analytics Configurations	No
List Bucket Inventory Configurations	No
List Bucket Metrics Configurations	No

Object operations:

Operation	Supported
DELETE/GET/HEAD/POST/PUT Object	Yes
Delete Multiple Objects	Yes
PUT Object - Copy	Yes
GET/PUT Object acl	Yes
Delete Multiple Objects	Yes
Abort Multipart Upload	Yes
Complete Multipart Upload	Yes
Initiate Multipart Upload	Yes
List Parts	Yes
Upload Part	Yes
Upload Part - Copy	No
DELETE/GET/PUT Object tagging	No
GET Object torrent	No
OPTIONS Object	No
POST Object restore	No

Note: For more information on Amazon S3 REST operations, see [Amazon S3 REST API documentation](#).

6.2.11.2 Supported Amazon Request Headers

The following Amazon S3 REST request headers are currently supported by the Acronis Storage implementation of the Amazon S3 protocol:

- Authorization
- Content-Length
- Content-Type
- Content-MD5
- Date
- Host
- x-amz-content-sha256
- x-amz-date
- x-amz-security-token

The following Amazon S3 REST request headers are ignored:

- Expect
- x-amz-security-token

Note: For more information on Amazon S3 REST request headers, see [Amazon S3 REST API Common Request Headers](#).

6.2.11.3 Supported Amazon Response Headers

The following Amazon S3 REST response headers are currently supported by the Acronis Storage implementation of the Amazon S3 protocol:

- Content-Length

6.2. Exporting Data via S3

- Content-Type
- Connection
- Date
- ETag
- x-amz-delete-marker
- x-amz-request-id
- x-amz-version-id

The following Amazon S3 REST response headers are not used:

- Server
- x-amz-id-2

Note: For more information on Amazon S3 REST response headers, see [Amazon S3 REST API Common Response Headers](#).

6.2.11.4 Supported Amazon Error Response Headers

The following Amazon S3 REST error response headers are currently supported by the Acronis Storage implementation of the Amazon S3 protocol:

- Code
- Error
- Message
- RequestId
- Resource

The following Amazon S3 REST error response headers are not supported:

- RequestId (not used)
- Resource

Note: For more information on Amazon S3 REST response headers, see [Amazon S3 REST API Error Response Headers](#).

6.2.11.5 Supported Authentication Scheme and Methods

The following authentication scheme is supported by the Acronis Storage implementation of the Amazon S3 protocol:

- [Signature Version 2](#).
- [Signature Version 4](#).

The following authentication methods is supported by the Acronis Storage implementation of the Amazon S3 protocol:

- [HTTP Authorization header](#).
- [Query string parameters](#).

6.3 Exporting Data via NFS

Acronis Storage allows you to organize nodes into a highly available NFS cluster in which you can create NFS shares. In Acronis Storage terms, an NFS share is an access point for a volume and as such it can be assigned an IP address or DNS name. The volume, in turn, can be assigned the usual properties: redundancy type, tier, and failure domain. In each share you can create multiple NFS exports which are actual exported directories for user data. Each export has, among other properties, a path that, combined with share's IP address, uniquely identifies the export on the network and allows you to mount it using standard commands.

On the technical side, NFS volumes are based on object storage. Aside from offering high availability and scalability, object storage eliminates the limit on the amount of files and the size of data you can keep in the NFS cluster. Each share is perfect for keeping billions of files of any size. However, such scalability implies IO overhead that is wasted on file size changes and rewrites. For this reason, an Acronis Storage NFS cluster makes a perfect cold and warm file storage but is not recommended for hot and high performance, often rewritten data (like running virtual machines). Integration of Acronis Storage with solutions from VMware, for example, is best done via iSCSI to achieve better performance.

6.3. Exporting Data via NFS

Note: Acronis Storage only supports NFS version 4 and newer, including pNFS.

6.3.1 Setting Up an NFS Cluster

Since NFS is based on object storage, creating an NFS cluster is similar to creating an S3 one. Do the following:

1. Assign the internal **Object Storage private** role and the public **NFS** role to a network interface on each node that will be in the NFS cluster. You can do so on the **NODES > node > NETWORK** screen.
2. On the **SERVICES > NFS** screen, select the desired available nodes to add to the NFS cluster.
3. Click **Create NFS cluster**.
4. Make sure that the network interface with the **Object Storage private** role is selected in the drop-down list of each node. The corresponding interfaces with the public **NFS** roles will be selected automatically.

Note: If necessary, click the cogwheel icon and configure NFS roles on the **Network Configuration** screen.

5. Click **CREATE**.

After the NFS cluster has been created, you can proceed to creating NFS shares.

6.3.2 Creating NFS Shares

To create an NFS share, do the following:

1. On the **SERVICES > NFS > SHARES** screen, click **ADD NFS SHARE**.
2. On the **Add NFS Share** panel, specify a unique name and an IP address, which must be unused and, if authentication is enabled, domain-resolvable. Click **PROCEED**.
3. In **Share size**, specify the size of the share in gigabytes. For users accessing exports, this value will be the filesystem size.
4. Select the desired tier, failure domain, and data redundancy type in the corresponding fields. For more details on these volume properties, see the *Acronis Storage Installation Guide*.

Note: You will be able to change the redundancy mode later.

5. Click **DONE**.

After the share has been created, you can proceed to creating NFS exports.

Warning: Do not mount NFS shares on cluster nodes. It may lead to node freeze.

6.3.3 Creating NFS Exports

To create a user NFS export, do the following:

1. On the **SERVICES > NFS > SHARES** screen, click the number in the **Exports** column in the row of the desired share. This will open the share screen.
2. On the share screen, create a root export that will contain user exports. To do this, click **ADD EXPORT**, specify root as the export name and / as path and select the read and write access mode.

This will create a directory with a default path, e.g., /0200000000000002. The path designates export location inside the share and is used (alongside share's IP address) to mount the export.

Important: Do not give the users access to the root export.

3. Mount the root export (e.g., as described in the *Acronis Storage User's Guide*).
4. In the mounted root export, create a subdirectory for a user export, e.g., export1.
5. Back on the share screen, click **ADD EXPORT**, enter a user export name, specify /export1 as path, and select the access mode.
6. Click **Done**.

Both the root and user exports are shown in the export list.

6.3.4 Setting Up User Authentication and Authorization

Acronis Storage allows you to authenticate users for access to specific NFS shares via Kerberos and authorize them to access specific NFS exports inside these shares via LDAP.

6.3.4.1 Authenticating NFS Share Users with Kerberos

To enable user authentication in an NFS share, do the following:

1. Assign a forward and reverse resolvable FQDN (fully qualified domain name) to share's IP address.
2. On the **SETTINGS > Security > KERBEROS** tab, specify the following Kerberos information:
 - 2.1. In **Realm**, your DNS name in uppercase letters.
 - 2.2. In **KDC service**, the DNS name or IP address of the host running the realm's KDC (key distribution center) service.
 - 2.3. In **KDC administration service**, the DNS name or IP address of the host running the realm's KDC administration service.

Note: Usually, the KDC and its administration service run on the same host.

3. On the Kerberos server, perform these steps:
 - 3.1. Log in as administrator to the Kerberos database administration program.
 - 3.2. Add a principal for the share with the command `addprinc -randkey nfs/<share_FQDN>@<realm>`. For example:

```
# addprinc -randkey nfs/share1.example.com@example.com
```

- 3.3. Generate a keytab (key table) for the principal and save it to a directory you can upload from. For example:

```
# ktadd -k /tmp/krb5.keytab nfs/share1.example.com@example.com
```

4. On the **SERVICES > NFS > SHARE** tab, select a share and click **Authentication**.
5. Upload the keytab file and click **SAVE**.

Important: Each share and client (user that mounts the export) must have its own principal and keytab.

6.3.4.2 Authorizing NFS Export Users with LDAP

By configuring access to a user directory via LDAP, you can control which users can access which NFS exports. You will need a directory of user accounts with desired NFS access parameters.

To configure access to an LDAP server, do the following:

1. On the **SETTINGS > Security > LDAP** tab, specify the following information:
 - **Address**, the IP address of the LDAP server;
 - **Base DN**, the distinguished name of the search starting point;
2. Click **Save**.

6.4 Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

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

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

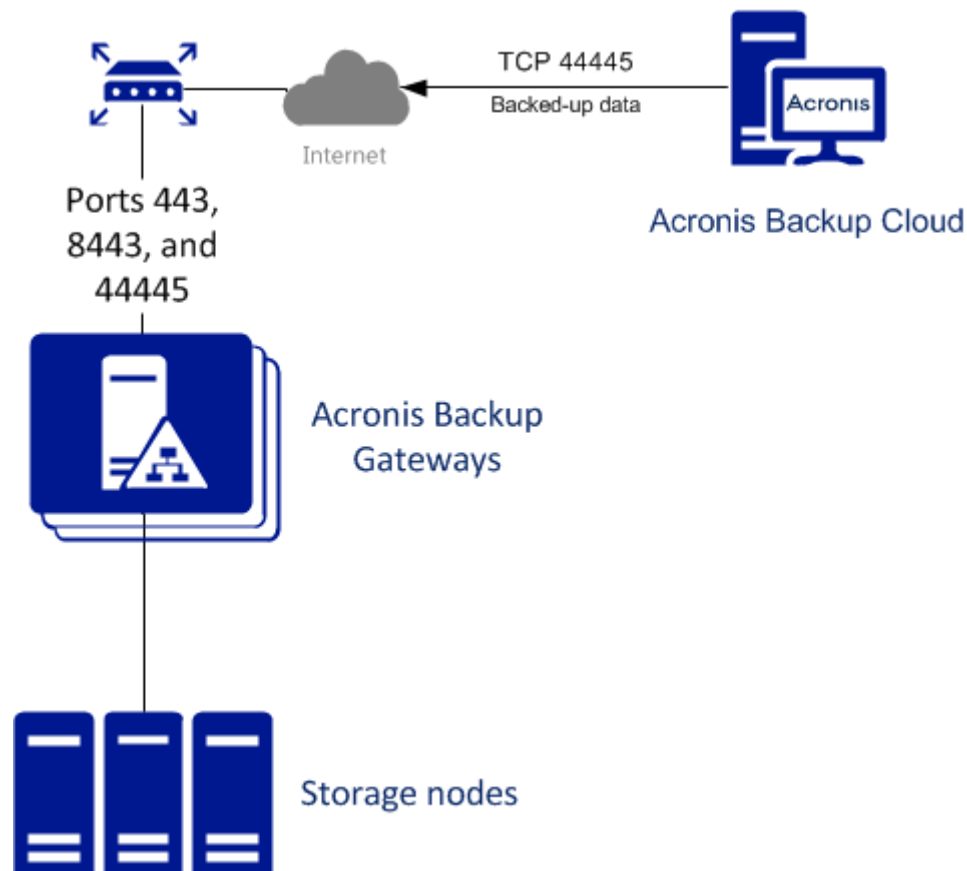
and data locality. Keeping backups in an NFS share or a public cloud implies the unavoidable data transfer and other overhead, which reduces overall performance.

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.

6.4.1 Understanding the Infrastructure

The Acronis Backup Gateway storage access point runs as services on the Acronis Storage nodes. It should be deployed on multiple Acronis Storage nodes for high availability.

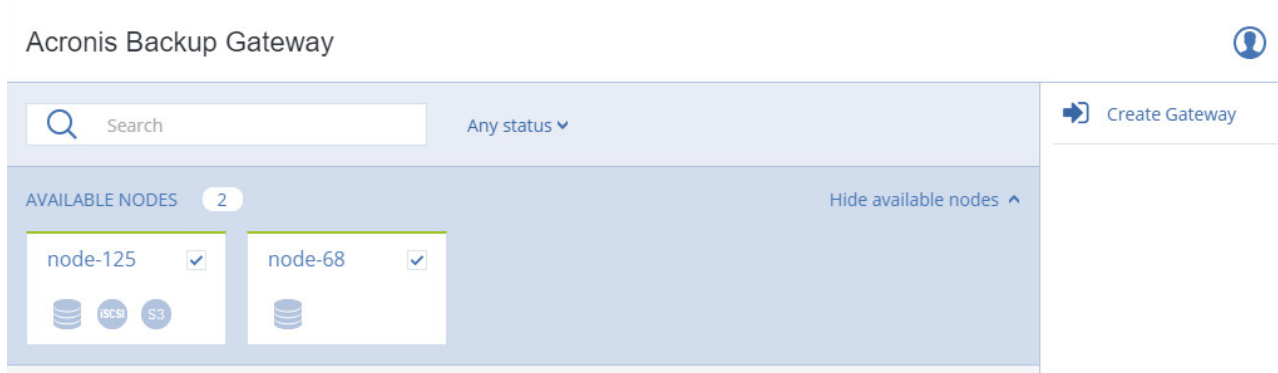


6.4.2 Connecting to the Acronis Storage Cluster via Acronis Backup Gateway

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

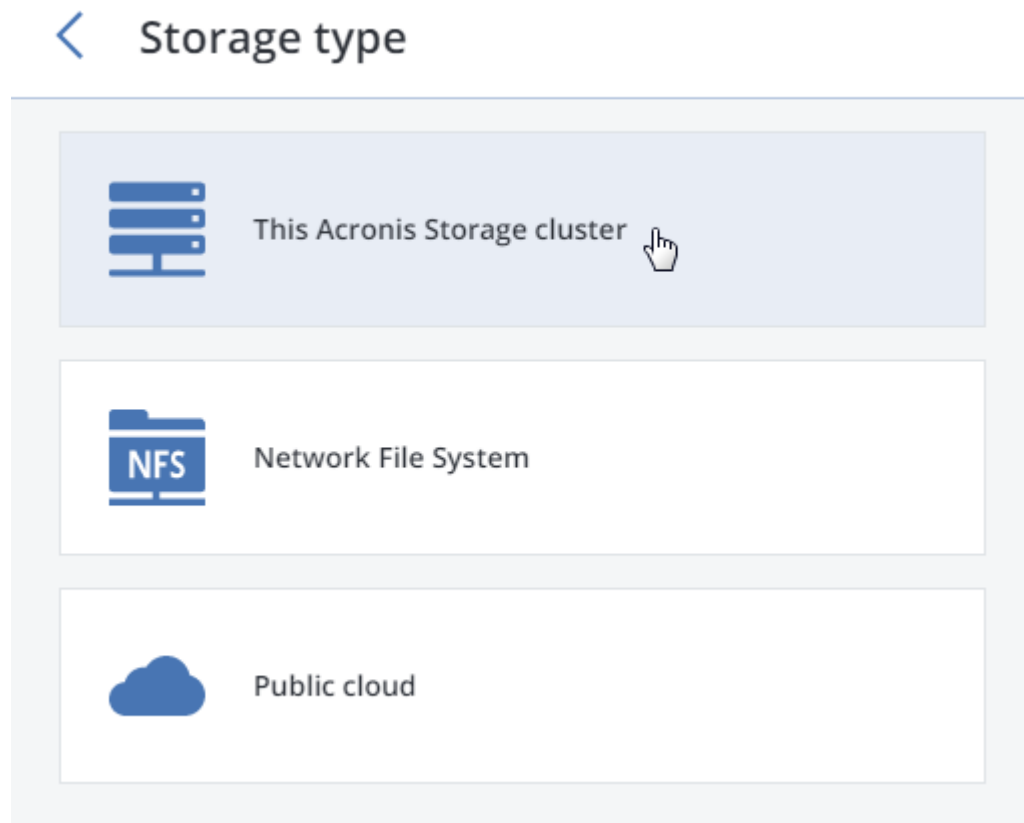
To connect Acronis Backup Cloud or Acronis Backup Advanced to the local Acronis Storage cluster via Acronis Backup Gateway, do the following:

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 a check box next to each cluster node where you want the gateway services to run.






3. Click **Create Gateway** then **This Acronis Storage cluster**.




6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway



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

✕ Configure Network

 10.250.14.34 	
ABGW private	ABGW public
<input type="text" value="ens160 - 10.250.14.34"/> 	ens160 - 10.250.14.34

 localhost 	
ABGW private	ABGW public
<input type="text" value="ens160 - 10.250.14.15"/> 	ens160 - 10.250.14.15

PROCEED

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

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

< 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	
Encoding 7+2	29% overhead	
Encoding 17+3	18% overhead	

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.

7. Click **NEXT**.

- 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.

< 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

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

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**.

6.4.3 Connecting to External NFS Shares via Acronis Backup Gateway

Note:

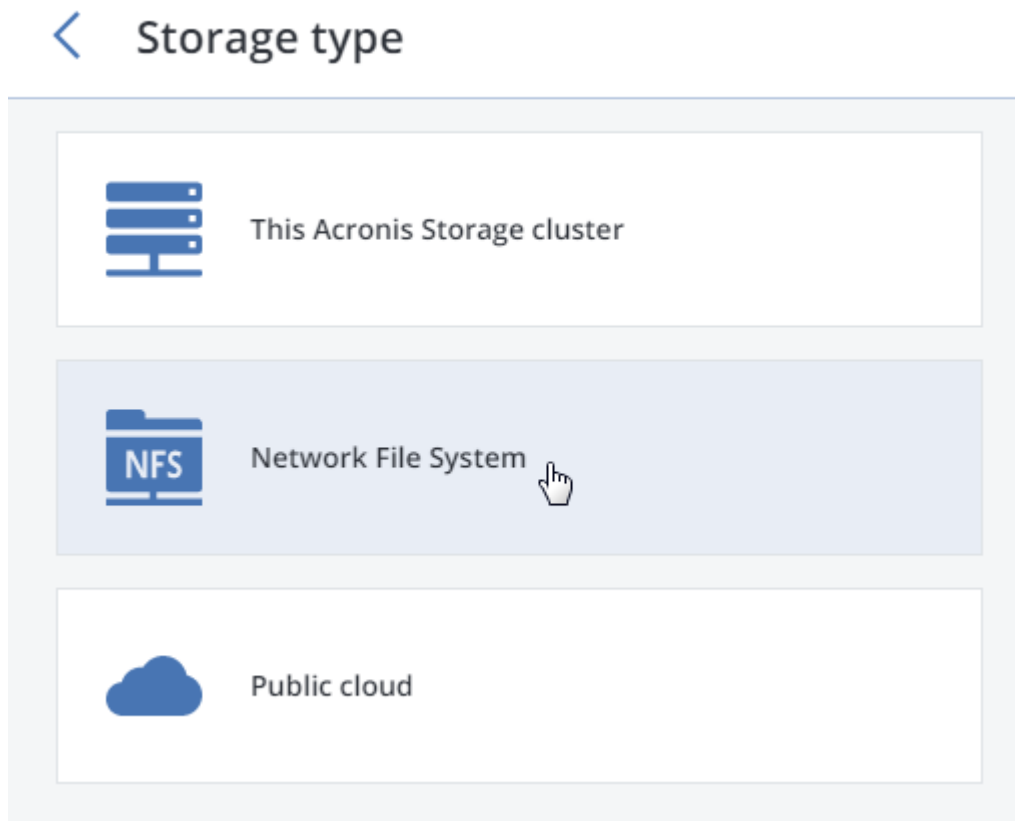
1. Acronis Storage does not provide data redundancy on top of NFS volumes. Depending on the implementation, NFS shares may use their own hardware or software redundancy.
2. In the current version of Acronis Storage, only one cluster node may store backups on an NFS volume.

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 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 a check box next to each cluster node where you want the gateway services to run.
3. Click **Create Gateway** and **Network File System**.

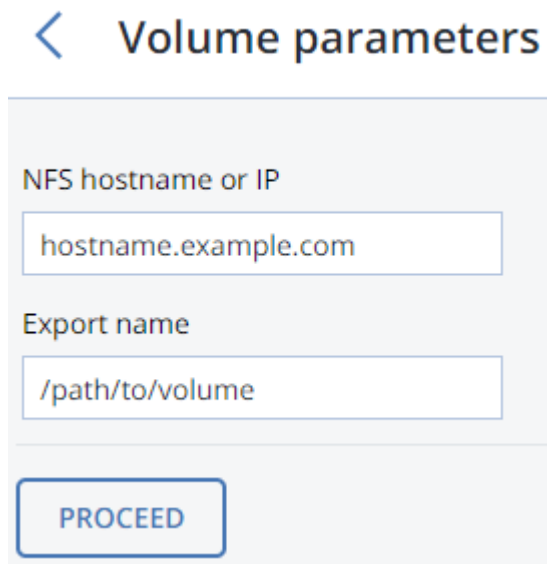


4. Make sure the network interface with the assigned Acronis Backup Gateway network role is selected. The gateway service will listen on the IP address assigned to this interface. Click **NEXT**.



6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

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



< Volume parameters

NFS hostname or IP

hostname.example.com

Export name

/path/to/volume

PROCEED

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.

< 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 add nodes to the Acronis Backup Gateway cluster, adjust the DNS settings accordingly.

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

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**.

6.4.4 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, IJ, 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.

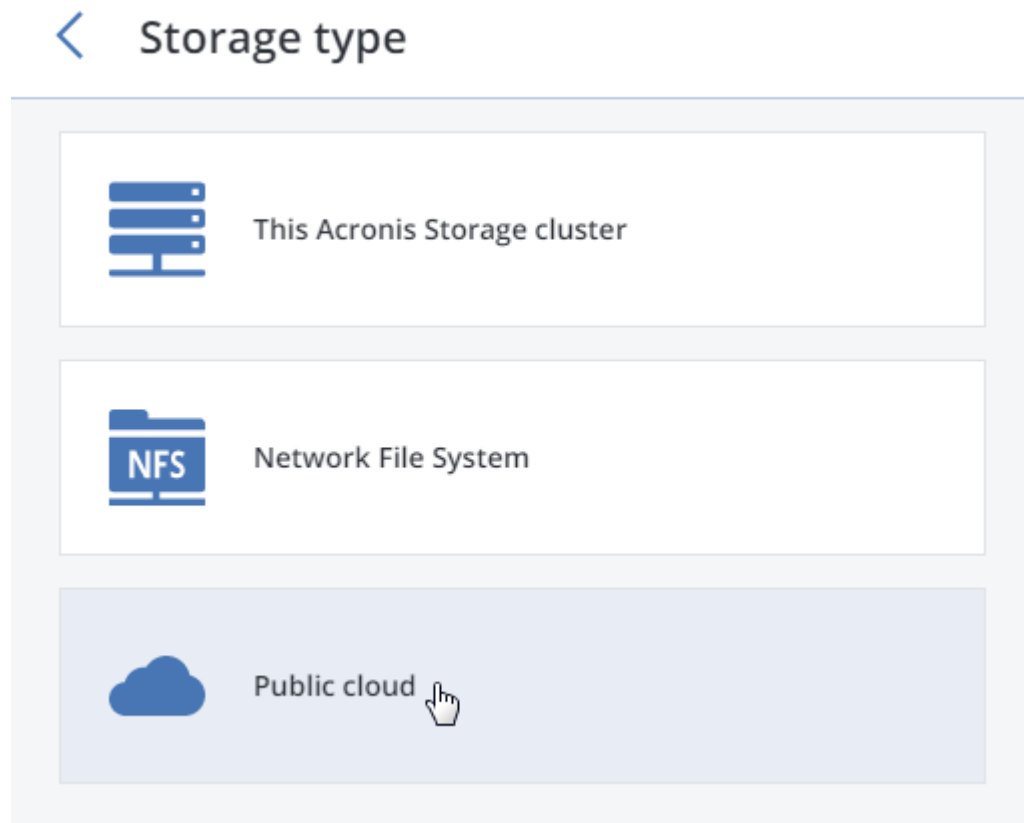
2. You must update Acronis Backup Agents to version 4492 (Windows/Mac) or 4470 (Linux). Otherwise agents' attempts to place backups in the new storage backend will result in "Backup failed" errors.
3. If you are to store backups in an Amazon S3 cloud, keep in mind that Acronis Backup Gateway may sometimes 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 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 a check box next to each cluster node where you want the gateway services to run.
2. Click **Create Gateway** then **Public Cloud**.

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway



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. In case of Google Cloud, select a JSON file with keys to upload.
- 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**.

6.4.5 Migrating Backups from Acronis Storage Gateways

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

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 (local cluster, NFS, or public cloud). 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.

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

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 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 change your Acronis Backup Cloud configuration even if you change nodes in the Acronis Backup Gateway cluster (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. On the **SERVICES > Acronis Backup Gateway > Nodes** screen, select one or more nodes and click **Migrate**.
2. Select the source storage version and click **NEXT**.
3. 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.

4. Provide the credentials for the management portal of the Acronis Backup Cloud installation that the source storage is registered in and click **NEXT**.
5. 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**.

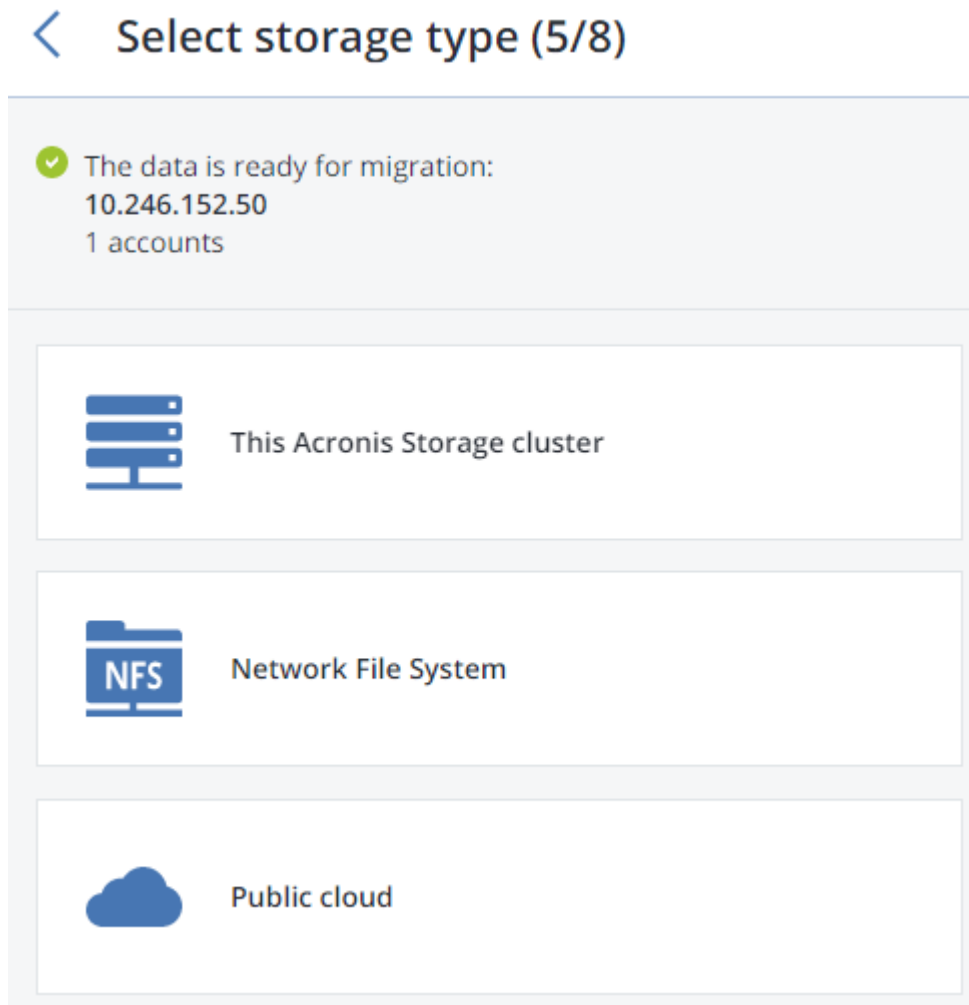
Important:

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 cluster, adjust the DNS settings accordingly.

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

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

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway



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

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

8. Click **NEXT**.
9. 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.

< 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 4492 (Windows/Mac) or 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

10. Click **NEXT**.

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

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

6.4.6 Monitoring the Acronis Backup Gateway Cluster

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

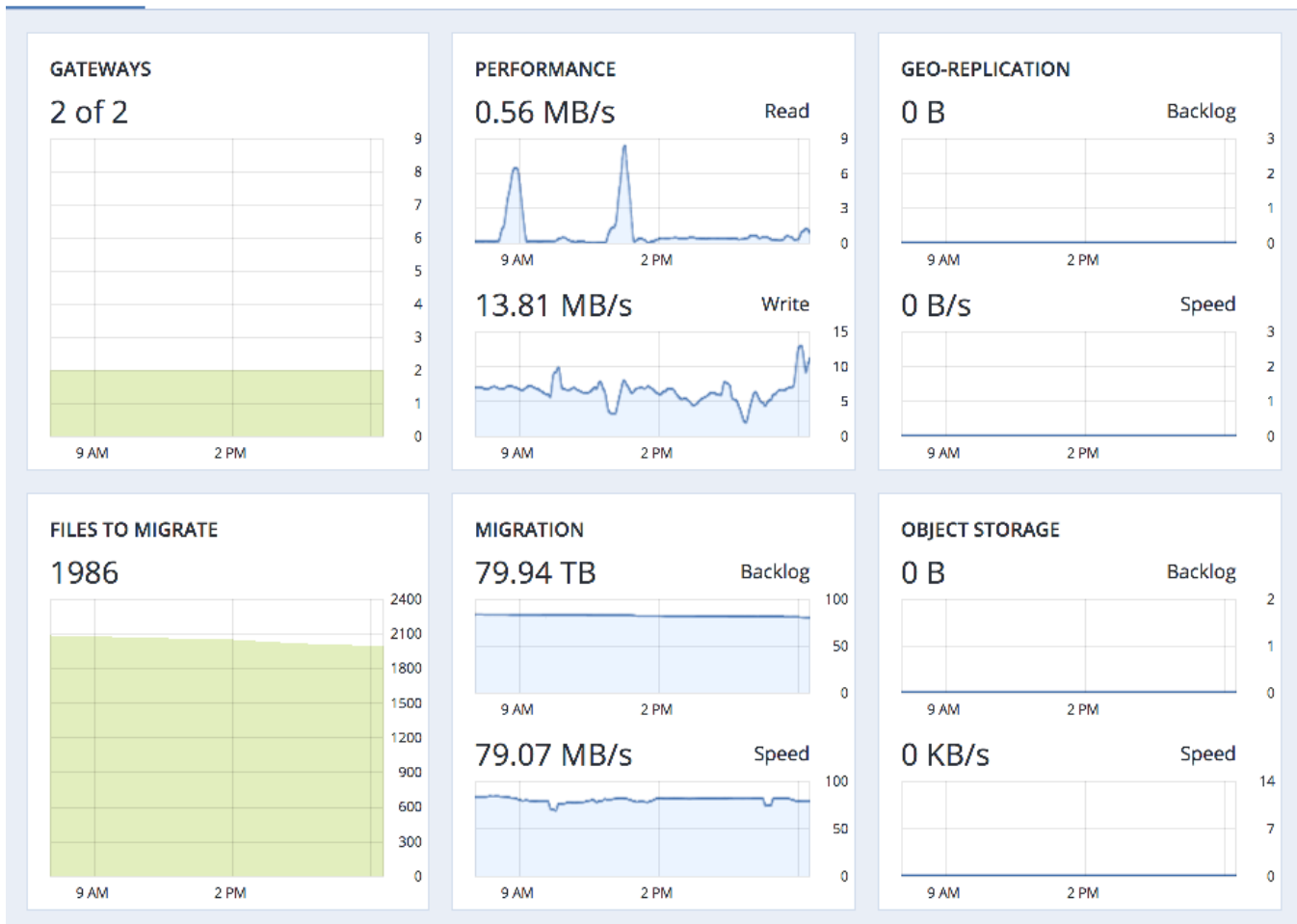
- the performance of Acronis Backup Gateway services,
- the geo-replication speed and backlog (the amount of data waiting to be replicated),
- migration speed and backlog (the amount of data waiting to be migrated),
- object storage speed and backlog (the amount of data waiting to be uploaded to public 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



6.4.7 Releasing Nodes from the Acronis Backup Gateway Cluster

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

6.4. Connecting Acronis Backup Software to Storage Backends via Acronis Backup Gateway

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

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

Releasing the last node is different as it means that the Acronis Backup Gateway cluster will be deleted and unregistered from your Acronis backup software.

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 cluster and unregisters it from your Acronis backup software.

✕ 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

- 2.2. **Force release**. Releases the last node, deletes the Acronis Backup Gateway cluster 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 cluster 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**.