

Acronis

Acronis Storage

Table of contents

1	Introduction	3
2	Acronis Storage basics.....	3
3	Acronis Storage redundancy modes.....	3
4	Server roles	5
4.1	Metadata Server (MDS)	5
4.2	Storage Server (STS).....	5
4.3	Front-end Server (FES).....	5
5	Requirements	6
5.1	Hardware requirements	6
5.2	Network requirements	8
5.3	Software requirements.....	9
6	Deployment.....	10
6.1	Initial node deployment.....	10
6.2	Booting up other nodes	11
6.2.1	Booting from Expansion ISO	12
6.2.2	Booting from PXE Server.....	12
6.3	Roles assignment	13
7	Integration with Acronis Backup Cloud	14
8	Updating Acronis Storage.....	15
9	Changing the redundancy mode	16
9.1	Evaluation mode to Express mode	16
9.2	Express mode to Advanced mode	16
9.2.1	Booting the physical servers.....	16
9.2.2	Migrating the MDS nodes.....	17
9.2.3	Migrating the FES nodes.....	18
9.2.4	Selecting the Advanced mode.....	19

1 Introduction

Acronis Storage is a cost-efficient software storage solution with cluster-level erasure coding that allows optimal use of raw storage capacity at the highest level of resilience.

Acronis Storage is designed to run on commodity hardware, thus eliminating the dependence on expensive, special-purpose hardware. Simplified deployment allows linear growth of system capacity by adding extra drives to the existing nodes; or by adding new nodes via PXE or a special, pre-configured ISO.

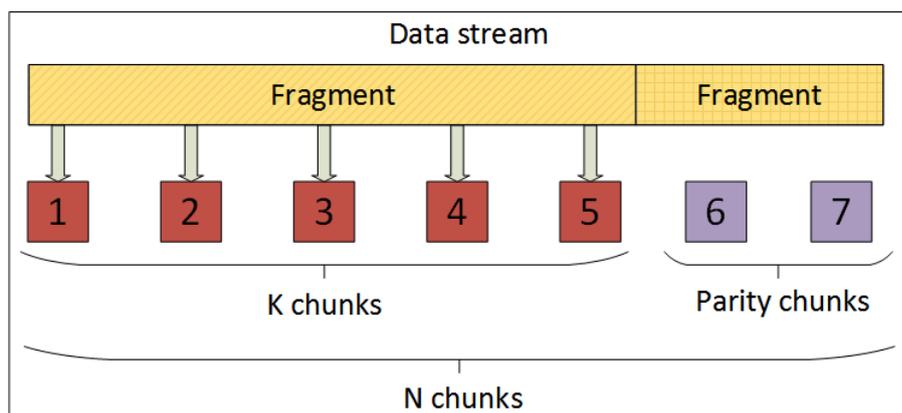
Acronis Storage offers simplified management and monitoring via a web console, with REST API for integration into existing management environments.

This document describes how to deploy Acronis Storage for using with Acronis Backup Cloud.

2 Acronis Storage basics

Acronis Storage breaks the data stream that comes from Acronis Backup Cloud into 320MB **fragments**. To ensure fault tolerance, each fragment is stored on multiple storage servers (nodes) as a set of **chunks** with some redundancy.

Acronis Storage leverages the so-called N/K redundancy scheme: each fragment is split into K chunks, then a certain number of additional (parity) chunks are added for redundancy, and then all of the chunks are distributed among N servers (one chunk per server). The system can survive failure of any (N-K) storage servers without data loss. The numbers N and K are determined by the storage system configuration.



3 Acronis Storage redundancy modes

Acronis Storage supports three redundancy modes. You must choose the redundancy mode when deploying Acronis Storage. For information about changing the redundancy mode at a later time, refer to "Changing the redundancy mode (p. 16)".

Advanced mode (recommended)

This mode provides a scale-out storage platform with software-level redundancy.

The storage can be based on commodity hardware that does not have built-in data redundancy. For hardware that has built-in data redundancy, this mode provides an additional software redundancy layer.

At least *eight* nodes are required. The system can survive a failure of *two* nodes without data loss. The data redundancy overhead is 40 percent, which means that 1.4 GB of disk space is required to store 1 GB of data.

Express mode

This mode is designed to provide an additional software redundancy layer when deployed on virtual hosts that share a common storage device that has built-in data redundancy.

At least *six* nodes are required. The system can survive a failure of *one* node without data loss. The data redundancy overhead is 20 percent, which means that 1.2 GB of disk space is required to store 1 GB of data.

This mode assumes a smooth transition to the advanced mode.

Evaluation mode

This mode does not provide software-level redundancy; therefore it creates no data redundancy overhead.

This mode is designed for product evaluation and assumes a mandatory transition to either the express or the advanced mode. For this purpose, we recommend *six* virtual nodes. The system cannot survive a node failure.

Do not use the evaluation mode in your production environment!

4 Server roles

Acronis Storage is deployed on bare metal. It does not require a general-purpose operating system to run on any of its nodes.

The Acronis Storage server roles are assigned to hard disk drives rather than to a node. A drive can be assigned only one role. If a node has more than one disk drive, it can run more than one server role. When a role is assigned to a disk drive, this disk is initialized and all of its data is deleted.

4.1 Metadata Server (MDS)

A **metadata server (MDS)** stores information about file fragments and the location of chunks that make up these fragments. It is the most critical component of the system.

Several MDS nodes are needed to build a high-availability metadata cluster. A standard configuration includes three metadata nodes: one master and two subordinates. The metadata is continuously replicated from the master node to the subordinate nodes. If the master node fails, one of the subordinate nodes is elected as the new master node.

We recommend that you dedicate two hard disk drives to the MDS role. The software RAID1 array will be automatically created on these disks, to increase the MDS reliability.

A **management component (MGMT)** is installed with each MDS role. This component enables you to use the Acronis Storage web console for system deployment, monitoring and management.

When the master MDS node fails over to a different node, the management component automatically starts on that node so that the web console is available at any time.

4.2 Storage Server (STS)

The Storage Server (STS) role is responsible for storing data chunks.

4.3 Front-end Server (FES)

The Front-end Server (FES) role allows Acronis Backup Cloud backup agents to access the Acronis Storage system for backup data transfer.

5 Requirements

5.1 Hardware requirements

Advanced mode

Three nodes for the **MDS+STS** roles:

- RAM: 64 GB DDR3 ECC
- CPU: Dual Intel Xeon E5 (for example, Intel Xeon E5-2620 V2)
- HDD: Six or more 4TB+ 7200RPM SATA HDDs (for example, Seagate SV35 or Seagate Megalodon). Smaller disks (500GB+) can be used for the MDS roles.
- HBA controller for disks (for example LSI 2308 HBA with IT Mode/Pass-through). Use of a RAID controller is not recommended.
- One network interface with 2-4 bonded (LACP IEEE 802.3ad) 1 Gbps adapters or a 10 Gbps adapter.
- 2U-4U chassis (depending on the number of disk drives)
- Redundant power supply unit (PSU)

Three nodes for the **FES+STS** roles:

- RAM: 64 GB DDR3 ECC
- CPU: Single Intel Xeon E5 (for example, Intel Xeon E5-2620 V2)
- HDD: Six or more 4TB+ 7200RPM SATA HDDs (for example, Seagate SV35 or Seagate Megalodon). Smaller disks (500GB+) can be used for the FES roles.
- HBA controller for disks (for example LSI 2308 HBA with IT Mode/Pass-through). Use of a RAID controller is not recommended.
- Two network interfaces. Each interface requires 2-4 bonded (LACP IEEE 802.3ad) 1 gigabit per second adapters or a 10 gigabits per second adapter.
- 2U-4U chassis (depending on the number of disk drives)
- Redundant power supply unit (PSU)

Two (or more) nodes for the **STS** role:

- RAM: 32 GB DDR3 ECC
- CPU: Single Intel Xeon E5 (for example, Intel Xeon E5-2620 V2)
- HDD: Six or more 4TB+ 7200RPM SATA HDDs (for example, Seagate SV35 or Seagate Megalodon)
- HBA controller for disks (for example LSI 2308 HBA with IT Mode/Pass-through). Use of a RAID controller is not recommended.
- One network interface with 2-4 bonded (LACP IEEE 802.3ad) 1 Gbps adapters or a 10 Gbps adapter.
- 2U-4U chassis (depending on the number of disk drives)
- Redundant power supply unit (PSU)

The following diagram shows the recommended hardware configuration and role assignment for Acronis Storage in the advanced mode. The software RAID1 array will be automatically created for the MDS roles.



Express and Evaluation modes

We recommend the following configuration:

- VMware vSphere 5.1
- Six virtual machines in a high-availability setup

For each of the virtual machines:

- CPU: minimum two cores.
- RAM: minimum 16 GB.
- Virtual disks: 30GB+ for the MDS and FES roles, 1TB+ for the STS roles.
- vmxnet3 virtual network adapters: two for each machine running the FES role, one for each of the other machines.

- When creating a virtual machine, set "Red Hat Enterprise Linux 6 (64-bit)" as the operating system. (Installation of the operating system is not required.)

The recommended VM configuration and role assignment for the express and evaluation modes are shown in the diagram above (nodes 1-6).

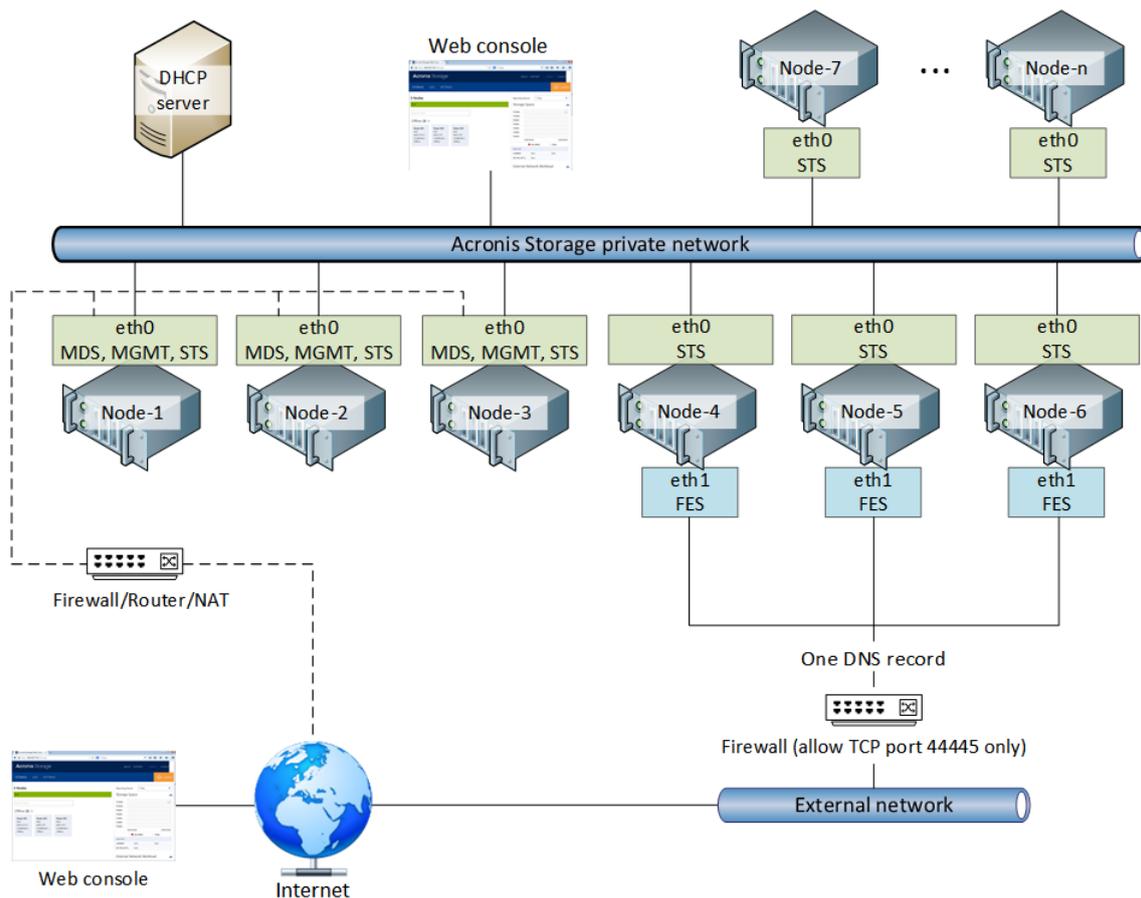
5.2 Network requirements

- A dedicated private network (VLAN or physical) for the Acronis Storage nodes.
- A DHCP server in the Acronis Storage private network.
- Three IP addresses located in the same subnet of the Acronis Storage private network for the three nodes running the MDS role.
- One additional IP address for the MGMT component (a unique IP address, not that of an MDS). This address will be used for the web console access and communication with Acronis Backup Cloud. Internet access must be configured for this IP address through the NAT device.

Important *These IP addresses will be reserved for MDS and MGMT by using IP aliasing. Exclude these IP addresses from the DHCP IP range to avoid conflicts that may cause the system malfunction.*

- One public static IP address in the external network for each FES node.
- A single DNS record for all of the FES nodes.
A backup agent randomly selects one of the FES nodes behind the DNS name to stream the backed-up data. If the node becomes inaccessible, the agent automatically switches to another node after two connection re-attempts.
- The FES nodes must be protected by a firewall that allows traffic only on TCP port 44445.

The following diagram illustrates the typical network configuration for Acronis Storage.



5.3 Software requirements

For the smooth operation of the web console, use one of the following web browsers:

- Google Chrome 27 or later
- Mozilla Firefox 20 or later
- Windows Internet Explorer 10.0 or later
- Safari 5.1 or later

6 Deployment

This section describes how to deploy the recommended Acronis Storage configurations presented in "Hardware requirements" (p. 6).

The deployment procedures vary for the initial node and the remaining nodes.

The first node that you deploy will run the MDS and STS roles. Each role will be installed on a dedicated disk drive. A management component (MGMT) will be installed on the same disk drive with the MDS role. This component enables you to use the Acronis Storage web console for system deployment, monitoring, and management.

Once the initial node is deployed, all of the nodes can be configured by using the web console.

6.1 Initial node deployment

In this step, you will deploy the initial node of the Acronis Storage system and define the most critical system parameters. The node will be assigned the MDS and STS roles.

Warning All data will be deleted from this machine.

1. Download the Acronis Storage ISO file.
If you do not have the download link, do the following:
 - a. Log in to the Acronis Backup Cloud account management console (<https://baas.acronis.com/>).
 - b. In the **Groups** list, select the root group.
 - c. Click the **Storage** tab.
 - d. Click **Add**.
 - e. Click **Download Acronis Storage ISO Image**.
2. For a physical machine, do any of the following:
 - Create a bootable USB flash drive by using the ISO file and one of the free tools available online. For example, "ISO to USB".
 - Burn a CD/DVD using the ISO file.For a virtual machine: connect the ISO file to the virtual machine as a CD/DVD drive.
3. Boot the machine from the Acronis Storage bootable media.
4. Enter common parameters for the **external** network.
 - a. Network mask
 - b. Gateway address
 - c. DNS addresses, separated by a space

```
Loading, please wait...
Welcome to Acronis Storage installation (ver. 1.3.65238)!
Initializing network, please wait...

Networks list:
eth0: 10.250.144.223/255.255.248.0, MAC: 00:0c:29:3c:96:90, vendor: NIC Vendor
eth1: 192.168.113.149/255.255.255.0, MAC: 00:0c:29:3c:96:9a, vendor: NIC Vendor

Please provide common parameters for external network:
Enter netmask:
> 255.255.248.0
Enter gateway address:
> 10.250.144.1
Enter DNS addresses separated by space:
> 10.250.32.60
```

5. Enter three IP addresses, separated by a space, for the three nodes that will run the MDS role. These must be the addresses within the same subnet of the Acronis Storage **private** network.

```
Enter static IP addresses for three Metadata nodes.
All three addresses must be in the same subnet.
Separate addresses with a Space.
> 192.168.113.150 192.168.113.151 192.168.113.152
```

6. Enter an IP address that will be used for the web console access. This must be an address within the Acronis Storage **private** network.

```
Enter another static IP address that will be used for management Web Console access.
> 192.168.113.153
```

7. Select the Acronis Storage redundancy mode. The following modes are available:
 - **Advanced mode**
 - **Express mode**
 - **Evaluation mode**

For information about redundancy modes, refer to "Acronis Storage redundancy modes" (p. 3).

8. Once the deployment is completed and the services have started, the web console address in the Acronis Storage **private** network is displayed.

```
Initializing disk /dev/sdc...
Initializing disk /dev/sda...
Initializing disk /dev/sdb...
[Finished]

Initializing network... [OK]
Starting MetadataService... [OK]
Starting StorageService... [OK]
Starting ManagementService... [OK]

Node is ready.

Web Console is available at "https://192.168.113.153".
```

You can now log in to the Acronis Storage web console and use the default credentials:

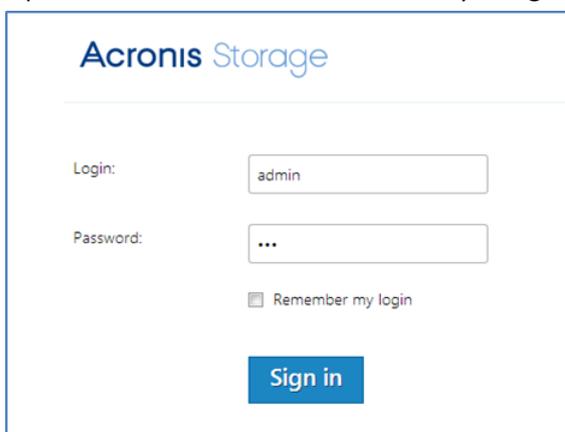
- Login: **admin**
- Password: **Acron1\$** (case-sensitive)

Note To improve the security of your Acronis Storage system, we recommend changing the web console access credentials immediately after the first login, in **Settings > Access control**.

6.2 Booting up other nodes

In this step, you will boot up the remaining nodes to enable assigning Acronis Storage roles to them.

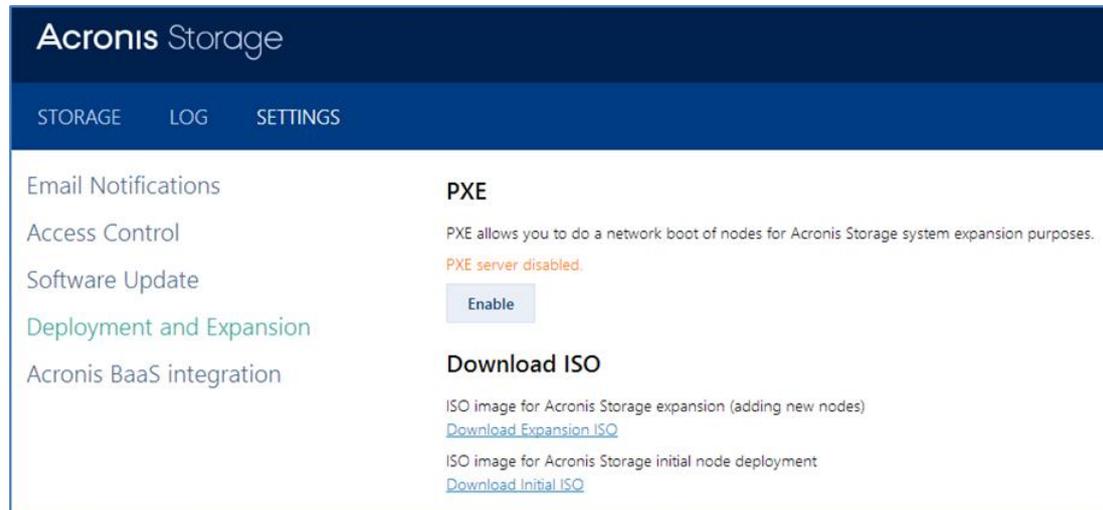
1. Open the web console in a browser, by using the IP address from the previous instructions.



2. Log in with the default credentials:
 - Login: **admin**
 - Password: **Acron1\$** (case-sensitive)

Note We recommend changing the web console access credentials immediately after the first login, in **Settings > Access control**.

3. Go to the **Settings** tab.
4. Click **Deployment and Expansion**.



The Acronis Storage nodes can be deployed by using either a PXE server or a special Expansion ISO, which is downloadable from the web interface.

6.2.1 Booting from Expansion ISO

To prepare the Expansion ISO:

1. On the **Deployment and Expansion** tab, click **Download Expansion ISO**. The ISO already contains necessary configuration files with MDS nodes IP addresses.
2. For physical machines, do any of the following:
 - Create a bootable USB flash drive by using the ISO file and one of the free tools available online. For example, "ISO to USB".
 - Burn a CD/DVD using the ISO file.

For virtual machines: connect the ISO file to each of the virtual machines as a CD/DVD drive.

Boot each of the nodes prepared for adding to Acronis Storage from the **Expansion ISO**. The boot process does not require a user interaction. No data is deleted from the machines during the boot process. The data will be deleted later, when the roles are assigned to the nodes via the web console.

```
Loading, please wait...
Initialize network... [OK]

Node is ready.

Web Console is available "https://192.168.113.153"
```

The nodes are now ready for further configuration via the web console.

6.2.2 Booting from PXE Server

Preboot eXecution Environment (PXE) allows you to do a network boot of nodes for storage system expansion purposes.

Prior to starting this procedure, ensure that each of the nodes is capable of booting up from the network.

1. On the **Deployment and Expansion** tab, click the **Enable** button under **PXE**.

Note Acronis Storage PXE does not support failover. If the node with the PXE server goes down, repeat step 1 of this procedure. PXE will be re-initiated on one of the remaining nodes.

2. Reboot the nodes prepared for adding to the Acronis Storage system, and ensure that they have booted from the network. The boot process does not require a user interaction. No data is deleted from the machines during the boot process. The data will be deleted later, when the roles are assigned to the nodes via the web console.

```

Loading, please wait...
Initialize network... [OK]

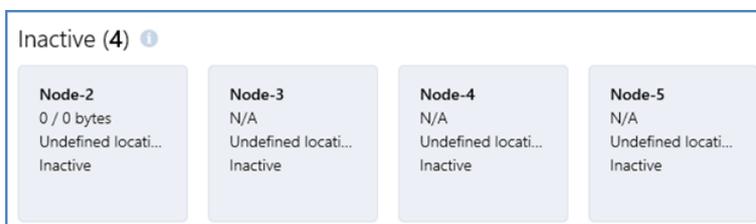
Node is ready.
Web Console is available "https://192.168.113.153"
  
```

The nodes are now ready for further configuration via the web console.

6.3 Roles assignment

In this step, you will activate the remaining nodes to make Acronis Storage fully functional.

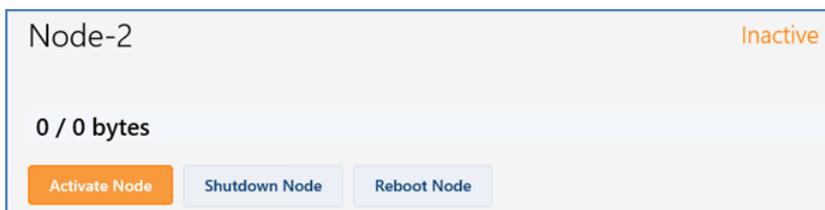
After booting the new nodes from the Expansion ISO or PXE, the nodes appear in the web console on the **Storage** tab in the **Inactive** group.



To make the nodes active, you need to assign the MDS, STS or FES roles to the nodes' disk drives. For the recommended role assignments, refer to the diagrams in "Hardware requirements" (p. 6).

To assign the roles to the second and the third node

1. Click a node to open its properties.



2. Click **Activate Node**.

The system offers the default role assignment scheme. This scheme has the MDS and STS roles enabled.

The roles are automatically distributed between the disk drives of the node according to the following scheme:

- Two disk drives are dedicated to the **MDS** role (in RAID1).
- The rest of the disk drives are dedicated to the **STS** role.



3. Click **Activate** to complete the setup.

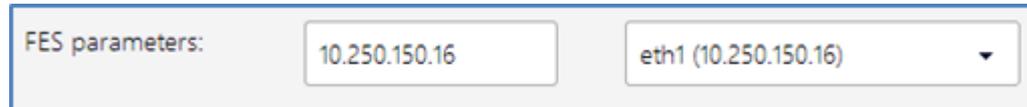
To assign the roles to the fourth, the fifth and the sixth nodes

The nodes must have an external network interface.

1. Click a node to open its properties.
2. Click **Activate Node**.

The system offers the default role assignment scheme. This scheme has the **STS** role enabled for every disk.

3. Enable the FES role by clicking **FES** in the roles section.
4. Specify a network interface and a static IP address in the **external** network for the **FES** role.

A screenshot of a web form titled "FES parameters:". It contains two input fields. The first is a text box containing the IP address "10.250.150.16". The second is a dropdown menu showing "eth1 (10.250.150.16)" with a downward arrow on the right.

5. Select the disk to assign the FES role to.
6. Click **Activate** to complete the setup.

To assign the STS roles to the rest of the nodes

Do the following for each node:

1. Click a node to open its properties.
2. Click **Activate Node**.

The system offers the default role assignment scheme. This scheme has the **STS** role enabled for every disk.

3. Click **Activate** to complete the setup.

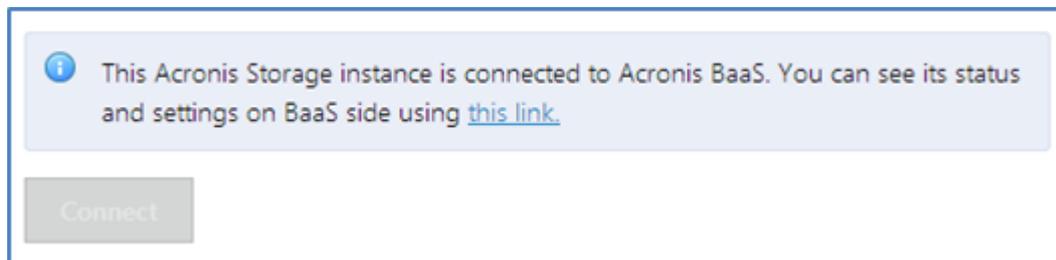
7 Integration with Acronis Backup Cloud

1. In the web console, click the **Settings** tab.
2. Click **Acronis BaaS integration**.
3. Specify:
 - a. The Acronis Backup Cloud management server address, which matches the account management console address (<https://baas.acronis.com/>).
 - b. The DNS name of the front-end servers. If you have only one FES, you can specify its IP address.
 - c. The Acronis Backup Cloud administrator login (email address)

- d. The Acronis Backup Cloud administrator password

Field	Value
Acronis Storage operation mode	Express (N/K/Q = 5/5/6)
BaaS Management Server address *	https://baas.acronis.com
Front-end Server(s) DNS name *	10.250.153.12
BaaS administrator login *	admin@domain.com
BaaS administrator password *	...

4. Click **Connect**.



5. This instance of Acronis Storage is now connected to Acronis Backup Cloud. To view its status and settings in the Acronis Backup Cloud account management console, select your root group and click the **Storage** tab. You can create an End-user Company (EUC) and during its creation select the storage as a destination for backups.

8 Updating Acronis Storage

1. Download the latest Acronis Storage ISO file.
To find the download link, follow step 1 in "Initial node deployment" (p. 10).
2. Log in to the Acronis Storage web console, and then click the **Settings** tab.
3. Click **Software Update**.
4. Click **Browse**, and then select the ISO file that you downloaded in step 1.
5. Click **Upload**.
The system uploads the file, and then shows the update type.
 - Minor update. No Acronis Storage downtime is required; the nodes will be auto-rebooted one by one.
 - Major update. A short Acronis Storage downtime is required; as all nodes will be rebooted at once.
6. Click **Update** to begin the update process. Wait until you see the **Update completed** message.

9 Changing the redundancy mode

It is possible to change the Acronis Storage redundancy mode from **Evaluation** to **Express**, and from **Express** to **Advanced**.

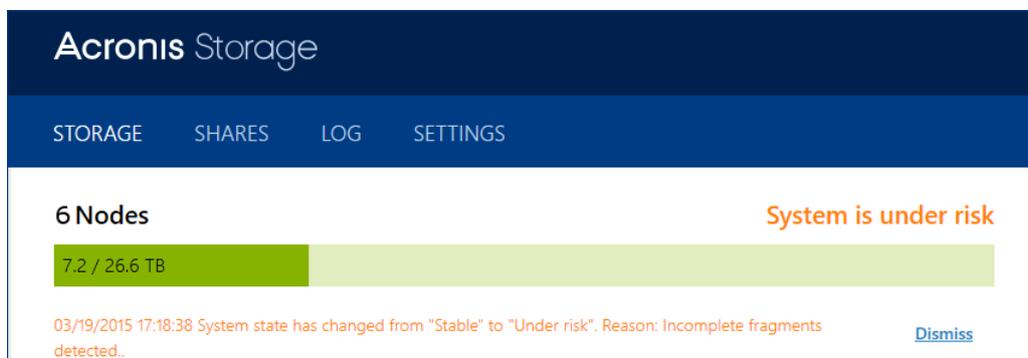
Before changing the redundancy mode, consider the following:

- Changing the mode causes no storage system downtime.
- Changing the mode increases the redundancy overhead for the data that is already present in the storage. As a result, the total occupied space will increase.

9.1 Evaluation mode to Express mode

1. In the Acronis Storage web console, click the **Settings** tab.
2. Click **Redundancy mode**.
3. Select **Express**.
4. Click **Apply**.

The system starts creating additional parity chunks for the data. On the **Storage** tab, the system state changes to **System is under risk**.



The total size of chunks to create is shown in the **Redundancy health** section of the **Storage** tab.

After all additional chunks are created, the system state changes to **System is stable**, which means that the redundancy mode was successfully changed.

9.2 Express mode to Advanced mode

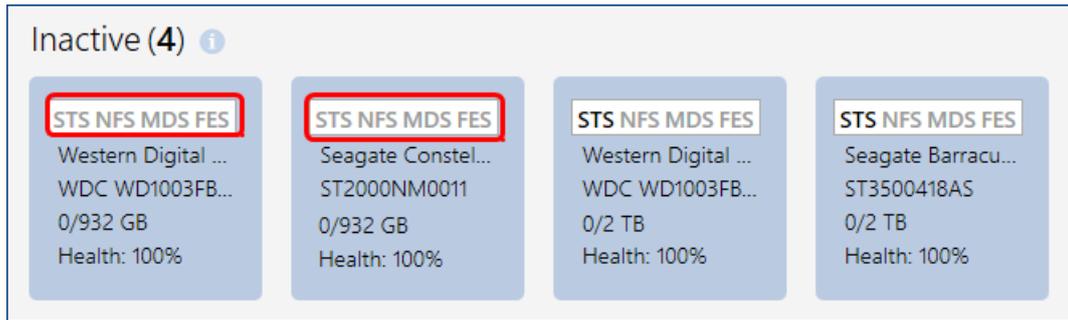
To change the mode to **Advanced**, you must have eight physical nodes that meet the hardware requirements (p. 6).

9.2.1 Booting the physical servers

Ensure that the physical servers are connected to the Acronis Storage private network.

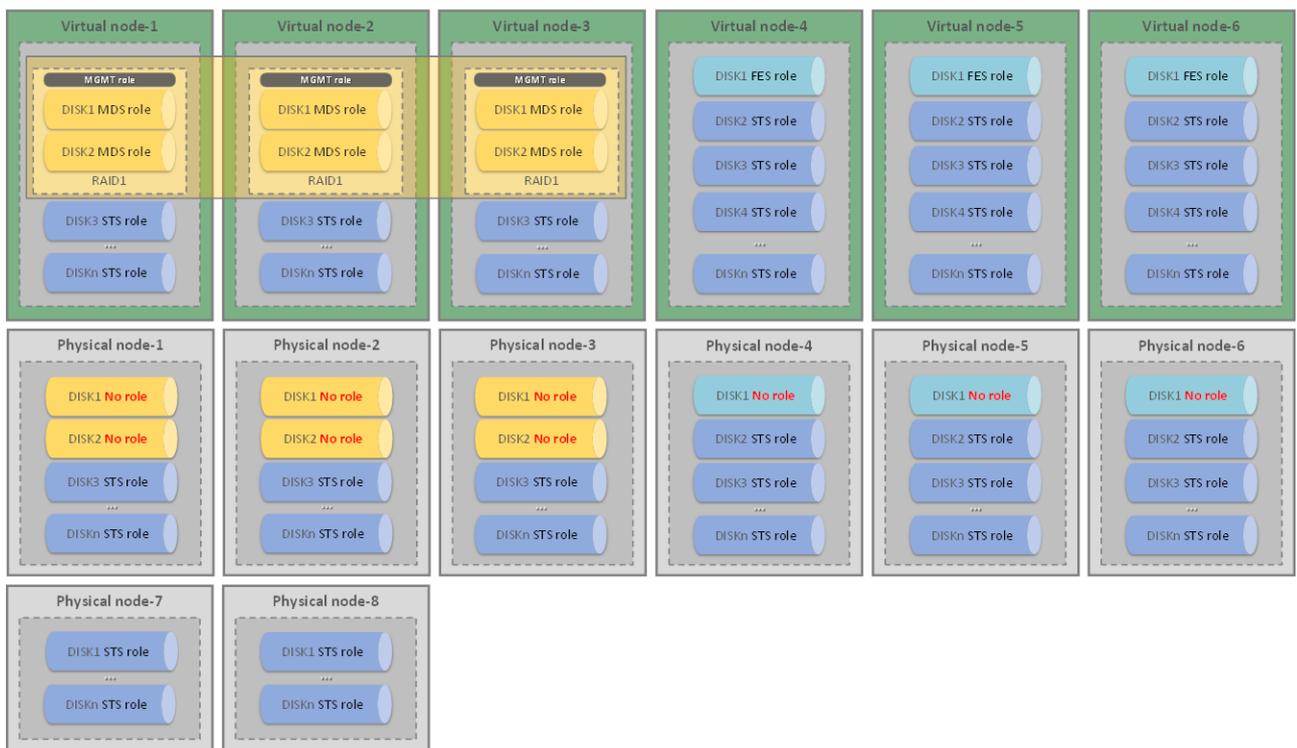
1. Boot the physical servers from an expansion ISO or from a PXE server, as described in "Booting up other nodes" (p. 11).
2. Assign *only* the STS roles to the nodes' disks, as described in "Roles assignment" (p. 13).

- On each of the three servers intended for MDS, leave two blank disks.



- On each of the three servers intended for FES, leave one blank disk.

You should now have 14 nodes in your Acronis Storage private network. The following diagram shows the role assignment at this stage.



9.2.2 Migrating the MDS nodes

The MDS nodes must be migrated in the following order:

- Subordinate MDS nodes without the MGMT component.
- Subordinate MDS node with the MGMT component, if such a node exists.

3. Master MDS node (shown in bold in the Acronis Storage web console).

mds01 4.6 / 4.6 GB MDS STS MGMT KVM port 5 Active	2	mds02 0 / 0 bytes MDS STS KVM port 3 Active	3	mds03 1015 GB / 3.1 TB MDS STS KVM port 4 Active	1
--	----------	---	----------	---	----------

Use the following procedure to migrate the MDS nodes in the order specified above.

To migrate an MDS node

1. Ensure that the system is in the **System is stable** state. If the state is **Under risk**, wait while the system resolves the redundancy issues.
2. Deactivate one of the virtual MDS nodes:
 - a. Select the node to deactivate.
 - b. Click **Deactivate node**.
3. Assign the MDS role to the first and the second disks of a physical server. For information about how to assign roles to disks, refer to "Roles assignment" (p. 13).

The system starts migrating the MDS and STS roles to the new node. This process may last up to several hours, because the data within the STS role is migrated, too. The progress is displayed in the **Nodes** section of the **Storage** tab.
4. Wait while the system finishes migrating the roles.

9.2.3 Migrating the FES nodes

- Ensure that the physical servers that will be assigned the FES role have public static IP addresses in the external network.
- Ensure that you have created a single DNS name for these IP addresses.

For more information about network requirements, refer to "Network requirements" (p. 8).

Use the following procedure to migrate each of the FES nodes.

To migrate an FES node

1. Ensure that the system is in the **System is stable** state. If the state is **Under risk**, wait while the system resolves the redundancy issues.
2. Deactivate one of the FES virtual nodes:
 - a. Select the node to deactivate.
 - b. Click **Deactivate node**.
3. Assign the FES role to the first disk of a physical server. For information about how to assign roles to disks, refer to "Roles assignment" (p. 13).

The system starts migrating the FES and STS roles to the new node. This process may last up to several hours, because the data within the STS role is migrated too. The progress is displayed in the **Nodes** section of the **Storage** tab.
4. Wait while the system finishes migrating the roles.

9.2.4 Selecting the Advanced mode

After all nodes are migrated from virtual to physical machines, change the redundancy mode to **Advanced**. The steps are similar to the ones described in "Evaluation mode to Express mode" (p. 16).

Copyright Statement

Copyright © 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.