

Acronis

Acronis Software-Defined Infrastructure 2.5

Appliance Quick Start Guide

March 21, 2019

Copyright Statement

Copyright ©Acronis International GmbH, 2002-2019. All rights reserved.

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

"Acronis Compute with Confidence", "Acronis Startup Recovery Manager", "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; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 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; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Contents

- 1. About the Appliance 1**
 - 1.1 Appliance Exterior 1
- 2. Safety Instructions 3**
- 3. Installing the Appliance 4**
 - 3.1 Unpacking the Appliance 4
 - 3.2 Mounting the Appliance into Rack 5
 - 3.3 Connecting Cables to the Appliance 8
 - 3.4 Configuring the Appliance 9
- 4. Enabling High Availability 14**
 - 4.1 Enabling Management Node High Availability 16
- 5. Managing Licenses 19**
 - 5.1 Installing License Keys 20
 - 5.2 Installing SPLA Licenses 21
- 6. Getting Technical Support 23**
- 7. Appendix: Specifications 25**
 - 7.1 Technical Specifications 25
 - 7.1.1 Power Supply Specifications 26
 - 7.1.2 Chassis Dimensions and Weight 26
 - 7.2 Environmental Specifications 27
 - 7.2.1 Air Quality Requirements 27

CHAPTER 1

About the Appliance

The appliance comprises five nodes in a 19-inch 3U rackmount server chassis. The appliance deploys into a universal and easy-to-use software-defined infrastructure solution that combines virtualization and storage, which allows you to create and manage virtual machines and offers object, block, and file storage, including a local repository for cloud backups.

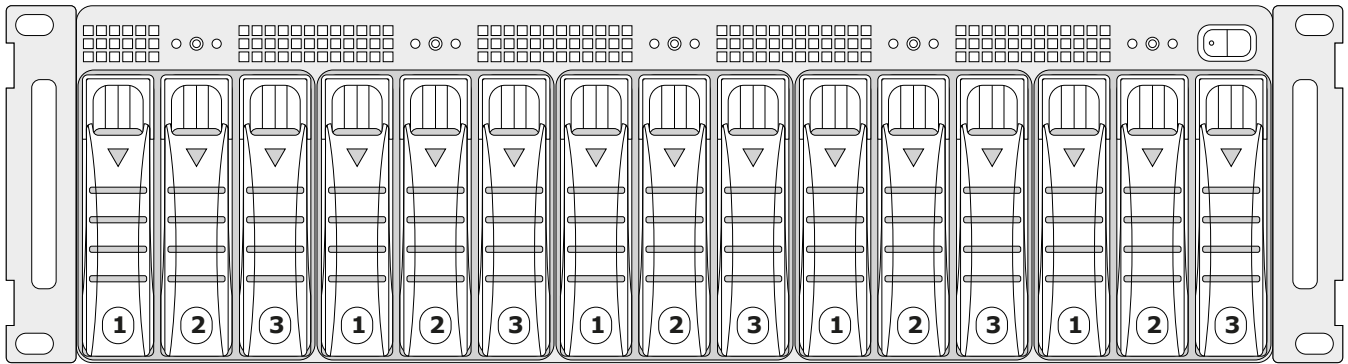
The appliance comes in several models that vary by storage capacity:

Model	Raw storage, TB	Usable storage*, TB	
		Capacity	Performance
SDI-5060	60	31	18
SDI-5120	120	62	36
SDI-5150	150	77	45
SDI-5180	180	93	54

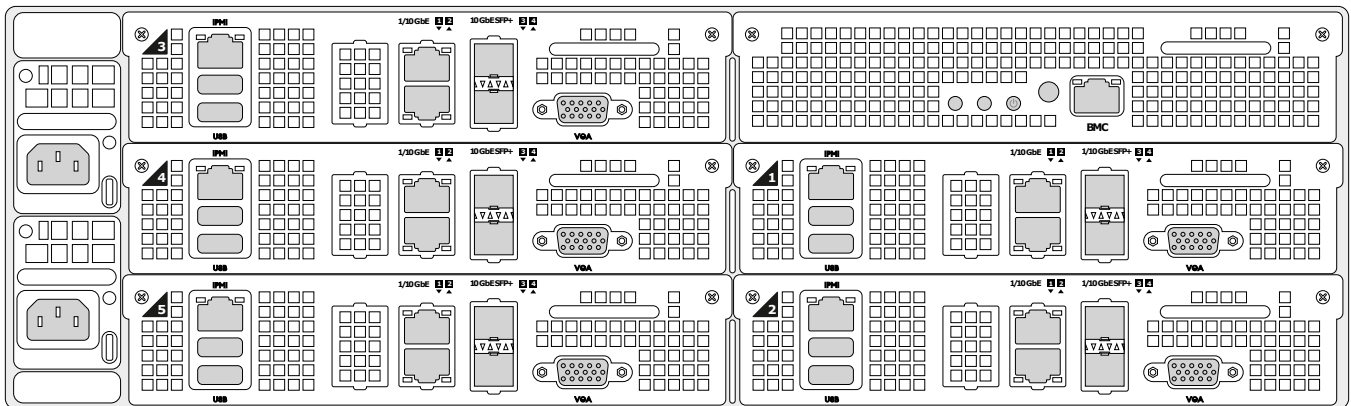
* With the recommended redundancy scheme. Erasure coding 3+2 is recommended for capacity; replication=3 is recommended for performance.

1.1 Appliance Exterior

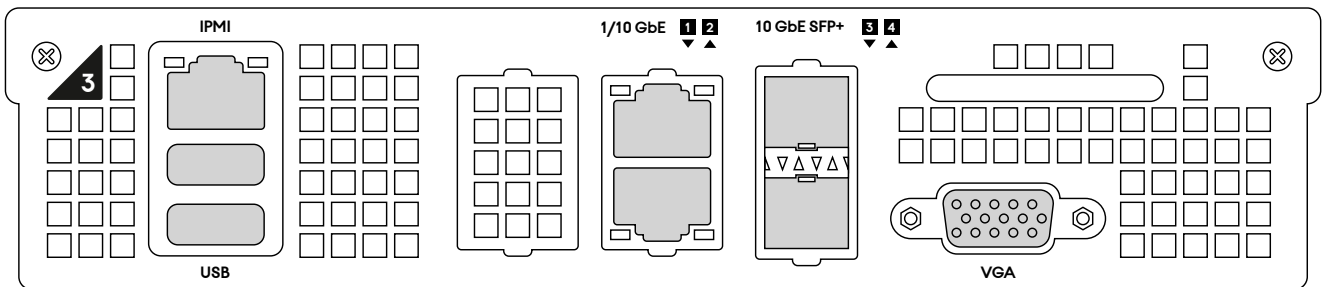
The appliance consists of five identical nodes. On the front of the appliance, under the front bezel are the power/reset buttons, a power LED of each node as well as the main power switch. The front panel also provides access to disks of each node: three per node, ordered left to right, i.e. the leftmost three disks are of node #1, the next three are of node #2, etc.



On the back of the appliance are two power sockets and a number of connectivity options.



Each node has its own network, IPMI, USB, and VGA ports.



The IPMI, USB, and VGA ports are only needed for advanced diagnostics. IPMI allows accessing the nodes over the network for out-of-band management via a remote console. The USB and VGA ports allow you to connect a keyboard and a monitor to a node if the network is unavailable.

Day-to-day management of the appliance is done over the network through the admin panel, as described later in the guide.

CHAPTER 2

Safety Instructions

Warning: The appliance may only be repaired by a certified service technician. You may only perform troubleshooting as authorized by the support team. Damage due to unauthorized repairs is not covered by the warranty.

CHAPTER 3

Installing the Appliance

Before installing the appliance, make sure you have the following:

- 3U of server rack space,
- at least ten free 1/10 GbE ports in a network switch (10 GbE recommended),
- at least ten RJ45-to-RJ45 patch cables to connect the appliance to the switch,
- at least six free 1 GbE ports in a network switch for out-of-band management,
- two power sockets.

To install the appliance, perform the following steps:

1. Unpack the appliance.
2. Mount the appliance into rack and connect cables.
3. Configure the appliance using the wizard.
4. Log in to the admin panel and install a license.
5. Set up the desired workload in the admin panel.

These major steps are described in more detail in the following sections.

3.1 Unpacking the Appliance

Inspect the packaging contents for damage before mounting the appliance and connecting power.

The following items will be located in the packaging. Make sure that the following contents are present

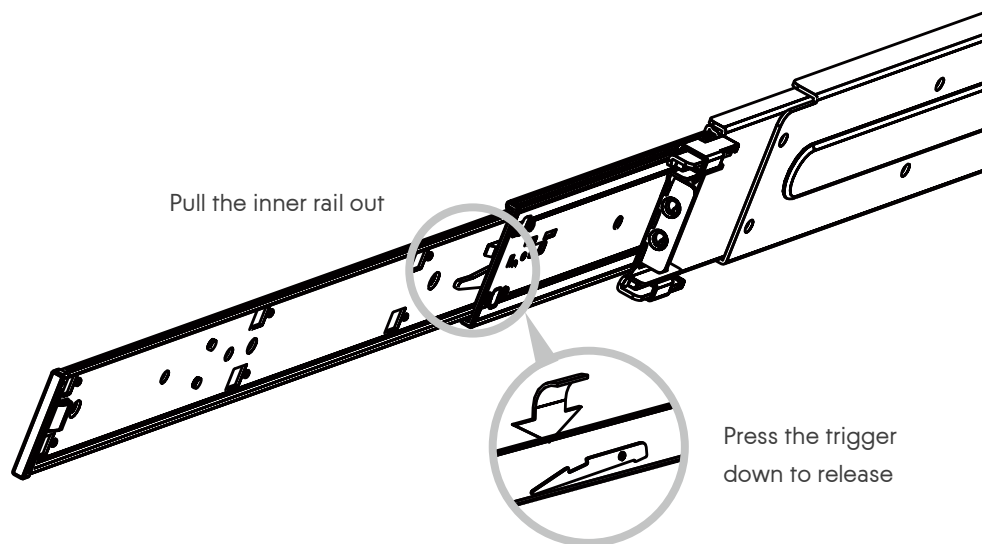
before continuing: the appliance chassis, mounting rails, two power cables, this quick start guide.

3.2 Mounting the Appliance into Rack

The appliance comes with a set of server rails. Follow the steps further to install the rail and mount the appliance into the rack.

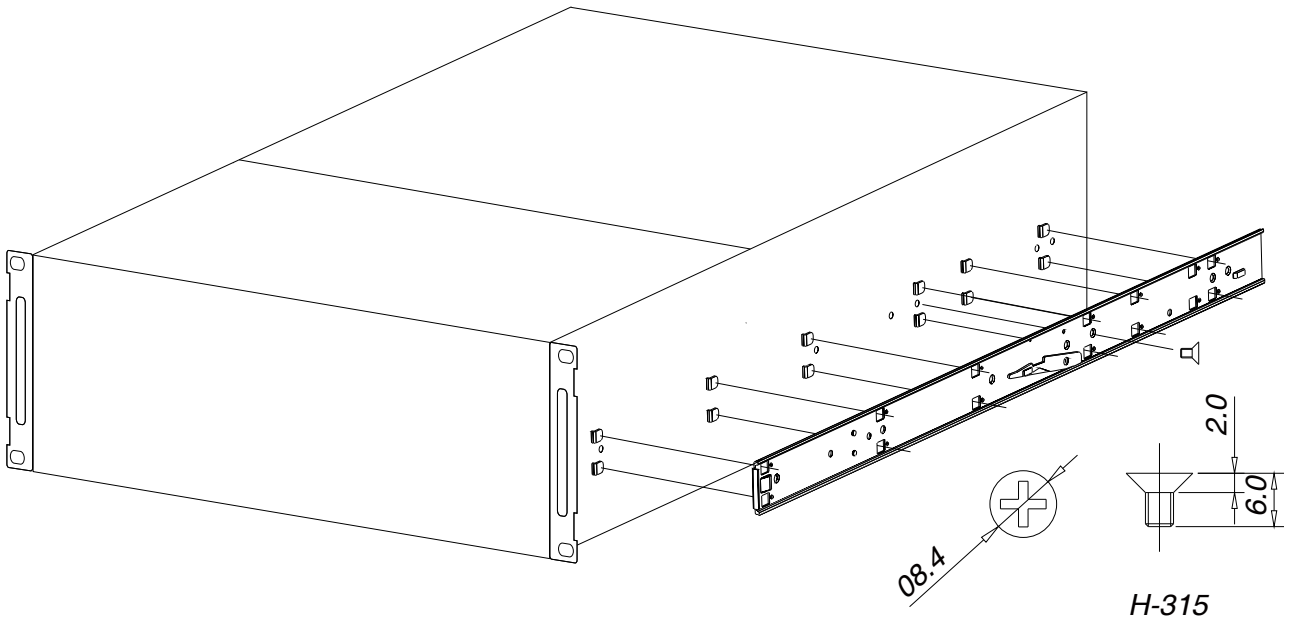
1. Separate inner and outer rails.

Separate the inner rail from the outer rail by sliding the inner rail forward until the locking tab is visible, per the illustration below. Depress the tab and separate the inner rail from the outer rail by sliding the two apart.



2. Attach the inner rail to the appliance.

Align the rectangular cut-outs on the inner rail to the pre-formed bayonets on the side of chassis. Secure the inner rail with a screw from the standard screw kit after all the bayonets go through the cutouts and properly engage.

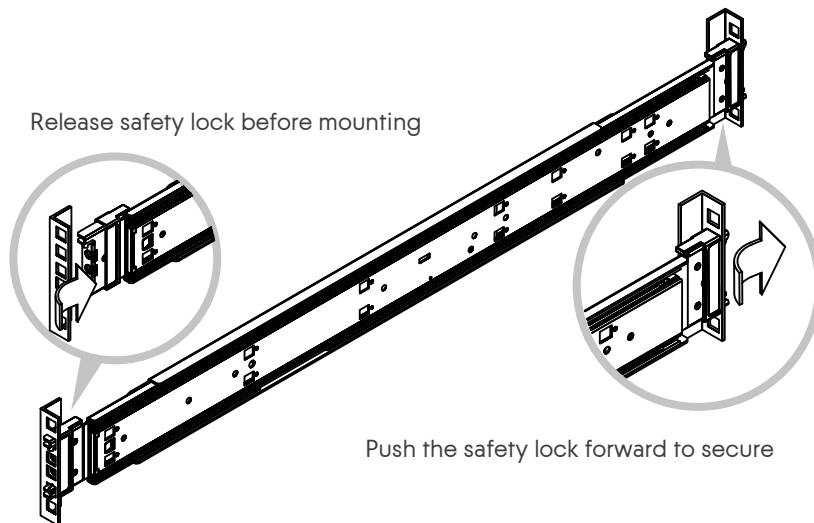


3. Install the outer rail into the rack.

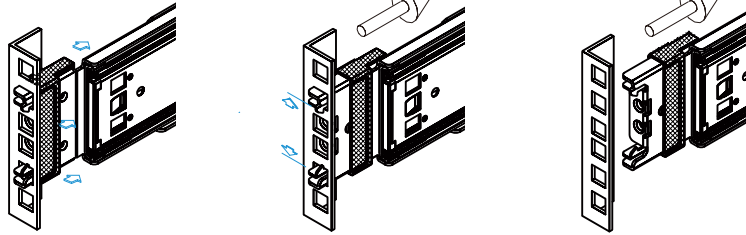
When selecting the location, note that the rails are in the middle of the appliance. Make sure that you install the outer rails with 1U clearance above and below.

Make sure that the safety lock is unlocked before mounting the brackets.

Insert the locating pins into the upper and lower square holes on the rail from the back of rail. Push the safety lock forward to secure the bracket.



Uninstall the bracket

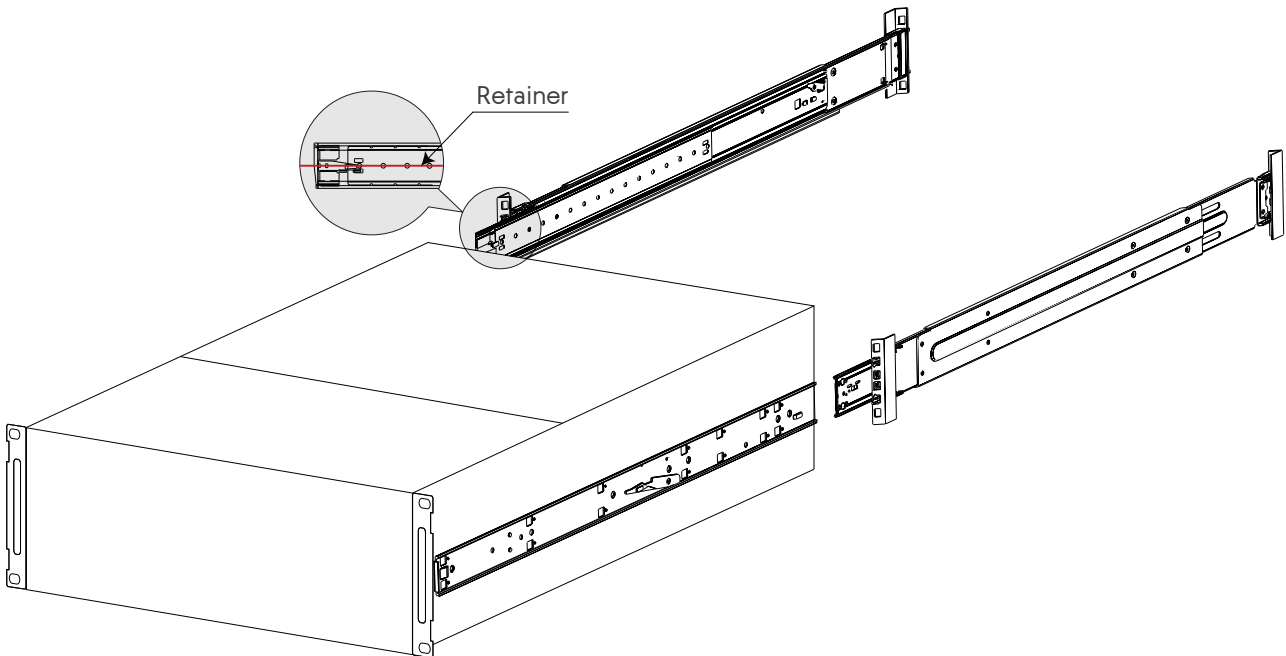


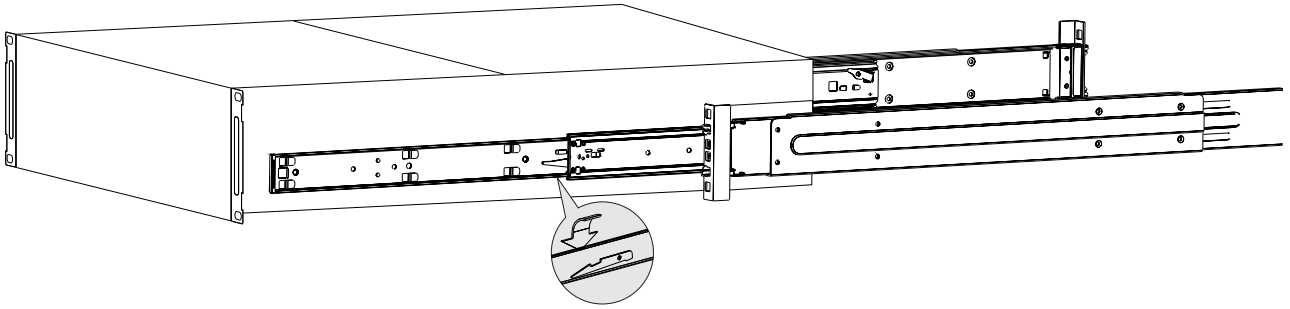
4. Mount the chassis into the cabinet.

Important: Two people are required to perform this step.

Insert the inner rail into the outer rail as shown on the figure.

Important: Make sure that the ball retainer is fully open before installing the chassis. Otherwise, you risk damaging the chassis!



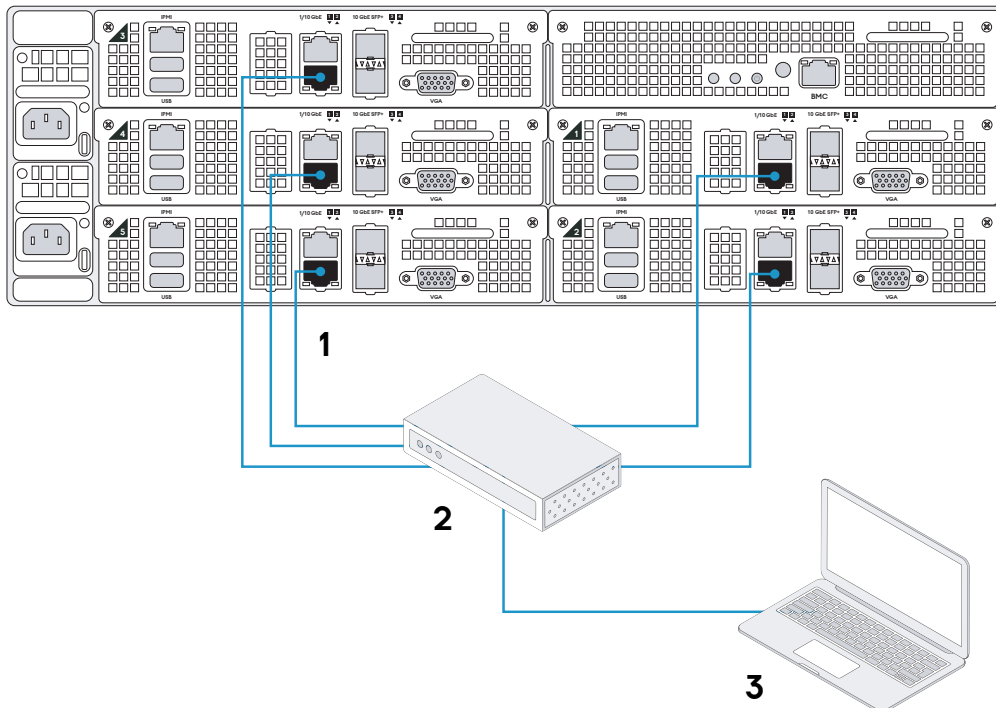


3.3 Connecting Cables to the Appliance

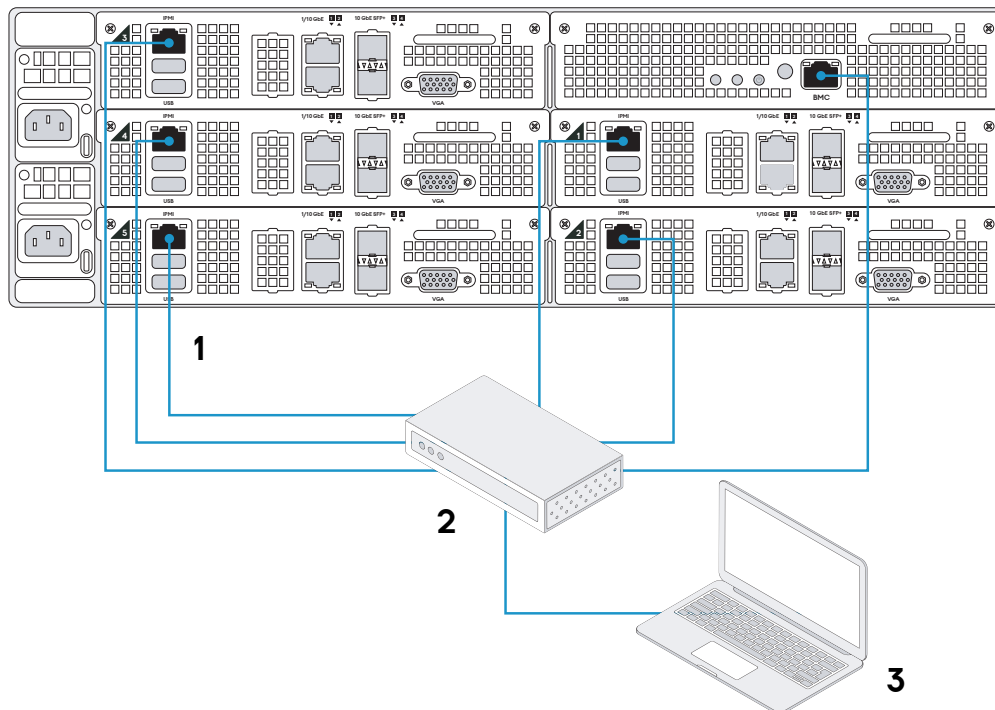
Note: For more details on configuring the network infrastructure, see the complete *Installation Guide*.

To prepare the appliance for configuration, do the following:

1. Connect the appliance to the electrical outlets using the supplied power cables.
2. Connect network interfaces #1 of all nodes (**1** on the diagram) to a switch (**2** on the diagram) with access to a dedicated subnet for your software-defined infrastructure. The nodes have preconfigured IP addresses: 10.20.20.11 to 10.20.20.15. Connect the admin laptop (**3** on the diagram) to the same switch.



- (Optional) Connect the out-of-band management network interfaces of each node and the chassis (1 on the diagram) to a switch with access to the IPMI subnet for your appliance (2 on the diagram). The nodes have preconfigured IPMI IP addresses: 10.20.30.11 to 10.20.30.15. The chassis has the preconfigured IPMI IP address 10.20.30.10. Connect the admin laptop (3 on the diagram) to the same switch.



3.4 Configuring the Appliance

Perform the following steps to configure the appliance:

- Turn on the power: (a) press and hold down the main switch for five seconds, (b) press the power buttons of each node.
- Connect an admin laptop (from which you will configure the appliance) to the network. Assign a static IP address to it from the same subnet that nodes are in, e.g., 10.20.20.100. As mentioned before, the nodes have preconfigured IP addresses: 10.20.20.11 to 10.20.20.15.
- On this computer, open a web browser and visit the default primary node IP address 10.20.20.11. The wizard has been tested to work in the latest Firefox, Chrome, and Safari web browsers.
- Once the configuration wizard is displayed, click **Configure**.



5. Review and accept the license agreement then click **Next**.

Configure appliance

Software license agreement

Read the user agreement, if you agree with the terms of the agreement, confirm it

future updates to the Acronis Privacy Statement and the Acronis Licensing Policy, each of which may be updated from time to time (see <http://www.acronis.com/Legal.htm>), constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. You may not assign or transfer any of your rights or obligations under this Agreement to a third party without the prior written consent of Acronis. Acronis may freely assign this Agreement. Any attempted assignment or transfer in violation of the foregoing will be void.

12 CONTACTING ACRONIS

Users with questions about this Agreement or the Privacy Statement may contact Acronis at: www.acronis.com/support.

13 CHANGES TO THIS AGREEMENT

Acronis may amend this Agreement including any referenced policies and other documents from time to time. If we make material changes to this Agreement, we will notify You by posting the change on our website or sending You an e-mail at your primary email address. Any changes to this Agreement will be effective immediately for new end users; otherwise for existing end users, the changes will be effective upon the earlier of thirty (30) calendar days following e-mail notice to You or thirty (30) calendar days following our posting of the notice on our website.

I accept the End-User License Agreement

Next

6. On the next step, enter the following:

- New host names for all nodes (or leave the default names). You can rename the nodes to fit your organization's naming policies or make them relevant to your organization.

- New static IP addresses for network interfaces 1 on all nodes. If you leave the fields empty, the default addresses 10.20.20.11 to 10.20.20.15 will be used.
- Network mask. Consult your network administrator for the proper network/subnet mask.
- At least one local DNS server.
- Gateway. Consult your network administrator for the proper gateway address.
- Domain name (optional). If this system will be visible from the Internet or if you wish to bind it to your organization's domain, provide the domain prefix and suffix.
- Time zone and time. Since nodes communicate with each other, they must be on the same time zone and have the same time in order to ensure proper synchronization. Click **Change time settings** to set the correct time zone and time.

Important: Entered values cannot be changed later.

Configure appliance

Configure network parameters

Enter new IP addresses for the currently connected network interface 1 on each node and provide other details, including the network mask, DNS servers, gateway, and domain name.

<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ● node1 Master 172.20.201.11 </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ● node2 172.20.201.12 </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ● node3 172.20.201.13 </div>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ● node4 172.20.201.14 </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> ● node5 172.20.201.15 </div>
---	---

Network mask	Gateway	DNS server	2nd DNS server (optional)
255.255.255.0	172.20.201.1	8.8.8.8	8.8.4.4

11:18 AM, W. Europe Standard Time — UTC+01:00 [Change time settings](#)

Back
Next

If one or more nodes are not reachable from the primary node, they will be marked as offline. In this case, make sure the nodes are powered on and connected to the correct network. Deployment will be

blocked until all nodes are green (accessible and configurable by the primary node).

Note: You will be able to configure bonds and VLANs later in the admin panel.

Click **Next**.

7. On the next step, enter the cluster name (you cannot change it later) and cluster administrator password.

Configure appliance

System parameters
Set up access to the appliance. Note that the cluster name cannot be changed later.

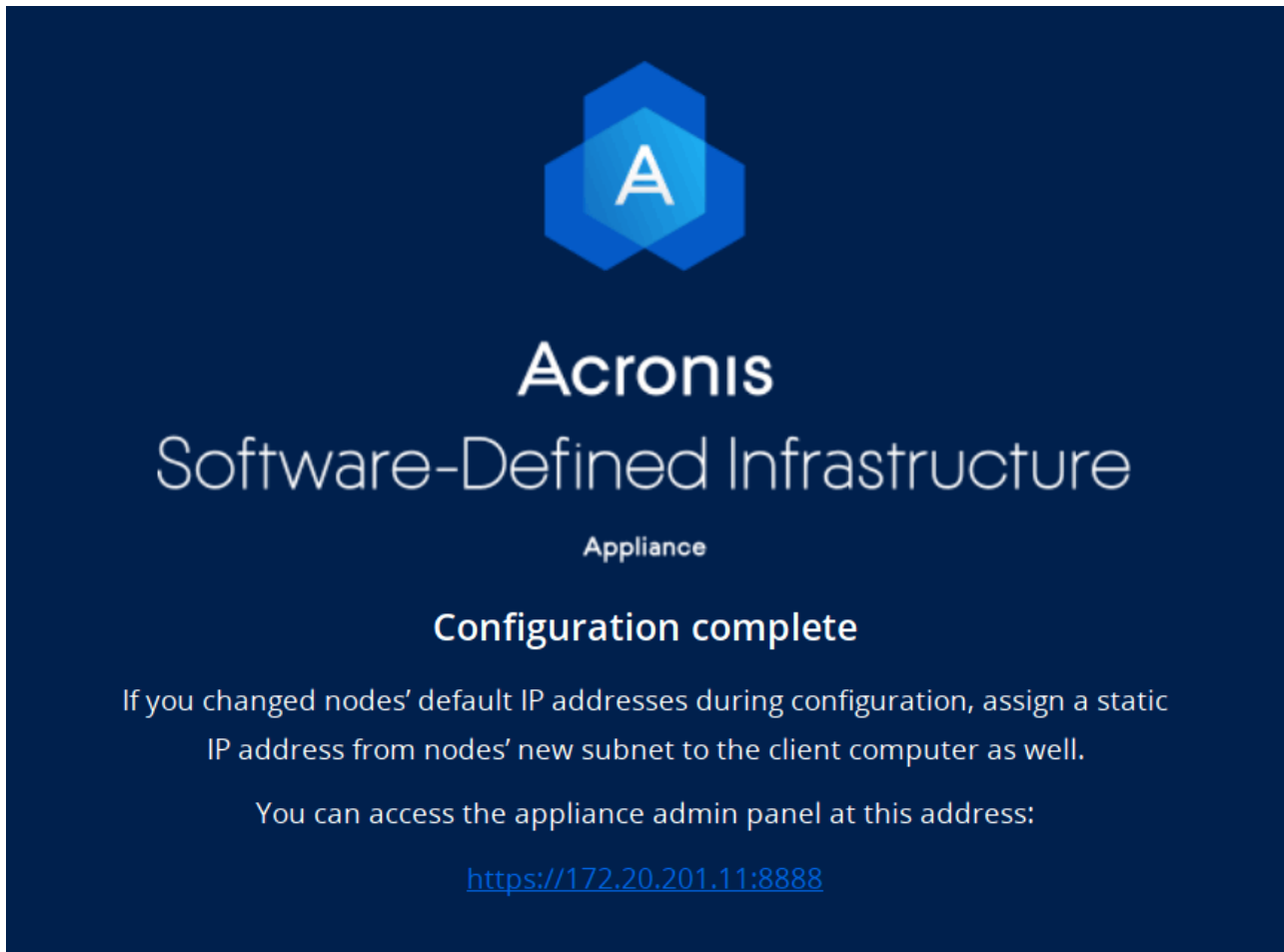
Cluster name

Administrator password

Confirm password

Click **Submit**. Configuration will begin, as indicated on the progress bar.

8. Wait until the progress bar reaches the end and change the IP address of the admin laptop to a free one from which you can access the appliance.
9. Once configuration is completed, you will see a link to the cluster admin panel. Log in with the username `admin` and the specified password. The admin panel has been tested to work at resolutions 1280x720 and higher in the latest Firefox, Chrome, and Safari web browsers.



10. Proceed to **SETTINGS** > **Licenses** and upgrade the default trial license either by a key or SPLA (for more details, see *Managing Licenses* (page 19)). If you do not have a license, contact your sales representative.
11. If you need to make additional changes to network configuration, e.g., create bonds and VLANs, connect cables to the network interface 2 and SFP slots and follow the instructions in the *Administrator's Guide*.

After deployment, enable high availability of the management node as described in *Enabling High Availability* (page 14). After that you can configure the cluster for the desired workload as described in the *Administrator's Guide*.

CHAPTER 4

Enabling High Availability

High availability keeps Acronis Software-Defined Infrastructure services operational even if the node they are located on fails. In such cases, services from a failed node are relocated to healthy nodes according to the [Raft consensus algorithm](#). High availability is ensured by:

- Metadata redundancy. For a storage cluster to function, not all but just the majority of MDS servers must be up. By setting up multiple MDS servers in the cluster you will make sure that if an MDS server fails, other MDS servers will continue controlling the cluster.
- Data redundancy. Copies of each piece of data are stored across different storage nodes to ensure that the data is available even if some of the storage nodes are inaccessible.
- Monitoring of node health.

To achieve complete high availability of the storage cluster and its services, we recommended that you do the following:

1. deploy three or more metadata servers,
2. enable management node HA, and
3. enable HA for the specific service.

Note: The required number of metadata servers is deployed automatically on recommended hardware configurations; Management node HA must be enabled manually as described in the next subsection; High availability for services is enabled by adding the minimum required number of nodes to that service's cluster.

On top of highly available metadata services and enabled management node HA, Acronis Software-Defined Infrastructure provides additional high availability for the following services:

- Admin panel. If the management node fails or becomes unreachable over the network, an admin panel instance on another node takes over the panel's service so it remains accessible at the same dedicated IP address. The relocation of the service can take several minutes. Admin panel HA is enabled manually (see *Enabling Management Node High Availability* (page 16)).
- iSCSI service. If the active path to volumes exported via iSCSI fails (e.g., a storage node with active iSCSI targets fails or becomes unreachable over the network), the active path is rerouted via targets located on healthy nodes. Volumes exported via iSCSI remain accessible as long as there is at least one path to them.
- S3 service. If an S3 node fails or becomes unreachable over the network, name server and object server components hosted on it are automatically balanced and migrated between other S3 nodes. S3 gateways are not automatically migrated; their high availability is based on DNS records. You need to maintain the DNS records manually when adding or removing S3 gateways. High availability for S3 service is enabled automatically after enabling management node HA and creating an S3 cluster from three or more nodes. An S3 cluster of three nodes may lose one node and remain operational.
- Backup gateway service. If a backup gateway node fails or becomes unreachable over the network, other nodes in the backup gateway cluster continue to provide access to the chosen storage backend. Backup gateways are not automatically migrated; their high availability is based on DNS records. You need to maintain the DNS records manually when adding or removing backup gateways. High availability for backup gateway is enabled automatically after creating a backup gateway cluster from two or more nodes. Access to the storage backend remains until at least one node in the backup gateway cluster is healthy.
- NFS shares. If a storage node fails or becomes unreachable over the network, NFS volumes located on it are migrated between other NFS nodes. High availability for NFS volumes on a storage node is enabled automatically after creating an NFS cluster.

Also take note of the following:

1. Creating the compute cluster prevents (and replaces) the use of the management node backup and restore feature.
2. If nodes to be added to the compute cluster have different CPU models, consult the section "Setting Virtual Machines CPU Model" in the *Administrator's Command Line Guide*.

4.1 Enabling Management Node High Availability

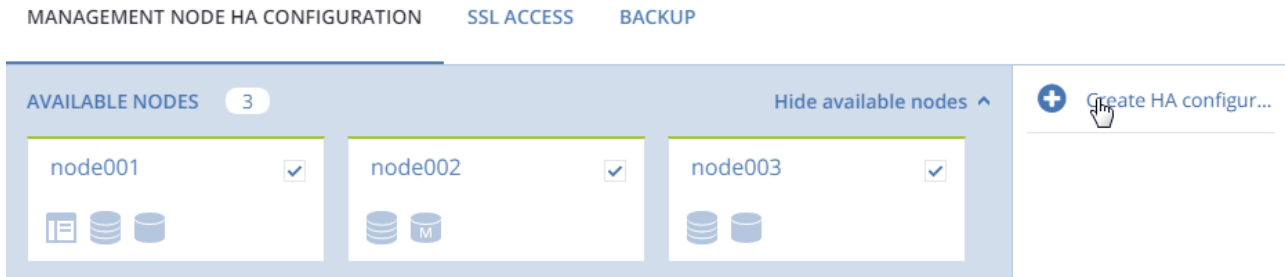
Management node HA and compute cluster are tightly coupled, so changing nodes in one usually affects the other. Take note of the following:

1. Each node in the HA configuration must meet the requirements to the management node listed in the *Installation Guide*. If the compute cluster is to be created, its hardware requirements must be added as well.
2. The HA configuration must include at least three nodes at all times. Because of this, removing nodes from the HA configuration (whether or not the compute cluster exists) is only possible if the required minimum remains after removal. For example, to remove one of the minimum three nodes from the HA configuration, a fourth node must be added to it first.
3. If the HA configuration has been created before the compute cluster, all nodes in it will be added to the compute cluster.
4. If the compute cluster has been created before HA configuration, only nodes in the compute cluster can be added to the HA configuration. For this reason, to add a node to HA configuration, add it to the compute cluster first.
5. If both the HA configuration and compute cluster include the same four or more nodes, a node must first be removed from the HA configuration to be removed from the compute cluster.

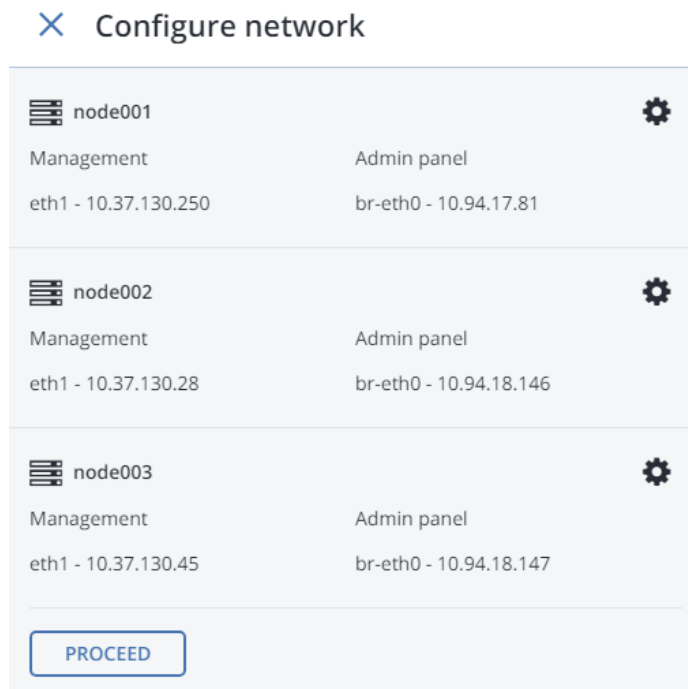
If both the HA configuration and compute cluster include the same three nodes (the required minimum), single nodes cannot be removed from the compute cluster. In such a case, the compute cluster can be destroyed completely, but the HA configuration will remain; this is also true vice versa, the HA configuration can be deleted, but the compute cluster will continue working.

To enable high availability for the management node and admin panel, do the following:

1. Make sure that each node is connected to a network with the **Admin panel** traffic type.
2. On the **SETTINGS > Management node** screen, open the **MANAGEMENT NODE HA CONFIGURATION** tab.



3. Select three to five nodes and click **Create HA configuration**.
4. On **Configure network**, check that correct network interfaces are selected on each node. Otherwise click the cogwheel icon for a node and assign networks with the **Internal management** and **Admin panel** traffic type to its network interfaces. Click **PROCEED**.



5. Next, on **Configure network**, provide one or more unique static IP addresses for the highly available admin panel, compute API endpoint, and interservice messaging. Click **DONE**.

< Configure network

Assign unique dedicated virtual IP addresses to these services:

- Admin panel (public access to this web UI)
- Compute API (public access to compute APIs)
- Internal management (private interservice messaging)

In an HA event, virtual IP addresses will automatically migrate to a healthy node in the management HA cluster to keep services accessible.

Virtual IP address for
Compute API, Admin panel

Virtual IP address for
Internal management

DONE

Once the high availability of the management node is enabled, you can log in to the admin panel only at the specified static IP address (on the same port 8888).

To remove nodes from the HA setup, select them in the list on the **MANAGEMENT NODE HA** tab and click **Release nodes**.

CHAPTER 5

Managing Licenses

The appliance comes with a three-year license to all its storage space. After three years, you will need to prolong the subscription. Alternatively, you can switch to SPLA licensing and use the appliance with Acronis Data Cloud.

Acronis Software-Defined Infrastructure supports the following licensing models for production environments:

- 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.
- 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 these resources. With SPLA, Acronis Software-Defined Infrastructure automatically sends reports to Acronis Data Cloud once every four hours. If no reports have been received for two weeks, the license expires.

Note: SPLA license is valid for Cloud Partners. If SPLA is enabled, you can connect Backup Gateway only to Acronis Backup Cloud and not to Acronis Backup 12.5 or Acronis Backup Advanced 12.5. To connect ABGW to these products, you will need to use license keys. Furthermore, Acronis Backup Gateway usage is not counted in SPLA in Acronis Software-Defined Infrastructure. SPLA only counts universal usage that is not related to backup. Backup usage is shown in the Acronis Backup Cloud section of Acronis Data Cloud.

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.

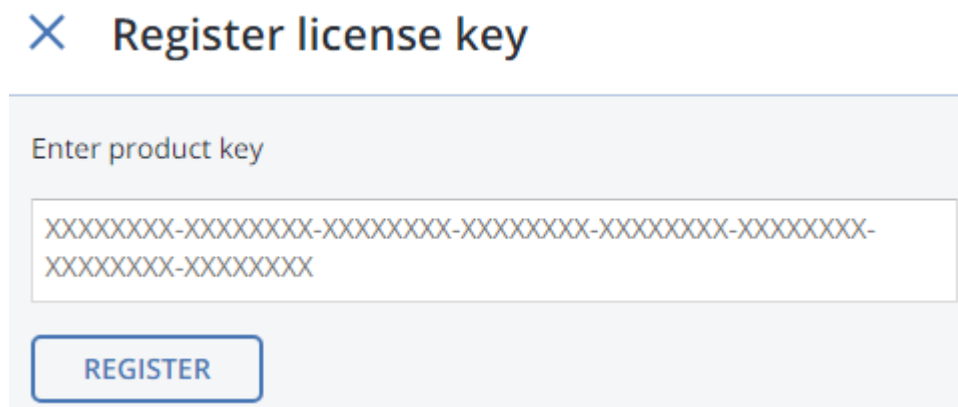
- Switching from SPLA to a license key changes the licensing model to subscription or perpetual. After doing so, ask your service provider to terminate your SPLA by either disabling the Storage application for your account or deleting the account.

Important: If a license expires, all write operations to the storage cluster stop until a valid license is installed.

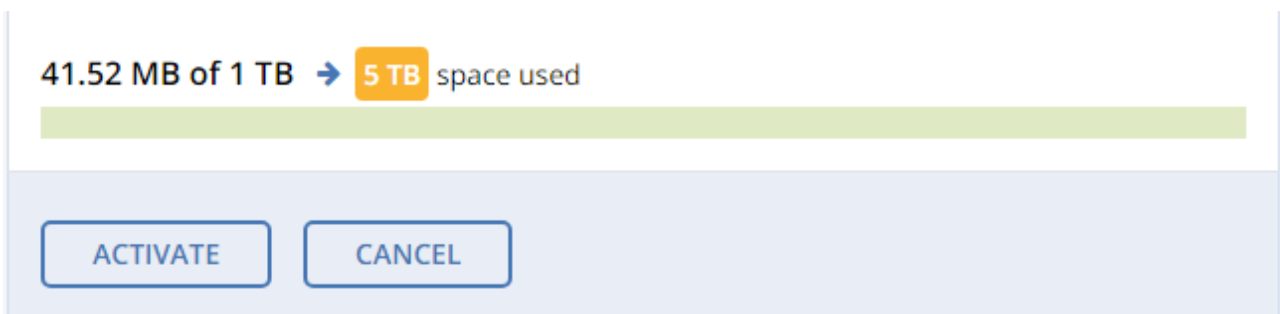
5.1 Installing License Keys

To install a license key, do the following:

1. If you are switching from SPLA, ask your service provider to terminate the agreement by either disabling the **Software-Defined Infrastructure** application for your account or deleting the account.
2. On the **SETTINGS > Licenses** screen, click **Upgrade** and **Register key**.



3. In the **Register license key** window, paste the license key and click **REGISTER**.



4. Back on the **Licenses** screen, click **Activate** if you are activating from a trial or choose one of the

following:

41.52 MB of 5 TB space used

Choose an activation option:

Upgrade

Prolong

ACTIVATE CANCEL

- **Upgrade**, to add storage capacity to the active license.
- **Prolong**, to prolong the soon-to-be-expired license.

And click **Activate**.

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

5.2 Installing SPLA Licenses

To install a SPLA license, do the following:

1. On the **SETTINGS > 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 login page of Acronis Data Cloud.

Note: For more information on datacenters, see <https://kb.acronis.com/servicesbydc>.

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.

CHAPTER 6

Getting Technical Support

If you need technical support, please contact Acronis as follows:

1. Visit the contact support page at <https://www.acronis.com/en-us/support/contact-us/>.
2. Log in to your account.
3. Select the product you are using.
4. Choose how you would like to contact the support team: via e-mail or phone.

Please be ready to provide support engineers with remote access to your appliance, per your Service Level Agreement. To maintain security, it is recommended to whitelist only specific IP addresses communicated to you by support engineers and block external access from any other addresses. For more information, see the Knowledge Base at <https://kb.acronis.com/sdiremote>.

You can also use the following self-service resources:

- Knowledge base, <https://kb.acronis.com/>, a repository of frequently asked questions, step-by-step instructions, and articles about known issues. Visit the following knowledge base sections for information on this appliance and related software solutions:
 - Appliance, <https://kb.acronis.com/acronis-appliance>
 - Acronis Cyber Infrastructure, <https://kb.acronis.com/acronis-cyber-infrastructure>
 - Acronis Backup Cloud, <https://kb.acronis.com/acronis-backup-cloud>
 - Acronis Backup 12.5, <https://kb.acronis.com/acronis-backup-12-5>
- User documentation, guides describing how to use this appliance as well as Acronis software, <https://www.acronis.com/support/documentation>.

For information on appliance warranty, see the Support section at <https://www.acronis.com/en-us/support/hwappliancesupport>.

CHAPTER 7

Appendix: Specifications

This chapter lists technical and environmental specifications of the appliance.

7.1 Technical Specifications

The following table lists appliance hardware parts.

Chassis	3U
CPU	Intel Atom C3958 @ 2.00GHz, 16 cores, 31W TDP, VT-d support, w/o Hyper-Threading
RAM	32GB (up to 256GB), Samsung, 2x16GB DDR4-2400 ECC
OS drive	1x Intel S4600 240GB 2.5-inch SSD
Cache drive	1x Intel S4600 240GB 2.5-inch SSD
Storage drives	3x Seagate 4/8/10/12TB enterprise SATA HDD per node, 15x in total
Network	2x 1/10GbE RJ45, 2x 10GbE SFP+
Power supply	750W 1+1, current share and cold redundancy depending on power loads (also see table below)
IO ports	Rear: 2x USB 2.0, 1x VGA, 2x 1/10GbE RJ45, 2x 10GbE SFP+, 1x GbE RJ45 management
Software	Acronis Software-Defined Infrastructure 2.5
Data protection	Replication and erasure coding via storage policies

Continued on next page

Table 7.1.1 – continued from previous page

Redundancy	Hot-swappable data disk drives 2x hot-swappable power supplies No single point of failure Non-disruptive online software upgrades
Monitoring, management	CLI, GUI, API, IPMI

7.1.1 Power Supply Specifications

The following table lists appliance power supply specifications.

Voltage, frequency	100-240 V, 50/60 Hz			
Power consumption, W	750			
Heat dissipation max (BTU/hr)	2,300			
Max inrush, A	40			
Input current	AC input		Max. current	
	100–127 Vac, 8.8 A		200–240 Vac, 4.3 A	
Power supply efficiency (Platinum class)	10% load	20% load	50% load	100% load
	80%	90%	94%	91%
Input power factor correction*	Output power	20% load	50% load	100% load
	Power factor	>0.80	>0.95	>0.95

* Tested at 230 Vac, 50 Hz and 115 Vac, 60 Hz. The input power factor is greater than values in the table at power supply's rated output and meets Energy Star® requirements.

7.1.2 Chassis Dimensions and Weight

Appliance chassis dimensions are 435x130x600 (WxHxD).

The total weight of the chassis is 34.5 kg.

7.2 Environmental Specifications

Appliance environmental specifications are listed in the following tables.

Store temperature	-40°C to 85°C (-40°F to 185°F)
Store temperature gradient	20°C (68°F) per hour
Operating temperature	10°C to 35°C (50°F to -95°F)
Operating temperature gradient	20°C (68°F) per hour
Relative humidity percentage range for storage	10% ~ 95% (non-condensing)
Relative humidity percentage range for operating	10% ~ 85% (non-condensing)
Vibration for storage	1.87 Grms (10-500 Hz)
Vibration for operating	0.26 Grms (5-350 Hz)
Shock for storage	65G for 2ms
Shock for operating	5G
Altitude for storage	12,000m (39,370 ft)
Altitude for operating	3,048m (10,000 ft)

7.2.1 Air Quality Requirements

The air must be free of:

- Corrosive dust and/or corrosive contaminants;
- Conductive dust or conductive particles (such as zinc whiskers).

Airborne residual dust must have a deliquescent point* less than 60% relative humidity. (*The relative humidity at which crystalline materials begin adsorbing large quantities of water from the atmosphere.)

Gaseous corrosion level in terms of (in Angstrom) as per ISA:

- Copper reactivity rate must be less than 300 Å/month, class G1(ANSI/ISA71.04-1985).
- Silver reactivity rate must be less than 200 Å/month (AHSRAE TC9.9).