Acronis

Acronis Cyber Appliance

Table of contents

1 About Acronis Cyber Appliance

Acronis Cyber Appliance provides a 5-node Acronis Cyber Infrastructure cluster in a 19-inch 3U rackmount server chassis. Acronis Cyber Appliance deploys into a universal and easy-to-use software-defined infrastructure solution that combines virtualization and storage. Powered by Acronis Cyber Infrastructure, it allows you to create and manage virtual machines, and offers object, block, and file storage, including a local repository for cloud backups. You can also deploy Acronis Cyber Backup in the Acronis Cyber Infrastructure compute cluster, and have both the storage and the backup server running on Acronis Cyber Appliance.

Acronis Cyber Appliance comes in several models, which vary by storage capacity:

Model	Raw storage, TB	Usable storage[1], TB	
		Capacity	Performance
15031	60	31	18
15062	120	62	36
15078	150	78	45
15093	180	93	54
15108	210	108	60
15124	240	124	69

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

1.1 Acronis Cyber Appliance exterior

Acronis Cyber 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 the disks for each node: three per node, ordered left to right, that is, the leftmost three disks are for node #1, the next three are for node #2, etc.
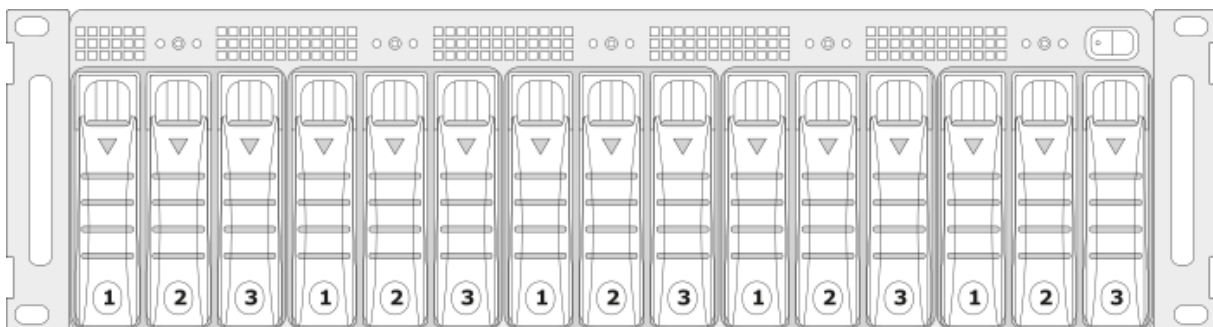
On the back of Acronis Cyber Appliance are two power sockets and a number of connectivity options.
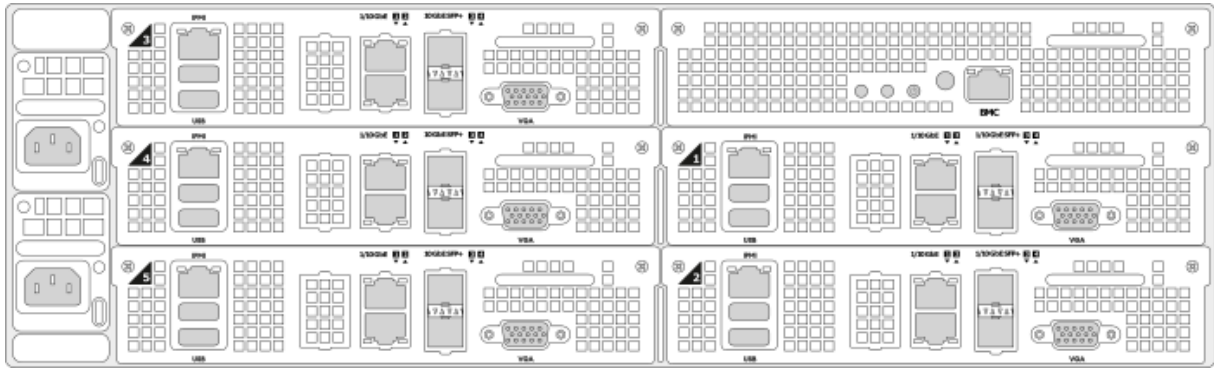
Each node has its own network, IPMI, USB, and VGA ports.
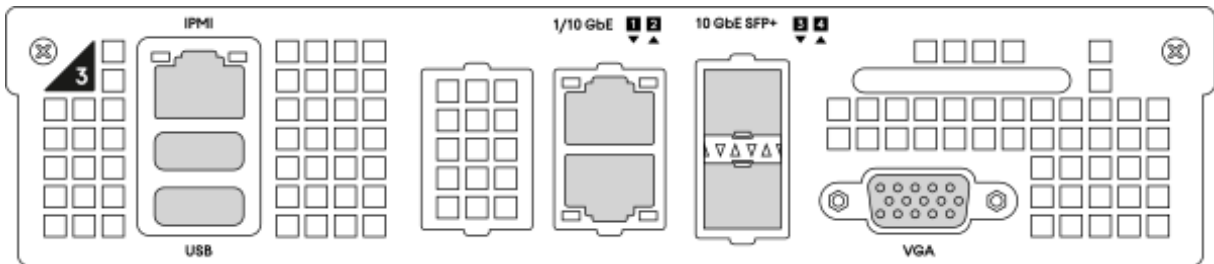
The IPMI, USB, and VGA ports are only needed for advanced diagnostics. IPMI allows accessing the nodes over the network for out-of-band management via a remote console. The default IPMI password to access the management node via SSH is **Acronis!Infra%30** (it changes to a user-specified password during deployment). 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 Acronis Cyber Appliance is done over the network through the admin panel, as described later in the guide.

2 Safety instructions

Warning!

Acronis Cyber 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.

If you need to reset a node to the factory default settings, contact the support, as described in "Getting technical support" (p. 29).

3 Installing Acronis Cyber Appliance

Before installing Acronis Cyber Appliance, make sure you have the following:

- 3U of server rack space in a standard 19-inch cabinet
- At least five free 1/10 GbE ports in a network switch (10 GbE recommended)
- At least five RJ45-to-RJ45 patch cables to connect the appliance to the switch
- Two power sockets

If you want to set up network bonding, you will additionally need (a) five free 1/10 GbE ports in a network switch (10 GbE recommended) and (b) five RJ45-to-RJ45 patch cables to connect the appliance to the switch.

If you want to have access to the nodes from a remote console for out-of-band management, you will additionally need (a) six free 1 GbE ports in a network switch and (b) six RJ45-to-RJ45 patch cables to connect the appliance to the switch.

To install Acronis Cyber Appliance, perform the following steps:

1. Unpack Acronis Cyber Appliance.
2. Mount the appliance into a rack.
3. Connect cables to the appliance.
4. Configure Acronis Cyber Appliance by using the wizard.
5. Log in to the admin panel and install a license.
6. Set up the desired workloads in the admin panel.

Steps one through five are described in the following sections. For more information about step six, refer to the Administrator Guide.

3.1 Unpacking Acronis Cyber Appliance

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

Before continuing, make sure the following items are present in the packaging: the appliance chassis, mounting rails, two power cables, and this quick start guide.

3.2 Mounting Acronis Cyber Appliance into rack

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

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

Pull the inner rail out

Press the trigger
down to release
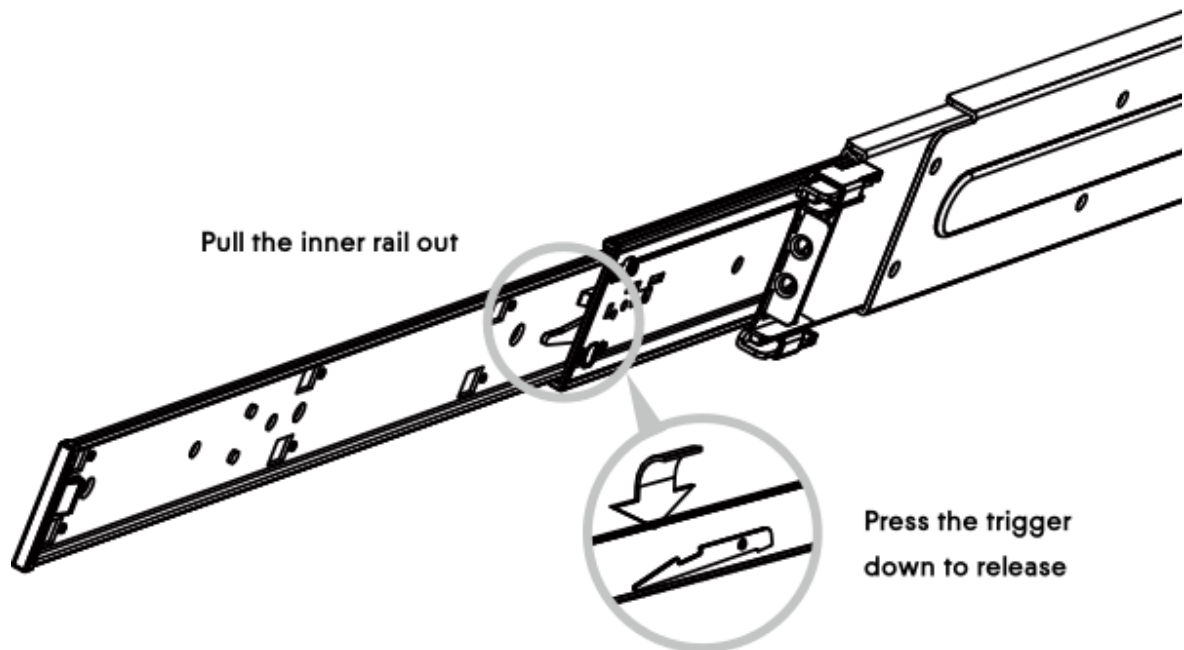
2. Attach the inner rail to the appliance.

   Align the rectangular cutouts on the inner rail to the pre-formed bayonets on the side of the chassis. Secure the inner rail with a screw from the standard screw kit after all the bayonets go through the cutouts and properly engage.
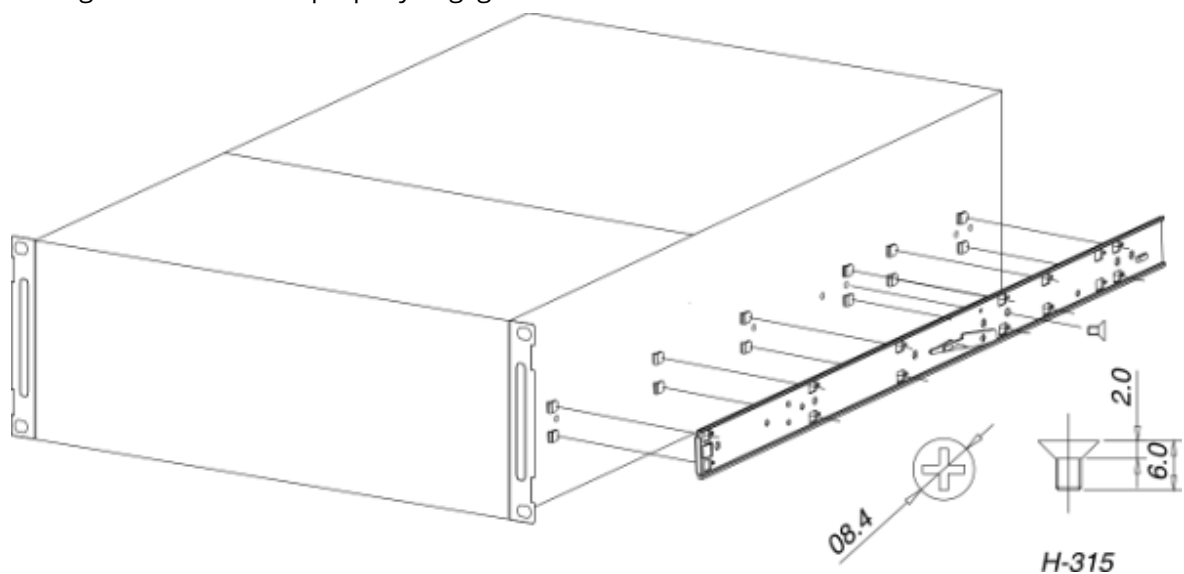
Ø8.4

2.0

6.0

H-315

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.

Release safety lock before mounting

Push the safety lock forward to secure

Uninstall the bracket
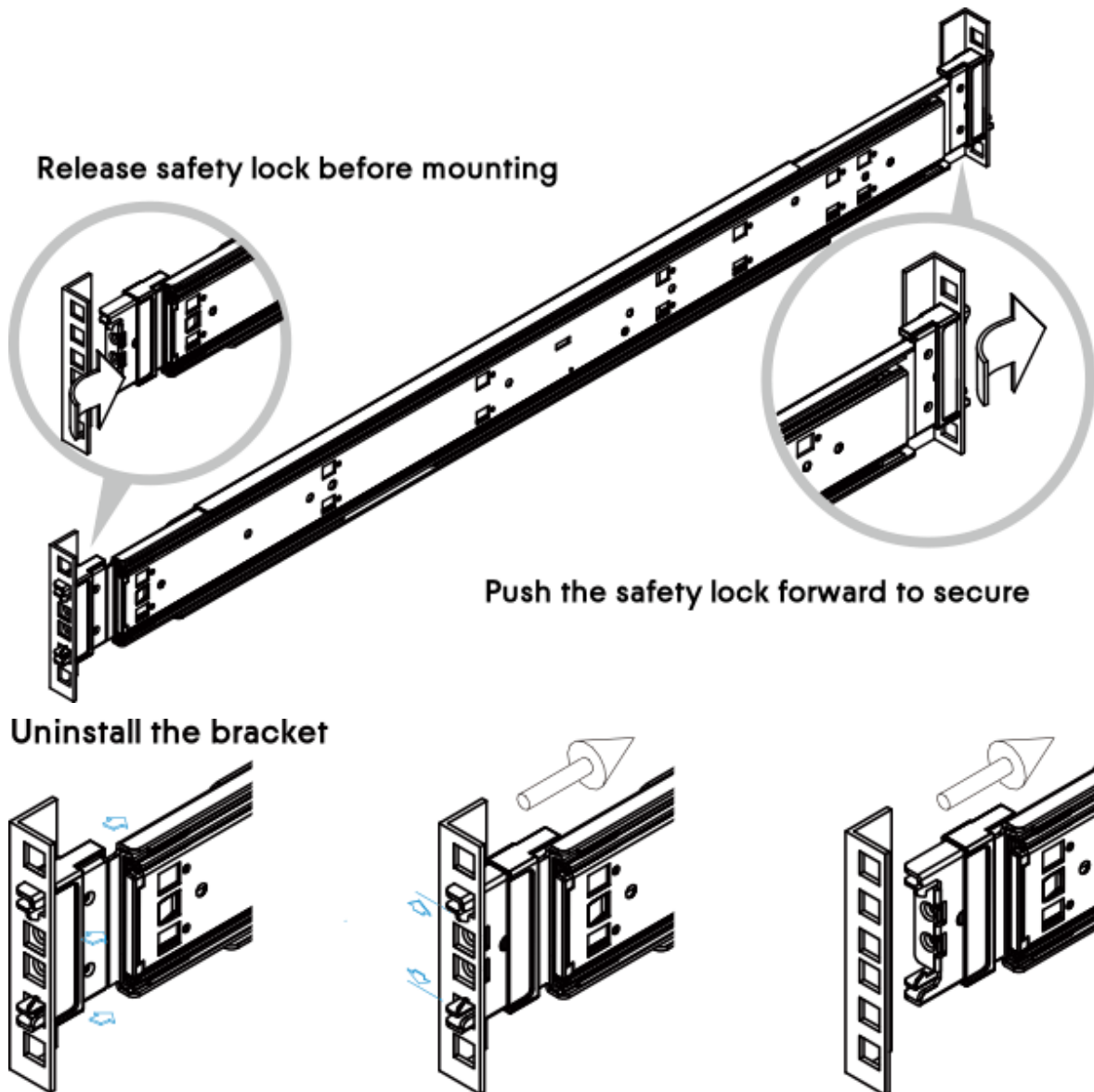
4. Mount the chassis into the cabinet.

Important
Two people are required to perform this step.

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

Important
Make sure that the ball retainer is fully open before installing the chassis. Otherwise, you risk damaging the chassis!
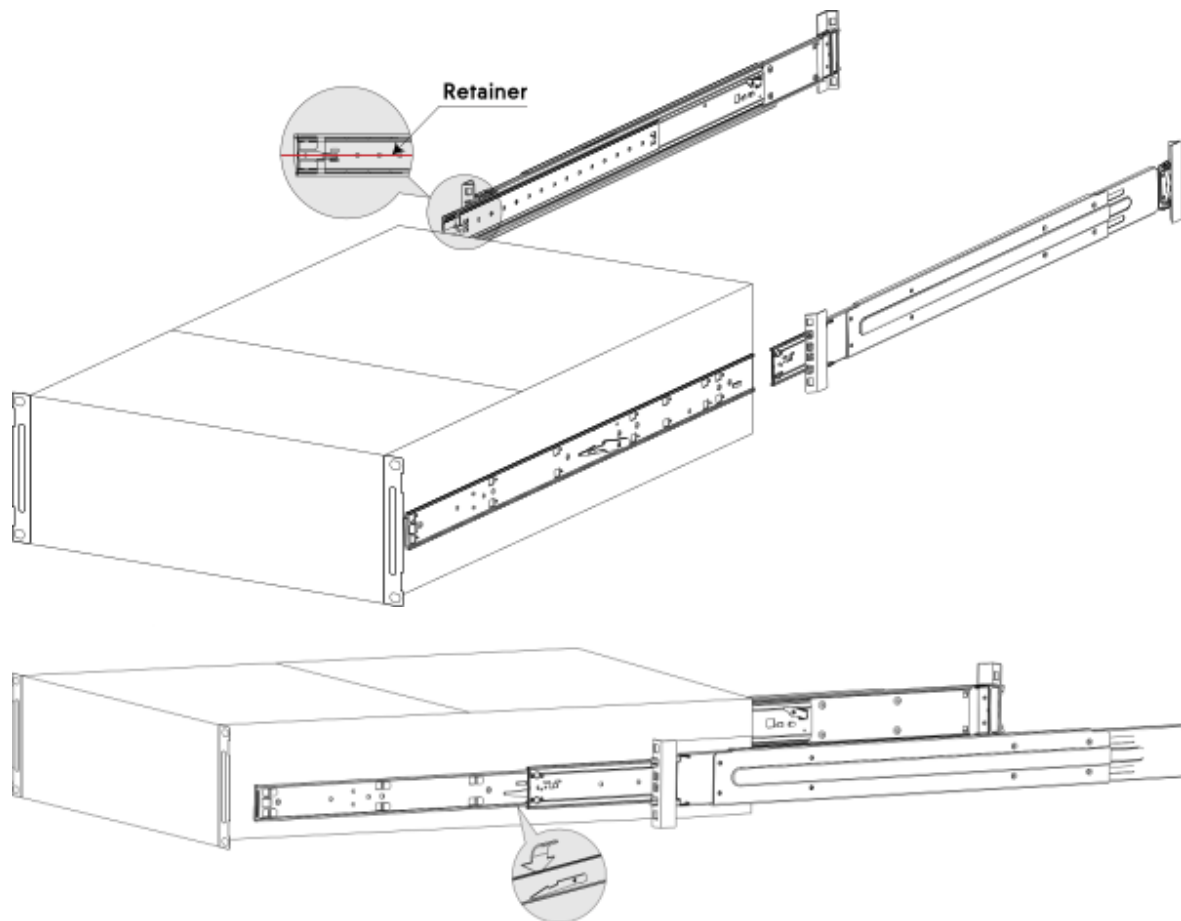
3.3 Connecting cables to Acronis Cyber Appliance

Note

For more details on configuring the network infrastructure, refer to the Administrator Guide.

To prepare Acronis Cyber Appliance for configuration, do the following:

1. Connect the appliance to the electrical outlets by using the supplied power cables.
2. On every node, connect any SFP+ or RJ45 network port (**1** on the diagram) to a switch (**2** on the diagram) with access to a dedicated subnet for your infrastructure. Then, connect the admin laptop (**3** on the diagram) to the same switch. The diagram below shows an example of the cable connection.
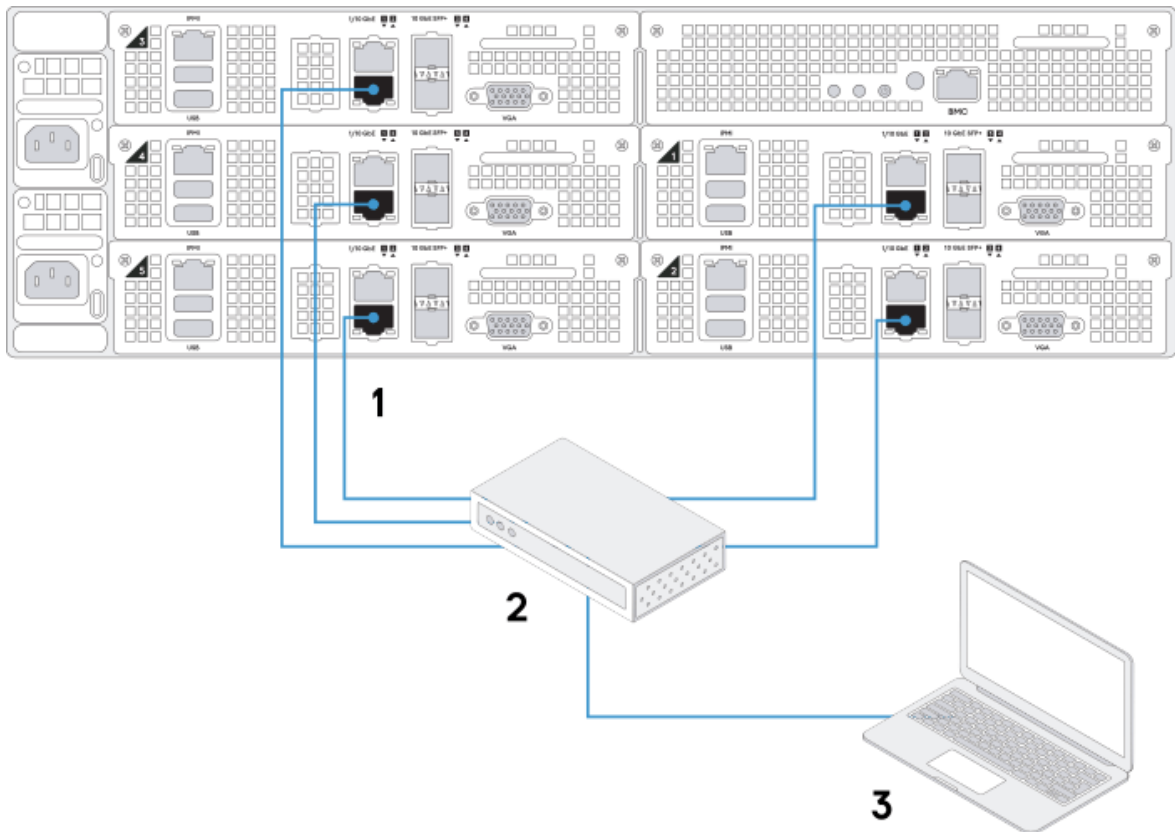
Important
The nodes have preconfigured IP addresses: 10.20.20.11 to 10.20.20.15.

---

3. (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.
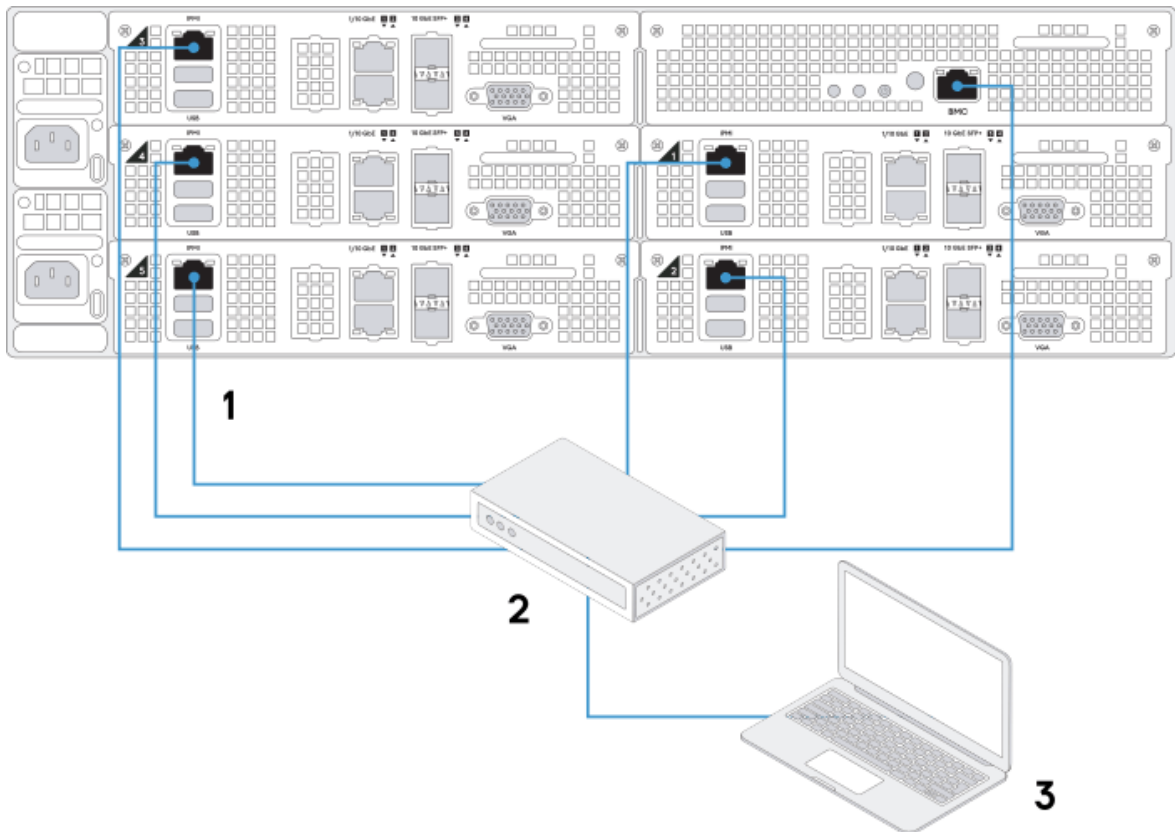
3.4 Configuring Acronis Cyber Appliance

Perform the following steps to configure Acronis Cyber Appliance:

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

In the wizard, you can create a new cluster or connect the appliance to a cluster already created with Acronis Cyber Infrastructure

3.4.1 Creating a new cluster

1. Once the configuration wizard is displayed, click **Configure**. Do not disconnect the appliance until the end of the configuration.
2. Review and accept the license agreement. Then, click **Next**.

Configure appliance

Accept license agreement
Read the user agreement. If you agree with its terms, accept it and proceed to the next step.

foregoing will be void.

12 CONTACTING ACRONIS

Users with questions about this Agreement or the Privacy Statement may contact Acronis at: https://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

🌐 Change language   Next

3. At the next step, select **Create a new cluster**.

Create a new cluster
◉   You will need to provide network parameters, name, and administrator password
for the new cluster. After deployment, you will have a ready-to-use cluster.

4. Under **Configure network parameters**, enter the following:
    - A gateway. Consult your network administrator for the proper gateway address.
    - A network mask. Consult your network administrator for the proper network/subnet mask.
    - At least one local DNS server.
    - A virtual IP address at which you will access the admin panel. You can read more about its high availability in the "Enable management node high availability" in the Administrator Guide.
    - New host names for all nodes (or leave the default names). Each node must have a unique name. Otherwise, the installation will stop. You can rename the nodes to fit your organization's naming policies.
    - New static IP addresses for the network interfaces connected on all the nodes. If you leave the fields empty, the default addresses of 10.20.20.11 to 10.20.20.15 will be used.

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. The deployment will be blocked until all nodes are green (which means they can be accessed and configured from the primary node).

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

---

5. Under **Appliance name**, enter the cluster name. You cannot change it later.

6. Under **Password**, enter a password to log in to the local Acronis Cyber Infrastructure admin panel.

Password

The password is required to log in to the local Acronis Cyber Infrastructure admin panel. The appliance will be accessible in a private network and via remote management in the Acronis Cyber Cloud.

Administrator password	Confirm password
••••••••	••••••••

The password must be at least 8 characters long, with at least one capital letter and one digit.

7. Under **Date and time**, it is recommended to select the **Set the date and time automatically** check box. You can clear it to select a custom time zone and time. Keep in mind that the nodes communicate with each other. Therefore, they must be on the same time zone and have the same time in order to ensure proper synchronization.

Date and time

Time zone configuration is required for the correct work with the cloud services

☑ Set the date and time automatically (recommended)

8. Click **Submit**. The configuration will begin, as indicated on the progress bar.
9. Wait until the progress bar reaches the end. If you changed the nodes' default IP addresses, assign a static IP address from the nodes' new subnet to the admin laptop from which you can access Acronis Cyber Appliance.

3.4.2 Joining the existing cluster

You can connect the appliance to the existing Acronis Cyber Infrastructure cluster. For this, you will need the private IP address of the management node and the administrator credentials for the existing cluster. After the appliance is configured, all five nodes will be added to and managed from the admin panel of the existing cluster.

1. Once the configuration wizard is displayed, click **Configure**. Do not disconnect the appliance until the end of the configuration.
2. Review and accept the license agreement. Then, click **Next**.

Configure appliance

Accept license agreement
Read the user agreement. If you agree with its terms, accept it and proceed to the next step.

foregoing will be void.

12 CONTACTING ACRONIS

Users with questions about this Agreement or the Privacy Statement may contact Acronis at: https://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

🌐 Change language   **Next**

3. On the next step, select **Join the existing cluster**.

⦿ **Join the existing cluster**
You will need to provide the management node IP address and administrator password of the existing cluster. After deployment, this appliance will be joined to the existing cluster and manageable from its admin panel.

4. Under **Configure network parameters**, enter the following:
   - A network mask. Consult your network administrator for the proper network/subnet mask.
   - New host names for all nodes (or leave the default names). You can rename the nodes to fit your organization's naming policies.

   Note
   Each node in the existing cluster and in the appliance must have a unique name. If at least two nodes have the same name, the installation will stop.

   - New static IP addresses for the network interfaces connected on all the nodes.

   Note
   Use IP addresses from the network/subnet of the existing cluster. The installation will be blocked until all of the five nodes are given IPs from the same subnet/network as the existing cluster.

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. The deployment will be blocked until all nodes are green (which means they can be accessed and configured from the primary node).

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

Configure network parameters
Enter new IP addresses for the currently connected network interfaces on each node and provide other details.

Network mask
255.255.255.0

Node name	IP address	Link	
node1	10.20.20.11	● Up	PRIMARY
node2	10.20.20.12	● Up	
node3	10.20.20.13	● Up	
node4	10.20.20.14	● Up	
node5	10.20.20.15	● Up	

5. Under **Join existing cluster**, enter the private IP address of the management node and the administrator password of the existing cluster.

Join existing cluster
Specify the management node's private IP address of the existing cluster.

Management node's private IP address
192.168.150.5

Specify the administrator password of the existing cluster.

Administrator password
● ● ● ● ● ●

6. During the deployment, the Acronis Cyber Infrastructure versions are compared in the existing cluster and in the appliance. If there are major discrepancies, you will be asked to specify a network configuration for access to the Internet. Then, the necessary updates will be downloaded, and the appliance will be upgraded or downgraded to match the version of the existing cluster.

3.4.3 Configuring the cluster by using the admin panel

1. Once the configuration is completed, you will see a link to the cluster admin panel. Log in with the username and password for the cluster.

2. If you need to make additional changes to the network configuration, for example, create bonds and VLANs, connect the cables to other network ports and follow the instructions in "Set up network bonding" and "Create VLAN interfaces" in the Administrator Guide.

3. In case you created a new cluster, update the product to the latest version after the deployment (refer to "Managing updates" (p. 21)). Proceed to **Settings** > **Licenses** and upgrade the default trial license either by a key or an SPLA (for more details, refer to "Managing licenses" (p. 18)). If you do not have a license, contact your sales representative.

4. Then, you can configure the cluster for using Acronis Cyber Backup (refer to "Configuring Acronis Cyber Infrastructure and Acronis Cyber Backup" (p. 23)), or another desired workload, as described in the Administrator Guide.

4 Managing licenses

Acronis Cyber Appliance is licensed for two types of deployments:

- Hybrid cloud. Comes with a 3-year hardware warranty and requires a subscription for Acronis Cyber Backup Cloud. After 3 years, the hardware warranty needs to be renewed for another 1 or 3 years.

  For this deployment type, you will need to install an SPLA license, as described in "Installing SPLA licenses" (p. 20).
- Private cloud. Comes with a 3-year license for Acronis Cyber Infrastructure and hardware warranty. After 3 years, both the license and warranty need to be renewed for another 1 or 3 years.

  For this deployment type, you will need to install a license key, as described in "Installing license keys" (p. 19).

For more details on licensing options, see https://kb.acronis.com/content/62324.

Acronis Cyber 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). The SPLA implements a pay-as-you-go model: it grants unlimited storage capacity and customers are charged for their actual usage of these resources. With an SPLA, Acronis Cyber Infrastructure automatically sends reports to Acronis Cyber Cloud once every four hours. The license is displayed with the expiration date of two weeks, which counts from the last sent report and is prolonged after each report. If no reports have been received for two weeks, the license expires. For reports to reach their destination, the cluster must be able to access the Acronis datacenter that has been used to enable the SPLA. Make sure that TCP port 443 is open.

  Note
  An SPLA license is valid for Cloud Partners. If an SPLA is enabled, you can connect Backup Gateway only to Acronis Cyber Backup Cloud and not to Acronis Cyber Backup. To connect Backup Gateway to these products, you will need to use license keys. Furthermore, Acronis Backup Gateway usage is not counted in the SPLA in Acronis Cyber Infrastructure. The SPLA only counts universal usage that is not related to backup. Backup usage is shown in the Acronis Cyber Backup Cloud section of Acronis Cyber Cloud.

You can switch the licensing model at any time:

- Switching the licensing mode (for example, from a license key to an SPLA, or from a subscription to perpetual) terminates the previously used key even if it has not yet expired. Terminated keys cannot be used again.
- Switching from an 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 Acronis Cyber Infrastructure 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.
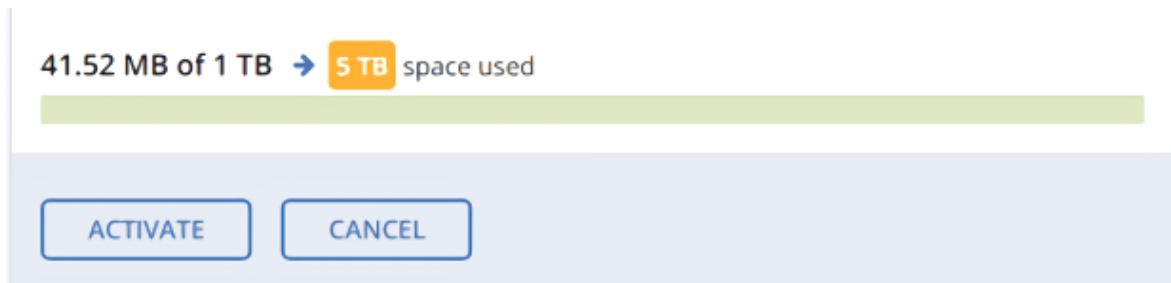
4.1 Installing license keys

To install a license key, do the following:

1. If you are switching from an SPLA, ask your service provider to terminate the agreement by either disabling the Acronis Cyber Infrastructure application for your account or deleting the account.

2. On the **Settings** > **Licenses** screen, click **Upgrade**, and then click **Register key**.
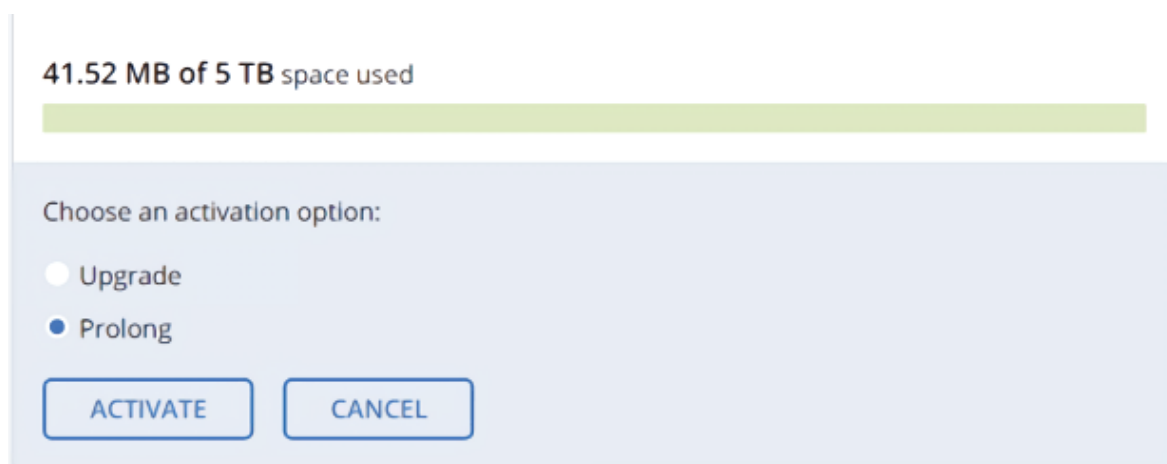

3. In the **Register license key** window, paste the license key, and then click **Register**.

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

    - **Upgrade**, to add storage capacity to the active license.
    - **Prolong**, to prolong the license which is about to expire.

Then click **Activate**.

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

4.2 Installing SPLA licenses

To install an SPLA license, do the following:

1. On the **Settings** > **Licenses** screen, click **Upgrade**, and then click **Use SPLA**.
2. In the **Use SPLA** window, select a region from the drop-down list. If your datacenter is not listed there, just enter its URL directly into the drop-down field, for example: **https://eu-cloud.acronis.com**. Then, click **Activate**. You will be redirected to the login page of Acronis Cyber Cloud.

   Note
   For more information on datacenters, refer to https://kb.acronis.com/servicesbydc.

3. Log in to Acronis Cyber 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 Cyber Cloud. You will be able to monitor its resource usage and download reports.

5 Managing updates

Acronis Cyber Infrastructure supports non-disruptive rolling updates. Cluster nodes are updated one by one, with the data availability unaffected. During the update, the node enters maintenance mode and its workloads and VMs are migrated to other nodes. After the update, the node returns to operation. For more information on the maintenance mode, refer to "Perform node maintenance" in the in the Administrator Guide.

Take note of the following before you start updating nodes:

- Nodes must be updated only in the admin panel or via the `vinfra` tool (refer to "Managing updates" in the Administrator Command Line Guide). Do not use `yum update`.
- Disable any third-party repositories.
- To check for and download updates, the cluster must be healthy and each node in the infrastructure must be able to open an outgoing Internet connection. This means that nodes must not be offline, and the cluster DNS must be configured and point to a DNS table to resolve external host names. For more details, refer to "Add external DNS servers" in the Administrator Guide.
- Unassigned nodes can be updated.
- Updates are applied to one cluster node at a time.

To update the storage cluster from the admin panel, do the following:

1. Open the **Settings** > **Updates** screen. The date of the last check is displayed in the upper right corner. Click the round arrow to check for new updates. If updates are available for a node, that node's update status changes to **Available**.
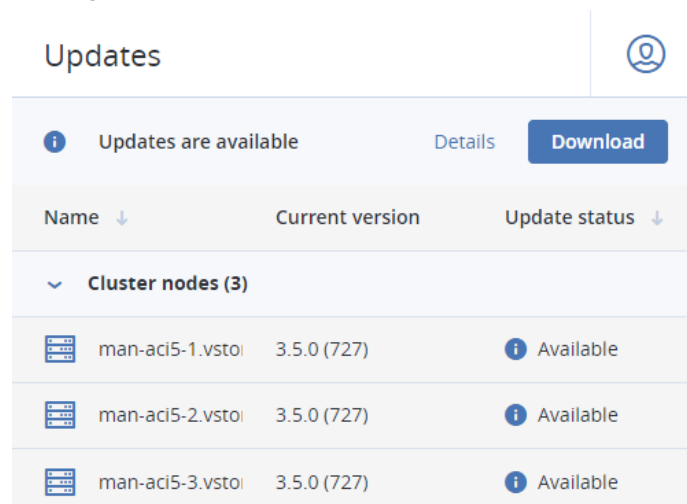
2. Click **Download** in the upper right corner to get the updates. When the updates are downloaded to a node, its update status changes to **Ready to install**. After the updates have been downloaded for all of the nodes, the button will change to **Install**. Click it to continue.
3. In the **Install updates** window, choose how to proceed if a node needs to be rebooted but cannot enter maintenance mode. To avoid downtime, nodes that need to be rebooted are placed in maintenance mode one by one during the update. Nodes that cannot enter maintenance mode

are skipped and not updated by default. By selecting the check box, you can instead stop the update if some of the nodes cannot enter maintenance mode. Nodes that have already been updated will remain so. Click **Install**.
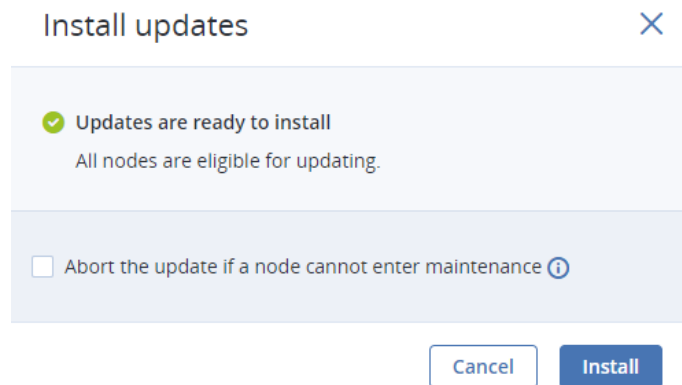
While the updates are being installed, you can pause or cancel the process.

4. If you have chosen to abort the update in case some of the nodes cannot enter maintenance, and at least one node actually cannot enter it, then a window will open showing the reasons for that. You will need to decide how to proceed. You can cancel the update, solve the issues, and retry updating without downtime. Or you can force the update on the listed nodes at once. In the latter case, the nodes in question will be rebooted, potentially causing a downtime of services running on them.

After the update is complete, the node statuses will change to **Up to date**.

To update the kernel with ReadyKernel, refer to "Updating kernel with ReadyKernel" in the Administrator Command Line Guide.

6 Configuring Acronis Cyber Infrastructure and Acronis Cyber Backup

This section describes how to deploy and configure Acronis Cyber Backup in the form of the "All-in-One Appliance" virtual machine in Acronis Cyber Infrastructure. You can then connect your Acronis Cyber Appliance cluster to Acronis Cyber Backup as a storage backend. As a result, you will have both the storage and the backup server running on Acronis Cyber Appliance.

6.1 Deploying the compute cluster

Before creating a compute cluster, make sure the network is set up according to recommendations in "Set up networks for the compute cluster" in the Administrator Guide. The basic requirements are: (a) the traffic types **VM private**, **VM public**, **Compute API**, and **VM backups** must be assigned to networks; (b) the nodes to be added to the compute cluster must be connected to these networks and to the same network with the **VM public** traffic type.

Once you've configured the networks, you can proceed to create the compute cluster:

1. On the **Compute** screen, click **Create compute cluster**.
2. In the **Nodes** section, select all the nodes and make sure the network state of each selected node is **Configured**. Then, click **Next**.
   If the node network interfaces are not configured, click the cogwheel icon, select the networks as required, and then click **Apply**.
3. In the **Physical network** section, leave the IP address management disabled if you want the IP address for Acronis Cyber Backup Appliance virtual machine to be allocated by an external DHCP server. Otherwise, you can enable it. For more information, refer to "Deploy the compute cluster" in the Administrator Guide.
4. On the **Summary** step, review the configuration, and then click **Create cluster**.

You can monitor compute cluster deployment on the **Compute** screen.

6.2 Deploying the Acronis Cyber Backup "All-in-One" Appliance virtual machine

6.2.1 Downloading the Acronis Cyber Backup "All-in-One" Appliance

1. Go to https://account.acronis.com/ and log in to your account. If you do not have one, you will need to create it—refer to https://kb.acronis.com/regacc.
2. Register your Acronis products, if not done before. For more information, see https://kb.acronis.com/productwebreg.
3. In the **Products** section, locate the Acronis Cyber Backup download links. For more information, refer to https://kb.acronis.com/latest.

4. Download **AcronisBackup_All-in-One_Appliance.zip**.

5. Extract **AcronisBackupAppliance.iso**.

6. Add this image to the Acronis Cyber Infrastructure compute cluster as follows:

   a. On the **Compute** > **Virtual machines** > **Images** tab, click **Add image**.

   b. In the **Add image** window, click **Browse**, and then select the ISO file.

   c. Specify the image name and select the **Generic Linux** OS type. Click **Add**.

   For more information, refer to "Upload, edit, and remove images" in the Administrator Guide.

6.2.2 Deploying the Acronis Cyber Backup "All-in-One" Appliance

The Acronis Cyber Backup "All-in-One" Appliance is a pre-configured virtual machine that you deploy in Acronis Cyber Infrastructure. For more information about the appliance, refer to Acronis Backup appliance.

a. On the **Compute** > **Virtual machines** > **Virtual machines** tab, click **Create virtual machine**. A window will open where you will need to specify the VM parameters.

b. Specify a name for the new VM.

c. In **Deploy from**, select **Image**.

d. In the **Images** window, select **AcronisBackupAppliance.iso**, and then click **Done**.

e. In the **Volumes** window, you do not need to add any volumes. The volume added automatically for the system disk is sufficient for Acronis Cyber Backup installation.

f. In the **Flavor** window, select the **large** flavor, and then click **Done**. This flavor will provide 4 vCPUs and 8 GB of RAM for the Acronis Cyber Backup virtual appliance.

g. In the network window, click **Add**, select a public virtual network interface, and then click **Add**. It will appear in the **Network interfaces** list. For more information on the interfaces, refer to "Create virtual machines" in the Administrator Guide.

h. Back in the **Create virtual machine** window, click **Deploy** to create and boot the VM.

Create virtual machine ✕

Review the virtual machine details and go back to change them if necessary.

| Name | Deploy from: | ● Image | ○ Volume |
| AB_appliance | | | |

Image	AcronisBackupAppliance.iso	✎
Volumes	Boot volume — 64 GiB, default 1st boot CD/DVD volume — 3 GiB, default 2nd boot	✎
Flavor	large — 4 vCPUs, 8 GiB RAM	✎
Networks	public — Auto, 192.168.128.0/24	✎

Cancel   **Deploy**

i. On the **Compute** > **Virtual machines** > **Virtual machines** tab, select the created virtual machine. Then, click **Console** and install the Acronis Backup OS by using the built-in VNC console.
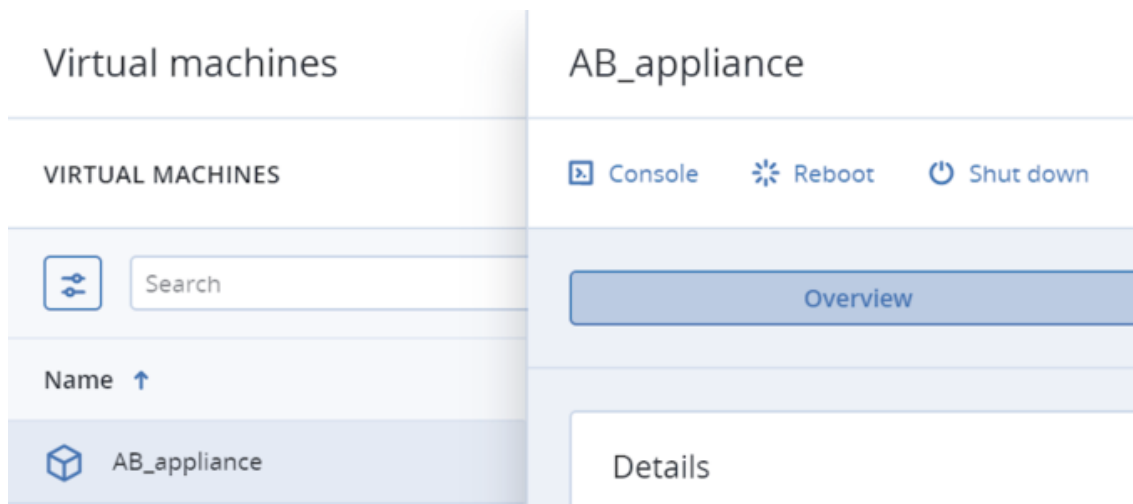
i. On the initial installer screen, select **Install or update Acronis Backup** and press **Enter**.
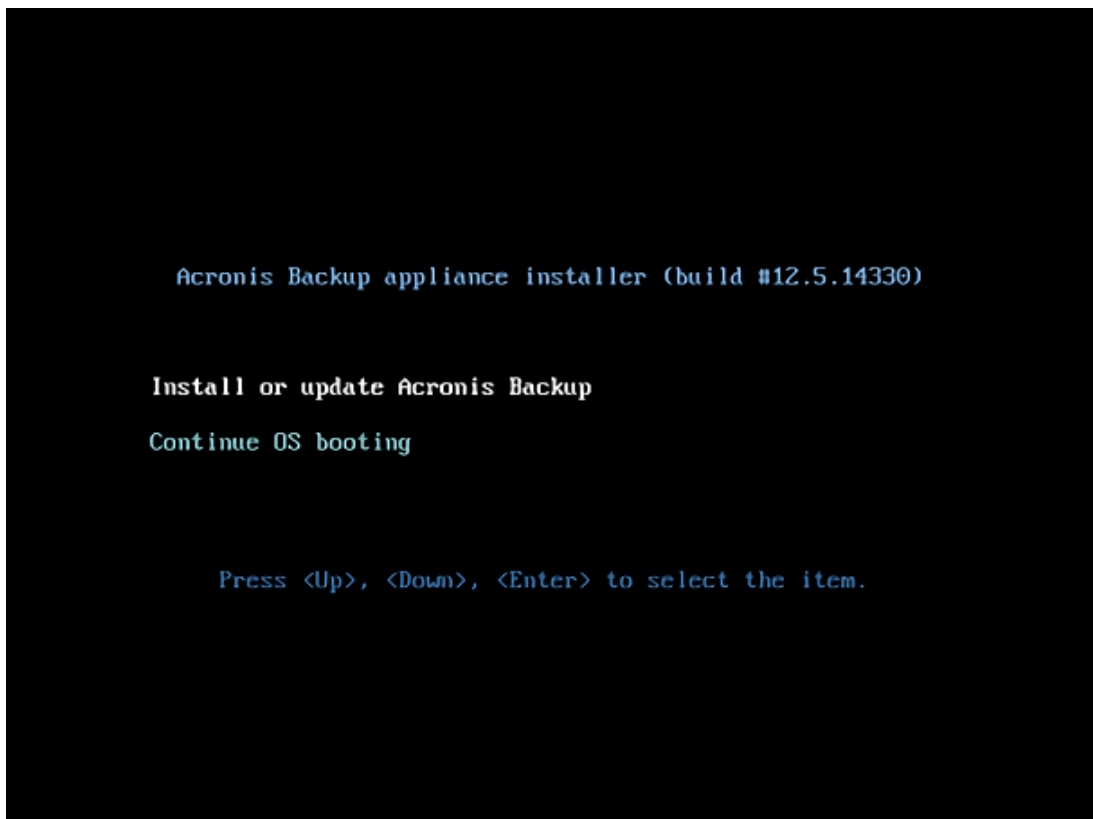
Note

The initial installer times out after 15 seconds, and the system will attempt to boot from the newly created virtual volume. If you see the message "Booting from local disk... No bootable device," restart the virtual machine by clicking **Send keys** > **Ctrl** + **Alt** + **Del**

---

ii. Specify the installation settings: a host name (optional) and a password for the root user.
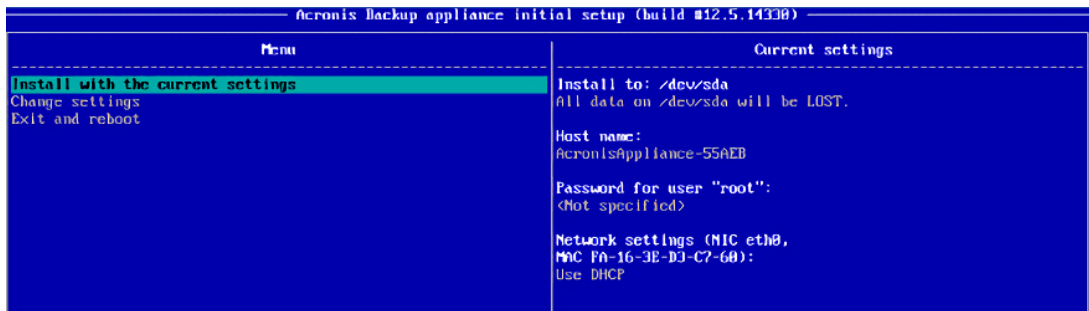
After the installation completes, the login screen details for the Acronis Cyber Backup console are displayed. Use the Acronis Cyber Backup console to configure and manage backup operations.
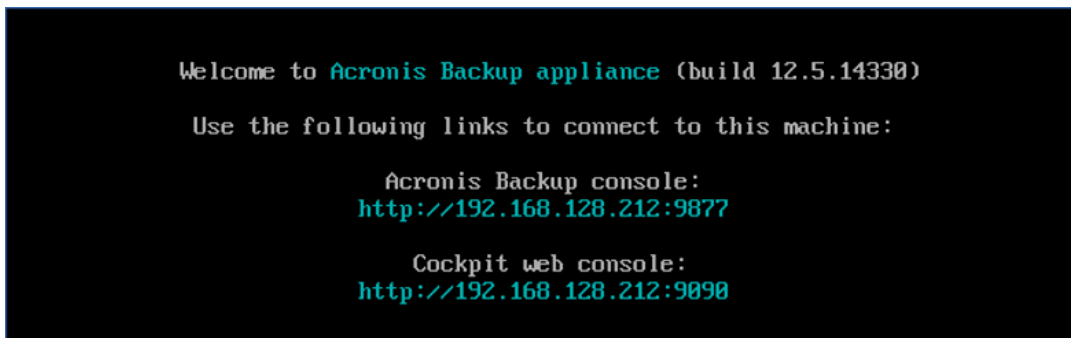
Note

To install the full Acronis Cyber Backup license, refer to https://kb.acronis.com/content/59467.

6.3 Creating Backup Gateway

1. In the Acronis Cyber Infrastructure admin panel, navigate to **Storage Services**, and then to **Backup Storage**. Here, you can see all of the nodes in the storage cluster that can be used as backup destinations. Select all of the nodes, and then click **Create gateway**. On the right pane, click **This cluster**.

2. Make sure the correct network interface is selected in the drop-down list. Click **Next**.

   If necessary, click the cogwheel icon and configure the node's network interfaces on the **Network configuration** screen.

3. Select the **Encoding 3+2** redundancy mode.

4. Specify a DNS name that will be associated with the selected cluster and used to register that cluster within Acronis Cyber Backup (like **backup.example.com**). The new DNS name is associated with each node's IP address in the selected cluster. A specific node for backup operations is selected automatically by the backup agent. Click **Next**.

5. To register this storage in backup software, specify the URL with the IP address or hostname of the machine used to access the Acronis Cyber Backup console (example: http://192.168.128.212:9877). If you use https, make sure the SSL certificate is trusted. Provide the credentials of the local management server administrator (for example, "root"). Click **Next**.

6. Finally, click **Done**.

6.4 Performing backup operations

6.4.1 Adding machines to be backed up

Before you can back up a machine, you must install a backup agent. Agents are applications that perform data backup, recovery, and other operations on the machines managed by Acronis Cyber Backup. Choose an agent, depending on what you are going to back up. For more information, see the full list of supported operating systems and environments.

1. Open the Acronis Cyber Backup console in your browser and log in.
2. To add a machine to the management server, click **All devices** > **Add**. You will be asked to select the setup program based on the type of the machine that you want to add.
3. Once the setup program is downloaded, run it locally on that machine.
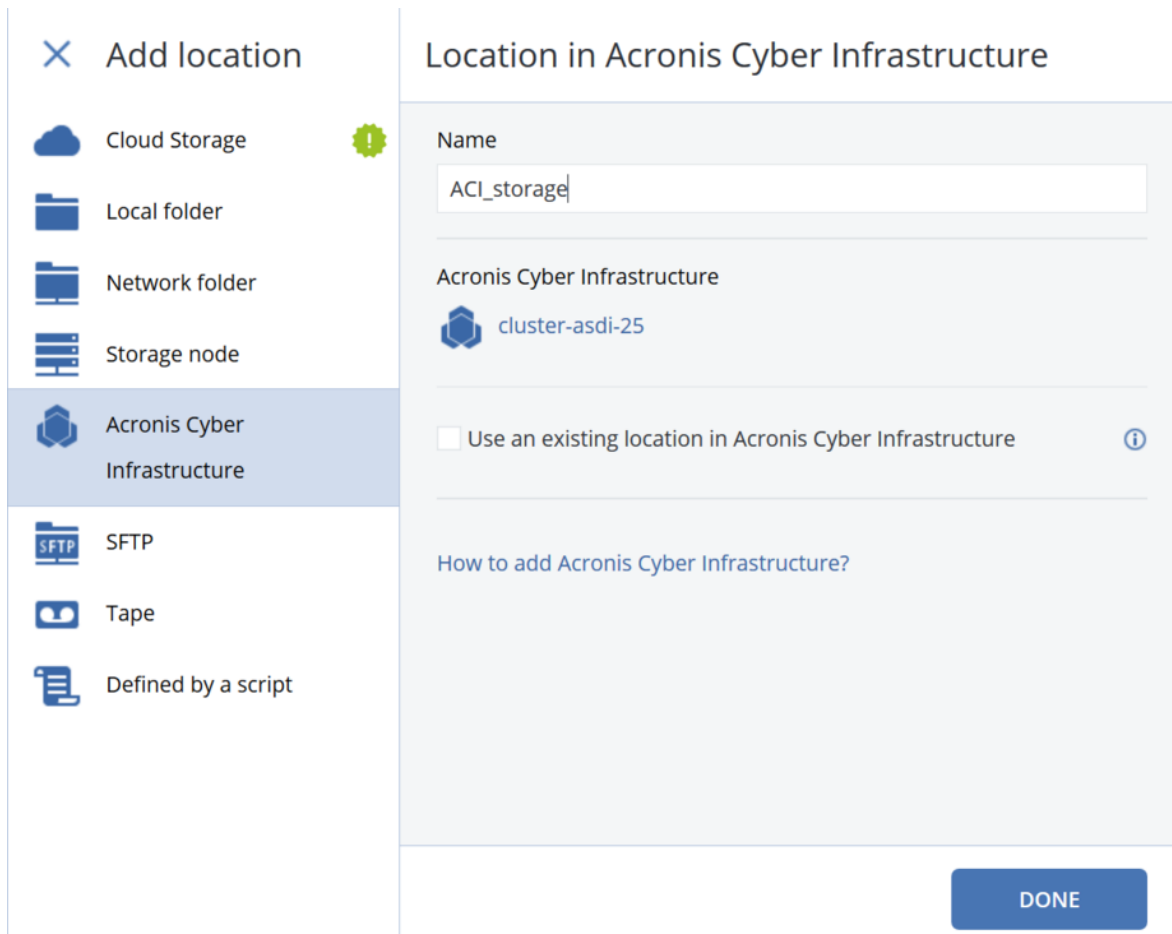
6.4.2 Configuring a backup plan

A backup plan is a set of rules that specify how data will be protected on a given machine. To create a backup plan, follow the steps:

1. Select the machines that you want to back up.
2. Click **Backup**. The new backup plan template opens.

3. Click **Where to back up**.
4. Click **Add location**, and then select **Acronis Cyber Infrastructure**.

5. Click **Done**.

6. Click **Create** to create a new plan. To run an existing backup plan, click **Run now**.

For detailed information on how to configure and use Acronis Cyber Backup, see the product documentation.

7 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 Acronis Cyber 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 to 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 Acronis Cyber Appliance and related software solutions:
  - Acronis Cyber Appliance, https://kb.acronis.com/acronis-appliance
  - Acronis Cyber Infrastructure, https://kb.acronis.com/acronis-cyber-infrastructure
  - Acronis Cyber Backup Cloud, https://kb.acronis.com/acronis-backup-cloud
  - Acronis Cyber Backup 12.5, https://kb.acronis.com/acronis-backup-12-5
- User documentation, and guides describing how to use Acronis Cyber Appliance as well as Acronis software, are available at https://www.acronis.com/support/documentation.

For information on Acronis Cyber Appliance warranty, see the "Support" section at https://www.acronis.com/en-us/support/hwappliancesupport.

8 Appendix: Specifications

This chapter lists the technical and environmental specifications of Acronis Cyber Appliance.

8.1 Technical specifications

The following table lists Acronis Cyber Appliance hardware parts.

Chassis	3U, 435x130x600 mm (WxHxD), 34.5 kg
CPU	Intel Atom C3958 @ 2.00GHz, 16 cores, 31W TDP, VT-d support, w/o Hyper-Threading
RAM	32 GB (up to 256 GB), Samsung, 2x16 GB DDR4-2400 ECC
OS drive	1x Intel S4600 240 GB 2.5-inch SSD
Cache drive	1x Intel S4600 240 GB 2.5-inch SSD
Storage drives	3x Seagate 4/8/10/12 TB 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 Cyber Infrastructure 4.0
Data protection	Replication and erasure coding via storage policies
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

8.1.1 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[1]	Output power	20% load	50% load	100% load
	Power factor	>0.80	>0.95	>0.95

[1]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.

8.2 Environmental specifications

Acronis Cyber 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)

8.2.1 Air quality requirements

The air must be free of:

- Corrosive dust and corrosive contaminants
- Conductive dust and conductive particles (such as zinc whiskers)

Airborne residual dust must have a deliquescent point less than 60 percent relative humidity. The deliquescent point is 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 A/month, class G1(ANSI/ISA71.04-1985).
- Silver reactivity rate must be less than 200 A/month (AHSRAE TC9.9).