Acronis Cyber Infrastructure 3.5

Quick Start Guide

March 30, 2020

Contents

CHAPTER 1

Introduction

1.1 About This Guide

This guide describes how to set up a full-fledged storage cluster on three nodes, deploy a compute cluster on top of it, and create a virtual machine.

1.2 Hardware Requirements

A minimum Acronis Cyber Infrastructure installation recommended for production consists of three nodes for storage and compute services with enabled high availability for the management node. This is to ensure that the cluster can survive failure of one node without data loss. The following table lists the *minimal* hardware requirements for all the three nodes. The recommended configurations are provided in the "Hardware Requirements" section of the *Installation Guide*.

Table 1.2.1: Node hardware requirements

Type	**Management and storage/compute node**
CPU	64-bit x86 processors with AMD-V or Intel VT hardware virtualization extensions enabled. 16 logical CPUs*
RAM	32 GB**

Continued on next page

Table 1.2.1 – continued from previous page

Type	Management and storage/compute node
Storage	1 disk: system + metadata, 100+ GB SATA HDD 1 disk: storage, SATA HDD, size as required
Network	1 GbE for storage traffic 1 GbE (VLAN tagged) for other traffic

* A logical CPU is a core (thread) in a multicore (multithreading) processor.

** Each chunk server (CS), e.g., storage disk, requires 1 GB of RAM (0.5 GB anonymous memory + 0.5 GB page cache). The total page cache limit is 12 GB. In addition, each metadata server (MDS) requires 0.2 GB of RAM + 0.1 GB per 100TB of physical storage space.

CHAPTER 2

Installing Acronis Cyber Infrastructure

Important: Time needs to be synchronized via NTP on all nodes in the same cluster. Make sure that the nodes can access the NTP server.

To install Acronis Cyber Infrastructure, do the following:

1. Prepare bootable media using the distribution ISO image (mount it to an IPMI virtual drive, create a bootable USB drive, or set up a PXE server).
2. Boot the server from the chosen media.
3. On the welcome screen, choose **Install Acronis Cyber Infrastructure**.
4. On step 1, please carefully read the End-User License Agreement. Accept it by ticking the **I accept the End-User License Agreement** checkbox and click **Next**.
5. On step 2, configure a static IP address for the NIC and provide a hostname: either a fully qualified domain name (hostname, domainname) or a short name (hostname).
6. On step 3, choose your time zone. Date and time will be set via NTP. You will need an Internet connection for synchronization to complete.
7. On step 4, specify what type of node you are installing. First, deploy one primary node. Then, deploy as many secondary nodes as you need.
    - If you chose to deploy the primary node, select two network interfaces: for internal management and configuration and for access to the admin panel. Also create and confirm a password for the

superadmin account of the admin panel.

- If you chose to deploy a secondary node, provide the IP address of the management node and the token. Both are obtained from the admin panel. Log in to the admin panel on port 8888. Panel's IP address is shown in the console after deploying the primary node. Enter the default username `admin` and the superadmin account password. In the admin panel, open **INFRASTRUCTURE** > **Nodes** and click **ADD NODE** to invoke a screen with the management node address and the token.

  The node may appear on the **INFRASTRUCTURE** > **Nodes** screen in the **UNASSIGNED** list as soon as token is validated. However, you will be able to join it to the storage cluster only after the installation is complete.

8. On step 5, choose a disk for the operating system. This disk will have the supplementary role **System**, although you will still be able to set it up for data storage in the admin panel. You can also create software RAID1 for the system disk to ensure its high performance and availability.
9. On step 6, enter and confirm the password for the root account and click **Start installation**.

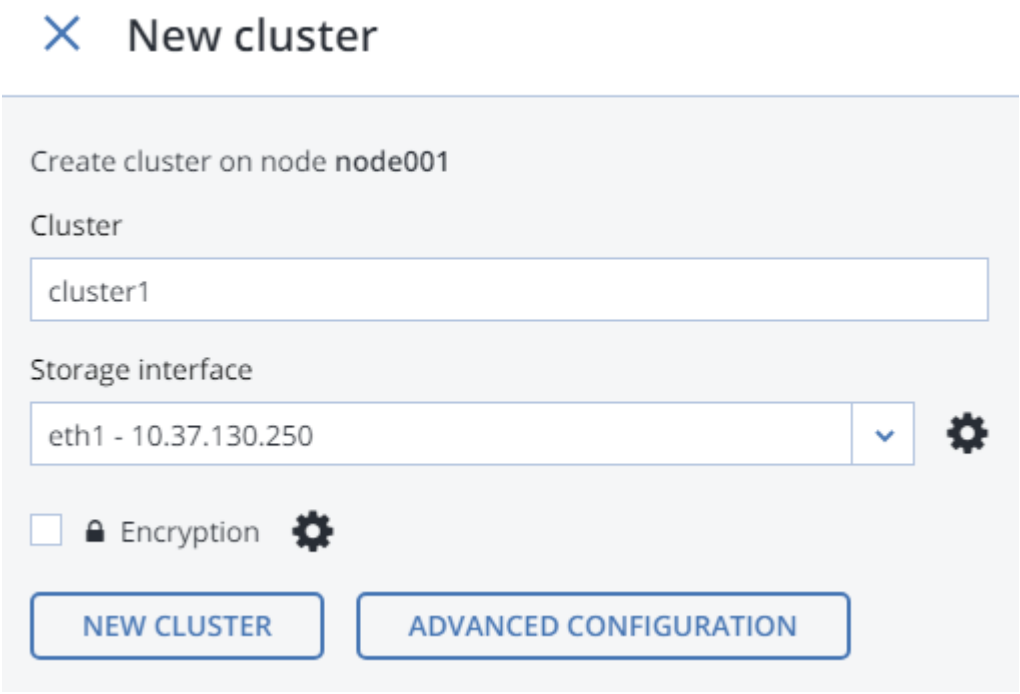
Once the installation is complete, the node will reboot automatically. The admin panel IP address will be shown in the welcome prompt.

CHAPTER 3

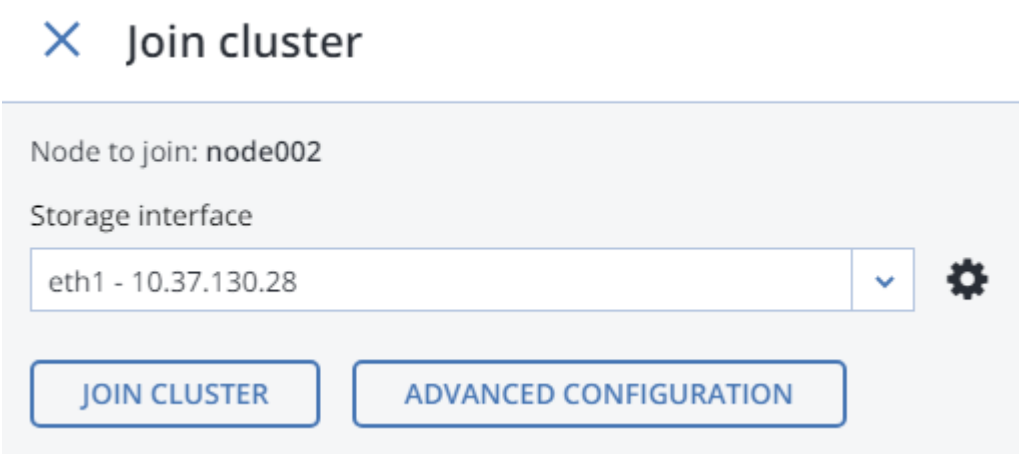
Creating the Storage Cluster

To create the storage cluster, do the following:

1. Open the **INFRASTRUCTURE** > **Nodes** screen and click a node in the **UNASSIGNED** list.
2. On the node overview screen, click **Create cluster**.
3. In the **Cluster** field, type a name for the cluster. The name may only contain Latin letters (a-z, A-Z), numbers (0-9), underscores (“_”) and hyphens (“-”).



4. Click **NEW CLUSTER**.
5. Click the next node in the **UNASSIGNED** list and click **JOIN CLUSTER**.



6. Repeat the previous step for the remaining unassigned nodes.

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

CHAPTER 4

Enabling Management Node High Availability

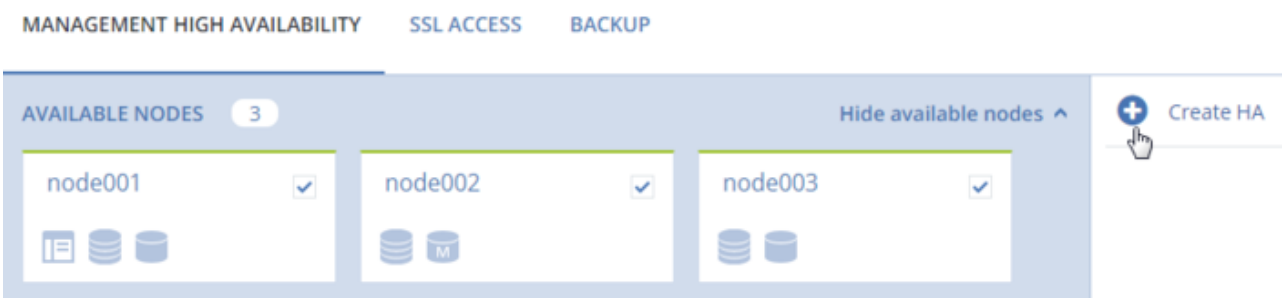
To make your infrastructure more resilient and redundant, you can create a high availability configuration of three nodes.

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

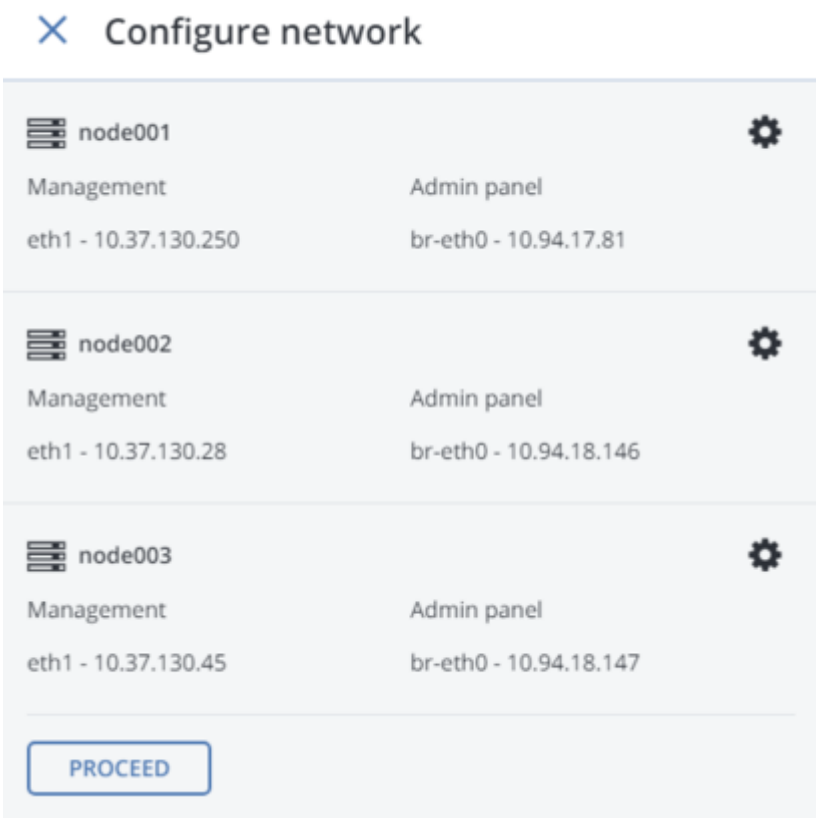
1. All nodes in the HA configuration will be added to the compute cluster.
2. Single nodes cannot be removed from the compute cluster as they are included in the HA configuration. In such a case, the compute cluster can be destroyed completely, but the HA configuration will remain. This is also true 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:

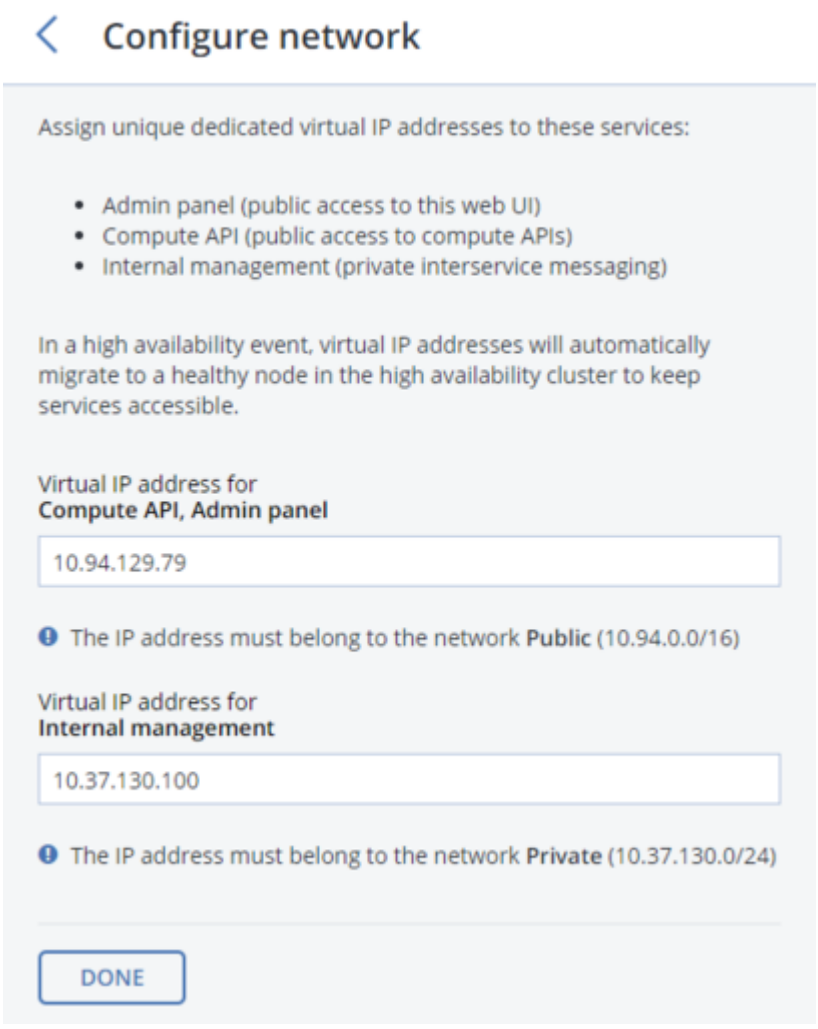
1. Make sure that each node is connected to a network with the **Admin panel** and **Internal management** traffic types.
2. On the **SETTINGS** > **Management node** screen, open the **MANAGEMENT HIGH AVAILABILITY** tab.



3. Select three nodes and click **Create HA**. The management node is automatically selected.
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 types 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**.



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

CHAPTER 5

Deploying Compute Cluster

Before creating a compute cluster, make sure the network is set up according to recommendations in the "Managing Networks and Traffic Types" section of the *Administrator's Guide*. The basic requirements are: (a) the traffic types **VM private**, **VM public**, and **Compute API** 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.

Besides, high availability for the management node should also be enabled (see the *Enabling Management Node High Availability* (page 7)).

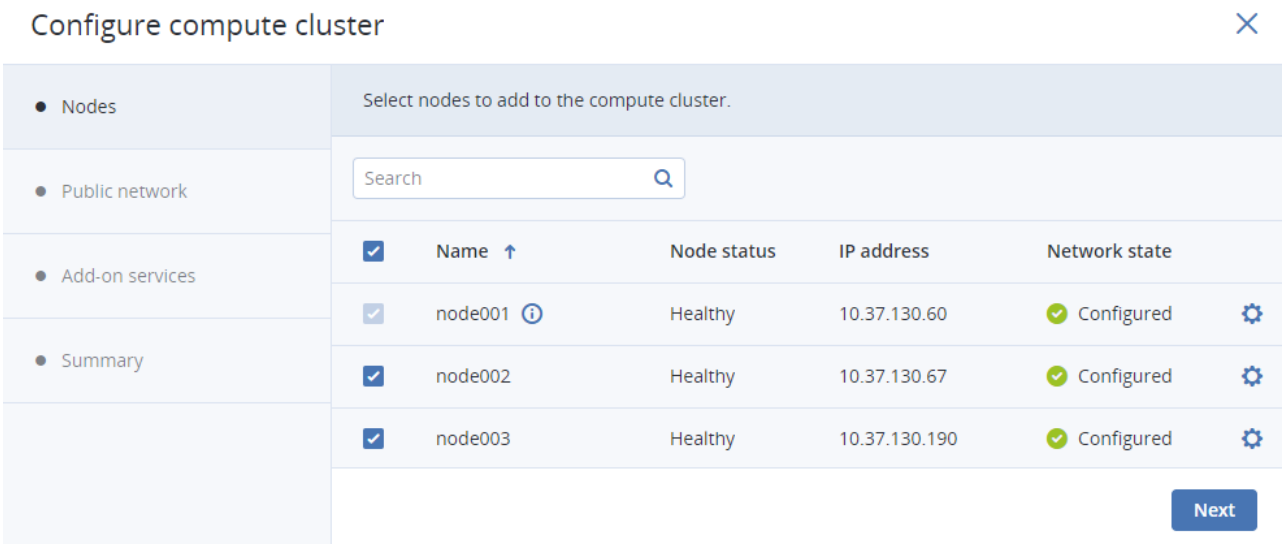
Also take note of the following:

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*.

To create the compute cluster, open the **COMPUTE** screen, click **Create compute cluster** and do the following in the **Configure compute cluster** window:

1. In the **Nodes** section, select nodes to add to the compute cluster, make sure the network state of each selected node is **Configured**, and click **Next**.

   Nodes in the management node high availability cluster are automatically selected to join the compute cluster.



If node network interfaces are not configured, click the cogwheel icon, select networks as required, and click **Apply**.

Note: The compute cluster must have at least three nodes to allow self-service users to enable high availability for Kubernetes master nodes.

---

2. In the **Public network** section, enable IP address management if needed and provide the required details for the public network.

   With IP address management enabled, Acronis Cyber Infrastructure will handle virtual machine IP addresses and provide the following features:

   - Allocation pools. You can specify ranges of IP addresses that will be automatically assigned to VMs.
   - Built-in DHCP server. Assigns IP addresses to virtual machines. With the DHCP server enabled, VM network interfaces will automatically be assigned IP addresses: either from allocation pools or, if there are no pools, from network's entire IP range. With the DHCP server disabled, VM network interfaces will still get IP addresses, but you will have to manually assign them inside VMs.
   - Custom DNS servers. You can specify DNS servers that will be used by VMs. These servers will be delivered to virtual machines via the built-in DHCP server.

   With IP address management disabled:

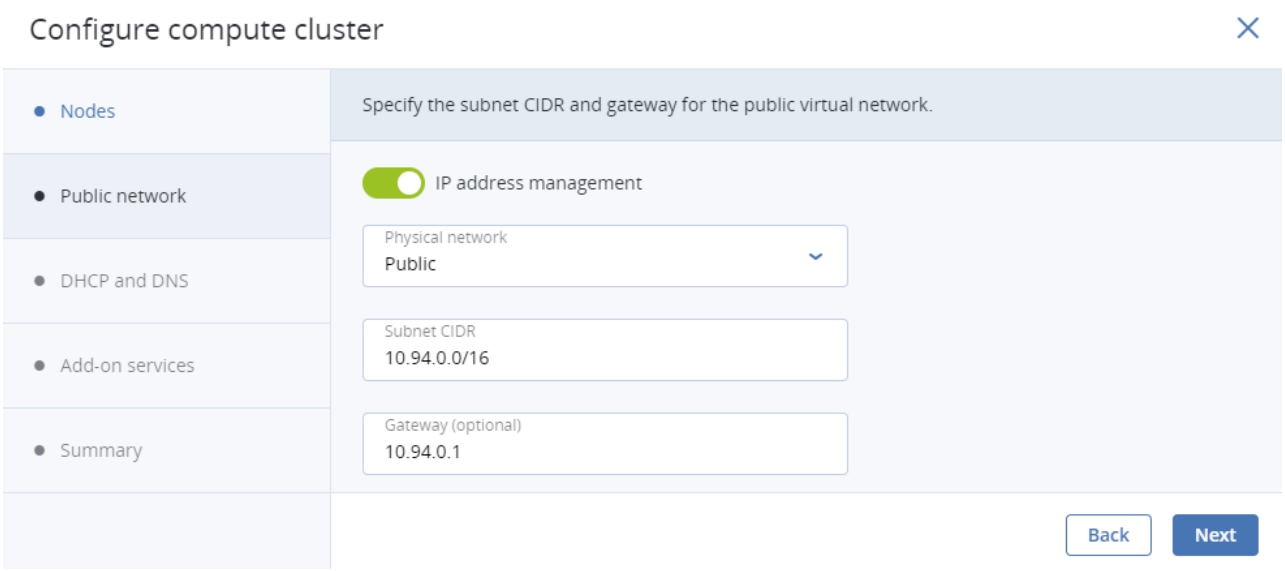
   - VMs connected to a network will be able to obtain IP addresses from DHCP servers in that network.

- Spoofing protection will be disabled for all VM network ports. Each VM network interface will accept all traffic, even frames addressed to other network interfaces.

In any case, you will be able to manually assign static IP addresses from inside VMs.

If you choose to enable IP address management, select a physical network to connect the public virtual network to and optionally specify its gateway. The subnet IP range in the CIDR format will be filled in automatically. If you choose to leave IP address management disabled, select a physical network to connect the public virtual network to.

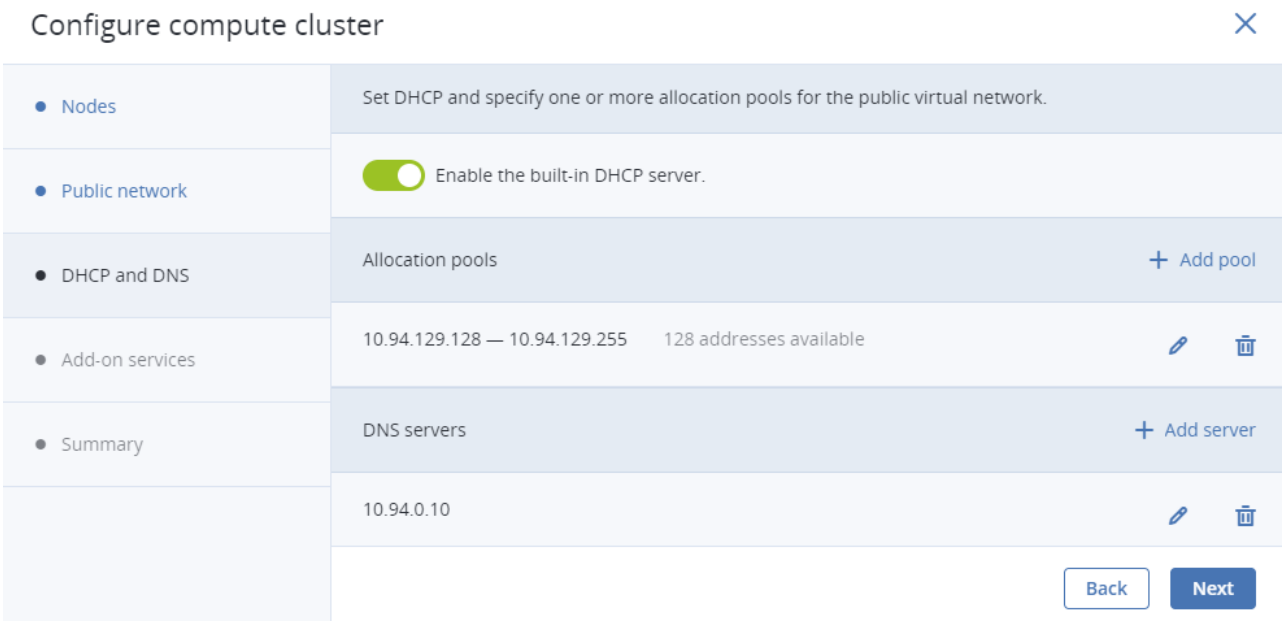
By default, the public network will be shared between all future projects. You can disable this option on the network panel after the compute cluster is created.



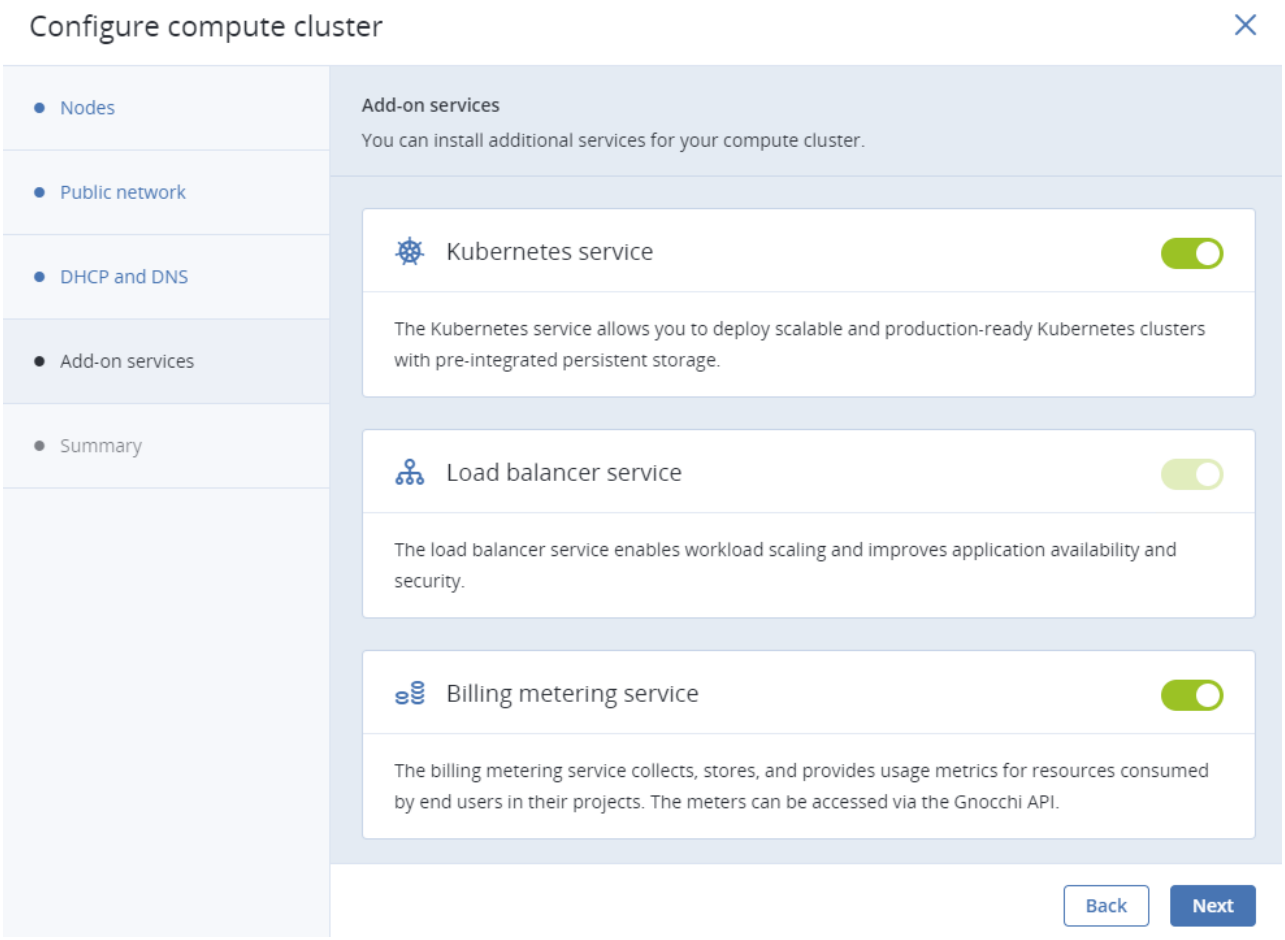
The selected public network will appear in the list of virtual networks on compute cluster's **NETWORKS** tab.

Click **Next**.

3. If you enabled IP address management on the previous step, you will move on to the **DHCP and DNS** section. In it, enable or disable the built-in DHCP server and specify one or more allocation pools and DNS servers. Click **Next**.



4. In the **Add-on services** section, enable additional services that will be installed during the compute cluster deployment. You can also install these services later (see the “Managing Add-On Services” section of the *Administrator’s Guide*).



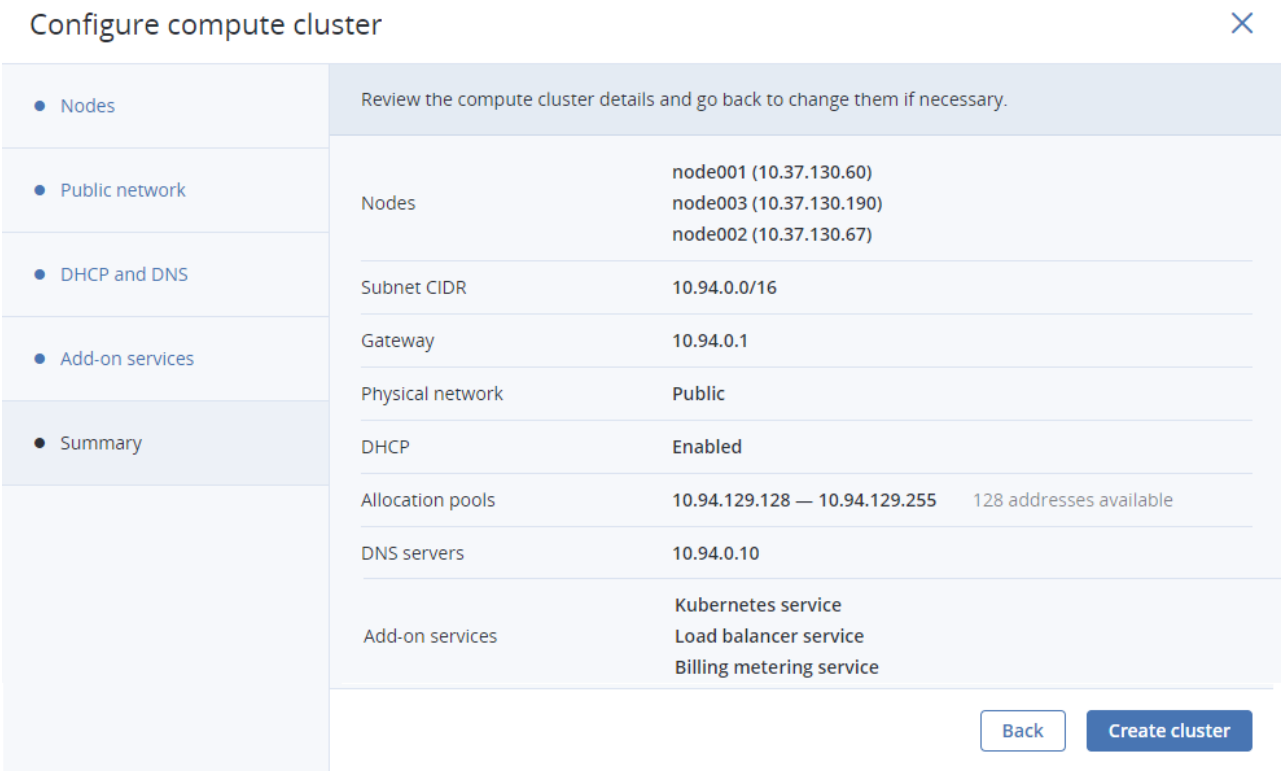
Important: To be able to deploy and work with Kubernetes clusters, make the following services accessible:

- the etcd discovery service at https://discovery.etcd.io from all management nodes and the public network with the **VM public** traffic type
- the public Docker Hub repository at https://registry-1.docker.io:5000 from the public network with the **VM public** traffic type
- the compute API from the public network with the **VM public** traffic type

If the **Compute API** traffic type is added to a private network that is inaccessible directly from the network with the **VM public** traffic type but exposed to public networks via NAT and available publicly via the DNS name, you need to set the DNS name for the compute API as described in “Setting a DNS Name for the Compute API” in the *Administrator’s Command Line Guide*.

Note: Installing Kubernetes automatically installs the load balancer service as well.

5. In the **Summary** section, review the configuration and click **Create cluster**.



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

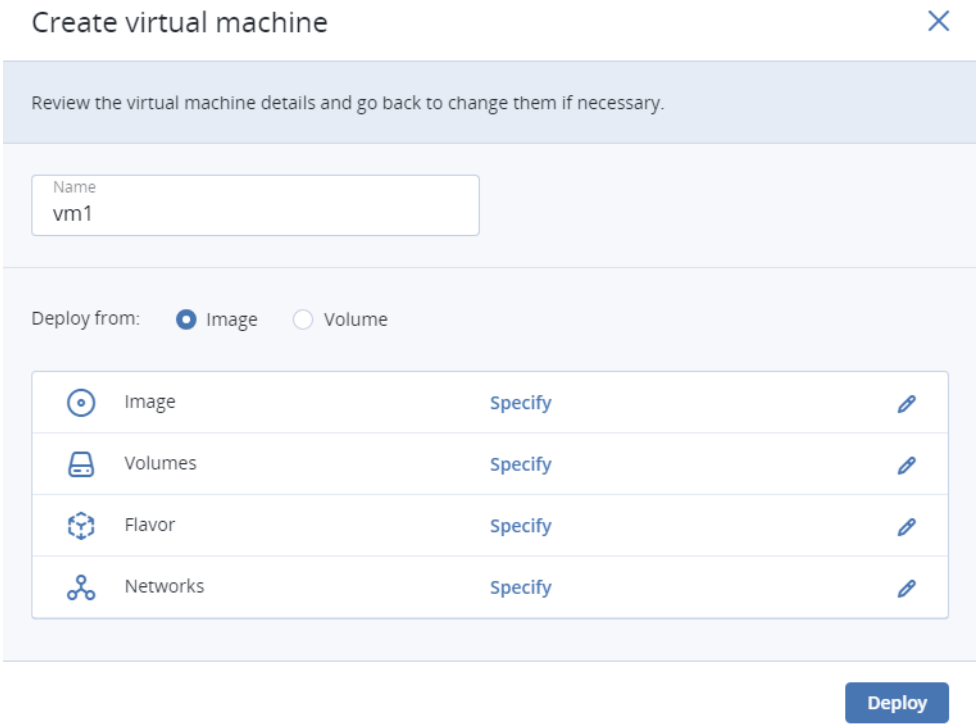
CHAPTER 6

Creating a Virtual Machine

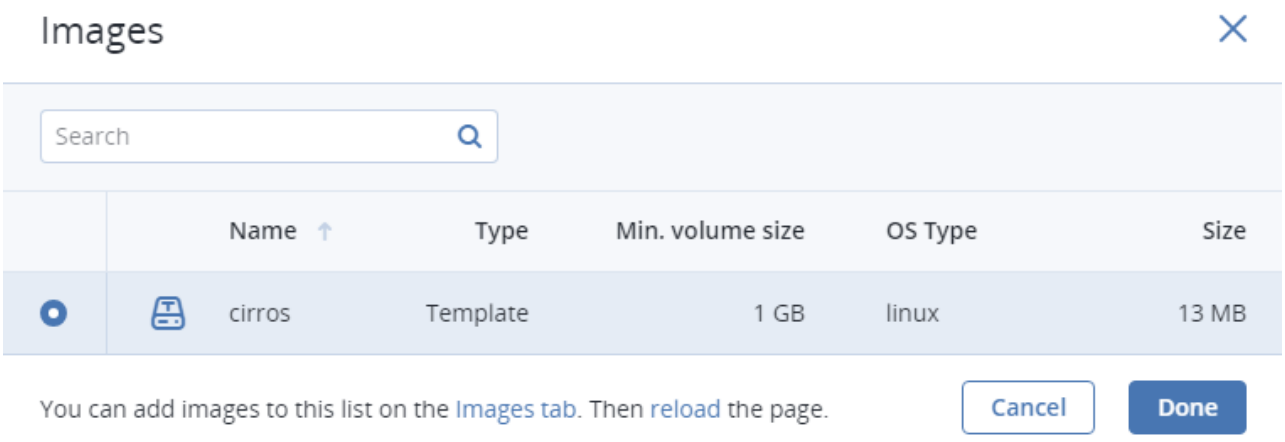
Note: For supported guest operating systems and other information, see the "Managing Virtual Machines" section of the *Administrator's Guide*.

To create a VM, do the following:

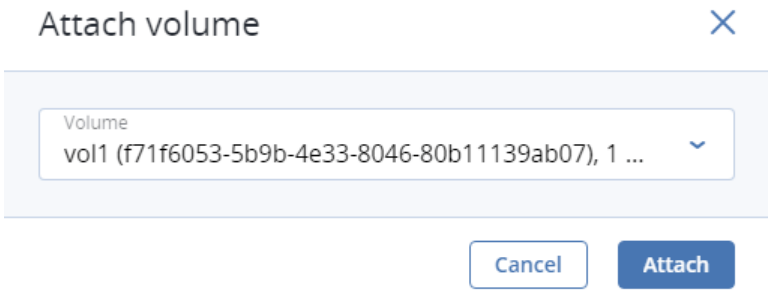
1. On the **COMPUTE** > **Virtual machines** > **VIRTUAL MACHINES** tab, click **Create virtual machine**. A window will open where you will need to specify VM parameters.

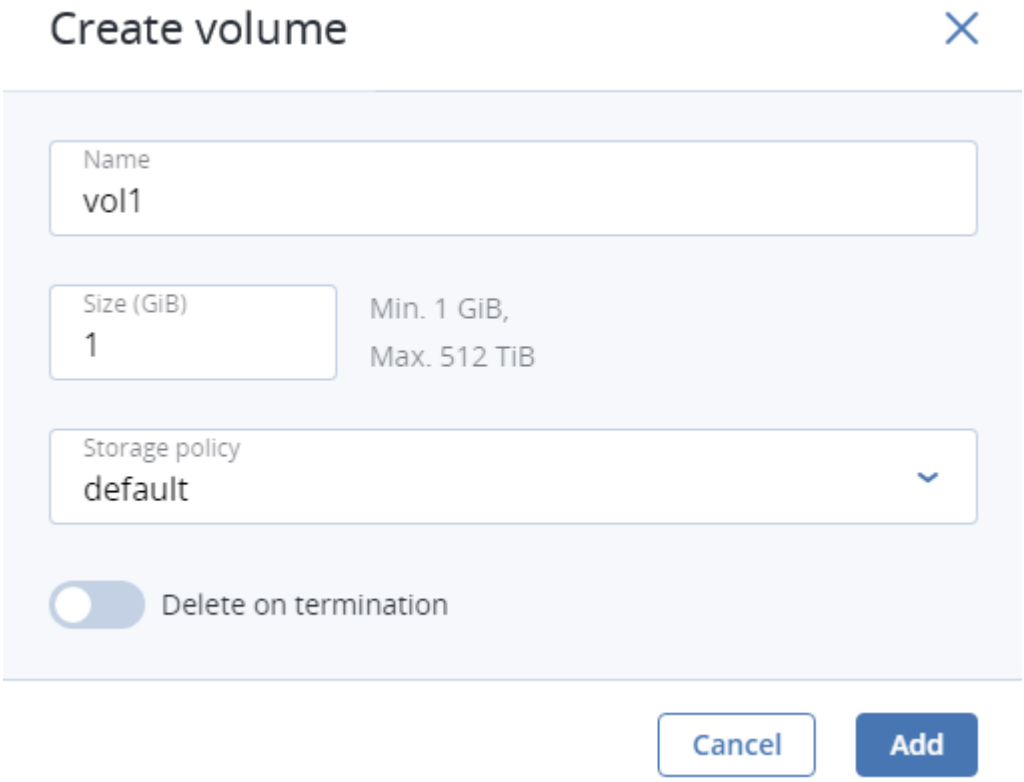


2. Specify a name for the new VM.
3. In **Deploy from**, choose **Volume** if you have a boot volume or want to create one. Otherwise, choose **Image**.
4. Depending on your choice, click the pencil icon in the **Volumes** or **Image** section and do one of the following:
   - In the **Images** window, select the ISO image or template and click **Done**.

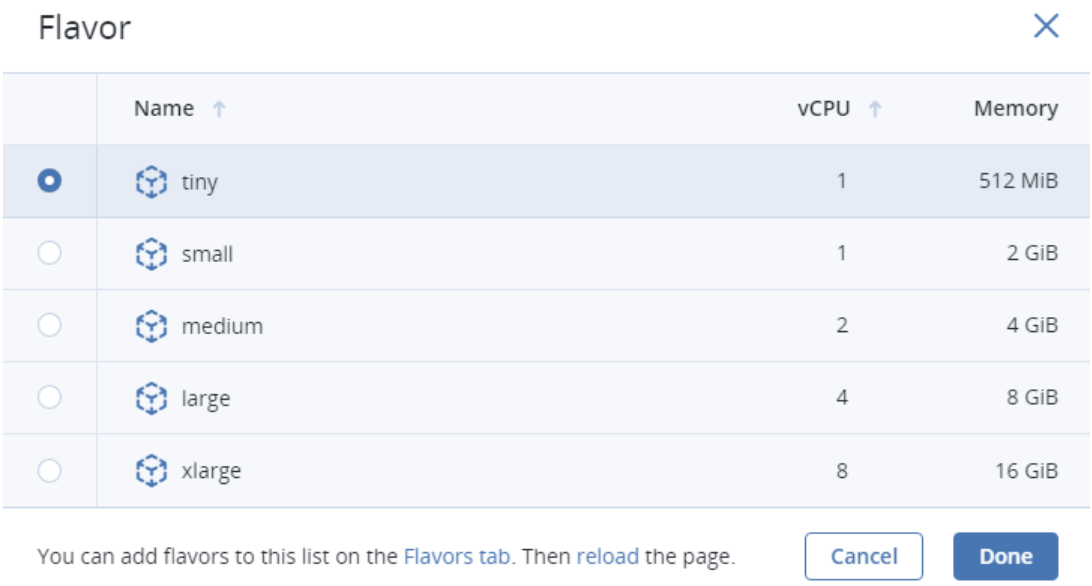


   - In the **Volumes** window, do one of the following:
     - If you have prepared a volume with an installed guest OS, click **Attach**, find and select the volume, and click **Done**.

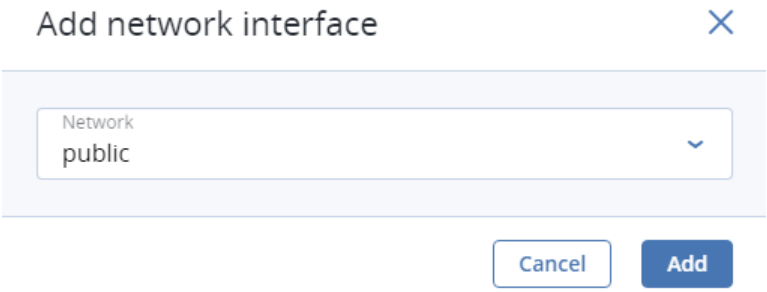




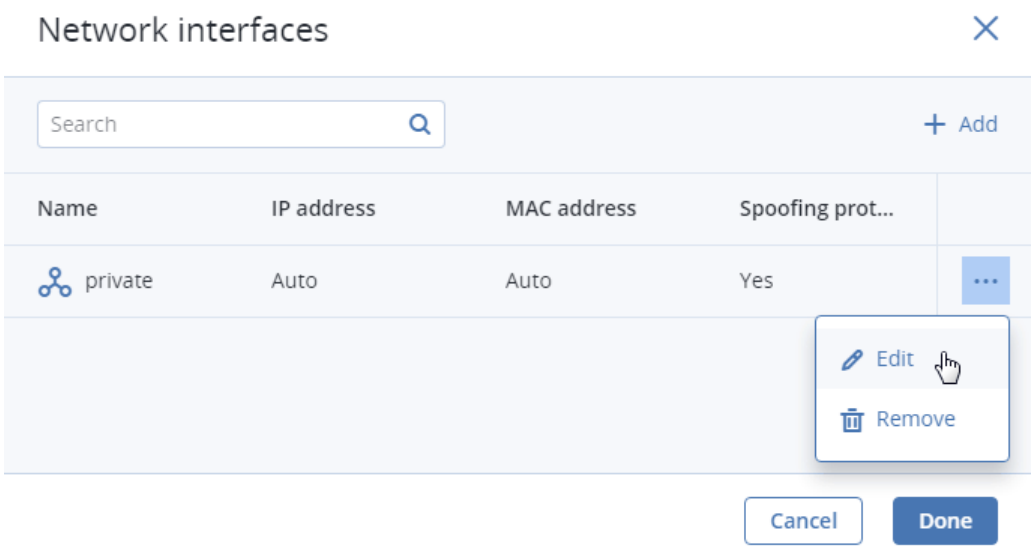
5. Optionally, in the **Volumes** window, click **Add** or **Attach** to create or attach any other volumes you need. To select a volume as bootable, place it first in the list by clicking the up arrow button next to it.
6. After you select an image or a volume, the **Placement** drop-down list is displayed. Placements are created by the administrator to group nodes or VMs sharing a distinctive feature, like a special license. Select the placement corresponding to the VM characteristics. For more information, see the "Managing Placements" section of the *Administrator's Guide*.
7. In the **Flavor** window, choose a flavor and click **Done**.



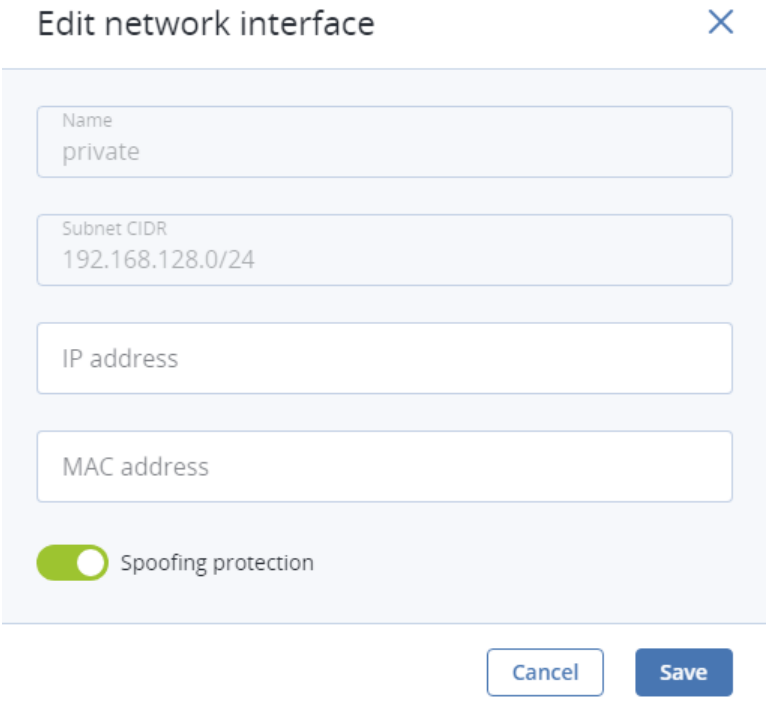
8. In the network window, click **Add**, select a virtual network interface and click **Add**. It will appear in the **Network interfaces** list.



You can edit additional parameters of newly added network interfaces, like IP and MAC addresses and spoofing protection. To do this, click interface's ellipsis icon, then **Edit**, and set parameters in the **Edit network interface** window.



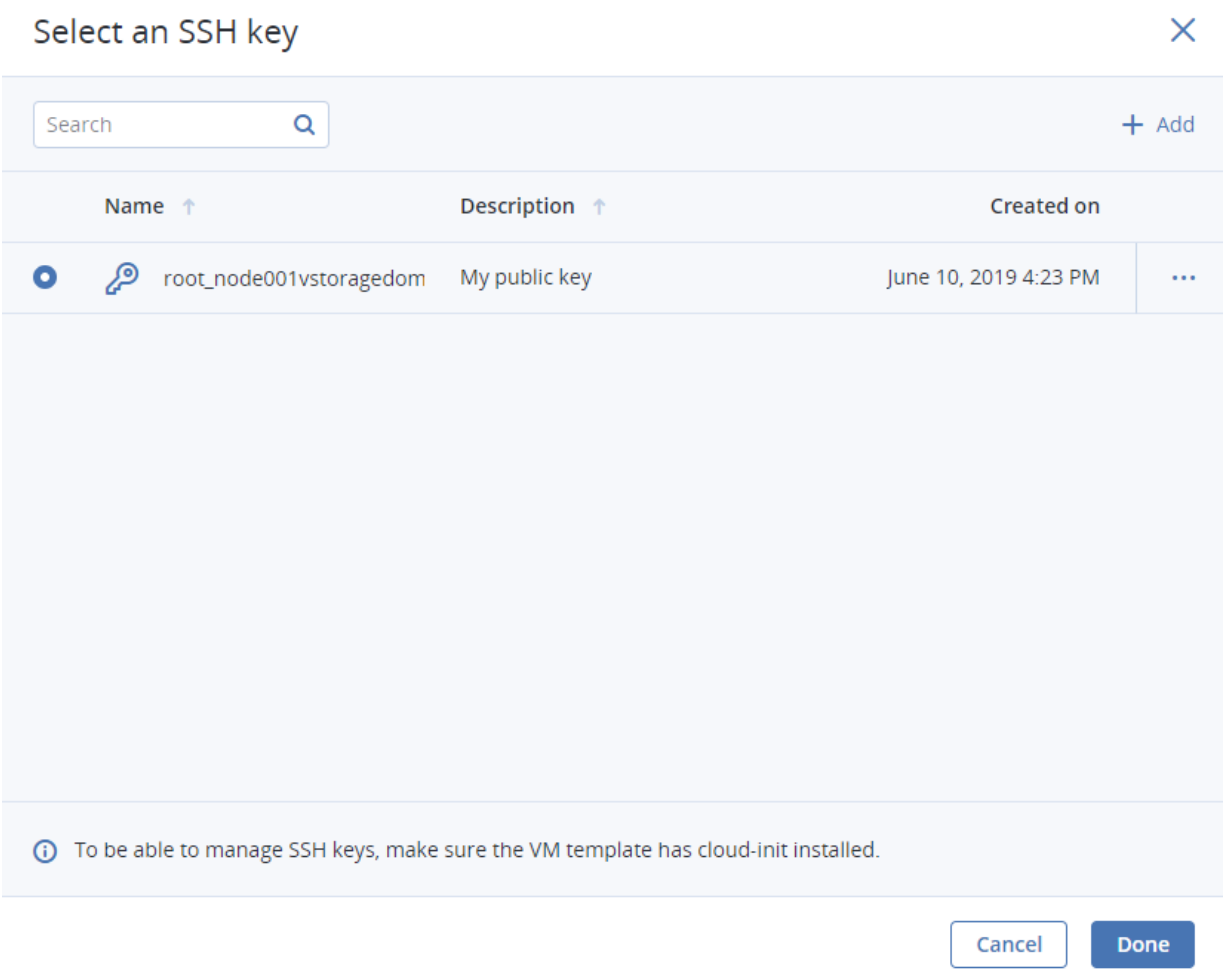
You will not be able to edit these parameters later. Instead, you will be able to delete the old network interface and replace it with a new one.



Click **Done**.

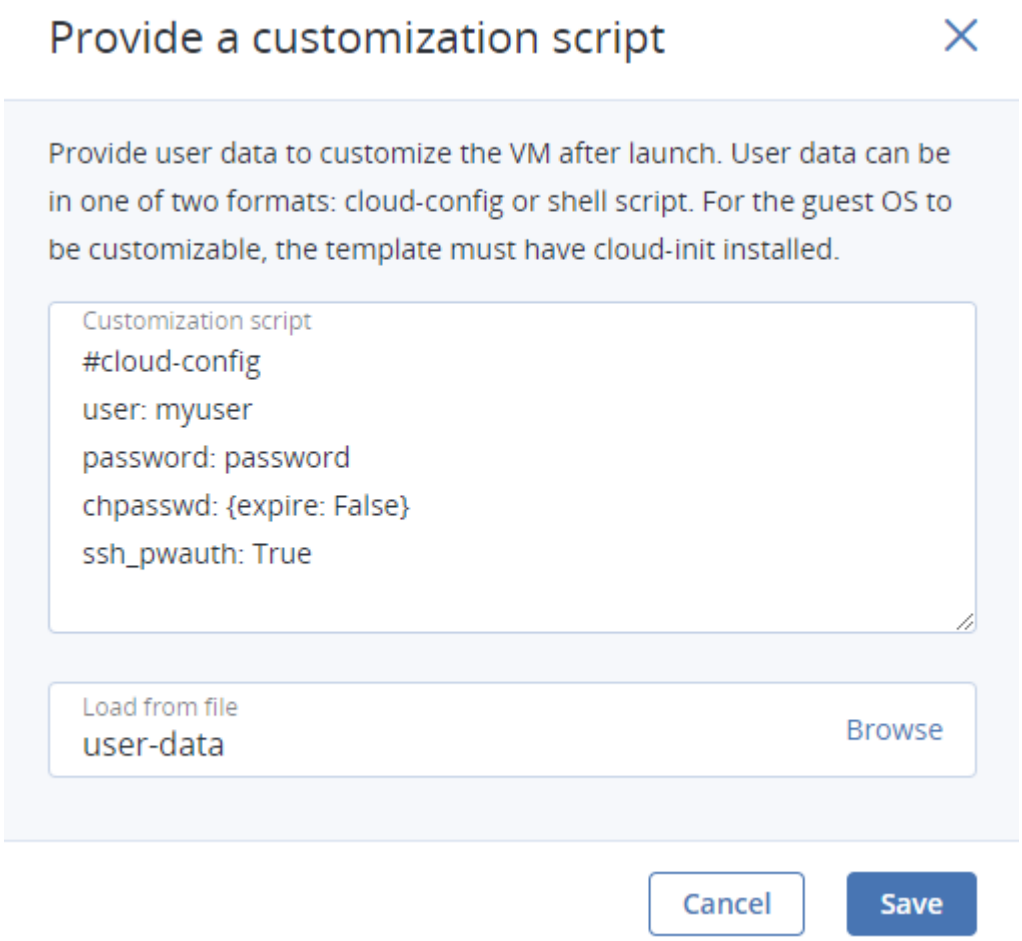
9. (Optional) If you are deploying the VM from a template or boot volume (not an ISO image), you can specify the following:

- An SSH key to be injected into the VM. To do it, select an SSH key in the **Select an SSH key** window, and click **Done**.



Note: To be able to connect to the VM via SSH, make sure the VM template or boot volume has cloud-init and OpenSSH installed (see the "Preparing Templates" section of the *Administrator's Guide*).

- User data to customize the VM after launch. You can specify user data in one of two formats: cloud-config or shell script. To do it, write a script in the **Customization script** field or browse a file on your local server to load the script from.



Note: For the guest OS to be customizable, make sure the VM template or boot volume has cloud-init installed (see the "Preparing Templates" section of the *Administrator's Guide*).

To inject a script in a Windows VM, refer to the Cloudbase-Init documentation. For example, you can set a new password for the account using the following script:

```
#ps1
net user <username> <new_password>
```

10. Back in the **Create virtual machine** window, click **Deploy** to create and boot the VM.
11. If you are deploying the VM from an ISO image (not a boot volume template or a volume with a pre-installed guest OS), select the VM, click **Console**, and install the guest OS using the built-in VNC console.

12. (Optional) If you are deploying the VM from a prepared template with an injected SSH key, you can connect to it via SSH using the username and the VM IP address:

    - For Linux templates, enter the username that is default for the cloud image OS (for example, for a CentOS cloud image, the default login is `centos`).
    - For Windows templates, enter the username that you specified during Cloudbase-Init installation.

    For example:

```
# ssh myuser@10.10.10.10
```