<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3</td>
<td>Exporting Storage Space via NFS</td>
<td>23</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Creating an NFS Cluster</td>
<td>24</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Creating NFS Shares</td>
<td>24</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Creating and Mounting NFS Exports</td>
<td>24</td>
</tr>
<tr>
<td>6.</td>
<td>Connecting Acronis Backup Software to Storage Backends via Backup Gateway</td>
<td>26</td>
</tr>
<tr>
<td>6.1</td>
<td>Configuring a Backup Gateway</td>
<td>27</td>
</tr>
<tr>
<td>6.2</td>
<td>Configuring Acronis Backup Cloud</td>
<td>29</td>
</tr>
<tr>
<td>7.</td>
<td>Monitoring the Storage Cluster</td>
<td>31</td>
</tr>
<tr>
<td>8.</td>
<td>Enabling High Availability</td>
<td>32</td>
</tr>
<tr>
<td>8.1</td>
<td>High Availability for the Management Node</td>
<td>32</td>
</tr>
<tr>
<td>8.2</td>
<td>High Availability for the Services</td>
<td>33</td>
</tr>
<tr>
<td>8.3</td>
<td>Testing High Availability</td>
<td>34</td>
</tr>
</tbody>
</table>
CHAPTER 1

Introduction

Virtuozzo Infrastructure Platform represents a new generation of hyper-converged infrastructures targeted at both service providers and end customers. It is a scale-out, cost-efficient, and multi-purpose cyber protection solution that combines universal storage and high-performance virtualization.

Virtuozzo Infrastructure Platform works seamlessly with Acronis Cyber Cloud's suite of products, Acronis Cyber Backup. It minimizes the number of technologies needed in data centers and provides for additional performance improvements.

This guide gets you started on Virtuozzo Infrastructure Platform and outlines the following steps to evaluate its main features:

1. Install and configure Virtuozzo Infrastructure Platform.
2. Create a storage cluster.
3. Create a compute cluster and allocate its resources.
4. Create virtual machines.
5. Export storage space via iSCSI, S3, NFS, Backup Gateway.
7. Enable and test high availability.

There are many different scenarios possible, but in this guide we'll walk you through the most common ones. The procedures outlined in this guide are typical and simplified for evaluation purposes. However, Virtuozzo Infrastructure Platform is supported by a complete and detailed documentation suite you should refer to for further guidance. For more information, see the Quick Start Guide, Installation Guide, Administrator’s Guide, Self-Service Guide, and Storage User’s Guide.
CHAPTER 2
Planning the Infrastructure

2.1 Hardware Requirements

There are many hardware configurations supported and described in the section “Planning Node Hardware Configurations” of the Installation Guide. However, for the evaluation purposes we recommend deploying three nodes. This is to ensure that the cluster can survive the failure of one node without data loss. The following table lists the minimum hardware requirements for each of the three nodes. To enable high availability, you will need three nodes meeting the requirements for the management node with storage and compute.

Table 2.1.1: Minimum node hardware requirements

<table>
<thead>
<tr>
<th>Type</th>
<th>Management node with storage and compute</th>
<th>Secondary node with storage and compute</th>
<th>Management node with storage and Backup Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>64-bit x86 processors with AMD-V or Intel VT hardware virtualization extensions enabled. 16 logical CPUs</td>
<td>64-bit x86 processor(s) with Intel VT hardware virtualization extensions enabled 8 logical CPUs</td>
<td>64-bit x86 processor(s) with AMD-V or Intel VT hardware virtualization extensions enabled 4 logical CPUs</td>
</tr>
<tr>
<td>RAM</td>
<td>32 GB</td>
<td>16 GB</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Type</th>
<th>Management node with storage and compute</th>
<th>Secondary node with storage and compute</th>
<th>Management node with storage and Backup Gateway</th>
</tr>
</thead>
</table>
| Storage      | 1 disk: system + metadata, 100+ GB SATA HDD
1 disk: storage, SATA HDD, size as required | 1 disk: system, 100 GB SATA HDD
1 disk: metadata, 100 GB SATA HDD (only on the first three nodes in the cluster)
1 disk: storage, SATA HDD, size as required | 1 disk: system + metadata, 120 GB SATA HDD
1 disk: storage, SATA HDD, size as required |
| Network      | 1 GbE for the private network
1 GbE (VLAN tagged) for the public network | 1 GbE for the private network
1 GbE (VLAN tagged) for the public network | 2 x 1 GbE |

You will also need at least two IPs in the public network (for highly available admin panel and for each NFS share), one IP in the private network (for highly available management node), and two DNS names (for S3 and Backup Gateway).

Following is a sample network layout for our evaluation scenario. Your host names and addresses may differ depending on your settings.

### Reserved addresses

**Private network**

- 196.1.1.34 HA internal management eth0

**Public network**

- 10.37.130.4 HA admin panel eth1
- 10.37.130.5 NFS share 1 eth1
- 10.37.130.6 NFS share 2 eth1

**DNS**

- s3.example.com S3 storage
- backup.example.com Backup Gateway
The DNS names are used by backup agents to send backups to and retrieve them from cloud storage. If your client machines and Virtuozzo Infrastructure Platform nodes are located in different datacenters, we strongly recommend configuring the DNS name in one of your favorite DNS services: Azure DNS for Azure, Amazon Route 53 for Amazon, or Google Cloud DNS for Google. If it is not possible for some reason, you have to manually add the DNS name to the `/etc/hosts` file on each node. On the other hand, if the client machines and Virtuozzo Infrastructure Platform nodes are located in the same datacenter, you can use a local DNS instead of a public one to speed up the backup. A local DNS can work only with a local IP address, so we recommend using NAT in this case.

We recommend using the Google Chrome browser for accessing Virtuozzo Infrastructure Platform and S3 storage in our evaluation scenario.

### 2.2 Understanding Storage Policies

Virtuozzo Infrastructure Platform can be used for the following scenarios: iSCSI block storage, NFS file storage, S3 object storage, Backup Storage (to store the backups created in Acronis Cyber Backup solutions). You can also use its built-in hypervisor to create compute virtual machines. In all these scenarios, the common unit of data is a volume. For the compute service, a volume is a virtual drive that can be attached to a VM. For iSCSI, S3, Backup Gateway, and NFS, a volume is the data unit used for exporting space. In all these cases, when you create a volume you need to define its **redundancy mode**, **tier**, and **failure domain**. These parameters make up a **storage policy** defining how redundant a volume must be and where it needs to be located.

Redundancy means that the data is stored across different storage nodes, and stays highly available even if some nodes fail. If a storage node is inaccessible, the data copies on it are replaced by new ones that are
distributed among healthy storage nodes. When the storage node goes up after the downtime, out-of-date data on it is updated.

With replication, Virtuozzo Infrastructure Platform breaks a volume into fixed-size pieces (data chunks). Each chunk is replicated as many times as set in the storage policy. The replicas are stored on different storage nodes if the failure domain is host, so that each node has only one replica of a given chunk.

With erasure coding (or just encoding), the incoming data stream is split into fragments of certain size. Then each fragment is not copied itself, instead a certain number (M) of such fragments are grouped, and a certain number (N) of parity pieces are created for redundancy. All pieces are distributed among M+N storage nodes (selected from all available nodes). The data can survive the failure of any N storage nodes without data loss. The values of M and N are indicated in the names of erasure coding redundancy modes. For example, in the 5+2 mode, the incoming data is split into 5 fragments and 2 more parity pieces (same size) are added for redundancy. Refer to the Administrator’s guide for detailed information on redundancy, data overhead, number of nodes, and raw space requirements.

To better understand a storage policy, let’s have a look at its main components (tiers, failure domains, and redundancy) for a sample scenario. For example, you have three nodes with a number of storage nodes: fast SSDs and high-capacity HDDs. Node 1 has only SSDs; nodes 2 and 3 have both SSDs and HDDs. You want to export storage space via iSCSI and S3, so you need to define a suitable storage policy for each workload.

- The first parameter, **tier**, defines a group of disks united by criteria (drive type, as a rule) tailored to a specific storage workload. For this sample scenario, you can group your SSD drives into tier 2, and HDD drives into tier 3. You can assign a disk to a tier when creating a storage cluster or adding nodes to it (see Creating the Storage Cluster (page 10)). Note that only nodes 2 and 3 have HDDs and will be used for tier 3. The first node’s SSDs cannot be used for tier 3.

- The second parameter, **failure domain**, defines a scope within which a set of storage services can fail in a correlated manner. The default failure domain is host. Each data chunk is copied to different storage nodes, just one copy per node. If a node fails, the data is still accessible from the healthy nodes. A disk can also be a failure domain, though it is only relevant for one-node clusters. As you have three nodes in this scenario, we recommend choosing the host failure domain.

- The third parameter, **redundancy** should be configured to fit out disks and tiers. In our evaluation example, you have three nodes: all of them have SSDs on tier 2. So if you select tier 2 in your storage policy, you can use the three nodes for 1, 2, or 3 replicas. But only two of your nodes have HDDs on tier 3. So if you select tier 3 in your storage policy, you can only store 1 or 2 replicas on the two nodes. In both cases, you can also use encoding, but for our evaluation let’s stick to replication: 3 replicas for SSDs and 2 replicas for HDDs.
To sum it up, the resulting storage policies are:

**Storage policy 1**
- 3 replicas
- Host failure domain
- Tier 2 (SSD)

**Storage policy 2**
- 2 replicas
- Host failure domain
- Tier 3 (HDD)
CHAPTER 3

Managing the Storage Cluster

This chapter outlines the steps to install Virtuozzo Infrastructure Platform and configure its initial settings for further deployment. First, you need to create a basic infrastructure on the management node, and then add secondary nodes to it in a similar manner. We recommend adding two secondary nodes for evaluation. Then, configure the networks and create a storage cluster on your nodes.

3.1 Installing Virtuozzo Infrastructure Platform

To obtain the distribution ISO image, you can visit the product page and submit a request for the trial version.

You can also download the ISO from the Acronis Cyber Cloud. To do that, in the management portal, select SETTINGS > Locations in the left menu. Click Add backup storage and click the Download ISO button in the open window. After you have obtained the distribution image, proceed to install Virtuozzo Infrastructure Platform.

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. Boot the server from the chosen media.

2. On the welcome screen, choose Install Virtuozzo Infrastructure Platform. Next, read and accept the End-User License Agreement.

3. Configure a static IP address for the NIC and provide a hostname. A dynamic IP is not recommended as it might cause issues with reaching the nodes. Check that the network settings are correct. At this stage, you can ping the static IP to check whether the network is working properly. Then, choose your time zone.

4. Specify what type of node you are installing: management or secondary.
Chapter 3. Managing the Storage Cluster

3.2 Configuring Networks

Now that you have installed Virtuozzo Infrastructure Platform on the management and two secondary nodes, you need to set up networks and interfaces. Use separate networks for internal and public traffic. Doing so will prevent public traffic from affecting cluster I/O performance and also prevent possible denial-of-service attacks from the outside.

1. To configure networks, go to the INFRASTRUCTURE > Networks screen on the admin panel. The advanced configuration is discussed in the “Managing Networks and Traffic Types” section of the Administrator’s Guide, but for our simplified deployment it is enough to customize the default Public and Private networks as follows:

<table>
<thead>
<tr>
<th>Network</th>
<th>Traffic types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Compute API, S3 public, iSCSI, NFS, ABGW public, Admin panel, SSH, VM public, SNMP, Self-service panel</td>
</tr>
</tbody>
</table>

Continued on next page
Table 3.2.1 – continued from previous page

<table>
<thead>
<tr>
<th>Network</th>
<th>Traffic types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>Storage, Internal management, OSTOR private, ABGW private, VM private, Admin panel, SSH</td>
</tr>
</tbody>
</table>

2. To configure interfaces, go to the INFRASTRUCTURE > Nodes screen and click a node’s name. On the node view, click NETWORK>. For the management node, both interfaces are already set up. You still need, however, to configure public network interfaces for every secondary node. Select an interface and click Assign network on the right menu. Select Public. You should now have one interface connected to the private network, and the other assigned to the public network. Repeat these steps for every secondary node to connect them to the private and the public networks.

3. Make sure your DNS settings are correct. To do that, go to the SETTINGS > Cluster DNS screen. Check that the cluster DNS is configured properly and points to a DNS able to resolve external host names.

The figure below shows the sample network infrastructure we are going to build for our evaluation scenario:
Chapter 3. Managing the Storage Cluster

Note: If you only have one network, do not connect one node to it via two interfaces. In case of one network, work with one public interface of the node.

3.3 Creating the Storage Cluster

Now that you have created the management and secondary nodes and configured networking, you can proceed to create the storage cluster.

1. Log in to the admin panel on port 8888. Panel's IP address is shown in the console after deploying the management node. Use the “admin” user name and the admin panel password you created in Installing Virtuozzo Infrastructure Platform (page 7).

2. Open the INFRASTRUCTURE > Nodes screen and click a node in the UNASSIGNED list.

3. On the node overview screen, click Create cluster and type a name. To add a secondary node, click Join cluster in the right pane.

4. For the evaluation scenario, you need to assign node's storage disks to various tiers (see Understanding Storage Policies (page 4)). For node 1, assign SSDs to tier 2. To do that, click Advanced configuration. You will be taken to the list of drives on the node on the Join cluster or New cluster panel. Select one or more drives on the list and click Configure on the right. On the Choose role screen, select the required tier. In a similar way, assign SSDs to tier 2 and HDDs to tier 3 for nodes 2 and 3. For more information on disk roles, see the “Creating the Storage Cluster” section of the Administrator's Guide.

5. Click NEW CLUSTER or JOIN CLUSTER. On the Configuration summary screen, check the disk settings. Click PROCEED. You can monitor disk configuration progress on the INFRASTRUCTURE > Nodes screen.
CHAPTER 4

Managing the Compute Cluster

Virtuozzo Infrastructure Platform offers high-performance virtualization, and its fundamental component is a compute cluster. It allows admins to create multiple tenants, virtual machines, and software-defined networks, as well as easily deploy container orchestration solutions like Kubernetes.

In this section, we will have a look at two common scenarios for the compute cluster:

• A service provider offers virtualization services to end customers. In this case, the SP can benefit from self-service panels with white-labeling, multitenancy, and easy resource management and allocation.

• An enterprise plans to adopt new software across its infrastructure. It can deploy virtual machines and install the software in them, for all employees to access and work with.

Although those two scenarios differ from each other significantly, the procedure within Virtuozzo Infrastructure Platform is similar:

1. Create the compute cluster.

2. Allocate resources to domains, projects (tenants), and users.

3. Create virtual machines for the end users.

In this chapter, we shall take a look at each of these steps.

4.1 Creating the Compute Cluster

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. The network state of each selected
node should be *Configured*, if you followed the instructions in *Configuring Networks* (page 8). Click *Next*.

2. In the **Public network** section, you can enable IP address management if you have a pool of IP addresses that you can use. It is also necessary for virtual routers, floating public IP addresses, and network load balancers. Otherwise, you can leave IP address management disabled.

3. In the **Add-on services** section, you can install additional services if you want to evaluate them as well. Or you can do it later as detailed in the *Administrator's Guide*.

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

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

4.2.1 Creating Domains, Projects, and Users

There are three user roles in Virtuozzo Infrastructure Platform: a system administrator, a domain administrator, and a project member. The following chart shows their typical functions at service providers and enterprises, along with their workspaces: admin or self-service panels.

- System administrators have full control over Virtuozzo Infrastructure Platform and can access the admin panel. This is the role you get by default when installing Virtuozzo Infrastructure Platform. These are usually infrastructure administrators of an MSP or the main IT department of an enterprise, depending on your business case.

- Domain administrators are in charge of their domains. A domain is a collection of virtualization projects (tenants) and users (end customers). Domain administrators have access to the self-service panel. They can create users as well as use project resources within allowed quotas: deploy and manage virtual machines, images, volumes, networks, routers, floating IPs, and SSH keys.

- Project members can manage resources within their projects using the self-service panel: deploy and manage virtual machines, images, volumes, networks, routers, floating IPs, and SSH keys. A project is a
set of compute and storage resources defined by quotas and accessible by assigned users.

Both domain administrator and project member roles have certain limitations. For instance, they cannot migrate virtual machines between nodes as nodes are not present at that level of abstraction.

In our evaluation scenario, you are the system administrator. Once you have created the compute cluster, you need to create a domain, a project, some end users, and assign them to the project. Then, create a storage policy for VM volumes to define their redundancy parameters. Next, configure virtual networking. After that, domain users will have access to their domains and projects via the self-service panel. There they will be able to create their own virtual machines, volumes, networks, etc.

Note: The self-service panel IP address is shown on the SETTINGS > Self-service screen in the admin panel.

The actions to perform in the self-service panel are described in the Self-Service Guide. For our evaluation, we shall stick to the operations with the compute cluster done from the admin panel.

1. Create a domain. To do this, log in to the admin panel and open the SETTINGS > Projects and users screen. Click Create domain in the upper-right corner. Specify a name and a description for the new domain. Click Create.

2. Create an admin account for the new domain. To do this, select the newly created domain and click Create user. Specify a login and a password and select the Domain administrator role. Check the Image uploading box to allow the new administrator to upload images for deploying virtual machines. Click Create.

3. Create a project. To do this, navigate to the domain’s PROJECTS tab and click Create project. Set the quotas and click Create. Make sure that you have enough CPU, RAM, storage, and network resources to deploy virtual machines (and add-on services, should you choose to enable them).

4. Create a project member. To do this, open the DOMAIN USERS tab and click Create user. Specify a login and a password and select the Project member role. Choose the project to assign the new member to. Click Create.

5. Optionally, customize the self-service panel’s look on the SETTINGS > Self-service screen by adding logos and selecting a color scheme. This way, managed service providers, for example, can offer branded virtualization services to end customers.
4.2.2 Creating Storage Policies

In order to create a new storage policy, on the COMPUTE > Storage screen open the STORAGE POLICIES tab and click Create storage policy. Specify a name, a tier, a failure domain, and a redundancy scheme. For the evaluation scenario, select the 2 replicas mode and Host as the Failure domain.

Now that you have created a storage policy, you can select it for volumes when creating virtual machines (see Creating Virtual Machines (page 15)). You can also apply it when creating volumes directly on the VOLUMES tab.

Storage policies can be used in project quotas. A policy created before a project will be enabled in its quotas. A policy created after a project will not be enabled for that project automatically. You will need to edit that project's quotas and select the policy manually.

4.2.3 Creating Compute Networks

Before deploying virtual machines, you need to configure networking on the COMPUTE > Network screen. A private virtual network lets virtual machines connected to it communicate with each other. A public virtual network connects your virtual machines to an existing physical network, so they can access the Internet, for example.

In order to create a new network, click Create virtual network and specify its type. Provide a name for the new network, a subnet CIDR, e.g., 192.168.0.1/24, and a gateway. Click Next to proceed. If you have a pool of IP addresses for your virtual machines, you can enable the built-in DHCP server to have these IP addresses automatically assigned to virtual machines. Click Create virtual network to complete the process.

Along with virtual networks, you can create floating IPs. A floating IP is a public IP address that you can manually assign to a private IP address of a virtual machine. It will let you access the virtual machine from the public network, even though it only has a private IP address. To create a floating IP, you will first need to link a public and a private network with a virtual router. For more details, see the “Managing Floating IP Addresses” section of the Administrator's Guide.

4.3 Creating Virtual Machines

Now that you have created a compute cluster, a domain and a project, a storage policy, and networks, you can proceed to create virtual machines.
In our evaluation scenario, you will create a virtual machine from an image. You can either upload one or use the Cirros image shipped by default. To upload an image, open the **COMPUTE > Virtual Machines > IMAGES** tab. You can use ISO images and templates (ready-to-use volumes in the QCOW2 cloud image format with the OS and apps installed). Click **Add Image** and select an ISO image from your local machine. Specify a name for the new image and select a compatible operating system from the drop-down list. Check the **Share between all projects** box, if you want to use this image as a template for future VM deployments. Click **Add**.

**Note:** Virtuozzo Infrastructure Platform supports a wide range of Windows and Linux guest operating systems that you can deploy virtual machines from (see the “Supported Guest Operating Systems” section of the Administrator’s Guide). Moreover, it uses a number of patented innovations to optimize the performance of deployed VMs. For example, Windows-based VMs should perform as if they were deployed on Hyper-V.

1. On the **COMPUTE > Virtual Machines** screen, click **Create virtual machine** and specify a name.

2. To create a VM from an image, select the image uploaded earlier. In the section **Volumes**, you will see the bootable volume automatically added based on the image data. You can change the volume’s storage policy. To do that, click the pencil sign in the **Volumes** section, in the **Volumes** window click the ellipsis icon, select **Edit** and change the policy in the **Edit volume** window. You can also add new volumes to the VM here.

3. In the section **Flavor**, select a flavor, a preset defining how many virtual CPUs and how much memory the virtual machine will have.

4. In the section **Networks**, add interfaces to virtual networks that your virtual machine should be connected to.

5. Click **Deploy** to start virtual machine creation. Watch the status of new virtual machine. Once it becomes **Active**, the VM is ready.

In order to access the newly created virtual machine, click its name and click **Console** in the right pane. On the **Monitoring** tab of the VM, you can see how much resources it uses.

**Note:** You can also migrate virtual machines from VMware vCenter using the **virt-v2v** tool, as described in the **Administrator’s Command Line Guide**, section “Migrating Virtual Machines from VMware vCenter to Virtuozzo Infrastructure Platform”.

Once your virtual machine is ready, you can perform a wide range of operations on it: stop and start,
suspend and resume, reboot, migrate, and more. For more details, refer to the “Managing Virtual Machines” section of the Administrator's Guide.
Exporting Storage Space

Virtuozzo Infrastructure Platform allows you to export storage space:

- as block storage via iSCSI for virtualization, databases and other needs. You can export cluster disk space to external physical or virtual hosts in the form of LUN block devices over iSCSI in a SAN-like manner.

- as object storage for storing unlimited number of files via an S3-compatible protocol. The S3-like object storage can store data like media files, backups, Open Xchange files, with the access provided via Dropbox-like applications. End users can run the applications for S3 after the data migration from Amazon S3 to Virtuozzo Infrastructure Platform. They can also build their own object storage services compatible with Amazon S3.

- via NFS. You can organize nodes into a highly available NFS cluster in which you can create NFS shares. In each share you can create multiple NFS exports which are actual exported directories for user data. Each export can be mounted using standard commands. On the technical side, NFS volumes are based on object storage. An NFS cluster makes a perfect cold and warm file storage but is not recommended for hot workloads with high performance requirements. For the best integration with VMware vSphere it’s recommended to use iSCSI protocol.

5.1 Exporting Storage Space via iSCSI

Virtuozzo Infrastructure Platform allows you to export cluster disk space to external operating systems and third-party virtualization solutions in the form of LUN block devices over iSCSI in a SAN-like manner.

You can create groups of redundant targets running on different storage nodes. To each target group you can attach multiple storage volumes with their own redundancy provided by the storage layer. These
volumes are exported by targets as LUNs.

Each node in a target group can host a single target for that group. If one of the nodes in a target group fails along with its targets, healthy targets from the same group continue to provide access to the LUNs previously serviced by the failed targets.

5.1.1 Creating Target Groups

To create a target group, open STORAGE SERVICES > Block storage > TARGET GROUPS and click Create target group. A wizard will open where you need to do the following:

1. On Name and type, enter a target group name and select iSCSI. Next, select at least two nodes to add to the target group for high availability.

2. On Targets, select iSCSI interfaces to add to the target group. On Volumes, select volumes to attach to target group LUNs, or you can add them later. For the evaluation scenario, skip the Access control settings.

3. On Summary, review the target group details. Click Create.

The created target group will appear on the TARGET GROUPS tab. Its targets will start automatically. Click the group name to view its details. On the TARGETS tab you can add more nodes for new targets. You can also view or add LUNs on the LUNS tab.

5.1.2 Creating Volumes

1. Open STORAGE SERVICES > Block storage > VOLUMES and click Create volume. A wizard will open.

2. On Name and size, enter a volume name and specify its size. Note that volumes can be extended later but not shrunk.

3. On Storage policy, select a redundancy mode, a storage tier, and a failure domain.

4. On Summary, review the volume details. Click Create.
5.1.3 Attaching Volumes to Target Groups

1. Open STORAGE SERVICES > Block storage > TARGET GROUPS, click the ellipsis icon of the desired target group, and click Add LUNs.

2. In the Attach window that opens, select volumes to attach to the target group or create them. Click Apply.

3. On the TARGET GROUPS tab, click the required target group name and go to the LUNS tab. Here you can see all the available LUNs.

5.1.4 Accessing iSCSI Targets from VMware vSphere

You can access iSCSI targets from Linux, Microsoft Hyper-V, and VMware vSphere. See the “Accessing iSCSI Targets” of the Storage User's Guide for more details on access from Linux and Microsoft Hyper-V. The following section describes the VMware vSphere scenario for evaluation.

Before using Virtuozzo Infrastructure Platform volumes with VMware vSphere, you need to configure it to properly work with ALUA Active/Passive storage arrays. It is recommended to change the default path policy to RR policy with the command:

```
# esxcli storage nmp satp set -s VMW_SATP_ALUA -P VMW_PSP_RR
```

Now you can reboot the host and create datastores from Virtuozzo Infrastructure Platform volumes exported via iSCSI. Log in to the VMware ESXi web panel and do the following:

1. In the Navigator, go to the Storage > Adapters tab and click Software iSCSI.

2. In the Configure iSCSI window, select Enabled. In the Dynamic targets section, click Add dynamic target and enter the IP addresses of your nodes.

   **Note:** You can see the IP addresses in the admin panel. On the INFRASTRUCTURE > Nodes screen, click the required node and copy its public network IP on the NETWORK section.

3. Click Save configuration.

4. Proceed to the Devices tab and click Refresh. The newly added disk will appear in the list of devices.
5. Select the disk and click **New datastore**. In the wizard that appears, enter a name for the datastore and select partitioning options. Click **Finish** to actually partition the disk.

**Warning:** Partitioning the disk will erase all data from it.

6. The ready-to-use disk will appear in the list of datastores. Select it and click **Database browser** to view its contents and upload files, so that you could proceed to check its accessibility.

### 5.2 Exporting Storage Space via S3

Virtuozzo Infrastructure Platform allows you to export cluster disk space to customers in the form of an S3-compatible object storage.

Object storage is optimized for storing billions of objects, in particular for application storage, static web content hosting, online storage services, big data, and backups. Compared to other types of storage, the key difference is that parts of an object cannot be modified, so if the object changes a new version of it is spawned instead. This approach eliminates the issue of conflicts.

Virtuozzo Infrastructure Platform can store replicas of S3 cluster data and keep them up to date in multiple geographically distributed datacenters. Geo-replication reduces the response time for local S3 users accessing the data in a remote S3 cluster, or remote S3 users accessing the data in a local S3 cluster, as they do not need an Internet connection. Geo-replication schedules the update of the replicas as soon as any data is modified. Its performance depends on the Internet connection speed, the redundancy mode, and cluster performance. If you have multiple datacenters with enough free space, it is recommended to set up geo-replication between S3 clusters residing in these datacenters as described in the “Exporting Data via S3” section of the *Administrator’s Guide*.

Before creating an S3 cluster, make sure you have a DNS name for the S3 gateway.
5.2.1 Creating an S3 Cluster

To create an S3 cluster, do the following:

1. In the left menu, click **STORAGE SERVICES > S3**. Select three nodes for our evaluation scenario, and click **Create S3 cluster** in the right menu.

2. Next, select a storage policy.

3. Specify the external (publicly resolvable) DNS name for the S3 endpoint that will be used by the end users to access the object storage. For example, `s3.example.com`. Click **Proceed**.

4. From the drop-down list, select an S3 endpoint protocol: HTTP, HTTPS or both. For our simple evaluation scenario, we recommend to select HTTPS and set the **Generate self-signed certificate** check box. Click **Done** to create an S3 cluster.

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

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

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

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

5.2.2 Managing S3 Users and Buckets

To add an S3 user, do the following:

1. On the **STORAGE SERVICES > S3 > USERS** screen, click **ADD USER**.

2. Specify an email address as user login and click **ADD**.

To automatically log in to the S3 portal with user credentials using the generated keys, in the admin panel select a user and click **Browse**. In this workspace you can create new buckets and monitor the contents of existing ones.

You can also log in to S3 storage using a third-party application, like CyberDuck, MountainDuck, or Backup Exec. For our evaluation scenario, connect to your S3 storage via CyberDuck following these steps:
1. In CyberDuck, click **Open Connection**.

2. Obtain your credentials from the Virtuozzo Infrastructure Platform admin panel:
   
   • Get the DNS name of the S3 endpoint on the **STORAGE SERVICES > S3 > OVERVIEW** tab.
   
   • Get the **Access Key ID** and the **Password**, on the **STORAGE SERVICES > S3 > USERS** tab. Select the required user and click **Keys** on the right to display the access key ID and the secure access key.

3. Specify your credentials in CyberDuck:

4. Once the connection is established, you can see the existing buckets and create new ones. Click **File > New Folder** to create a bucket. Specify a name for the new bucket, and then click **Create**. Use bucket names that comply with DNS naming conventions.

To manage files in buckets, you have to log in to the S3 portal as a user. For more information, see the “Accessing S3 Buckets” section of the *Storage User’s Guide*.

### 5.3 Exporting Storage Space via NFS

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

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

5.3.1 Creating an NFS Cluster

1. In the left menu, click **STORAGE SERVICES > NFS**.

2. Select node(s) and click **Create NFS cluster** in the right menu. For the evaluation scenario, we recommend selecting three nodes.

3. Click **CREATE**.

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

5.3.2 Creating NFS Shares

1. On the **STORAGE SERVICES > NFS > SHARES** screen, click **ADD NFS SHARE**.

2. On the **Add NFS Share** panel, specify a name (for example, share1) and a unique resolvable static IP address from the public network.

3. In **Share size**, specify the size. For users accessing exports, this value will be the filesystem size.

4. Select the desired tier, failure domain, and data redundancy type. Click **DONE**.

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

5.3.3 Creating and Mounting NFS Exports

1. On the **STORAGE SERVICES > NFS > SHARES** screen, click the number in the **Exports** column in the row of the desired share. This will open the share screen.

2. On the share screen, click **ADD EXPORT**, specify root as the export name and / as path and select the **Read and write** access mode. This will create a directory with a default path that designates export location inside the share and is used (alongside share's IP address) to mount the export. The root
export will be shown in the export list.

3. After creating the root export, you can mount it on Linux or MacOS as described in the *Storage User's Guide*. For our evaluation scenario, mount it on Linux with the following commands:

```bash
# mkdir /mnt/nfs
# mount -t nfs -o vers=4.0 <share_IP>:/<share_name>/ /mnt/nfs
```

where:

- `-o vers=4.0` is the NFS version to use.

- `<share_IP>` is the share IP address. You can also use the share hostname.

- `/<share_name>/` is the root export path, like `share1`.

- `/mnt/nfs` is an existing local directory to mount the export to.

To check the mounted storage, you can run `df -h`. 
Connecting Acronis Backup Software to Storage Backends via Backup Gateway

Virtuozzo Infrastructure Platform is integrated with both Acronis Backup and Acronis Backup Cloud. Its Backup Gateway feature adds public cloud storage capabilities to Acronis Cyber Cloud.

The Backup Gateway is intended for service providers who use Acronis Backup Cloud or Acronis Backup Advanced and want to organize an on-premise storage for their clients’ backed-up data. Acronis Backup protocol is optimized both for local and long-distance networks, so it can be used for branch office backup scenarios.

Besides, you can store backups on cloud services like Google Cloud, Microsoft Azure and AWS S3. In this case, the storage will be used as a proxy to a public or private cloud. Virtuozzo Infrastructure Platform supports many public clouds such as Amazon S3, Microsoft Azure, Google Cloud, and Alibaba Cloud. Moreover, it supports object storages in private clouds. Thus, your customers’ data can be stored and managed in the corresponding public or private cloud.

The Backup Gateway also allows to store backups on NAS via the NFS protocol. In this case, the cluster will be used as a proxy to a NAS, and the customers’ data will be stored and managed on the corresponding NAS.

In this section, we will show you how a managed service provider can set up a storage for storing and managing their customers’ backups for the Acronis Backup Cloud. The corresponding steps for Acronis Backup are similar.

Note: We assume that you have already created a partner account for the Acronis Backup Cloud and have
all the required credentials for it.

6.1 Configuring a Backup Gateway

Before configuring a backup gateway, make sure that the DNS configuration meets the requirements outlined in *Hardware Requirements* (page 2). Besides, port 44445 should be open for inbound/outbound connections for network interface with **ABGW public** role (that is the public network in our evaluation scenario).

1. Configure a new storage for storing and managing backups of your customers within the Virtuozzo Infrastructure Platform admin panel. To do this, log in to the Virtuozzo Infrastructure Platform and navigate to **Storage Services**, and then to **Backup Storage**.

2. Here you can see all the nodes in the storage cluster that can be used as backup destinations. Select the desired node or nodes and click **Create Gateway**. In the right panel, click **This cluster**. In our evaluation scenario, the customers' data will be stored and managed on the storage cluster nodes.

3. Select the appropriate data redundancy scheme that will be applied to your customers' backups.

4. Specify a DNS name that will be associated with the selected cluster and used to register that cluster within Acronis Backup Cloud (like *backup.example.com*). For more details, see *Hardware Requirements* (page 2). 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. It depends on a number of factors such as node availability and load.
5. Specify the URL of your Acronis Backup Cloud instance. By default, it is https://cloud.acronis.com. If you use Acronis Backup, at this stage you should use the IP address of the corresponding machine to access the Backup Management Console. Provide also a login and password for your partner account for Acronis Backup Cloud or admin account for Acronis Backup. Click Next.

You may want to test the DNS setup locally before going public. To do this, you can add the DNS name to the /etc/hosts file on machines you will access the backup gateway from. For example, 192.168.1.10 backup.example.com.

6. The deployment will start immediately. As soon as it is over, you will see three tabs: **OVERVIEW**, **NODES**, and **GEO-REPLICATION**. On the **OVERVIEW** tab, for example, you can see the information about the registered gateways and their performance.

**Note:** If the current storage does not have a public IP address and a DNS name, the Web Restore tool for Acronis Cyber Cloud cannot work properly.
Chapter 6. Connecting Acronis Backup Software to Storage Backends via Backup Gateway

6.2 Configuring Acronis Backup Cloud

1. Log in to the Acronis Backup Cloud and navigate to Settings > Locations. Make sure that the system created a new backup destination with the corresponding name derived from the DNS name. Set up the backup agents as described in the Acronis Backup User Guide.

2. Create a new customer and assign the new backup destination within the Acronis Backup Cloud. To do that, click New in the upper-right corner and select Customer. Specify the customer name, mode and language. Next, select services that you would like to provide to the new customer, for example, Acronis Backup Cloud. Besides, specify customer’s devices and workloads such as servers, workstations, etc. In the section Location, select the newly created storage in the drop-down box. Fill out other fields, such as customer’s email, language, first and last names and click Done to complete the whole process.

3. To confirm your account, check your email and follow the steps in the activation request.

4. After creating a customer, log in to Acronis Cyber Cloud as the admin and open the Clients screen. Click the created customer to open their Overview screen. Click Manage service to open the customer’s Backup Management Console.

5. On the Devices screen, click Add on the toolbar. Select the device you want to add. For our evaluation scenario, select a workstation with the OS currently in use. The backup agent installer will be downloaded.

6. In the backup agent installer, click Install. On the Almost done… screen, click Register the machine. Next, enter the device registration info and confirm it. Make sure you are using the customer’s account you’ve created: check the user in the upper-right corner. When the registration is completed, the added device will be displayed on the Devices > All devices screen of the customer’s Backup Management Console.

7. To create a backup from the customer’s machine, click the device and select Backup in the right menu. Click Add Backup Plan and specify its details. For our evaluation scenario, select Files/folders in What to Back Up. Then, select the items to back up, a destination cloud storage, and set None in Schedule. Click Create and the backup plan will be listed on the left. Click Run Now to start the backup process.

8. When the process is completed, you can view the backed-up files on the Backups > Locations screen. Click the required customer to see the files you uploaded earlier. Double-click the backup name to display its details on the right. You can click Recover Files/Folders to navigate to the uploaded files and download them if necessary.
Thus, you have configured the backup gateway in Virtuozzo Infrastructure Platform and the Acronis Backup Management Console, exported storage cluster space to Acronis Cyber Cloud, and uploaded some backups to your cloud storage.
CHAPTER 7

Monitoring the Storage Cluster

Virtuozo Infrastructure Platform provides built-in monitoring tools like a pre-integrated Prometheus engine and pre-configured Grafana dashboards, which show service state, availability and performance, as well as network bandwidth, migration/replication backlog, memory, and CPU usage. Integration with third-party systems is possible via 100%-compatible OpenStack APIs. You can ensure that systems are up and running smoothly, and troubleshoot problems before they impact end users or third-party systems.

1. To monitor the storage cluster, go to the MONITORING > Dashboard screen. Here you can get general information about the selected storage cluster for the last 30 minutes; 1, 6 and 12 hours; and for the last 7 days. The information displayed includes the read and write operations, chunk services’ health, and the physical and logical space usage. For more details, see the “Monitoring the Storage Cluster” section of the Administrator’s Guide.

2. For advanced monitoring, on the MONITORING > Dashboard screen, click Grafana dashboard. A separate browser tab will open with preconfigured Grafana dashboards of the storage cluster, hardware nodes, exports, etc. Two dashboards are dedicated to Acronis Backup Gateway. To see a detailed description for each chart, see the “Monitoring Backup Gateway” section of the Administrator’s Guide.

3. You can also monitor the backup gateway on the STORAGE SERVICES > Backup storage screen. Here you can see the information about the deployed backup storage cluster and its performance. Moreover, you can get the information about geo-replication of the selected backup gateways, as well as the data migrated from the legacy versions of Virtuozo Infrastructure Platform. Finally, you can get information about the storage usage in public clouds such as Amazon S3, Microsoft Azure, Google Cloud, or Alibaba Cloud.
CHAPTER 8

Enabling High Availability

High availability keeps Virtuozzo Infrastructure Platform services operational even if the node they are located on fails. In such cases, services from a failed node are relocated to healthy nodes.

You have previously built a cluster of three nodes, and can now make it more resilient and redundant. To do that, enable high availability for the management node, the admin panel and services.

8.1 High Availability for the Management Node

To enable high availability for the management node and the admin panel, follow these steps:

1. On the SETTINGS > Management node screen, open the MANAGEMENT HIGH AVAILABILITY tab.

2. Select three nodes and click Create HA. The management node is selected automatically.

3. On Configure network, make sure that for each node a private network interface is selected for internal management, and at least one public network interface is assigned to the admin panel.

4. Next, on Configure network, provide one or more unique static IP addresses.

5. Once you have enabled high availability for the management node, log in to the admin panel at the
specified static IP address (on port 8888).

8.2 High Availability for the Services

On top of highly available metadata services and enabled management node HA, Virtuozzo Infrastructure Platform 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 along with management node HA.

- **Virtual machines.** If a compute node fails or becomes unreachable over the network, virtual machines hosted on it are evacuated to other healthy compute nodes based on their free resources. The compute cluster can survive the failure of only one node. By default, high availability for virtual machines is enabled automatically after creating the compute cluster and can be disabled manually, if required.

- **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.

- **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.

- **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.

8.3 Testing High Availability

This section simulates an event in which the management node has failed:

1. Forcibly power off your Virtuozzo Infrastructure Platform management node.

**Note:** High availability keeps services operational if the node they are located on fails due to kernel
 crash, power outage, or becomes unreachable over the network. Graceful shutdown is not considered
 a failure event. So you should forcibly power off the node, or disconnect the network cable from it to
 test HA.

2. Open the **Infrastructure > Nodes** screen. The failed node has the **OFFLINE** status and is highlighted in
 red.

3. Even though one node has failed and is now unavailable, you can still access the following services:
   - Admin panel.
   - Virtual machines.
   - iSCSI: in the VMware vSphere, you can still access the volumes exported via iSCSI.
   - S3: you can still access your buckets via CyberDuck.
   - NFS: in the mounted root export, you can still access the data you uploaded.
   - Backup Gateway: in the Backup Management Console, you can still navigate to the backup you
     created earlier (it is accessible if you have properly configured the DNS name).

You have just run a demonstration where a node was forcibly powered off, causing the services and the data
to be evacuated to healthy nodes and remain available without downtime.