Acronis

acronis.com

Acronis Cloud Manager

Version 6.3

Getting Started Guide

REVISION: MONDAY, MARCH 10, 2025

Table of contents

What's new

Product improvements history

Version 6.3

- The new WMI-based approach is implemented in the VM backup plugin - switched to Hyper-V RCT API from VSS volume snapshot (legacy), leaving the option to use the old approach for backward compatibility.
- Added an ability to restore a VM from the backup archive with the new ID (without deleting the existing VM).
- Added the information about the storage usage by VMs to the VM list - the total space consumed and the number of the VHDs for each VM.
- Added the "Checkpoint" context menu option for VMs.
- Added the "Move" context menu option for VMs.
- When the new VHD is created in the VM settings, the same datastore as configured in the VM settings is set for the new VHD.
- Added detailed information to the Jobs to track the VM settings changes.
- Added an ability to change the VM checkpoint settings in the resource pool.

Version 6.2

- Implemented the two-factor authentication feature: to login to management console user will need to enter the one-time password from **Google authenticator** application along with the main password. After 10 unsuccessful logon attempts both because of wrong main password or one-time password from 2FA, the logon is blocked for the user for the period of one hour on the machine where the logon attempts are done.
- Added the ability to update only selected agents from the list of agents available for updating (management console, web portal).
- Added the ability to see under which user the current session is opened (web portal).
- In the **Checkpoints** window added the function of creating a checkpoint by clicking on the right mouse button.
- Optimized performance of the management console and the other product components.

Version 6.1

- Checkpoints Enhancement: Added the **Checkpoints**button (instead of **Checkpoint**) that navigates console to the selected VM with opened checkpoints tab. The **Create checkpoint** button is moved to the **Checkpoints** ribbon group. On the create checkpoint action the user is asked to type in the name of the checkpoint (the dialog contains the default value with the name-date for the checkpoint). The information about who initiated the checkpoint is stored in DB. The **Created by** info - user name is shown in the checkpoints tree.

- Extended VMs filtering: implemented search function that supports more than just the “VM name”. i.e. ability to search by IP address, host or operating system. Basically, ability to search by any information in any of the columns.
- **Create Backup** wizard - password is hidden: on the **Summary** page of the **Create backup** wizard password displayed hidden with ****.
- Added configurable custom properties for hosts and VMs.
- Guest console enhancement: the ability to connect to more than one VM at a time and opening VM settings does not block other windows.
- Displayed host extended info: extended tooltip info in the host tree: free memory, CPU model and frequency, number of cores.
- VM tree - logical view enhancement: added the **Undefined** category and all virtual machines that reside in no category are placed there.
- Summary info is added into the **Move VM** wizard including destination details.
- Added fibre channel adapter configuration.

Version 6.0

- Introduced the new concept of resources management and allocation to tenants: Resource pools, quotas and usage.
- Added ability to put Hyper-V hosts into maintenance mode (enable/disable) with configurable options to define the behavior of the hosted VMs: what to do with the VMs when the host is put into maintenance mode.
- Implemented dedicated guest connection view for Azure virtual machines in the web portal.

Version 5.1

- Added Microsoft Azure support to the web portal.

Version 5.0

- Representing the new web portal - web based graphical user interface.

Version 4.1

- GUI -
  - Re-branding the product to Acronis Cloud Manager

Version 4.0

- Installation -
  - Ability to select self-signed or custom certificates as an additional step when installing management service
- Datastore -
  - Auto Discovery of datastores

- Jobs –
  - Recording of login and log off events
  - Recording of console upgrades
  - Delete option is disabled
  - Disk copy percentage in the jobs view
  - Dock/pin panel
- Monitoring/Alerts
  - Dynamic optimization event alerts
  - Exporting alerts to syslog
- Azure Management/Administration
  - RBAC Feature to disable Azure & commands for tenants

Version 3.3

- Reporting/Dashboard –
  - New System Status Report – PDF output
  - New look for Zombie VMs report
  - Ability to schedule PDF Reports
- REST API Support –
  - VM Management/Monitoring/Reporting/Backup/SDN/Administration
- Management –
  - Loading time Improvements
  - Cluster to Cluster VM migration
  - Inspect Virtual Hard Disk
  - Support Anti Affinity Rules In Failover Cluster

Version 3.2

- Monitoring –
  - VM CPU Usage – VM Level monitoring shows Guest CPU usage.
  - Host Memory Usage – Total Memory Used By VM's and Total Memory used by OS Partition.
  - Host CPU Usage – This is the amount of CPU that the Hosts are using for Hyper-V, we will also show the total CPU % the operating system is using the host.
- Reporting – Custom Report Timeframe – Allows user to change the timeframe to generate, first start to more customizable reports.
- Management –
  - MAC Address Pools – Enterprise or Multi-Site clients can now use custom MAC address pools.
  - Replication Failure Notices – generates alerts and emails on Replication status and failures.
  - Current VMQ Status – shows the status of the virtual machine queue (VMQ) properties of VMQ-capable network adapters. VMQ is a scaling networking technology for switch that hashes incoming packets based on the destination MAC address.

    - Checkpoints in Grid – In the grid view of management pane the checkpoints on a given VM are shown.
    - Turn Off Warning – When VM is turned off, a warning about taking this action will now be shown.
    - Custom Column Saving – If users make changes to the grids in CM, these custom changes are saved now.
    - Settings Button on RDP Screen – Added a Settings button on the RDP screen for quick access to VM settings.
- Backup –
    - No VSS Backup – Optional ability to bypass VSS for OS Windows 2016 when running backups.
    - Backup Failure Notifications – New alerts and notifications on backup progress, success and failures. Includes email alert options.
- Installer – Links to Evolve – Links to evolve are now added to the installer, quick access to help.
- Licensing – TCP port 8443 added for easier registrations in closed and NAT environments.
- SDN –
    - VLAN and VXLAN networks management – Create and manage Datacenter networks or isolated Tenant networks.
    - Datacenter Firewall (ACL rules) – Create and manage access rules for North-South and East-West traffic in Datacenter or Tenant networks.
    - Load balancing in VXLAN and VLAN networks – Create and manage load balancers for Datacenter networks or isolated Tenant network.
    - Reduce cost of implementing LB features, replace NLB.
    - Backup / Restore – Backup and Restore SDN settings.

Version 3.1

- Initial Windows Server 2019 Support
- Multiple migrate operations – select multiple virtual machines at once for live migration
- Extended live migration settings – set the max number of simultaneous live migrations and storage migrations
- Run optimizer on demand – Option to run optimizer on demand, even out the load over the cluster (manual optimization)
- Built in failover cluster load balancing – If the host is running Windows 2016, give the option to enable or disable built-in failover clustering load balancing to avoid issues with the dynamic optimizer
- VM replication into Azure
- Syslog integration – ability to export log files
- Reporting – Introduction of the new plugin for VM lifecycle management – reporting of the various resources high/low utilization by virtual machines during last 30 days period and ability to export it in different output formats (PDF, PNG, XLSX)

Version 3.0

- Azure Management – 5nine Cloud Manager 3.0 introduces the new plugin designed to control Microsoft Azure subscriptions from its GUI. Basic operations with Azure virtual machines are currently available – create, edit, delete etc. Import VM from Hyper-V to Azure action is also implemented. Please refer to “Azure Management” section below for details.
- Active Directory Enhancements
- Upgrade Agent Management
  - Upgrading remote agents deployed in different networks/domains
- Backup Wizard Enhancements
- Log file Enhancements

Version 2.2

- Messaging Broker service update – Multi-protocol open source messaging broker and Erlang components are upgraded the latest 3.7.4 version
- UX/UI Improvements
  - Unite resource-based and event-based monitoring alert settings
    Resource-based and event-based monitoring alerts are united in a single wizard
  - Management Service Upgrade
    All previous settings are shown including passwords.
  - Add Descriptions to All Wizards
    Where necessary detailed descriptions of the objects were added: category, credentials, etc.
  - Hide logical view for users
    Only Cloud Manager administrators can view logical the view tab in the object tree.
- Backup Wizard Enhancements
  - Ability to create backup job for a group of objects.
  - Users are not allowed to edit backup jobs that were created by administrators.
  - Backup wizard texts are reworded and validated.
- Active Directory Enhancements
  - User/group AD browse dialog
    When adding Windows user credentials, a username does not have to be entered manually. AD browse dialog is used instead.
  - Ability to create a user group mapped to AD
    New type of user group is introduced: domain user group. Domain user group automatically synchronizes its users with the corresponding AD group. You can set permissions for the group and as soon as a user is added to the AD group they start having corresponding permissions in Cloud Manager
- SDN deployment – Basic Virtual Network Controller Support: a user can enter major SDN parameters and then special deployment scripts run deploying SDN infrastructure. Improvements include:

- Create, Read, Update and Delete operations are implemented for the following SDN objects: Logical networks, Virtual networks, Network interfaces, Virtual Switches, Servers, NC Credentials.
- Read operation is implemented for the following SDN objects: Load balancers, MAC Address Pools.

Introduction

Summary

Acronis Cloud Manager is a solution designed to help organizations efficiently manage Microsoft Hyper-V and Azure private and hybrid clouds. It provides multi-tenancy and role-based access control providing fine-grained control over virtualization hosts, networking and other resources to create and deploy Hyper-V and Azure virtual machines. The product has the following features:

- Easy-to-use and intuitive design for new or experienced Hyper-V admins.
- Hyper-V management in different Windows Server versions – 2022 / 2019 / 2016 / 2012 R2 - from a single console.
- Microsoft Azure subscriptions management from a local console.
- Centralized monitoring for Hyper-V hosts and all virtualized resources.
- Consolidated data of resources utilization by virtual machines for the last month (reporting).
- Software defined network management and deployment.
- Backup and DR capabilities for virtual machines.

System architecture

Acronis Cloud Manager is a modular solution that lets you build a scalable infrastructure for environments of different sizes and configuration. The installation package of Acronis Cloud Manager includes a set of components:

- Management server – Windows service that coordinates all operations performed by Acronis Cloud Manager.
- Management database – is used by the management server to store data about the Hyper-V infrastructure, jobs, users and so on. The database instance can be located on a SQL Server installed either locally (on the same machine where the management server is running) or remotely.
- Management console – provides the application user interface and allows user access to all features.
- Host agent – responsible for performing all commands from management server on a Hyper-V host. This component must be installed on every Hyper-V server managed by Acronis Cloud Manager.
- Multi-protocol open source messaging broker (59MgmtSvcRmq) –open source message broker software that implements the advanced message queuing protocol (AMQP). The 59MgmtSvcRmq service is written in the Erlang programming language and is built on the open telecom platform framework for clustering and failover.

You can co-install all components on the same machine, physical or virtual, or you can set them up separately for a more scalable approach. Advanced message queuing protocol (AMQP) is used as a message-oriented middleware for the communication between the management server and the host agents. HTTPS protocol is used for the communication between the console and the management server.

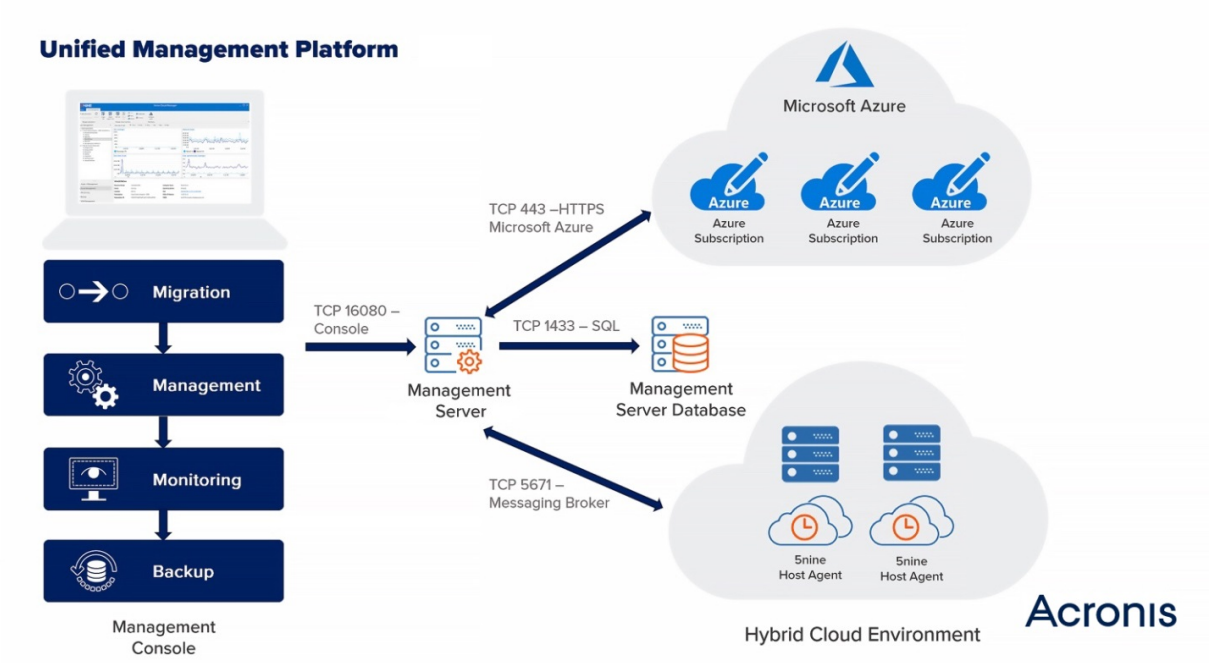


Figure 1 - Acronis Cloud Manager architecture

Plugins

Cloud Manager consists of the following plugins:

- Hyper-V Management
- Azure Management
- Hyper-V Monitoring
- Hyper-V Reporting
- Hyper-V Backup and DR
- Software defined network (SDN) Management
- Administration
- Usage

Deployment and configuration

System requirements

Acronis Cloud Manager server

Component	Requirement
Hardware	CPU: modern x64 processor 4 cores minimum Memory: 8 GB RAM minimum, 16 GB RAM recommended Hard disk space: 300 MB for product installation and sufficient disk space for Microsoft SQL Server and Acronis Cloud Manager database
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 10 • Microsoft Windows 8.1 • Microsoft Windows Server 2012 R2
Software	• Microsoft .NET framework 4.6.2 or later • Microsoft Visual C++ 2015 redistributable update 3
Database	Microsoft SQL Server (Full and Express): • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 (SP1) • Microsoft SQL Server 2014 (SP2) For production deployment of Acronis Cloud Manager server, it is recommended to use Microsoft SQL Server Standard Edition or higher.
Ports	5671 for messaging broker communication – can be changed during setup 16080 for communication to management console
Internet	Internet connection is necessary for the license activation/validation to the following URL/port: https://api2.5nine.com/api/validate, port 443

Acronis Cloud Manager console

Component	Requirement
Hardware	CPU: modern x64 processor 2 cores minimum. Memory: 2 GB RAM recommended. Hard disk space: 200 MB for product installation
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 10 • Microsoft Windows 8.1 • Microsoft Windows Server 2012 R2
Software	• Microsoft .NET framework 4.6.2 or later • Microsoft Visual C++ 2015 redistributable update 3
Ports	16080 – communication to management server 443 – communication to Microsoft Azure

Acronis Cloud Manager host agent

Component	Requirement
Hardware	CPU: modern x64 processor 4 cores minimum Memory: 8 GB RAM minimum, 16 GB RAM recommended Hard disk space: 300 MB for product installation
OS	Only 64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows 10 • Microsoft Windows 8.1 • Microsoft Windows Server 2012 R2
Software	• Microsoft .NET framework 4.6.2 or later • Microsoft Visual C++ 2015 redistributable update 3
Ports	5671 for messaging broker communication – can be changed during setup

Acronis Cloud Manager web portal

Component	Requirement
Hardware	Hyper-V virtual machine: CPU: modern x64 processor 4 cores minimum Memory: 8 GB RAM minimum VHD: 2 GB
OS	Ubuntu 20.04[1]
Software	Acronis Cloud Manager web portal components (pre-installed)
Ports	443

Licensing

Acronis Cloud Manager has two separate types of licenses – general one for Hyper-V management, including all its features and the license for Azure management.

Hyper-V management part is licensed per-core. Minimal license set for a Hyper-V host is 16 cores.

Azure management part is licensed per VM. Initially, a free license is installed by default, which includes quota for a maximum number of 5 virtual machines from the cloud. Azure license is installed and works separately on a global level and for each tenant. Default 5 VM licenses are only available to global users.

Acronis offers the following types of licenses for Acronis Cloud Manager:

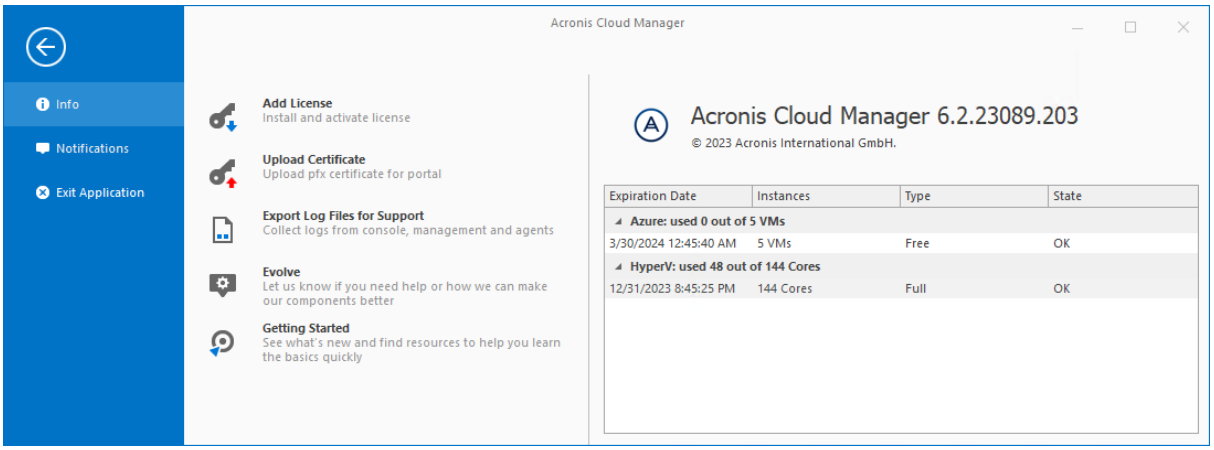
“Paid subscription license” –a full license that expires at the end of the subscription term. The subscription license term is normally 1-3 years from the date of license issue.

“Trial license” – a full license that can be used for product evaluation. The trial license is valid for 14 days from the moment of product download and contains 100 core limit.

“NFR license” – a full license that can be used for product demonstration, training and education. The person to whom the license is provided agrees that the license is not for resell or commercial use.

Information about licenses is available in the **Home** tab, available in every plugin.

[1]OS Ubuntu 18.04 and Acronis Cloud Manager web portal components are pre-installed on the VHD delivered with the setup archive.



Installation

Acronis Cloud Manager installation package represented in two options:

- Separate bootstrap application - including Acronis Cloud Manager components and links to documentation and online virtual labs to test pre-configured product.
- Setup package in ISO format - including Acronis Cloud Manager components both in bootstrap application and separate Windows Installation Package (.msi) files and prerequisites – Microsoft SQL Express and .NET 4.6.2.

To install Acronis Cloud Manager, using bootstrap application, run the Setup.exe application from the downloaded Acronis Cloud Manager archive (or from ISO setup package):

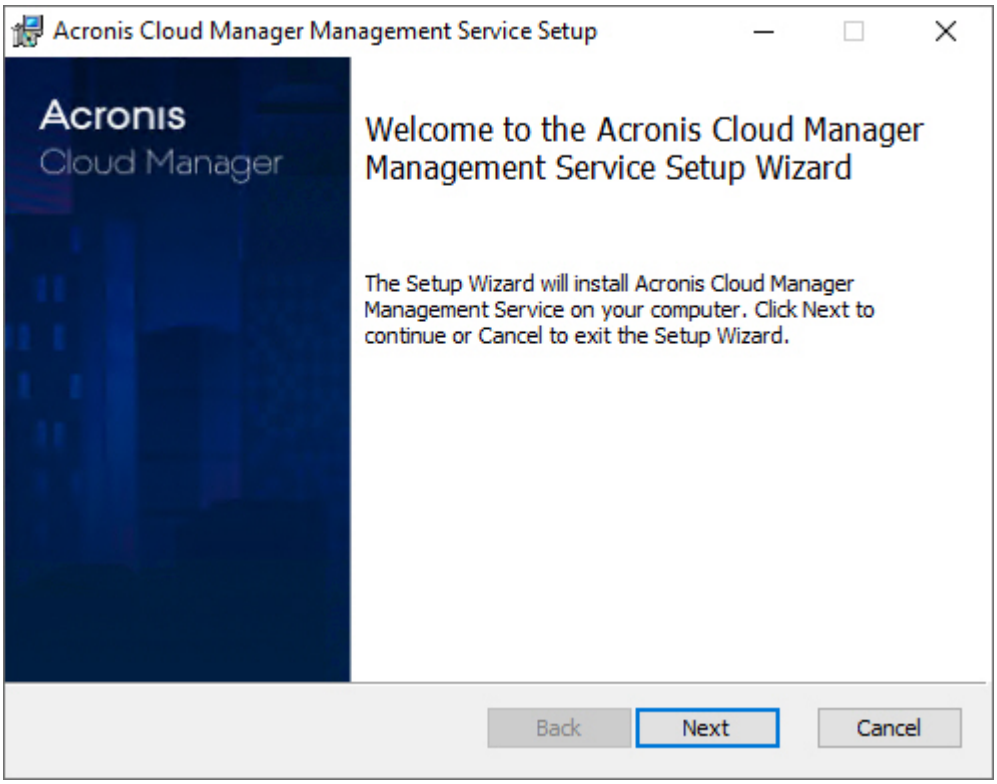
All 3 components can be installed from this bootstrap setup, but it must be run locally on each machine.

To install Acronis Cloud Manager from ISO, using either separate .msi files or similar bootstrap application, mount the Acronis Cloud Manager iso installation file and run the corresponding .msi file from its subfolders (Management, Console and Agent) or setup.exe bootstrap application.

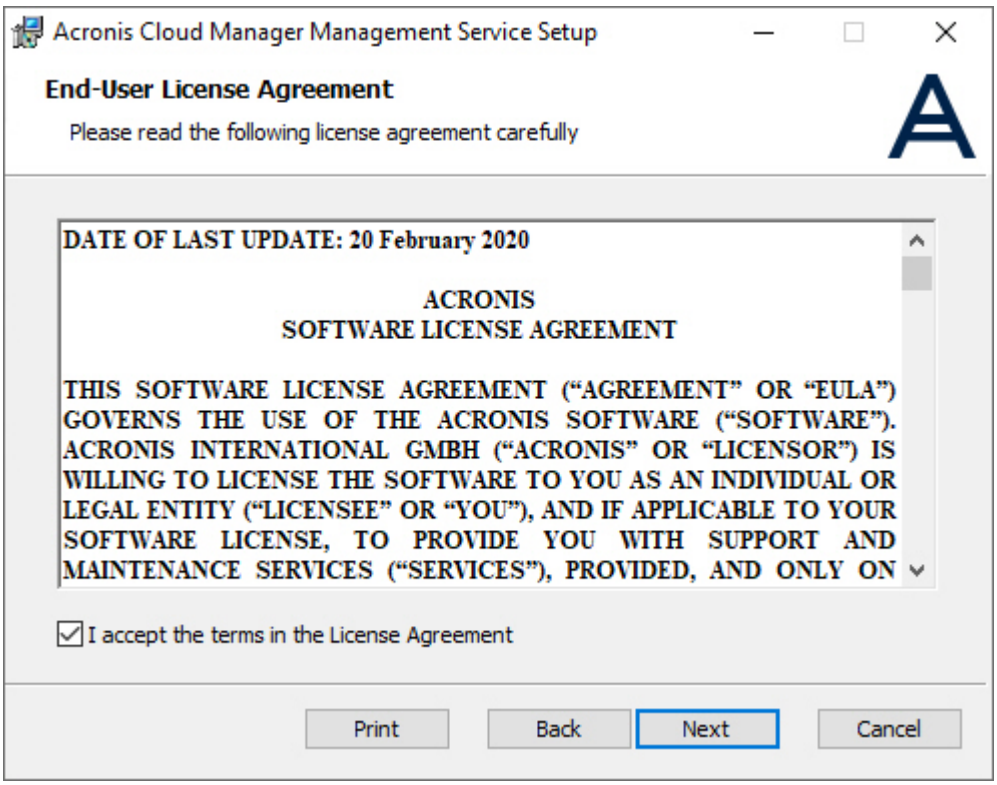
It is generally not necessary to install Host Agent component from bootstrap setup or a separate .msi file. It can be installed automatically from the Acronis Cloud Manager console when adding servers.

Management service setup

1. To run management service setup, select the first component in the bootstrap setup list and press the **Install** button or run **managementservice.setup.msi** from the **Management** setup ISO folder. The following window will be shown. Some steps will differ when installing this component from ISO. Press **Next**:

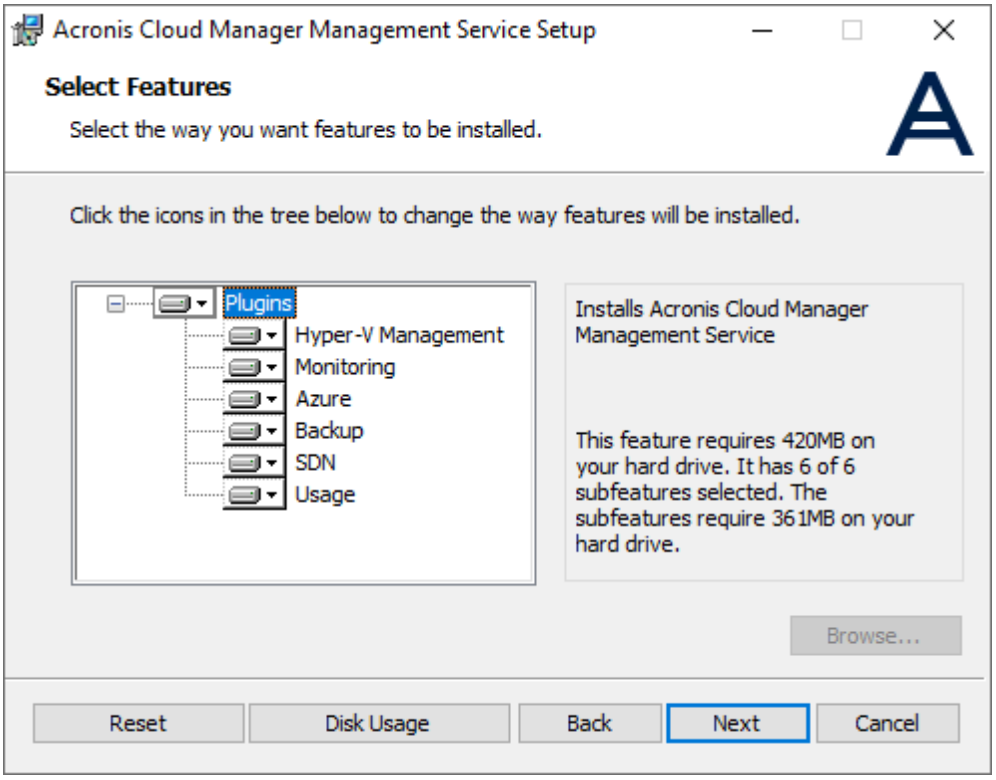


2. The Acronis software end user license agreement will appear.
   Read and accept it, then press **Next**:

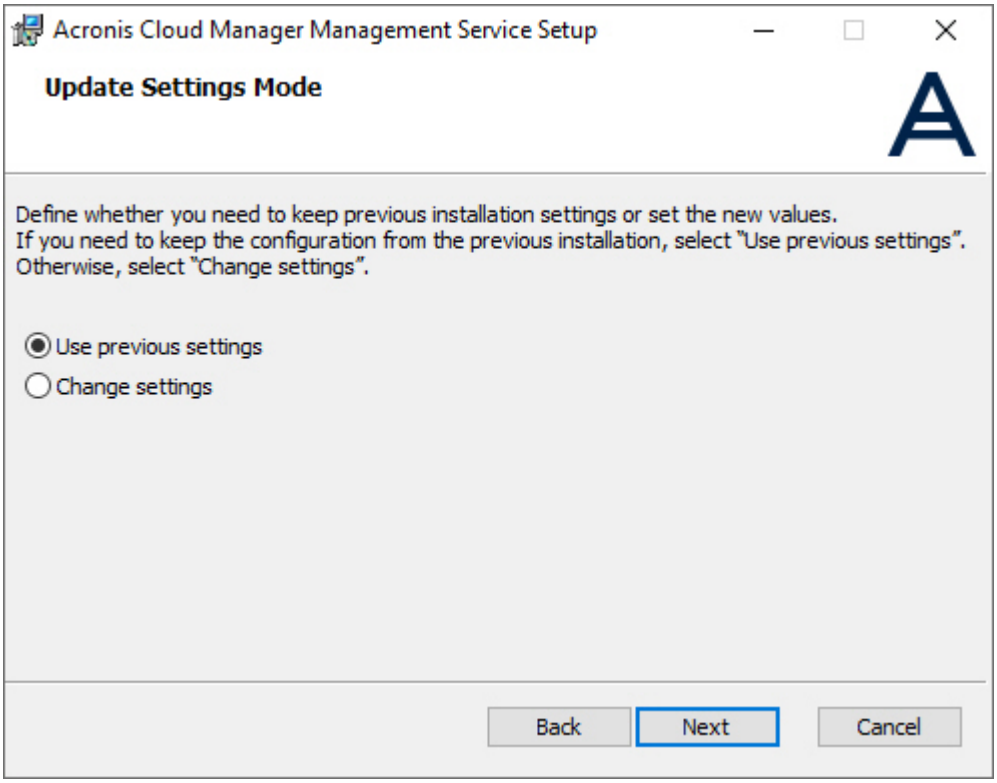


Note
When installing this component from ISO, the prerequisites check will be done in the background and the setup will install the corresponding missing Microsoft components in *silent* mode.

3. Select the plug-ins you want to use and press **Next**:



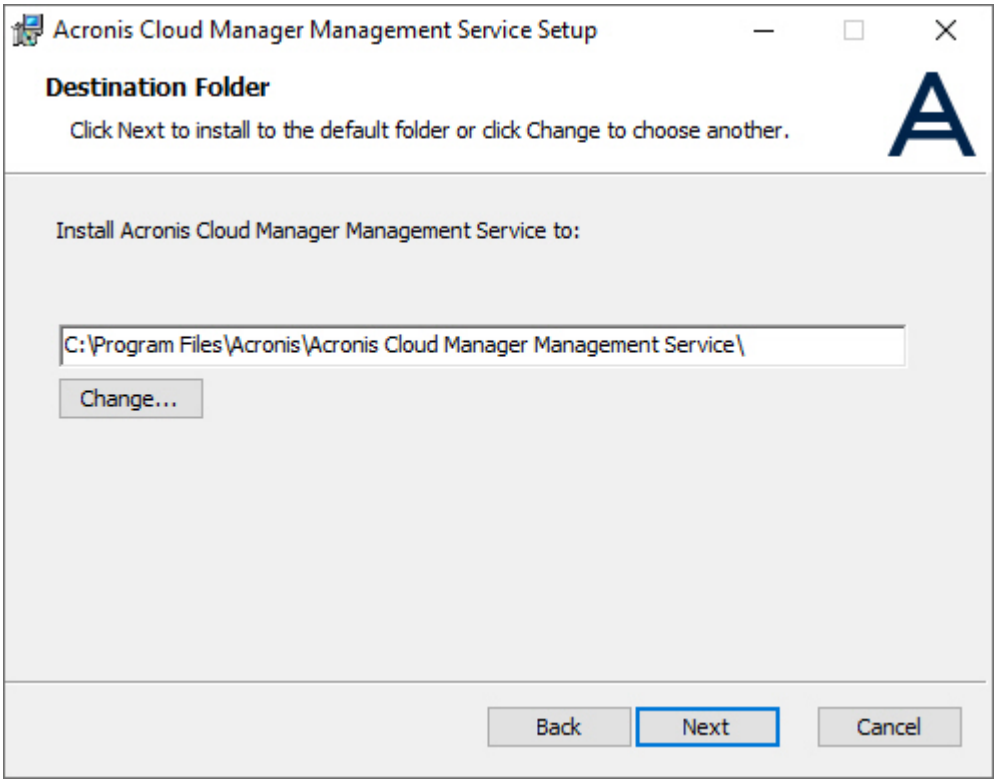
4. If you are performing an upgrade from a previous version, select the upgrade options:



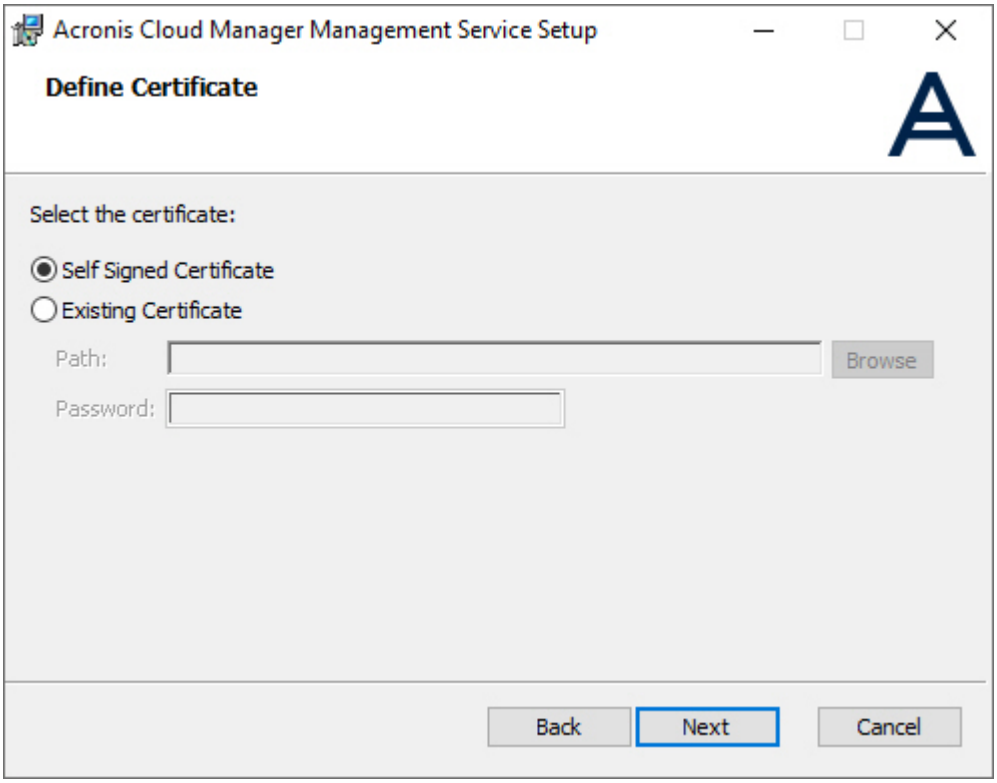
- **Use previous settings**: all installation existing settings will be kept, except asking you to confirm the service logon for the management service credentials (domain\user).

- **Change settings**: all credential settings can be changed without the need of uninstalling the management service

5. Select the destination folder for Acronis Cloud Manager management service and press **Next**:

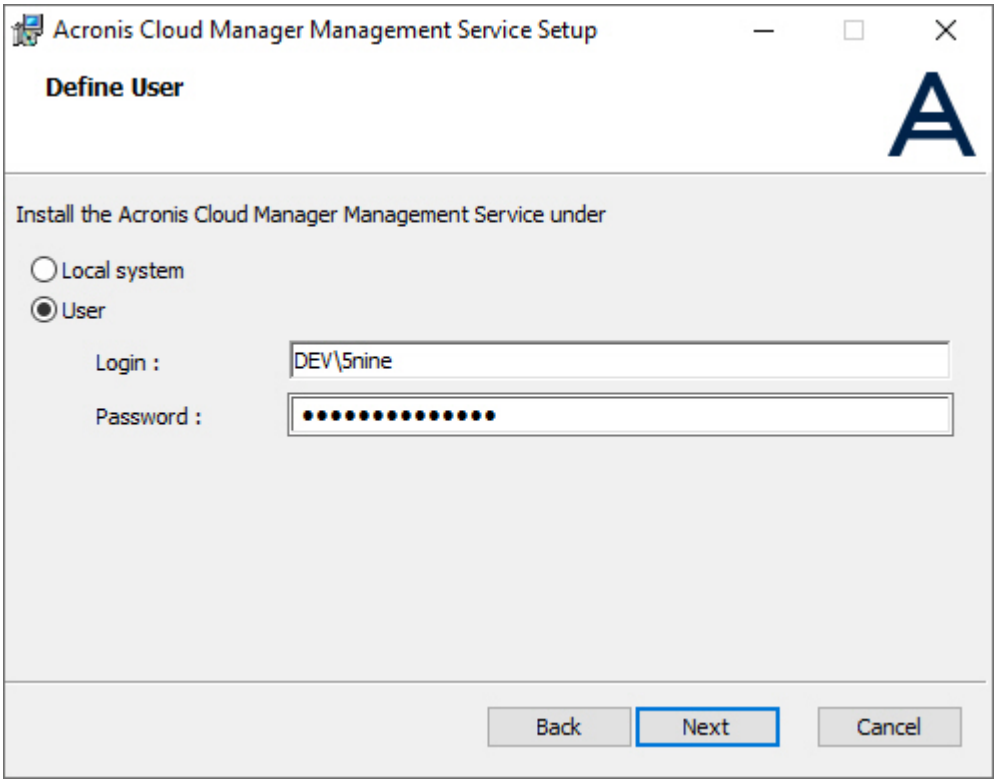


6. Select one of certificate configuration options:

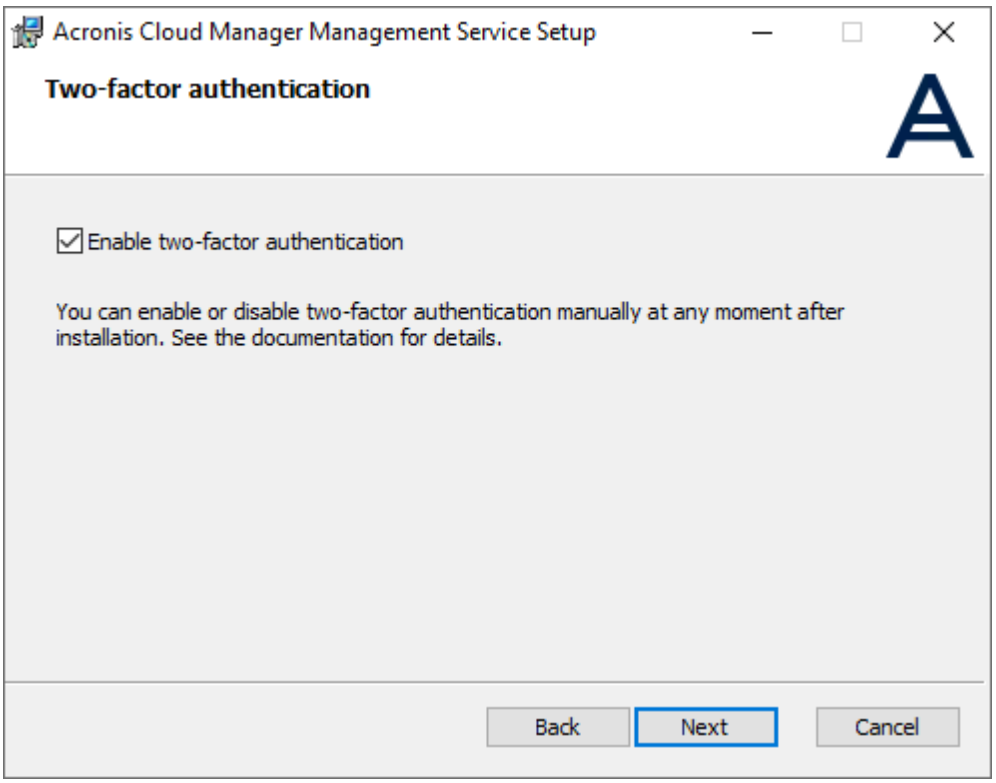


- **Self Signed Certificate** – Acronis Cloud Manager will automatically install self-signed certificate during management service setup;
- **Existing Certificate** – you will have to browse and select pre-configured existing certificate, then enter the password.

7. Provide user credentials for the user that will run management service and press **Next**:

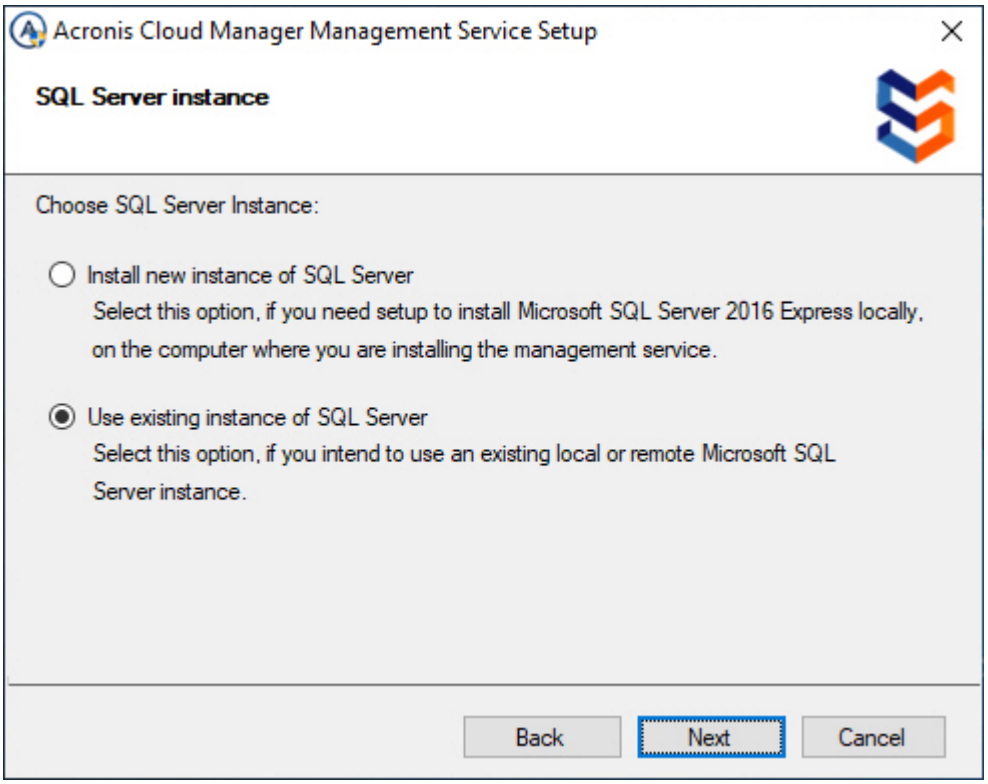


8. Enable the two-factor authentication if required and press **Next**:



You will be able to change this option after installation.

9. Applicable to ISO installer only: choose, which SQL server to use for database placement:

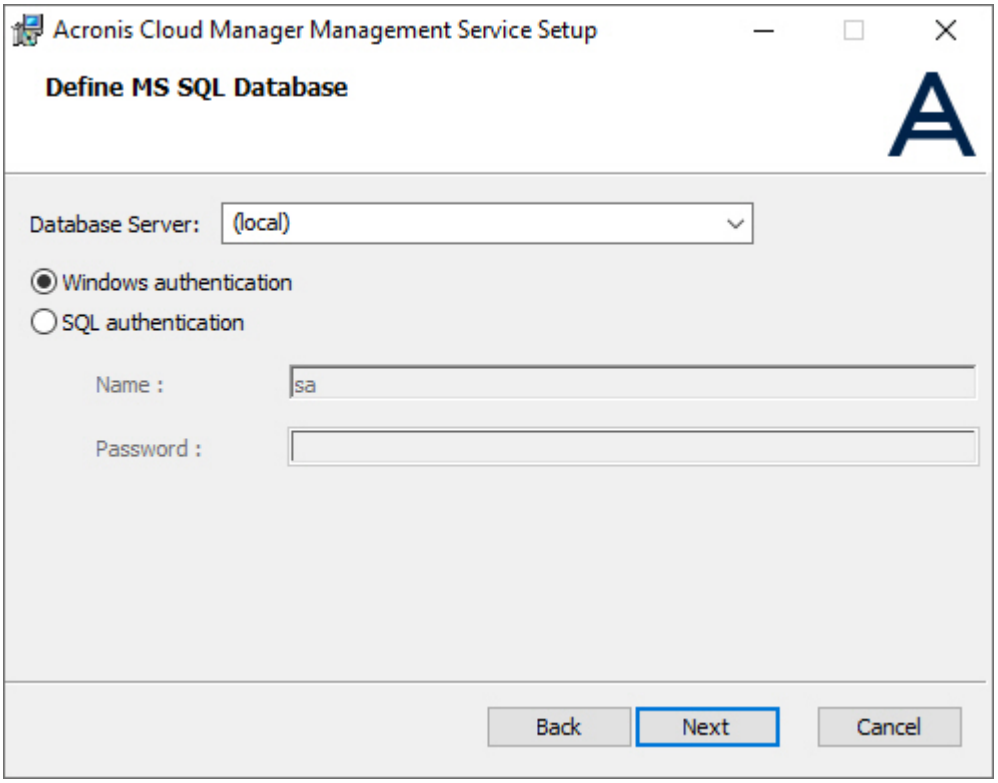


- **Install new instance of SQL Server** – setup will automatically initiate free Microsoft SQLEXPRESS® server installation onto the local machine. Make sure in advance that there is enough of free space on the local disk and all prerequisites for Microsoft SQLEXPRESS® server installation are met.
- **Use existing instance of SQL Server** – you will be asked to select any of existing MS SQL® or MS SQLEXPRESS® servers available in your environment at the following installation steps.

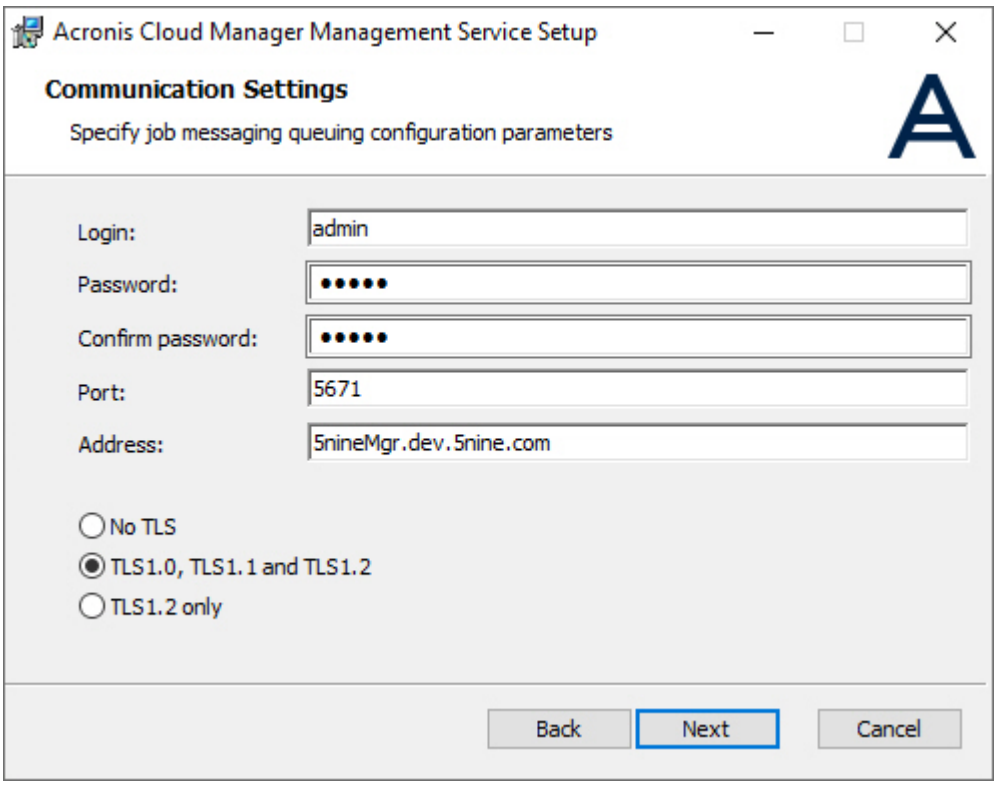
9. Select database server and set authentication method:

- **Windows Authentication** – can be selected if the user has been granted the necessary permissions on the selected SQL Server;
- **SQL Authentication** – use a specific SQL Server account (**sa** for example) and enter the relevant password.

Press **Next**:



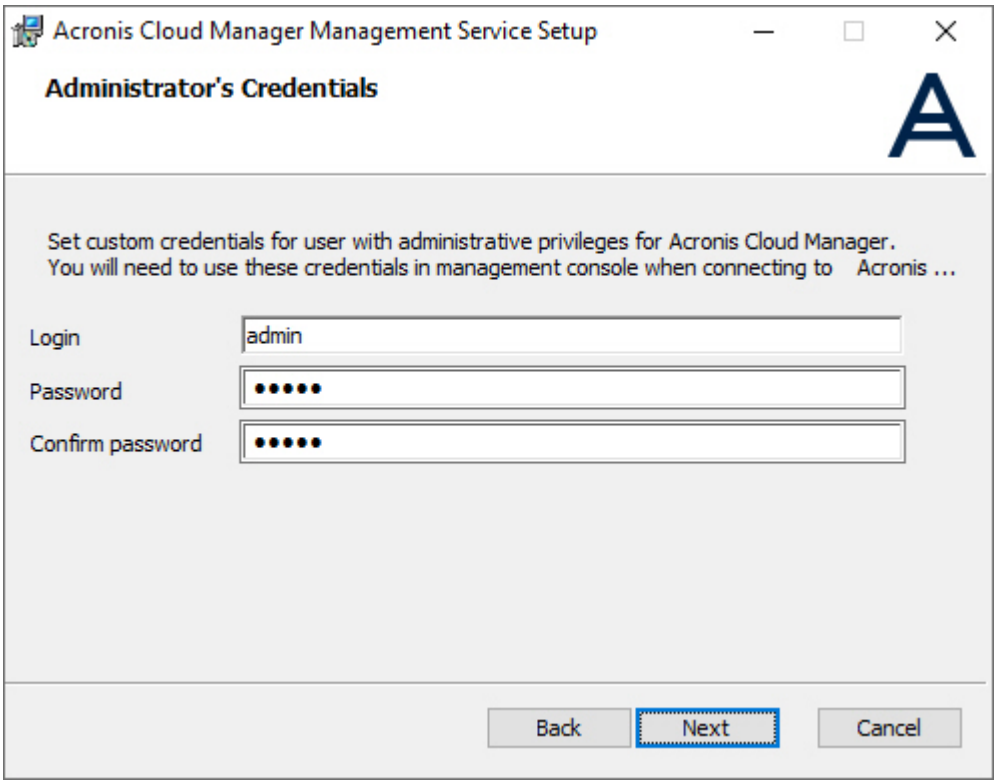
10. Specify job messaging queuing (broker) configuration parameters and TLS options, and then press **Next**:



TLS option depends on your environment's specific requirements. In most cases, the second (default) option that includes TLS 1.0, 1.1 and 1.2 compatibility is the proper choice.

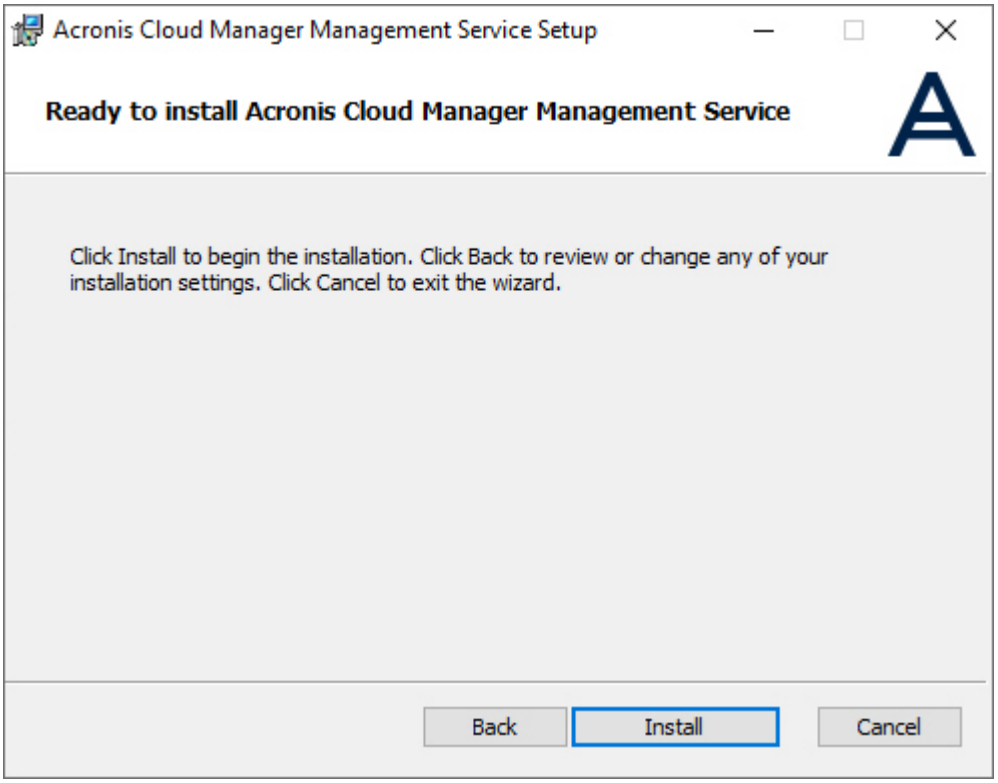
11. Provide master administrator's credentials to connect to management console without active directory login for example.

    The default username is **admin** for the first global administrator that you will need to use to login into the console for the first time. It is strongly recommended that alternate credentials are set for security.

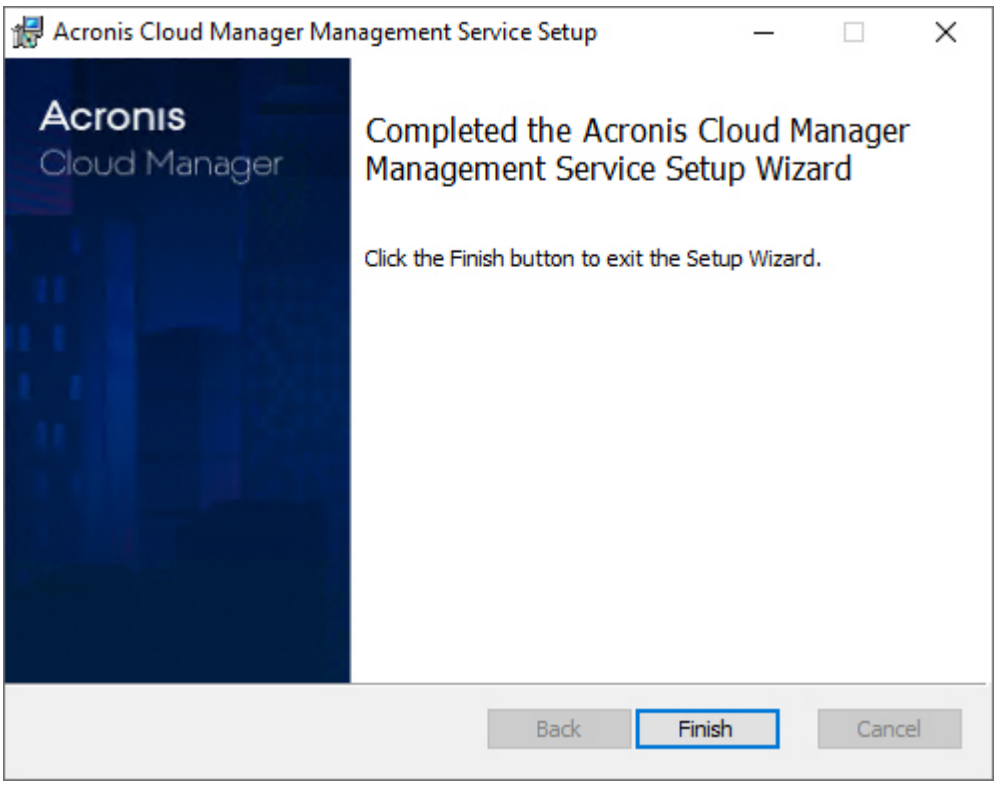


    Click **Next**.

12. Click **Install** to start installation:

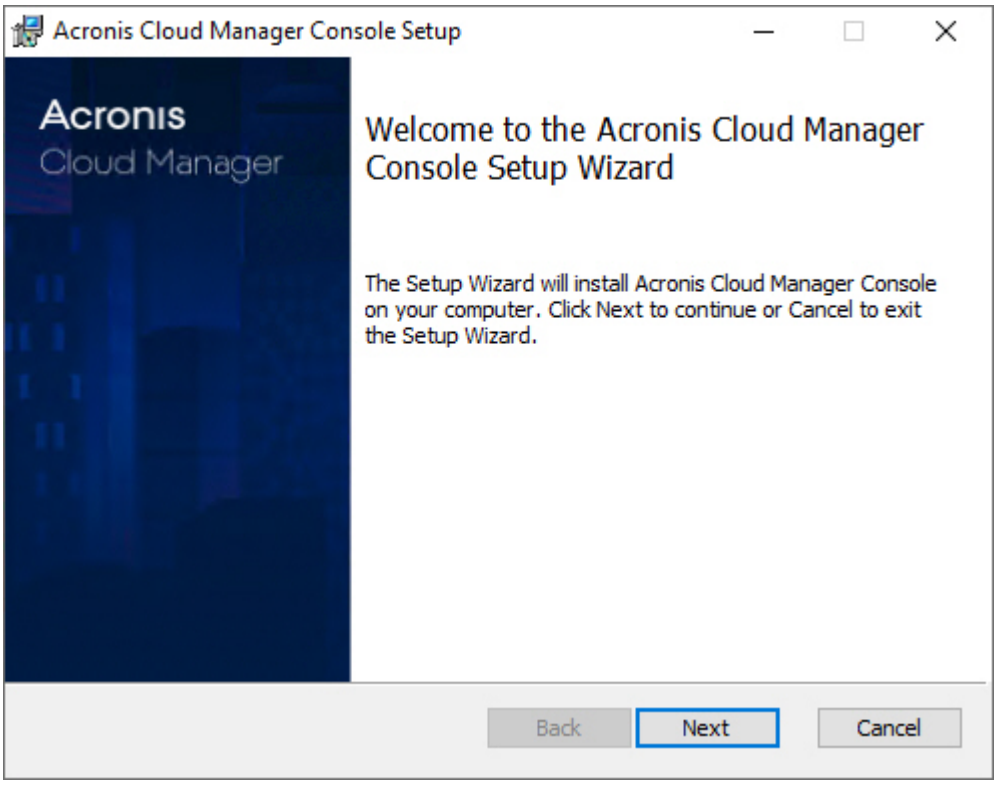


13. Click **Finish** when installation is complete:

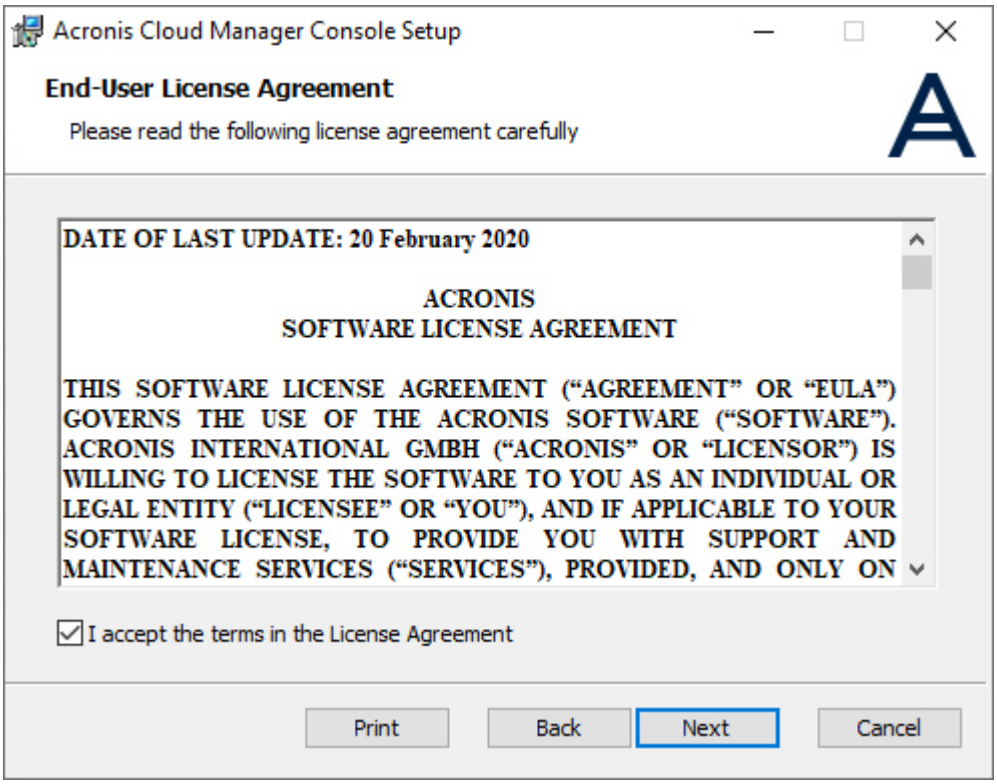


Console setup

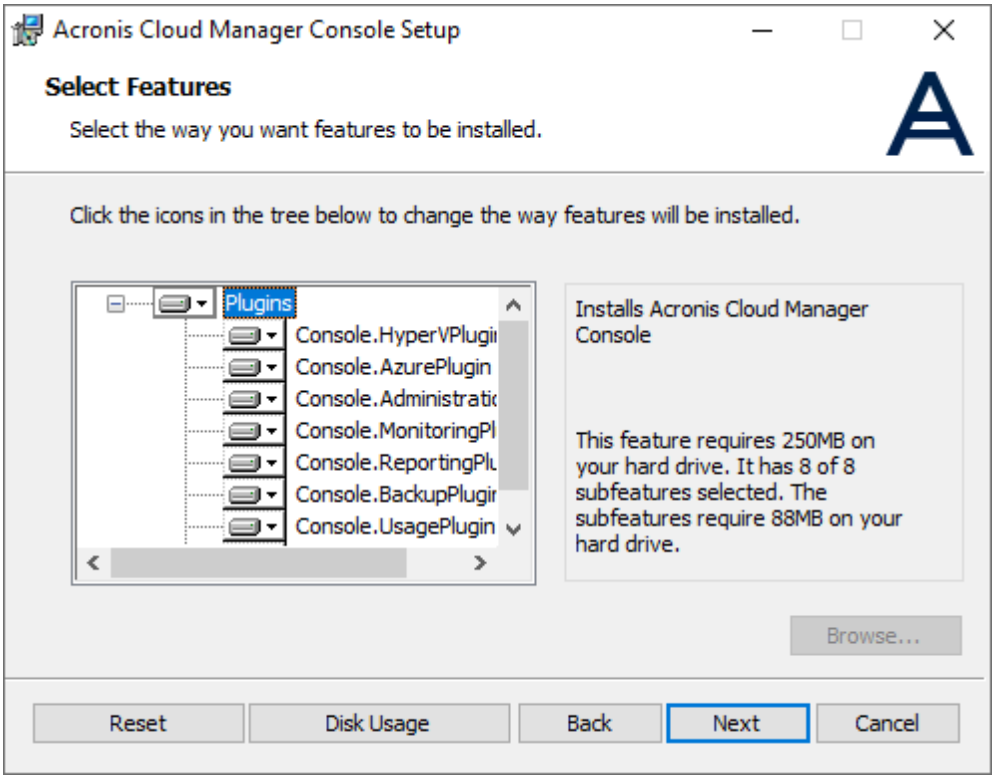
1. To run console setup, select the second component in the bootstrap setup list and press the **Install** button or run **console.setup.msi** from the **Console** setup ISO folder. The following window will be shown. Click **Next**:



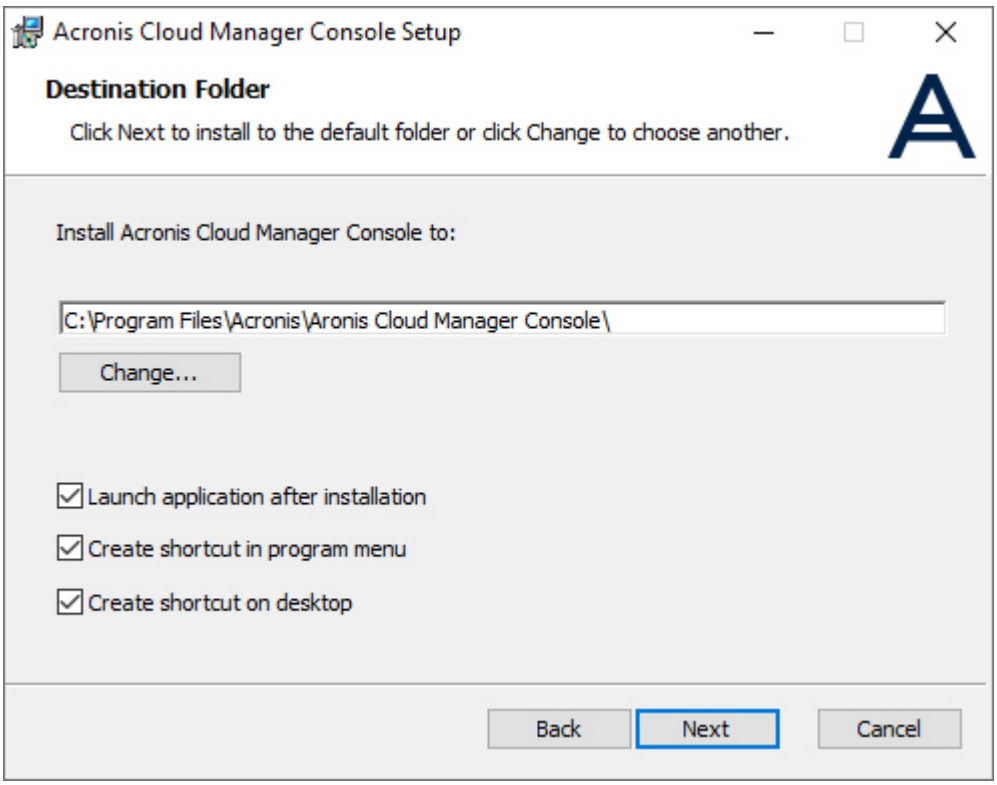
2. The Acronis software end user license agreement will appear.
   Read and accept it, then press **Next**:



3. Select the plugins you want to use and press **Next**:



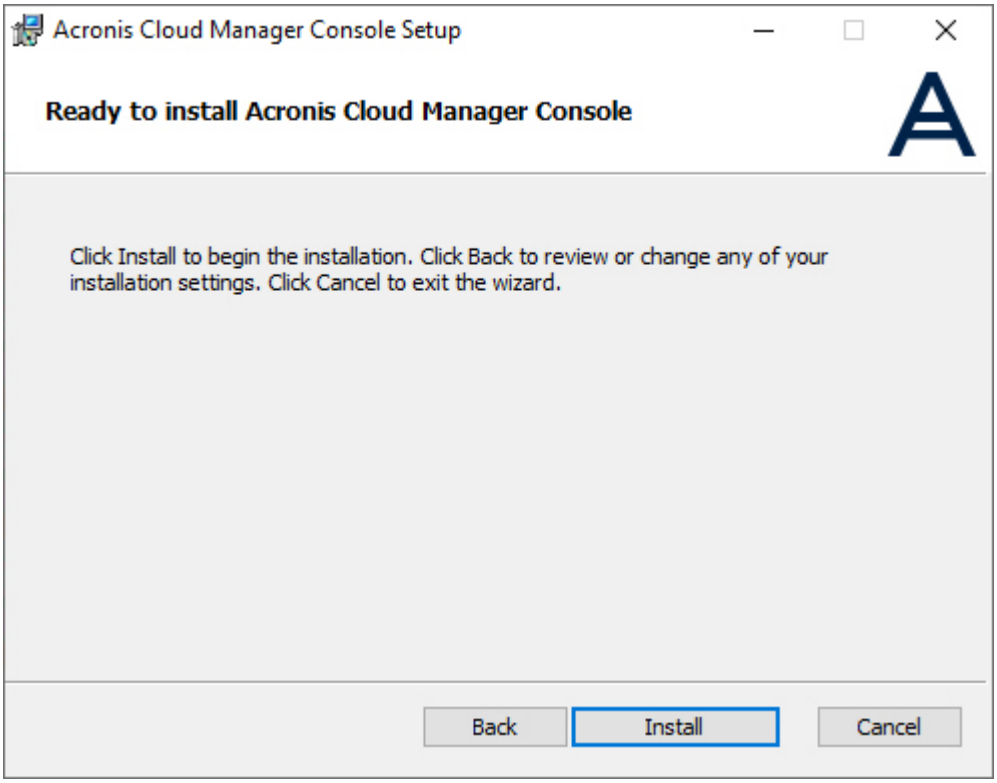
4. Select the destination folder for Acronis Cloud Manager and set the following program options (select or deselect depending on your preferences):



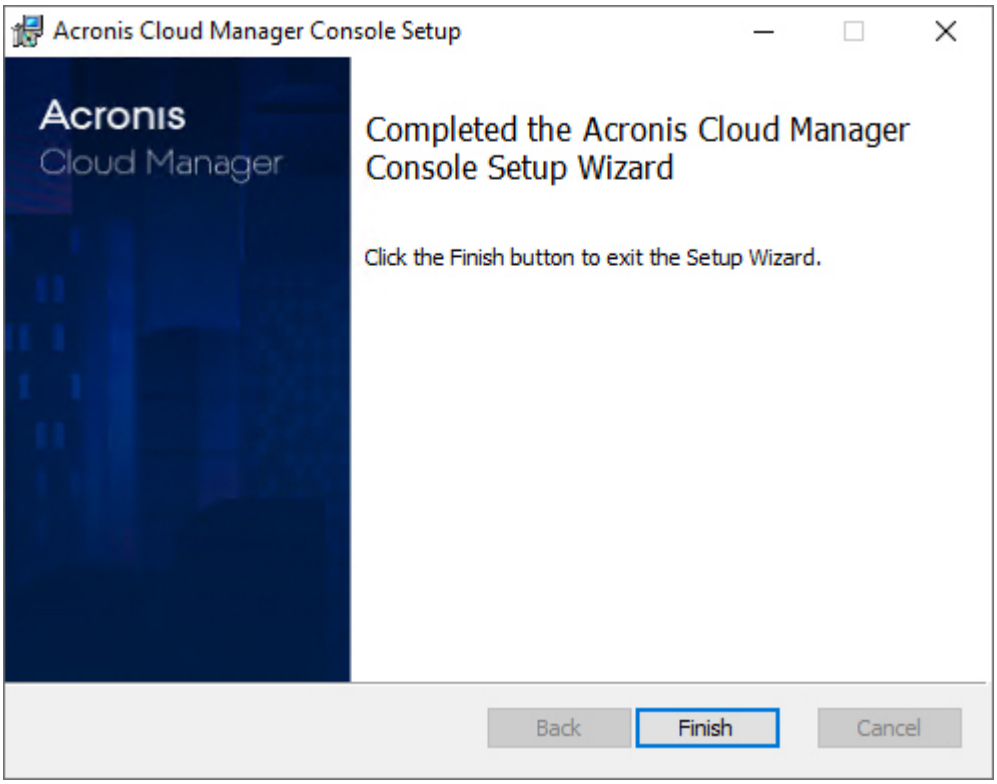
- **Launch application after installation**;
- **Create shortcut in program menu**;
- **Create shortcut on desktop**.

  Press **Next**.

5. Click the **Install** button to install the management console:



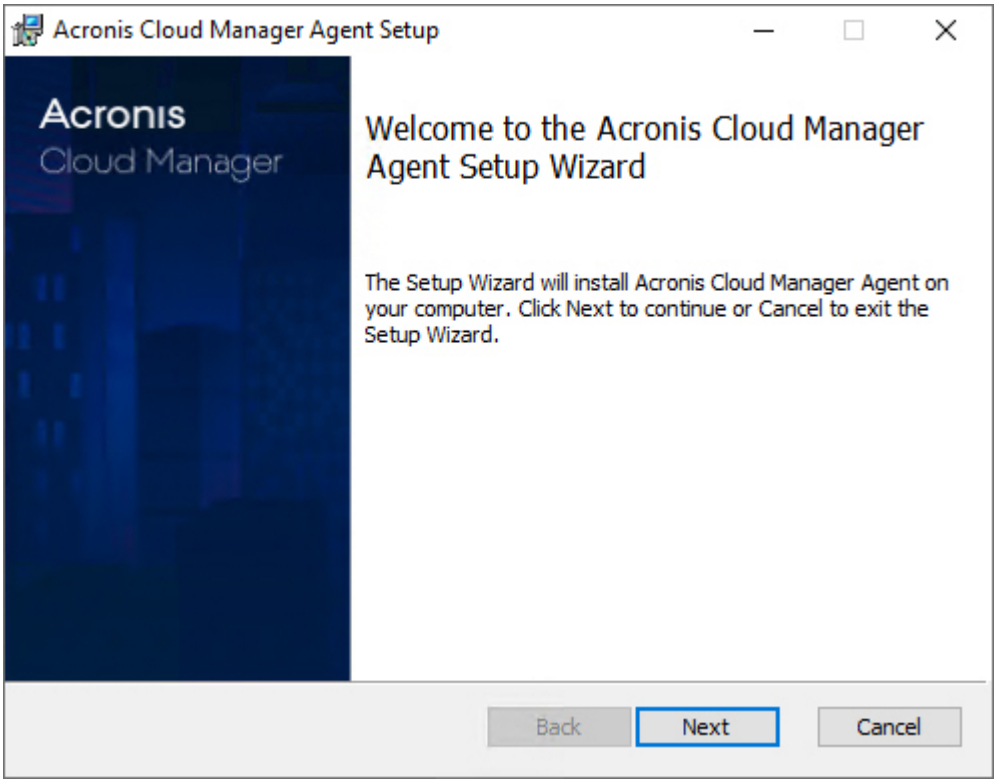
6. Click **Finish** when installation is complete:



Host agent setup

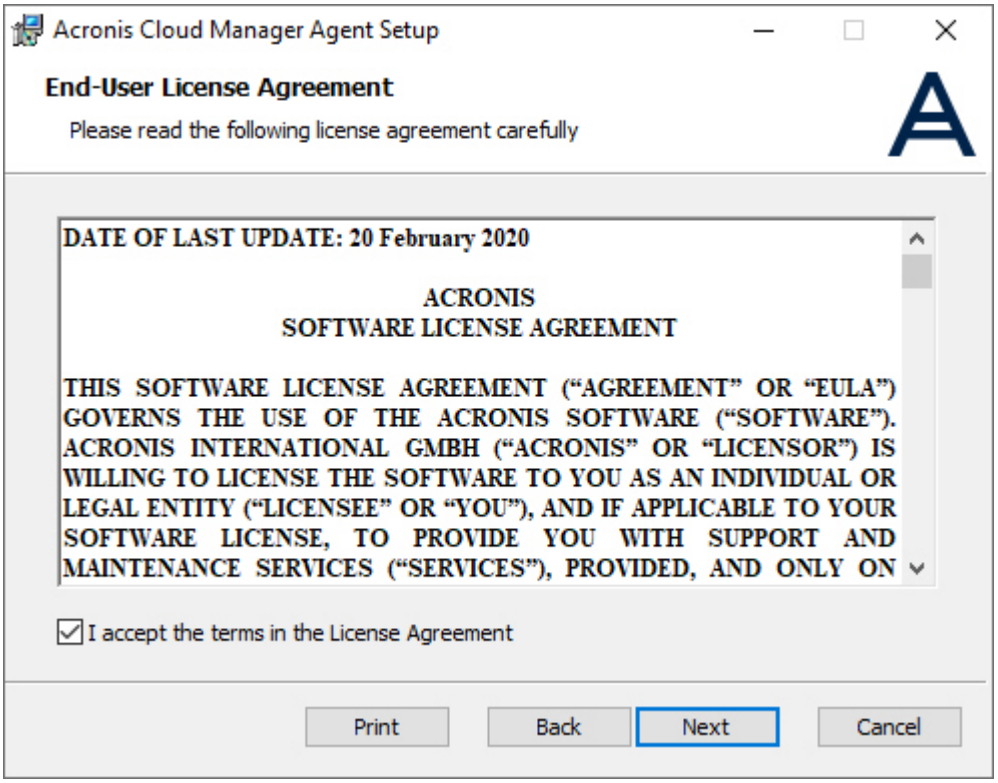
The host agent is installed automatically on a Hyper-V server when it is added to the objects tree in the management console. If there are any specific conditions or issues, you can also install it manually by selecting the third option in Acronis Cloud Manager bootstrap setup or running **agentservice.setup.msi** from the **Agent** setup ISO folder.

1. The following window will be shown. Press **Next**:

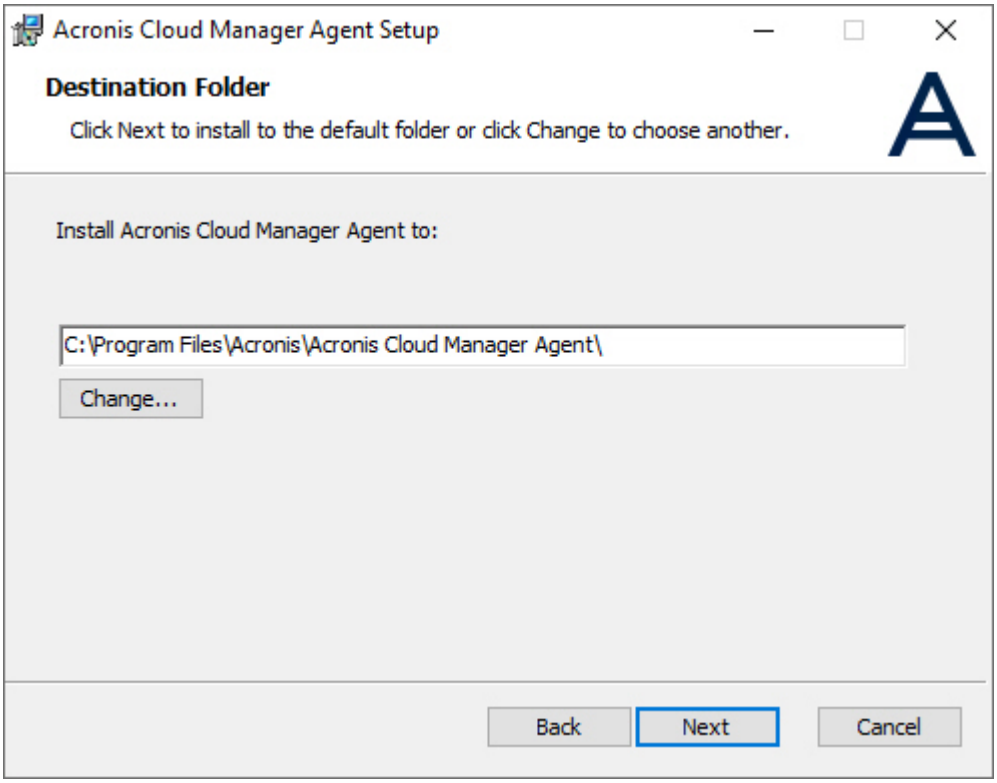


2. The Acronis software end user license agreement will appear.

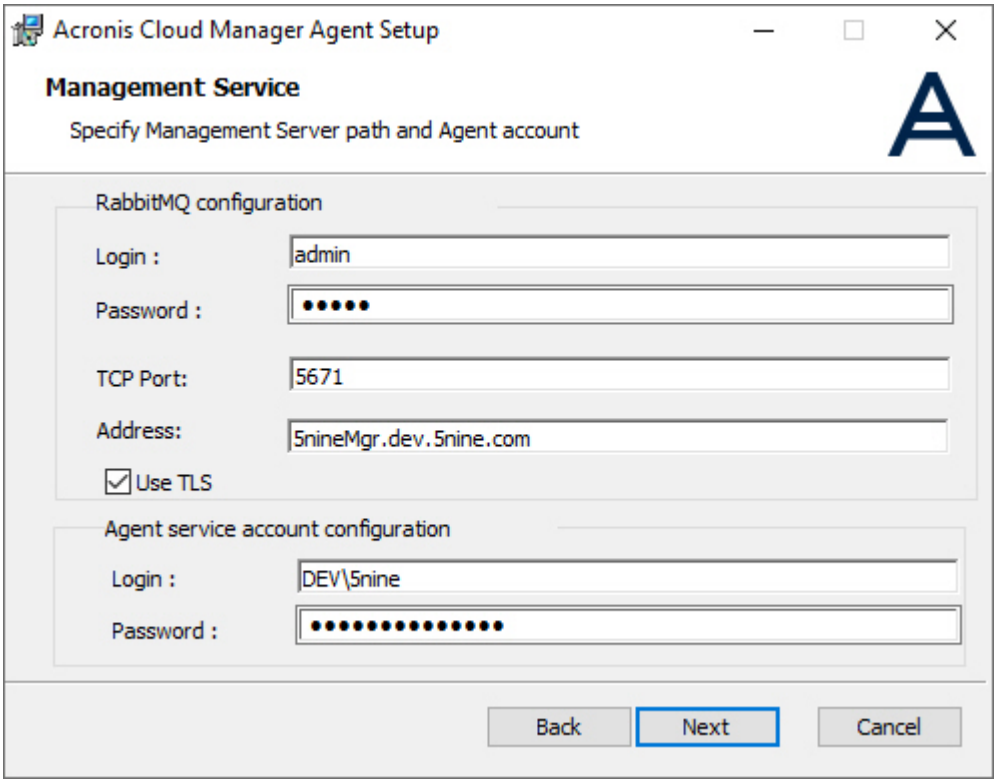
Read and accept it, then press **Next**:



3. Select the destination folder for Acronis Cloud Manager agent and press **Next**:



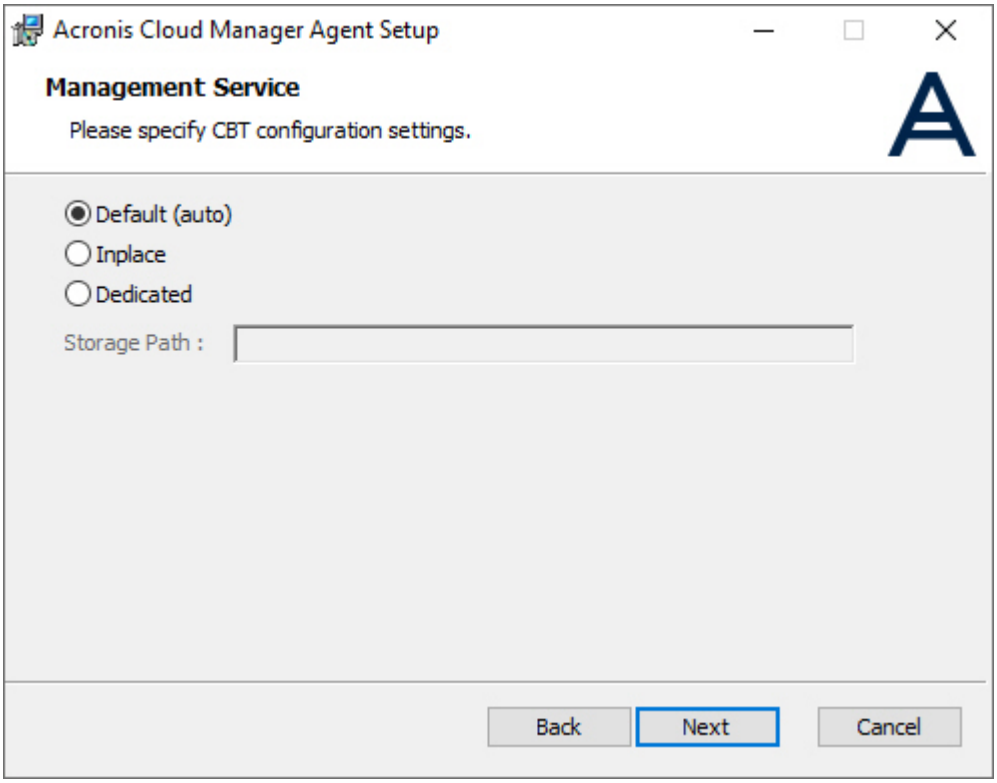
4. Set the management server and messaging queuing broker connection parameters, specify agent service account, enable TLS option (if applicable):



Note

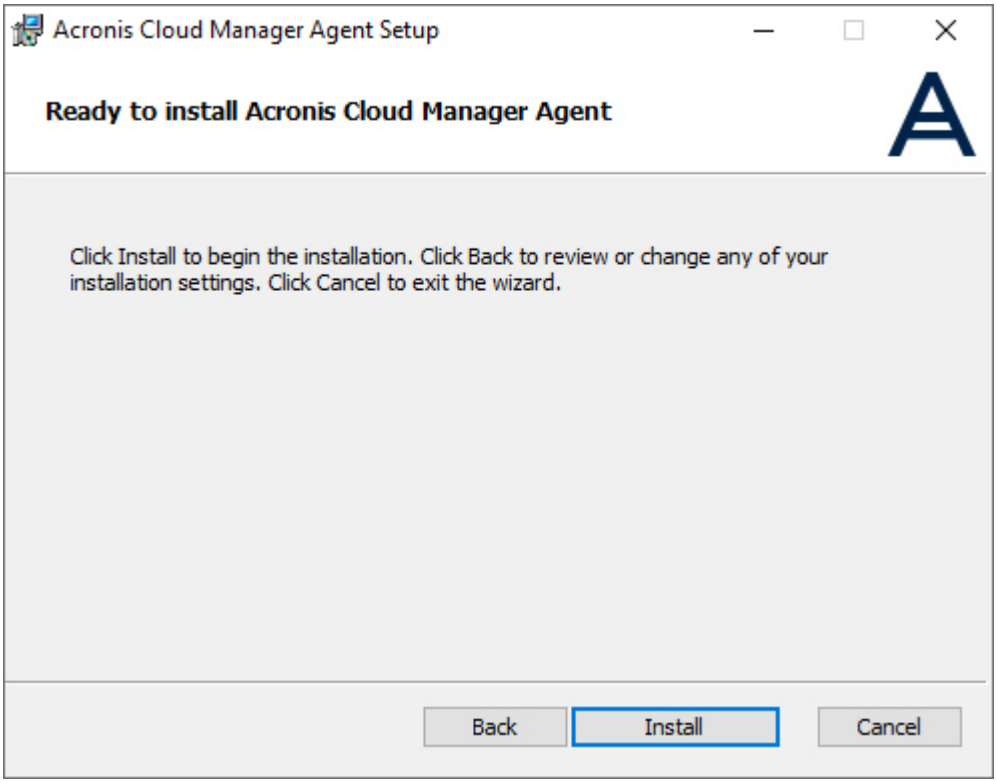
You will have to provide the same messaging broker configuration parameters that were used in management service setup. Specifically, this applies to the address of the messaging broker – it must be entered exactly in the same way as it had been specified during management service setup, including letter case as this parameter is case-sensitive! Otherwise the communication between agent and management service will not work. Then specify credentials to start agent service under and press **OK**.

5. Set CBT options:

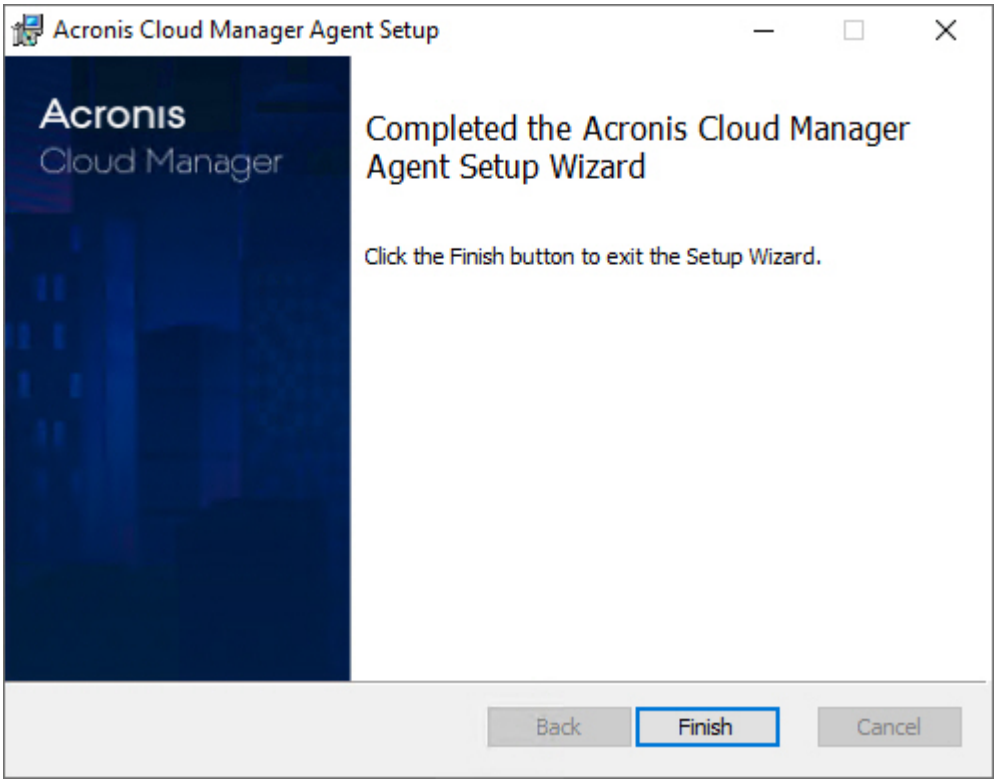


- **Default (auto)**: CBT data will be stored in the program-defined default location (**C:\Program Files\5nine\5nine CBT**);
- **Inplace**: CBT data will be stored together with virtual machine VHD;
- **Dedicated**: CBT data will be stored in the location, specified by user (**Storage Path**). The location should be available from the Hyper-V server's side.

6. Click **Install** to start installation:



7. Click **Finish** when installation is complete:



Moving management service to another server

To move management service to another server:

- Uninstall management service from the existing server (please refer to the "Uninstalling Acronis Cloud Manager" (p. 293) chapter below).
- Copy licenses from the old server to the new one - copy the whole folder C:\ProgramData\5nine\Licensing and place it with all its content onto the new server with exactly the same path. Then delete this folder with all its content from the old server.
- Open Windows registry on the old server and export the key HKEY_LOCAL_MACHINE\SOFTWARE\5nine\5nine Manager Datacenter by standard Windows means. Then merge it onto the new server.

Note
Ensure all values in the key are merged into the Windows registry on the new server. If it does not happen, then either enter them manually, or reconfigure Hyper-V host(s) credentials and Microsoft Azure subscription secret key (if applicable), using management console user interface.

- Install management service onto the new server. Use the existing database and your own .pfx certificate for management service (if applicable).
- Stop services: *5nine.Management.Service*, *59MgmtSvcRmq*.
- Copy the following files from the old server to the new one, using the same path - C:\ProgramData\5nine\5nine Manager Datacenter, rewriting existing ones:
  - 5nine_cert.pem
  - 5nine_cert_priv_key.pem
  - 5nine_root_cert.cer
  - 5nine_root_cert.pem
  - PortalSetings.prop
- Start services: *5nine.Management.Service*, *59MgmtSvcRmq*.
- It is recommended that FQDN/IP address for the new server are kept the same as they were used for the old one. If either of them is altered, then depending on which parameter is used for messaging broker (Rabbit MQ) and web portal connection, you will have to reconfigure those connections.

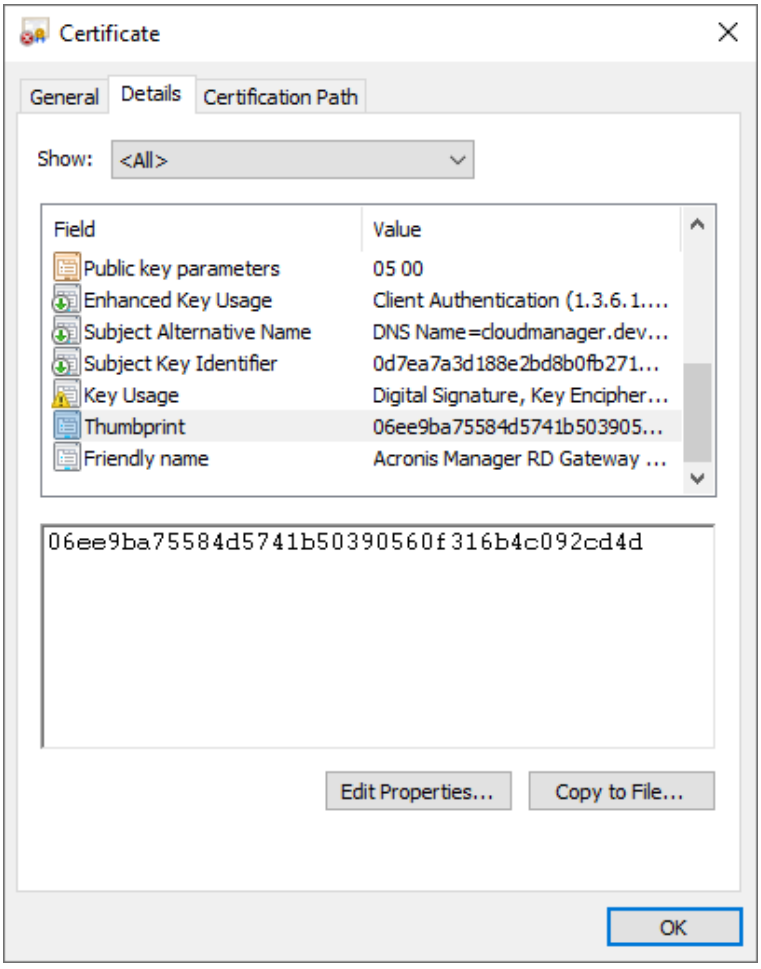
  For web portal please refer to the "Web management console installation" (p. 275) section below - you will have to re-pass through the initial script and enter the new IP/FQDN at the corresponding step of the script.

For host agents you will have to stop agents on hosts (*5nine.Agent.Service*) and edit the configuration file C:\Program Files\5nine\5nine Manager Datacenter Agent\5nine.Agent.exe.config:
<appSettings>
<add key="RabbitAddress" value="*myserver.address*" />
....
</appSettings>
Replace *myserver.address* with your actual data. Then save the configuration file and start agents. Another option is removing and reinstalling host agents from scratch, whichever is more convenient for your case.

Updating management service certificate

The certificate for management service is initially installed during the program setup. If you need to update it at some point afterward, there is the procedure to make it. To update management service certificate:

- Delete the previous certificate by executing this cmdlet:
  netsh delete sslcert ipport=0.0.0.0:16080
- Install the new PFX to the **Certificates - Local computer - Personal** container.
- Open the new certificate and copy its thumbprint:



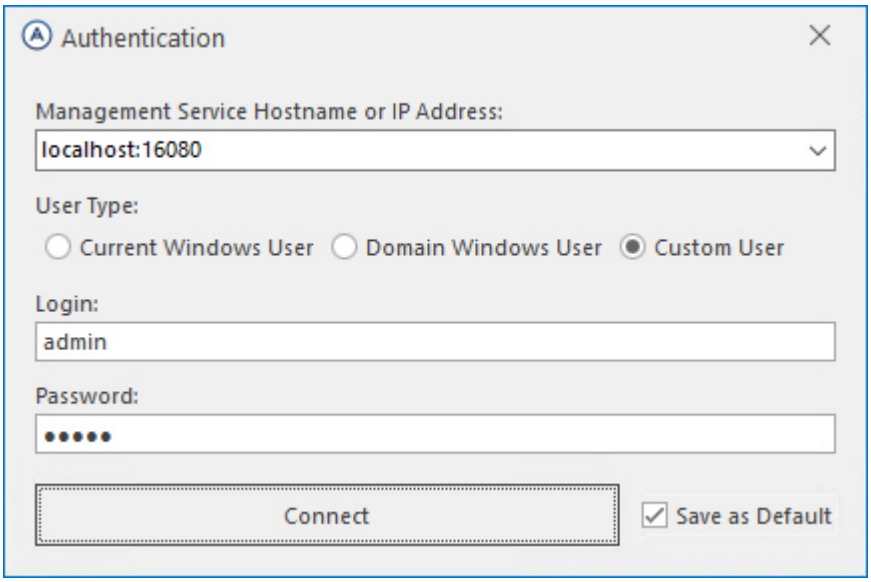
- Install the new certificate on the port via call:

netsh http add sslcert ipport=0.0.0.0:16080 certhash=<thumbprint> appId={7B8B7CD0-C173-4802-AEB7-DF20932E7140}

substitute *<thumbprint>* with your data.

Login to console

Launch the management console and enter the relevant credentials:



- Enter the management server hostname or IP address and the TCP port number (16080) into the **Management service hostname ot IP address** field. Example: *192.168.1.10:16080*; *mymanagementserver:16080*.
- Select the user type:
  - *Current Windows user* - to use the current Windows account credentials with which you have logged in to the computer where the management console is being launched.
  - *Domain Windows user* - to use the corporate domain (AD) account credentials.
  - *Custom user* - to login with the non-Windows/AD custom user credentials.

Note
All the accounts for the login options, described above, must be registered as Acronis Cloud Manager administrators or users in the **Administration** plugin prior to any login attempts. On the first console start you need to enter credentials that you entered upon management server setup as they are already registered as Acronis Cloud Manager administrator's credentials. At a later point, you will be able to add other users and/or change the default credentials.

- Enter the login into the **Login** field.
- Enter the password into the **Password** field.
- Enable the **Save as default** option to save the credentials for the future login attempts for the current Windows account. Saving the password will be prohibited if the corresponding option is configured. Please refer to the "Additional settings" (p. 43) section below.

Two-factor authentication

As a security concern, the two-factor authentication is implemented into Acronis Cloud Manager. If you chose to use it and have enabled the corresponding option during management service installation, then you will be required to configure the *Google authenticator* account on your mobile device after entering general Acronis Cloud Manager login and password and then enter the one-time password, generated by *Google authenticator* application before you are able to login to management console or web portal.

Ensure that you:

- Have downloaded and installed the *Google authenticator* application on your mobile device if you have not done so before.
- Have synced the time on your mobile device and management server.

Setting up 2FA:

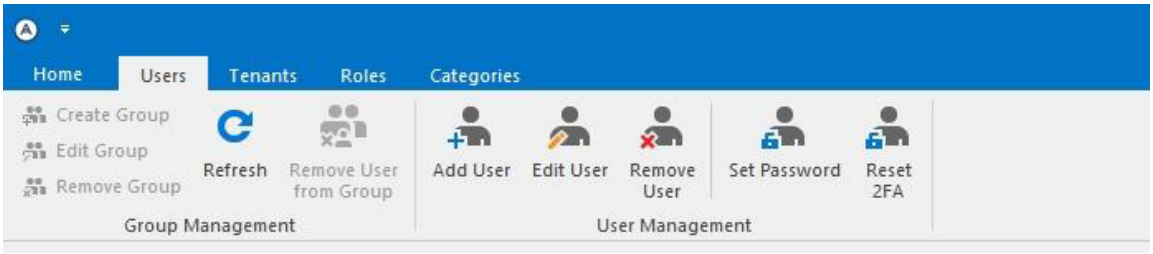
1. Scan the QR code that will appear on the screen upon entering the general Acronis Cloud Manager login and password as an example given below:

2. Enter the 6-digit one-time password, generated by *Google authenticator* into the field below QR code:

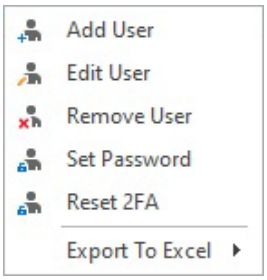
3. Click **Validate**. In the case of successful validation you will be allowed to login. You will be required to enter the one-time password each time at the further login attempts. Please keep your mibile device close and ready. Please, also make record (picture) of that QR code in the case you need to reconfigure your *Google authenticator* account.

In the case the QR code is lost by any user or admin, admin is able to reset 2FA both for himself and any other user to get the new QR code. Resetting 2FA:

- Via the management console: open the **Administration - Users** tab, select the target user and click the **Reset 2FA** button on the main ribbon:



or corresponding context menu command:



Then confirm the action.

- Via the configuration file: open the configuration file C:\Program Files\5nine\5nine Cloud Manager Management Service\5nine.Management.exe.config and add the Reset2FAForUser key into the

appSettings section:

<appSettings>

<add key="Reset2FAForUser" value="*user_name*" />

....

</appSettings>

Replace *user_name* with the actual user name, save the configuration file and restart the management service.

The two-factor authentication can also be enabled or disabled at any moment after installation. To enable or disable 2FA after the product installation:

Open the configuration file C:\Program Files\5nine\5nine Cloud Manager Management Service\5nine.Management.exe.config and assign/change the corresponding value (*True* to enable the 2FA or *False* to disable this option) to the TwoFactorAuthenticationEnabled key in the appSettings section:

<appSettings>

<add key="TwoFactorAuthenticationEnabled" value="True" />

....

</appSettings>

- Then save the configuration file and restart the management service.

Additional settings

There are additional configurable settings that help to enforce the security level when accessing Acronis Cloud Manager. They are configured in the appSettings section of the configuration file C:\Program Files\5nine\5nine Cloud Manager Management Service\5nine.Management.exe.config. Assign/change the corresponding value to the required key:

- Enable or disable password saving option. When a user enables the option *Save as default* while logging in to the management console or web portal, the system may save both login and password for the future attempts or the login only. To configure the password saving option, assign/change the corresponding value (*True* to allow saving both login and password or *False* to save only login without password) to the PasswordSavingEnabled key:

  <appSettings>

  <add key="PasswordSavingEnabled" value="True" />

  ....

  </appSettings>

- Set the maximum number of unsuccessful login attempts to the FailedAuthenticationMaxNumber key (the default value is *10*):

```
<appSettings>
<add key="FailedAuthenticationMaxNumber" value="10" />
....
</appSettings>
```

- Configure the lockout period for the exceeded number of unsuccessful login attempts, after which a user will have another chance to login. Set the corresponding value to the AuthenticationLockoutPeriod key in the *HH:MI:SS* format (the default value is *00:30:00*):

```
<appSettings>
<add key="AuthenticationLockoutPeriod" value="00:30:00" />
....
</appSettings>
```

- Set the retention period for unsuccessful attempts counter to the AuthFailsRetentionDays key (the default value is *90*):

```
<appSettings>
<add key="AuthFailsRetentionDays" value="90" />
....
</appSettings>
```

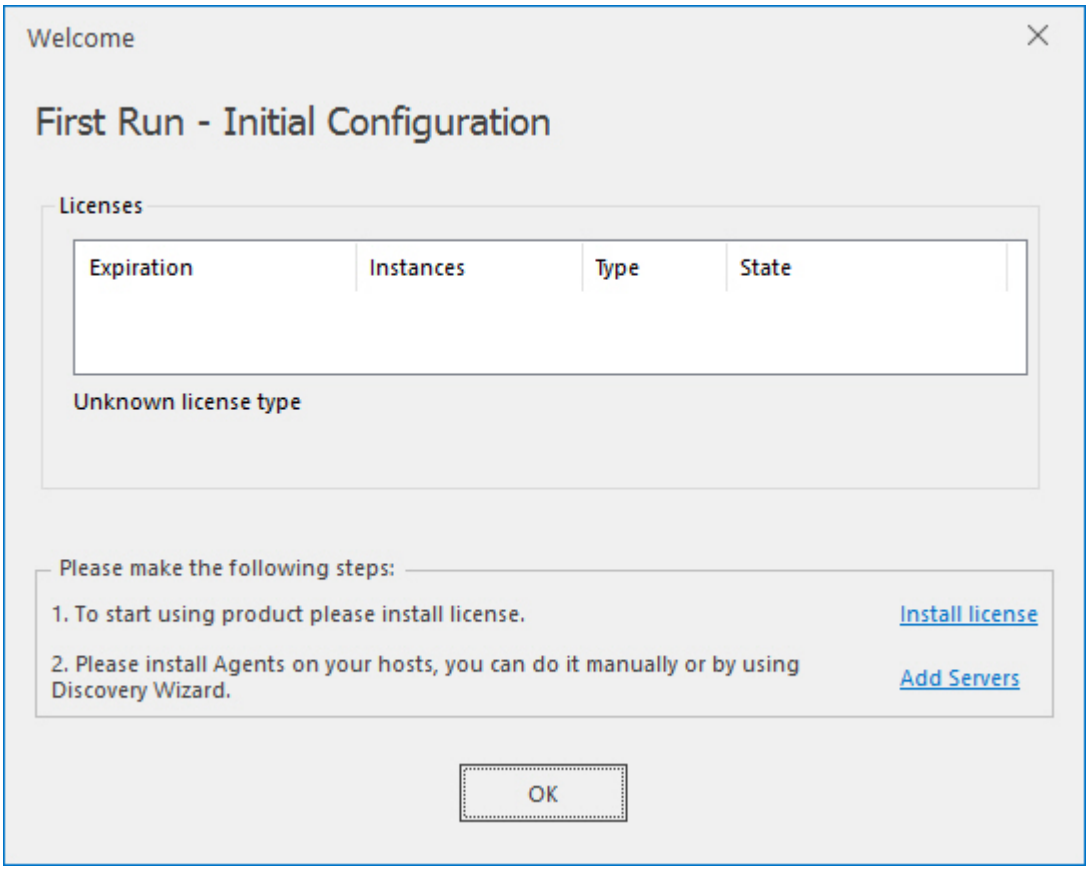
- Configure the user inactivity period, after which a user will be forced to re-login. Set the corresponding value to the UserInactivityLimit key in the *HH:MI:SS* format (the default value is *01:00:00*):

```
<appSettings>
<add key="UserInactivityLimit" value="10:00:00" />
....
</appSettings>
```

Then save the configuration file and restart the management service.

First run

1. On the first console start you will be asked to install the license and prompted to add Hyper-V servers:



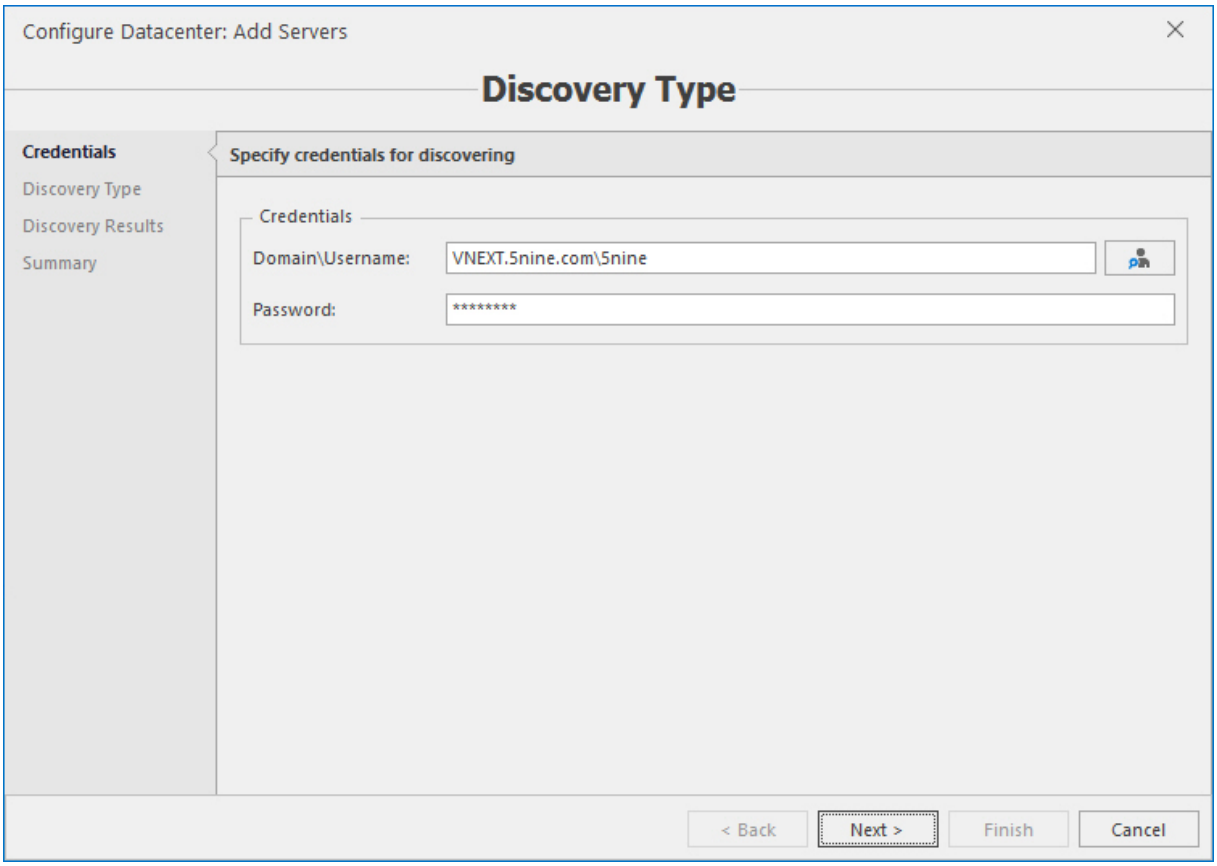
2. Click the **Install license** link and choose the **license.txt** file. You may either have a trial license that came with your trial email or a commercial license that would have been purchased. More information about the licensing and how to install the license at a later point can be found in the '"Licensing" (p. 17)' section below. Click **Add Servers** to add Hyper-V hosts or clusters. The adding servers process is described in the next section.

Adding Hyper-V servers

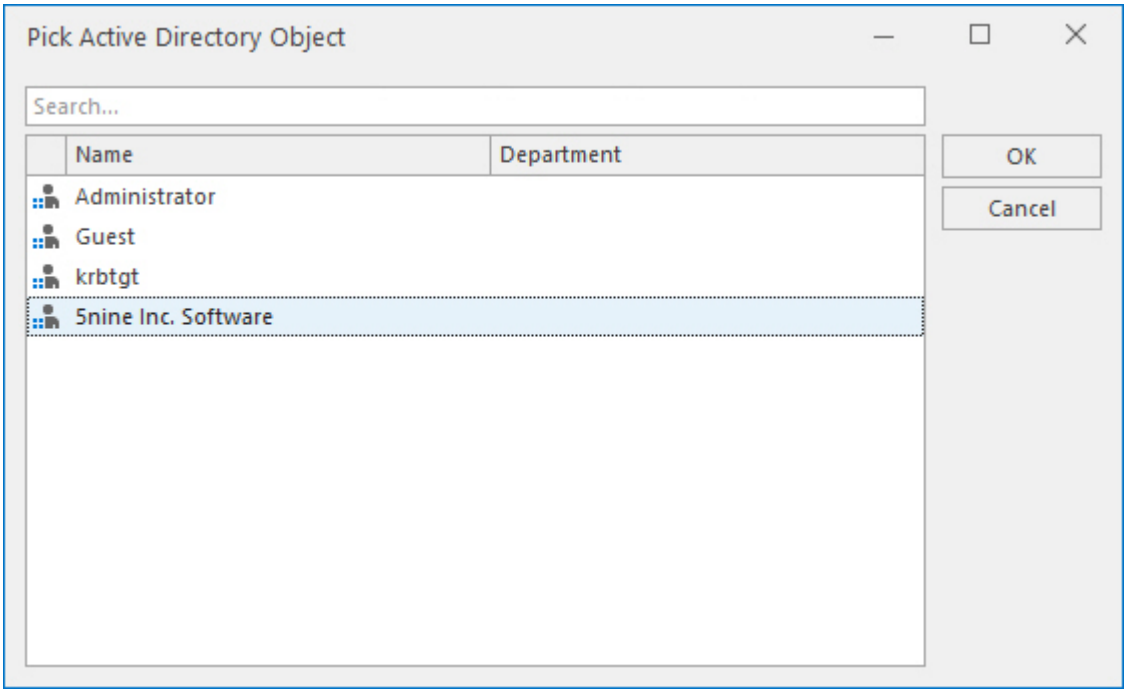
1. To start managing your virtual infrastructure, you must configure connections to Microsoft Hyper-V virtual management servers. You can connect the following types of servers:

- Standalone Hyper-V host;
- Hyper-V cluster.

2. For the initial launch the object tree will be empty. Adding new servers is implemented via **Add servers** wizard. To start the wizard press the, **Add servers** button in the toolbar at the top of the console.
3. After the **Add servers** wizard starts you need to specify credentials for discovery:



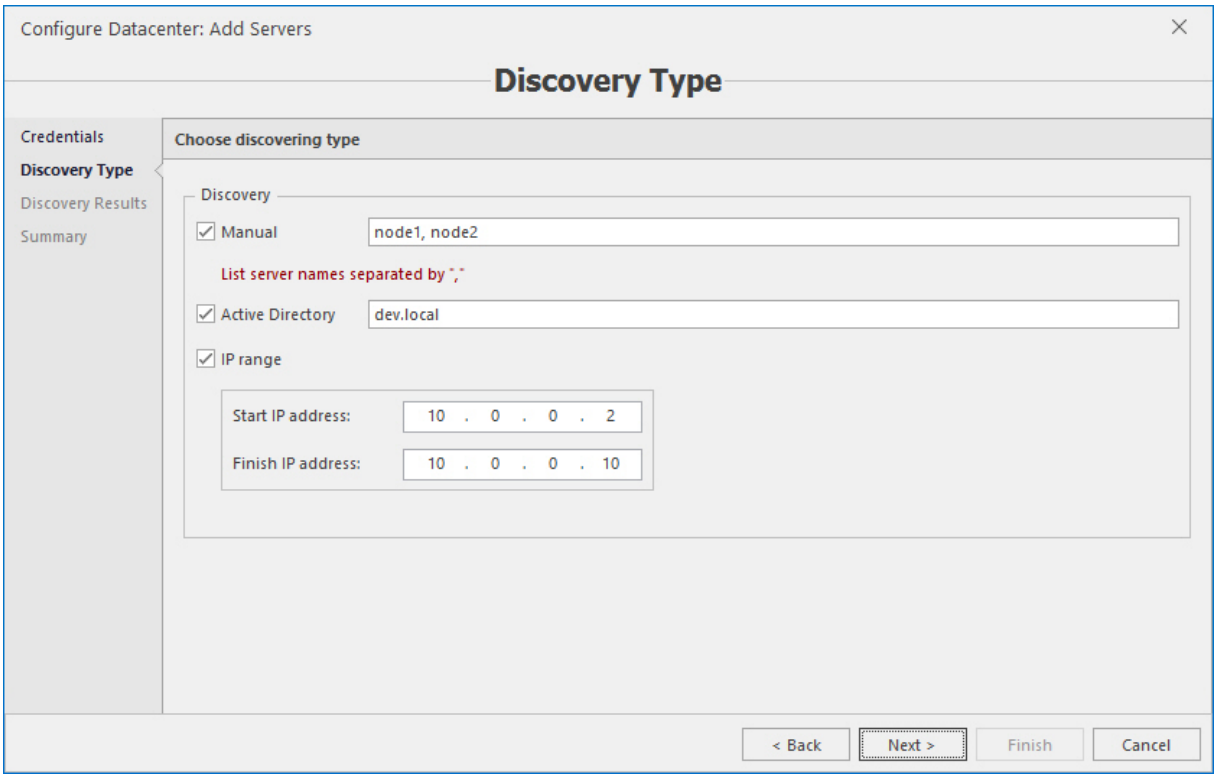
You may type in credentials manually or use AD discovery for that purpose, if you are working in a domain environment. To use AD discovery, press the button to the right of the **Domain\userame** filed and then select the AD account and click **OK**:



Then select discovery types and provide discovery data:

New servers can be added in 3 ways:

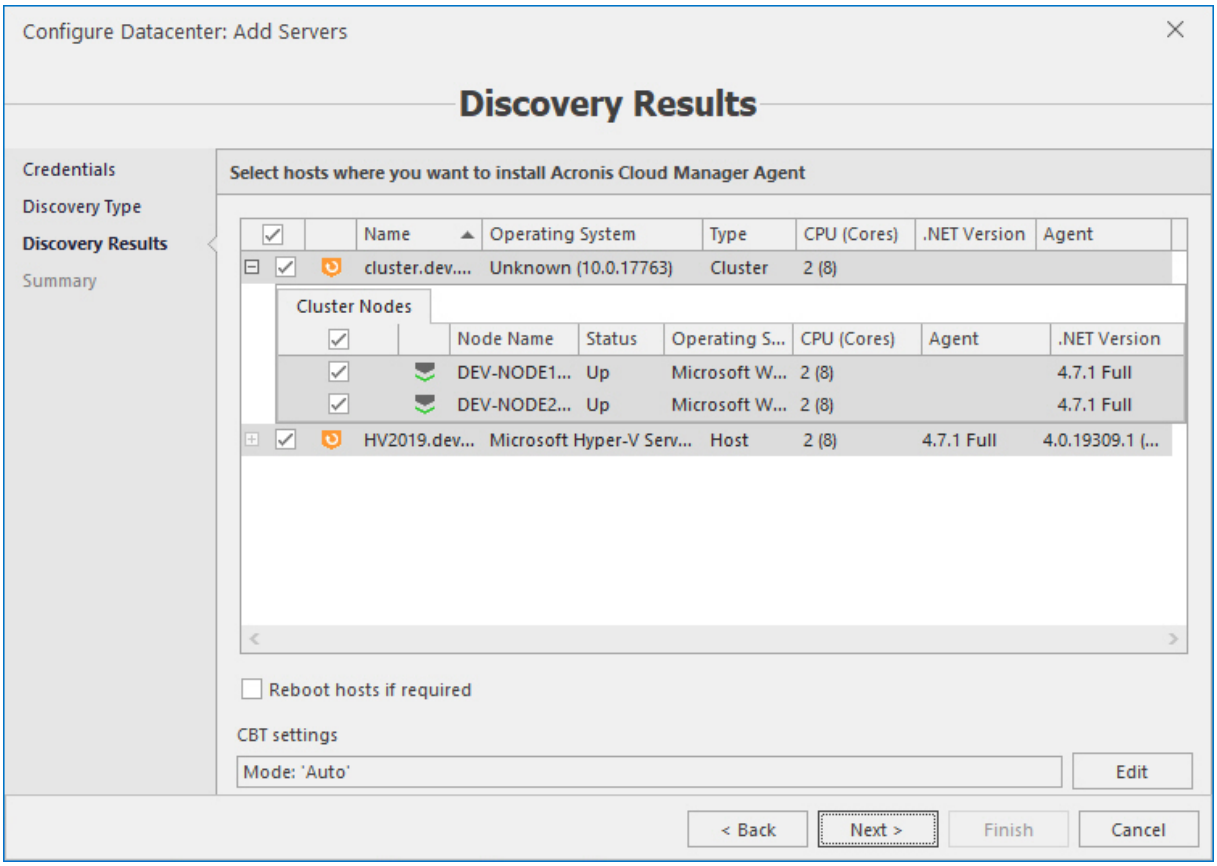
- **Manual** - Manually typing the addresses of servers separated by commas. You may use host name, FQDN or IP address.
- **Active Directory** – to search for available hosts or clusters using AD discovery.
- **IP Range** – to search for available hosts or clusters using IP discovery in the given IP range.



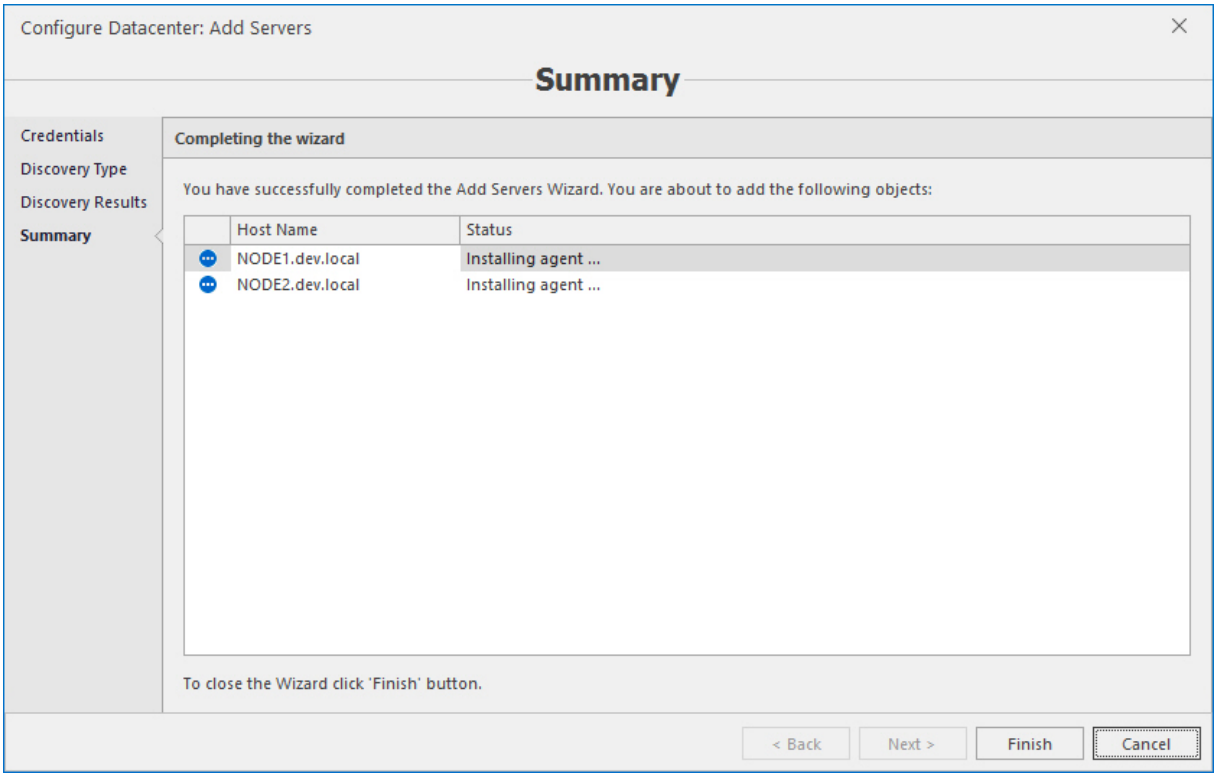
Note

AD and IP discovery can take quite significant time depending on your AD and network structure and performance. Once the discovery process completes, you will get the full list of servers that can be managed by Acronis Cloud Manager. Only those servers that match system requirements are selected automatically.

4. Select servers that you need to manage and press **Next**:



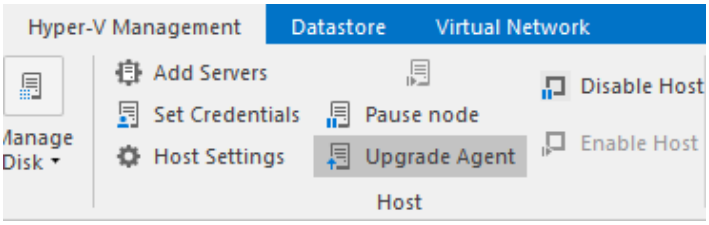
5. Host agents will be installed automatically on the servers that you selected on the previous step.



Note
When agents are installed servers will appear in the console objects tree automatically.

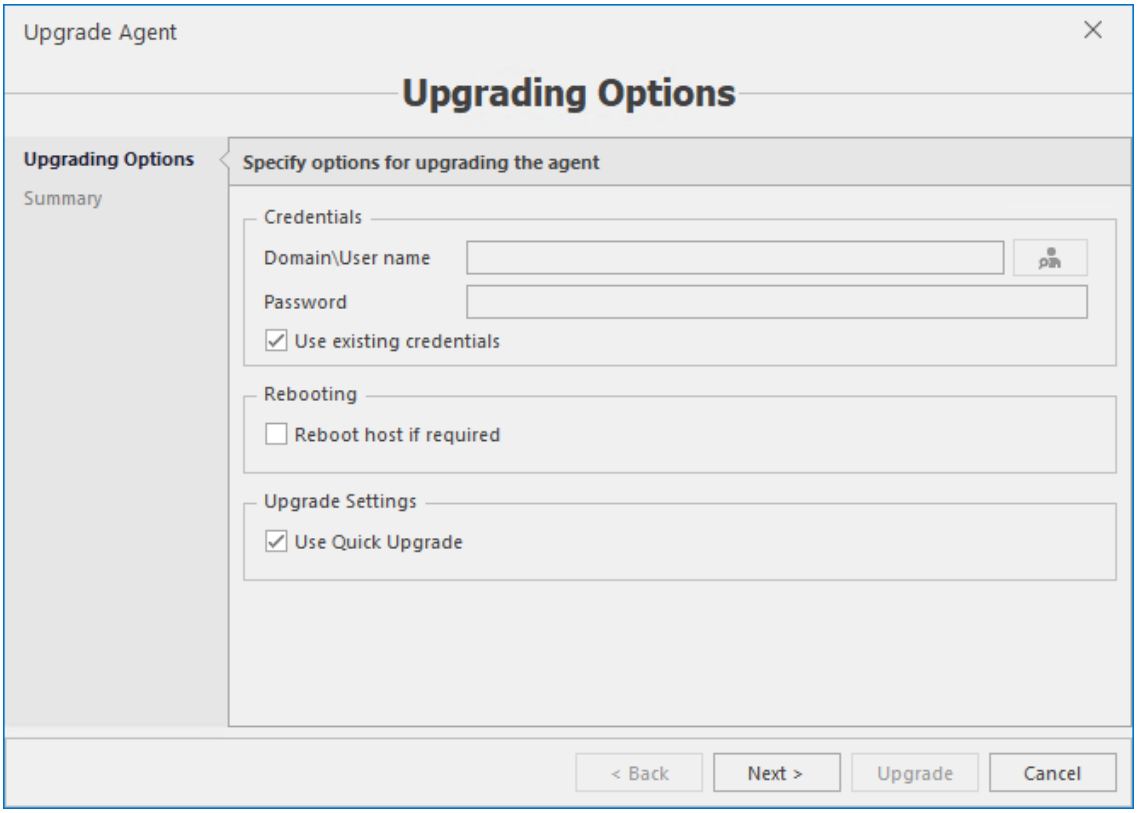
Upgrading host agents

If you are upgrading the product from the previous versions, upon completing management service and console upgrade, the product will detect the necessity and offer to upgrade host agents. Blue arrows will appear on host's icons in the object tree, displaying the necessity to upgrade the agents. Also, the corresponding command will appear in the context menu of the host objects and on the main ribbon:



Use the **Upgrade agent** command to proceed with the upgrade. You may select any host, eligible for upgrade. You will be able to choose which hosts should be upgraded further during the operation.

Configure agent upgrade options on the wizard:

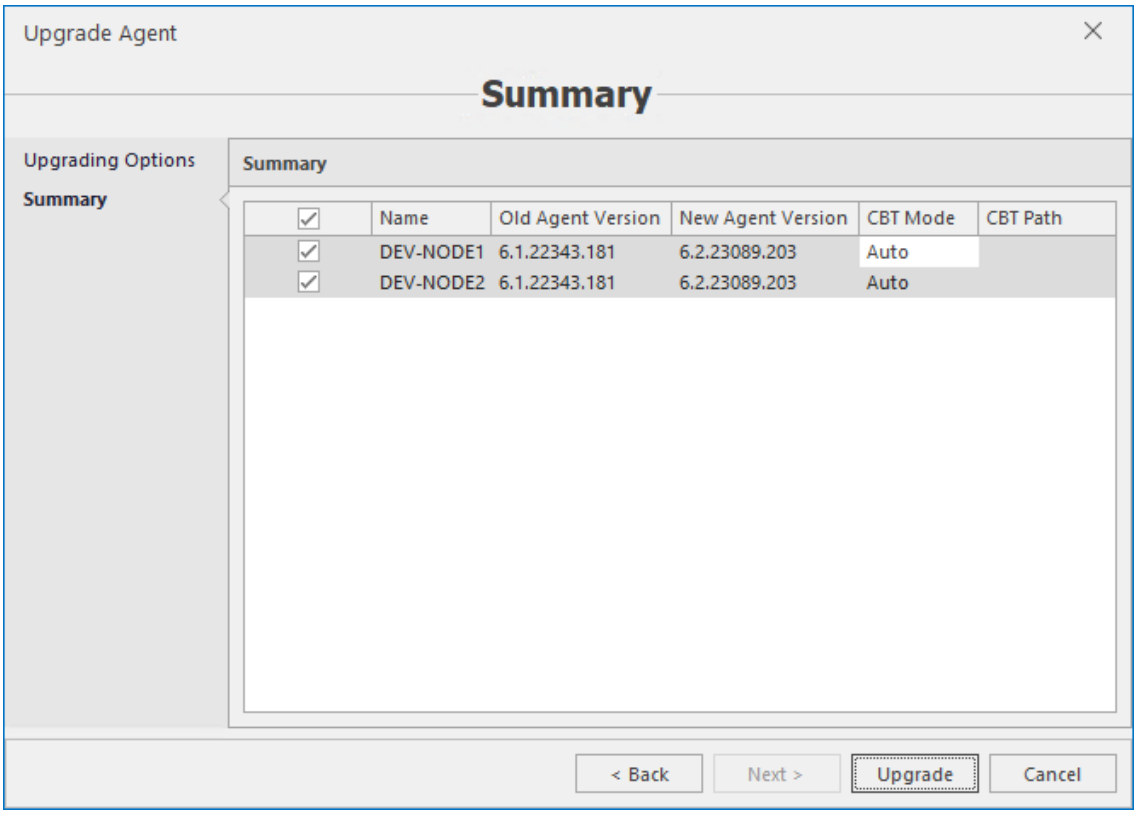


- Pick the active directory domain user and enter its password. Enable the **Use existing credentials** option if you have chosen a different account than was used previously and would like to use it further as host management credentials.

- In the case a reboot is needed on the host during the upgrade and you would like it is done silently during the upgrade process, enable the **Reboot host if required** option.
- Leave the **Use quick upgrade** option enabled as set by default to allow the new fastest agent upgrade method to be used. It consists of self-upgrade of the agents by sending the new .msi file directly to the host agents, which then completes the upgrade process. If this option is disabled, the old method will be used through Active Directory, which repeats the same process, occurring when adding the new Hyper-V hosts to the object tree, and takes the greater time to complete the upgrade.

Click **Next**.

Select the hosts that you need to upgrade right now and deselect those that you would like to upgrade later (or select all hosts to upgrade them all at once) and click **Upgrade** to start the process:



Nothing else is required from your side, when the upgrade process is complete, you will see the green marks on the host icons in the object tree, as they usually appear and the corresponding record in the job list.

Managing users, tenants and roles

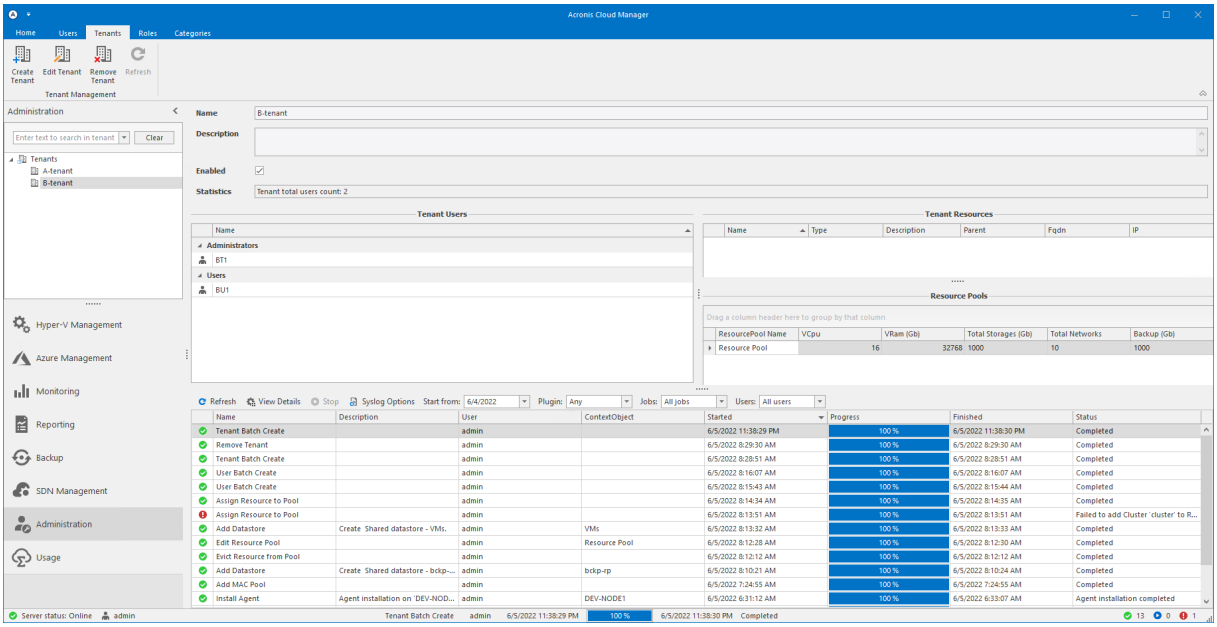
Acronis Cloud Manager supports multi-tenant environments when users can have granular permissions and roles to access Hyper-V infrastructure. It is a very convenient instrument for enterprise and service provider organizations. For example, a tenant can represent a department in a company or a corporate client for a service provider.

To use role-based access control (RBAC) capabilities or features you will need to set tenants, users and roles as a part of system configuration process.

- Credentials for system administrator are set in management console setup.
- Tenants, users and roles can be set in the **Administration** plugin under these credentials.

Tenants

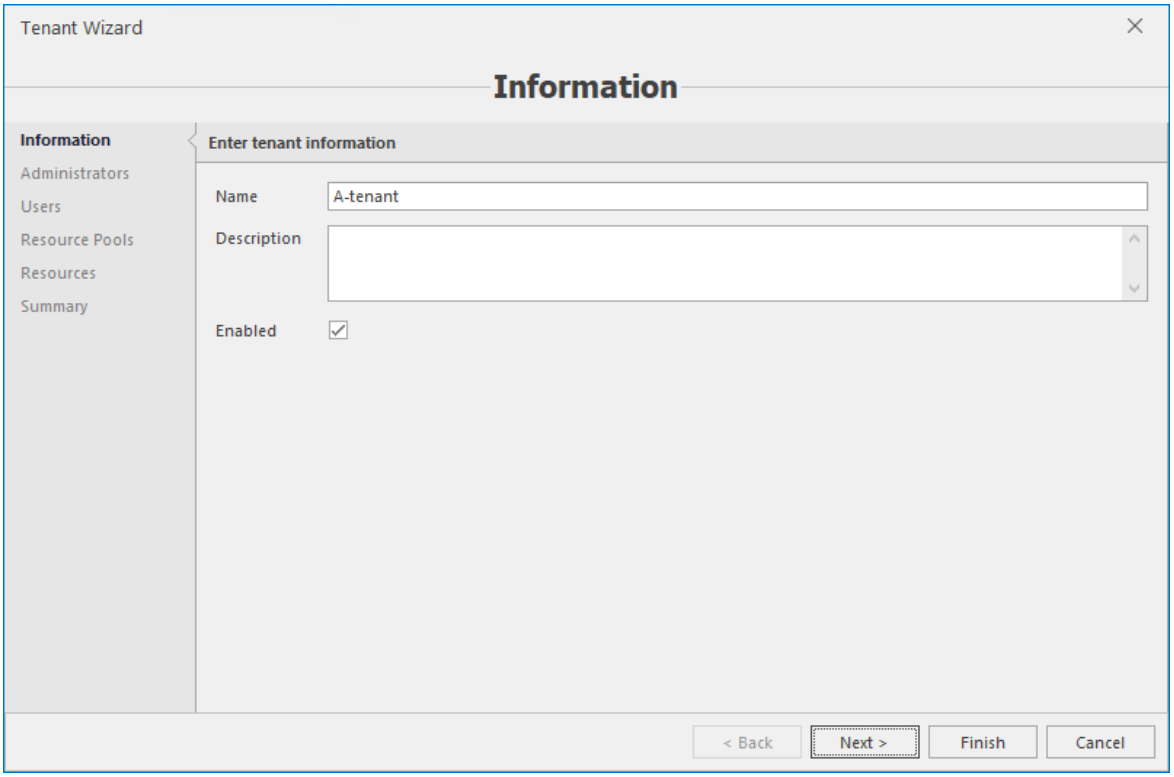
Tenants are managed on the **Tenants** tab of the **Administration** plugin:



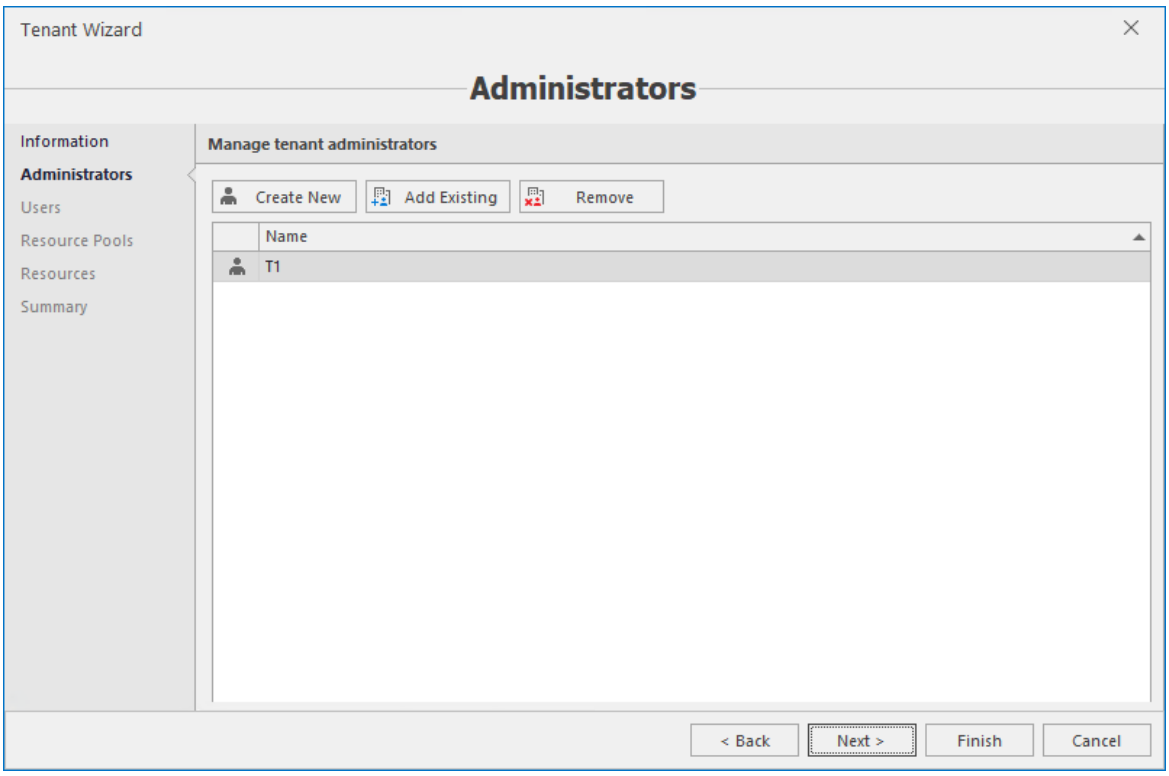
There is the tenants tree on the left side with the detailed description and parameters for each one on the right side. Tenant name and description is shown on the upper side, the **Tenant users** block contains tenant administrators and users. And there are two alternative blocks on the right: **Tenant resources** and **Resource pools**. First one shows data in the case of using traditional method of resources allocation to tenants, whereas the second one shows data in the case of using the new *resource pools* conception. Please refer to the" Resource pools, quotas and usage" (p. 243)

To create a new tenant:

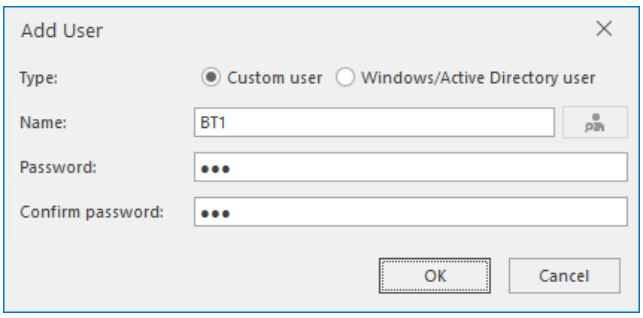
1. Press the **Create tenant** button to open the **Tenant** wizard. Define the tenant name and description. Tenant is enabled by default. If you do not need tenant users to be able to access the system, clear the **Enabled** checkbox.



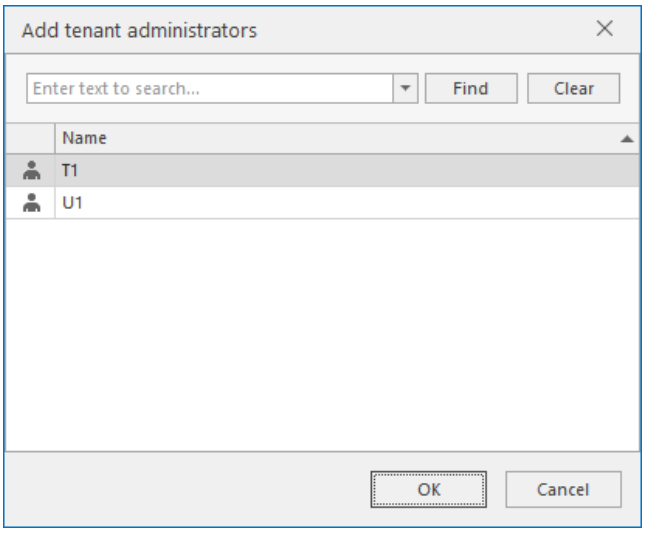
2. Define tenant administrators. They can be selected from the existing users list or a new one can be created.



Click the **Create new** button to create the new admin. The standard **Add user** dialog will appear where the new admin can be added:



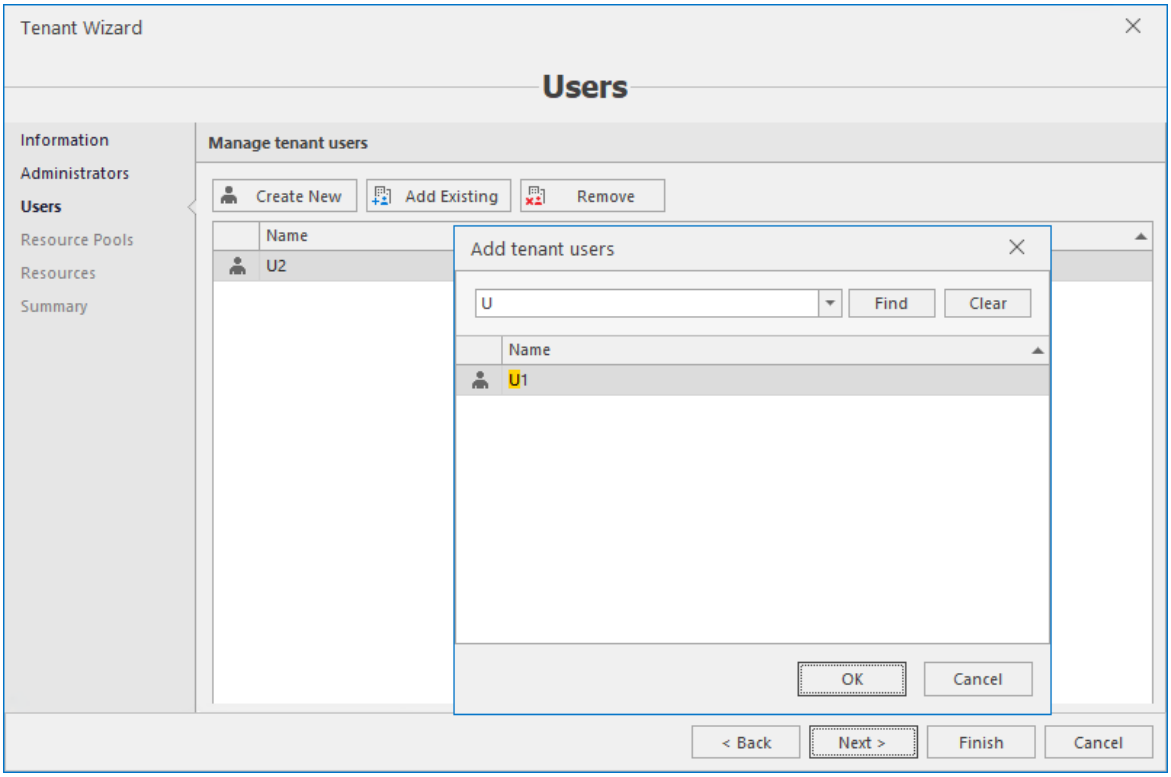
Click the **Add existing** button to add the existing "orphan" users from the global users list as a tenant admins (only free global users that are neither global admins nor associated with tenants can be selected):



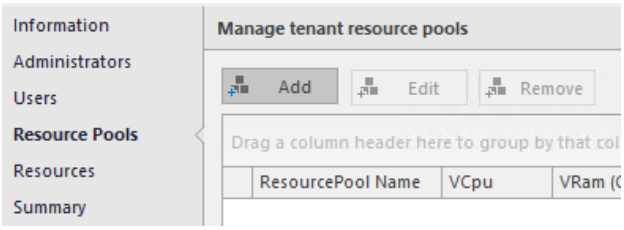
Click **OK** then click **Next**.

To remove the tenant admin, select it and click the **Remove** button.

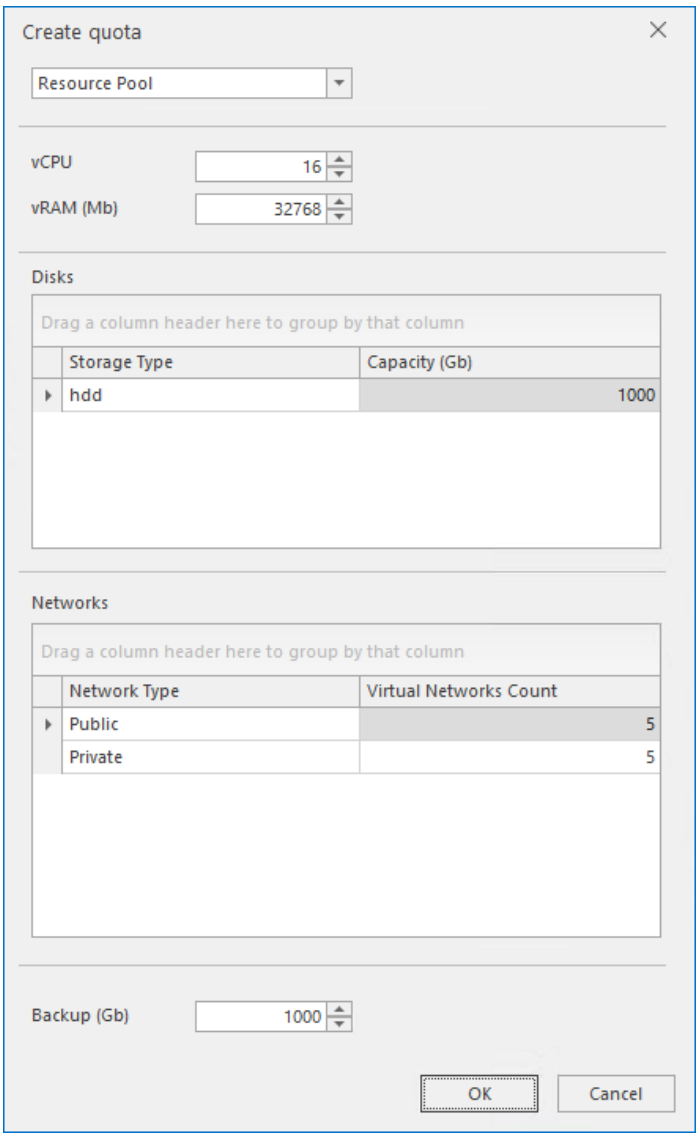
3. Add tenant users in the same way as admins:



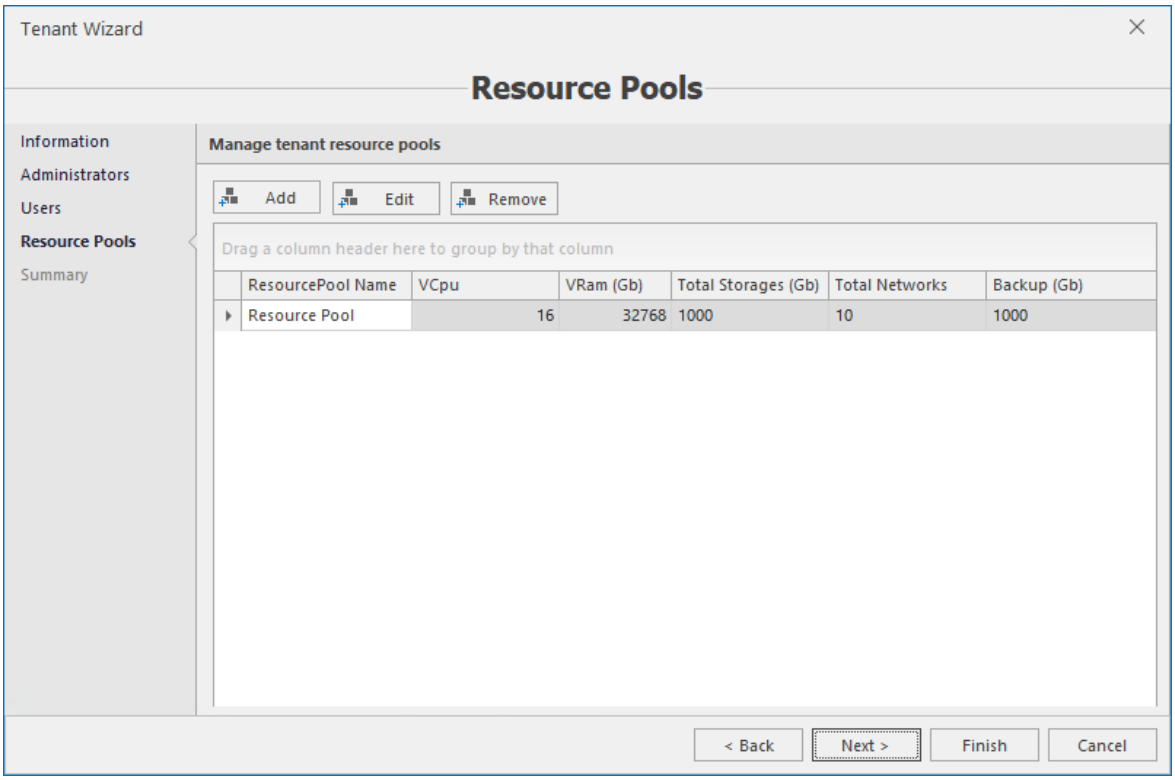
4. [For the resource pools conception] Assign resource pool to the tenant: on the **Resource pools** page click the **Add** button:



Set the quota limits - vCPU, vRAM, Storage capacity, networks and backup storage thresholds:



Click **OK**.



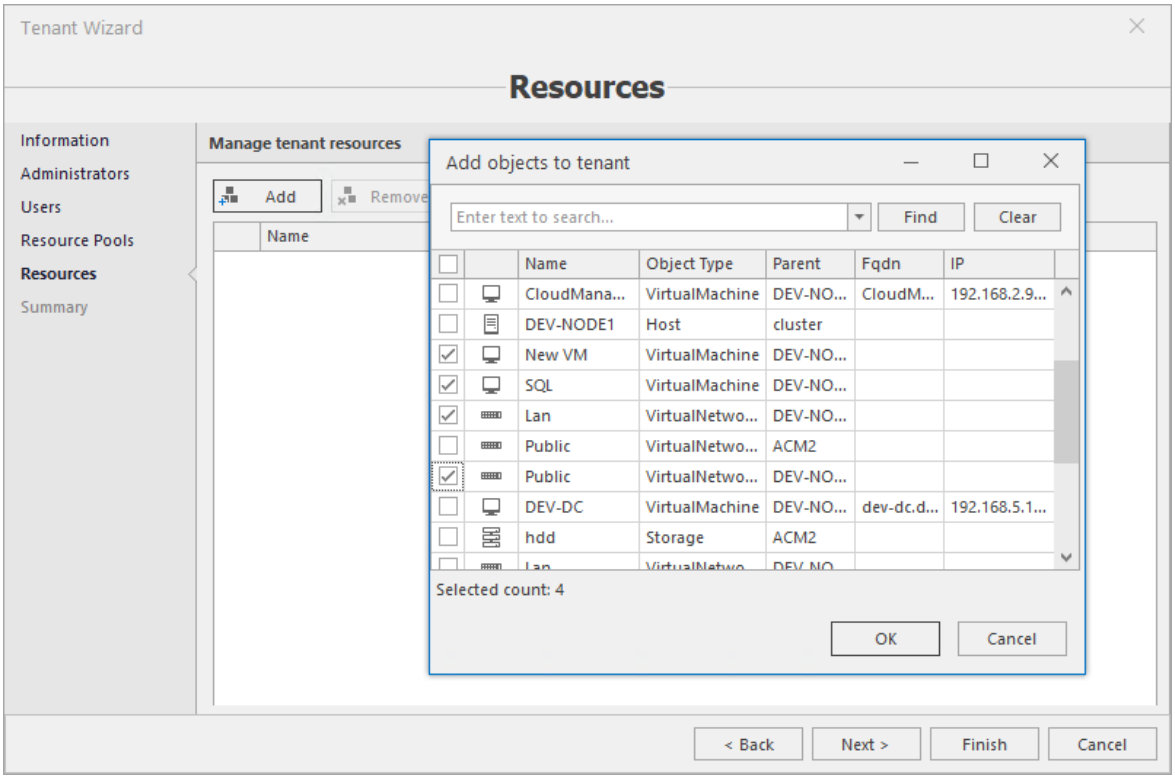
To edit the resource pool quota, selet the resource pool and click the **Edit** button, then set the new limits in the same way as described above.

To remove the resource pool from the tenant, selet the resource pool and click the **Remove** button.

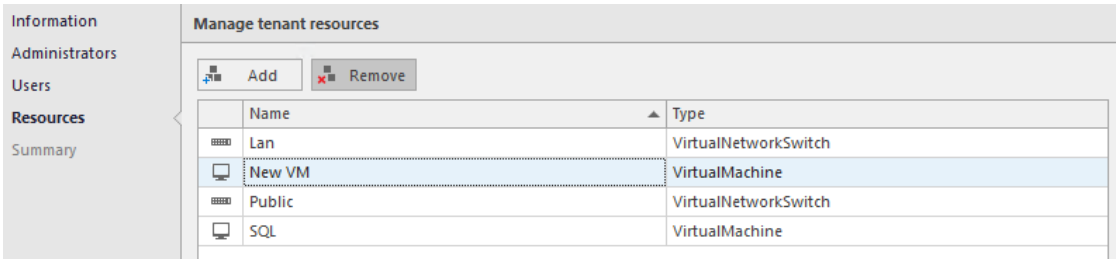
Click **Next**.

5. [For classic conception] Associate objects with the tenant. An object can be associated with a single tenant only. Tenant administrators have full access to all objects belonging to a tenant.

   Click the **Add** button and select the objects to add to the tenant.

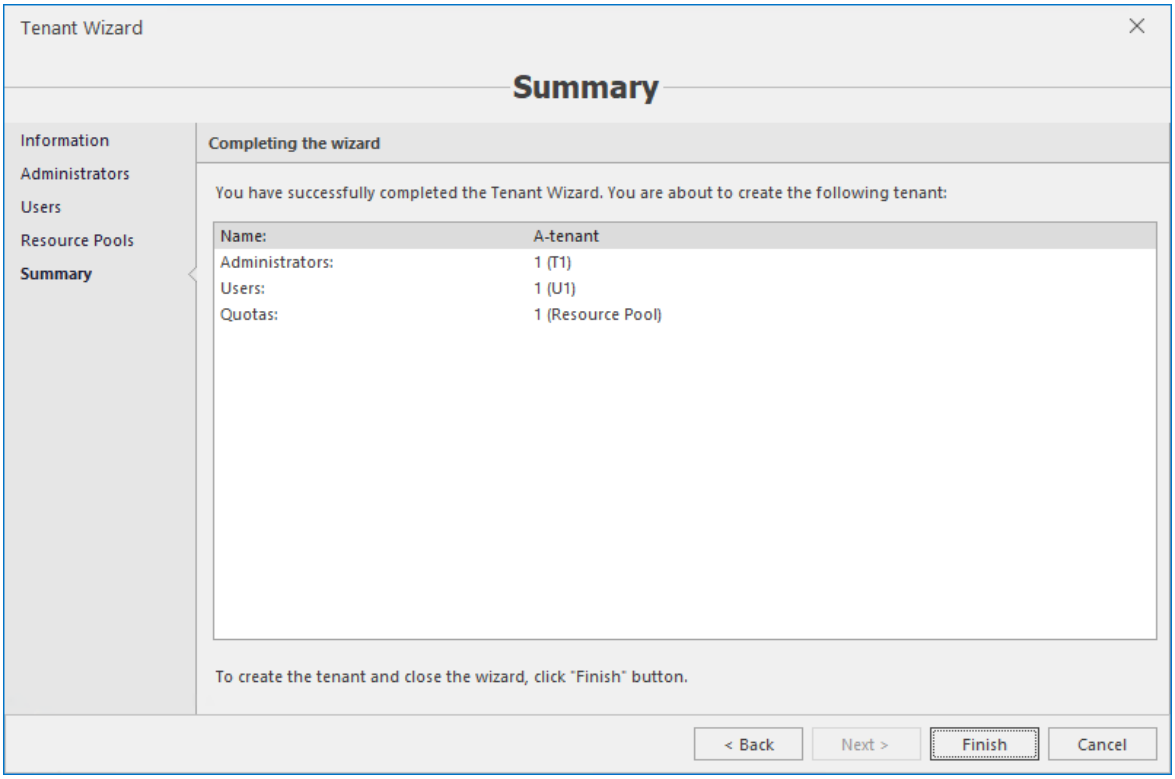


   To remove objects, select it one-be-one and click the **Remove** button.

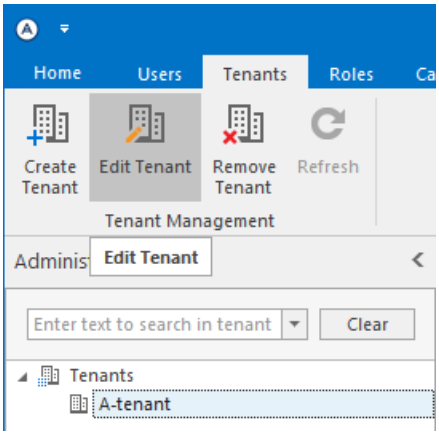


   Click **Next**.

6. Check summary information and, if everything is correct, press the **Finish** button to create the tenant.

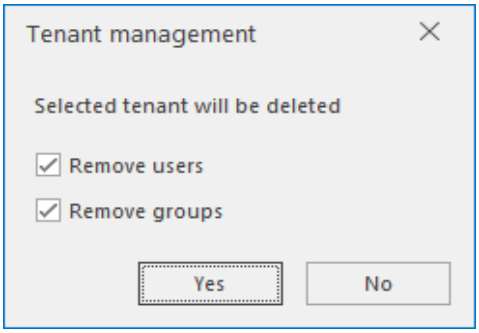


To edit the tenant, select it in the tree and press the **Edit tenant** button or corresponding context menu command:



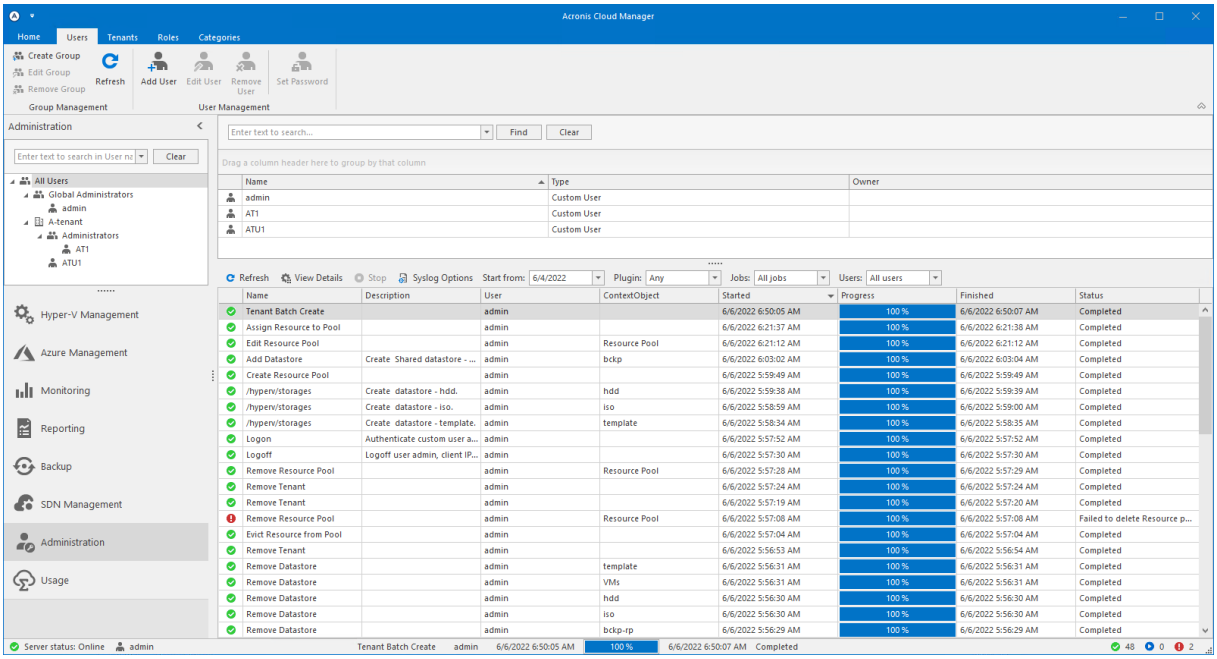
Then edit the required data in the same wizard as when creating the tenant.

To remove the tenant, select it in the tree and press the **Remove tenant** button or corresponding context menu command. Then choose if users and groups should be removed along:



Users

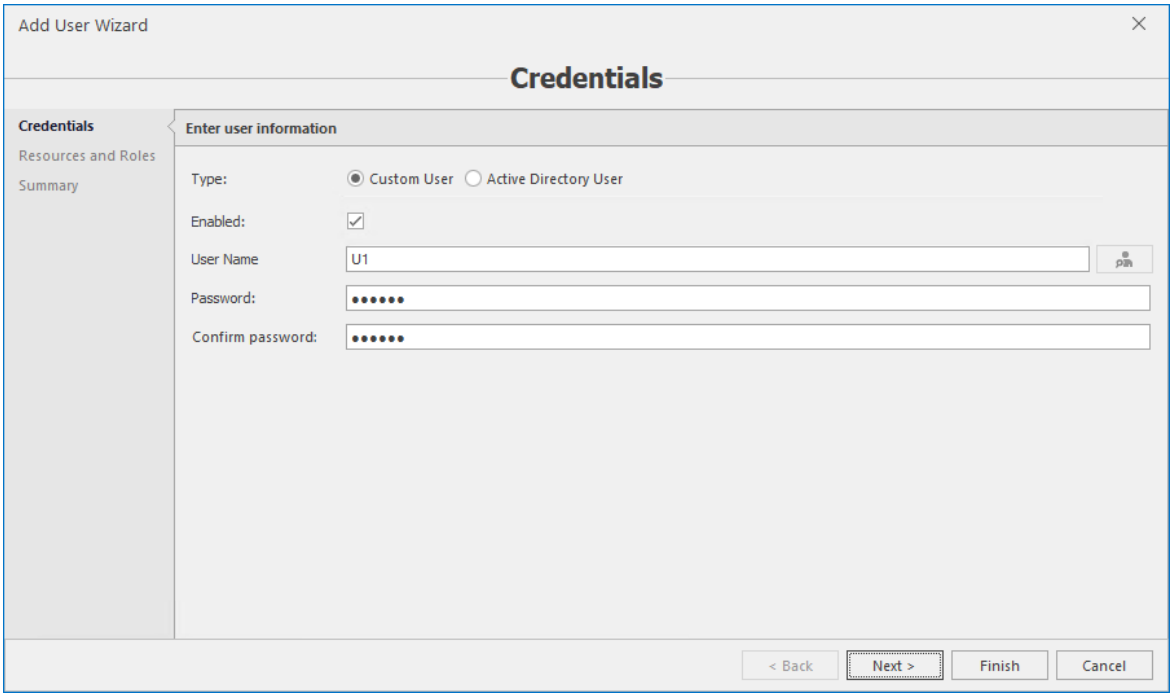
Users are managed on the **Users** tab of the **Administration** plugin.



There are users tree on the left side with hierarchy: all users - global administrators - tenant administrators - tenant users, and details on the right side.

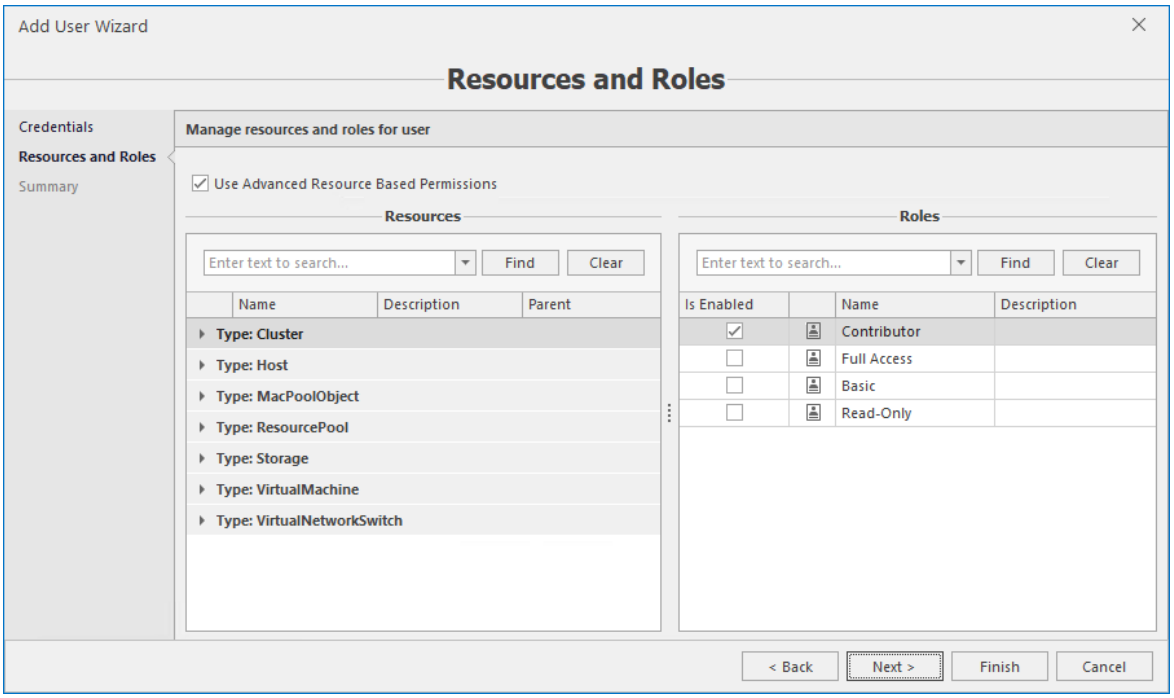
To create a new user:

1. Press the **Add user** button to start the **Add user** wizard.

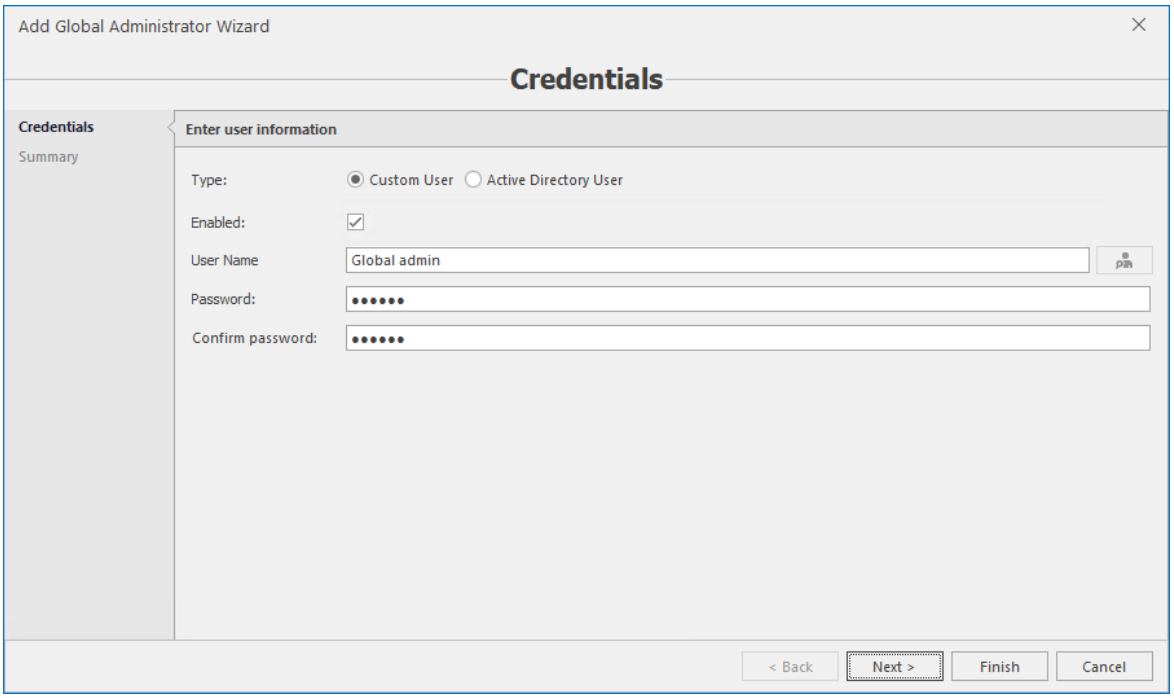


2. Define user type and set credentials. User is created enabled by default. If you do not need the user to be able to access the system, clear the **Enabled** checkbox.
3. Define user resources and roles. By default, there are 4 roles in the system:
   - **Contributor** - specific role that contains access only to the resource pool type of objects.
   - **Full access** - role that contains full access to all objects of any type.
   - **Basic** - limited role that contains access to some of operations with virtual machines and read-only access to all other types of objects.
   - **Read-only** - role that contains read-only access to all types of objects.

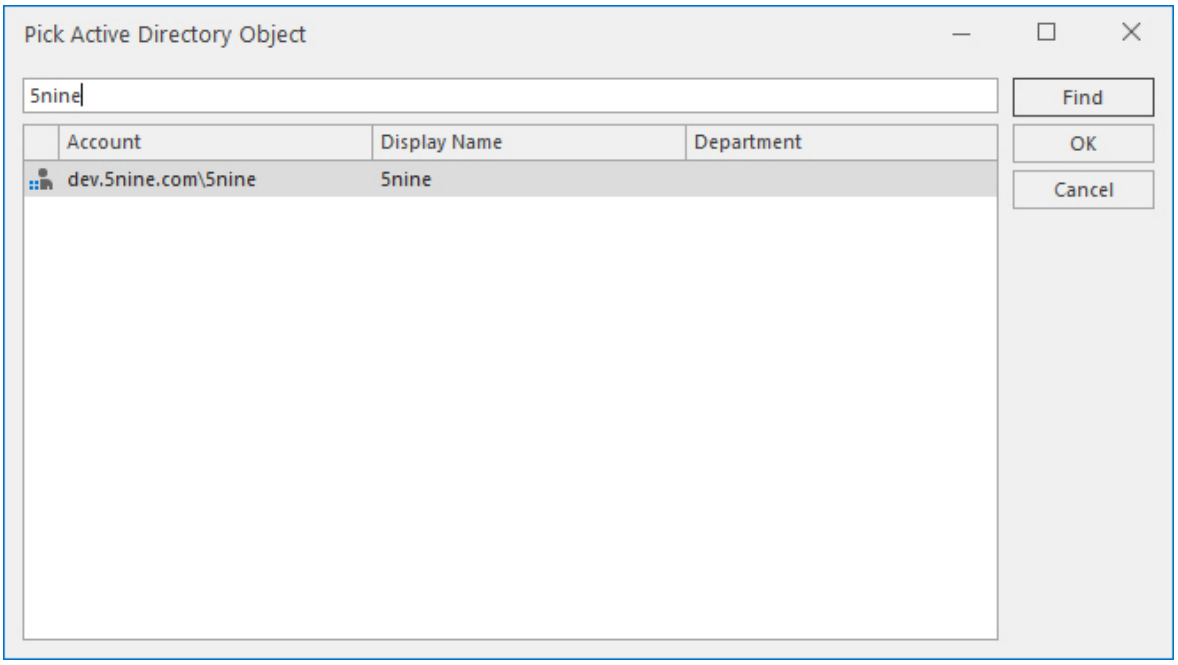
   You can define your own roles. Tenant users can have access only to the objects that are associated with the tenant.



4. If you are on the **Global administrators** entity in the object tree, then the **Add global administrator** wizard will be opened and the user will be added with global administrator's privileges, you will not be able to alter its permissions during the creation process like it's done for non-administrator users:

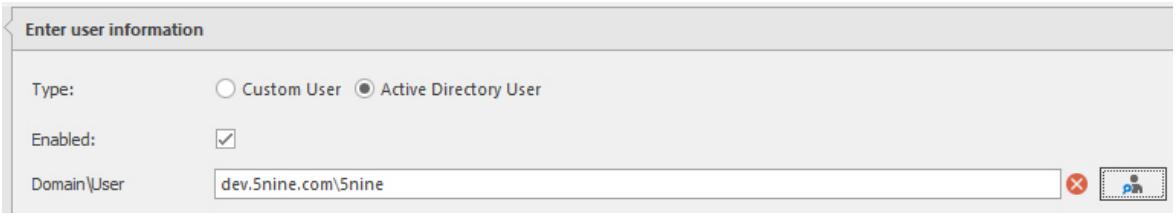


For active directory users, auto-discovery from the domain active directory is available – click the button to the right of the **User name** field to open the search dialog box:

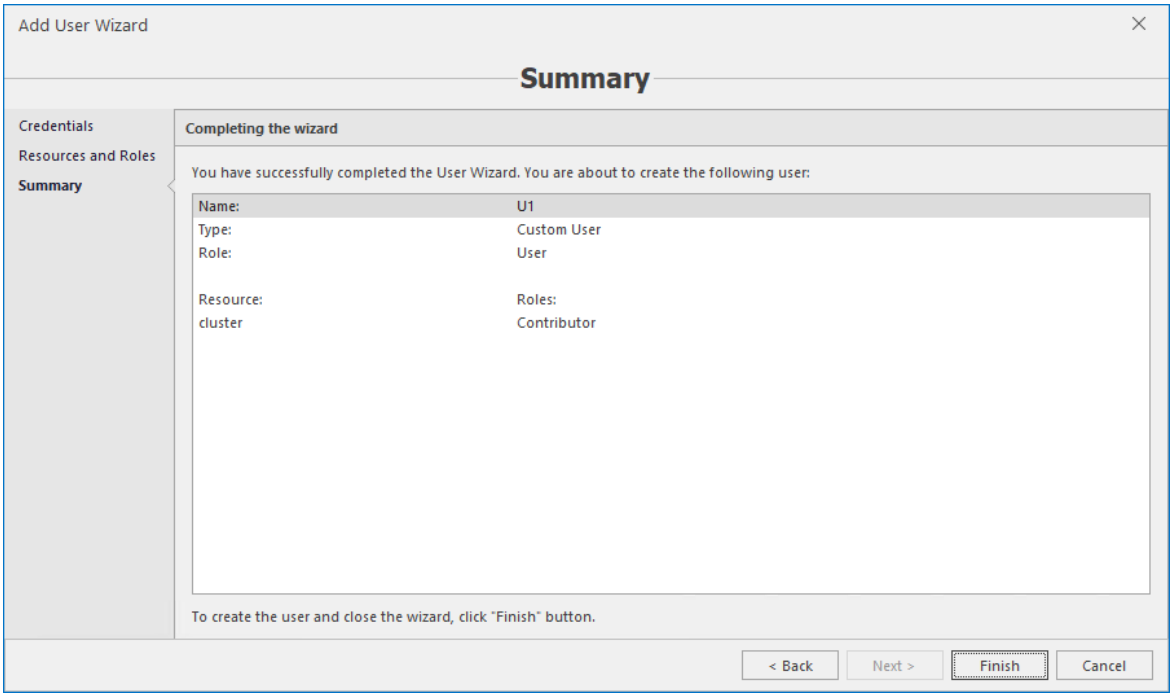


Start typing the user name into the upper field, then click **Find**. All found accounts will be displayed lower in the results list.

Select the required account and click **OK** – it will be entered into the main dialog box:



5. Check summary information and if everything is correct press the **Finish** button to create the new user.



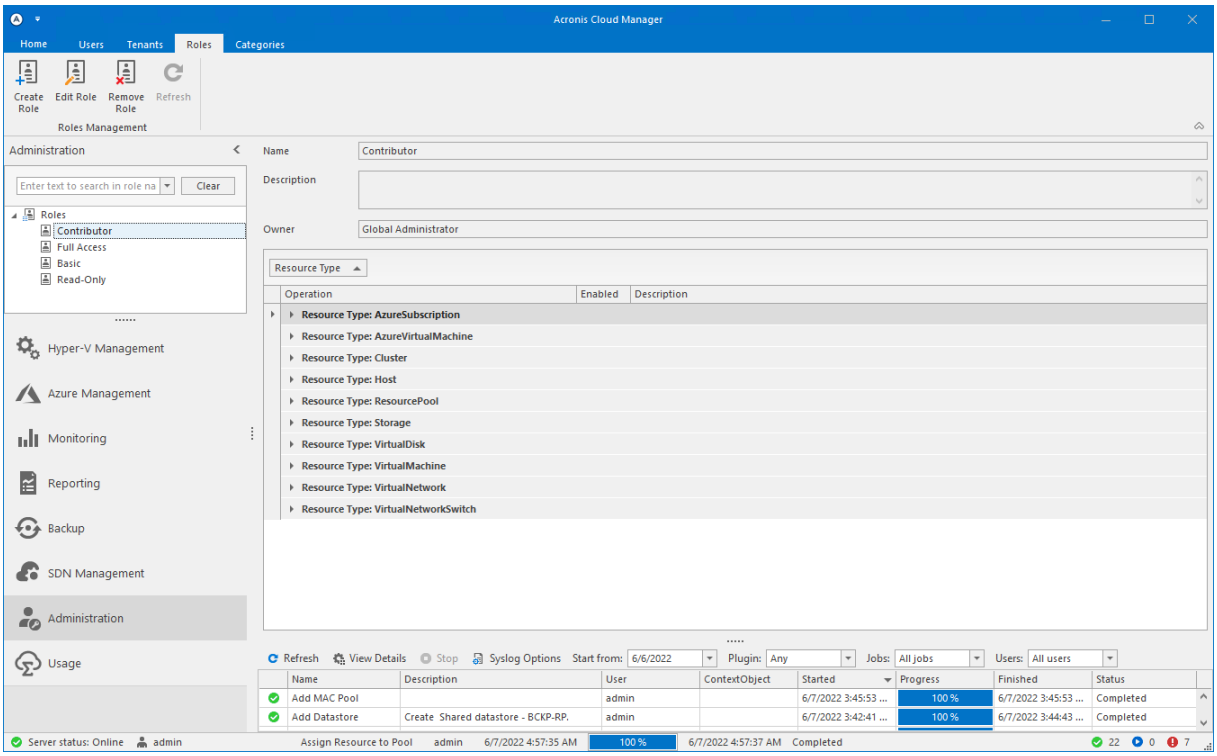
Roles

Roles usually combine granular permissions into the named groups for user convenience.

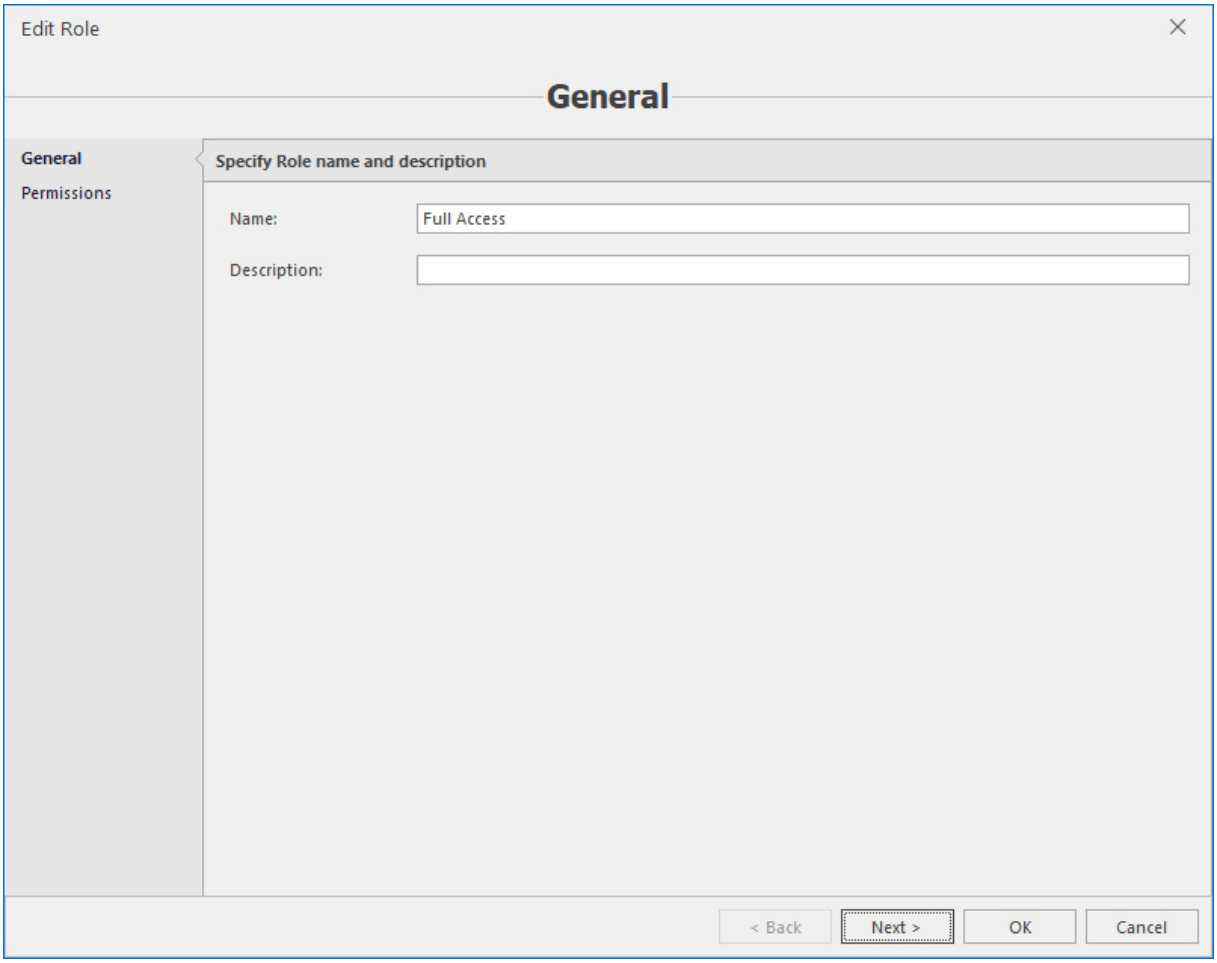
There is a set of granular permissions for every object type:

- **Cluster**.
- **Host**.
- **Virtual machine**.
- **Storage**.
- **Virtual network switch**.
- **Virtual network**.
- **Virtual disk**.
- **Azure subscription**.
- **Azure virtual machine**.
- **Resource pool**.

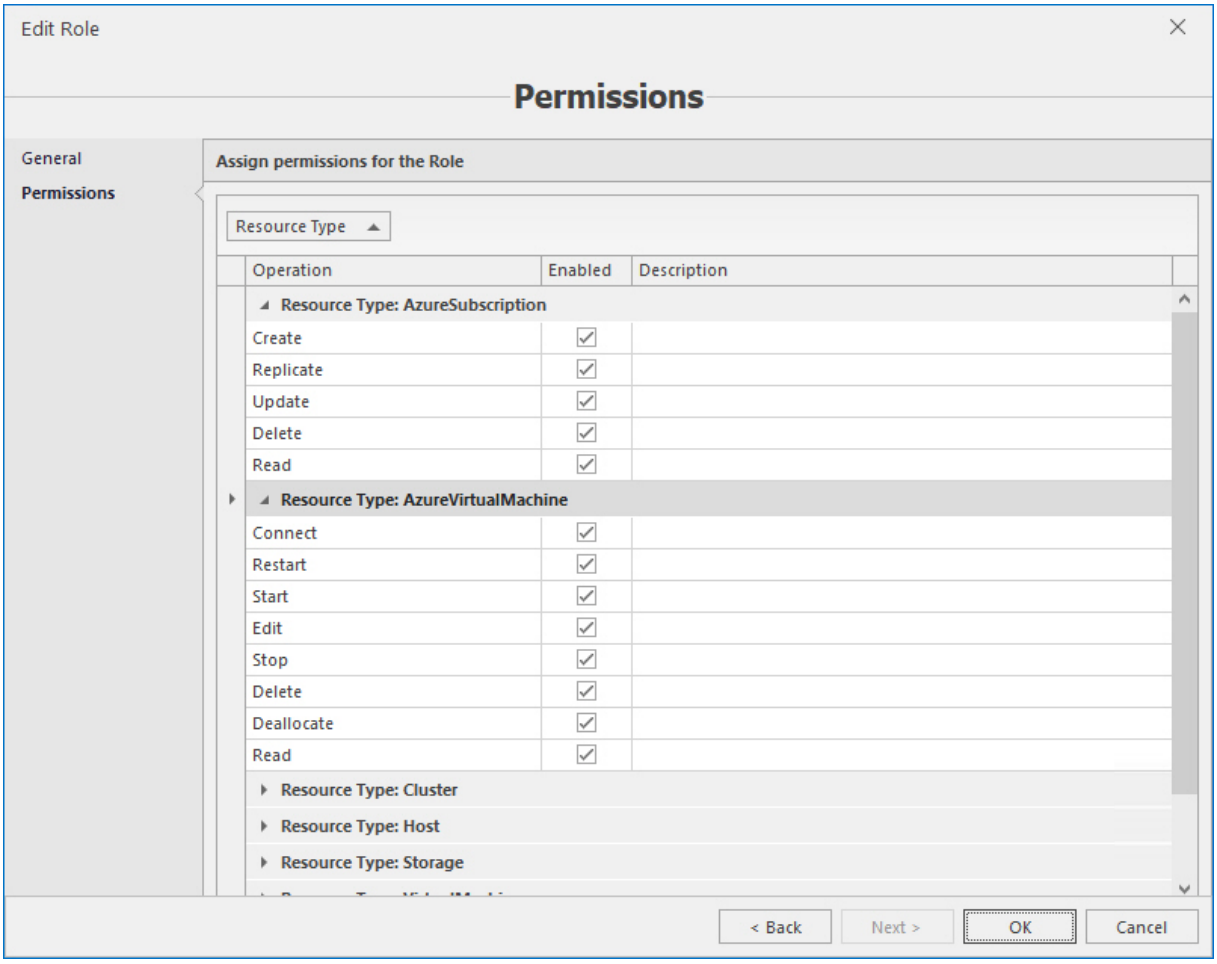
To create a role, go to the **Roles** tab, press the **Create role** button or select the existing role and press the **Edit** button:



The **Create Role** (**Edit Role**) wizard will be opened. On the **General** page specify name and description for the role:



On the **Permissions** page, select objects and permissions.

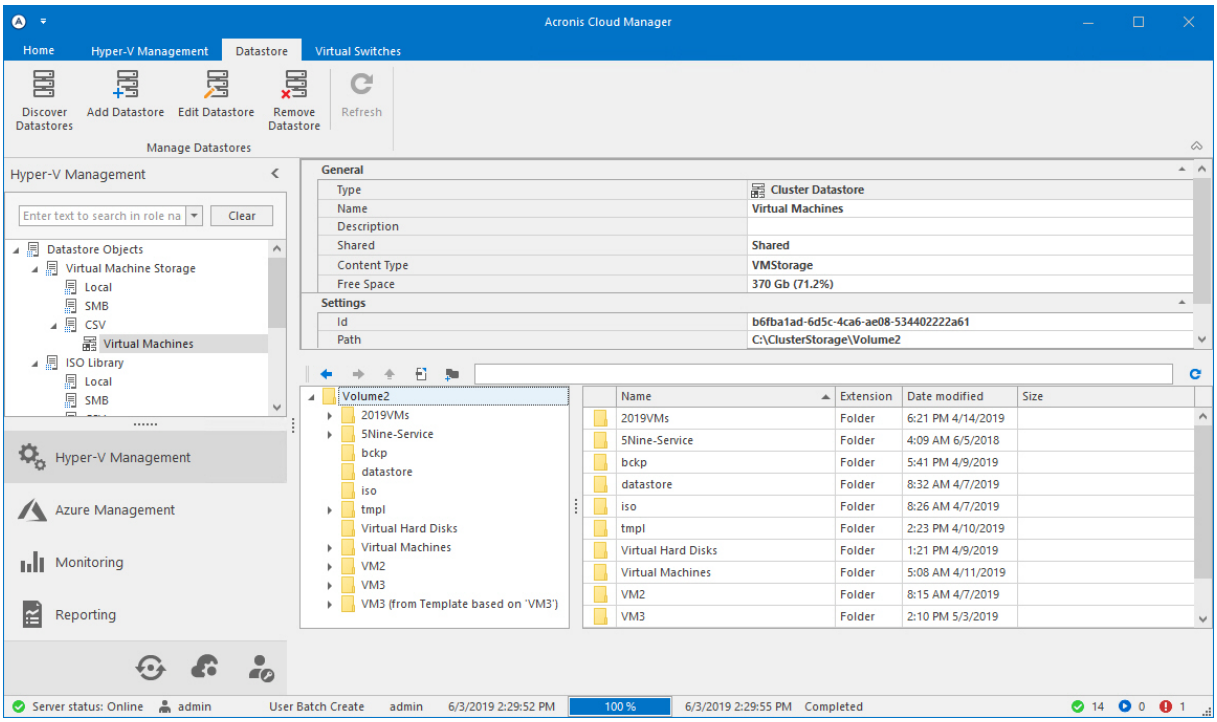


Click **OK** to save changes.

Configuring datastore

Datastore is an internal Acronis Cloud Manager entity necessary to organize and provide storage management for objects of different types: virtual machines, ISO, templates and backup files. Acronis Cloud Manager datastore objects are split into categories and types. Categories reflect storage object types – virtual machine, ISO library, template library and backup storage.

It is not possible to use the storage with the category that does not match object type to avoid confusing or mixing files of different types in the same folder on the storage disk. This makes the datastore ordered and easier to use. Storage types reflect physical location types where files are stored: Cluster shared volume, SMB and local disk. Access to these different locations is provided in different ways, which requires different approaches from the Acronis Cloud Manager side as well.

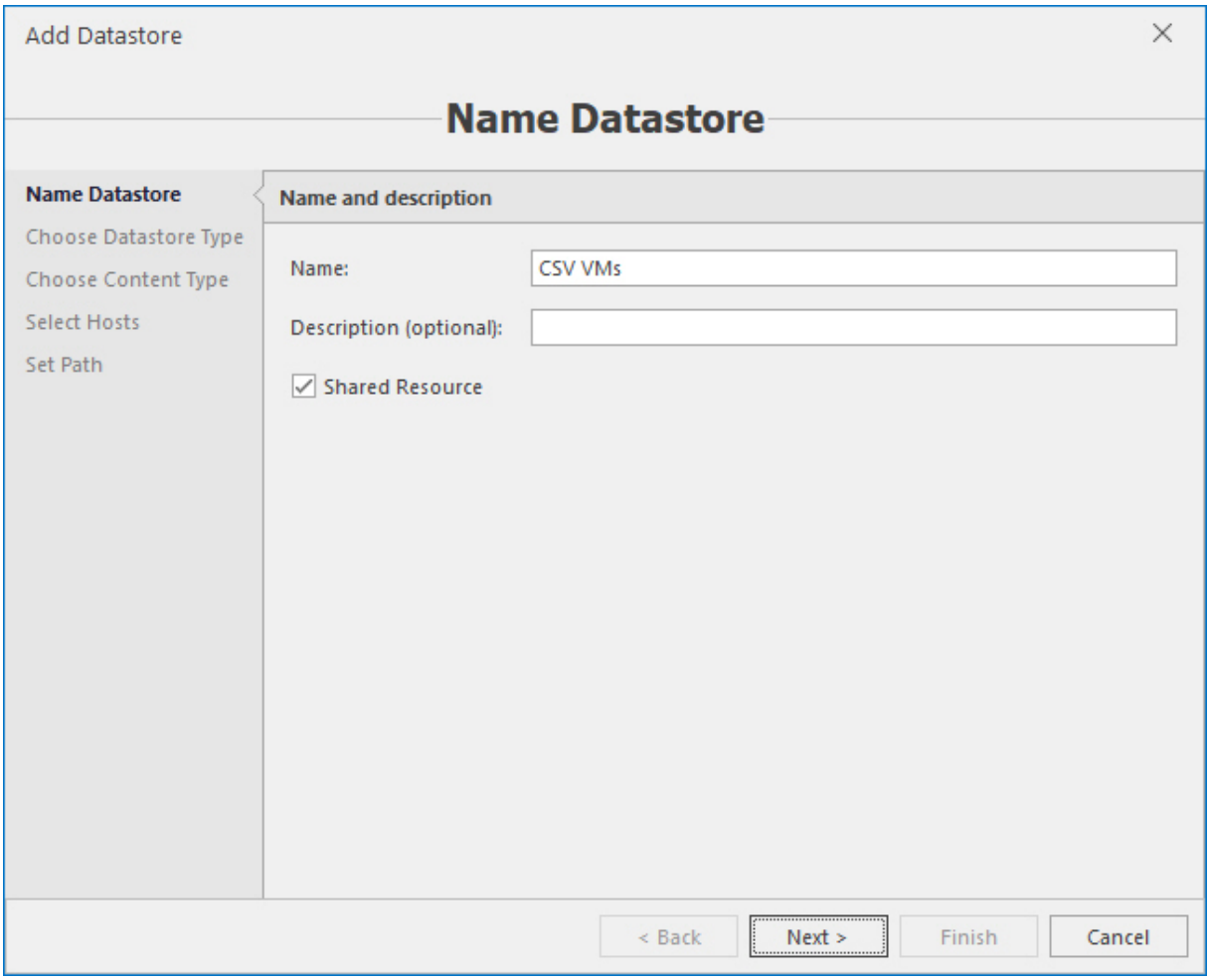


Datastores can be added manually via the **Add datastore** wizard or automatically by the **Run storage discovery** wizard.

Adding datastore

To add a datastore manually, click the **Add datastore** button on the main ribbon.

Define the datastore name and description.

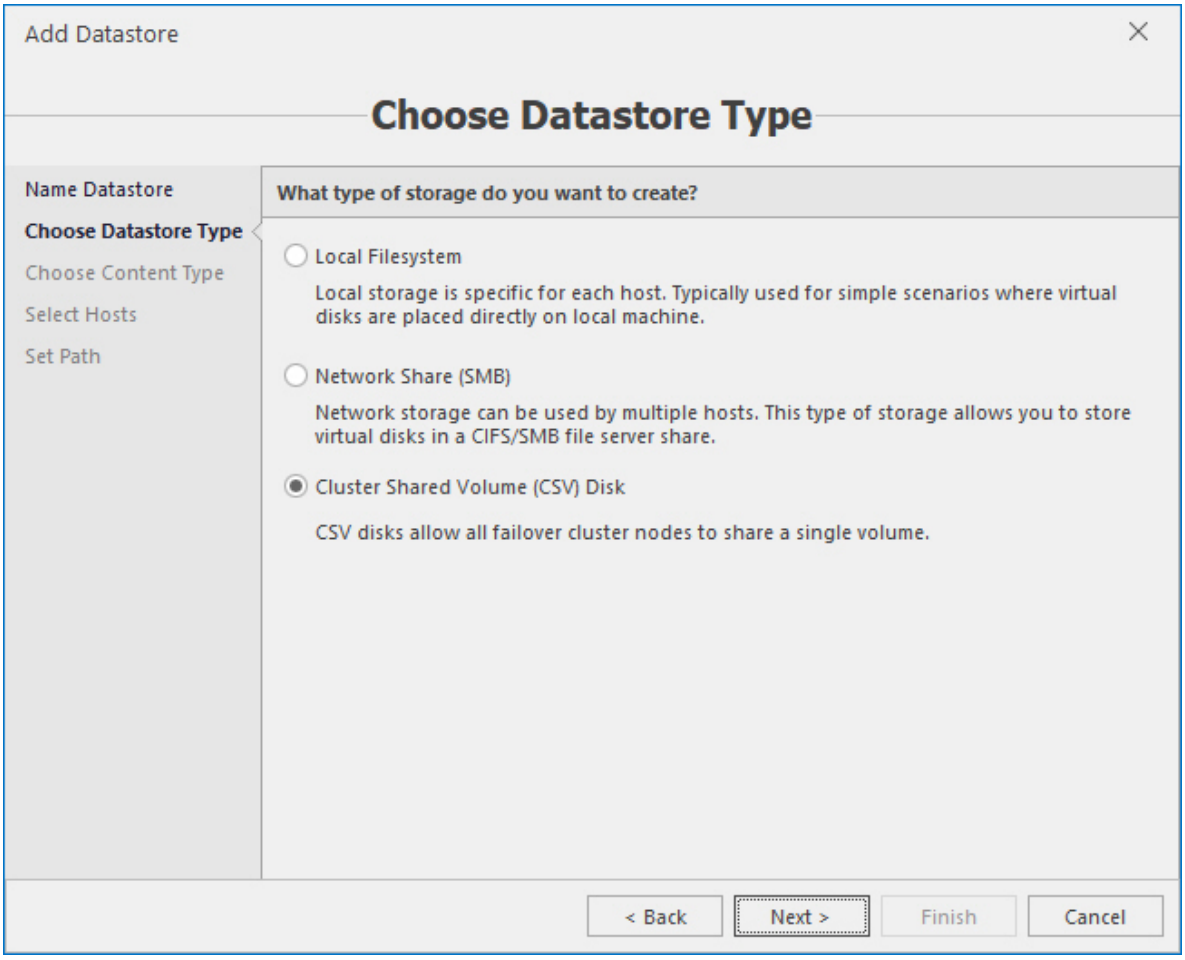


Enable the **Shared resource** option to allow this storage to be visible/available for all tenants. Otherwise only global users will be able to see it (in accordance with permissions as well).

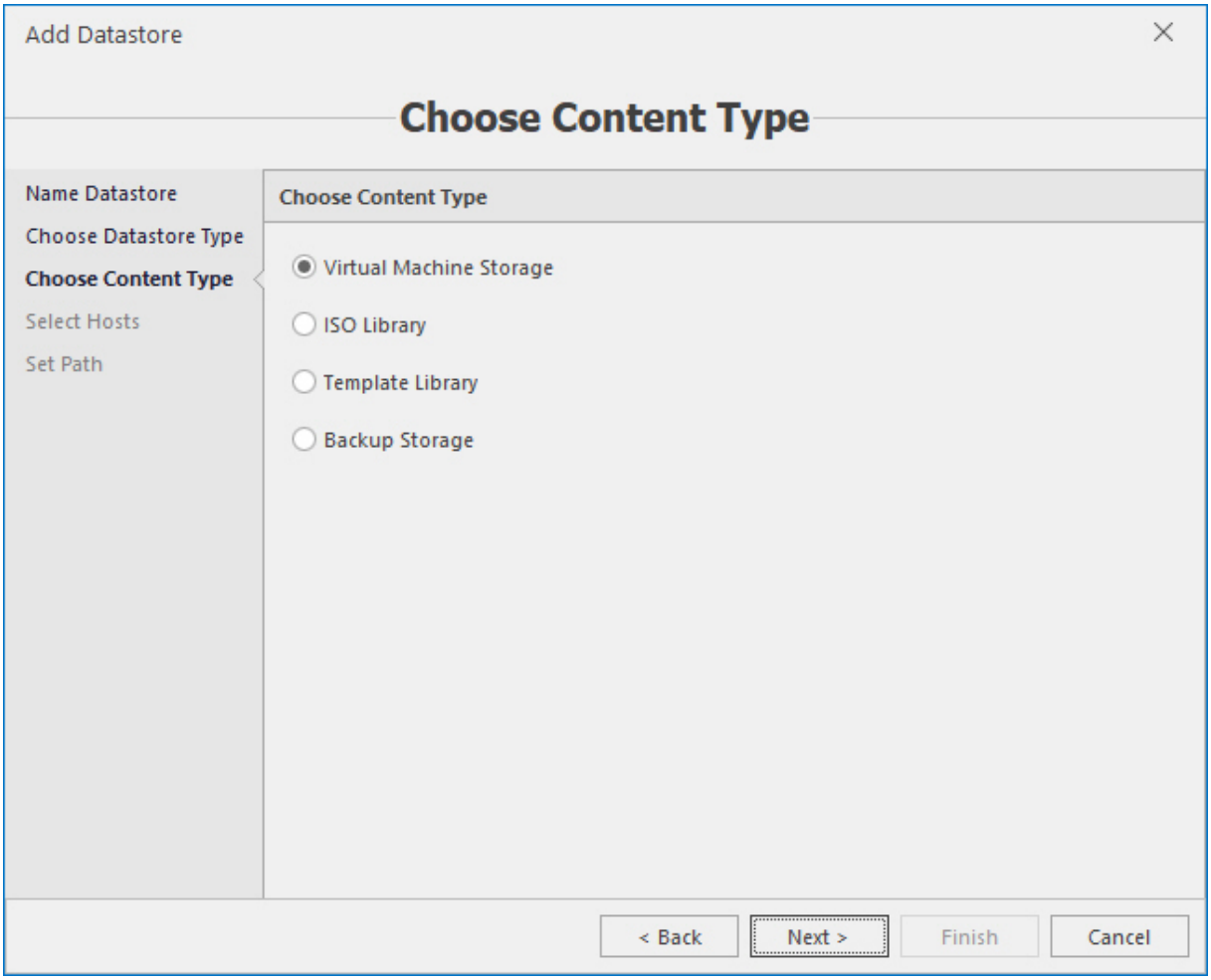
Acronis Cloud Manager supports 3 types of storage:

- **Local filesystem** – specific for a host. Typically used for simple scenarios where virtual disks are placed directly on local server.
- **Network share (SMB)** – can be used by multiple hosts. This type of storage allows to store virtual disks in a CIFS/SMB file server share.

- **Cluster shared volume (CSV) disk** – allows all cluster nodes work with the same storage.



Choose content type:

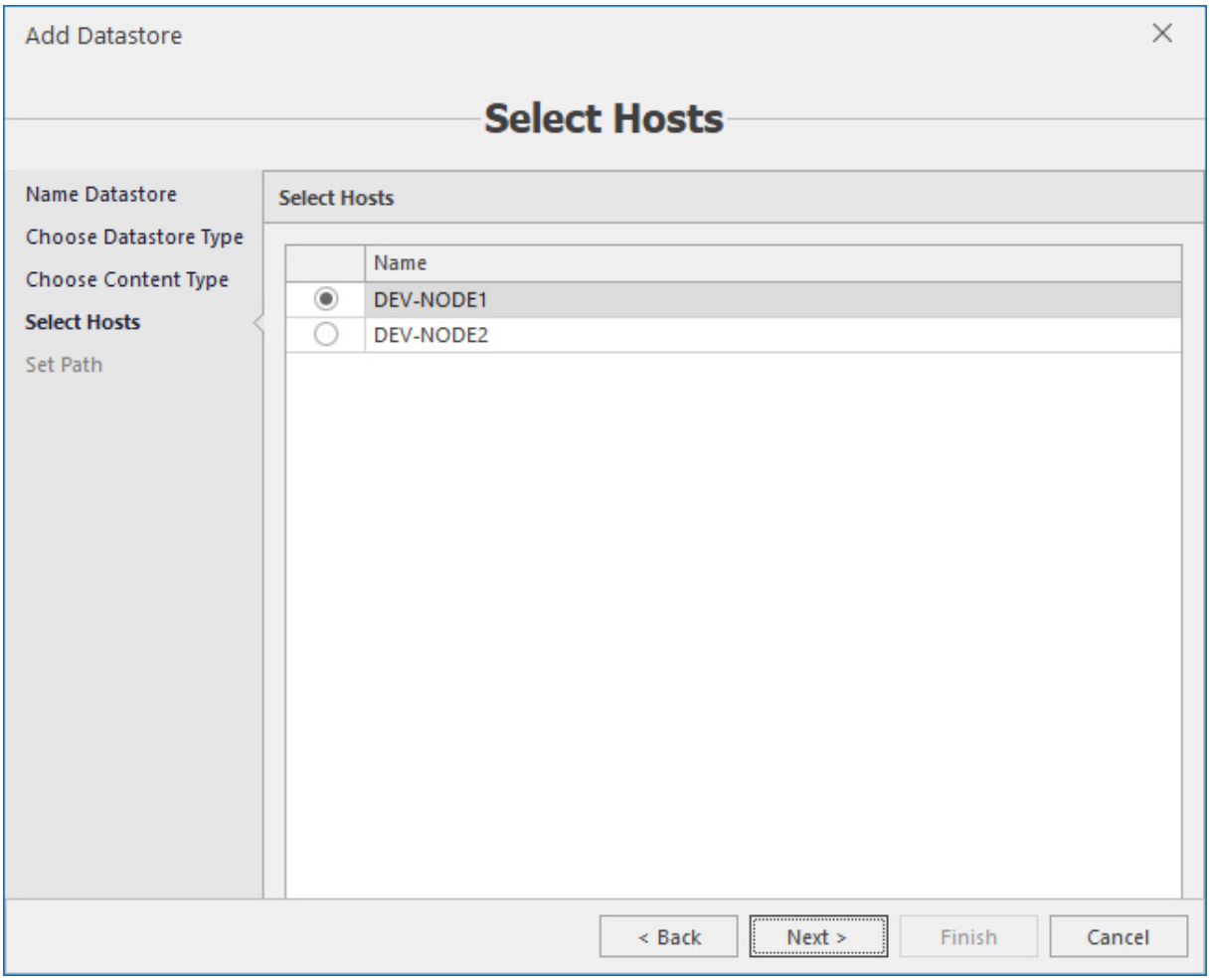


Note

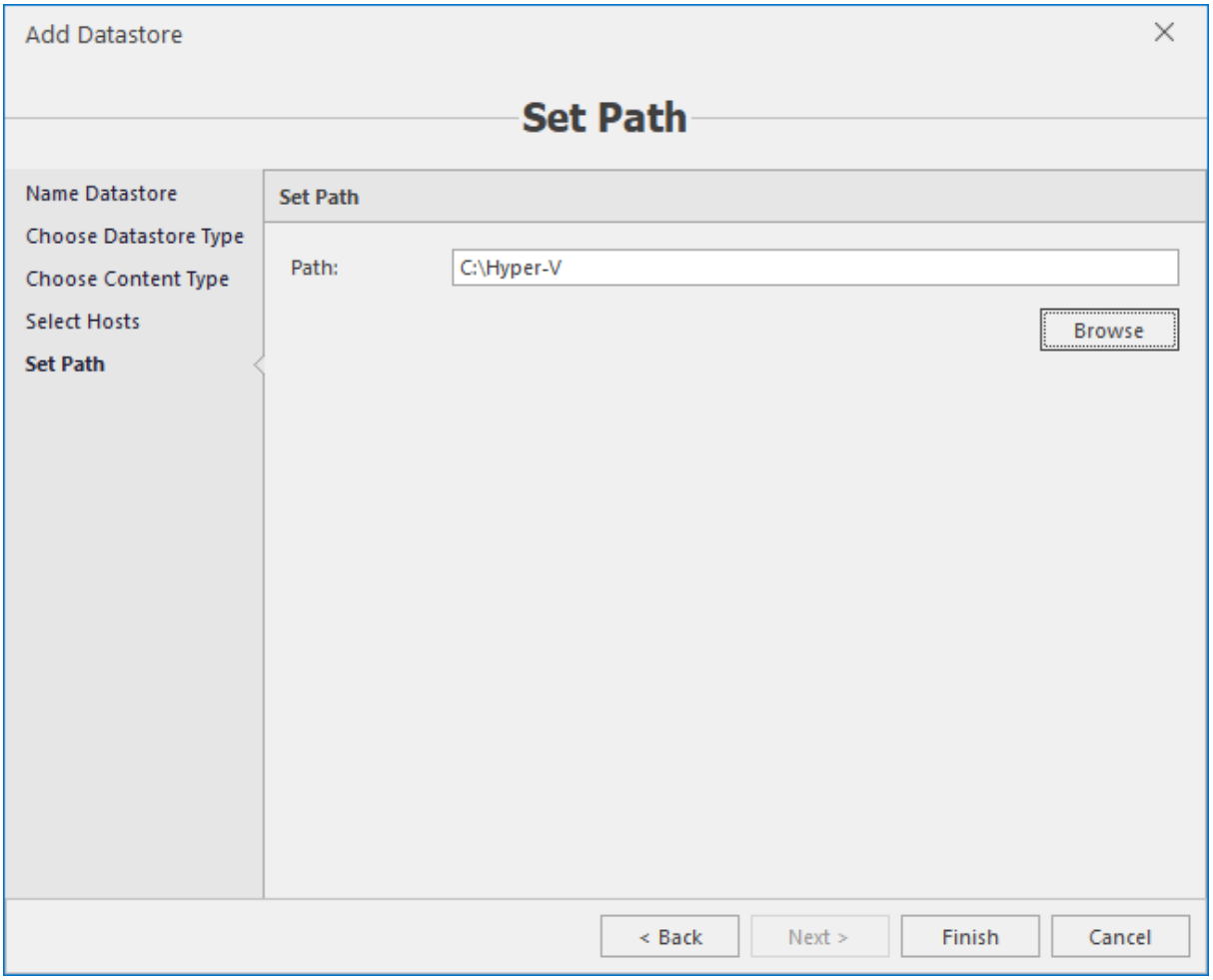
Datastore locations will be split by content to avoid disorder. Only matching locations will be available for selection to each content type. Depending on a storage type selected, next steps will differ.

Local filesystem

For the local filesystem type select the Hyper-V host where the datastore will be located. Then click **Next**.

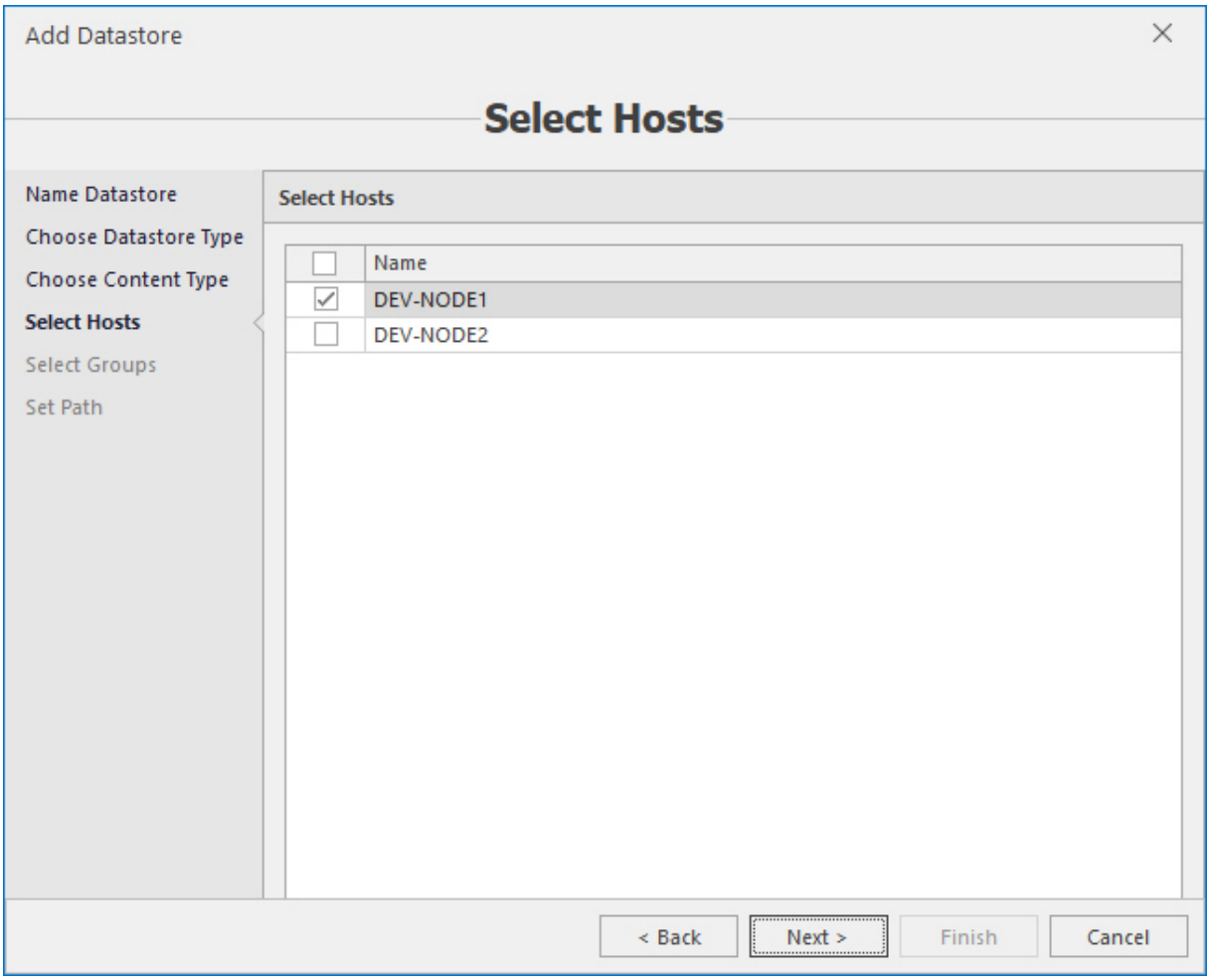


Type the path to the folder on the local file system of the selected server or click **Browse** to select the path, and then click **Finish**.

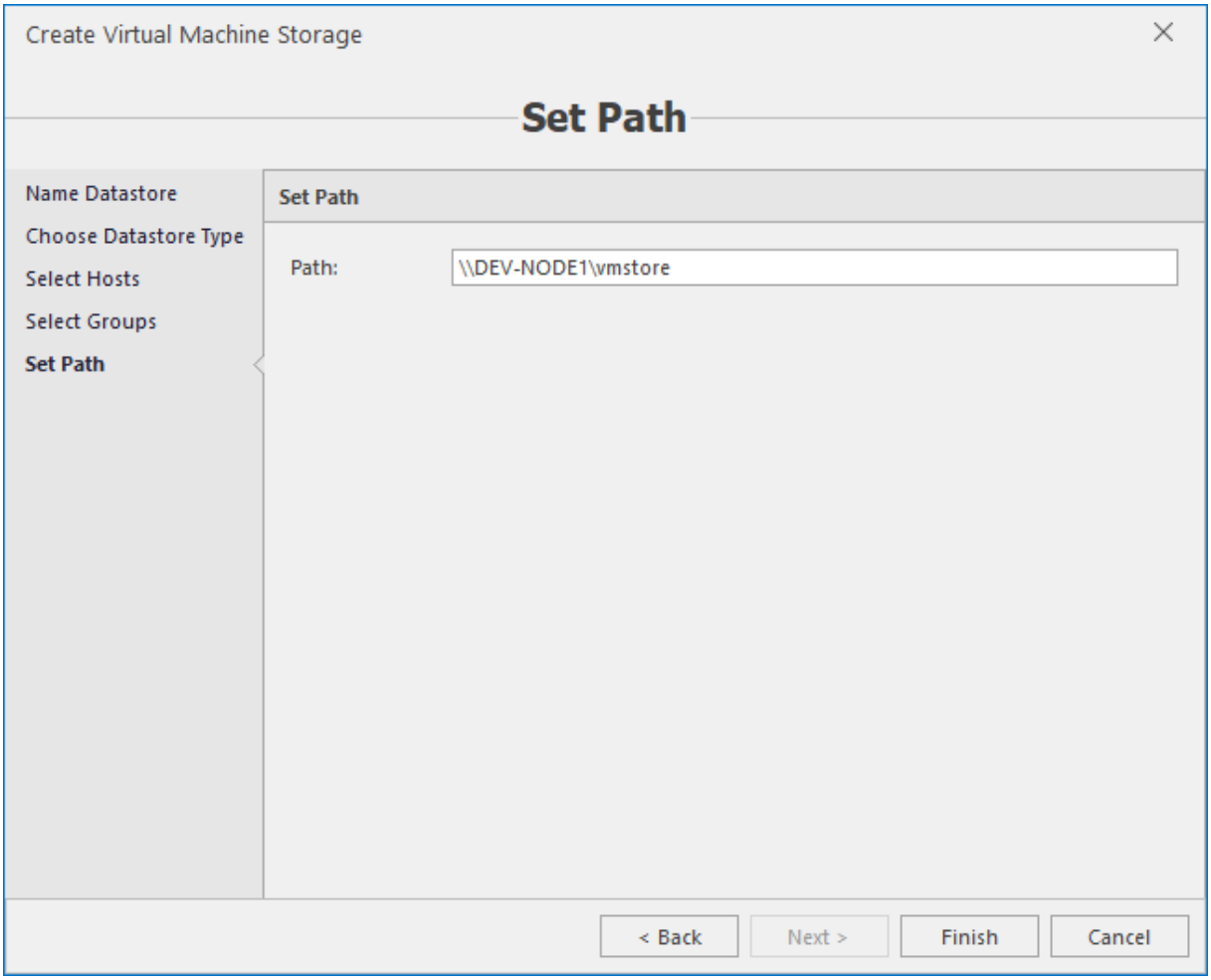


Network share

For the network share type enable host(s) that will have access to this datastore. Then click **Next**.

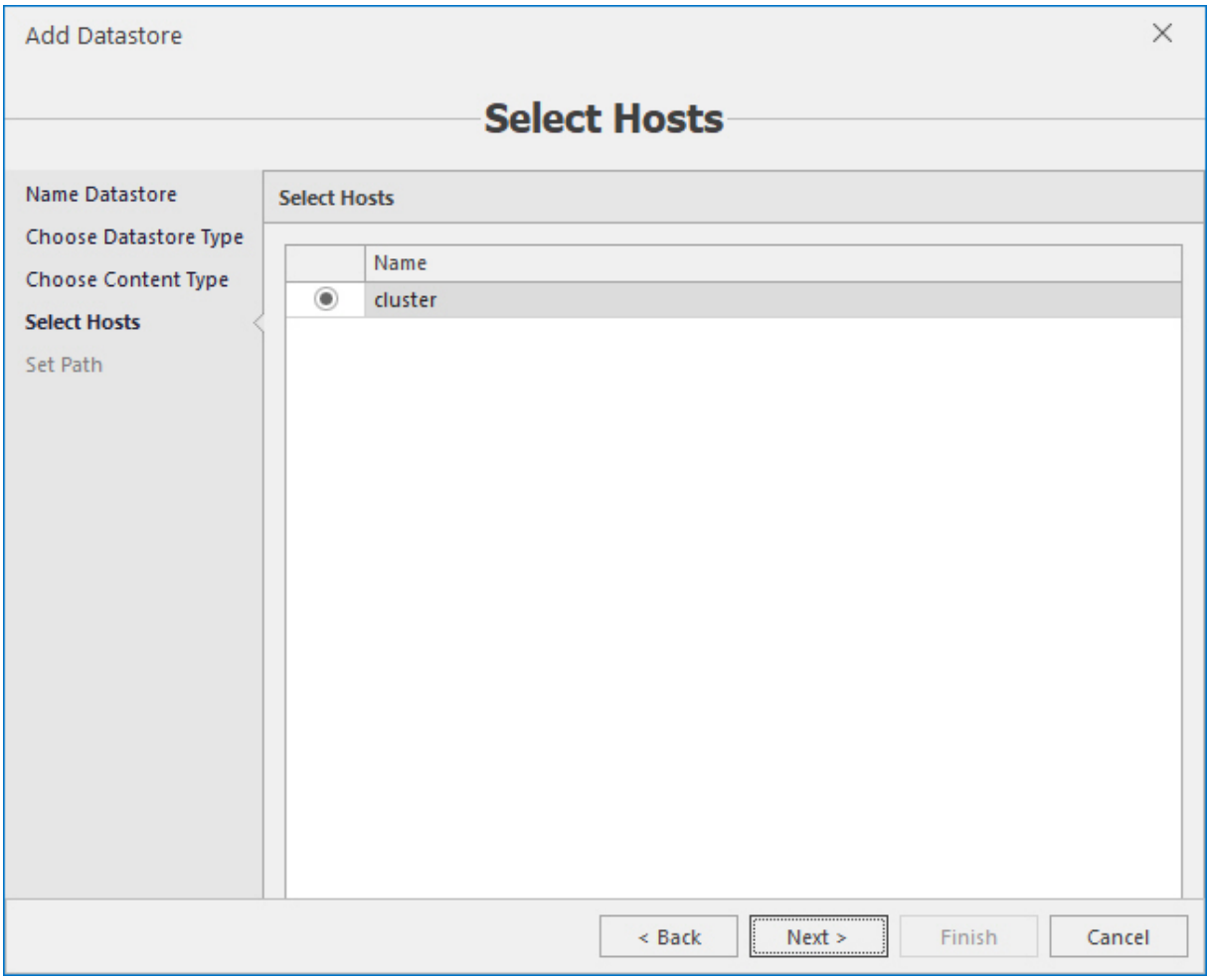


Type the path to the folder on the share using UNC format and then click **Finish**.

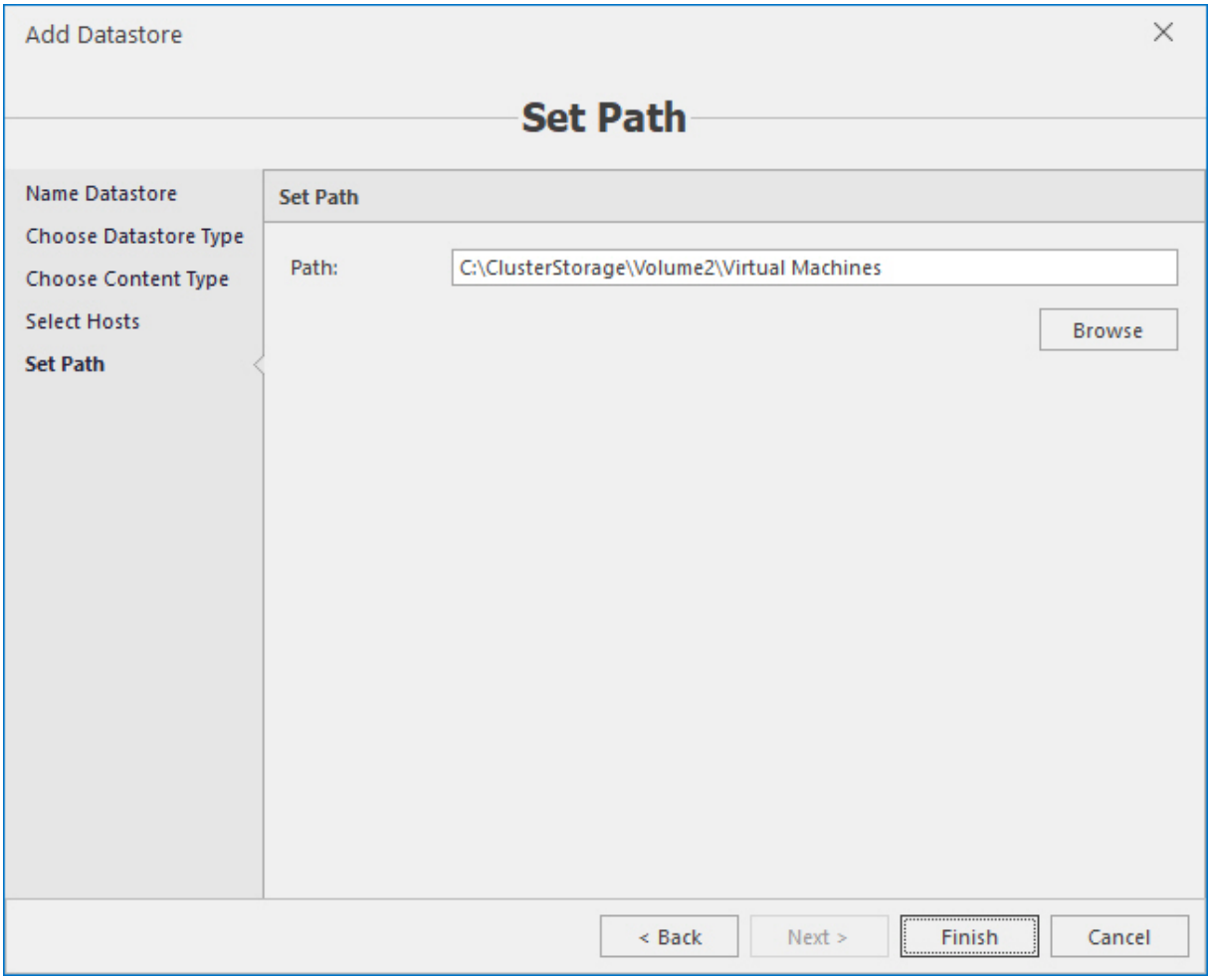


Cluster shared volume

For the CSV type select the cluster.

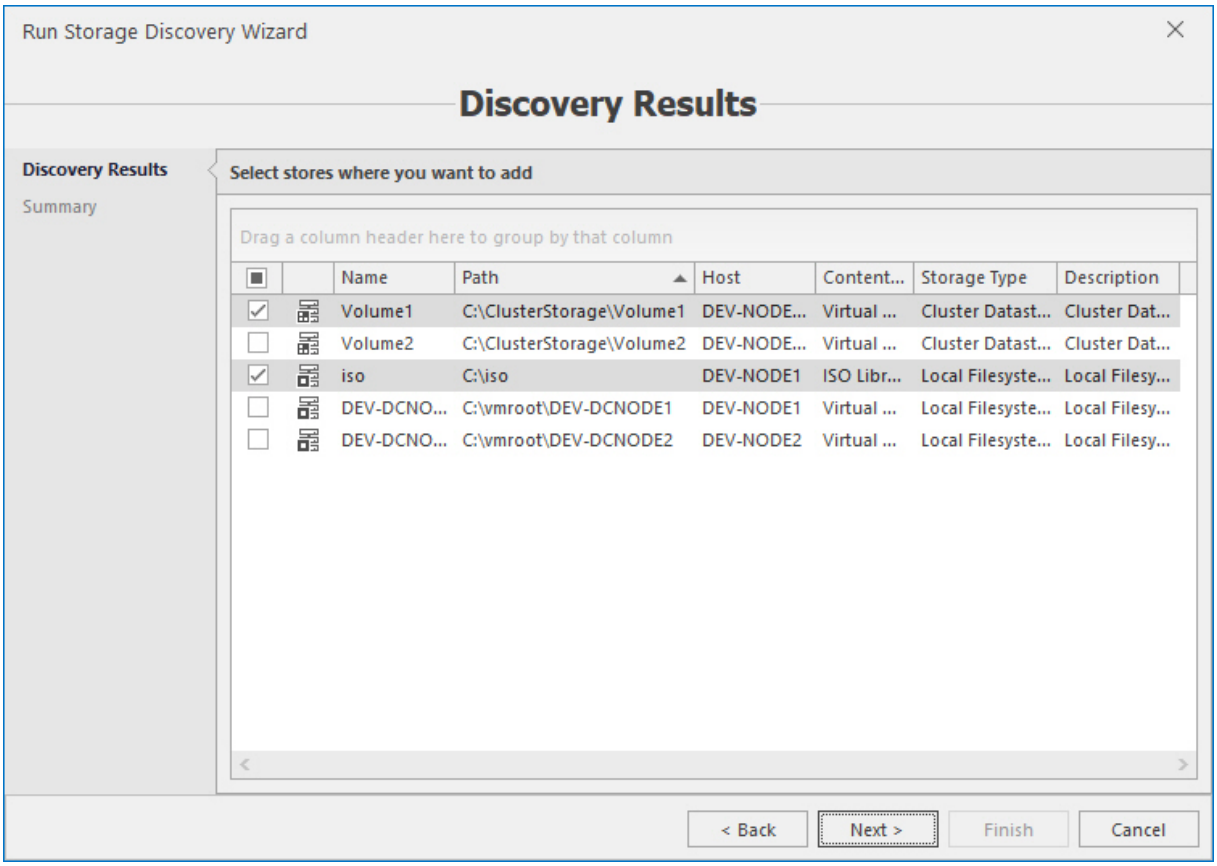


Type the path to the storage or click the **Browse** button to select the required folder with the path.

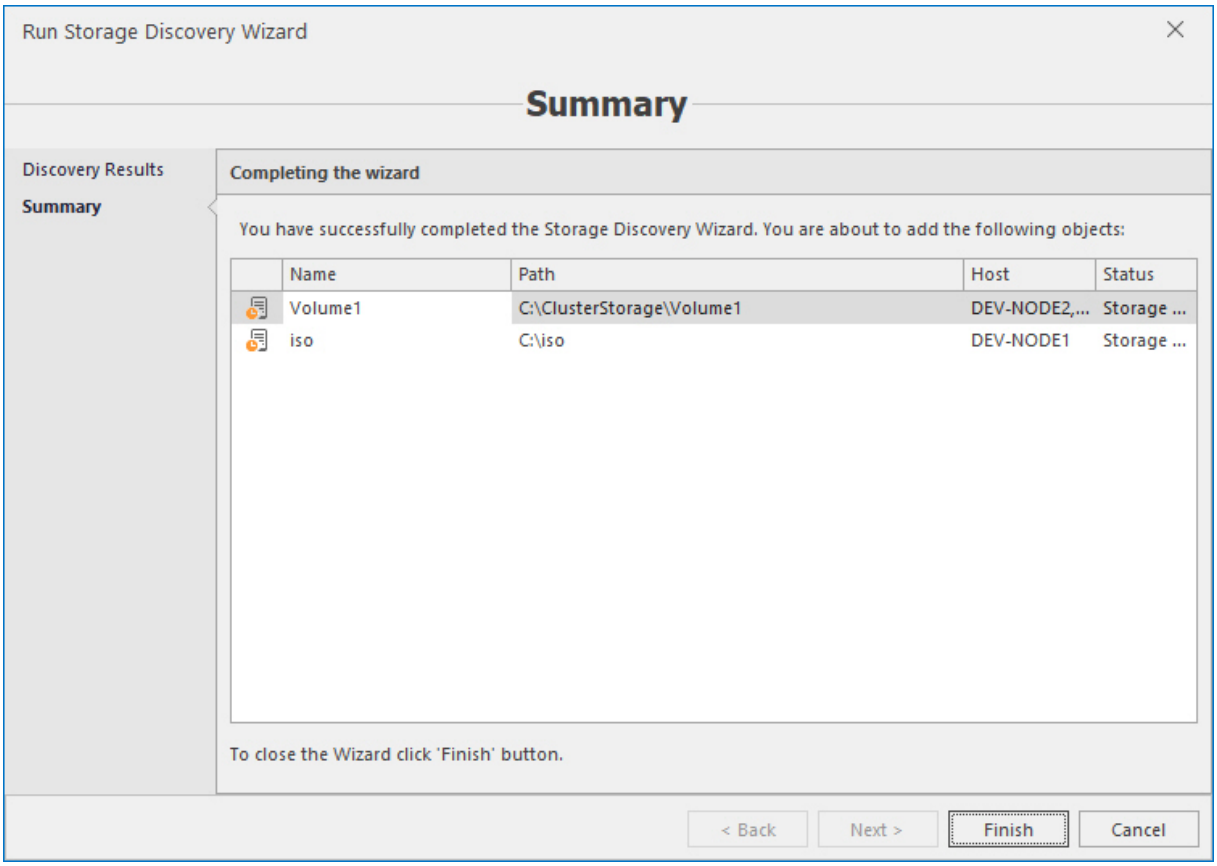


Running storage discovery

To evoke storage discovery, click the **Discover datastore** button on the main ribbon. The wizard will immediately start available storages discovery and then shows results on the first page, in accordance with its content:



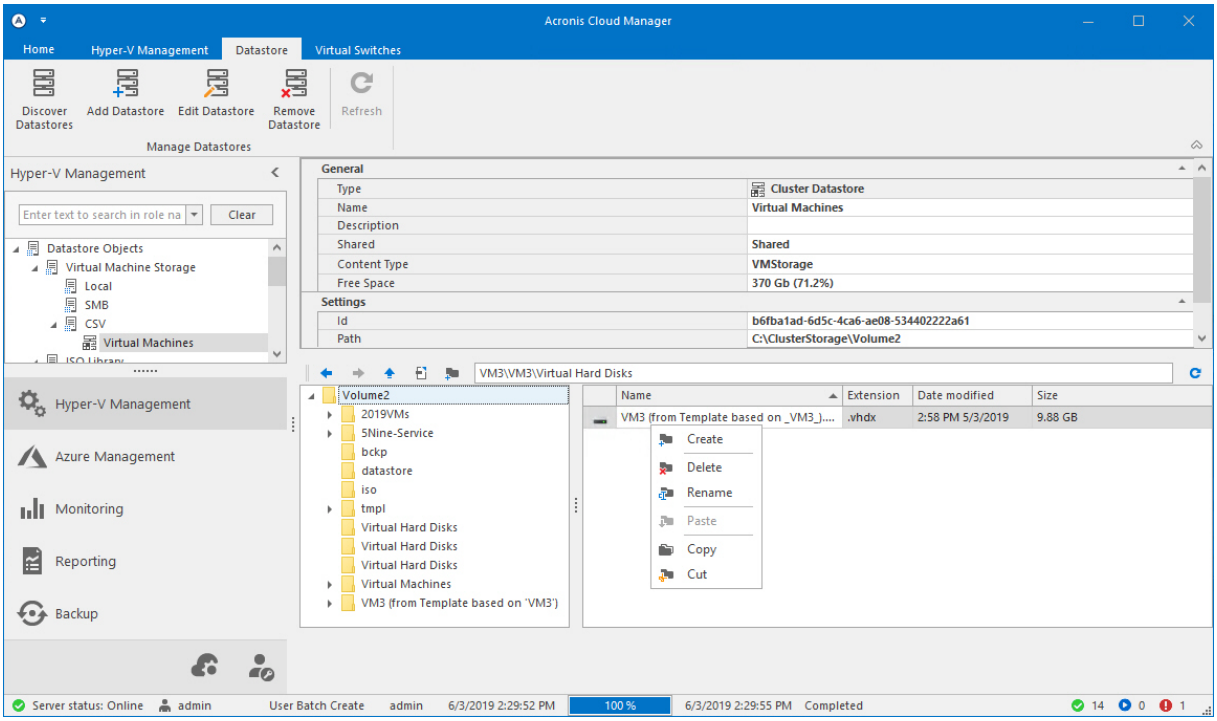
Select locations to add to the datastores and click **Next**.



Review summary and click **Finish** to complete adding the selected locations to the datastores. Added locations will be automatically sorted in accordance with its content and storage physical types.

Editing and removing datastore

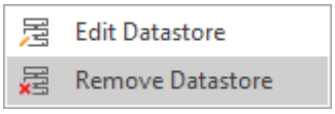
When a datastore is created you can navigate through its content. Also, for your convenience, there is an ability to perform operations on physical folders on the disk directly from Acronis Cloud Manager user interface – create, delete, rename and copy/move actions are available just like in standard file explorer.



To edit the datastore select it in the object tree and click the **Edit datastore** button on the main ribbon or the same command using right-click menu:

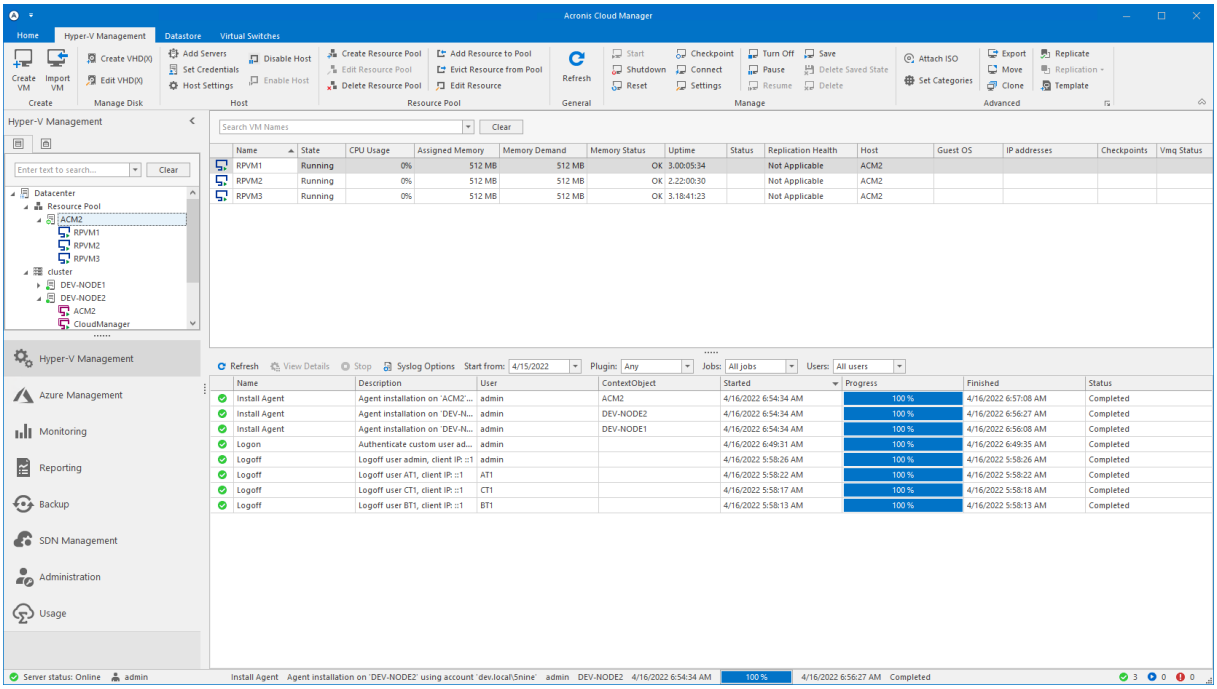
Then apply any required changes in the same way as when registering the datastore in the **Edit datastore** wizard.

To remove the datastore select it in the object tree and click the **Remove datastore** button on the main ribbon or the same command using right-click menu:



User interface

The user interface of Acronis Cloud Manager is designed to let you quickly find commands that you need and perform necessary Hyper-V management and other tasks.



There are the following main parts of user interface:

- Navigation pane.

  Navigation pane consists of 2 parts: objects tree and plugin selector. You need to select necessary plugin and then work with the tree to select an object.
- Ribbons and tabs

  Operation commands are organized into logical groups and collected under tabs on the ribbon. The ribbon is displayed at the top of the main application window. Commands for operations with items are also available in the context menu.
- Data area.

  Data area usually shows text or graphical information about object selected in the objects tree.
- Status bar.

  Status bar shows management server status and user name under which console is started.
- Jobs pin panel.

  Jobs pin panel shows status, progress and other information, related to jobs. Please, see the next chapter for details.

Job management

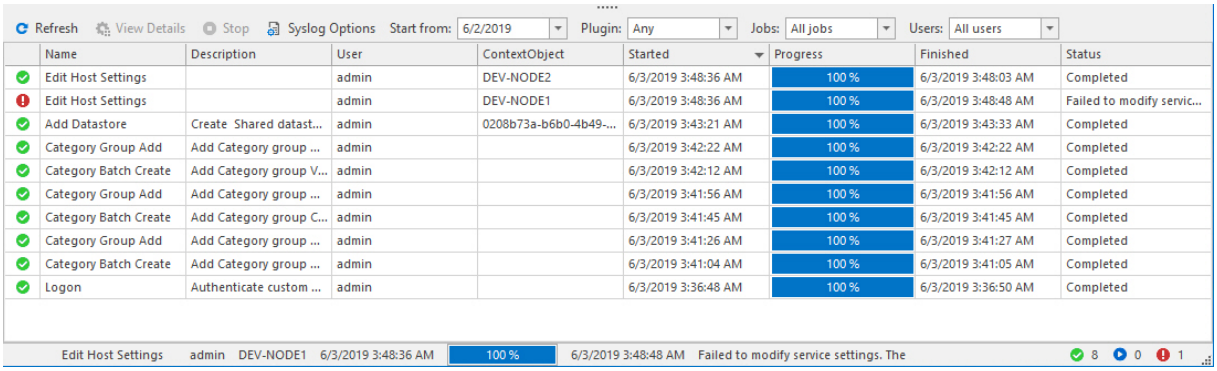
All processes, happening in Acronis Cloud Manager, are represented as jobs.

To see the detailed jobs information, click the bottom bar of the screen, where the status of the last job is shown. The jobs dock/pin panel will be shown at the bottom of the main window. Next click will collapse the jobs panel back.

Job list

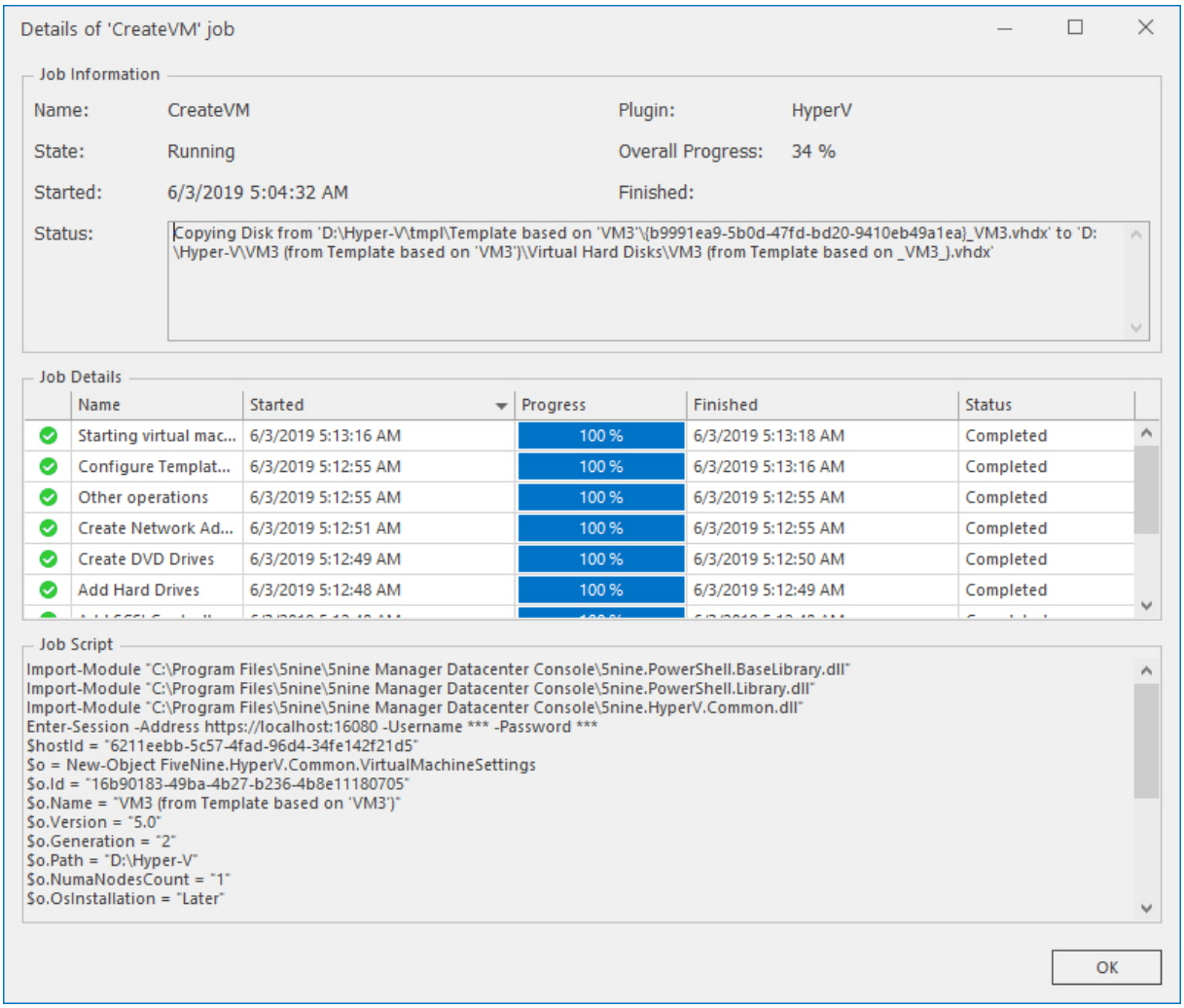
The list of jobs can be filtered out and you can stop or view details for the selected job.

Job details contain PowerShell script, which implementation is like a job command.



To do any action with the job, select it in the list and use the corresponding button on the command ribbon. The filter is available to select jobs by date and/or by plugin.

To view the job details, select the required job and click the **View details** button:

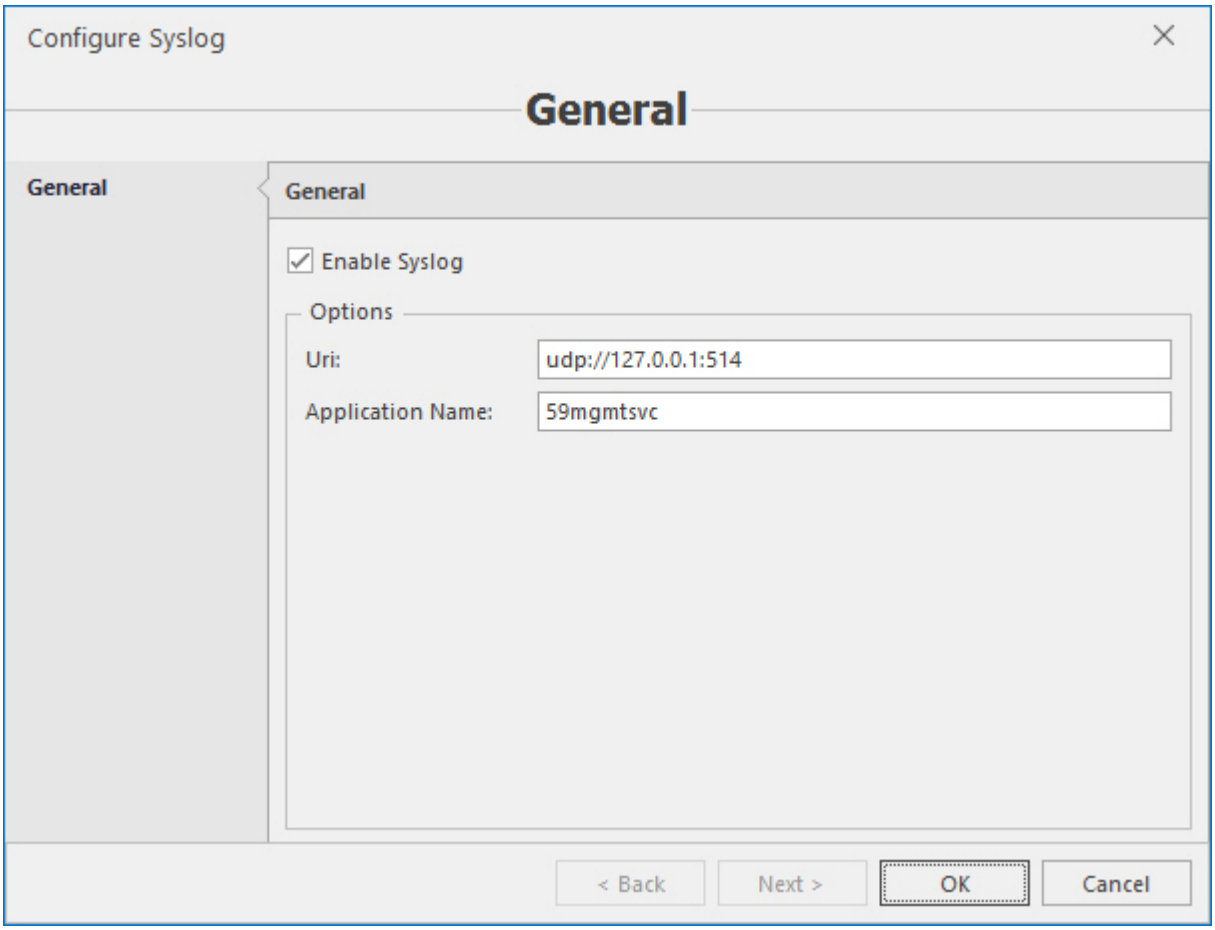


There is the detailed information about the job in the upper block – name, status, related plugin, progress and period. Middle block contains steps that are taken as the job is executed. Lower block contains the PS script that is run to complete the job.

Syslog integration

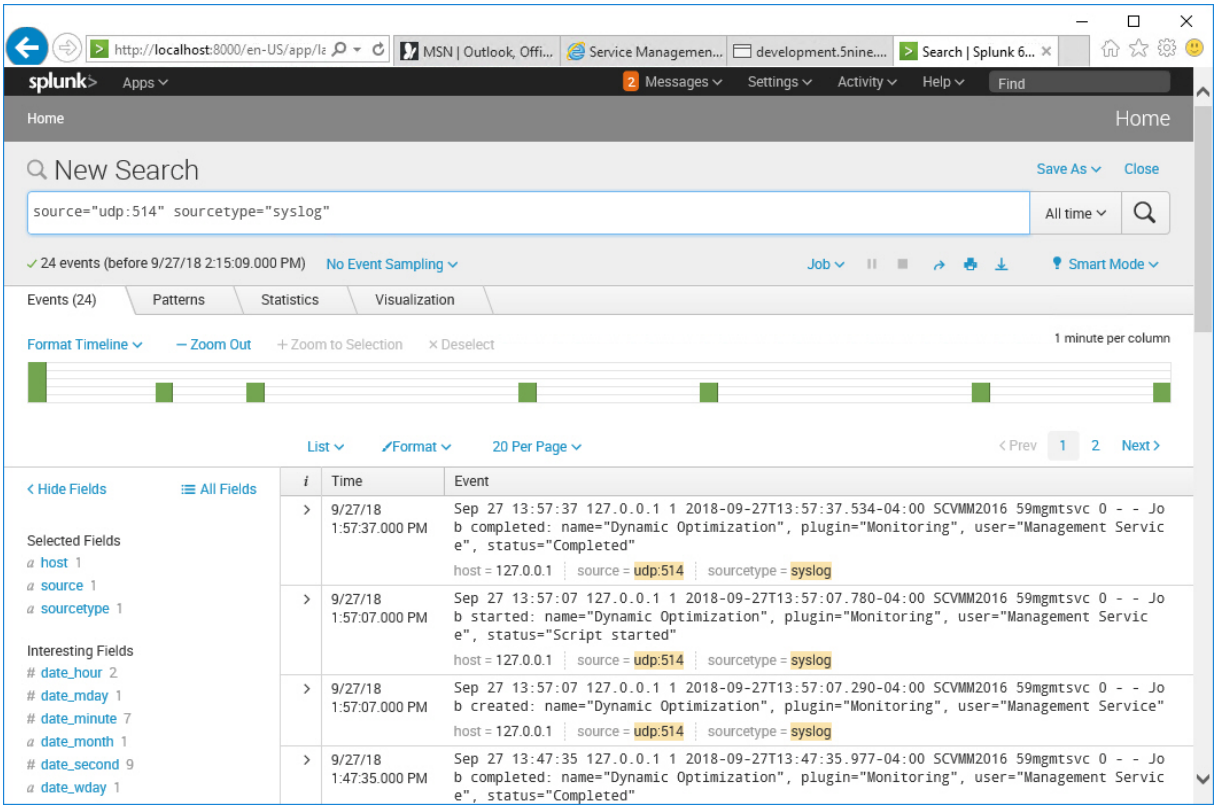
Jobs and event alerts can be exported to the external syslog server. Syslog server should be installed and properly configured in the environment in advance. RFC 5424 header is supported.

To set up syslog export, click the **Syslog options** button on the main ribbon.



To enable export jobs to the external syslog server, enable the **Enable syslog** checkbox. Then enter the syslog server URI in **udp://<syslog server IP address:port>** format. Default value is **udp://127.0.0.1:514**. Specify the application name – default value is **59mgmtsvc**, leave it as it appears. Click **OK**.

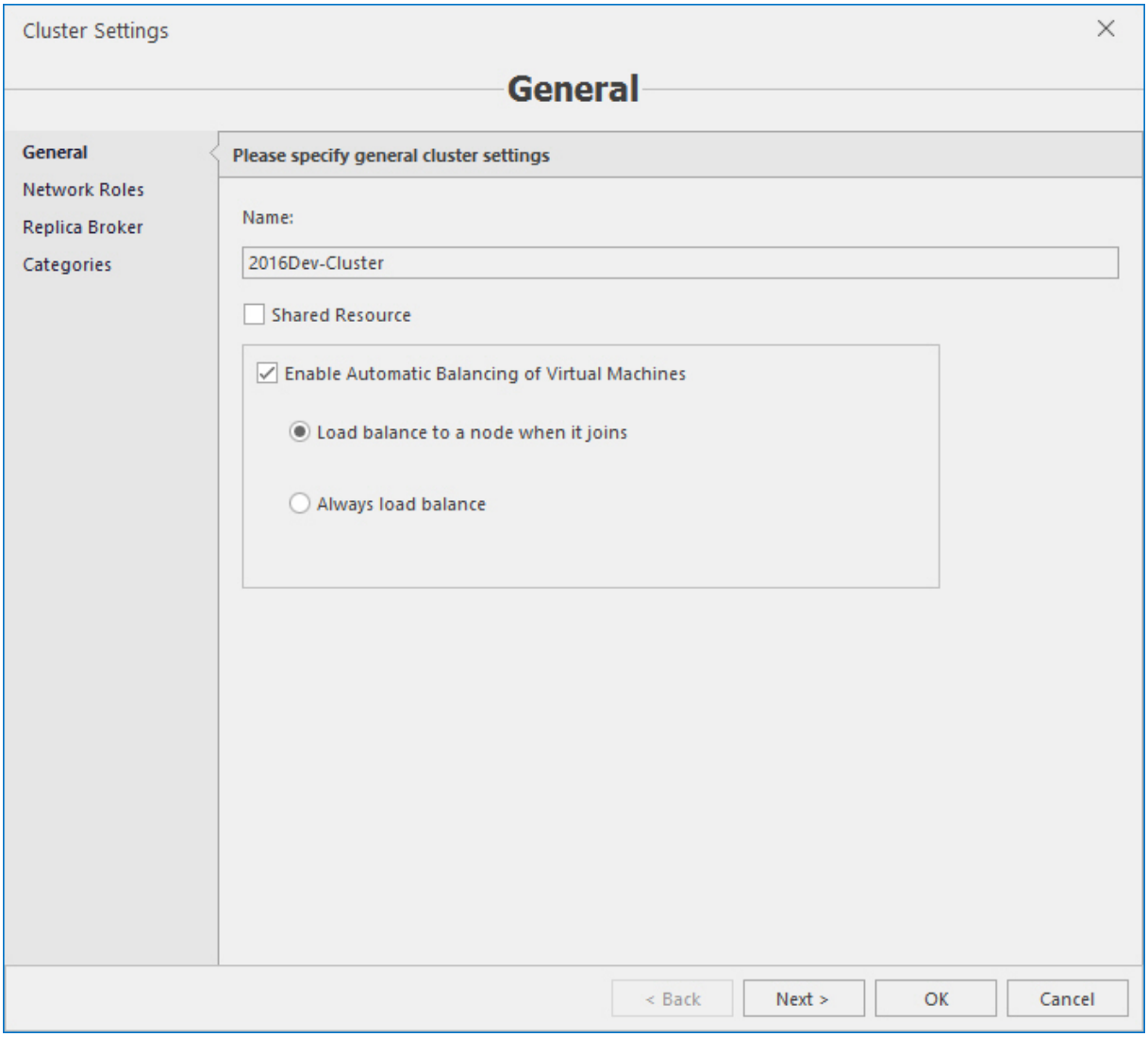
Now you may view and use syslog records as needed. Example, Splunk syslog output:



Hyper-V management

Cluster settings

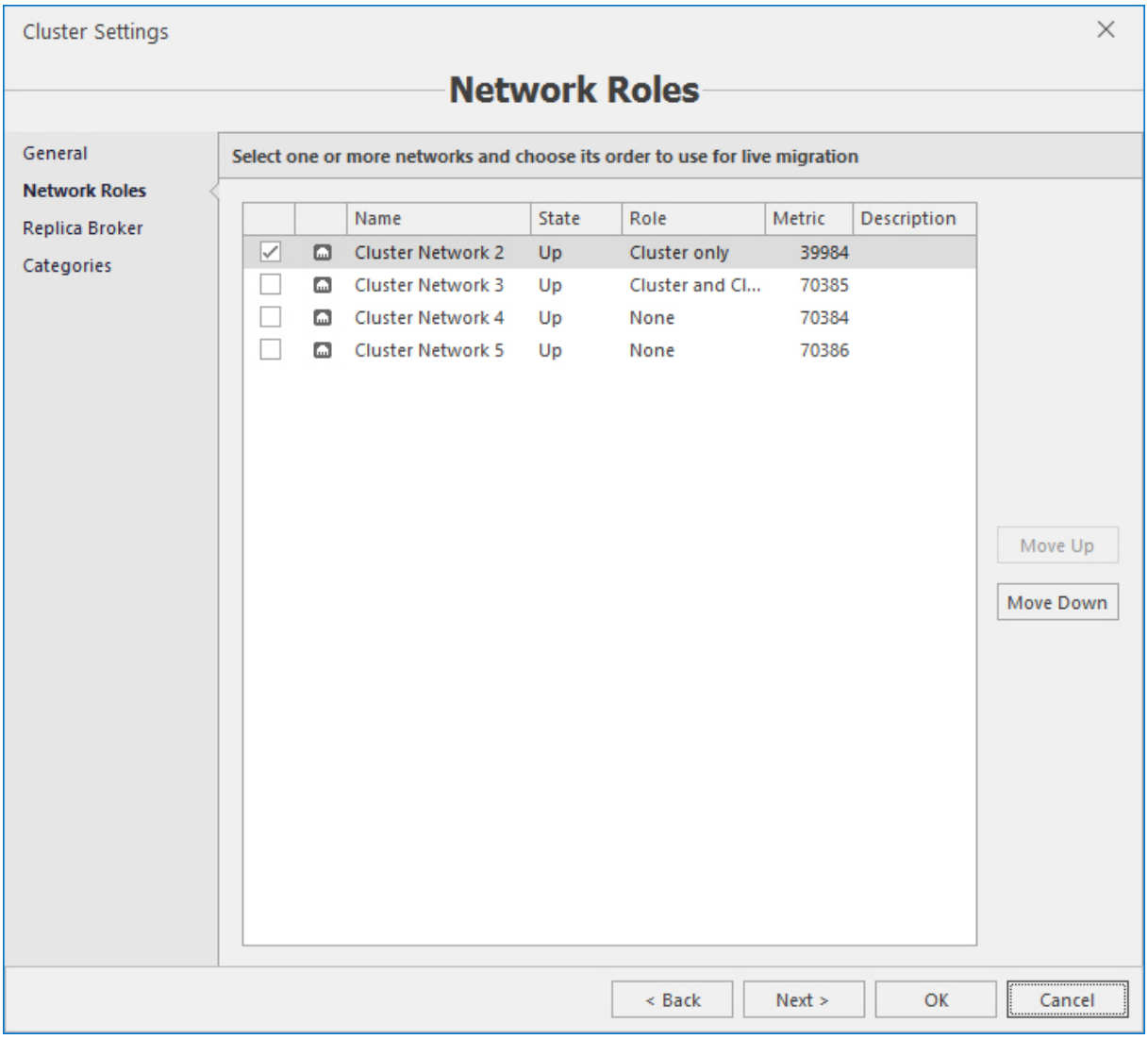
To access the cluster settings, select the cluster in the objects tree and press the **Cluster settings** button in the toolbar or right-click on the cluster name and select the corresponding context menu command.



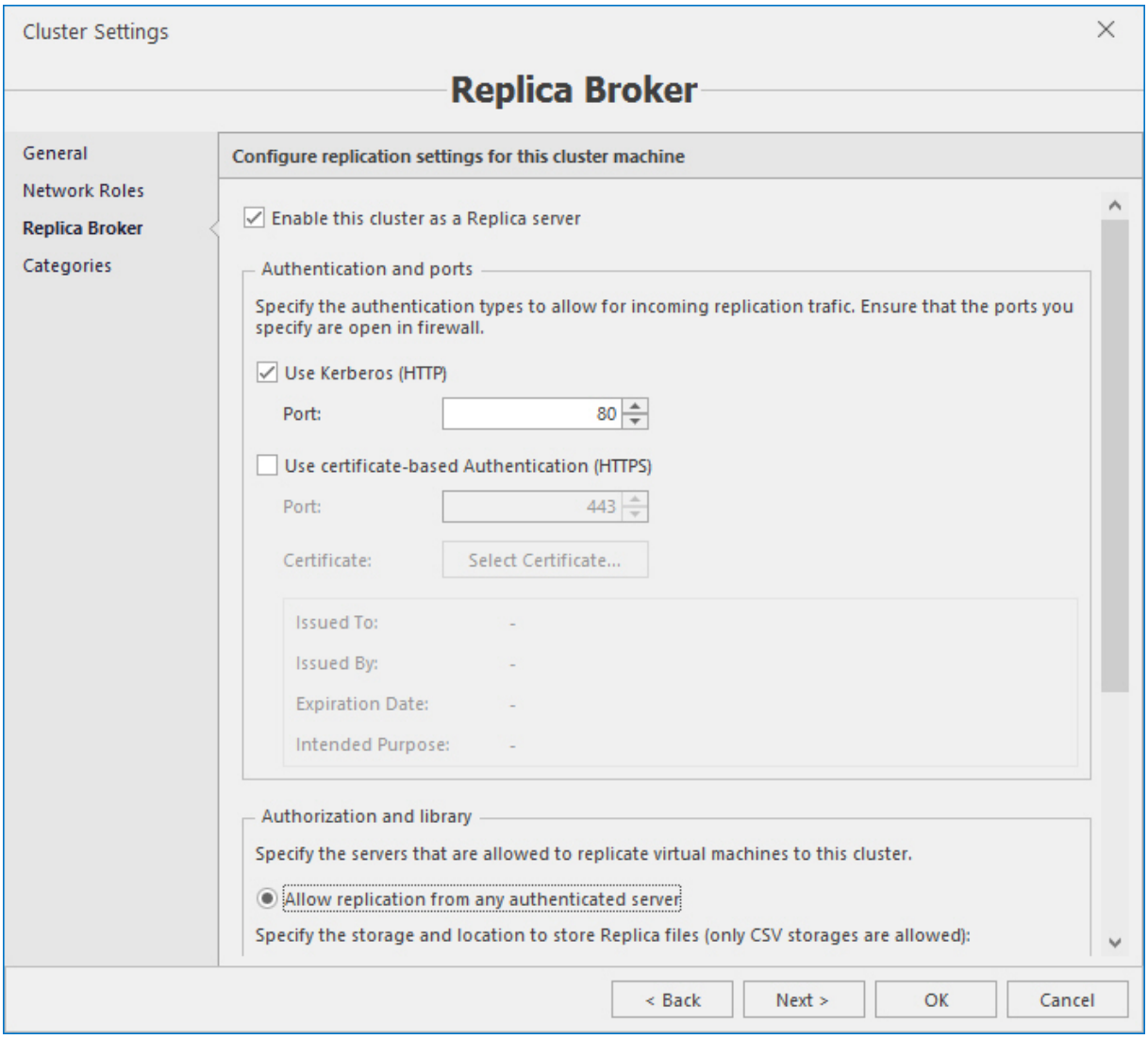
You can choose whether automatic load balancing of virtual machines is enabled or not in the cluster and its mode – always or just when the new node is joined to the cluster.

The **Shared resource** option determines whether this cluster is available for all tenants or just on the global level.

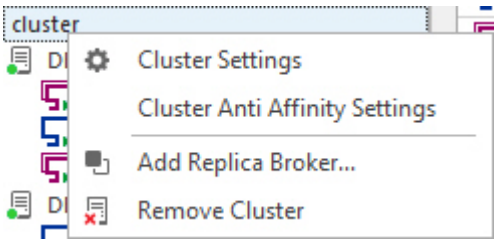
Select networks and their order for live migration.

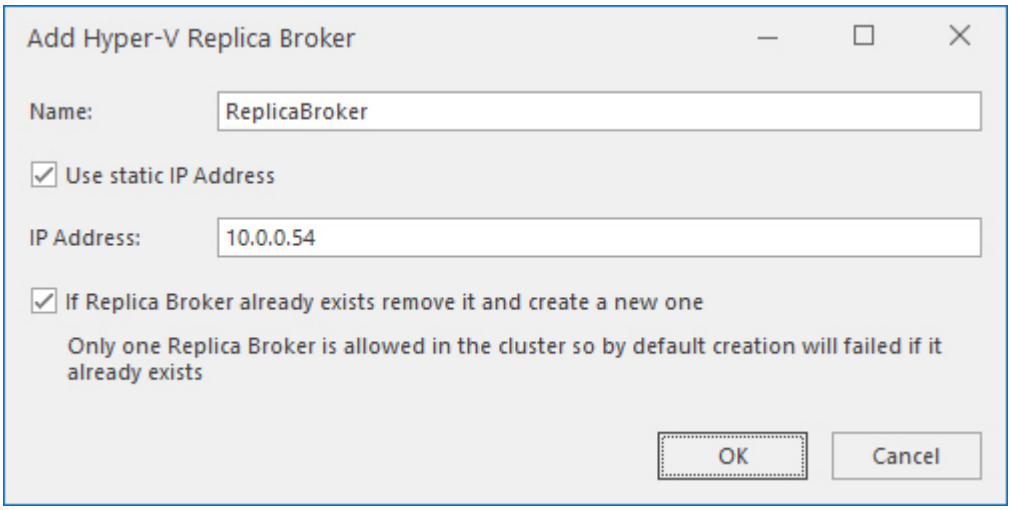


Configure replication settings for the cluster.

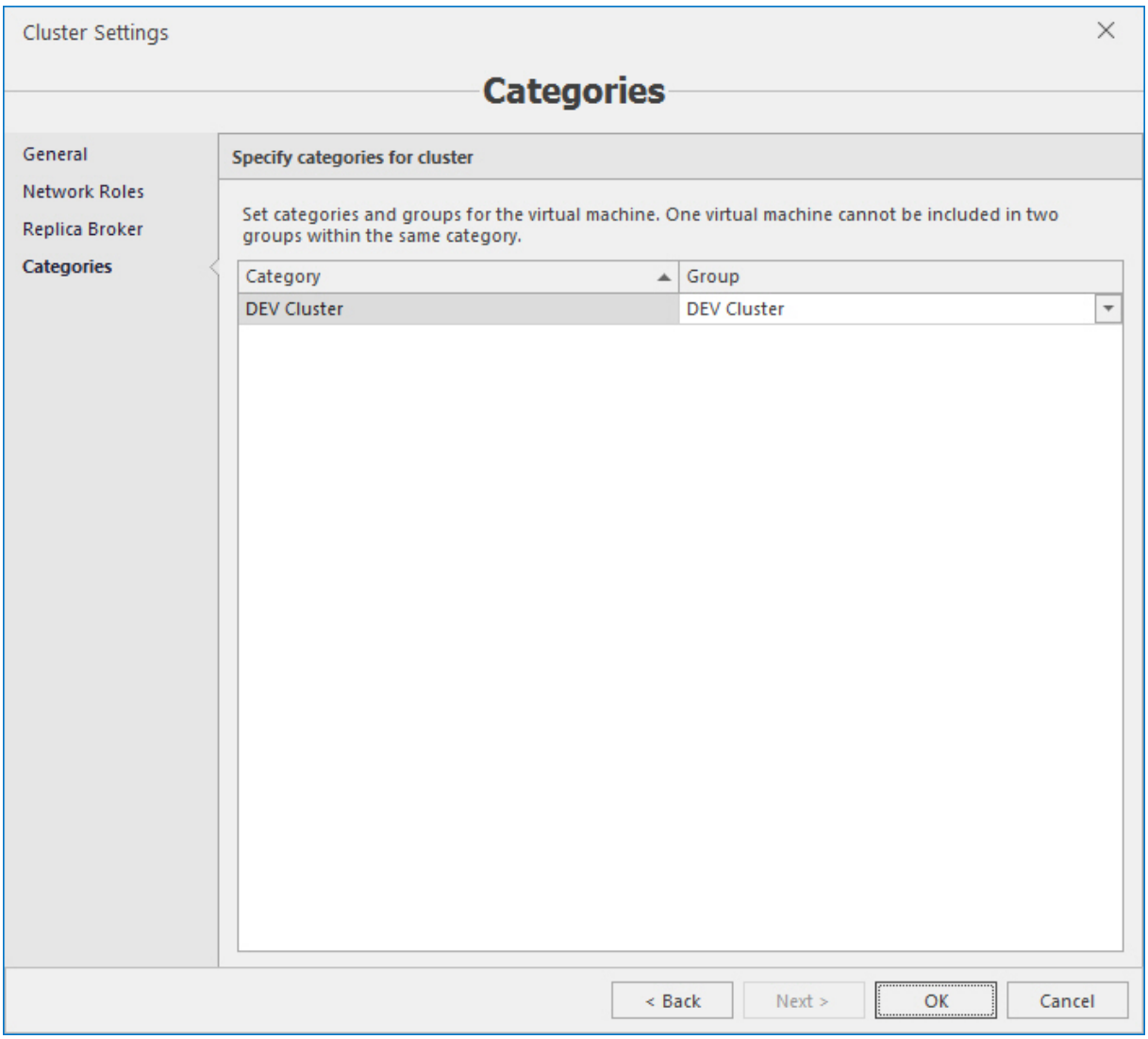


To add the new replica broker, click the **Add replica broker** context menu command and specify its parameters:





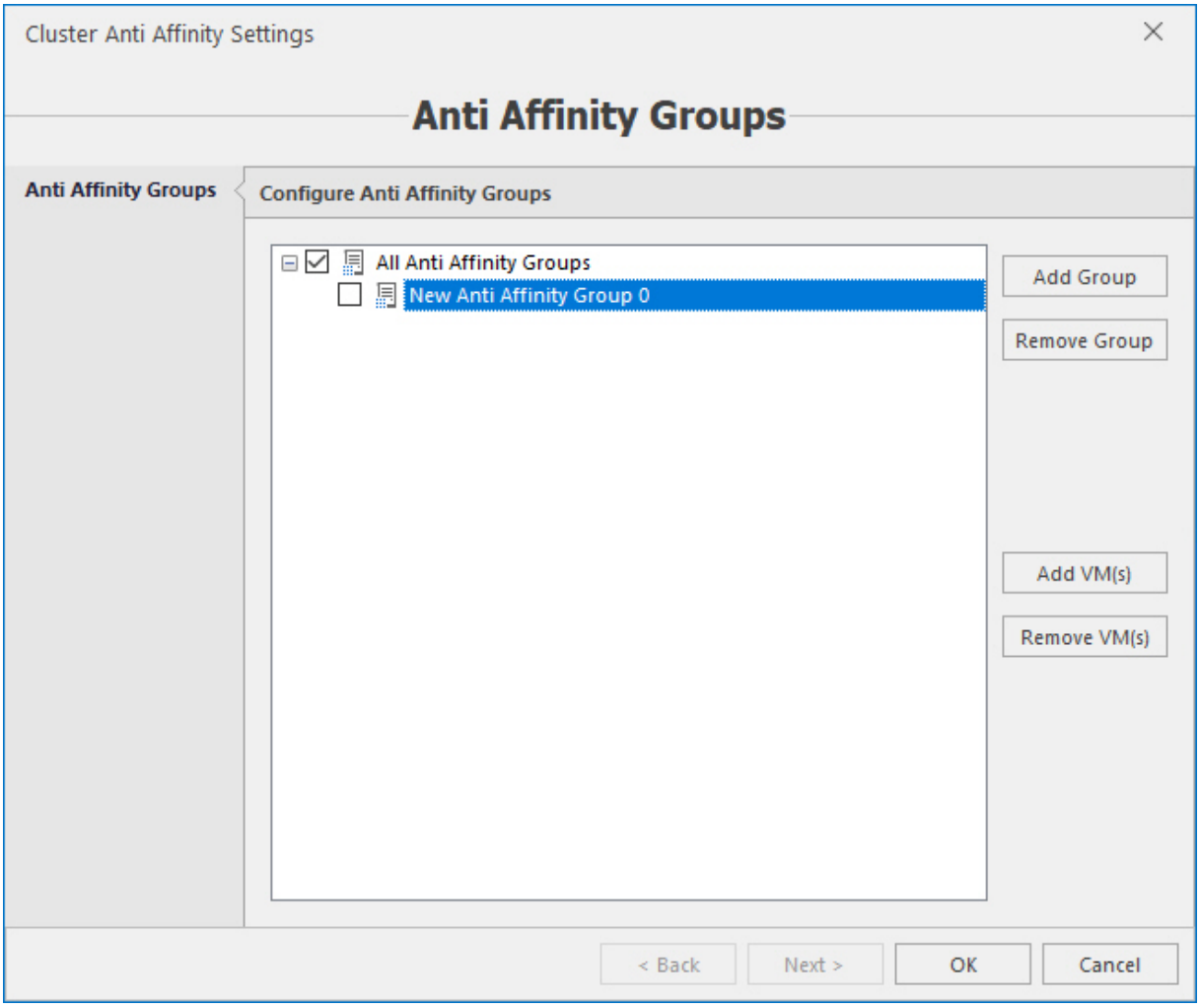
Specify the category and the group to display the cluster in the logical view:



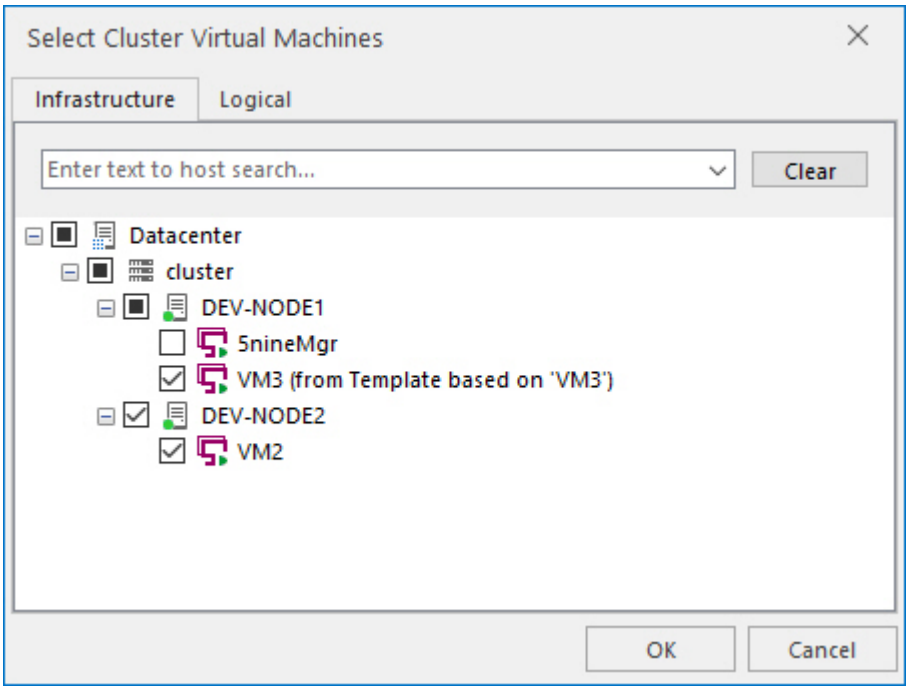
Cluster anti affinity settings

Cluster anti affinity settings are implemented to allow automatic control over HA virtual machines placement during cluster nodes outages in accordance with pre-defined parameters. It works in the following way – HA VMs are selected by user into anti affinity groups. VMs from the same group will be primarily placed onto different active nodes during the outage of one or more other nodes of the cluster (separately from each other) in accordance with technical ability, or, as a last method of lower priority, onto any available node as it happens in usual conditions without anti-affinity configuration.

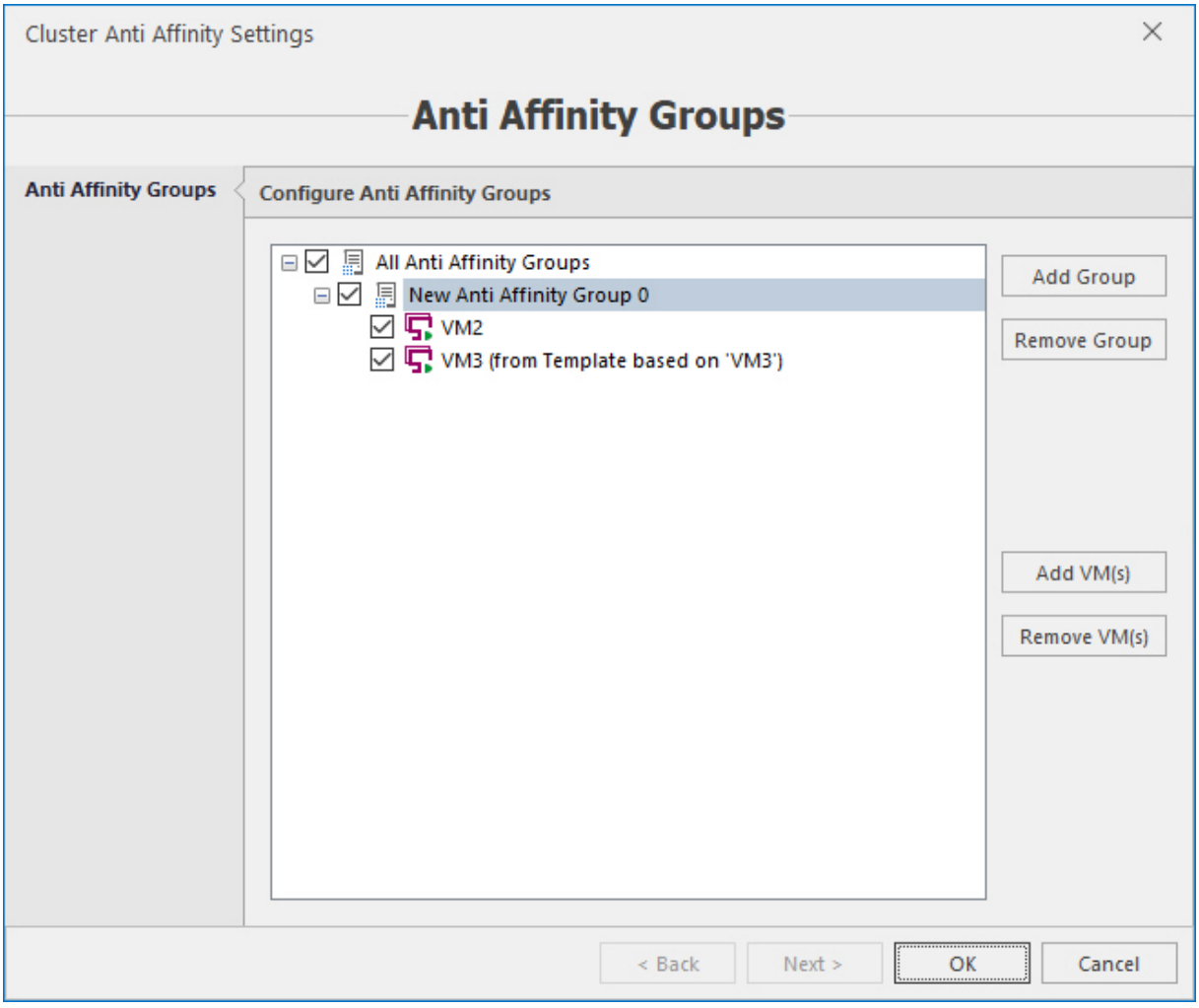
To configure cluster anti affinity settings, click the corresponding context menu command of the cluster and specify parameters in the wizard below:



- Click the **Add group** button to add the new group.
- Select the group and click the **Add VM(s)** button to add HA virtual machines to the group and then click **OK**:



Selected VMs will appear under the group in the tree:



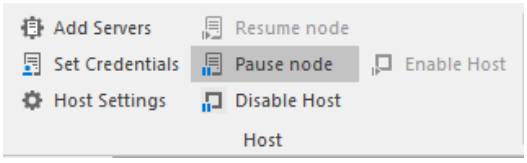
- To remove VM(s) or the whole group, click the corresponding button.
- Click **OK** to save changes and exit the wizard.

Cluster maintenance

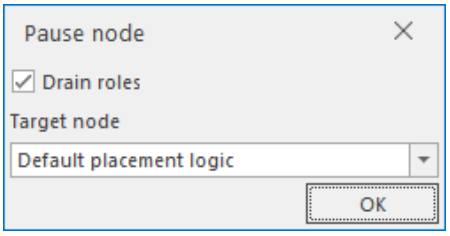
In the case maintenance operations with some of cluster nodes required, Cloud Manager allows setting the cluster nodes on maintenance with or without draining cluster roles.

To set the cluster node in maintenance mode:

- Select the cluster node in the object tree and press the **Pause node** button on the main ribbon or corresponding context-menu command:



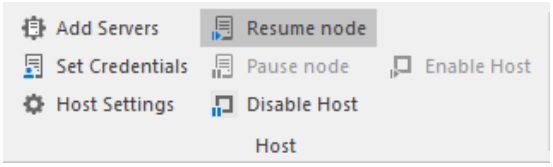
- Define whether cluster roles should be drained and the target node in the case they should be:



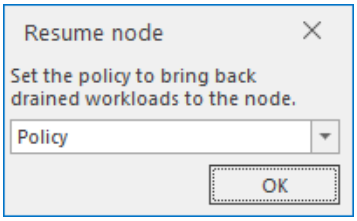
  - Check the **Drain roles** box to enable cluster roles migration.
  - Select the target node: **Default placement logic** to use the best possible node, or select the exact node from the drop-down list.

To resume the cluster node:

- Select the cluster node in the object tree and press the **Resume node** button on the main ribbon or corresponding context-menu command:



- Set the policy to bring back drained roles to the cluster node:



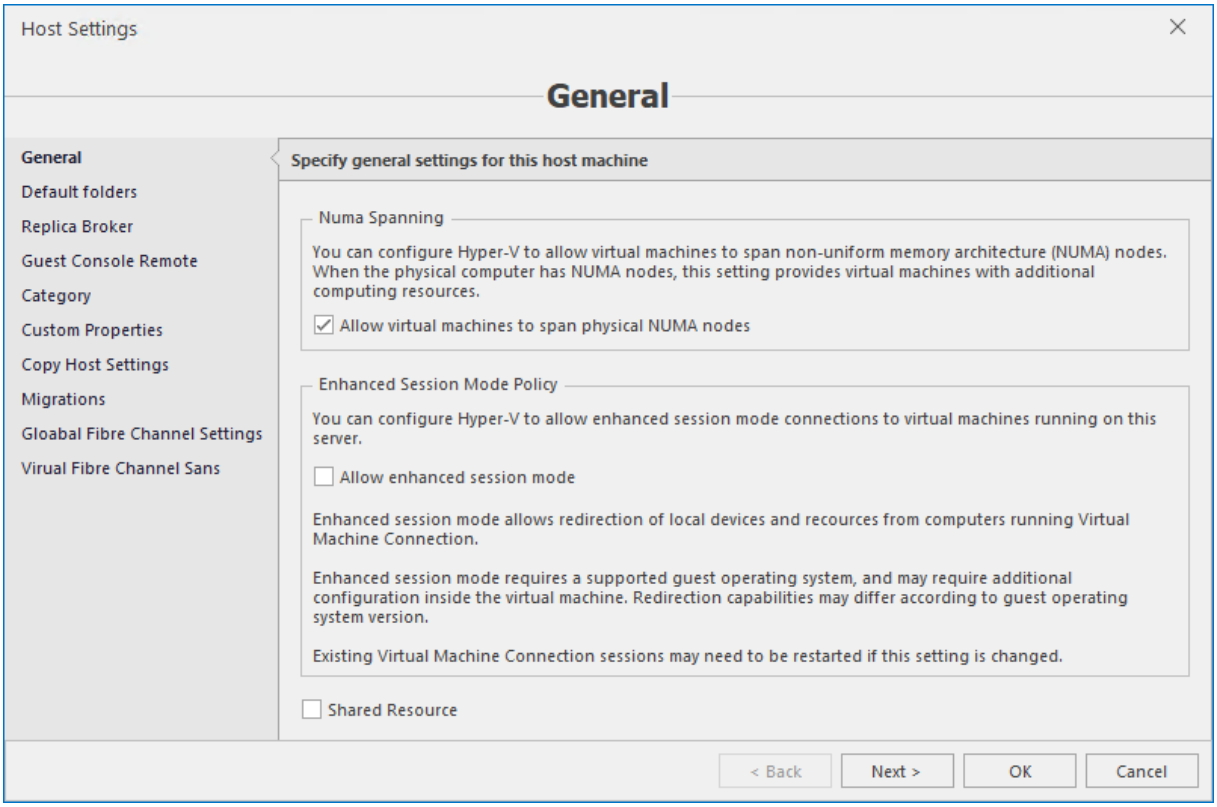
  - **NoFailback** - do not bring drained roles back to the resumed node.
  - **Immediate** - bring all drained roles back regardless of conditions.
  - **Policy** - using the default policy according to the conditions in the cluster.

Important

Make sure that there are enough of physical system resources, most importantly RAM on the target node when draining roles. Draining will fail if there are not enough resources to receive additional virtual machines.

Host settings

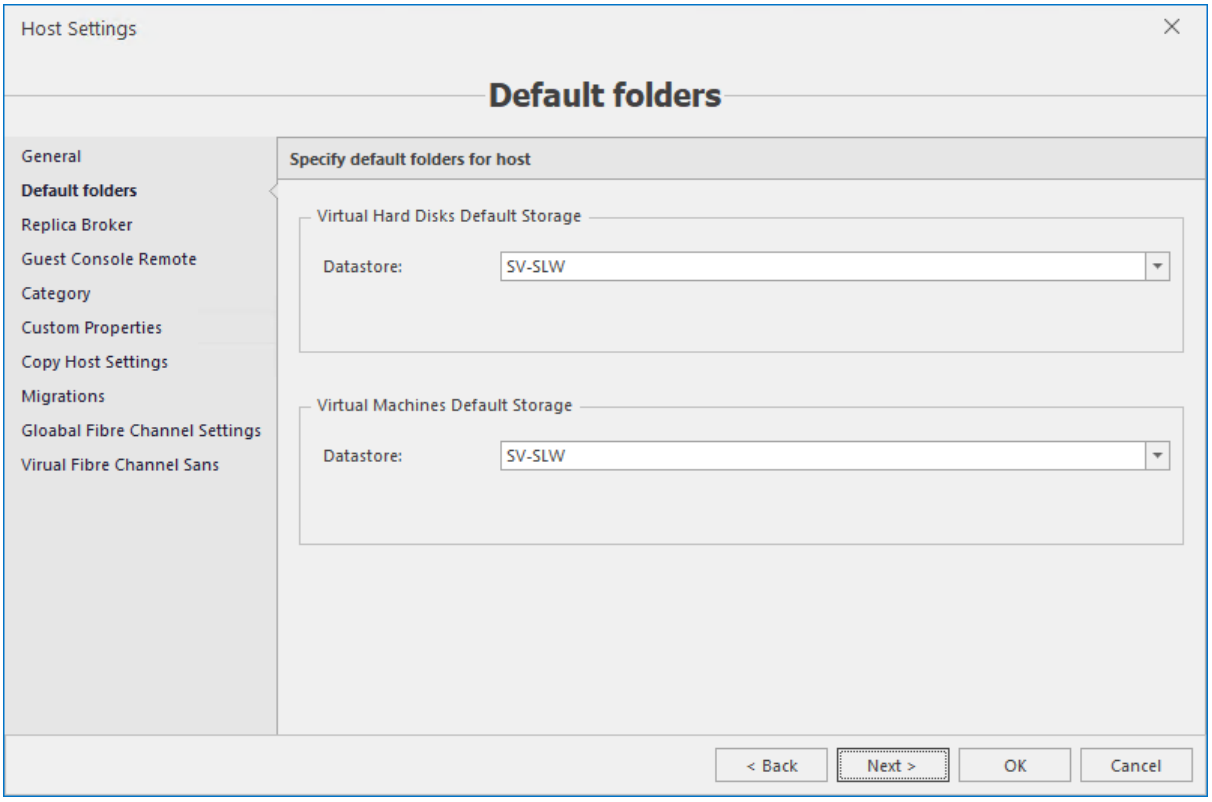
To access host settings, select the host in the objects tree and press the **Host settings** button in the toolbar.



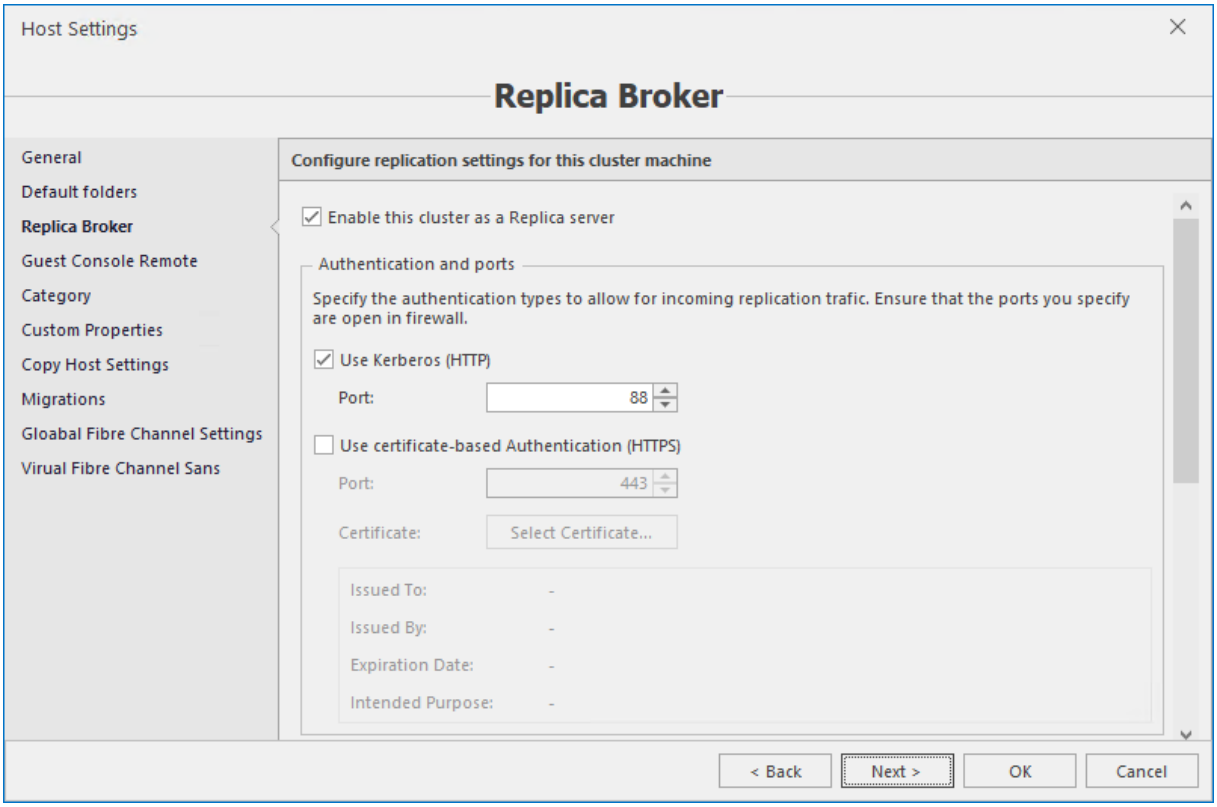
Note

You can define NUMA Spanning and enhanced session mode policy. The **Shared resource** option determines whether this host is available for all tenants or just on the global level. These settings can be applied to multiple hosts in the **Copy host settings** section.

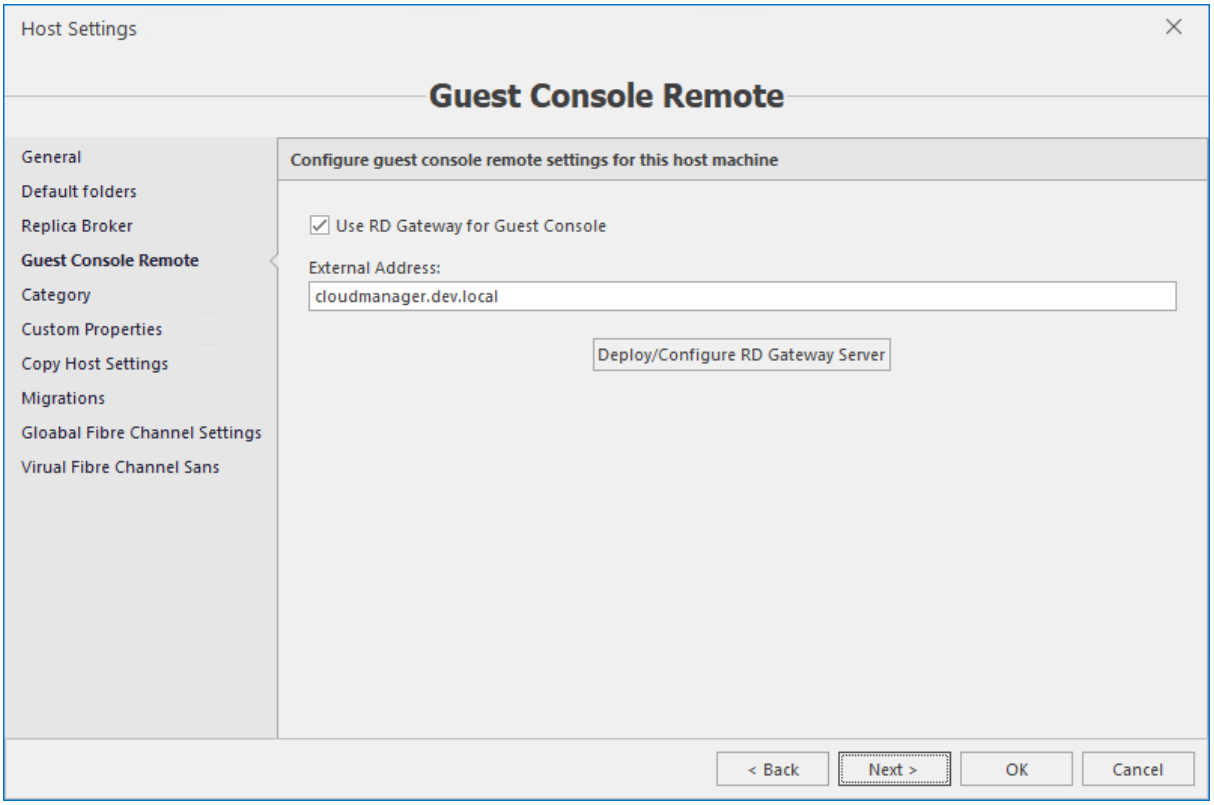
In the next section you can specify default storage for VM configuration files and disks:



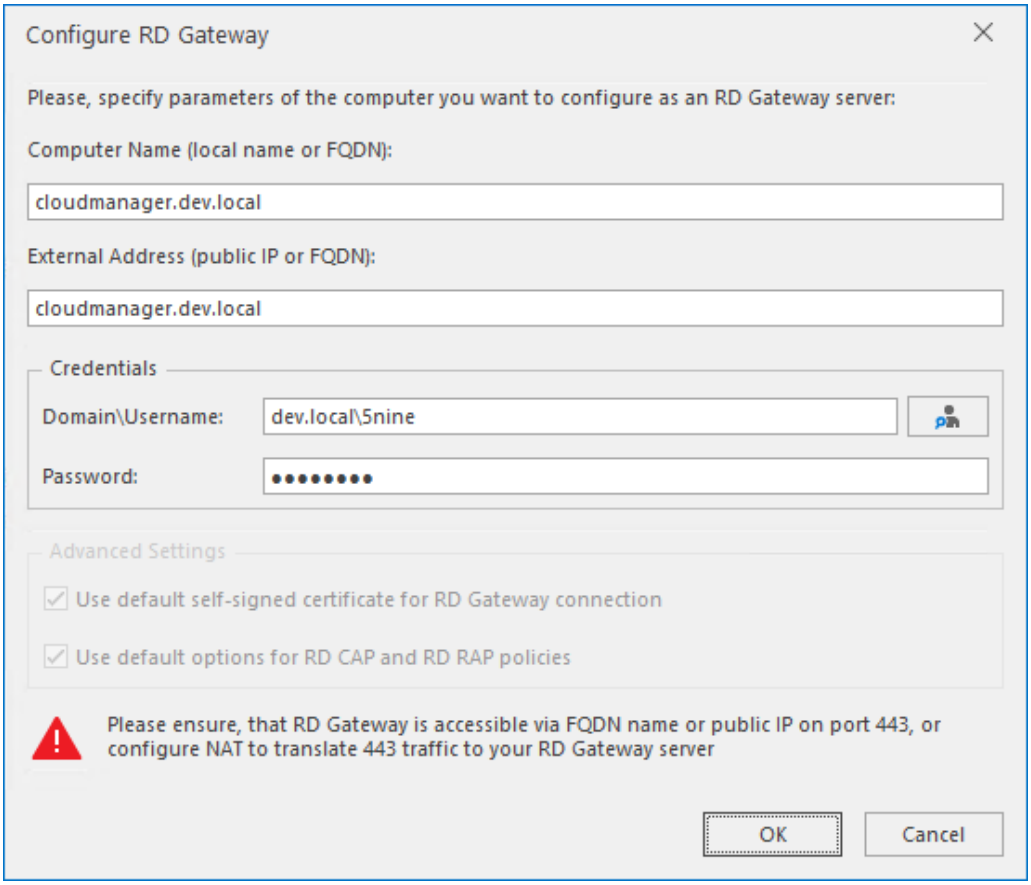
This area allows end user to configure replication settings for standalone hosts or a replica broker for a cluster.



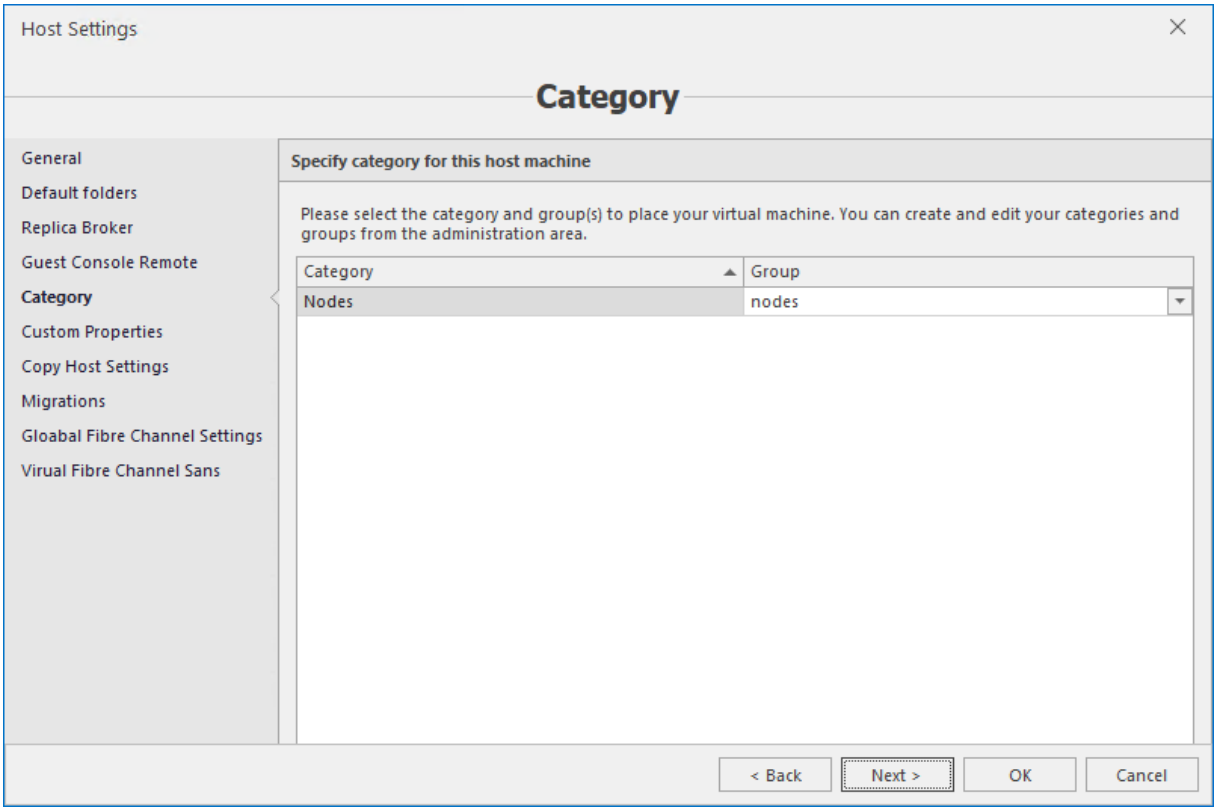
In the **Guest console remote** section set your remote desktop gateway (RDG) server parameters.



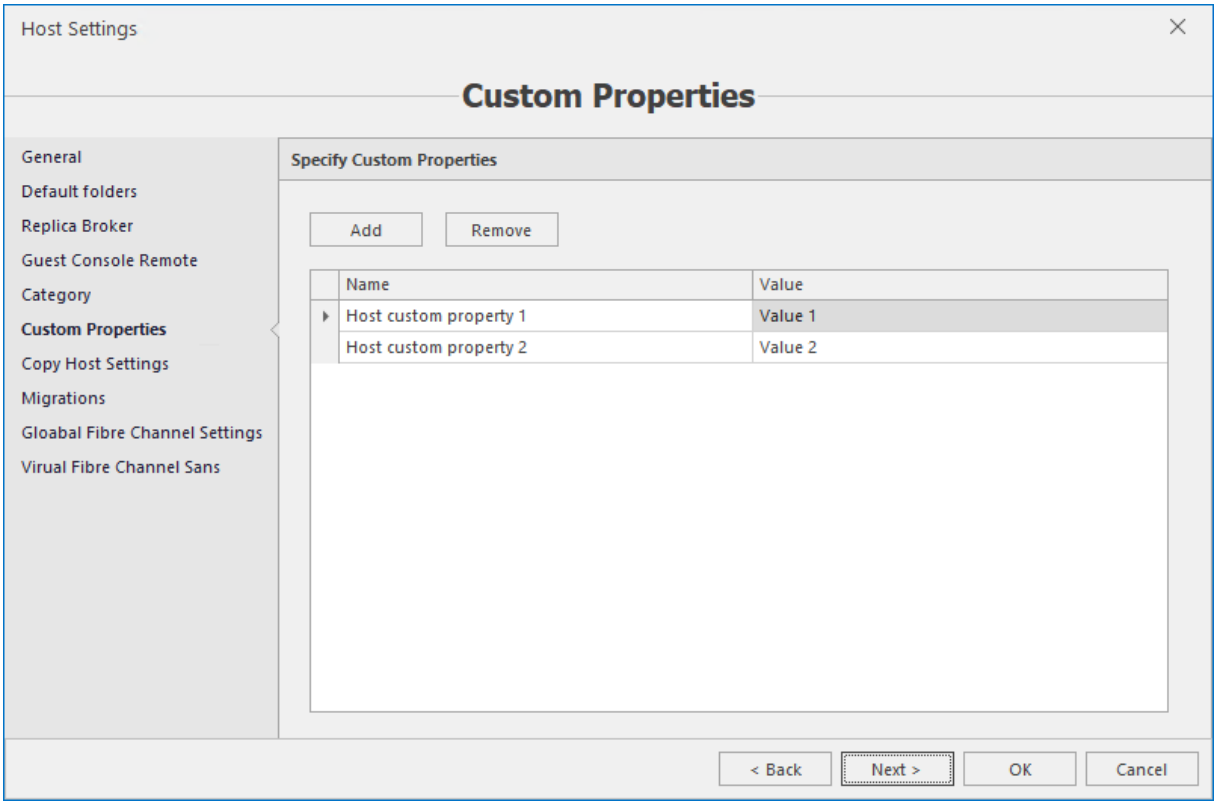
Press the **Deploy/configure RD gateway server** button to configure the RDG connection:



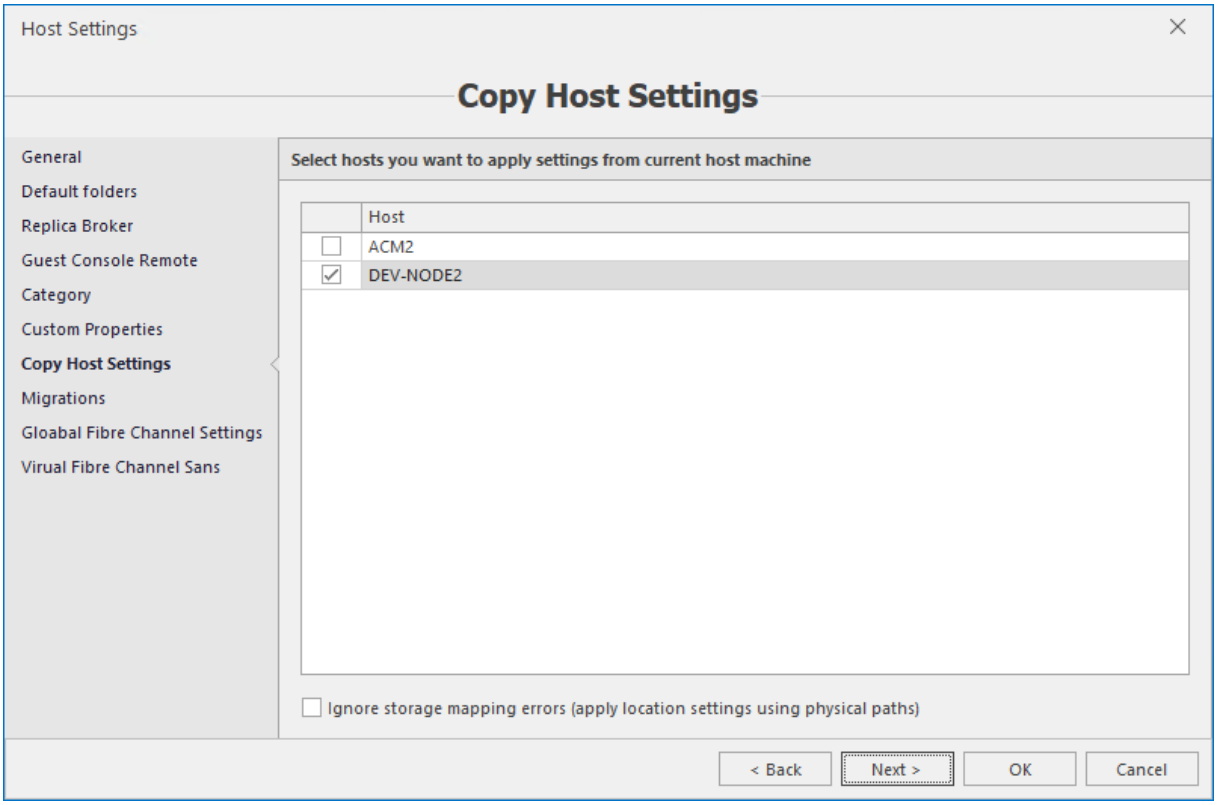
In the **Category** section specify the category and the group to display the host in the logical view:



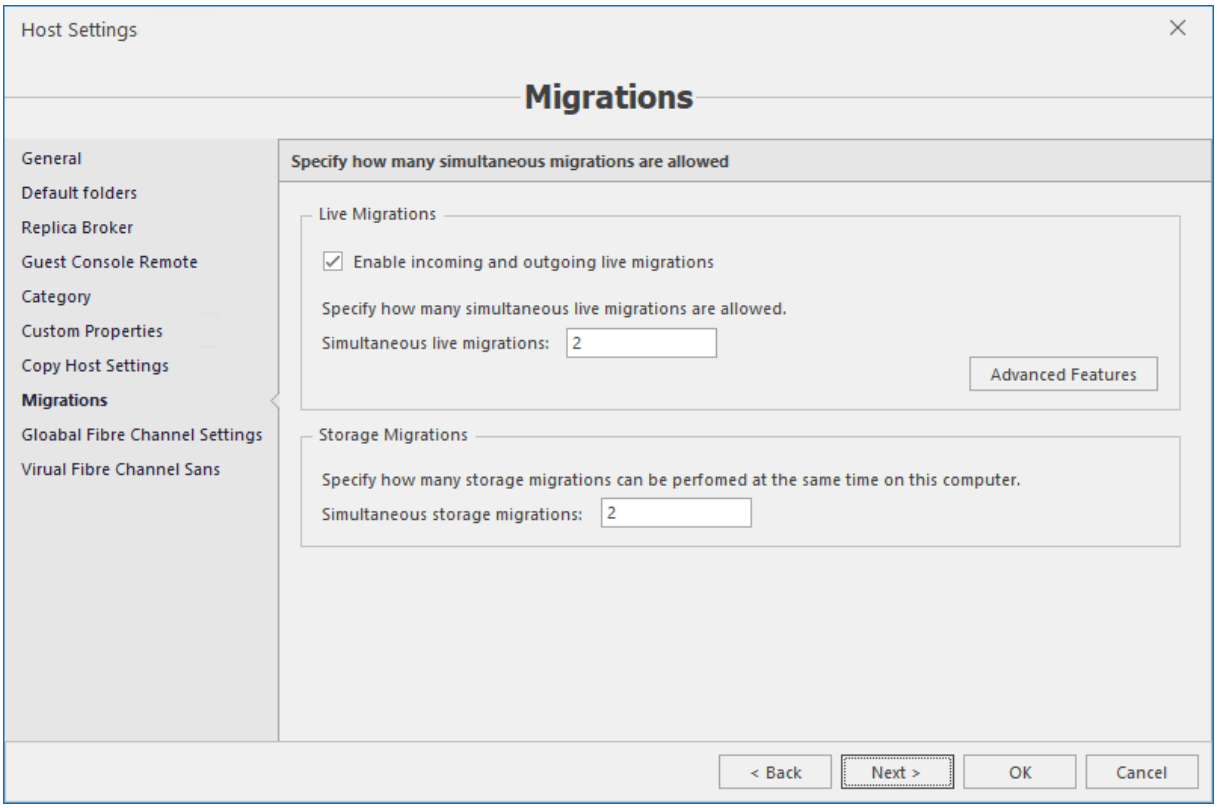
In the **Custom properties** section determine the set of your own properties for the host. These properties are for information purpose only without any functional affect.



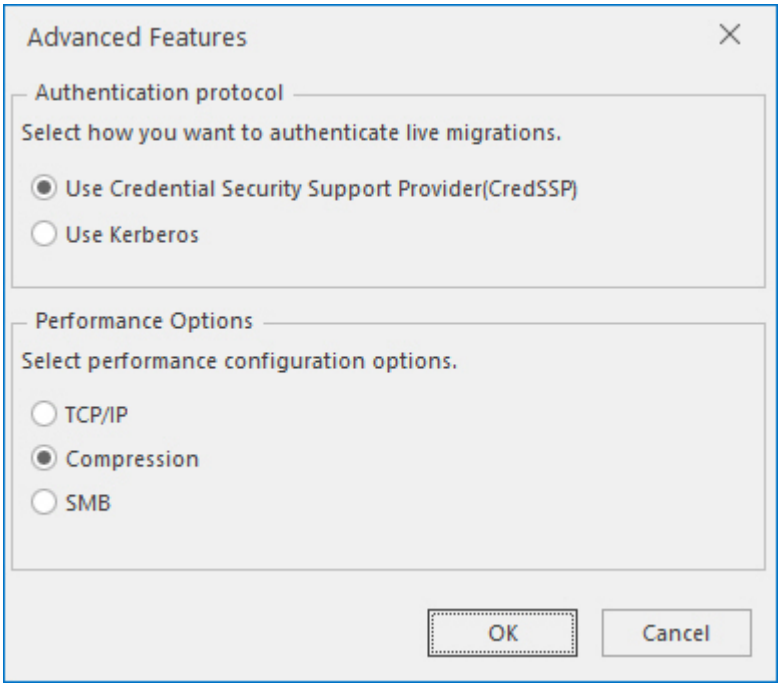
In the **Copy host settings** section configure if settings should be applied to other Hyper-V servers:



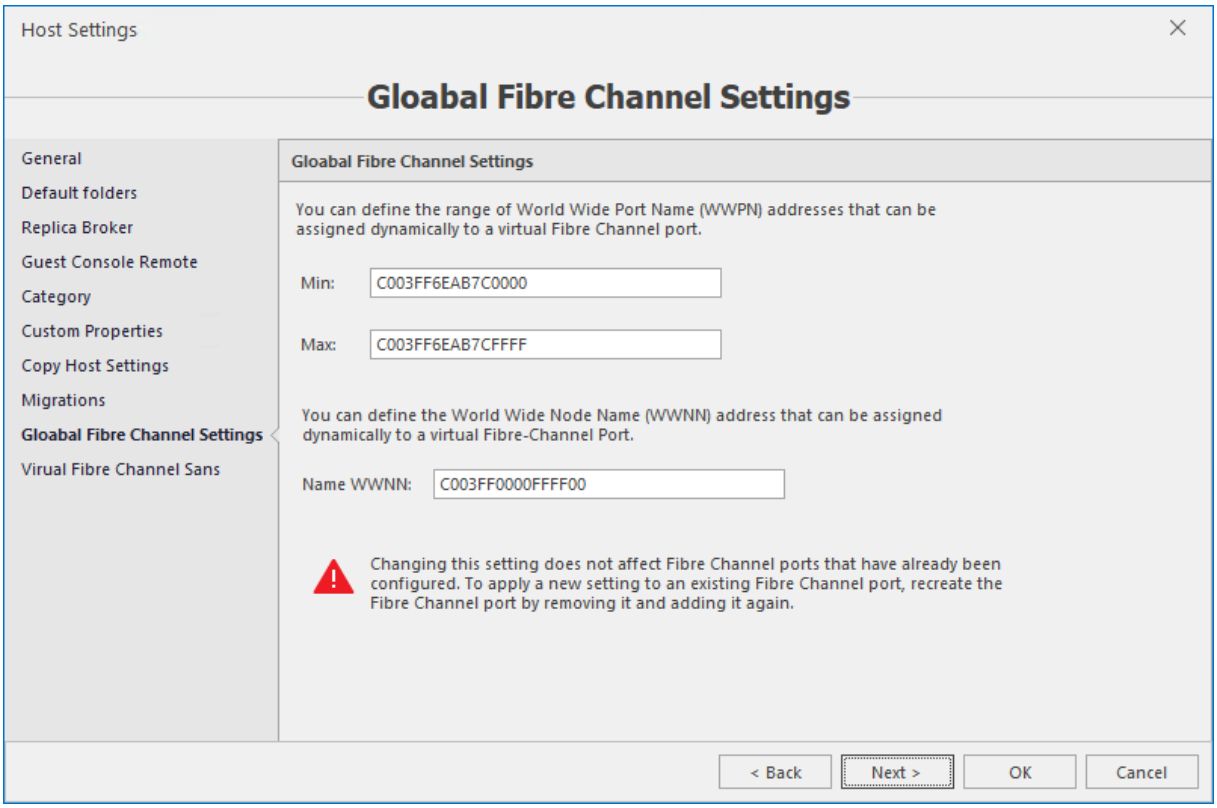
In the **Migrations** section you can enable and configure live migrations settings:



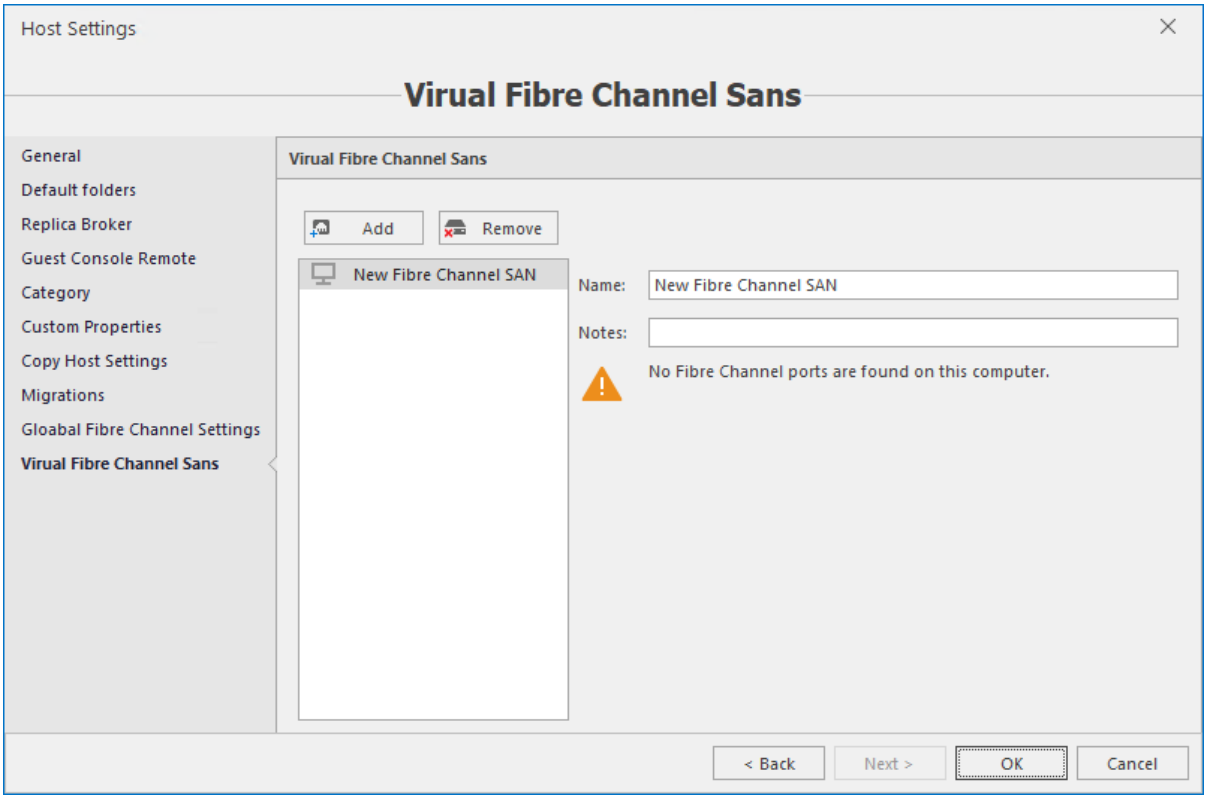
Click the **Advanced features** button to configure authentication protocol and performance options for VM live migrations:



Configure global fibre channel settings:



Add virtual fibre channel SANs:

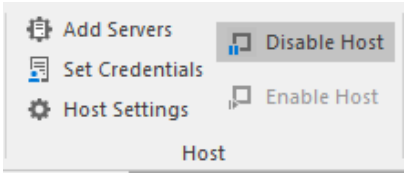


Host maintenance

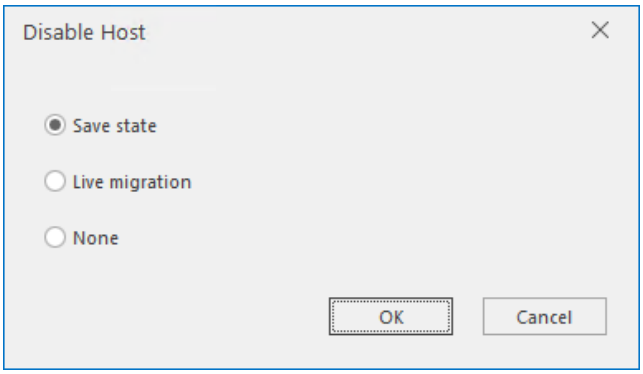
In case maintenance operations with some of standalone Hyper-V hosts are required, Cloud Manager allows setting the host on maintenance (disable) with several options what to do with virtual machines on that host while it is disabled.

To disable the host:

- Select the host in the object tree and press the **Disable host** button on the main ribbon or corresponding context-menu command:

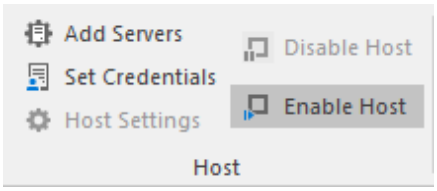


- Select the action that should be done with virtual machines on the host:



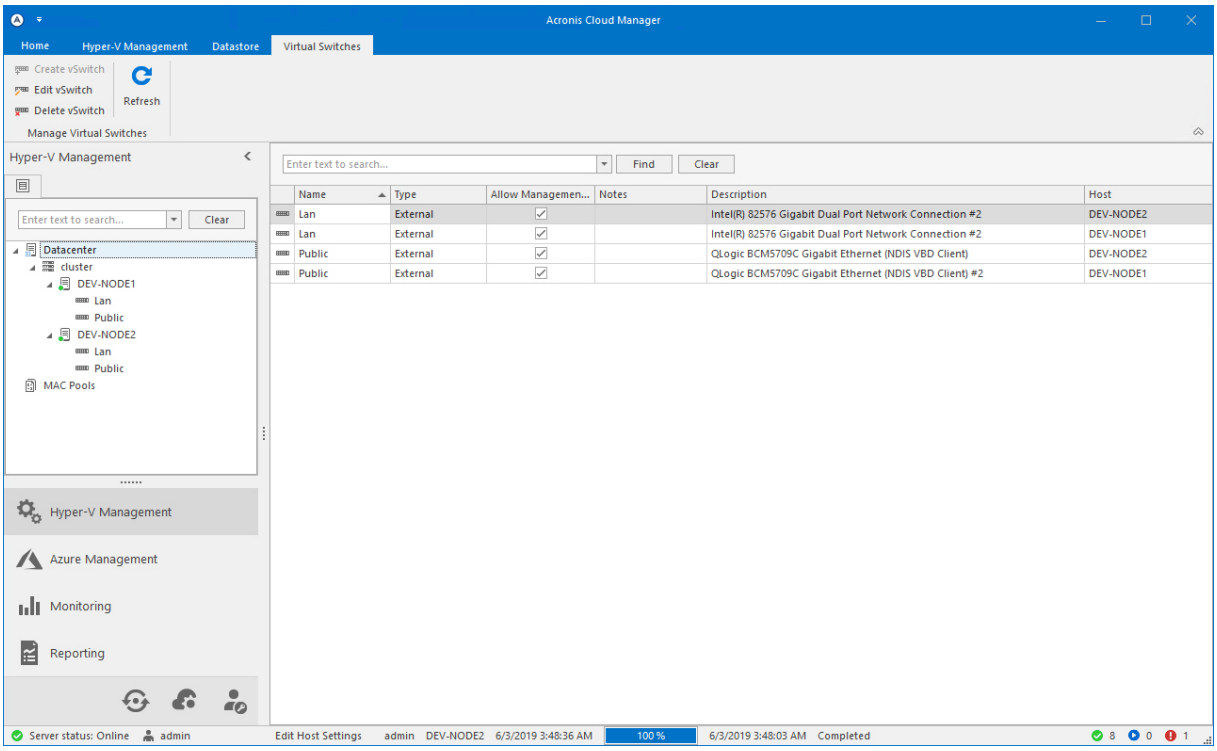
- **Save state** - set all virtual machines on the host in the saved state.
- **Live migration** - live-migrate VMs to another server, if such setting is configured on the host. In the other case this option will be disabled.
- **None** - do not apply any specific action to VMs on the host.

To resume the disabled host, select it in the object tree and press the **Enable host** button on the main ribbon or corresponding context-menu command:

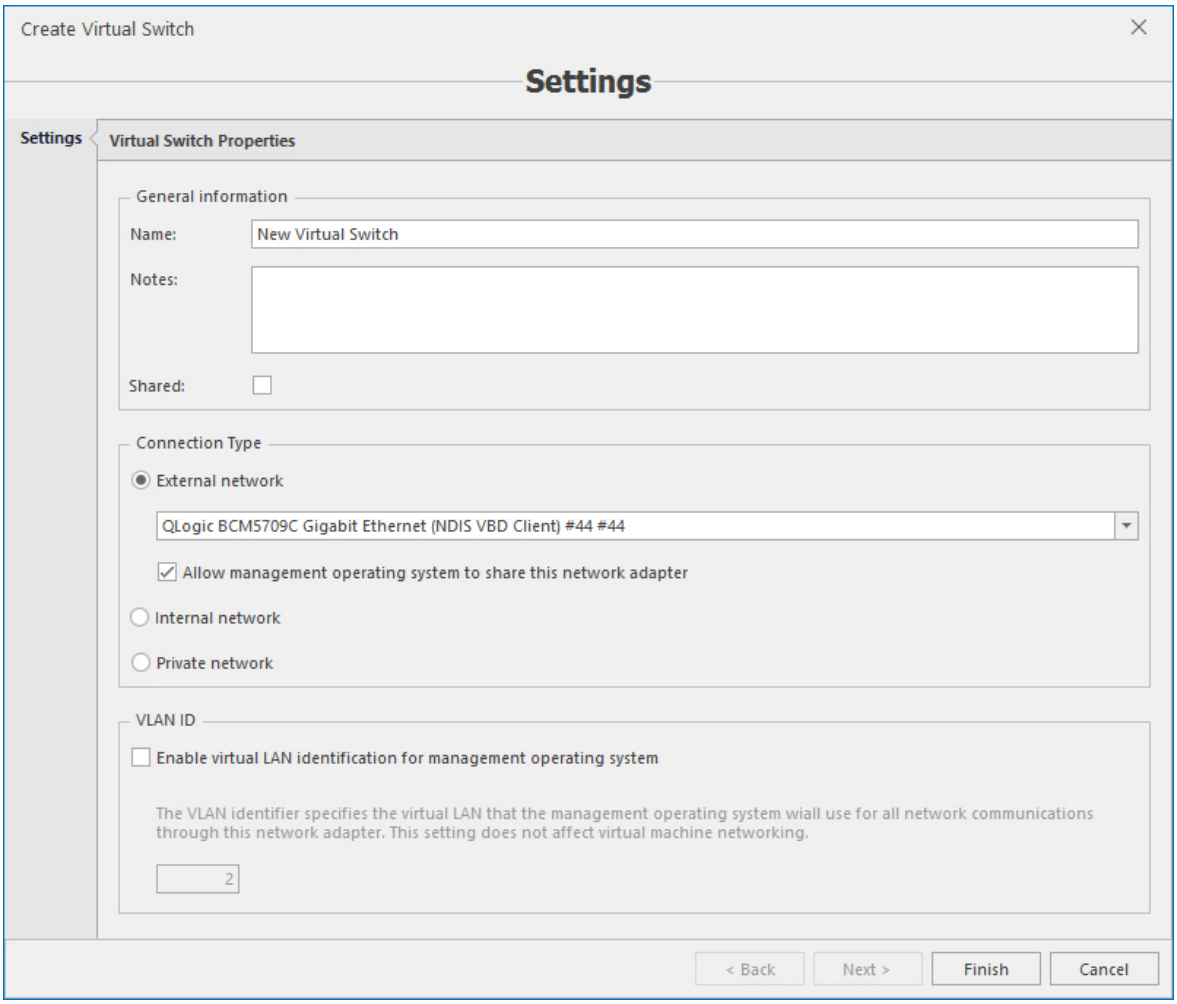


Configuring virtual switches

Virtual switch management is implemented in the **Virtual switches** tab. You can create, edit and delete virtual switches for all managed Hyper-V hosts.



1. To create the new virtual switch, select the host in the tree and press the **Create vSwitch** button in the toolbar.



2. Define name and description and select its type.

- **External netwrok**. In this type of a virtual switch, one of the physical NICs installed on the host is used to connect the VMs to the network.
- **Internal network**. In this type of a virtual switch, neither of the physical NICs of the host is supposed to be used for VMs that will be using this connection.
- **Private network**. In this type of a virtual switch, neither of the physical NICs of the host is supposed to be used for VMs that will be using this connection, nor the VLANs could be set for it.

The **Shared** option determines whether this virtual switch is available for all tenants or just on the global level. VLAN traffic identification can be set for external and internal switches.

3. Press **Finish** to create the virtual switch.

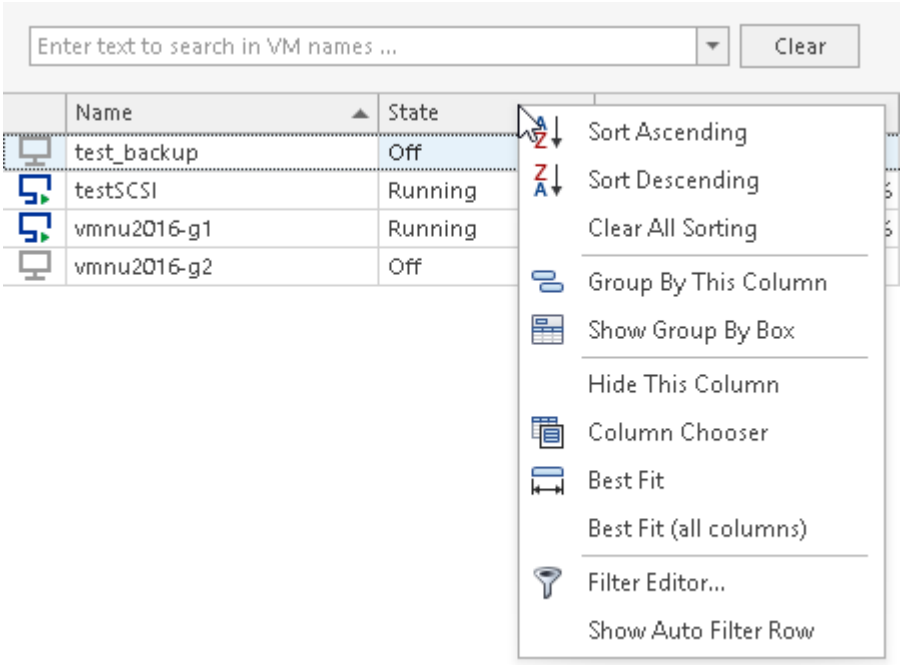
Operations with VMs

Customizing VM list view

The following options are available to configure the view of the **Hyper-V management** tab and displaying virtual machines:

- Search by name;
- Sorting by column;
- Group by column;
- Choose columns to show;
- Auto arrange (best fit);
- Filter.

To customize view press the left mouse button at the column heading:

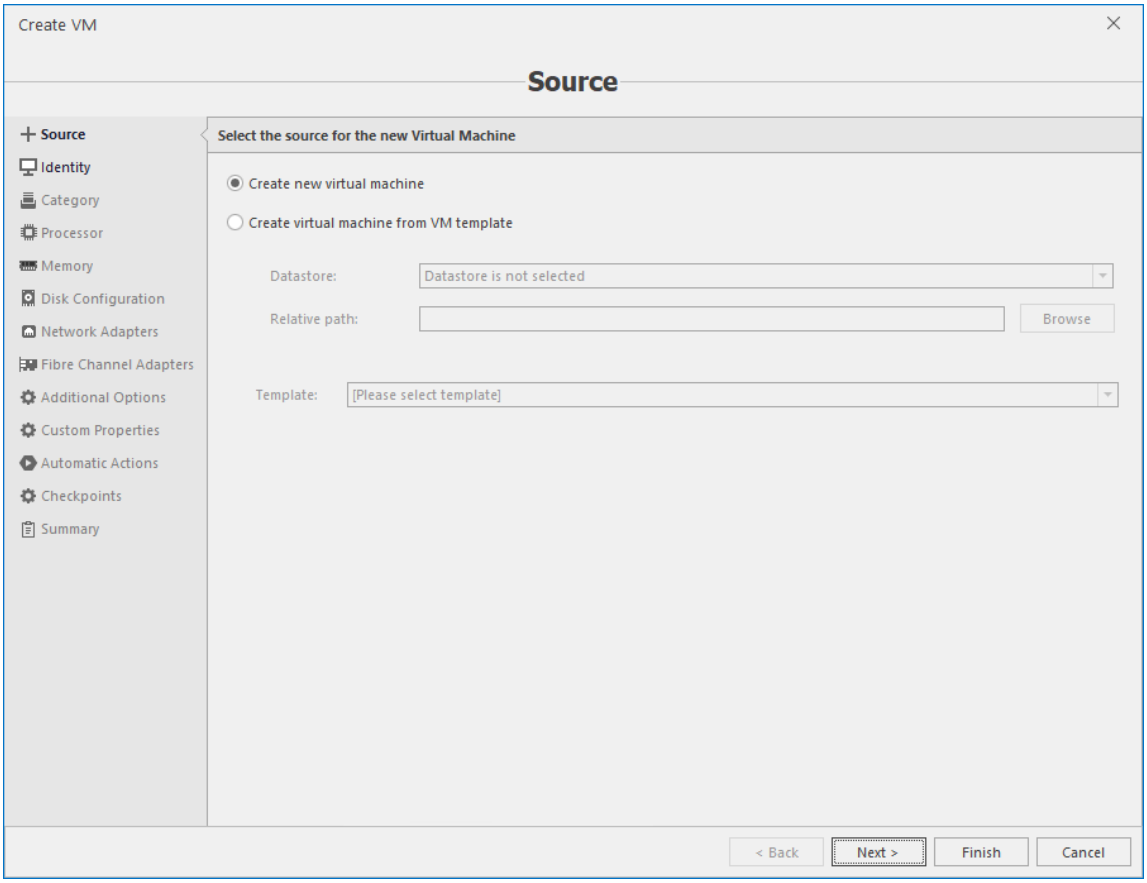


Creating VM

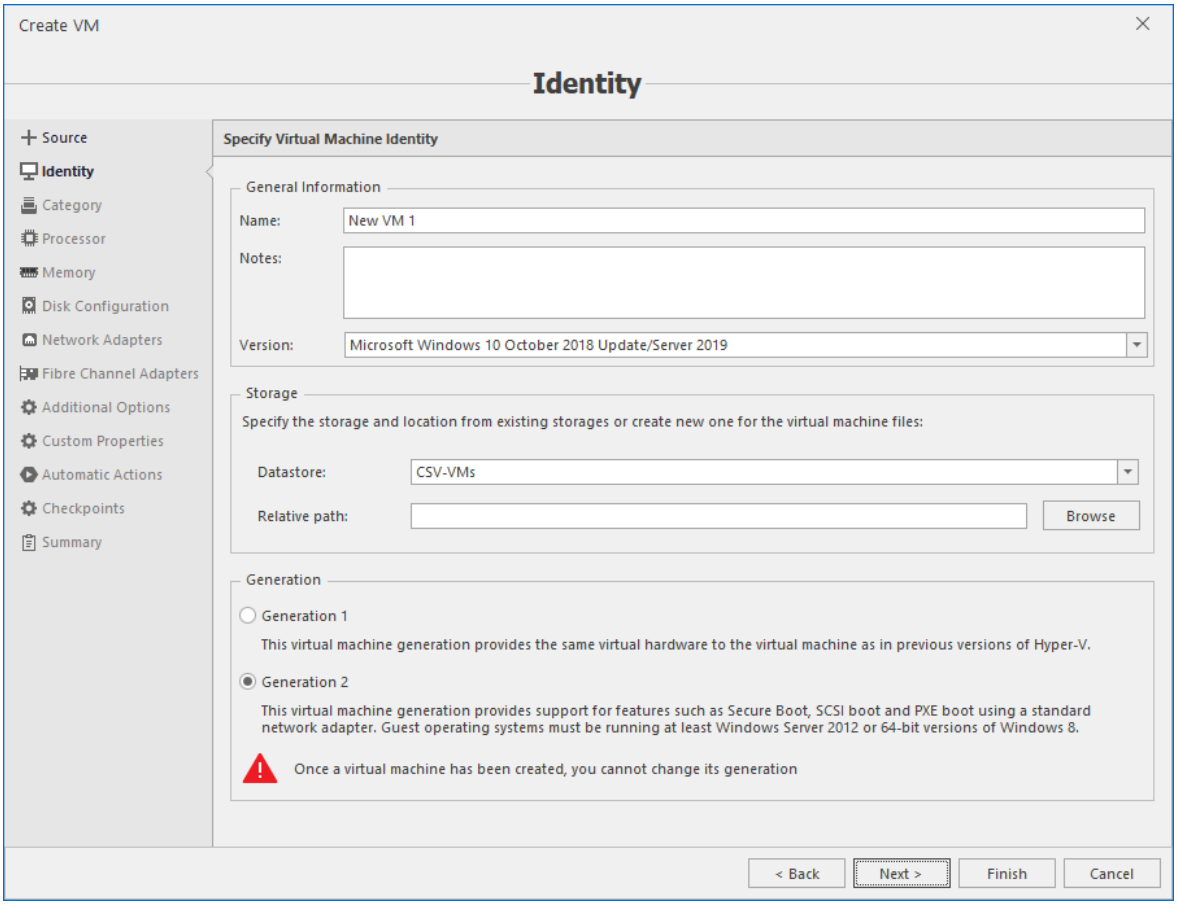
1. To create a VM select the Hyper-V host and press the **Create VM** button in the toolbar.

   Select the source – either the new blank VM with default settings or a template. When using the template, you will have to select the datastore/relative path, where the template is located, then select

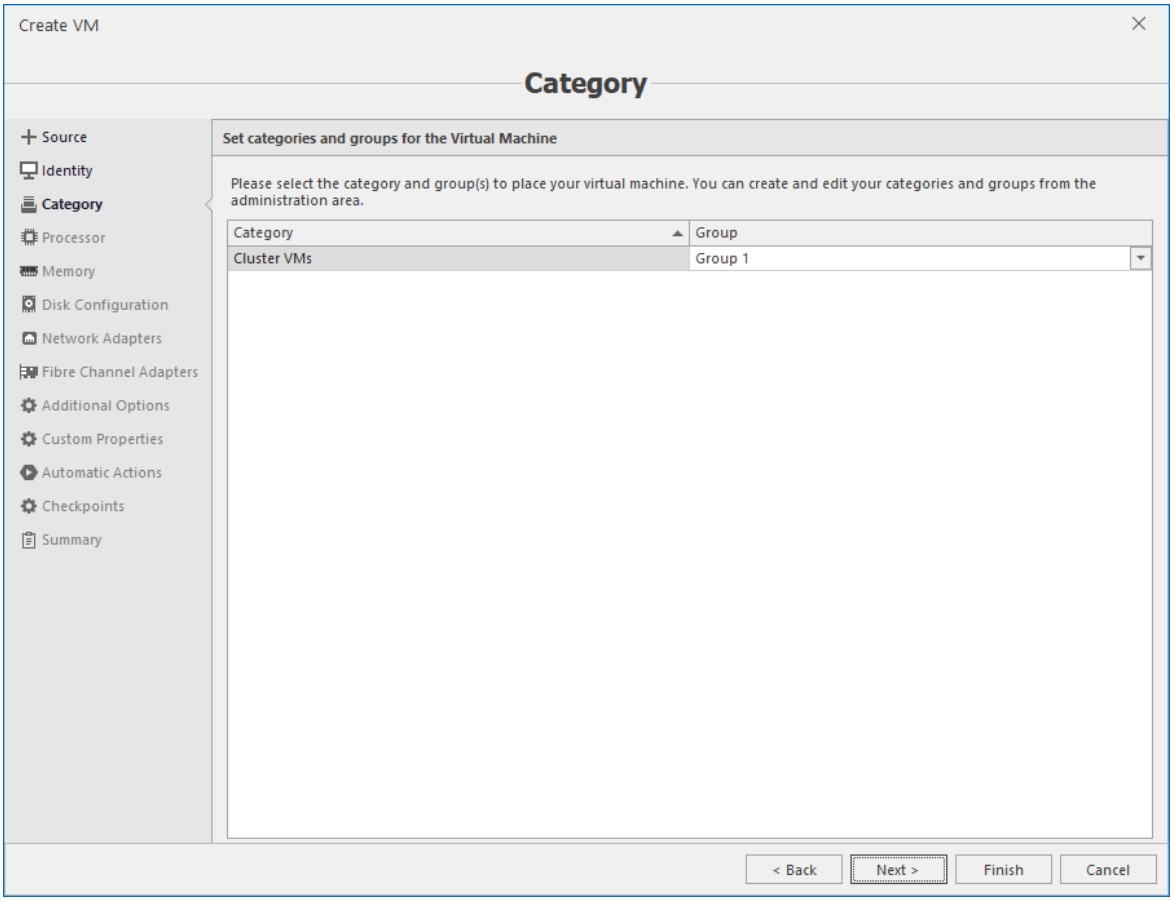
the required template in the corresponding fields.



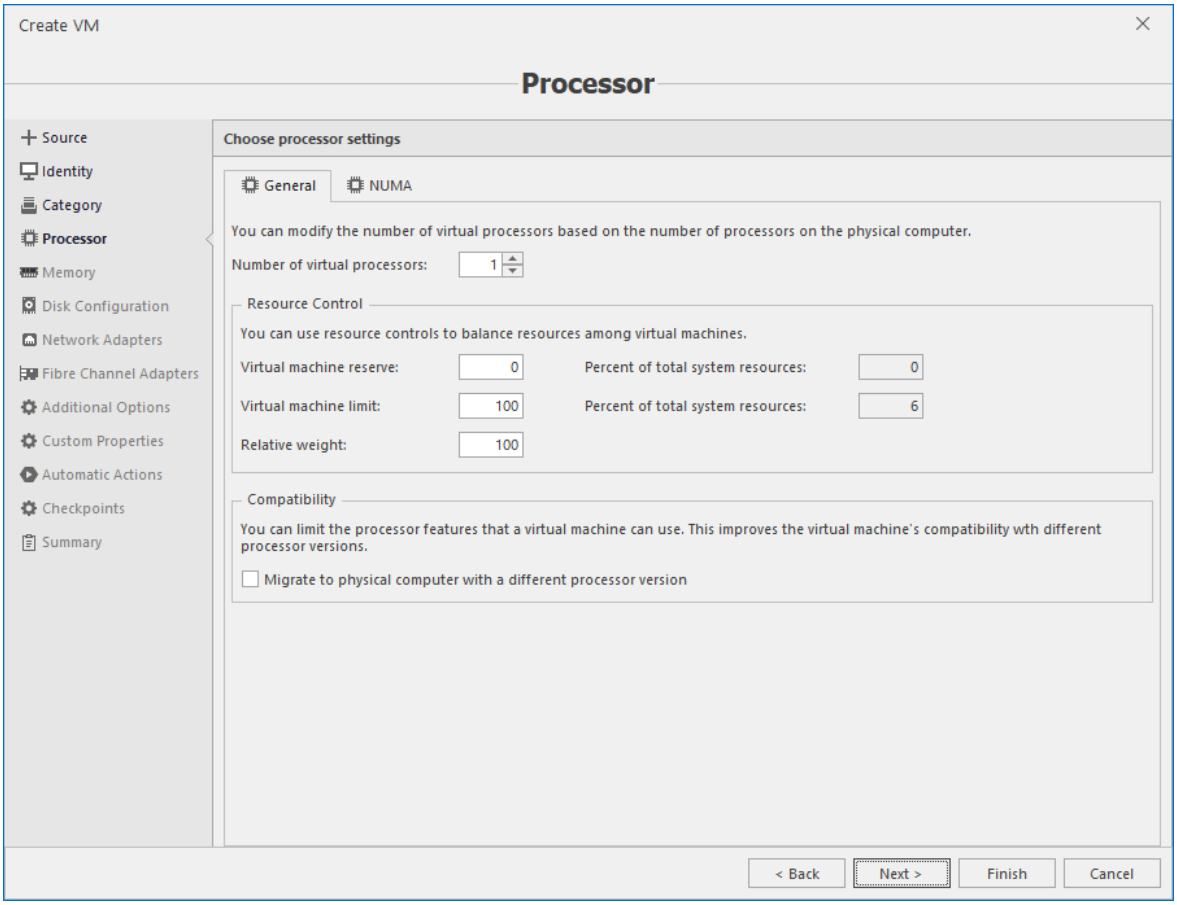
2. Specify VM identity:



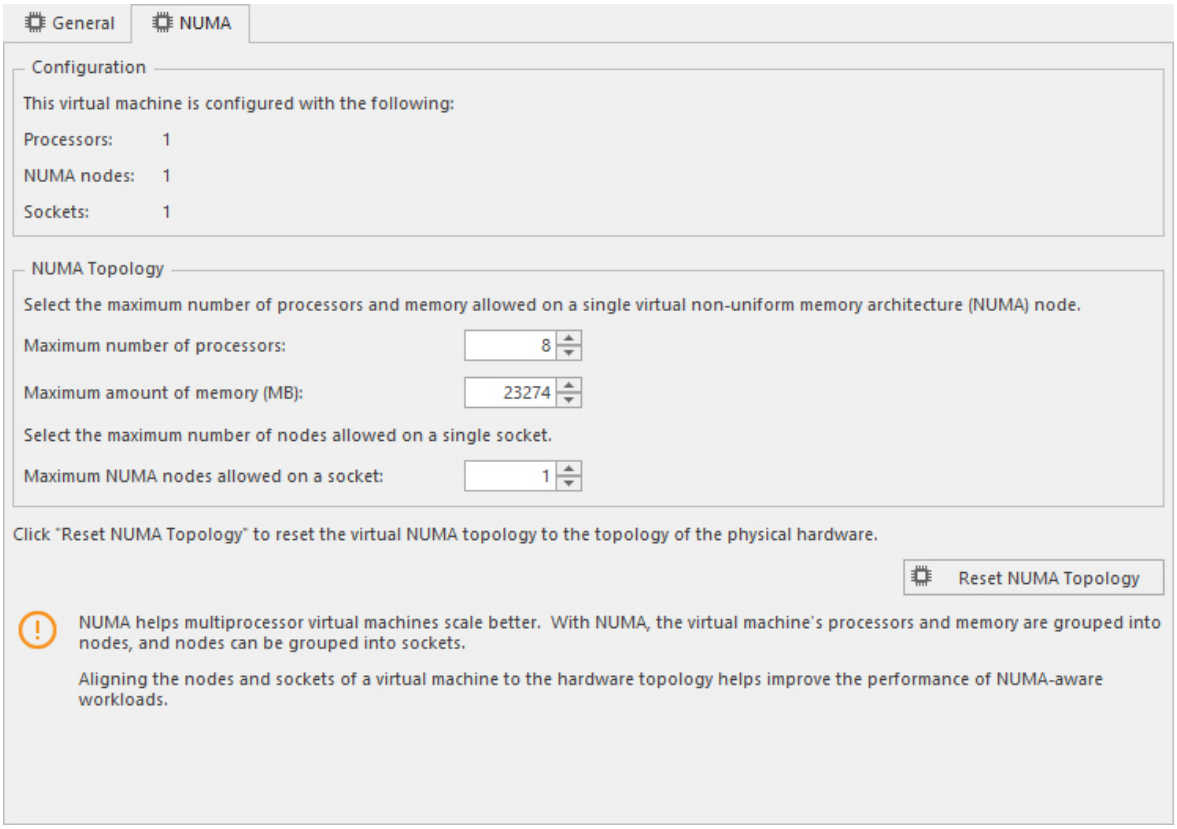
3. Define category and group to display VM in the logical view:



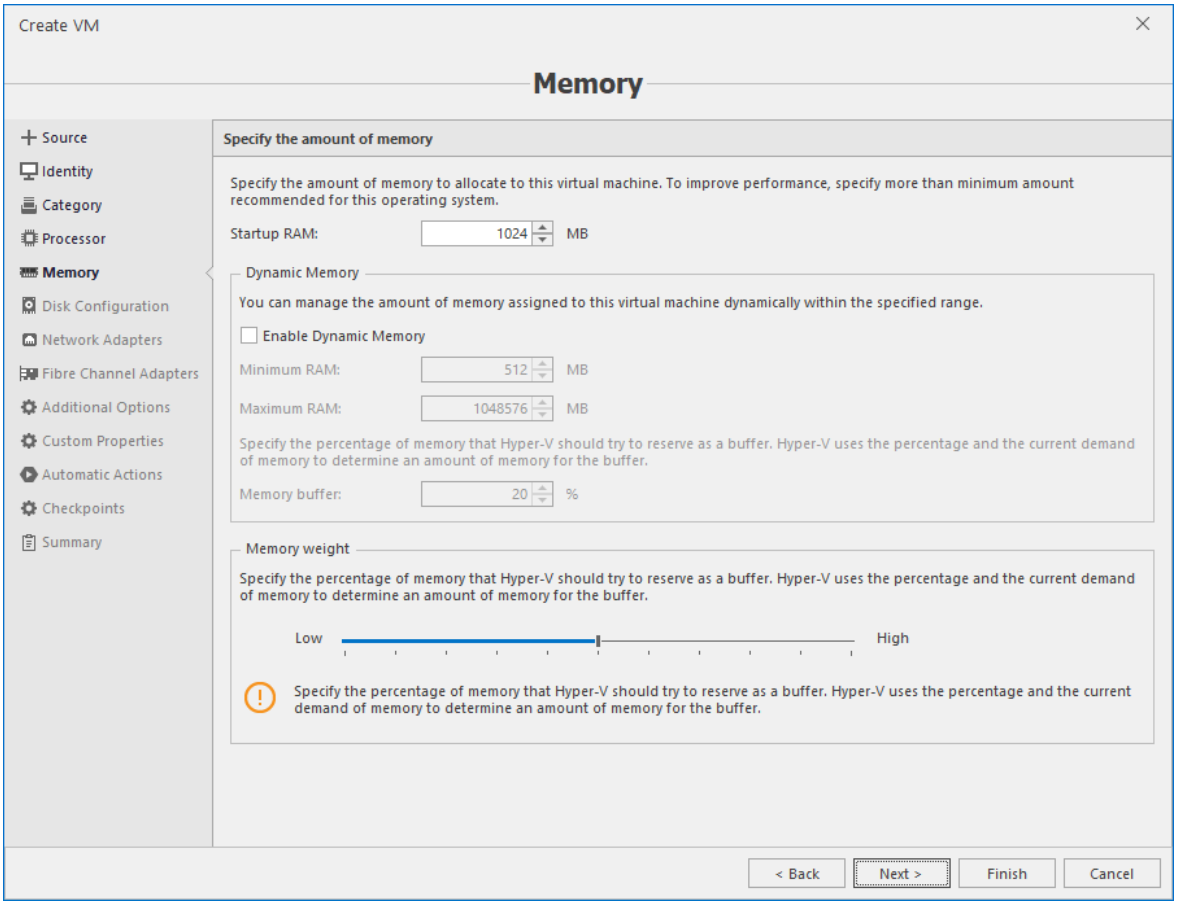
4. Define basic virtual CPU parameters:



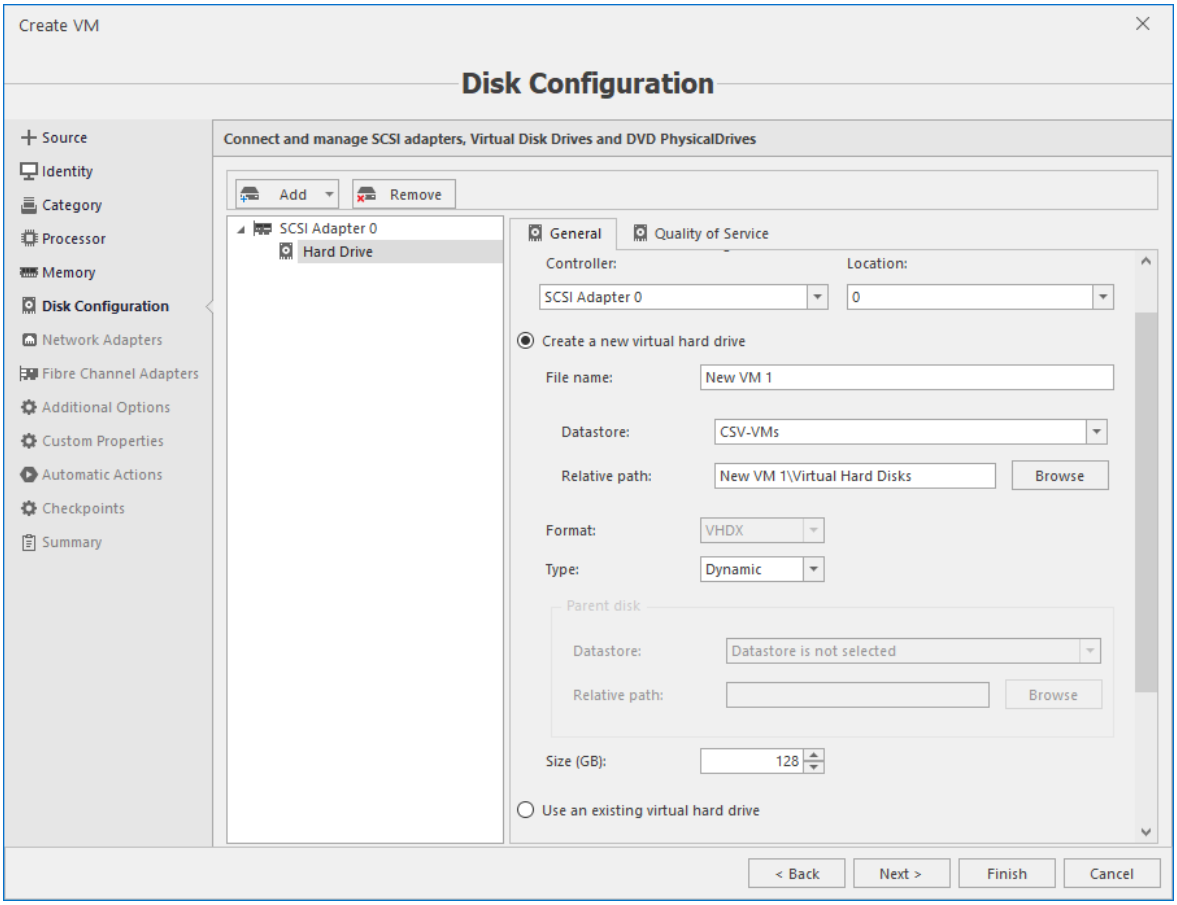
5. [Optional] If necessary, define NUMA parameters.



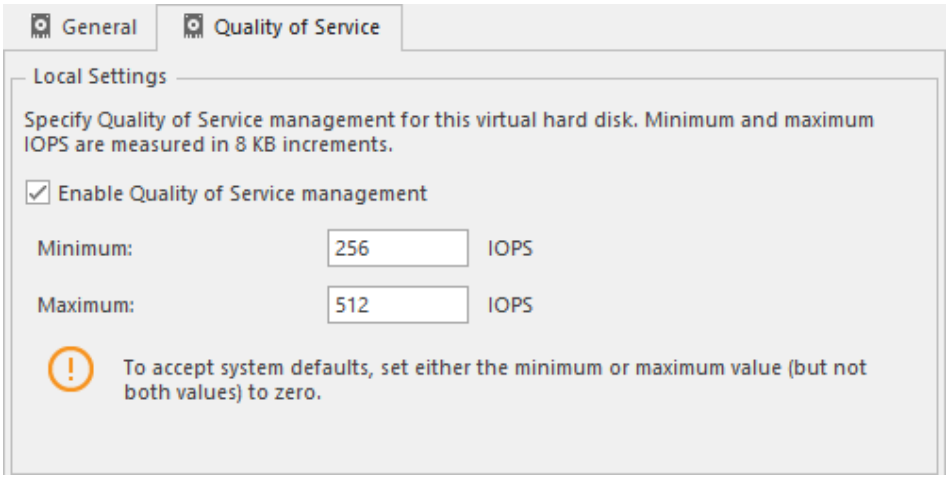
6. Specify amount of memory and dynamic memory options:



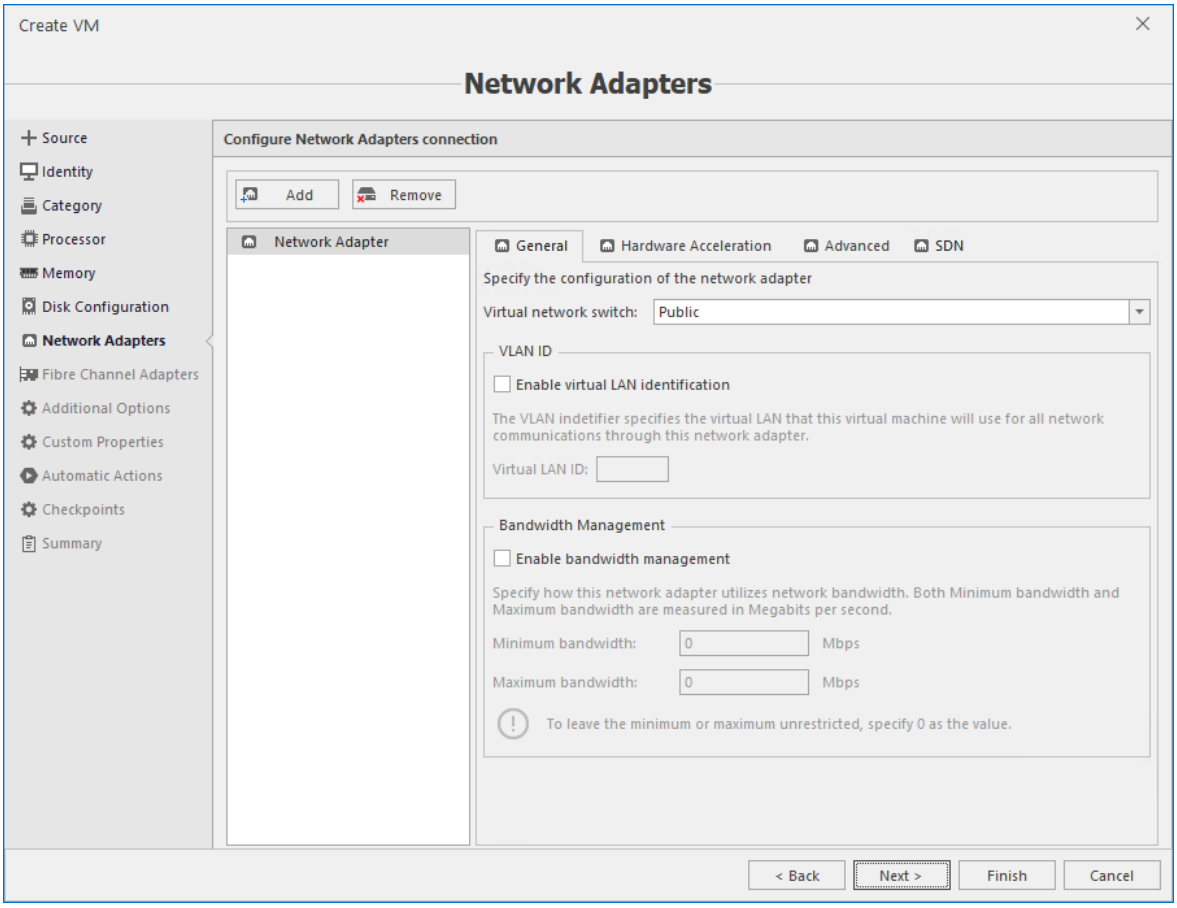
7. Add virtual disks to a VM.



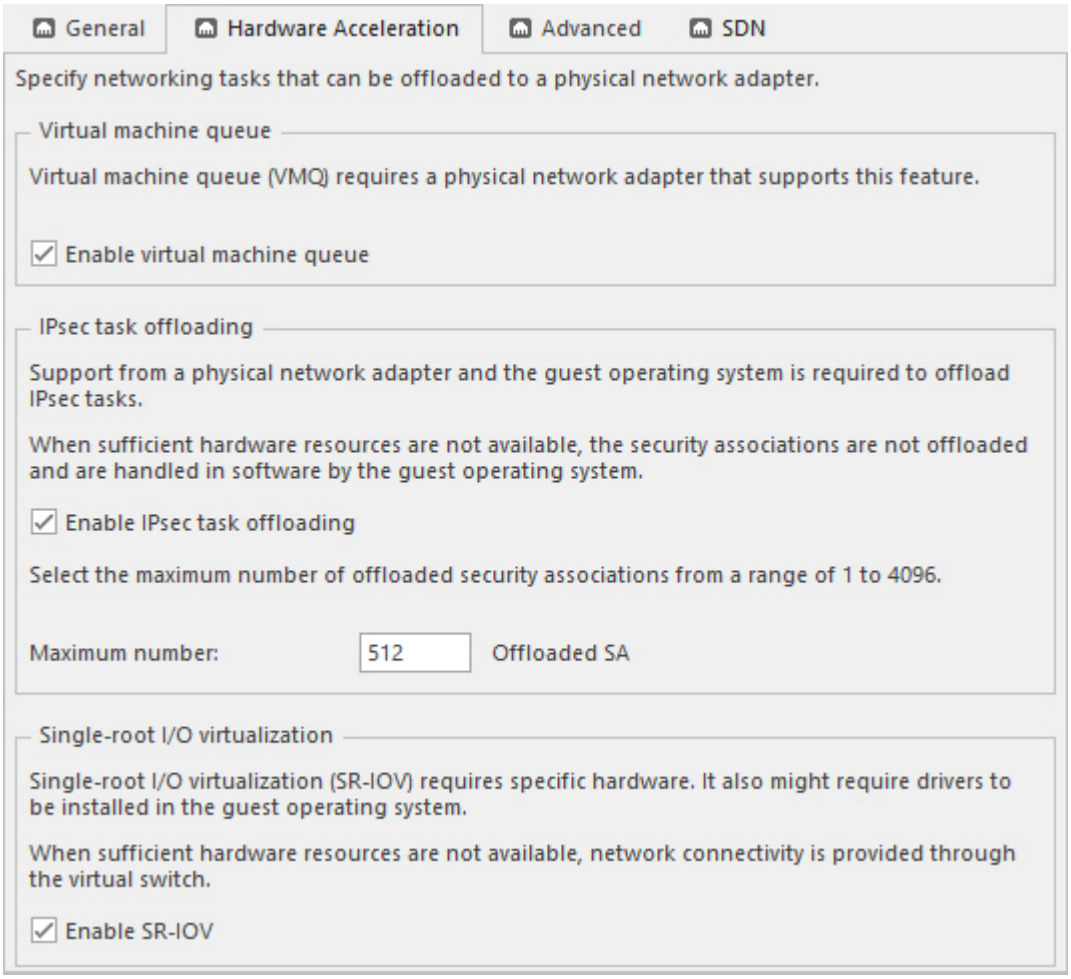
8. [Optional] If necessary provide QoS options disks.



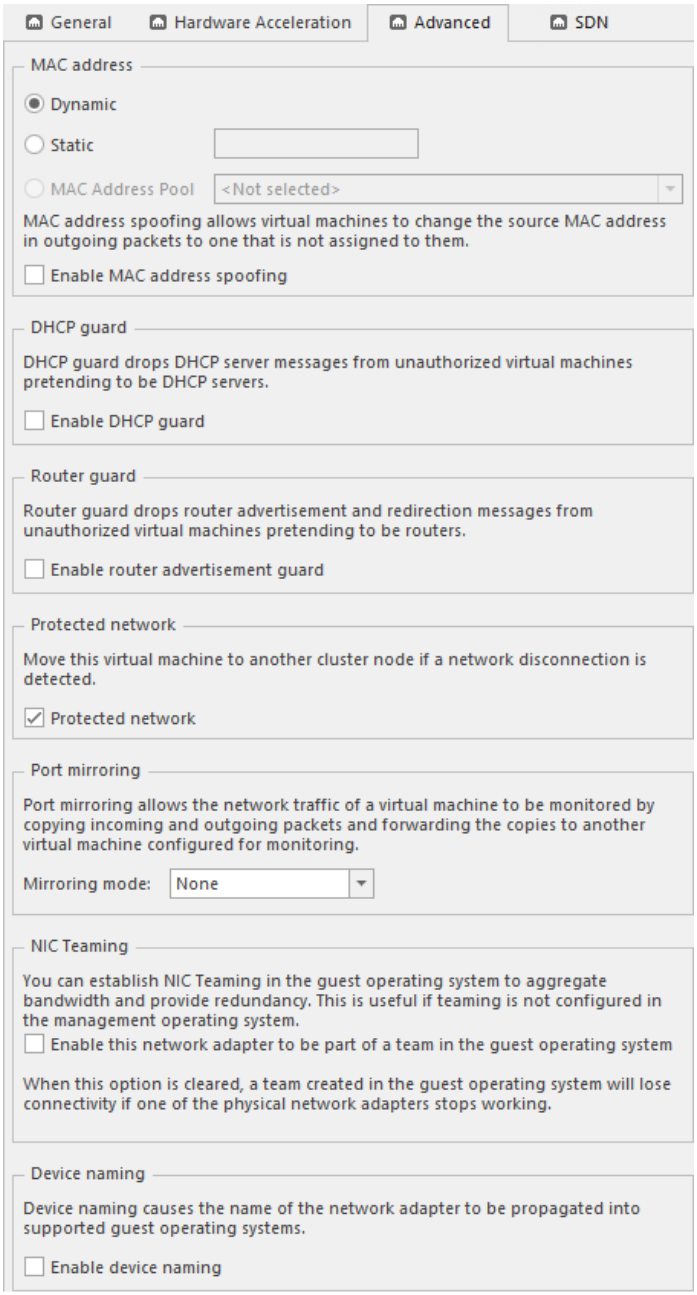
9. Define network configuration for this VM.



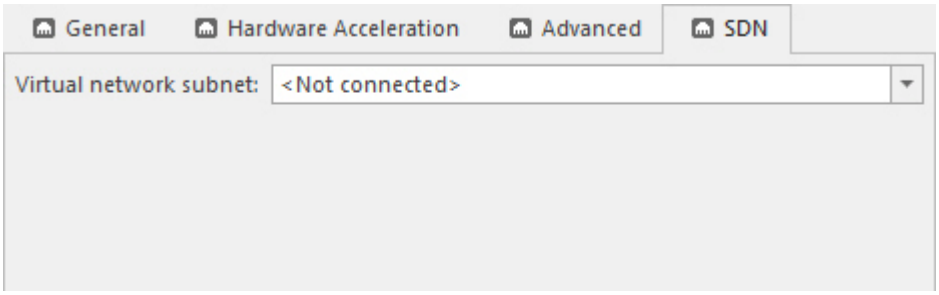
10. [Optional] If necessary, enable hardware acceleration options.



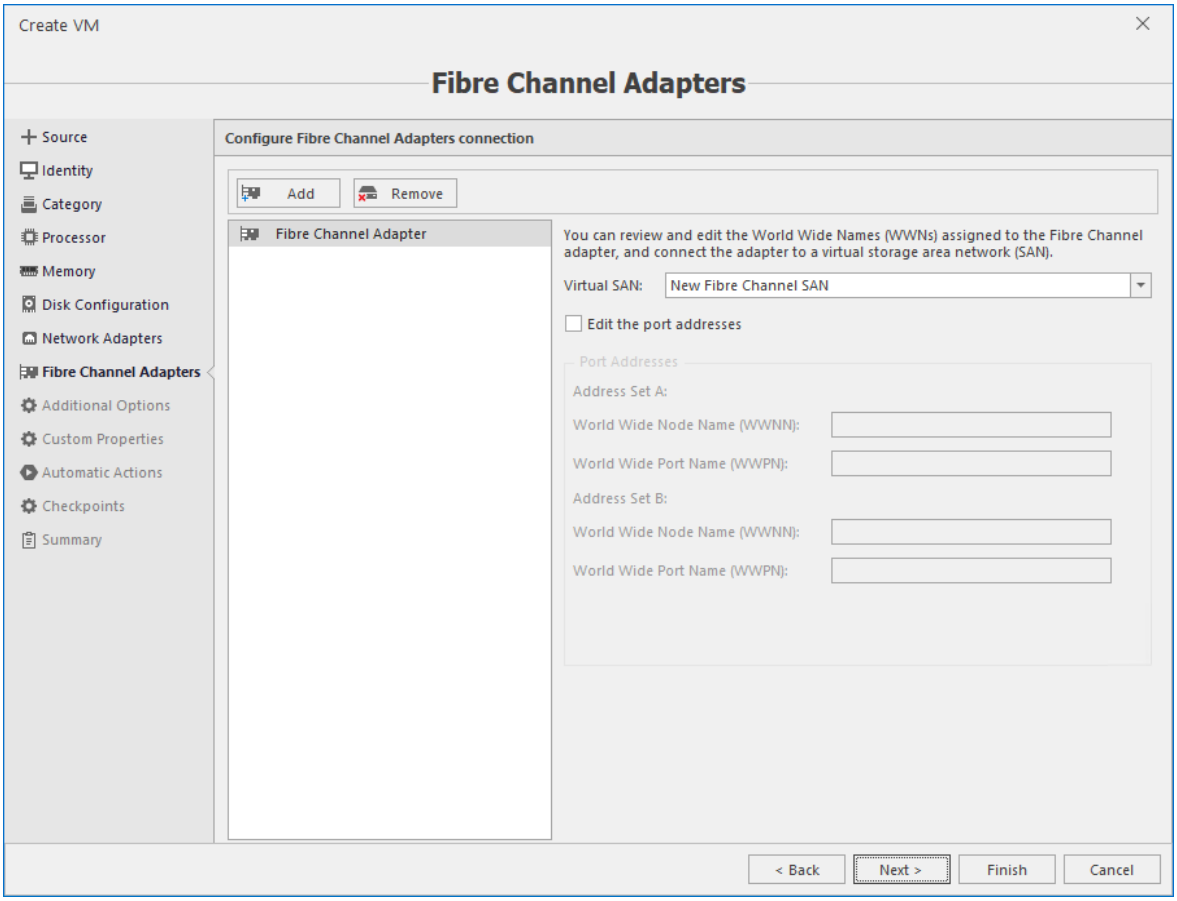
11. Define advanced network parameters:



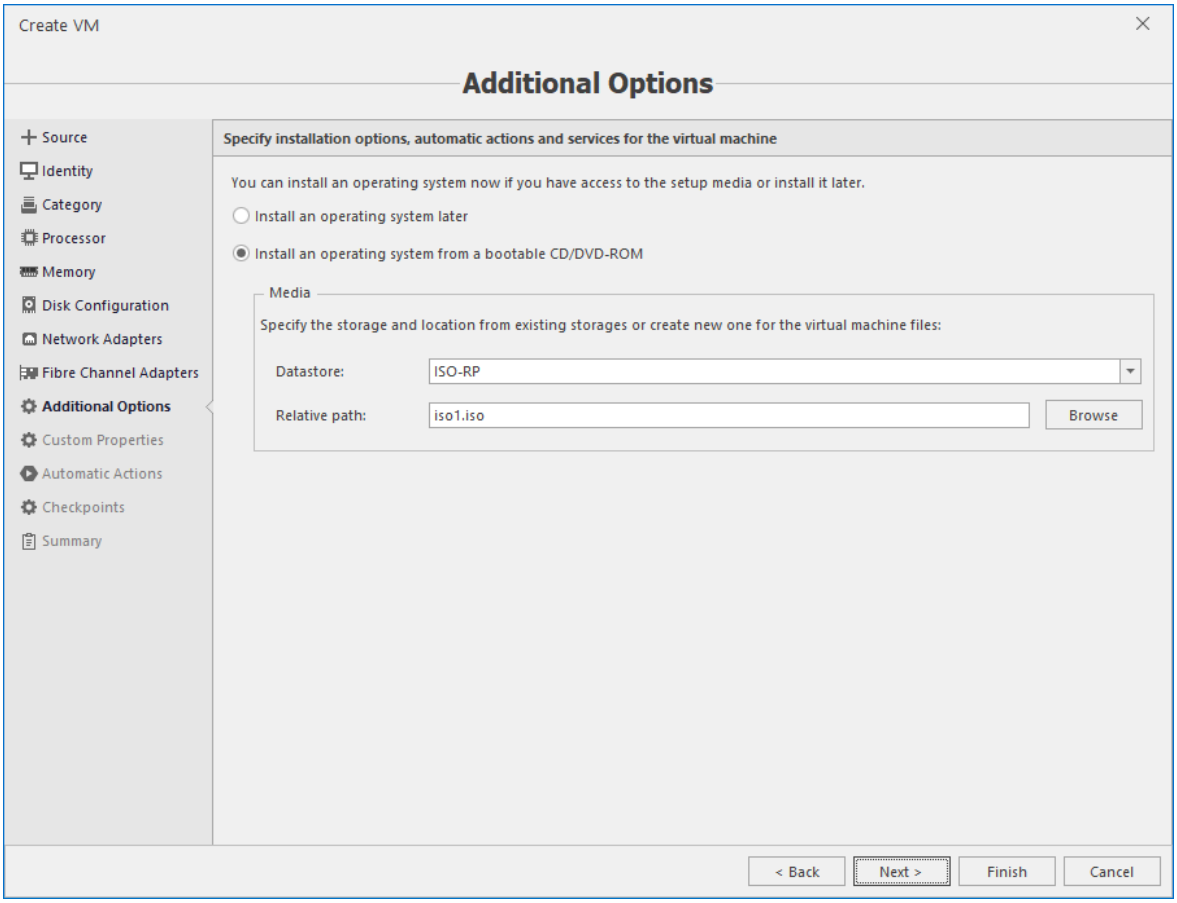
12. Configure SDN network if applicable.



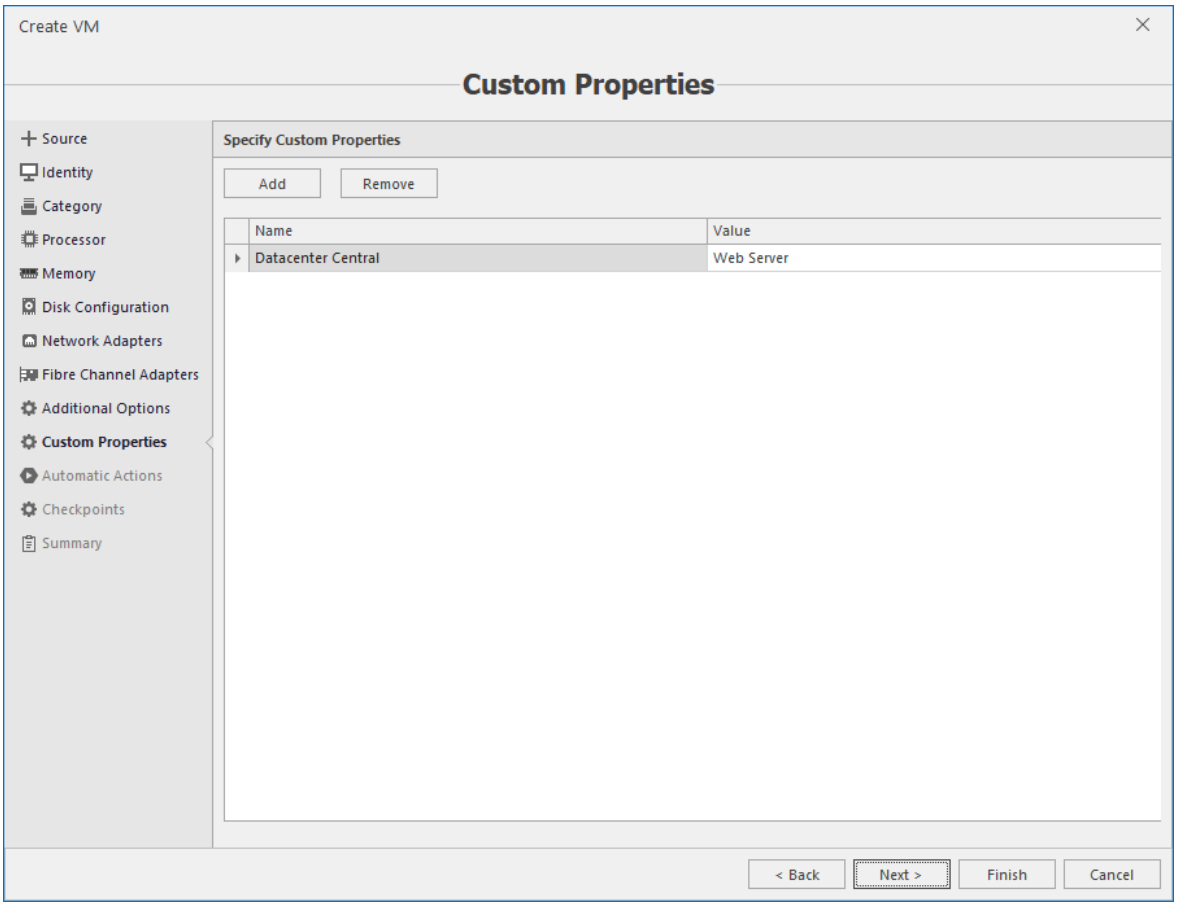
13. Configure fibre channel adapters if applicable.



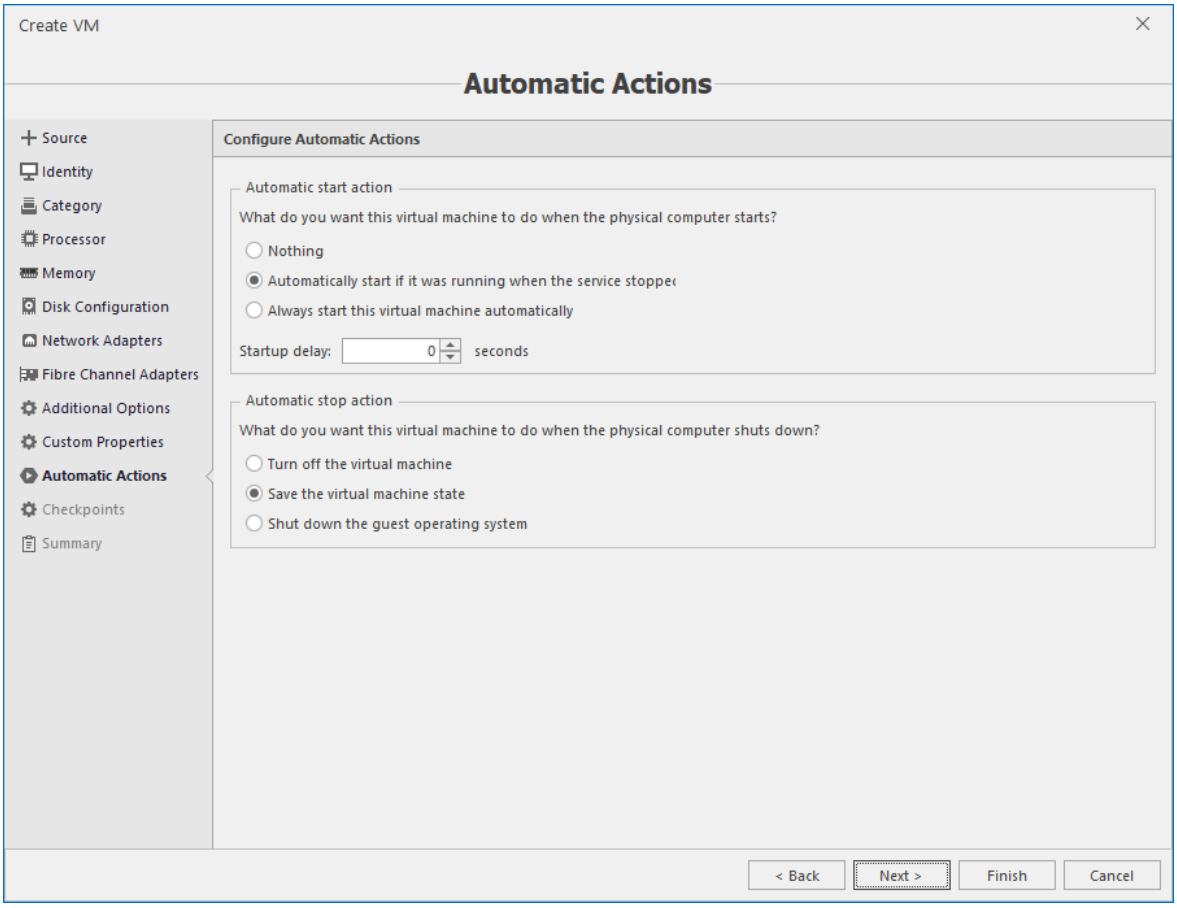
14. Specify OS installation options.



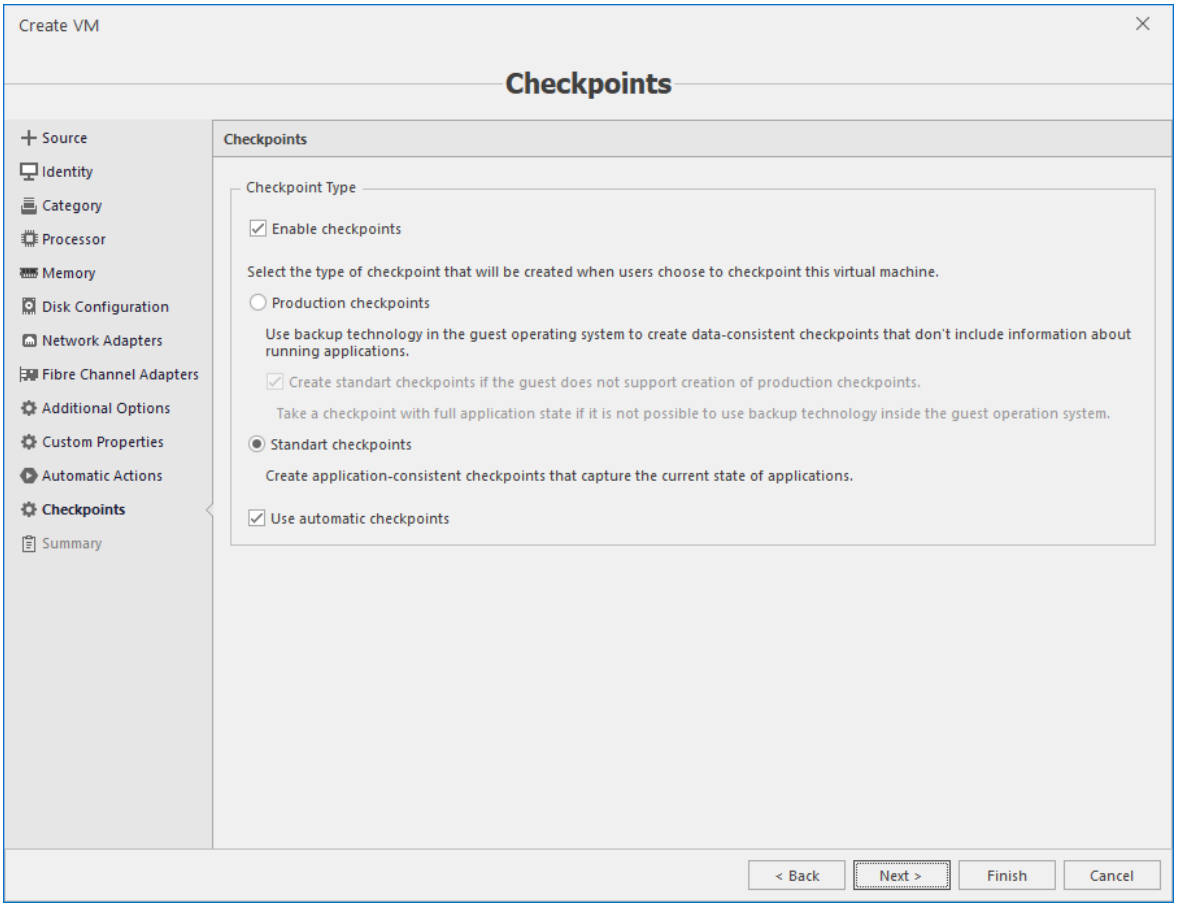
15. Add VM custom properties. While they will not have functional load, they will be displayed in the main window on the VM list (it is configurable option as for the other parameters) and can be used in filtering/ordering VMs on the list.



16. Configure automatic actions if necessary.

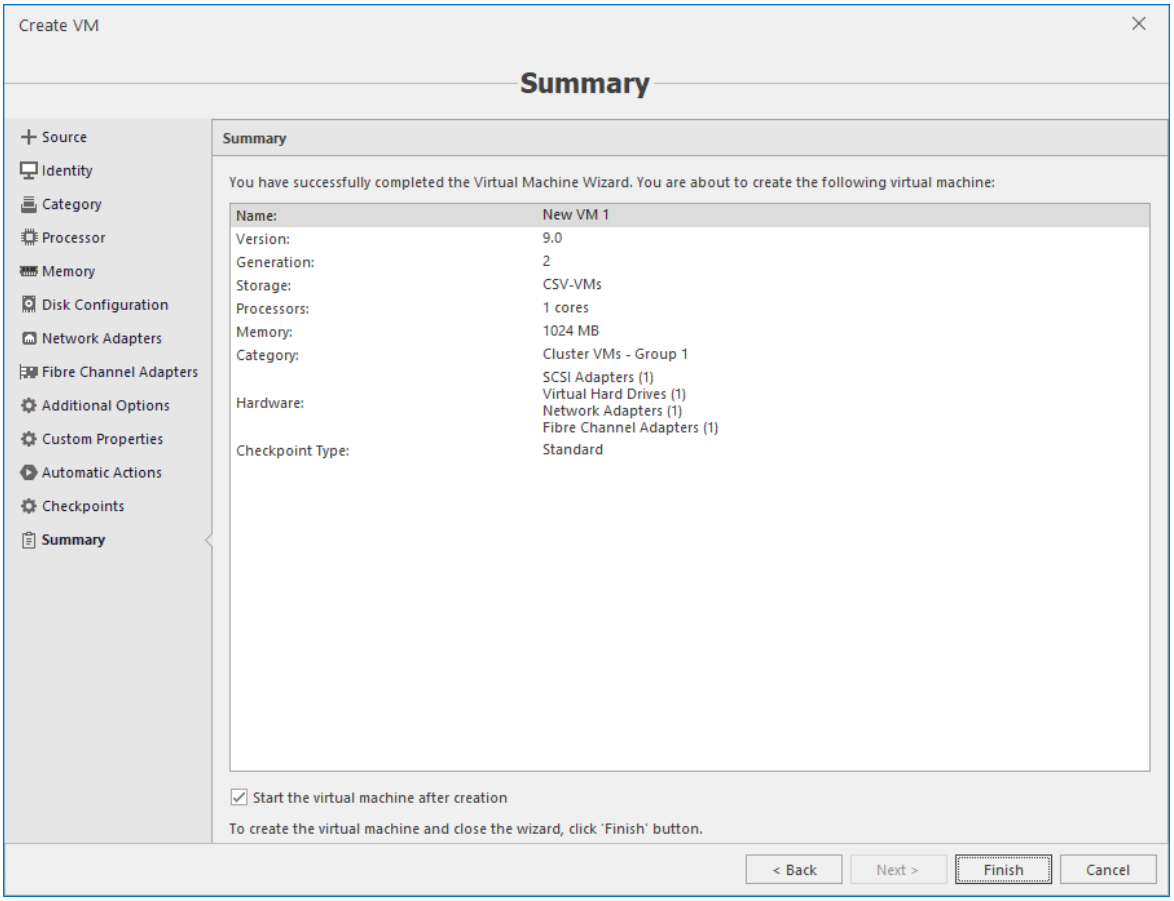


17. Configure the checkpoints creation options.



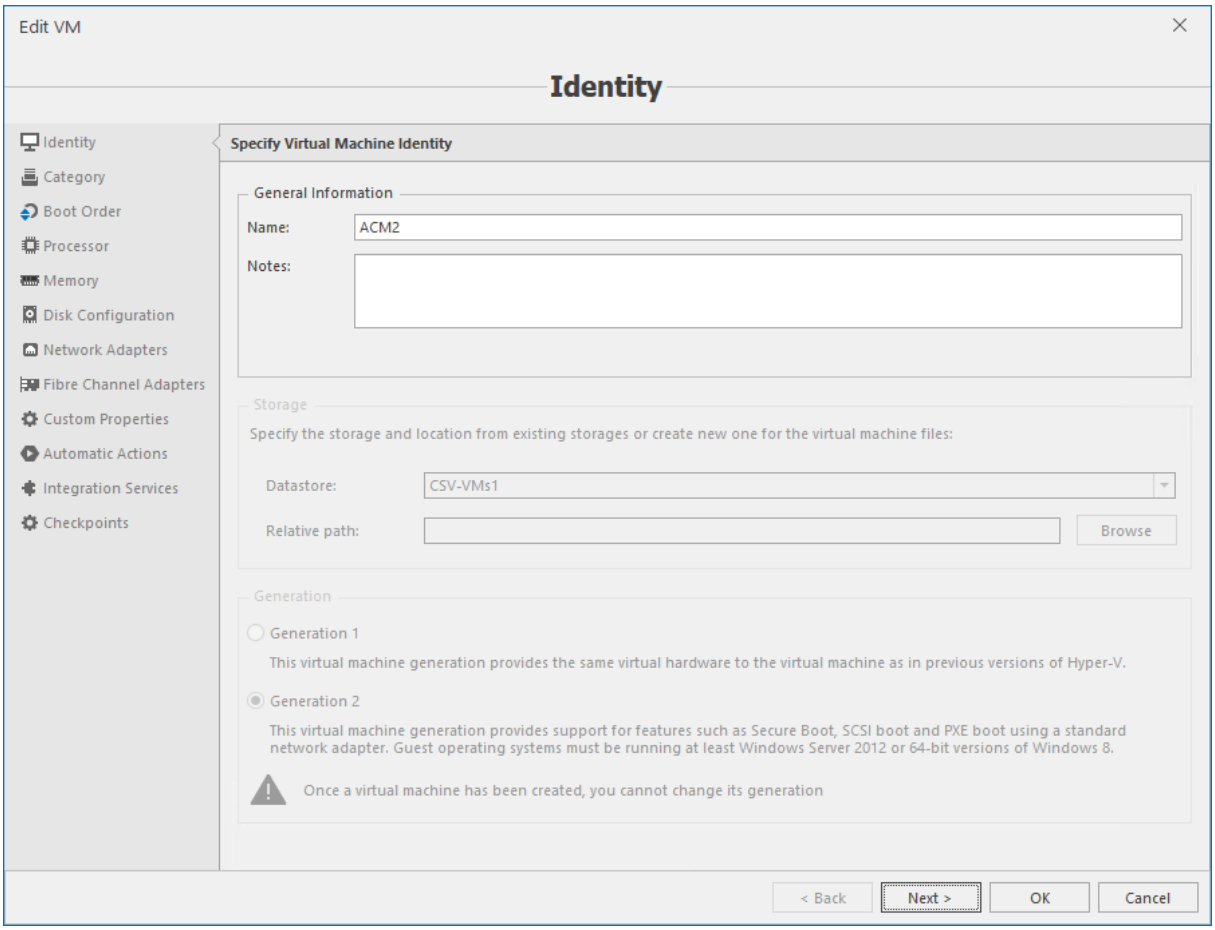
- Mark the **Enable checkpoints** box to enable checkpoints creation for the VM. If this box is unchecked, it will not be possible to create checkpoints for the current VM.
- Select the type of checkpoint to create by user or system (if the automatic creation option is enabled): **Production checkpoints** - to use backup technology in the guest OS that ensure data-consistency without information about running application; **Standard checkpoints** - to create application-consistent checkpoints that capture the current state of applications.
- Mark the **Use automatic checkpoints** option if you would like to let system check if the VM has checkpoints and create it automatically. If this option is enabled, the system will check if the VM has checkpoints or not each time the turned off VM is started, and if the VM has no checkpoints, an automatic checkpoint will be created, or it will happen likewise right after the new VM is created.

18. Check summary information and if everything is correct press **Finish** to create the new VM:



Editing VM settings

To edit VM settings select the VM and press the **Settings** button in the toolbar:



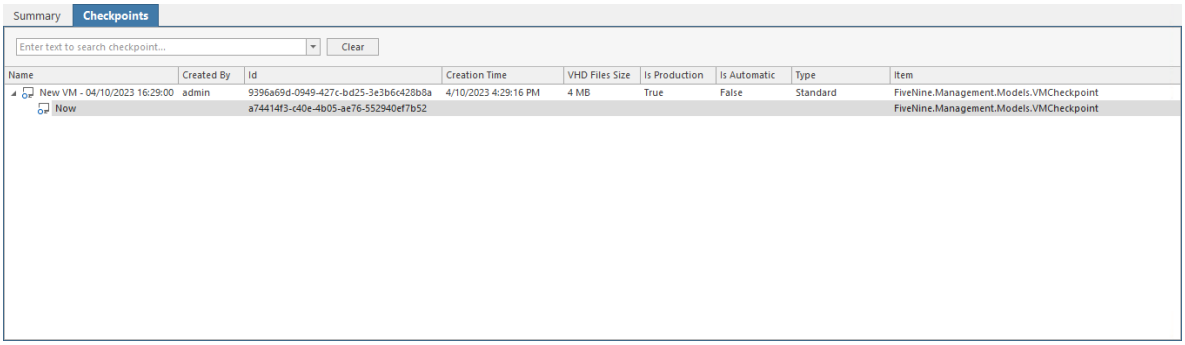
Note

You will find all options that were present when creating the VM. Some options, however, are not editable (like VM generation) or require the VM to be turned off to alter them.

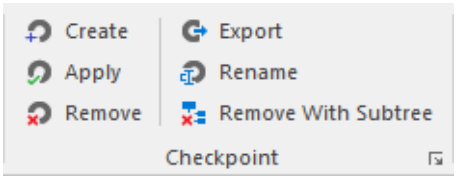
Standard operations

Acronis Cloud Manager supports standard operations with virtual machines (via toolbar or context menu commands):

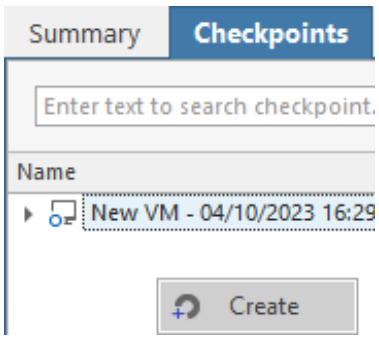
- Start.
- Turn off.
- Shut down.
- Save.
- Pause/resume.
- Reset.
- Rename.
- Delete.
- Operations with checkpoints: create, apply, remove, rename, export. To view VM checkpoints, select the VM in the objects tree and switch to the **Checkpoints** tab or click the **Checkpoints** button on the main ribbon or corresponding context menu item, which will lead you there likewise:



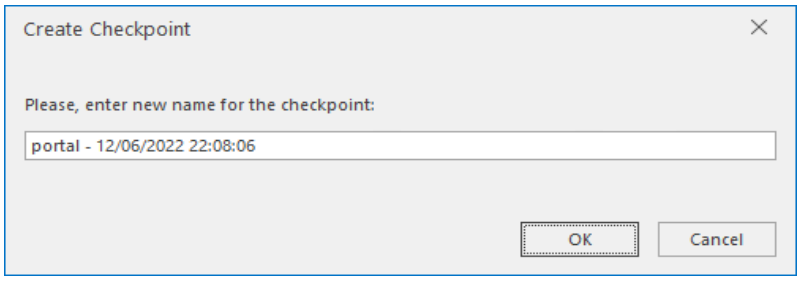
If VM has checkpoints, they will appear in the tab in a hierarchical tree view. Each one will display the creation date, time and the user name, who created it. All available operations will appear in the **Checkpoint** section of the main ribbon:



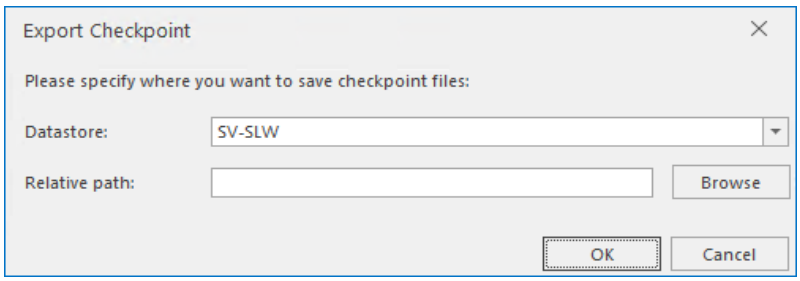
- To create the checkpoint click the **Create** button or right click on the empty space of the checkpoints field and press the **Create** context menu command:



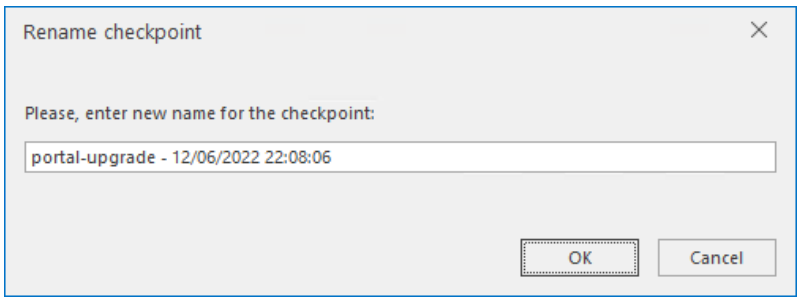
Then enter the name for the checkpoint if necessary (the default value will contain VM name, current date and time). Click **OK**:



- To apply the checkpoint, select it in the tree and click the **Apply** button.
- To remove the checkpoint (or remove it with the whole subtree), select it and click the **Remove** (**Remove with subtree**) button and confirm the operation.
- To export the checkpoint, select it and click the **Export** button. Then select the datastore and relative path to export the checkpoint to and click **OK**:

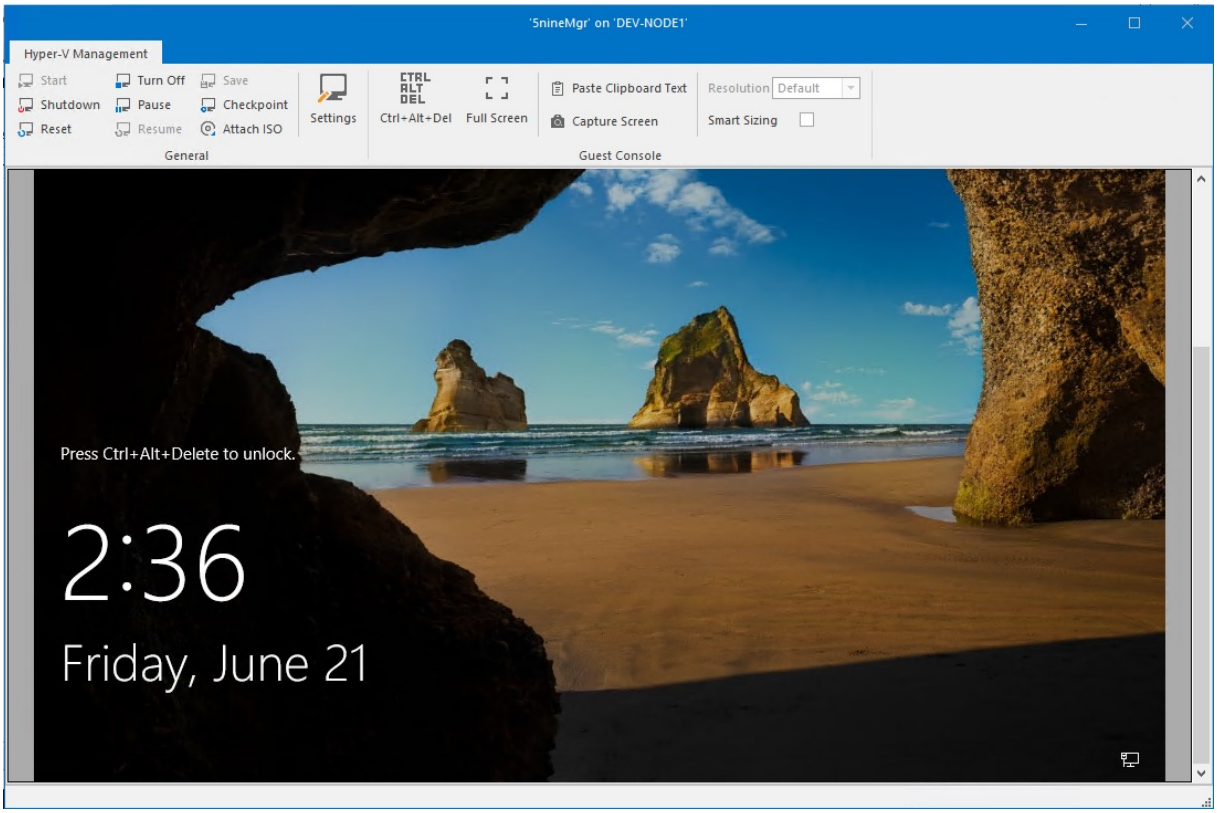


- To rename the checkpoint, select it and click the **Rename** button. Then enter the new name for the chekpoint and click **OK**:



- Connect via guest console.

Note
Prior to using VM guest console you need to set appropriate credentials for Hyper-V host in the objects tree. Then to view VM guest console select the VM in the objects tree and click the **Connect** button on the main ribbon. The guest console will be opened in the separate window:



Adding and removing VM to/from cluster

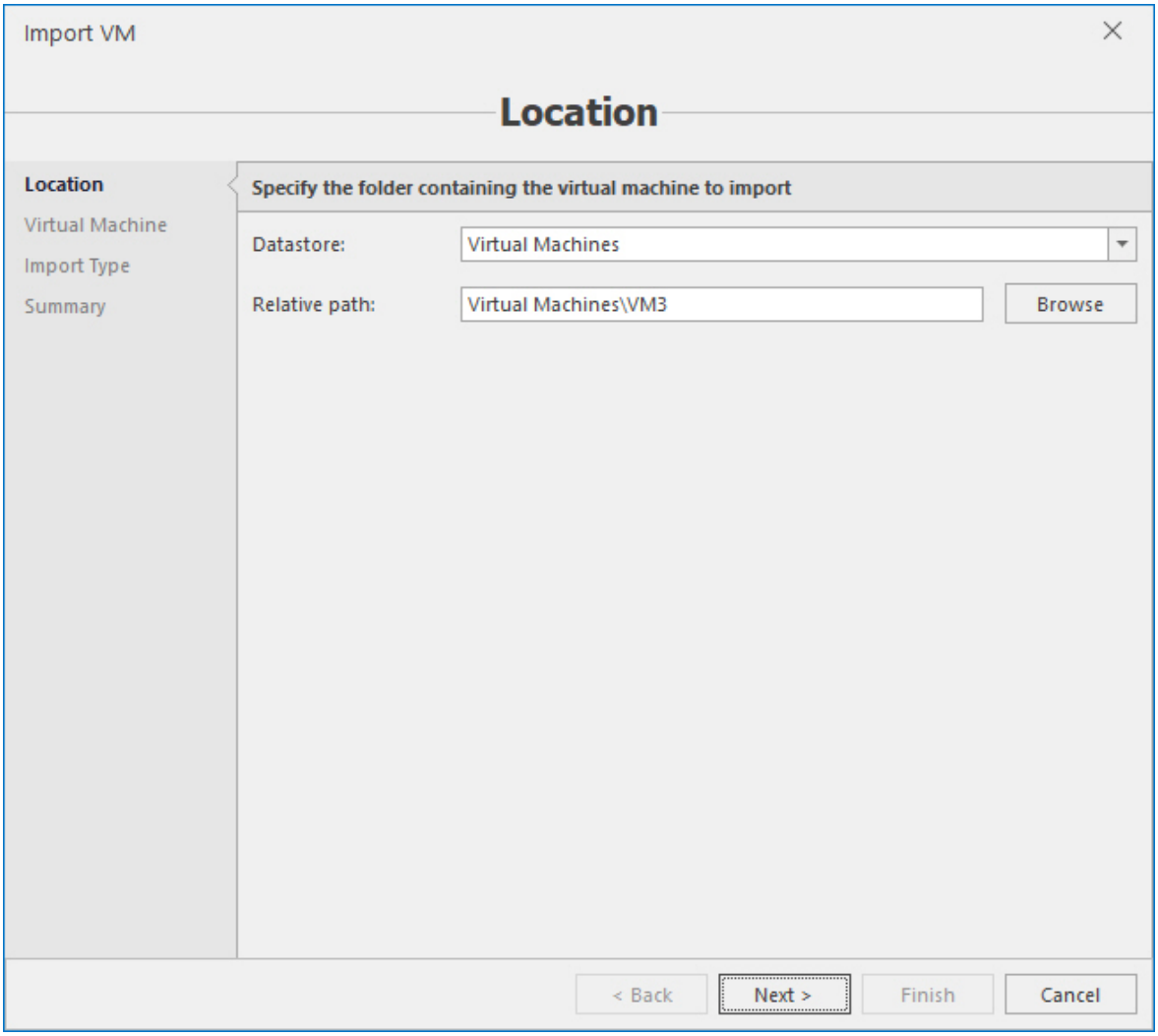
To remove the clustered VM from the cluster, select the cluster in the Acronis Cloud Manager object tree, and then select the VM that you need to remove from cluster and right click on it. Select the **Remove from cluster** command.

If you want to add a non-clustered VM to the cluster, select the **Add to cluster** command. Make sure you have moved the VM configuration files and VHD(s) to the CSV prior to adding it to the cluster.

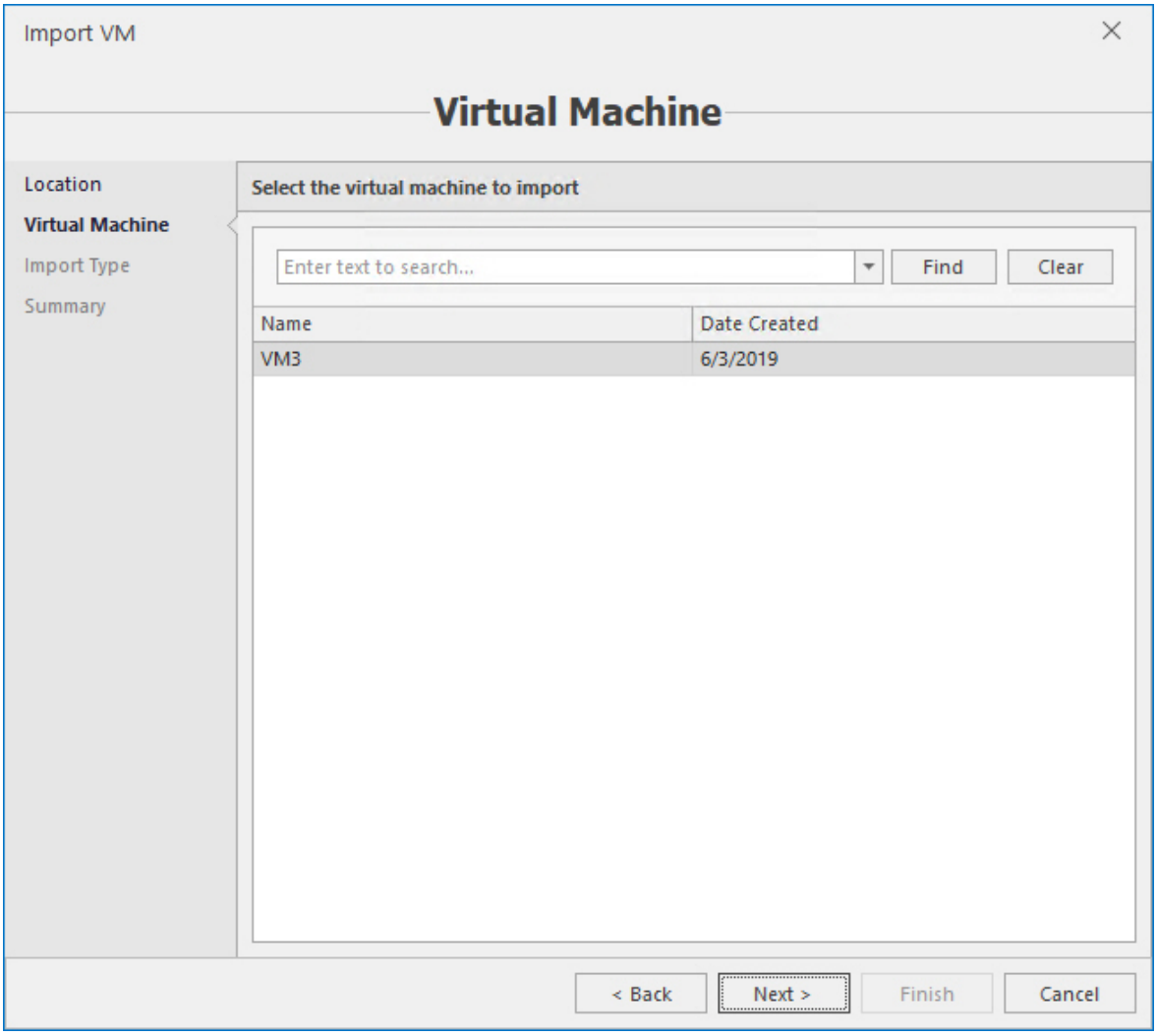
Importing VM

1. To import VM select the host and press the **Import VM** button on the main panel menu. The **Import VM** wizard will be opened.

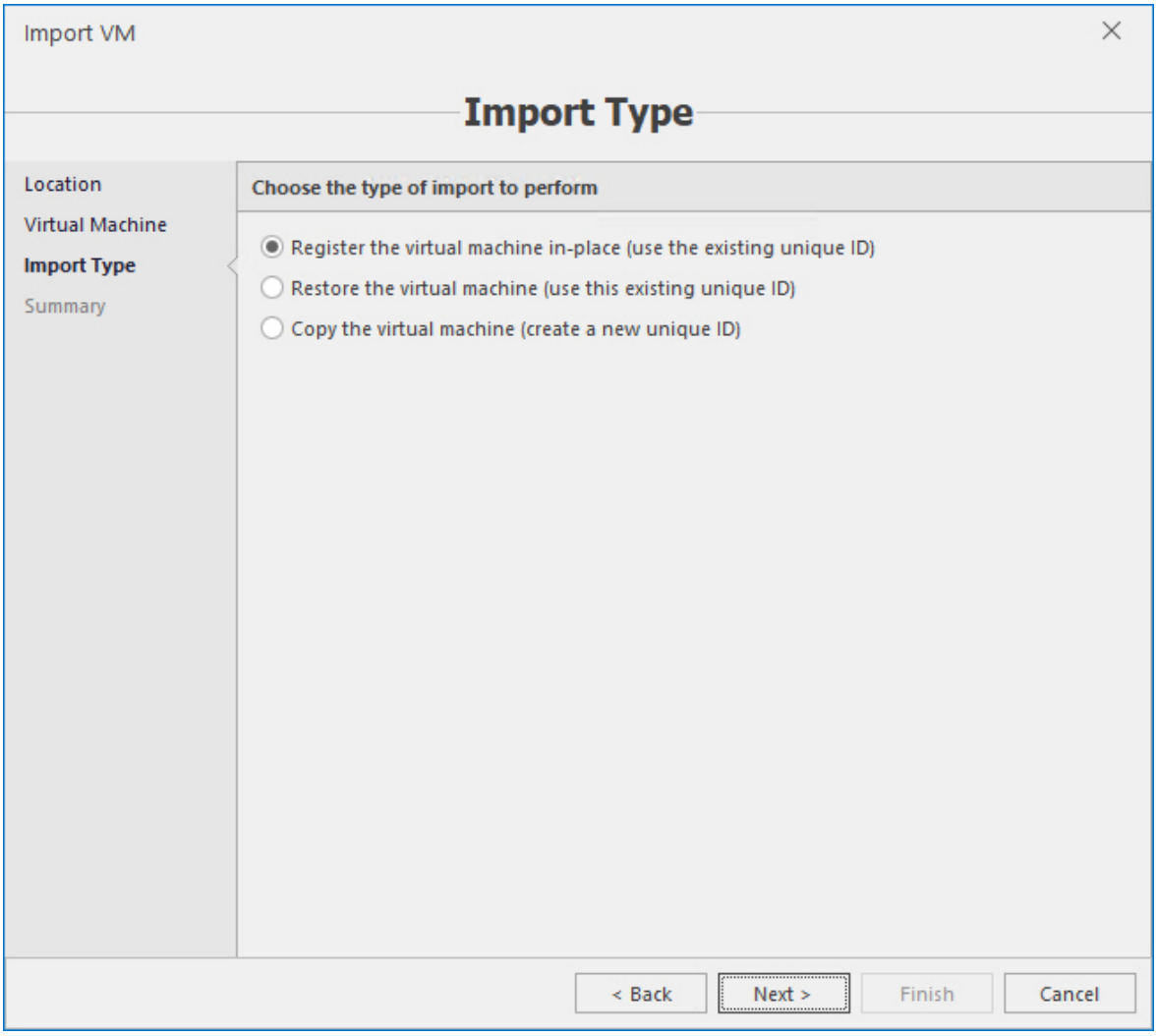
2. Select the datastore and define the relative path that contains VM data:



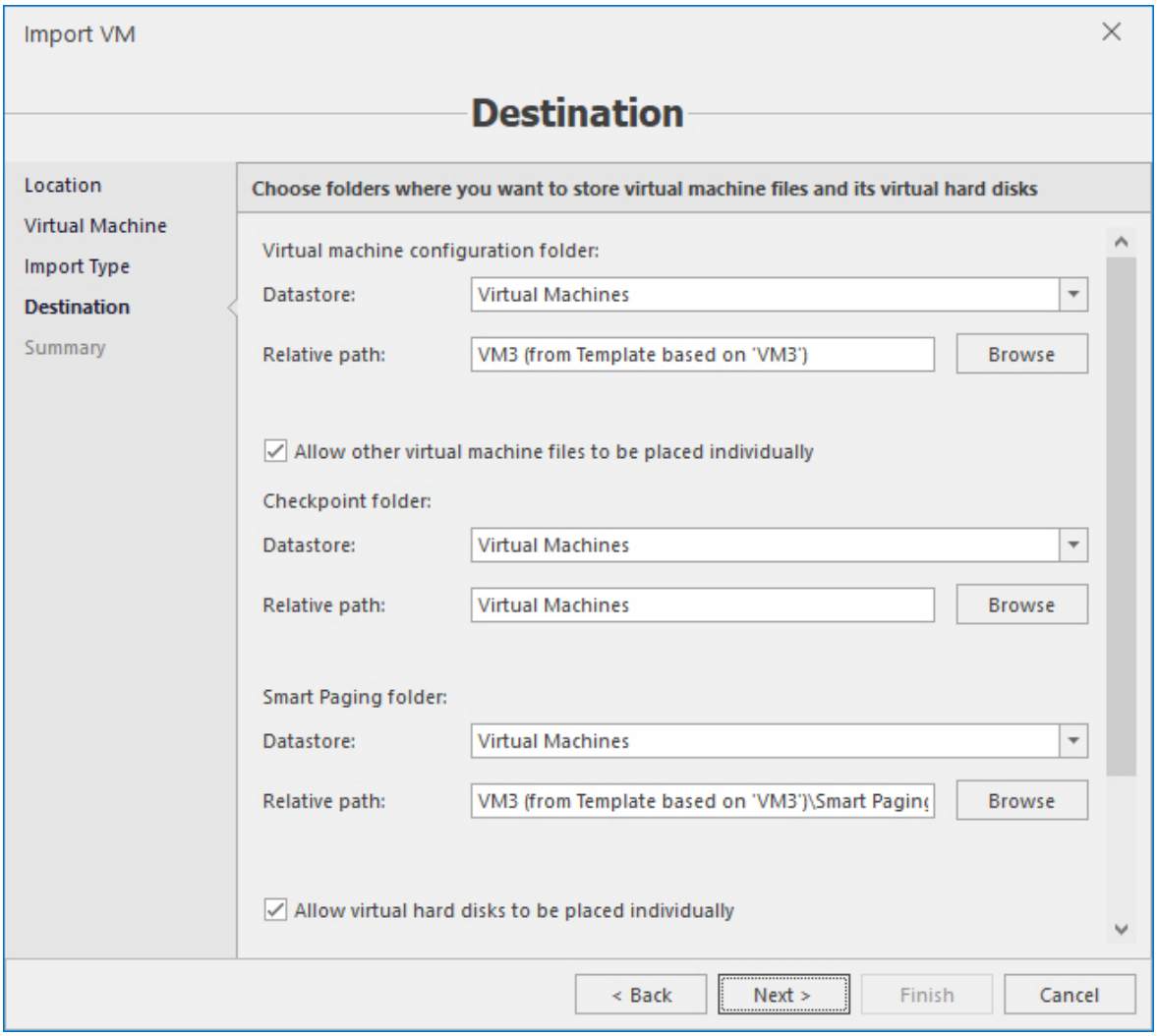
3. Select the VM data to import:



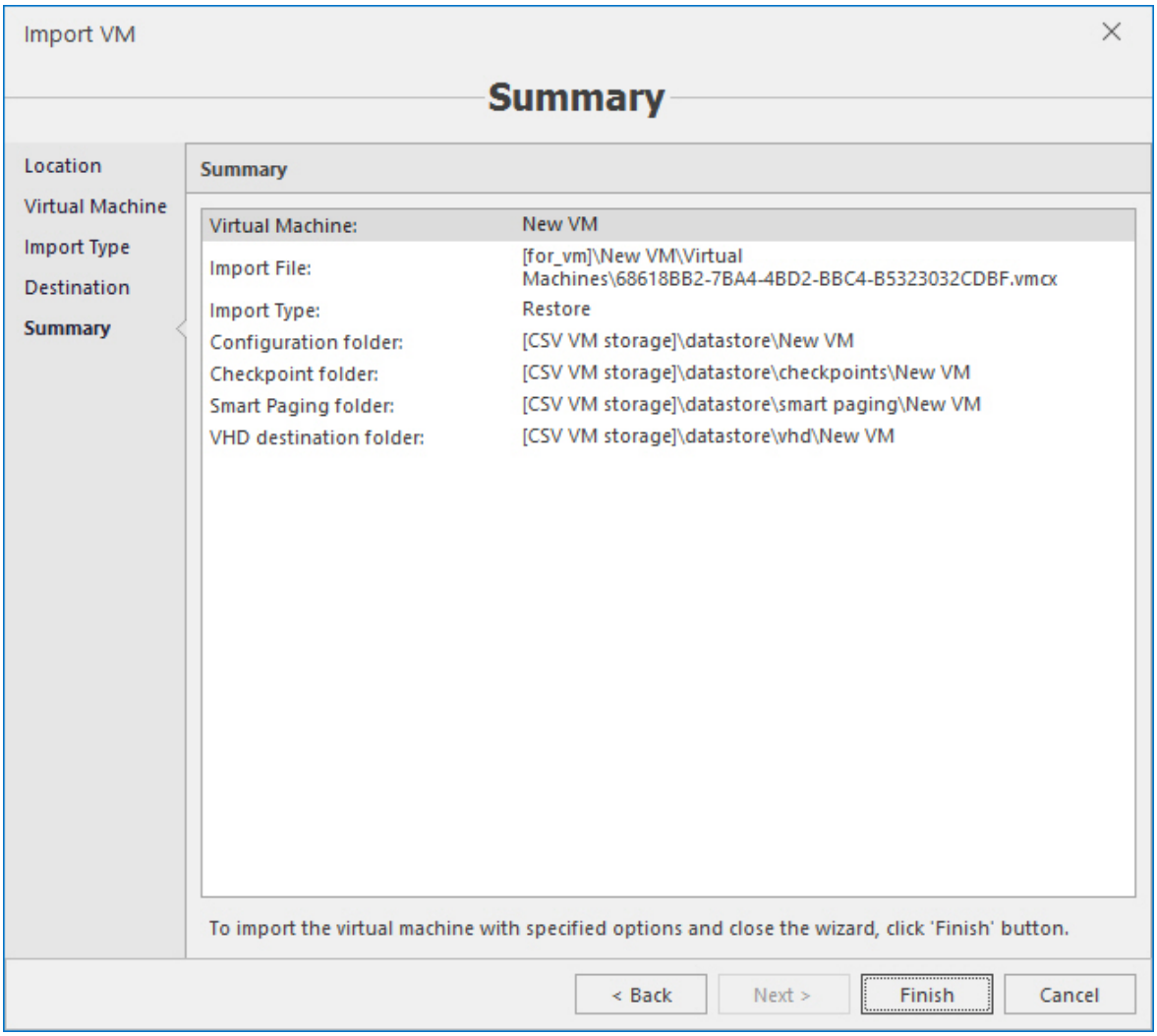
4. Select import type.



5. If the 2nd or 3rd option were selected at the previous step, provide destination options for a VM.

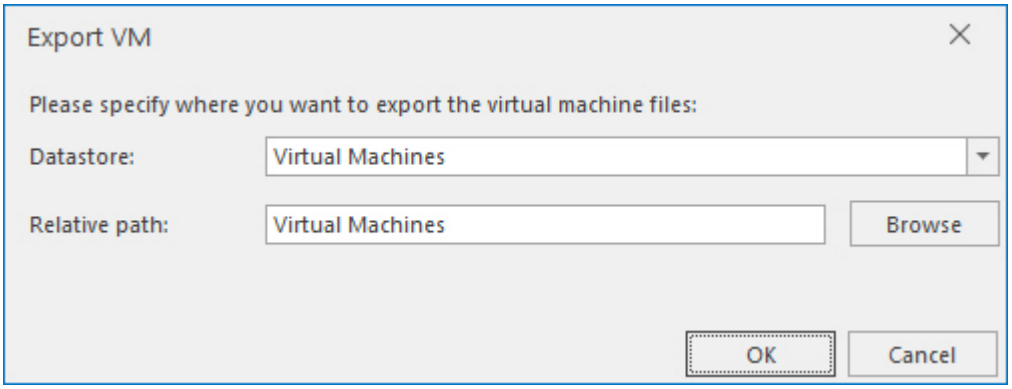


6. Check summary information and if everything is correct press **Finish** to start the VM import operation.



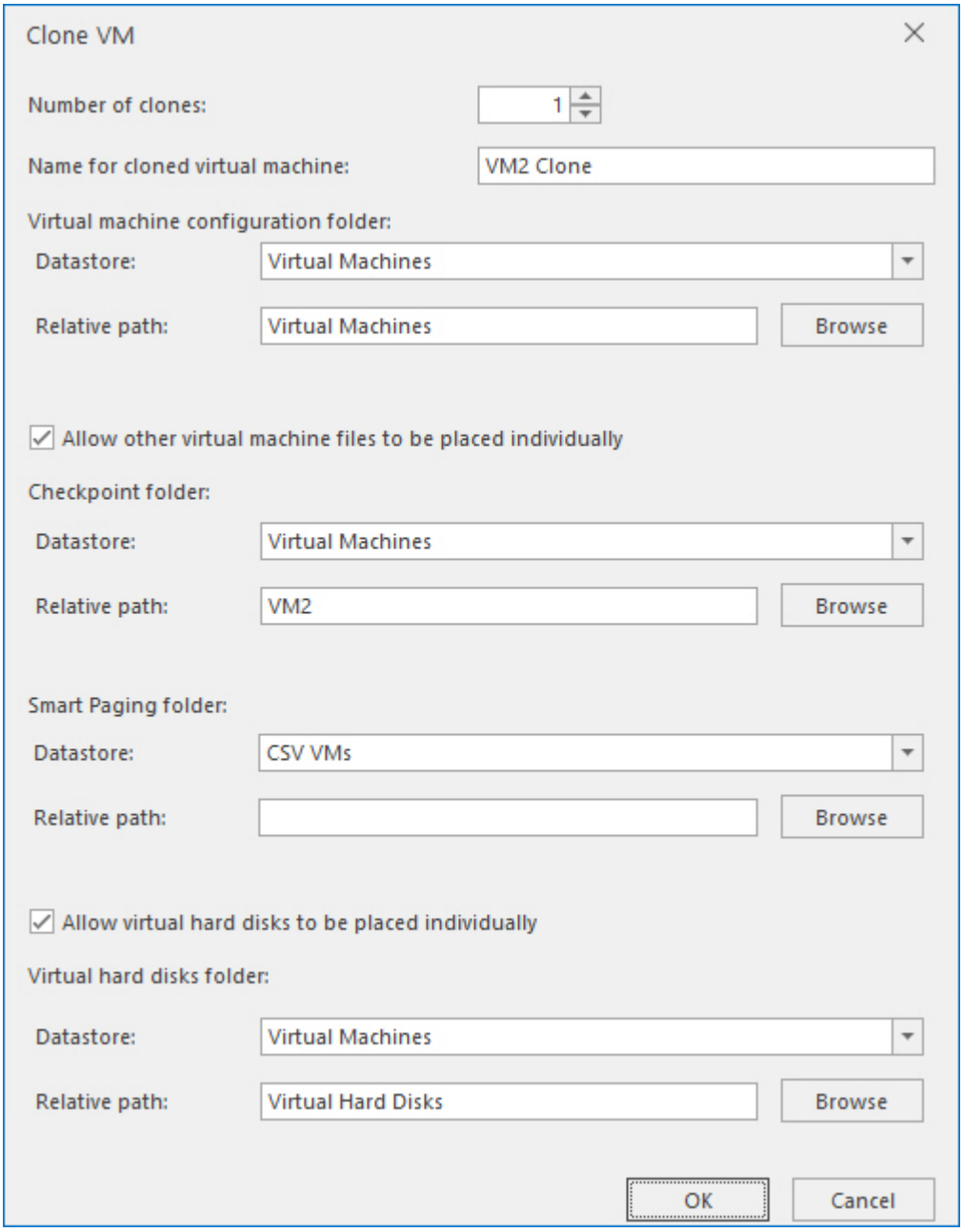
Exporting VM

1. To export VM select it and press the **Export VM** button in the toolbar. The **Export VM** dialog will be opened.
2. Define the datastore and the folder where you want the VM to be exported and press **OK**.



Cloning VM

To clone VM select it and press the **Clone VM** button in the toolbar. The **Clone VM** dialog will be opened.



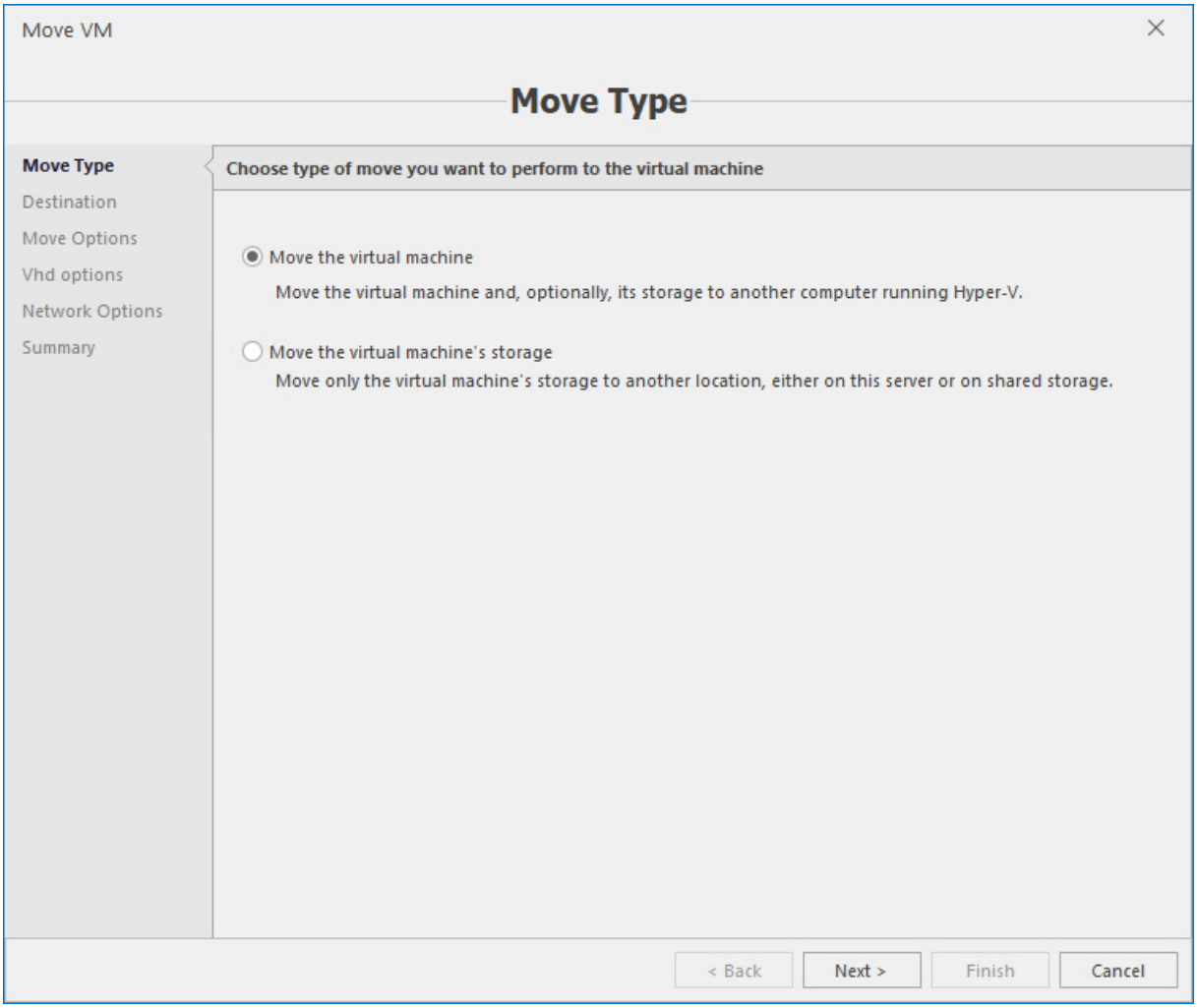
Provide the number of clones, clone name patterns and the datastore parameters and press **OK**.

Shared nothing VM migration

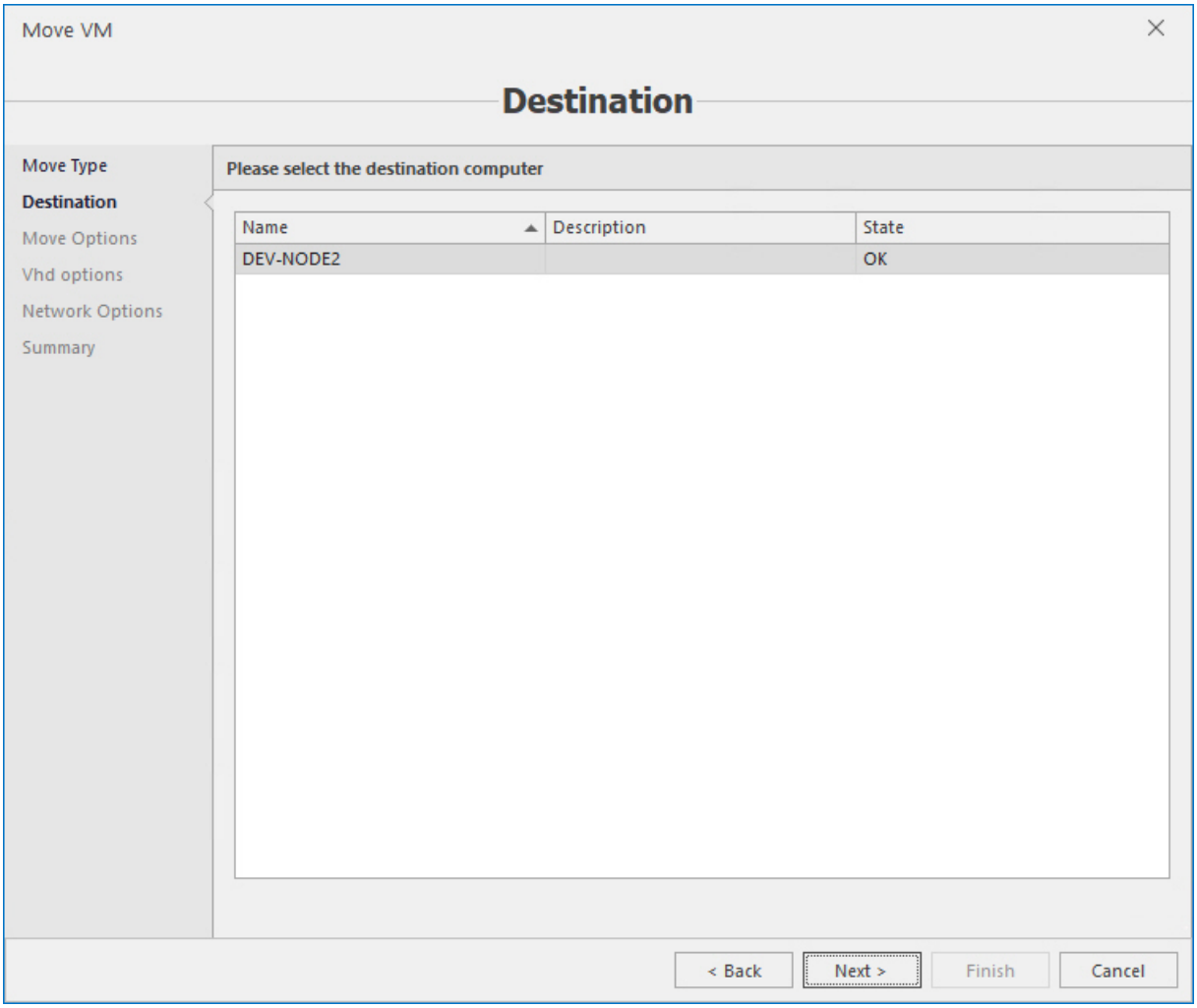
This operation allows moving VM with/without its storage or a VM storage only to another Hyper-V host. This operation is available for non-HA VMs in both clustered and non-clustered environments.

To move the non-HA VM select it and press the **Move VM** button in the toolbar. The **Move VM** wizard will be opened.

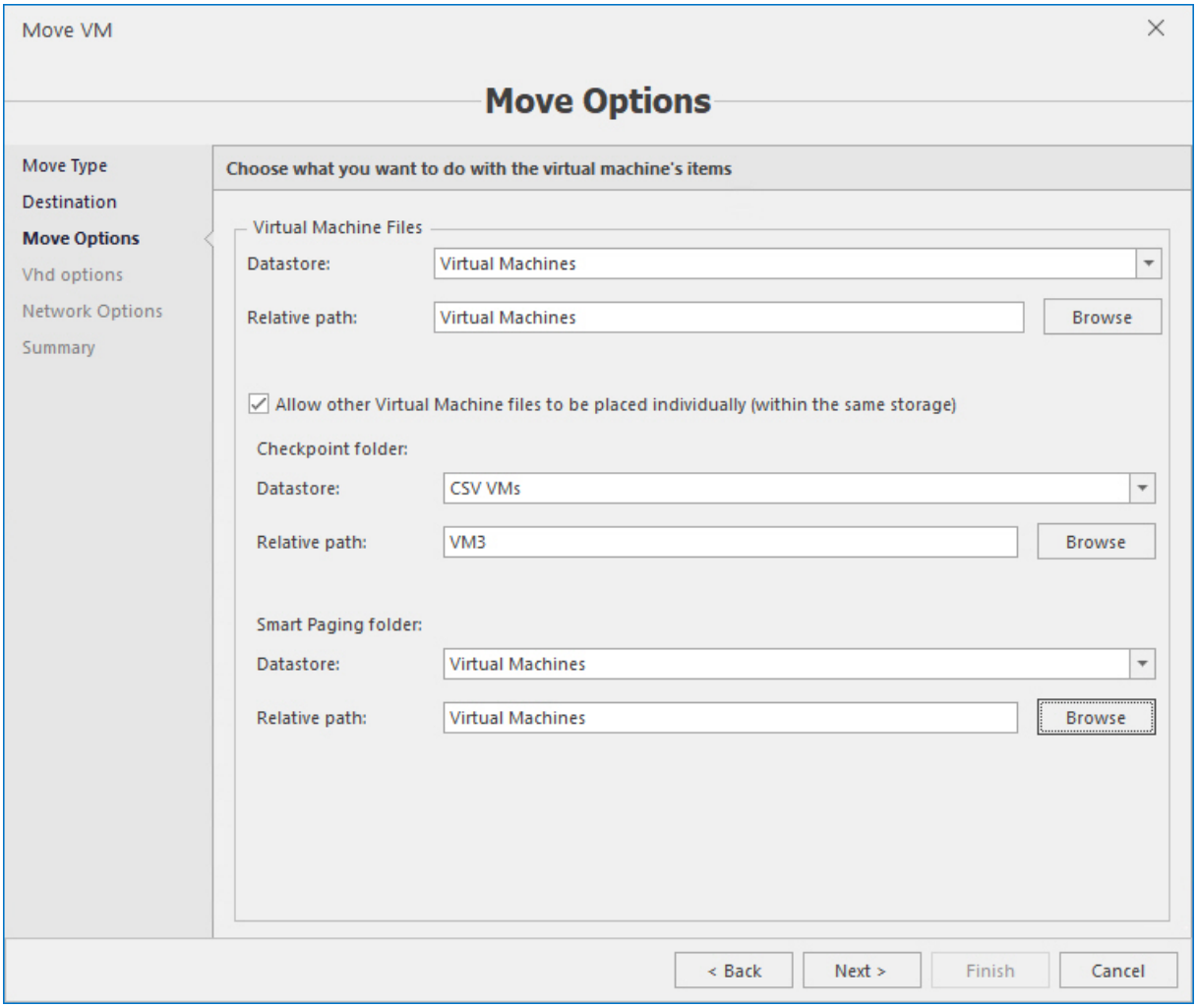
1. You can move the virtual machine or move just the virtual machine's storage here.



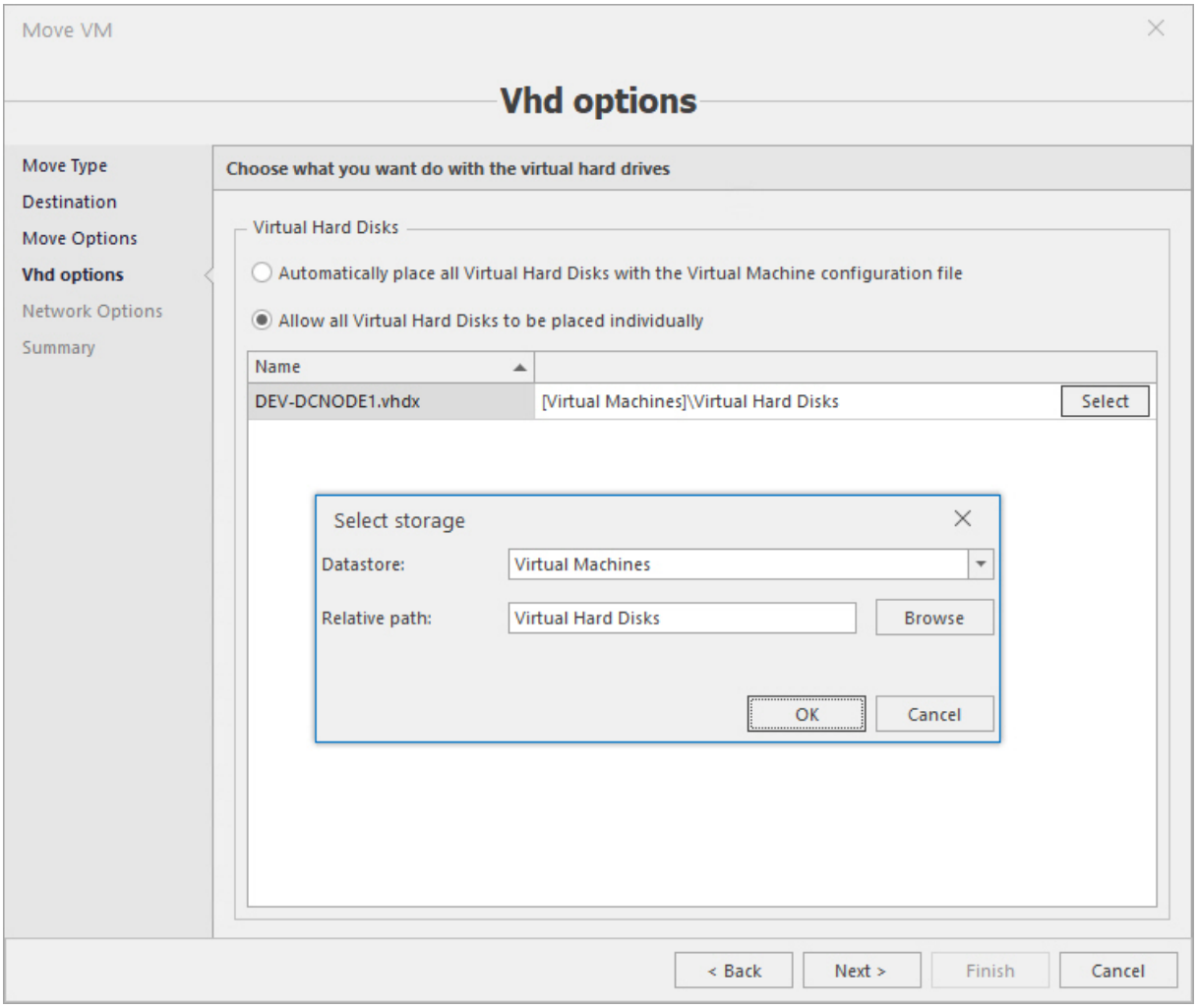
2. Select the destination host:



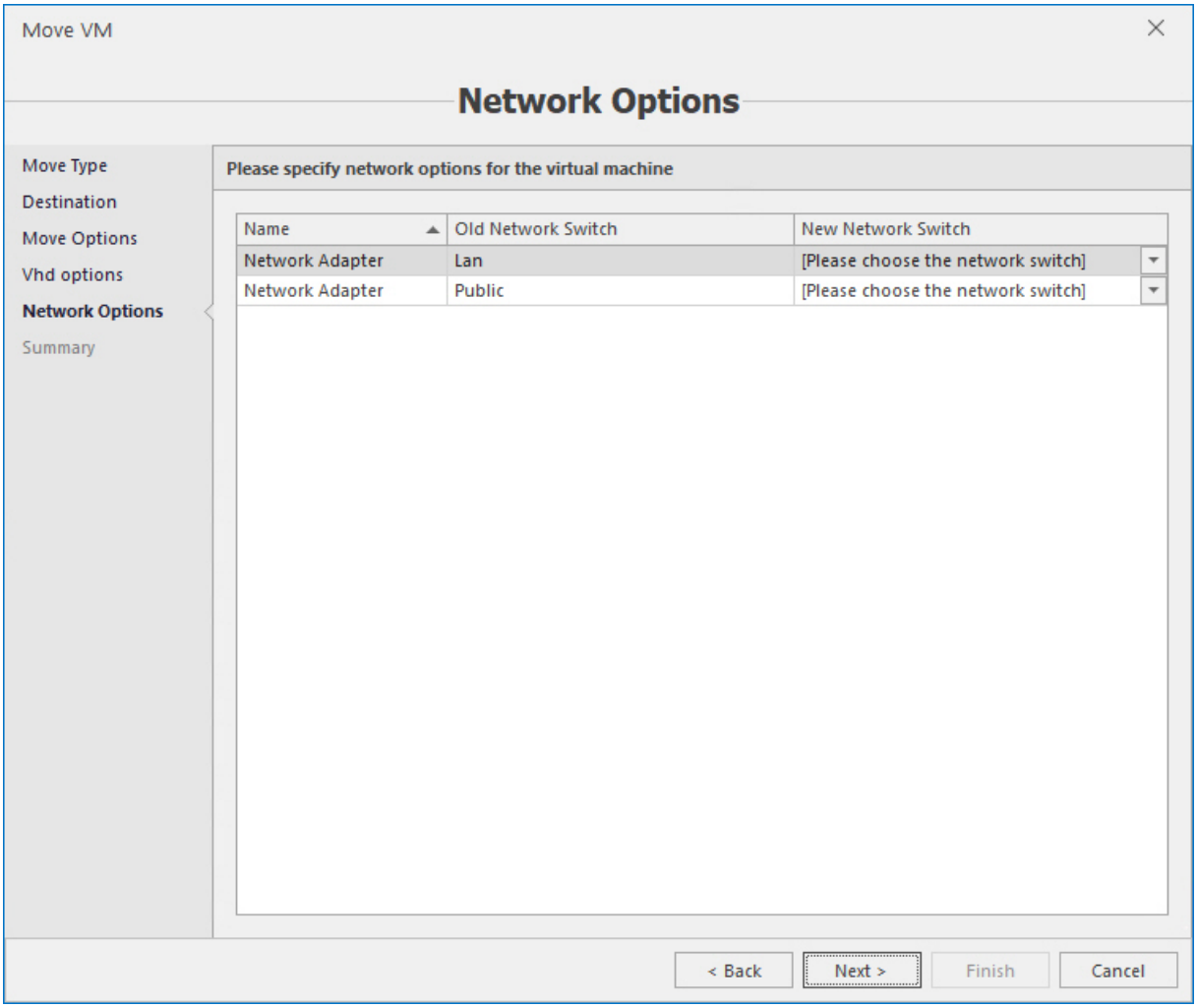
3. Specify move options:



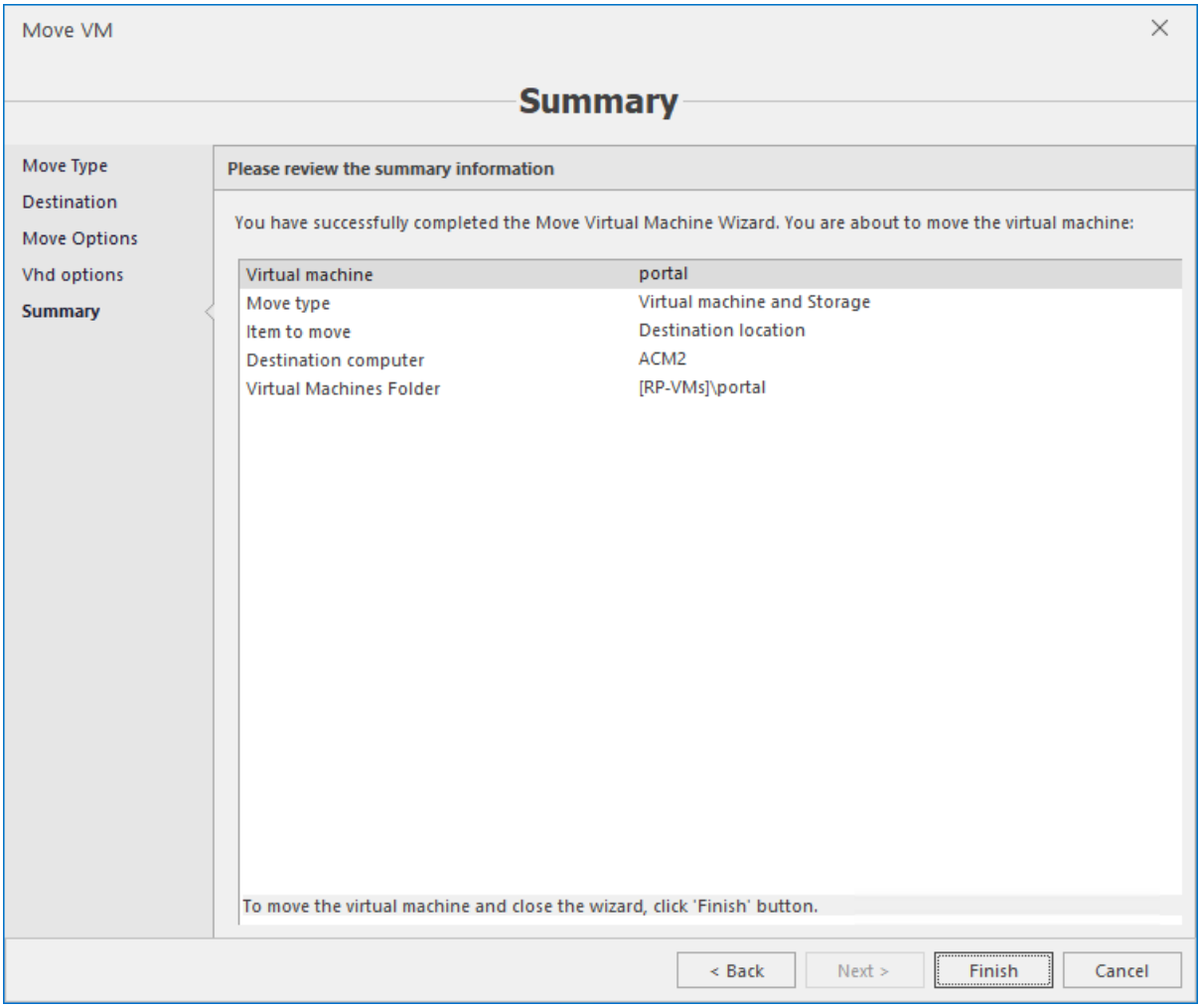
4. Select the parameters to move the VHD:



5. Select physical network that will be used for the operation:

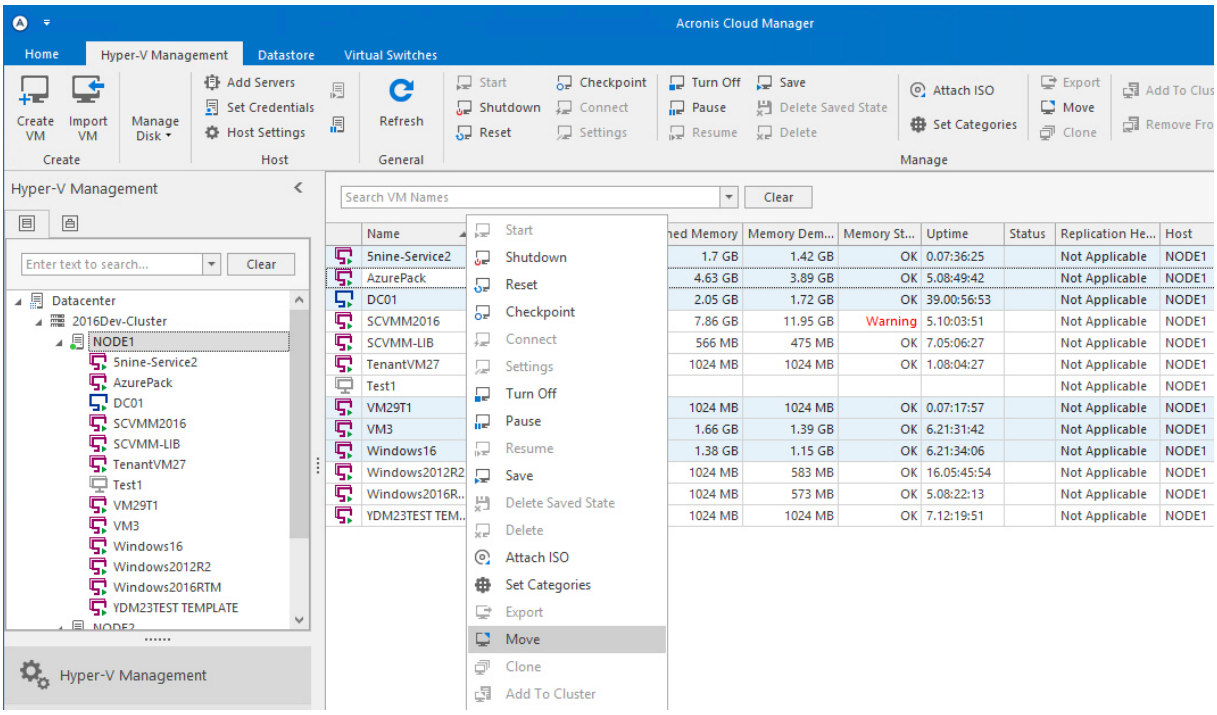


6. Check summary information and, if everything is correct, press **Finish** to move a VM/storage.

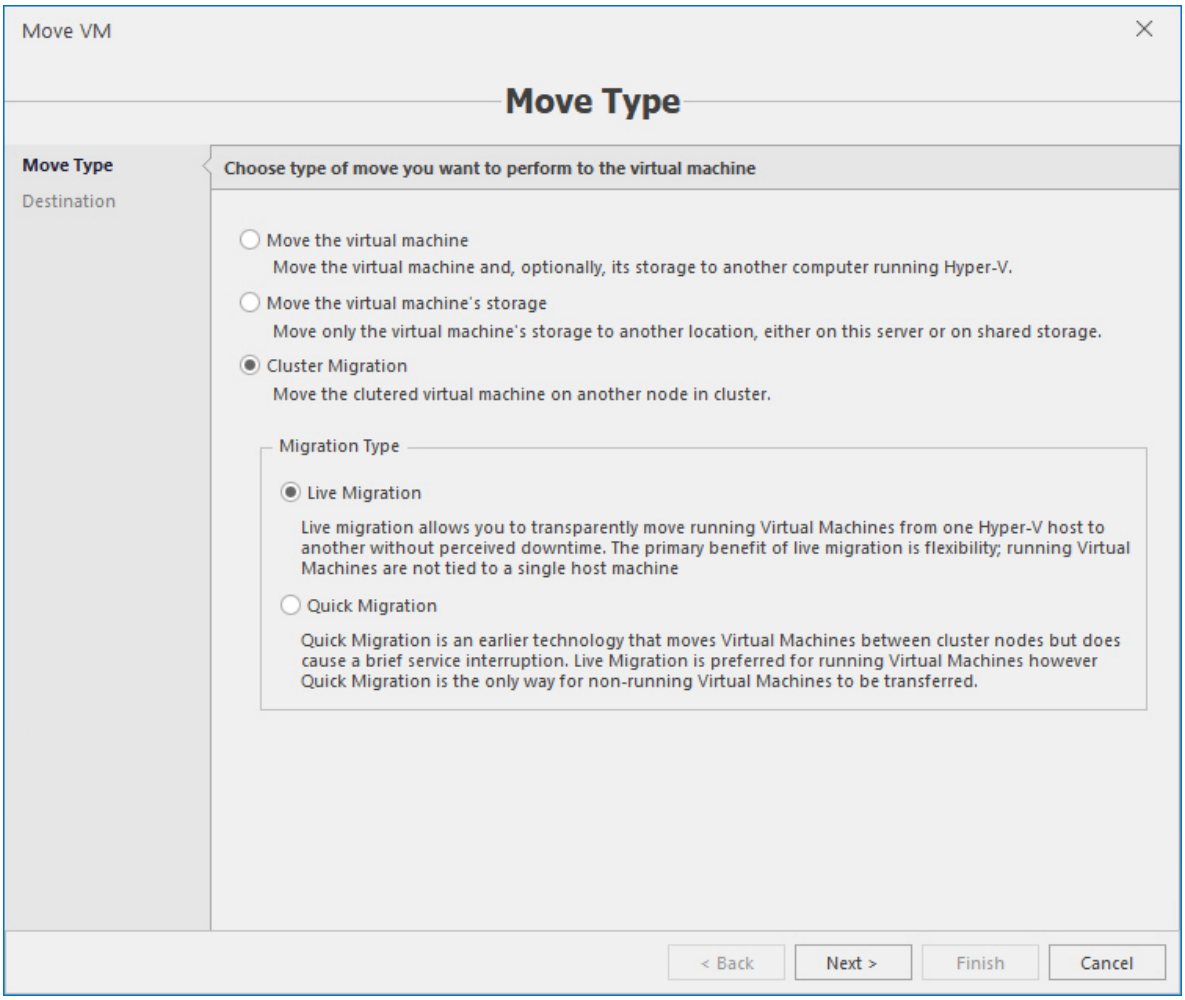


Live and quick VM migration

These operations apply to clustered VMs. To move the VM between nodes that joined into a cluster, first select the cluster in the Acronis Cloud Manager object tree, and then select the VM that you need to move to another node and click the **Move** button in the toolbar. You may select multiple VMs for this action. To do this, first select the target host in the object tree. Then select the VMs that you need to migrate on the right pane, using **Ctrl+Shift** keys and click the **Move** button on the main command ribbon or the corresponding context menu command by using the right-click.

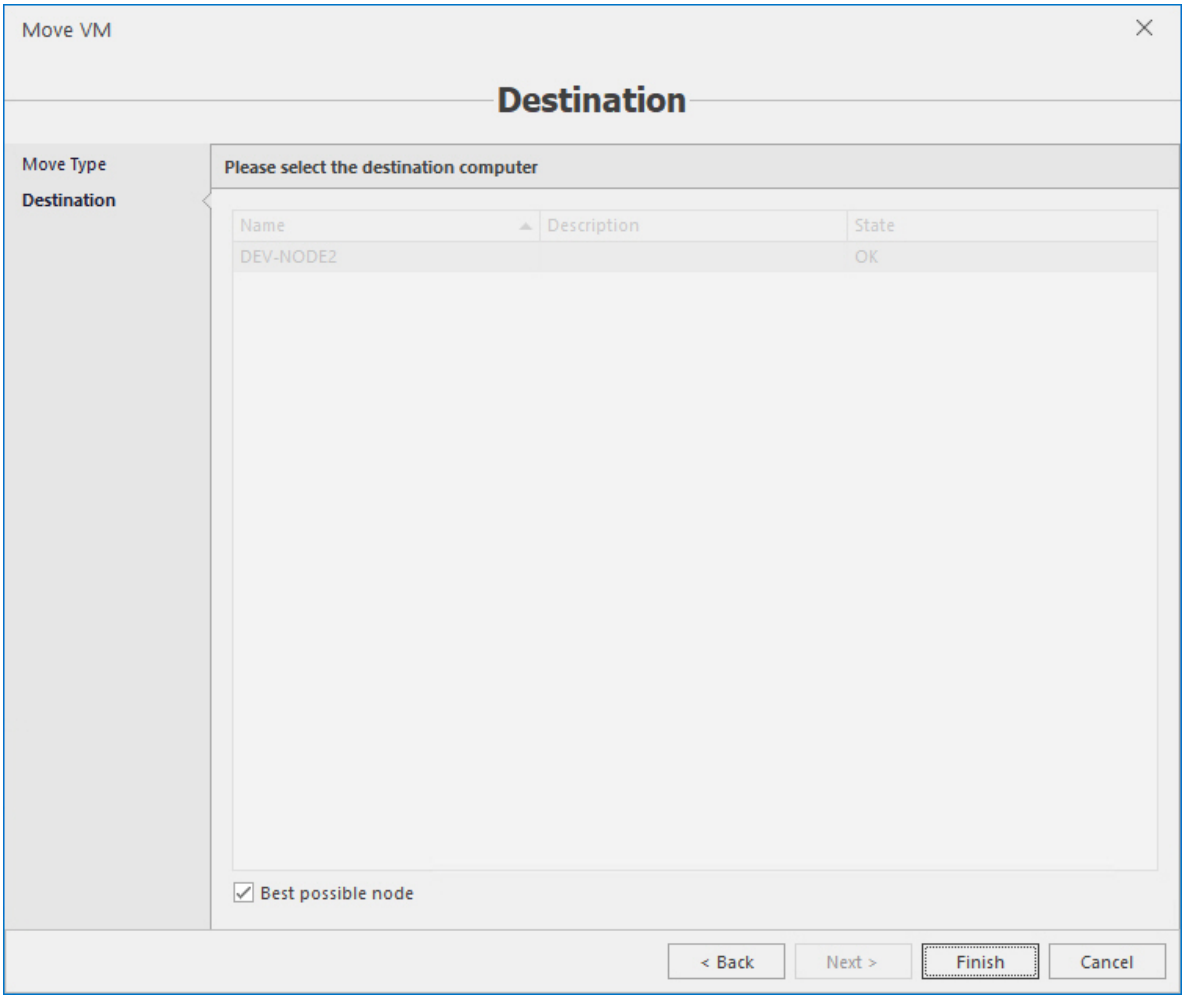


- Select the **Cluster migration** option and the migration type:



- **Live migration**. With this option, a virtual machine will be migrated without switching to the saved state and losing the access. This operation is applicable to virtual machines that are in active (running) state only.
- **Quick migration**. With this option, a virtual machine will be migrated to another node as quickly as possible, but it will be switched to the saved state during the operation. That means access to this virtual machine will be temporarily lost until it returns to the running state on the new node. This operation is applicable to virtual machines in any state – active (running), paused, saved or off.

- Select either **Best possible node** so that the system will choose it automatically or select the exact node you would like the VM to be moved to.

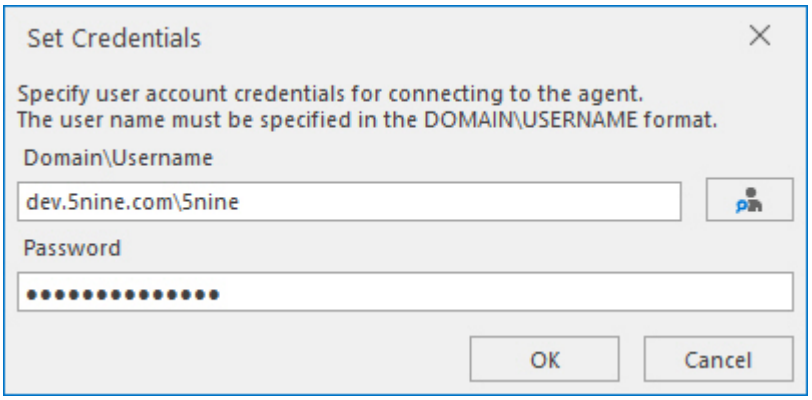


Press **OK** to start migration.

Guest console connection

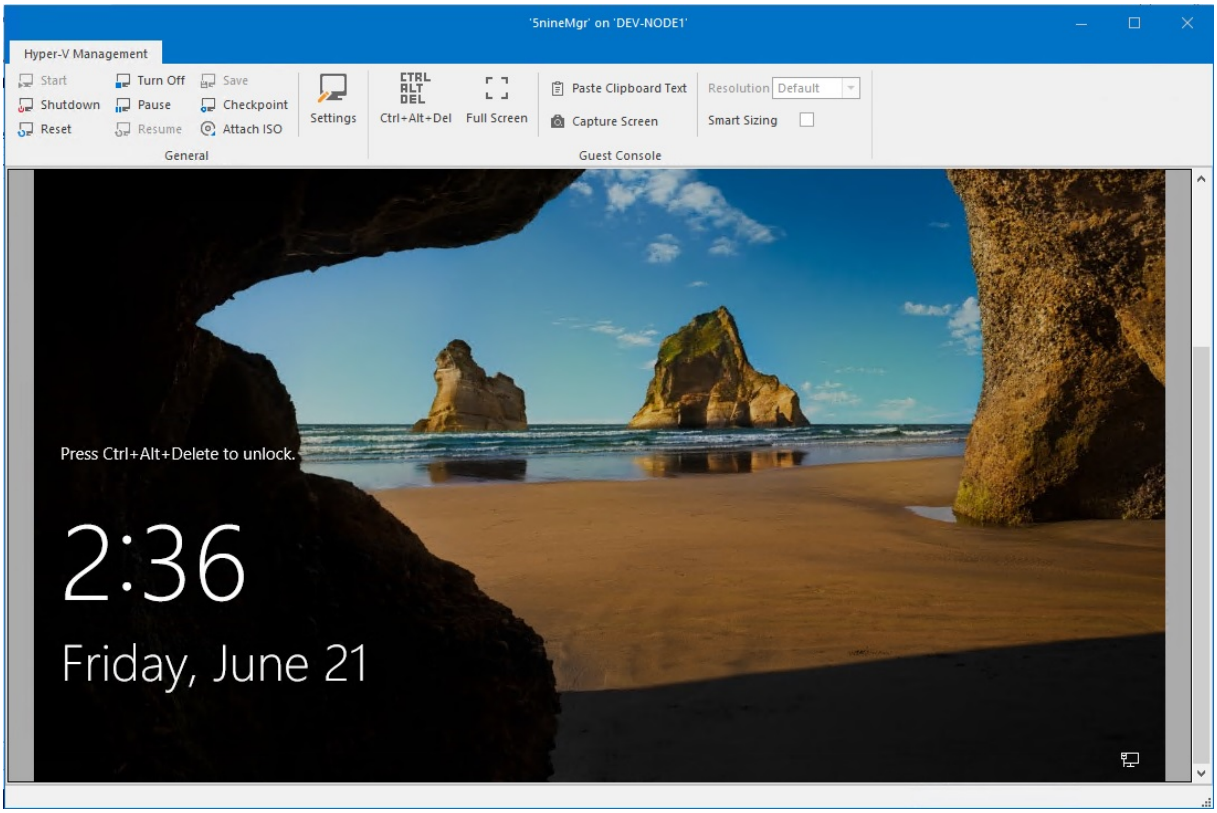
If management console is on the same network as management server and Hyper-V hosts then you need only set access credentials for every hosts in the objects tree.

Select the host and press the **Set credentials** button in the toolbar.



Note

If everything is configured, select the VM and click the **Connect** context menu command. Guest console for the selected VM will be opened in a separate window.



Hyper-V replication

Hyper-V replica allows virtual machines running at a primary site to be efficiently replicated to secondary location (replica site) across a WAN link. Primary and replica server must be Microsoft Hyper-V 2012 R2 as a minimum.

When replication is underway, changes in the primary virtual machines are transmitted over the network periodically to the replica virtual machines. The exact frequency varies depending on how long a replication cycle takes to finish (depending in turn on the network throughput, among other things). In the

latest versions of Windows Server, you can configure the replication frequency, so that the changes are sent every 30 seconds, every 5 minutes, or every 15 minutes.

You can also access recovery points up to 24 hours old (previously, recovery points up to 15 hours old were available).

If the primary server should fail unexpectedly, perhaps of a major hardware failure or a natural disaster, you can bring up the replica virtual machines to take over the workload — this is *unplanned failover*. In unplanned failover, there is the possibility of data loss, since there was no opportunity to copy over changes that might not have been replicated yet.

Prerequisites

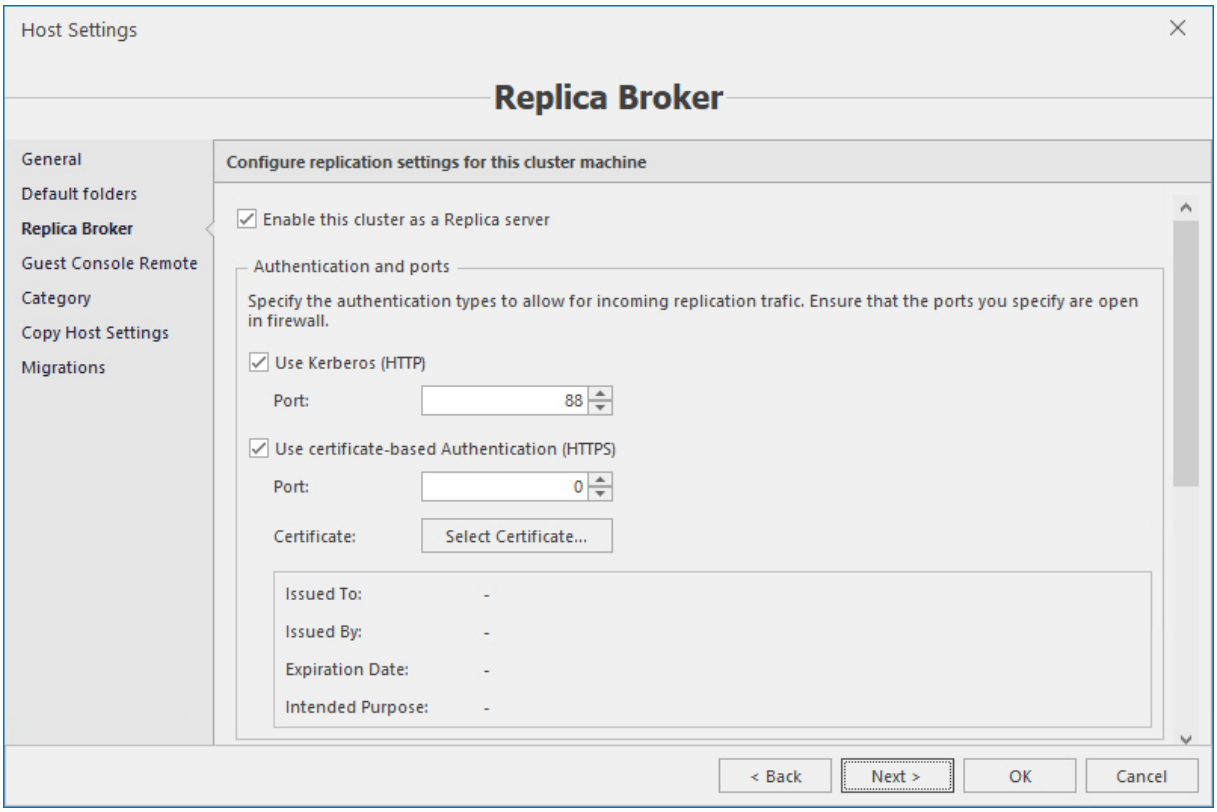
To take advantage of the Hyper-V replica, which is included as part of the Hyper-V server role, the following pre-requisites must be met:

- Hardware that supports the Hyper-V role on Windows Server;
- Sufficient storage on both the primary and replica servers to host the files used by virtualized workloads;
- Network connectivity between the locations hosting the primary and replica servers;
- Properly configured firewall rules to permit replication between the primary and replica sites;
- An X.509v3 certificate to support mutual authentication with certificates (if desired or needed)

To start VM replication, select the VM and press the **Replicate** button in the toolbar.

Host replication settings

Replication settings is a part of host settings. You need to set replication settings if a Hyper-V host is supposed to be used as a replica server.

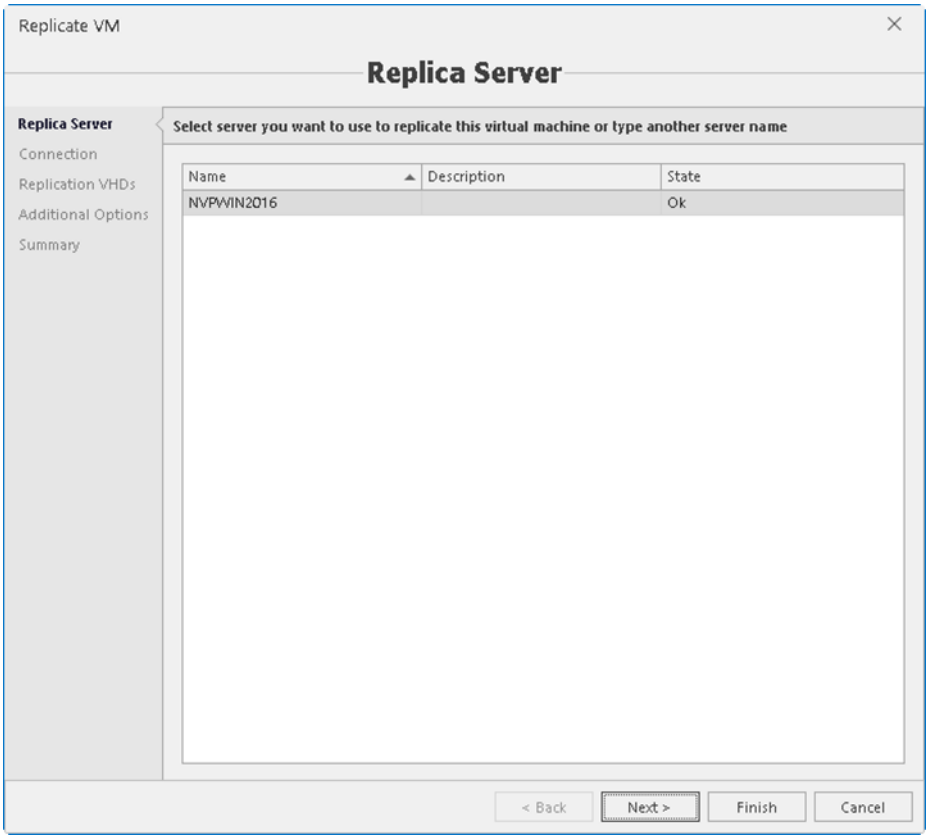


There are the following settings:

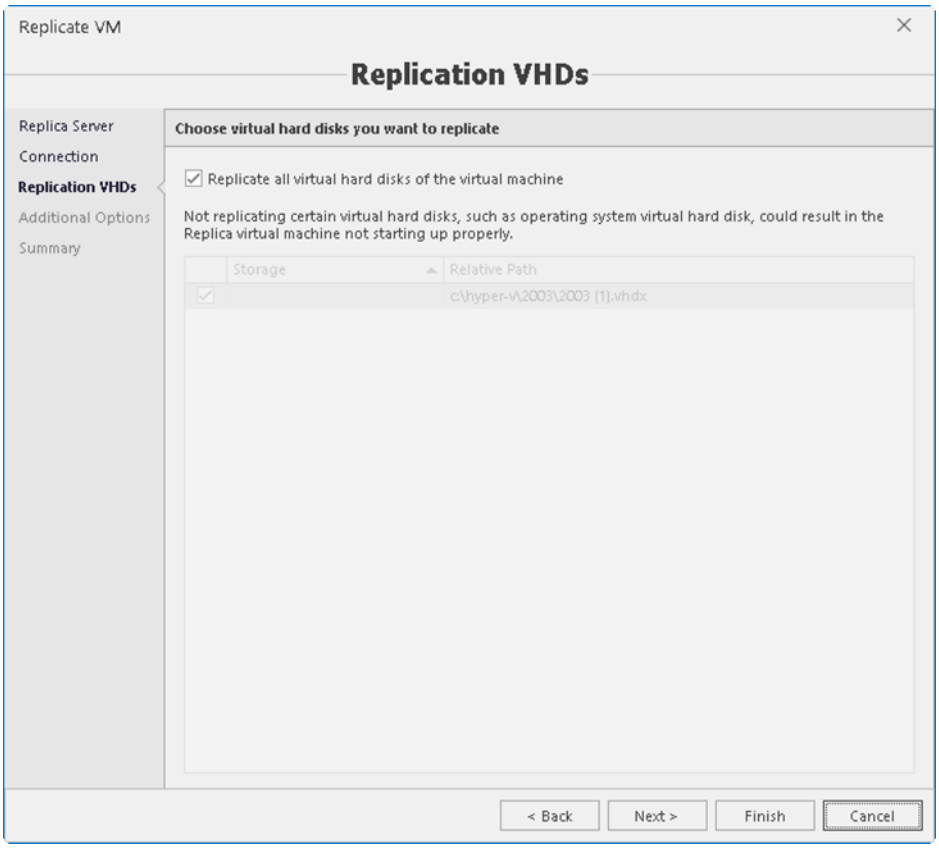
- **Enable this computer as a replica server** – mark this option to set the current Hyper-V host as a replica server.
- Authentication parameters:
  - **Use Kerberos (HTTP)** – this authentication option uses Kerberos authentication protocol via HTTP port 80 (default).
  - **Use certificate-based authentication (HTTPS)** – this authentication method uses pre- installed certificate and works via HTTPS port 443 (default). Press the **Select Certificate** button to choose pre-installed certificate on the current Hyper-V host:
- Authorization and storage parameters:
  - **Allow replication from any authenticated server**. Any Hyper-V host that is set as a replica server in the environment will be allowed to send replica files. Specify the default location by typing or browsing to the folder to store replica files.
  - **Allow replication from the specified servers**. Only specified Hyper-V hosts will be allowed to send replica files. Click **Add** to add the authorized server to the list:
  - **Default storage for replica files on the current Hyper-V host**. Default location on the current Hyper-V server to store replica files.

Starting VM replication

To start VM replication, select the VM and select the **Replicate** command on the main ribbon or from VM's context menu. VM replication wizard will be shown.

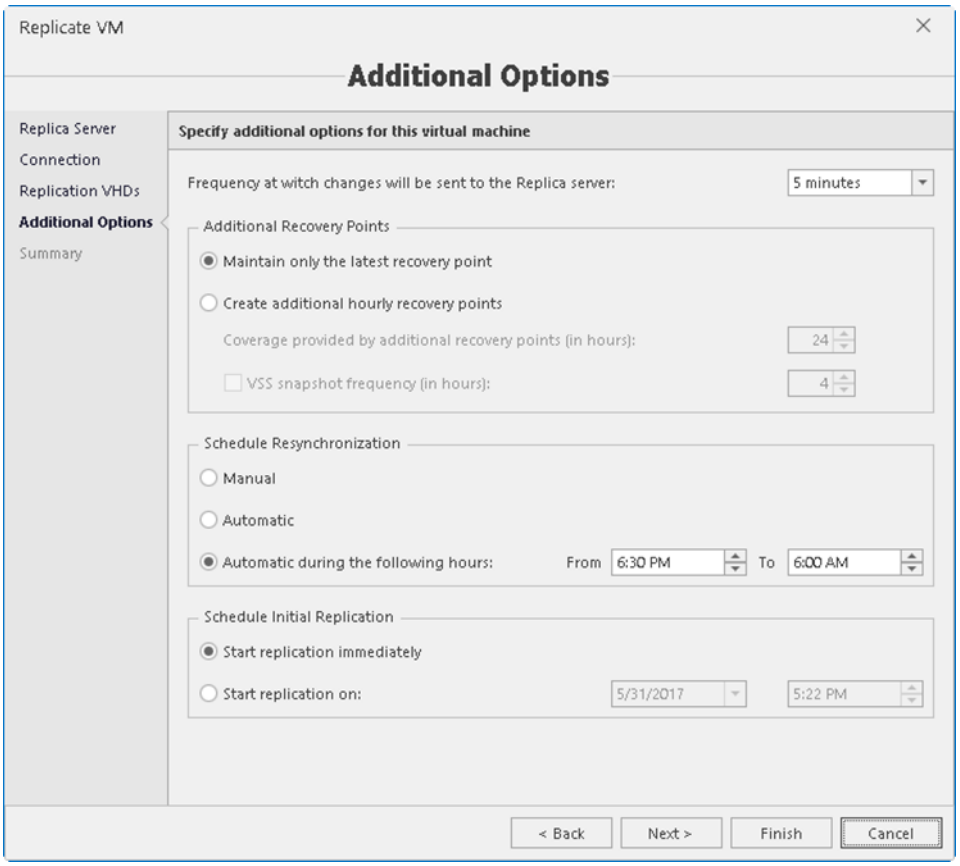


1. Select replica server where you want the VM replicated from the list and press **Next**.

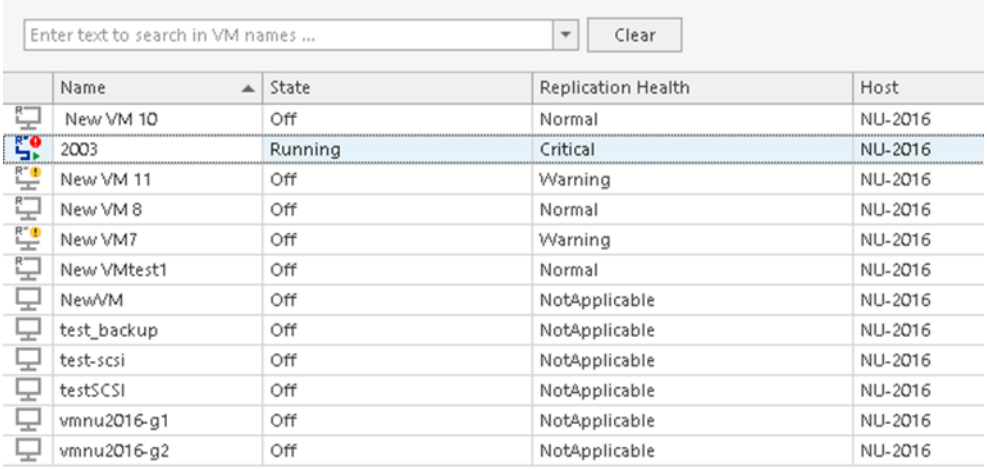


2. Define additional replication options:

- Replication frequency
- Recovery points
- Schedule resynchronization
- Initial replication options

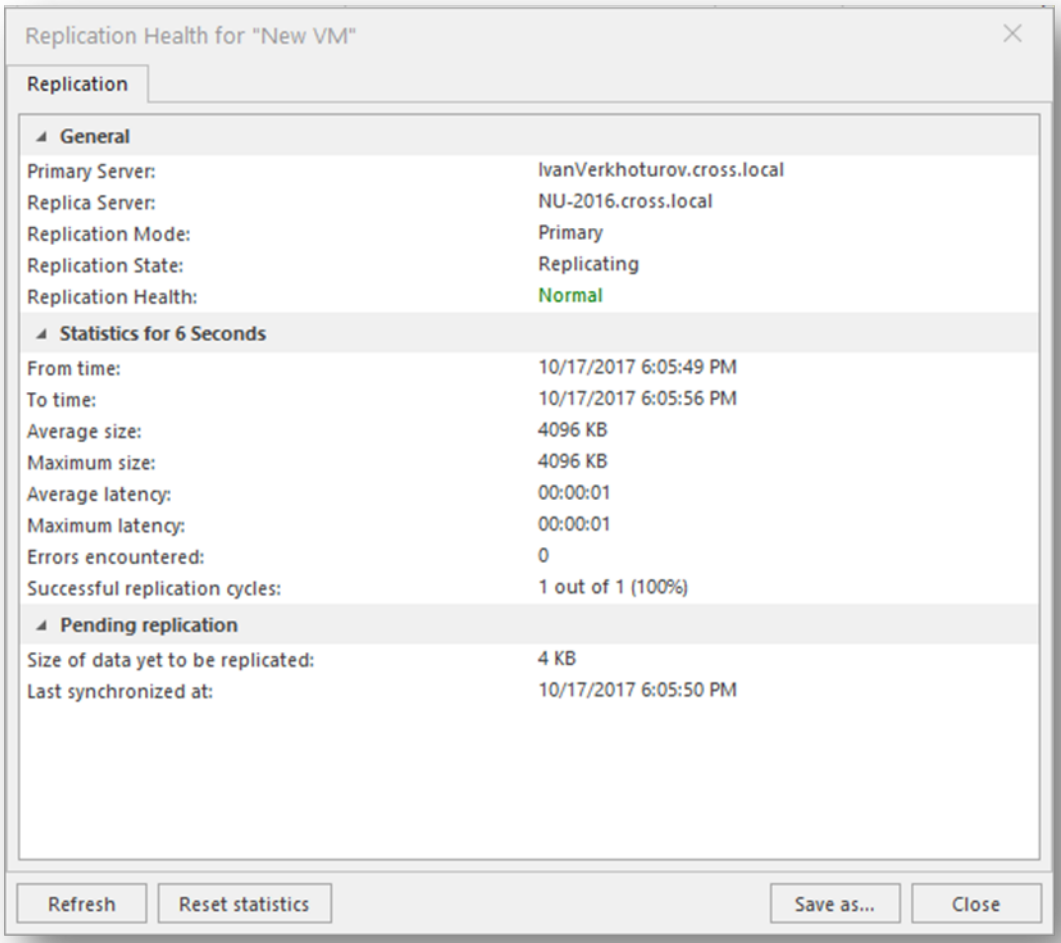


3. Press **Finish** to start VM replication. Once VM is replicated its replication health will be shown in the **Replication health** column in the list of VM and in VM details.



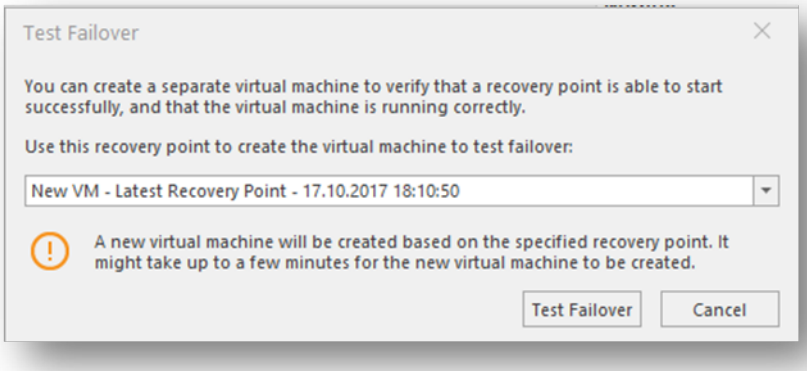
Name	State	Replication Health	Host
New VM 10	Off	Normal	NU-2016
2003	Running	Critical	NU-2016
New VM 11	Off	Warning	NU-2016
New VM 8	Off	Normal	NU-2016
New VM7	Off	Warning	NU-2016
New VMtest1	Off	Normal	NU-2016
NewVM	Off	NotApplicable	NU-2016
test_backup	Off	NotApplicable	NU-2016
test-scsi	Off	NotApplicable	NU-2016
testSCSI	Off	NotApplicable	NU-2016
vmnu2016-g1	Off	NotApplicable	NU-2016
vmnu2016-g2	Off	NotApplicable	NU-2016

Please note - Status window with details about replication health is available:



Note

Acronis Cloud Manager also allows administrators to perform replication failover testing to ensure that everything will work as expected in the event of a disaster.

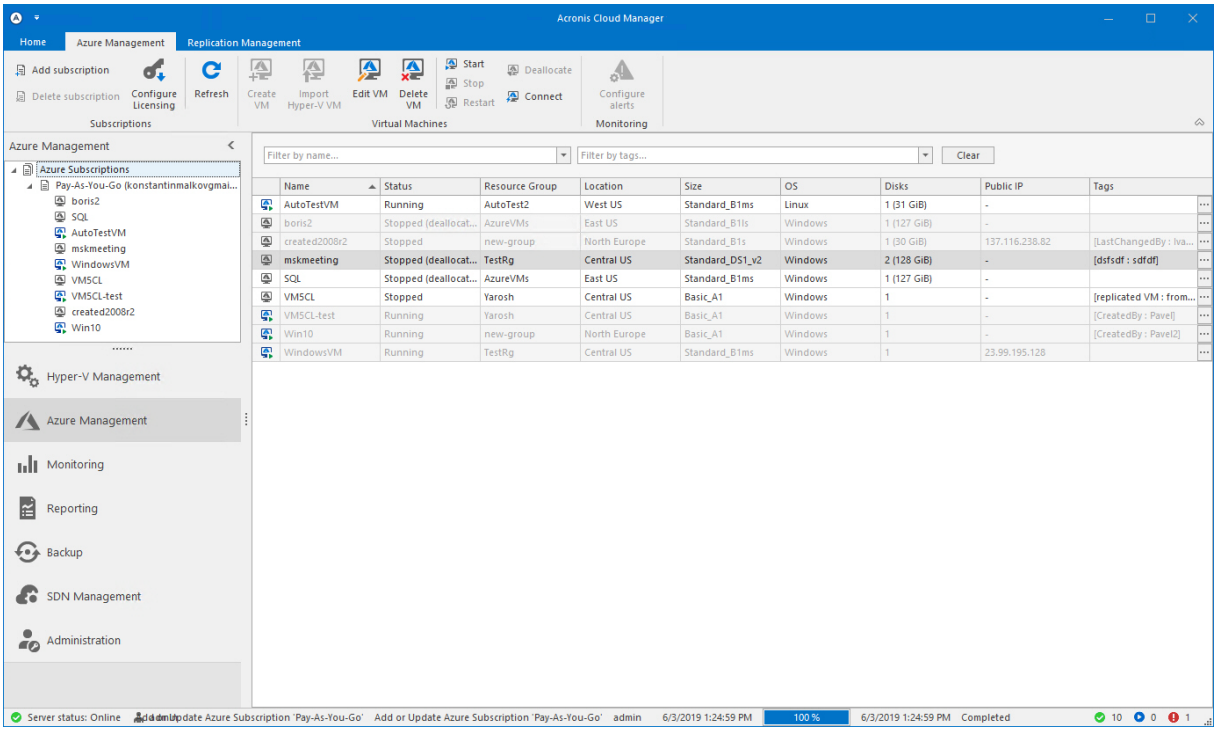


Azure management

Acronis Cloud Manager includes a special plugin to control Microsoft Azure subscriptions from its GUI. It allows performing basic operations with Azure cloud virtual machines and convert Hyper-V VMs into Azure.

General view

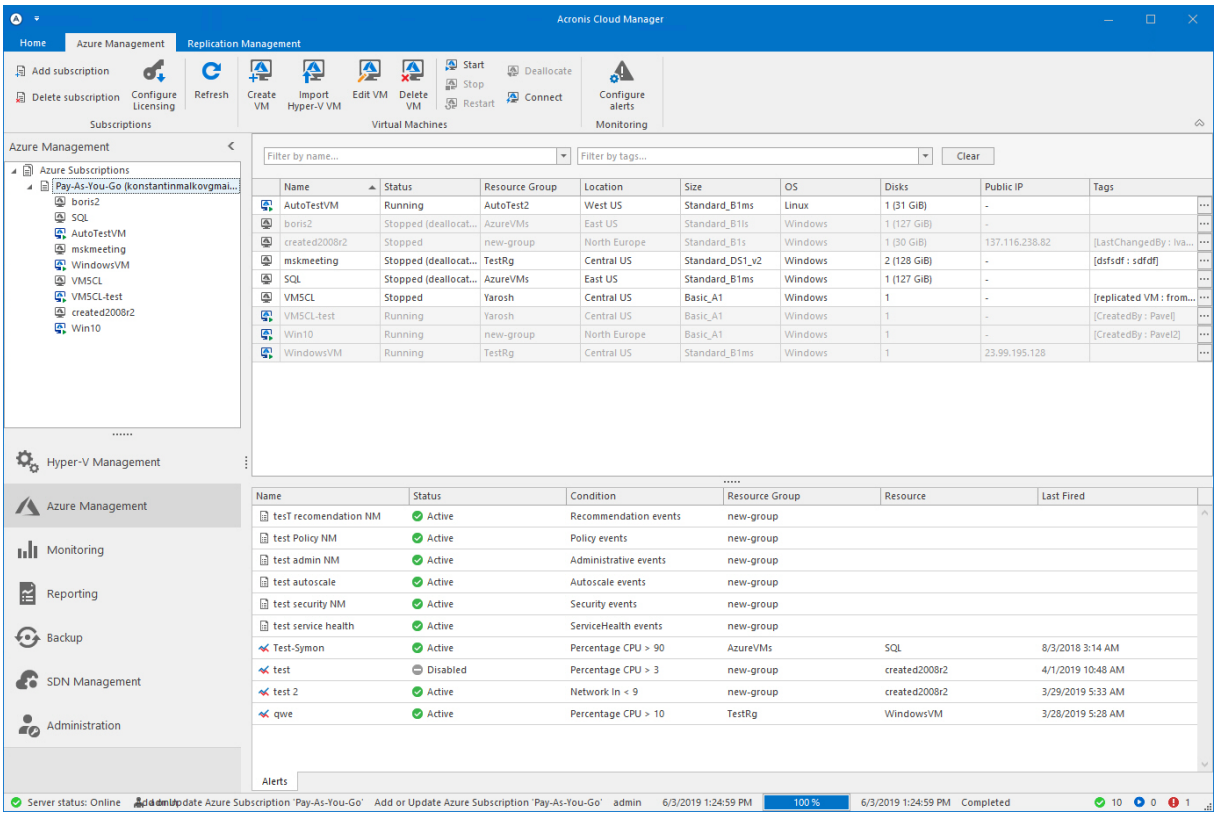
The **Azure management** section view looks similar to **Hyper-V management** – there is an object tree on the left pane and VM list on the right pane. Tools and controls are logically grouped and located on the upper ribbon.



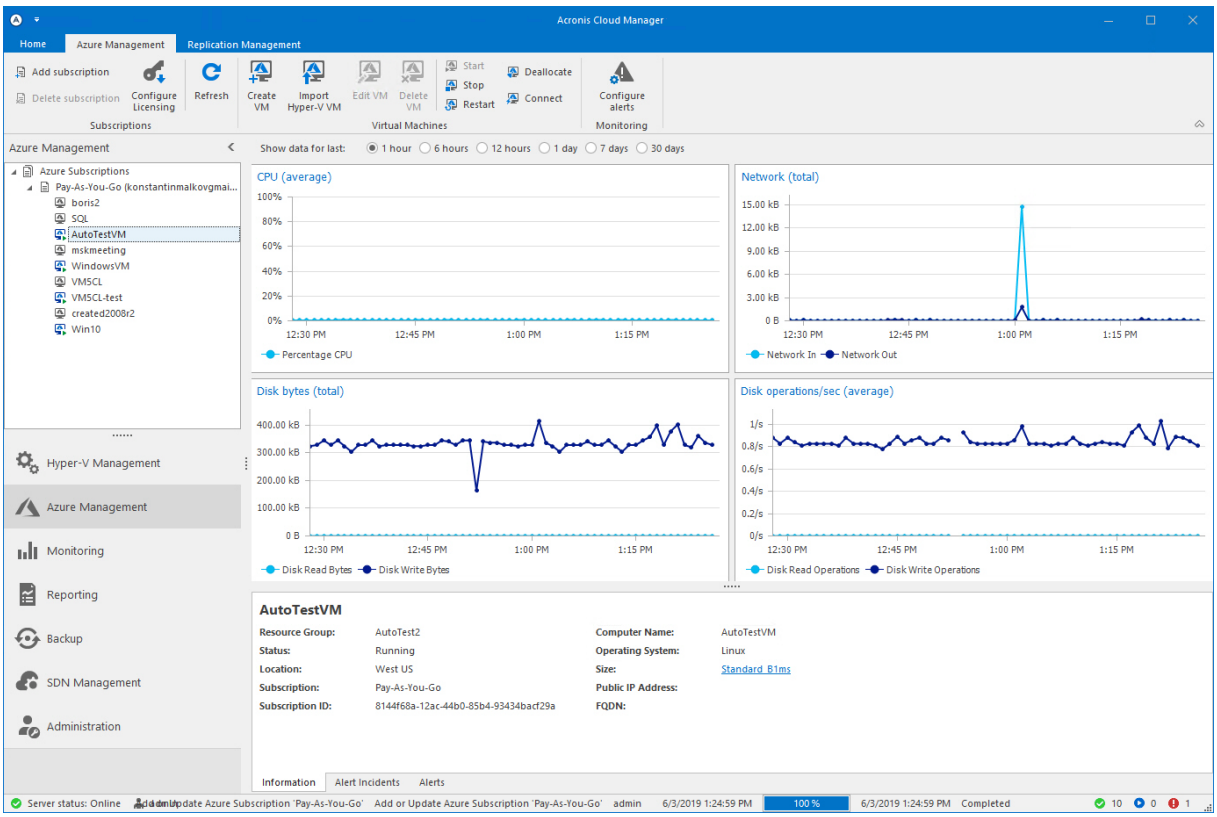
Object tree contains Azure subscriptions instead of hosts as root entries, having VMs under them.

VM view

Selecting a VM from the list on the right pane will enable corresponding controls on the upper ribbon, which are applicable for the current VM state (i.e. **Start** if VM is not currently running, etc.), and the list of the latest alerts for selected VMs in the lower part of the right pane:

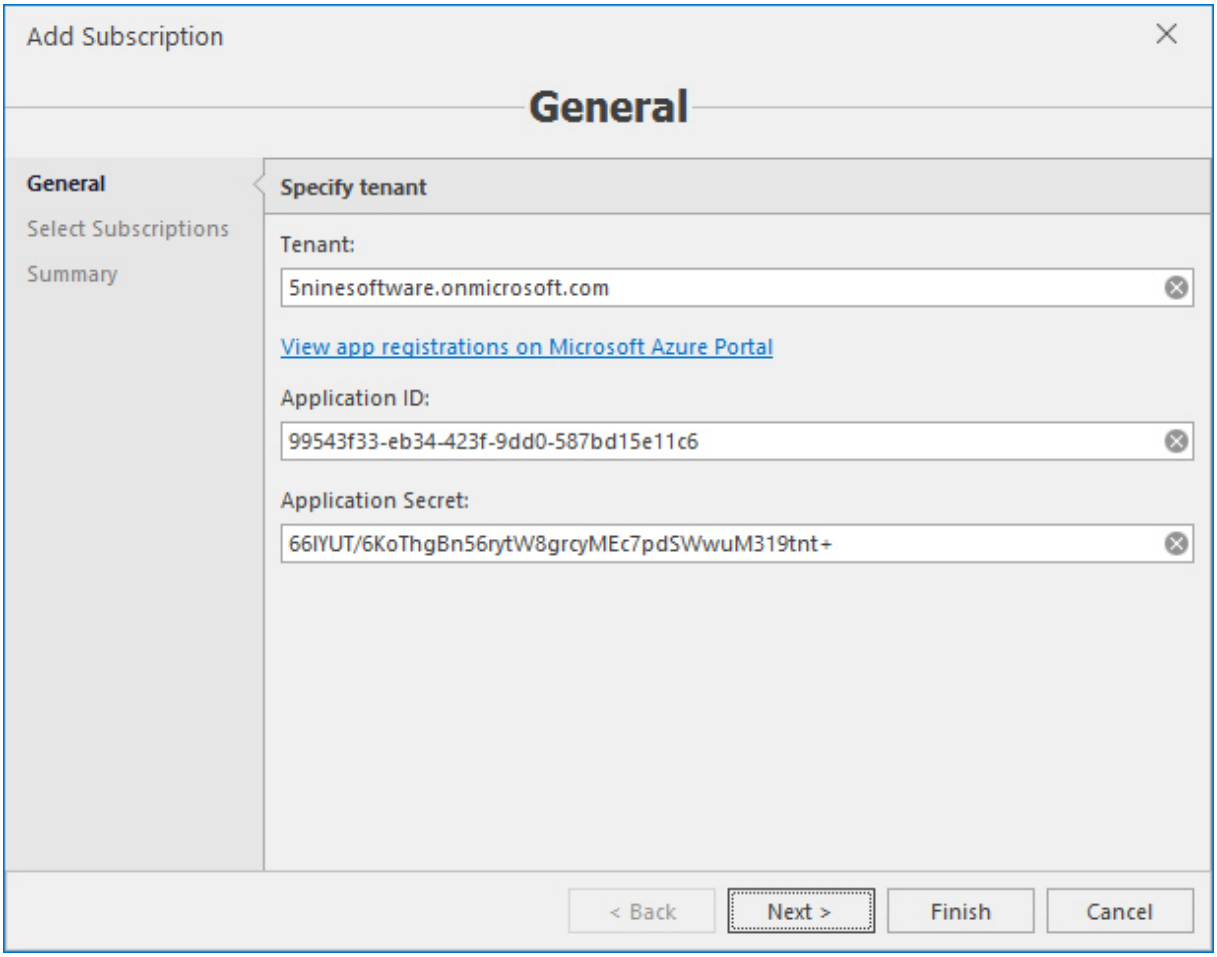


Selecting VM in the object tree on the left pane will display graphs for VM performance counters, VM info and alerts on the right pane:



Adding and removing Microsoft Azure subscription

First thing you have to do when starting your work with Azure management is to add your Microsoft Azure subscription to the object tree. To do this, click the **Add subscription** button on the main ribbon, which will open the **Add subscription** wizard:

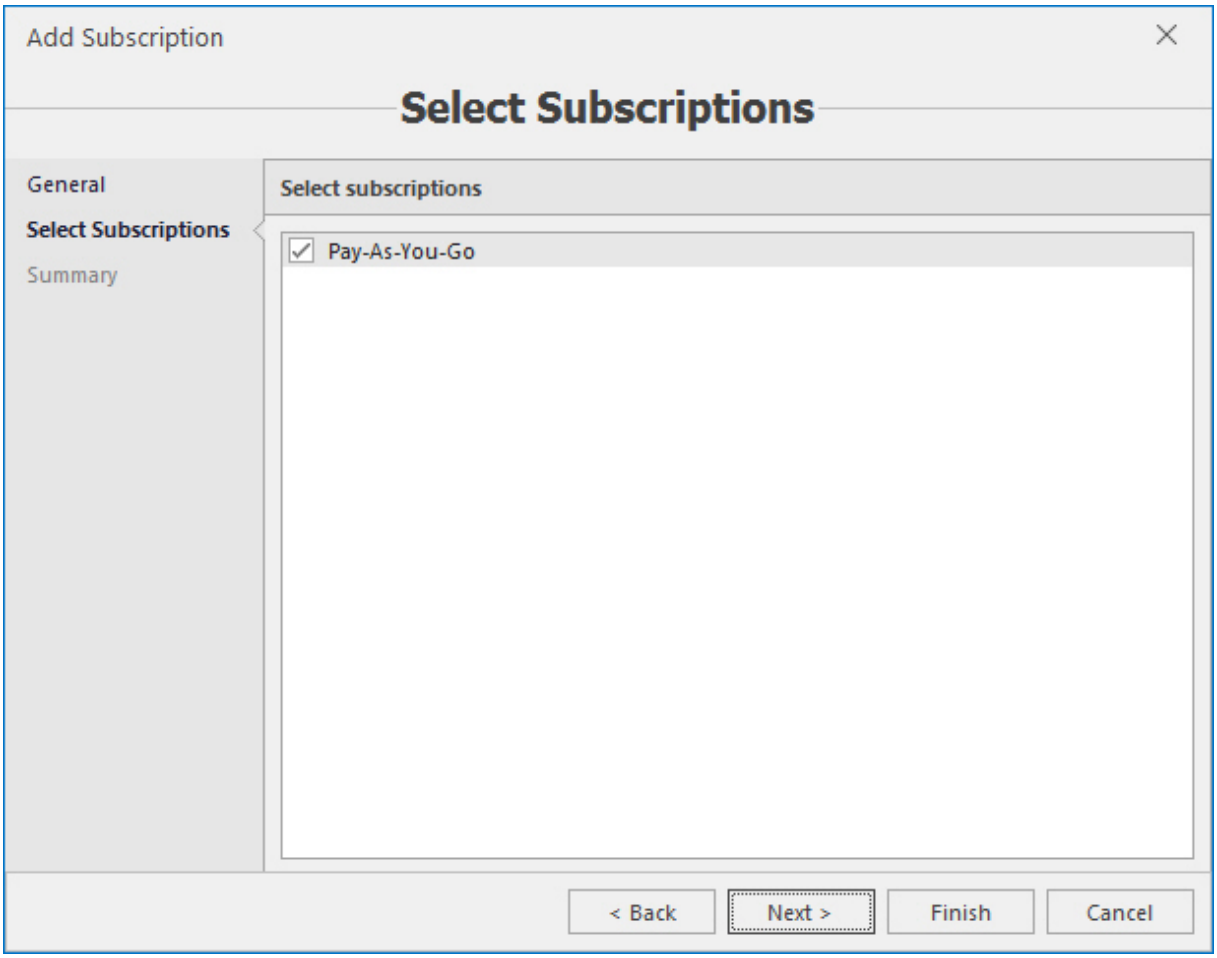


On the first screen, specify your tenant ID, application ID and application secret key. If required, the link View app registrations on Microsoft Azure portal will open your browser and lead you to Microsoft Azure portal to review your subscriptions.

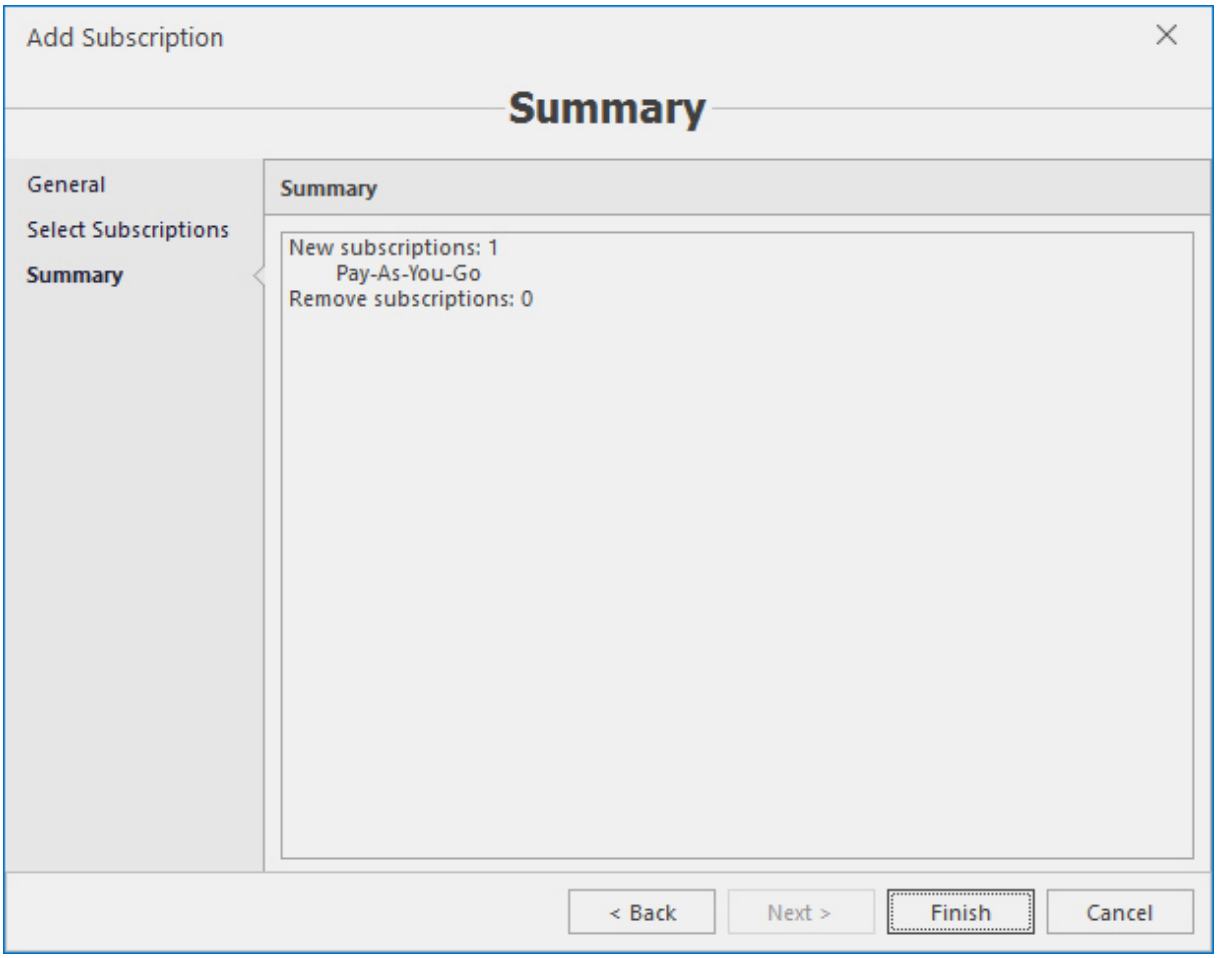
Note
You will have to login to your Microsoft account first to be able to view the Azure subscriptions.

Click **Next**.

On the second screen, select the subscriptions that you want to add to the object tree among available ones in the list and click **Next**:

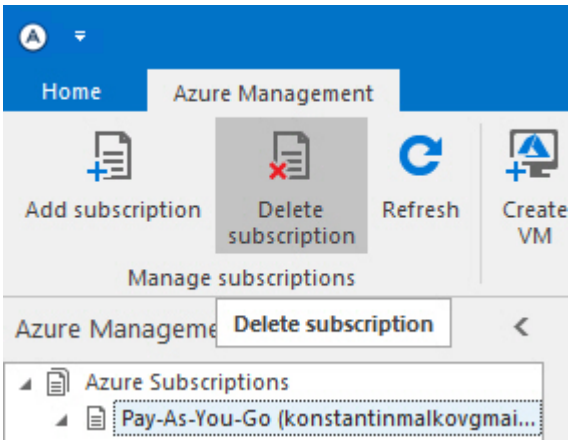


Review the summary on the third screen and click **Finish** to add the selected subscription(s) to the object tree:



The subscription will be added to the tree.

To remove Microsoft Azure subscription from Acronis Cloud Manager's tree, select the required subscription in the tree and click the **Delete subscription** button on the main menu ribbon:



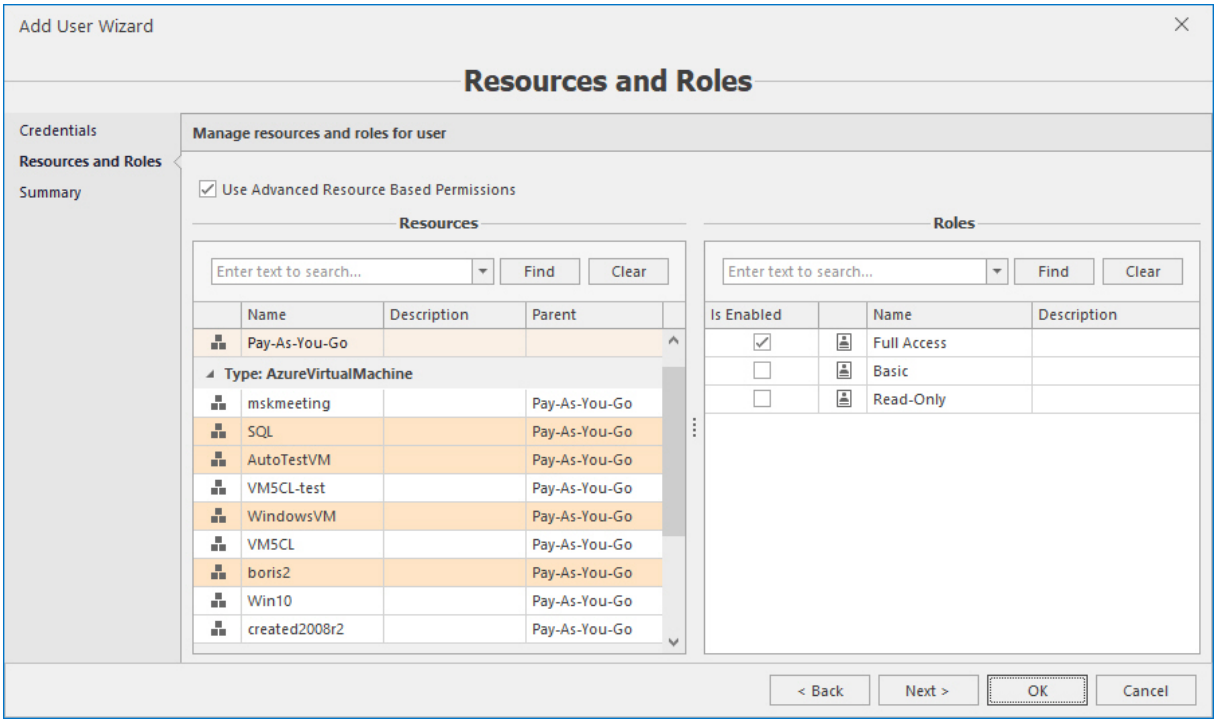
Role-based access control

Azure subscriptions are added separately on global and tenant levels. Global administrator can delegate permissions on Azure subscriptions (full access, separate Azure VMs and/or operations) added on global

level to global users without administrative privileges and to tenant administrators. Tenant administrator can delegate permissions to tenant users without administrative privileges.

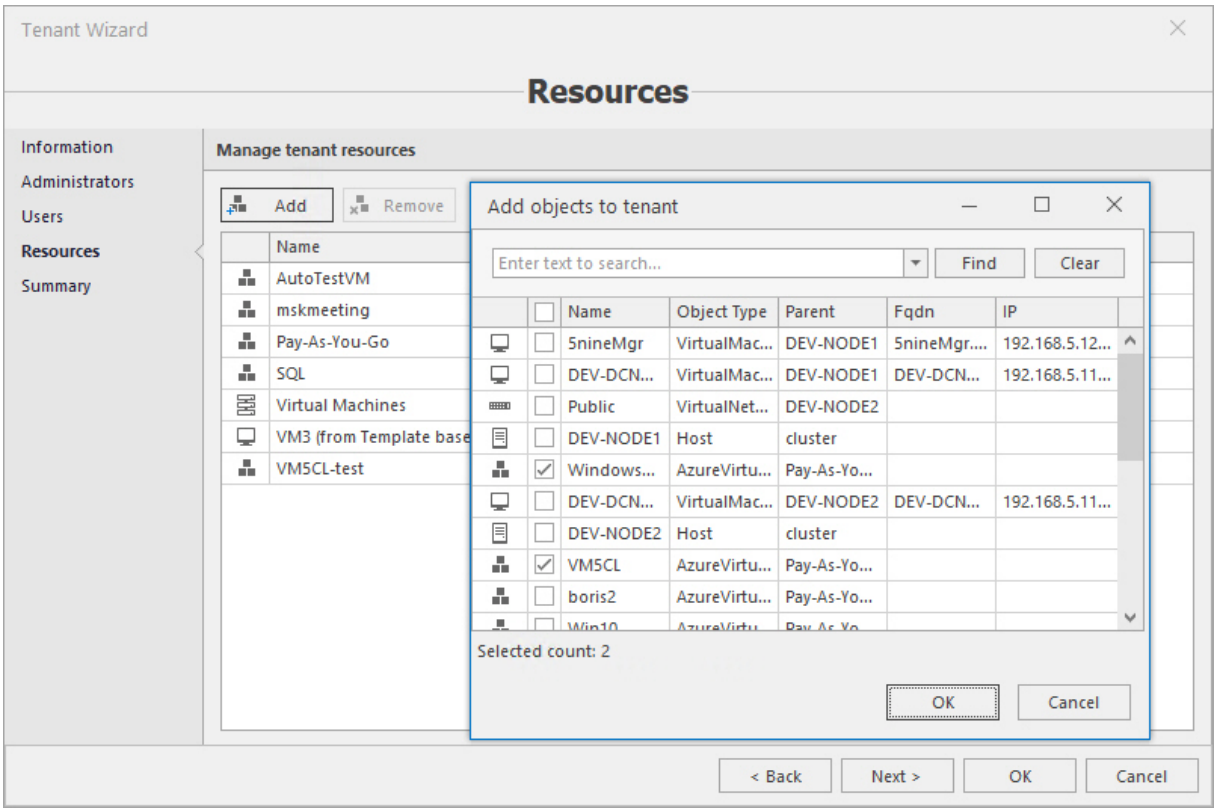
Permissions for Azure subscriptions are delegated in the standard way as it's done for any other type of resources (please, refer to the "Managing users, tenants and roles" (p. 50) section above for detailed information).

Adding Azure resources to global users:



Select subscriptions and VMs you need to delegate permissions on and click **OK** to add those resources to the user. Operations available for each resource are configured in roles settings (please, refer to the "Managing users, tenants and roles" (p. 50) section above for detailed information). Tenant administrator is able to do the same on tenant level.

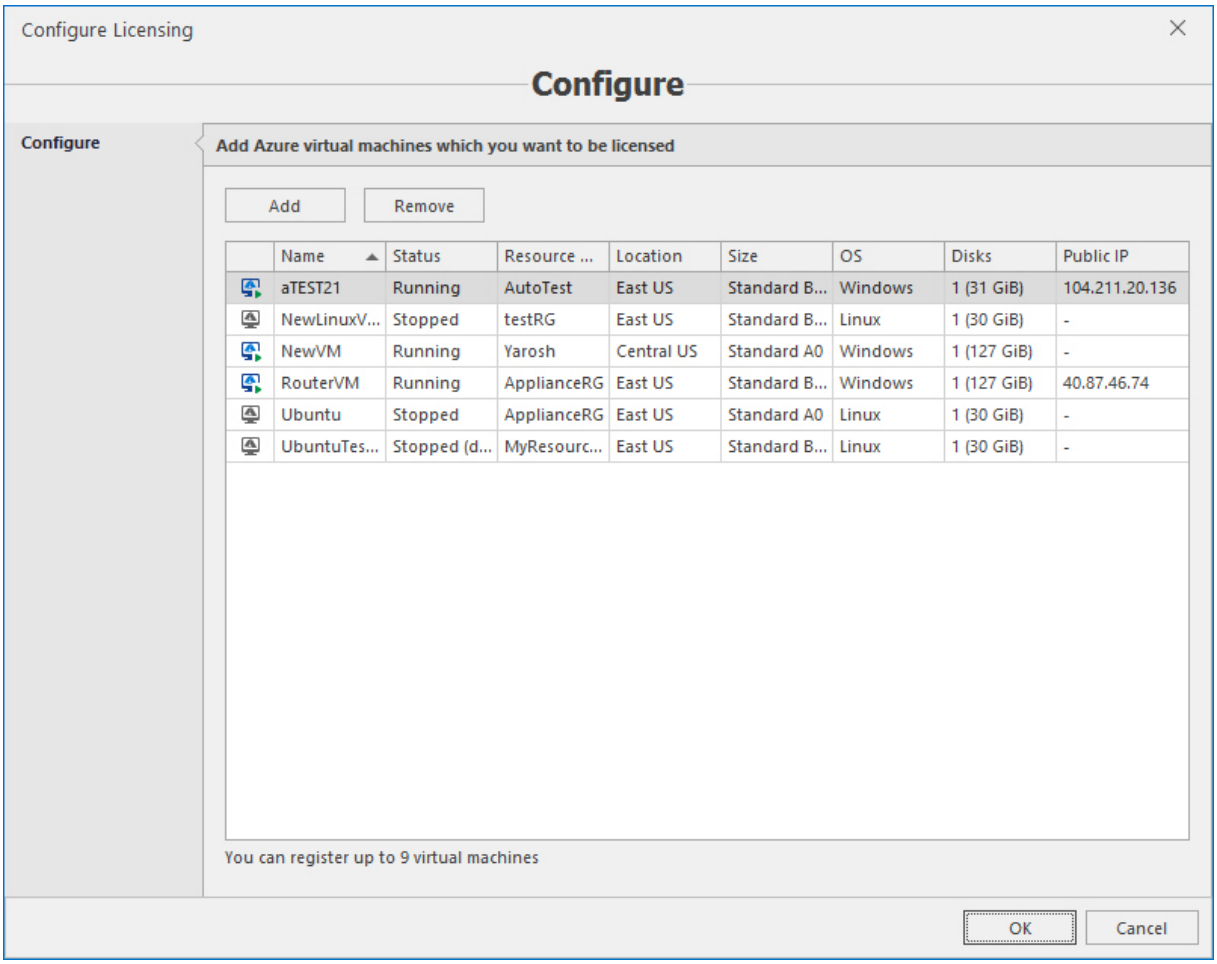
Adding Azure resources to tenant:



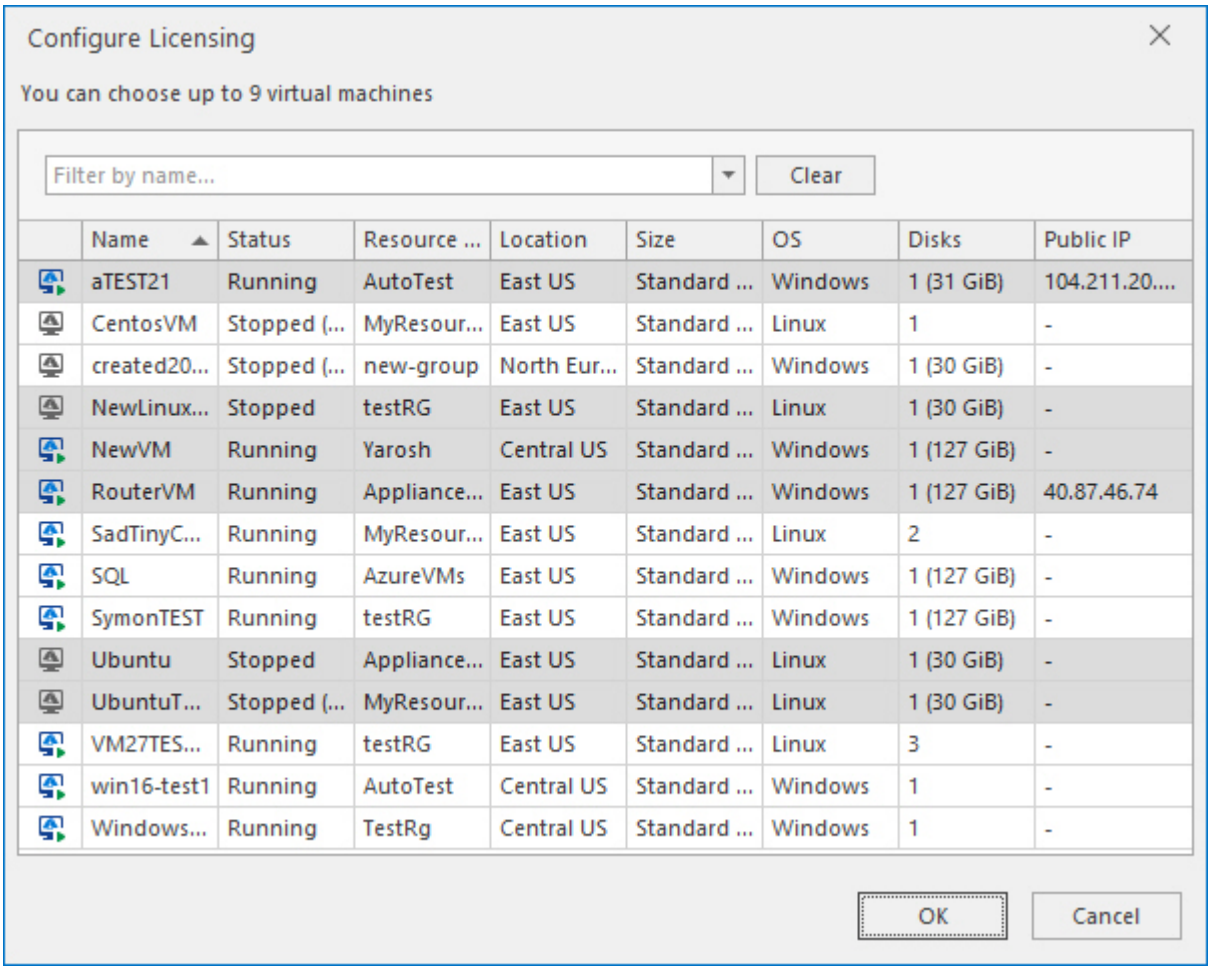
Configuring Azure licensing

Azure management part is licensed per VM. Initially, a free license is installed by default, which includes quota for a maximum number of 5 virtual machines from the cloud. Azure license is installed and works separately on a global level and for each tenant. Default 5 VM licenses are only available to global users and additional Azure VM licenses can be purchased which requires a separate license file.

Without the valid Azure license, Acronis Cloud Manager will still display Azure VMs, but all of them will be inactive and inoperable – no actions against them will be possible. After installing the Azure license, you will need to configure it – select VMs from your added Azure subscriptions that you need to be active and available for management. To configure the license, click the **Configure Licensing** button on the main ribbon:



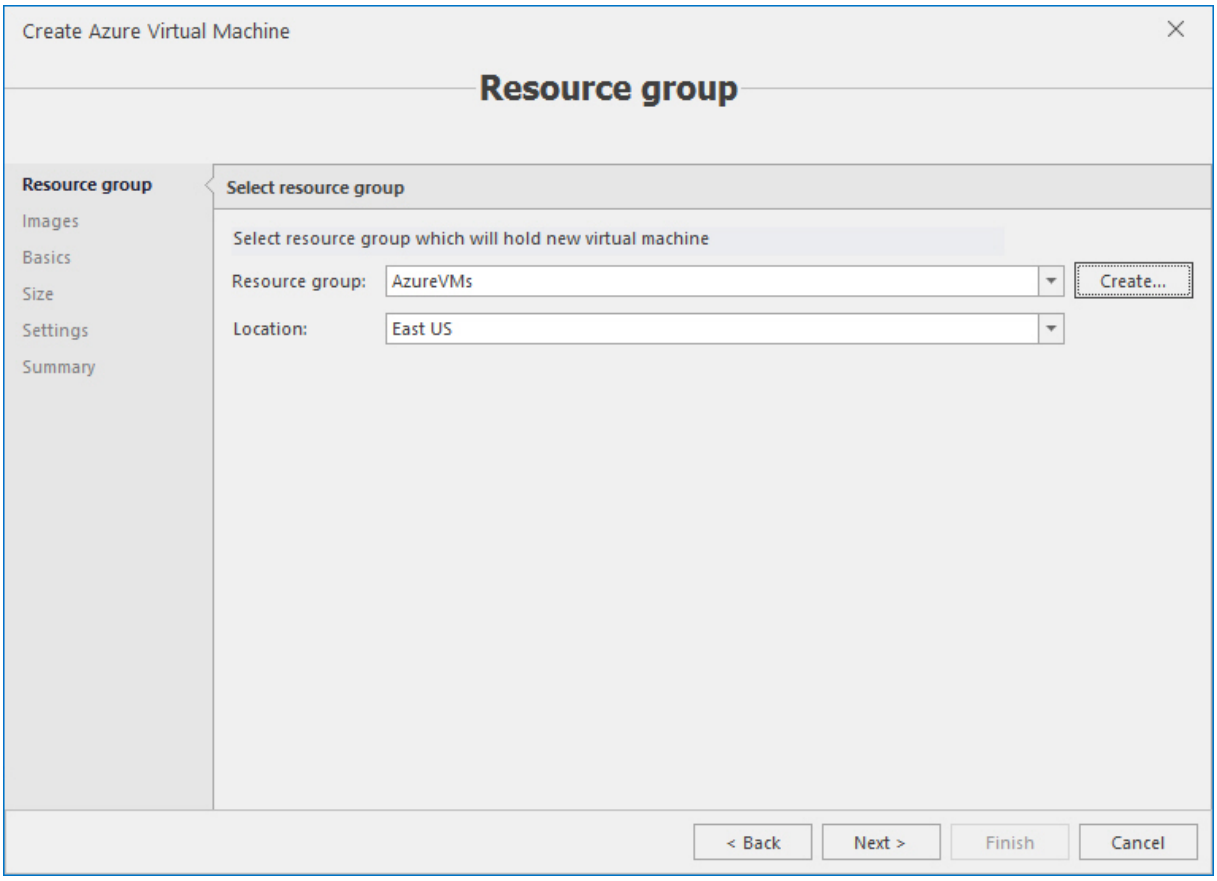
The wizard displays virtual machines that have been already selected from the subscription(s) limited by max number of the license quota. It is written in the lower part of the wizard how many VMs you may currently register. To add new VMs from the subscription click the **Add** button:



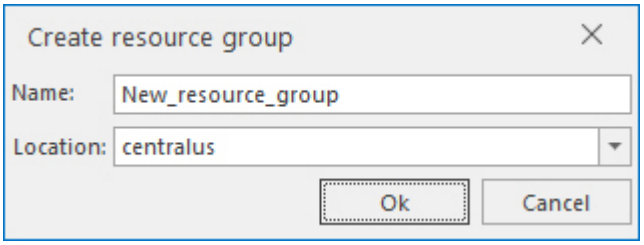
Choose VMs, using your mouse, **Shift+Ctrl** keys as needed, then click **OK** in the dialog window and on the main window of the wizard. Selected VMs will become active and available for management.

Creating/deleting VM

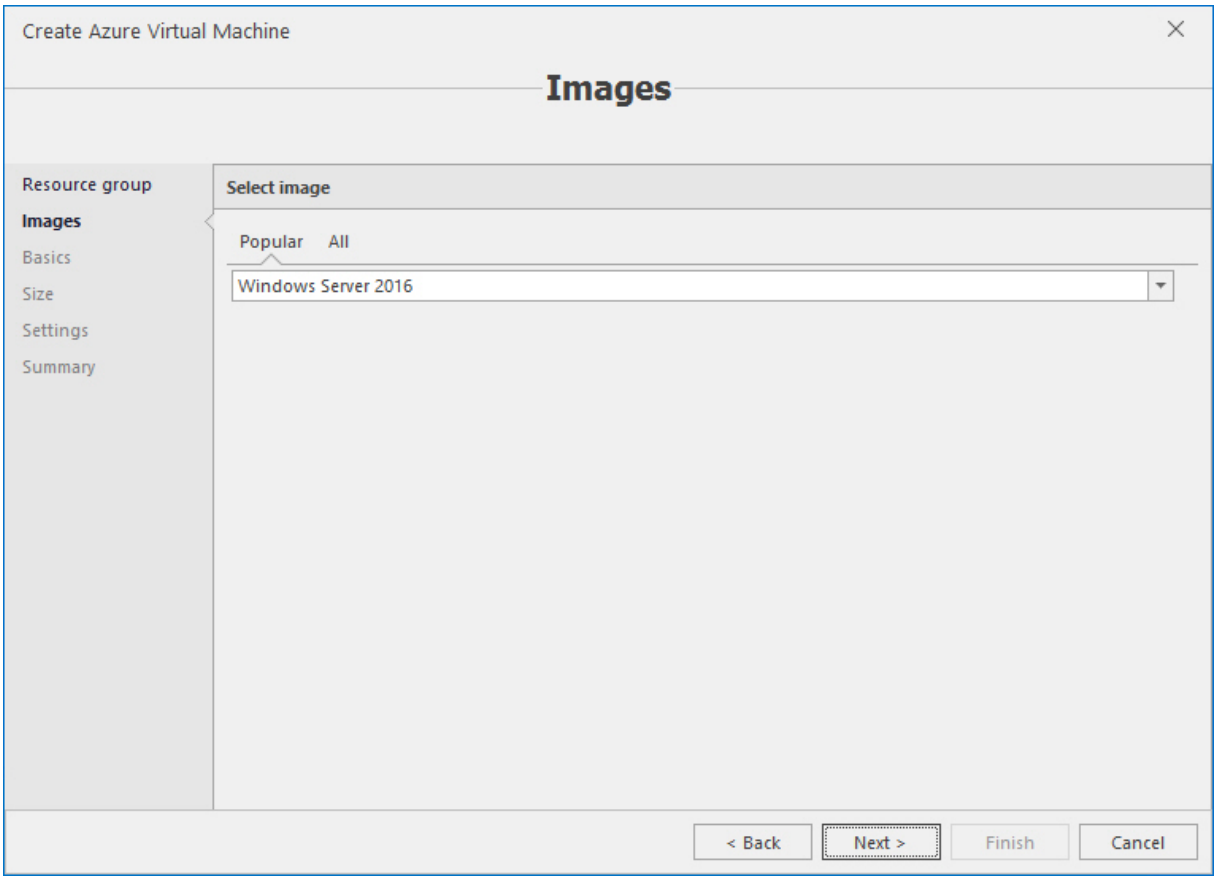
To create a new Azure VM, click the **Create VM** button on the main ribbon. The **Create Azure virtual machine** wizard will open:



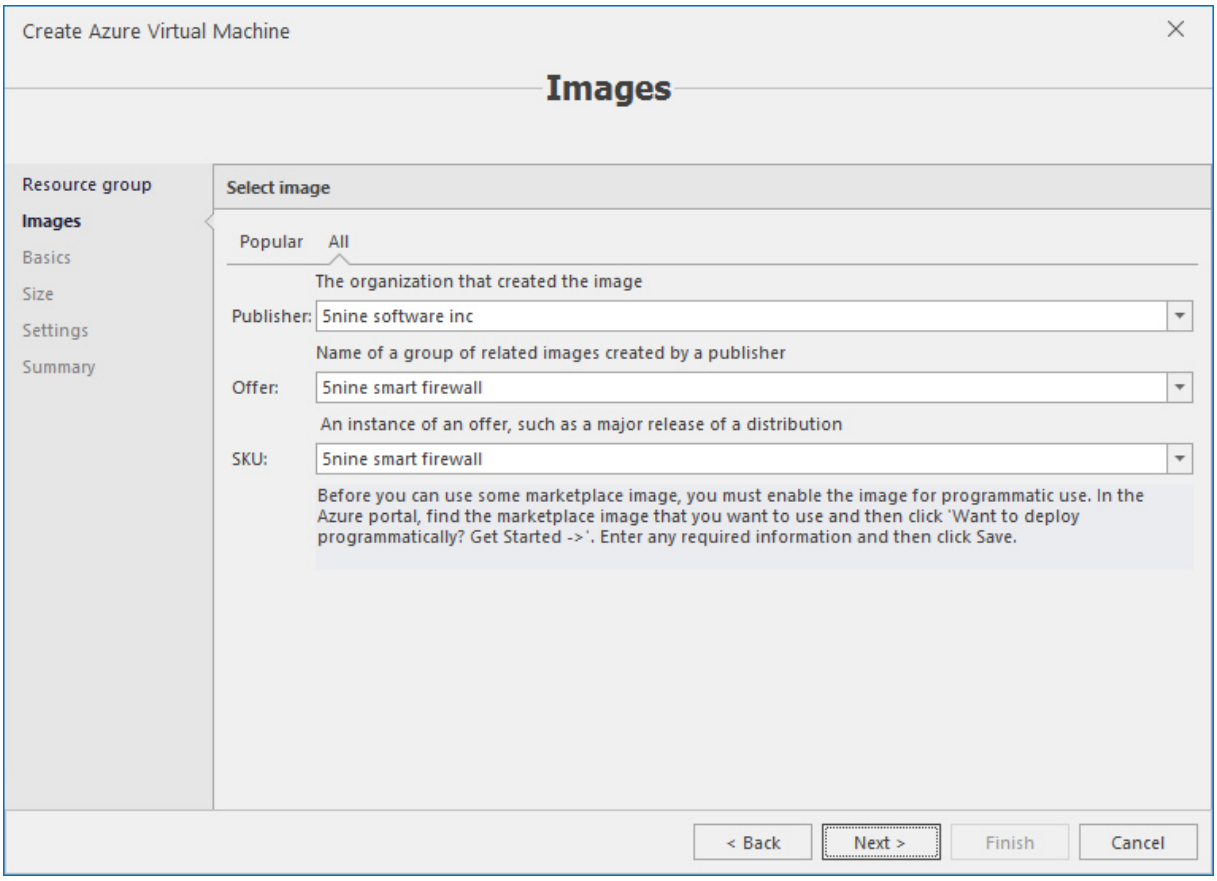
Select resource group and location, create the new resource group if necessary – click the **Create** button to the right from the **Resource group** field.



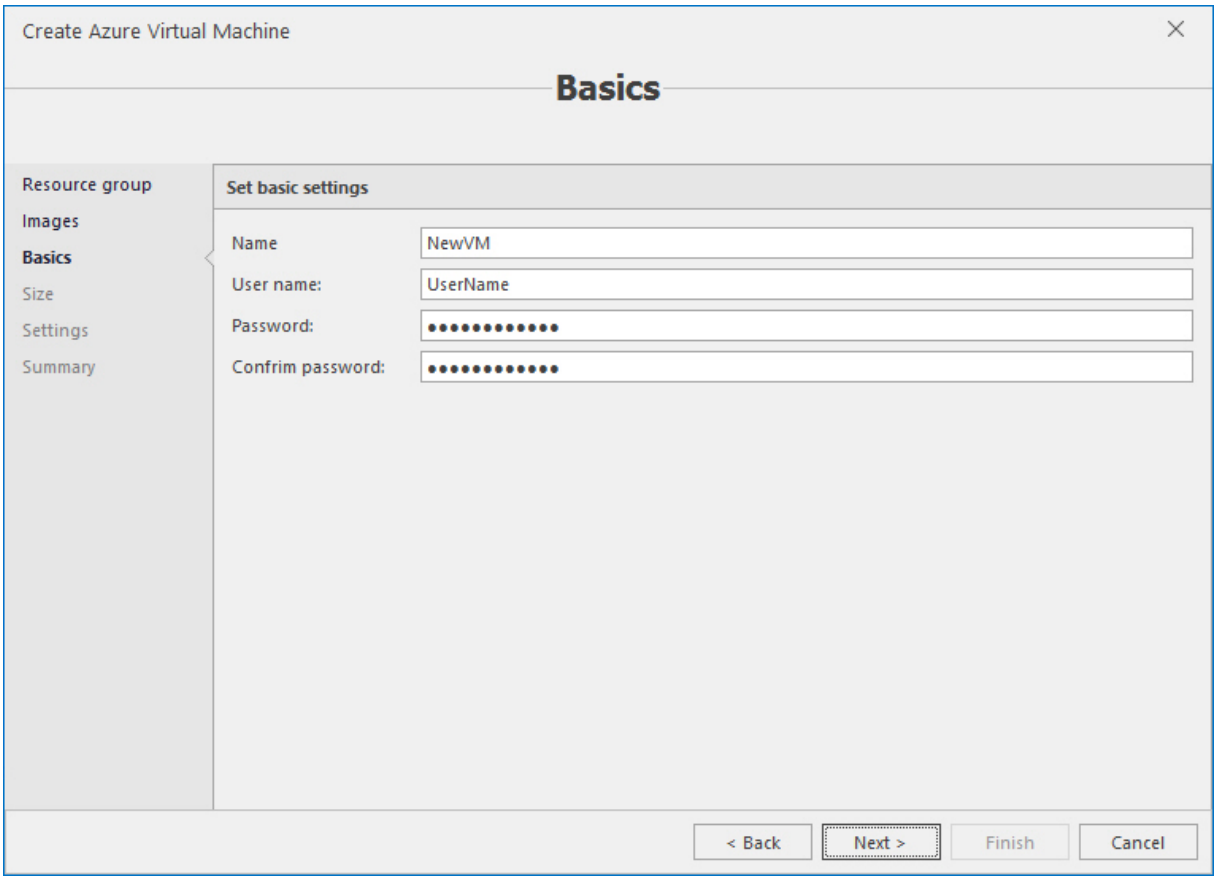
Type in the name and select the location.Then click **Next**.



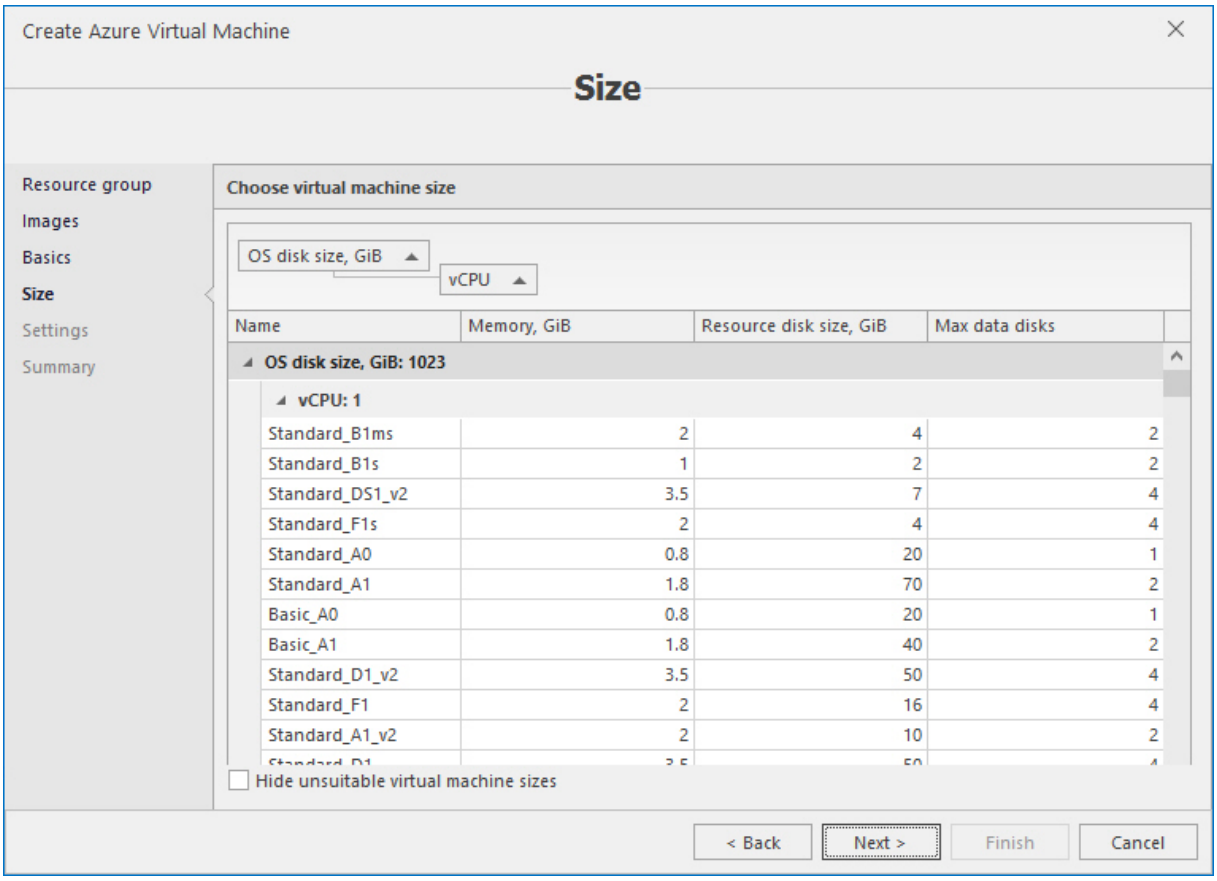
Either select one of popular images, or specify publisher, name of group of related images and SKU. Click **Next**.



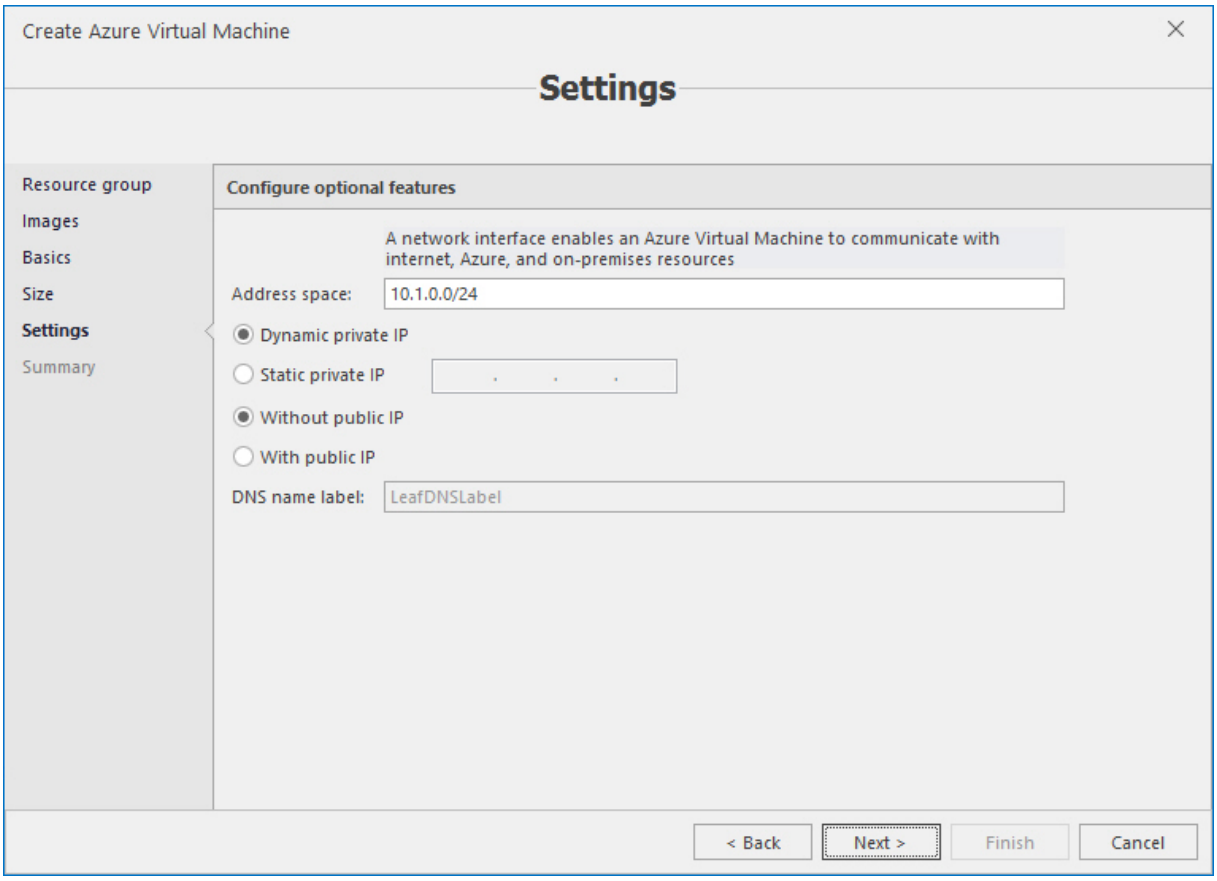
Enter VM name and credentials – user name and password. Click **Next**.



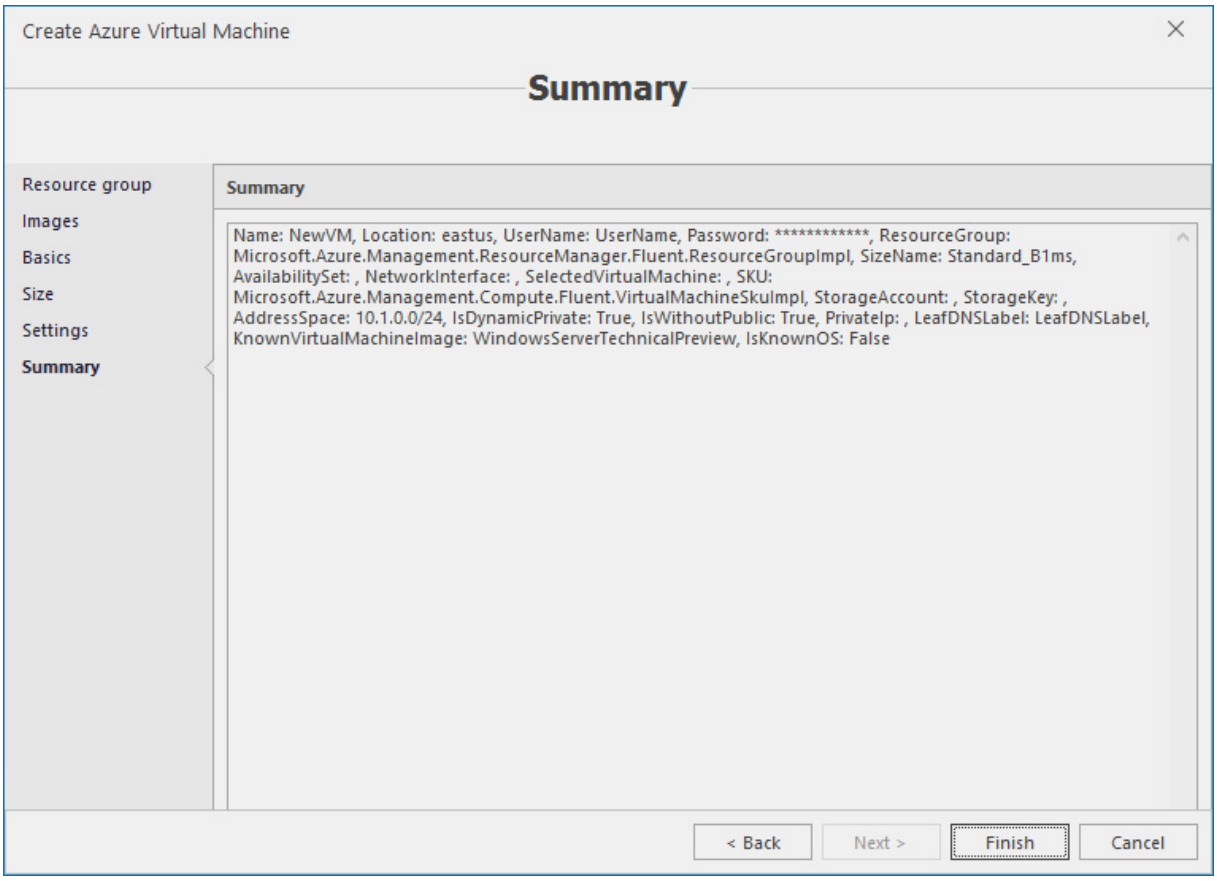
Select available VM size. Click **Next**.



Set IP addresses. Click **Next**.



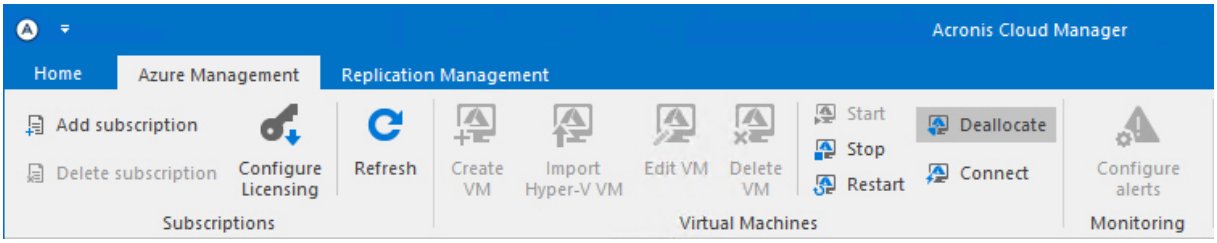
Review the summary and click **Finish**.



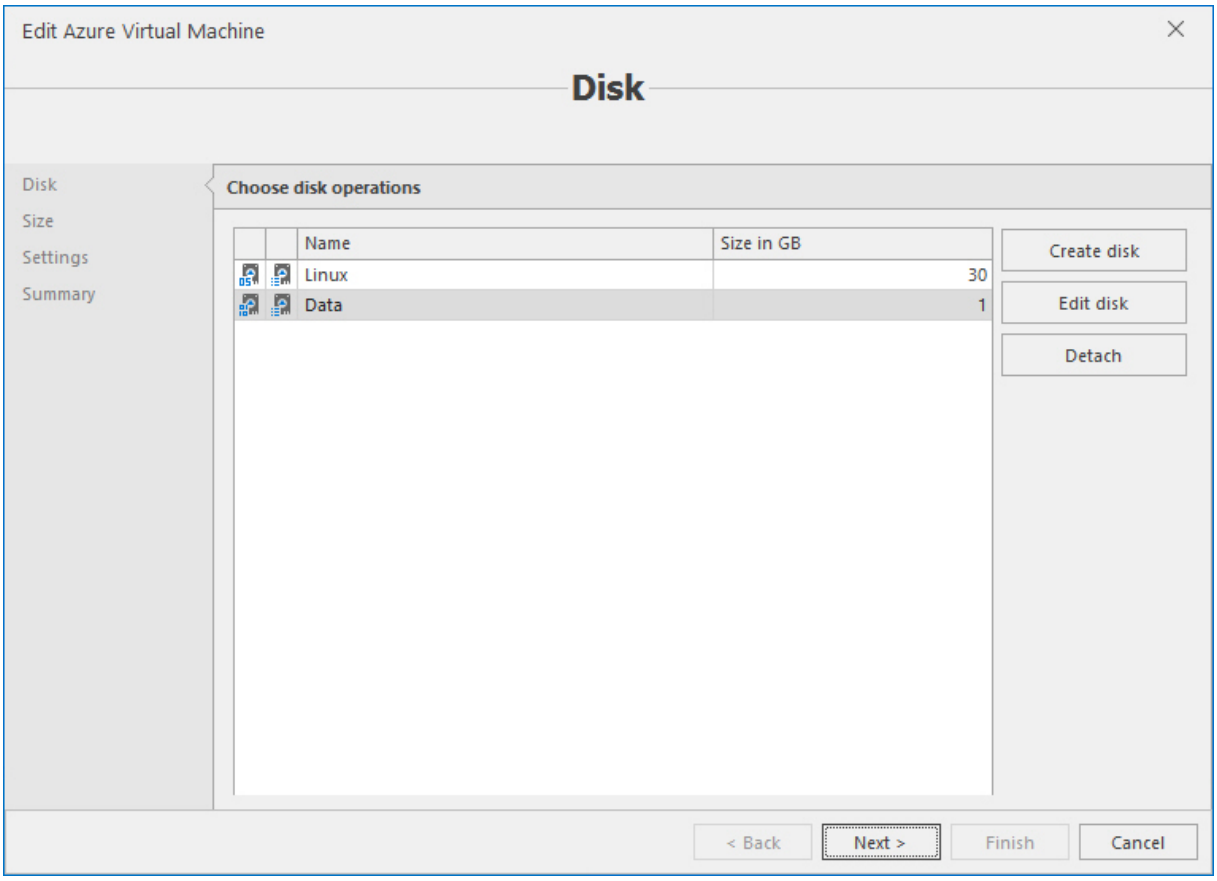
To delete Azure VM, select it, make sure it is in stopped state, and then click the **Delete VM** button on the main ribbon.

Editing VM

To edit Azure VM, you need to deallocate its resources first. Select virtual machine and click the **Deallocate** button on the main ribbon:

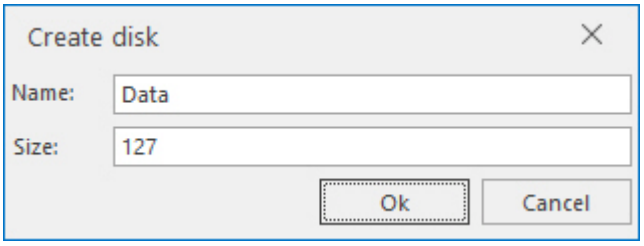


When the process is finished (you may control this using Jobs dialog window), click the **Edit VM** button on the main ribbon. The **Edit Azure virtual machine** wizard will be opened:



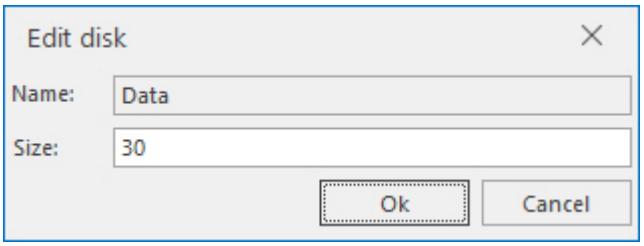
The following actions with virtual disk are available on the first screen: create new disk, edit disk and detach disk.

1. To create virtual disk, click the **Create disk** button.



Enter the name for a new disk and its size, and then click **OK**.

2. To edit the virtual disk, select it and click the **Edit disk** button.

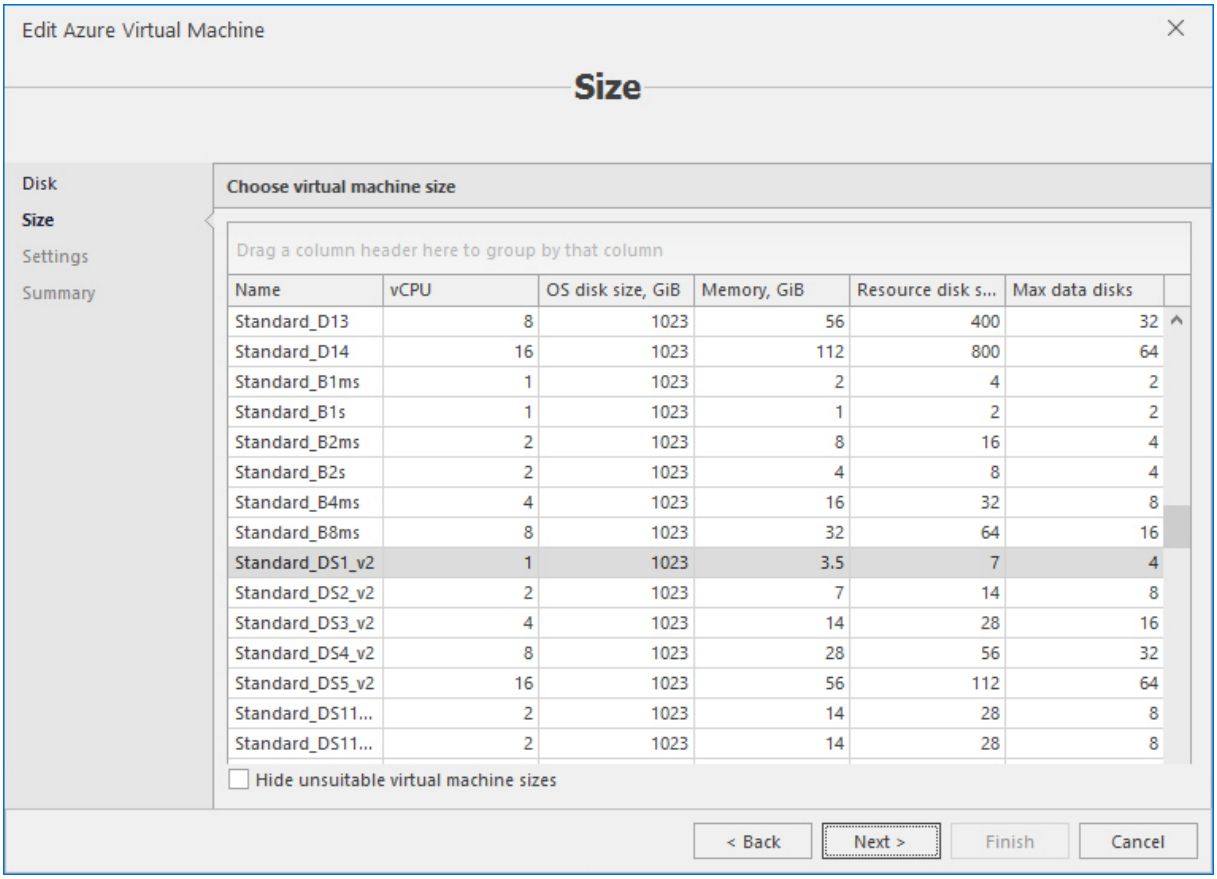


Edit the necessary parameters for the virtual disk (name and/or size), and then click **OK**.

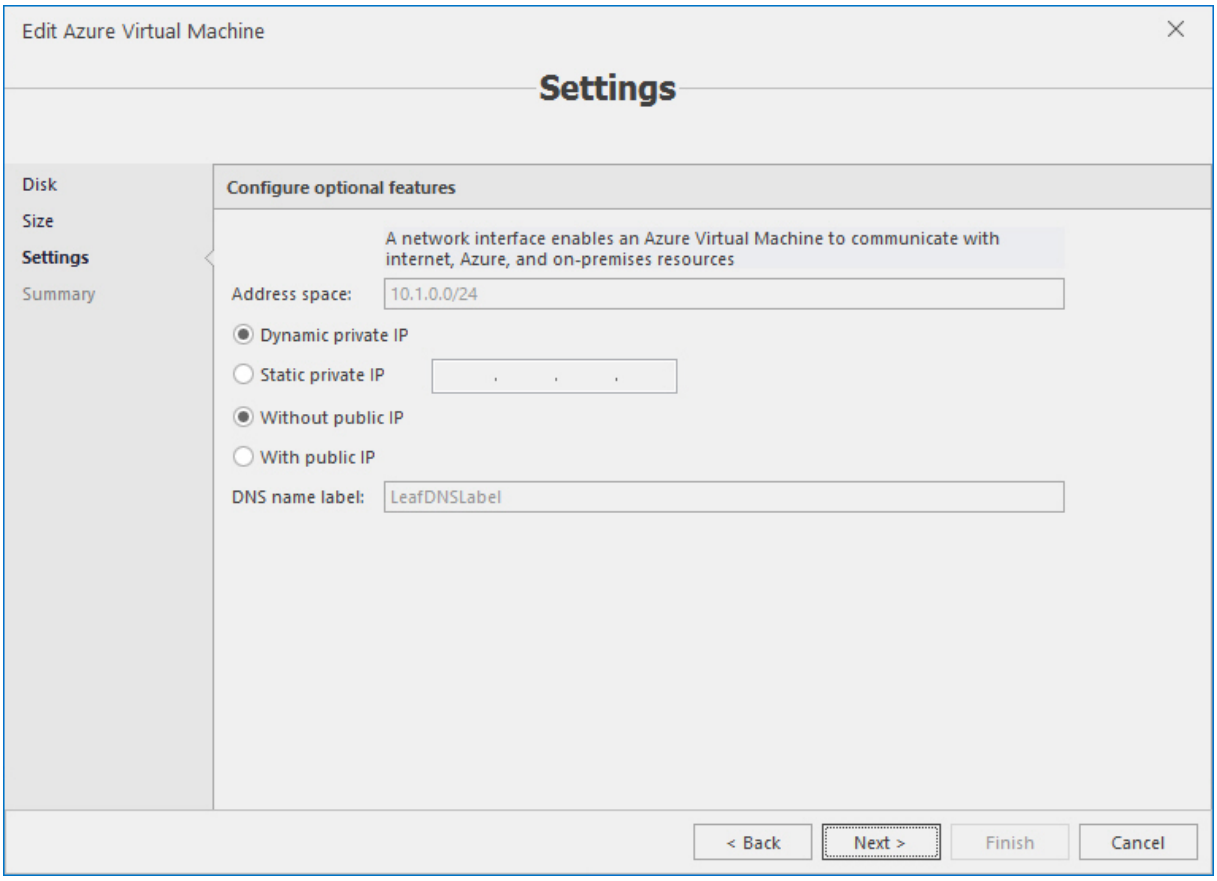
3. To detach virtual disk, select it and click the **Detach** button.

Click **Next**.

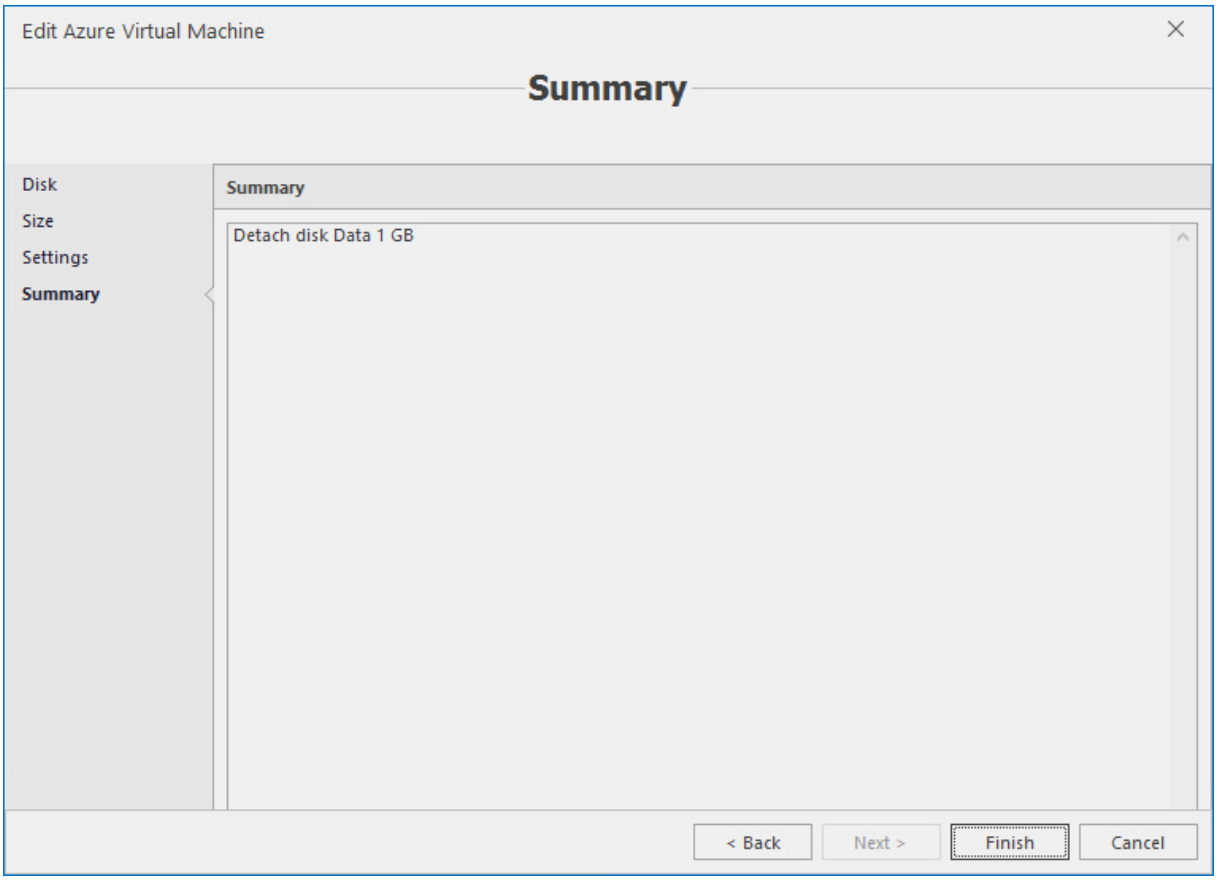
On the next screen, select the new size for Azure VM if necessary. Click **Next**.



On the next screen, edit Azure VM IP settings, if necessary. Click **Next**.

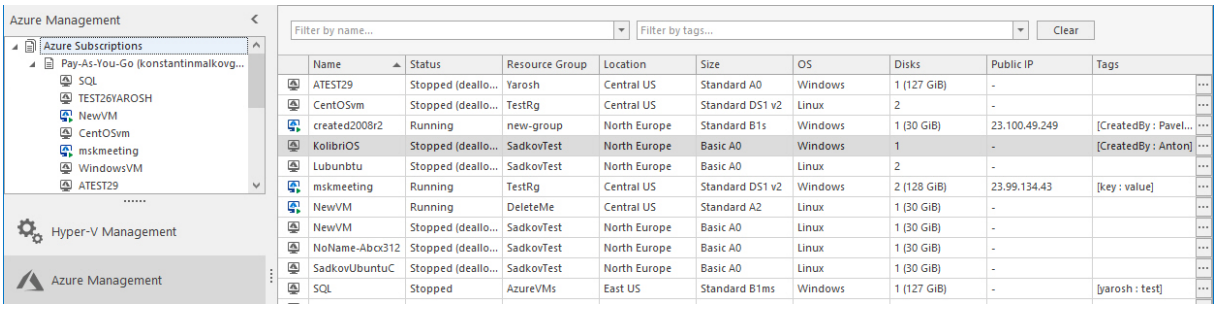


Review the summary and click **Finish**.

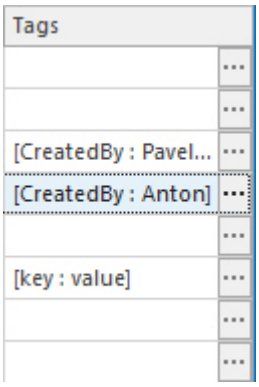


Editing tags

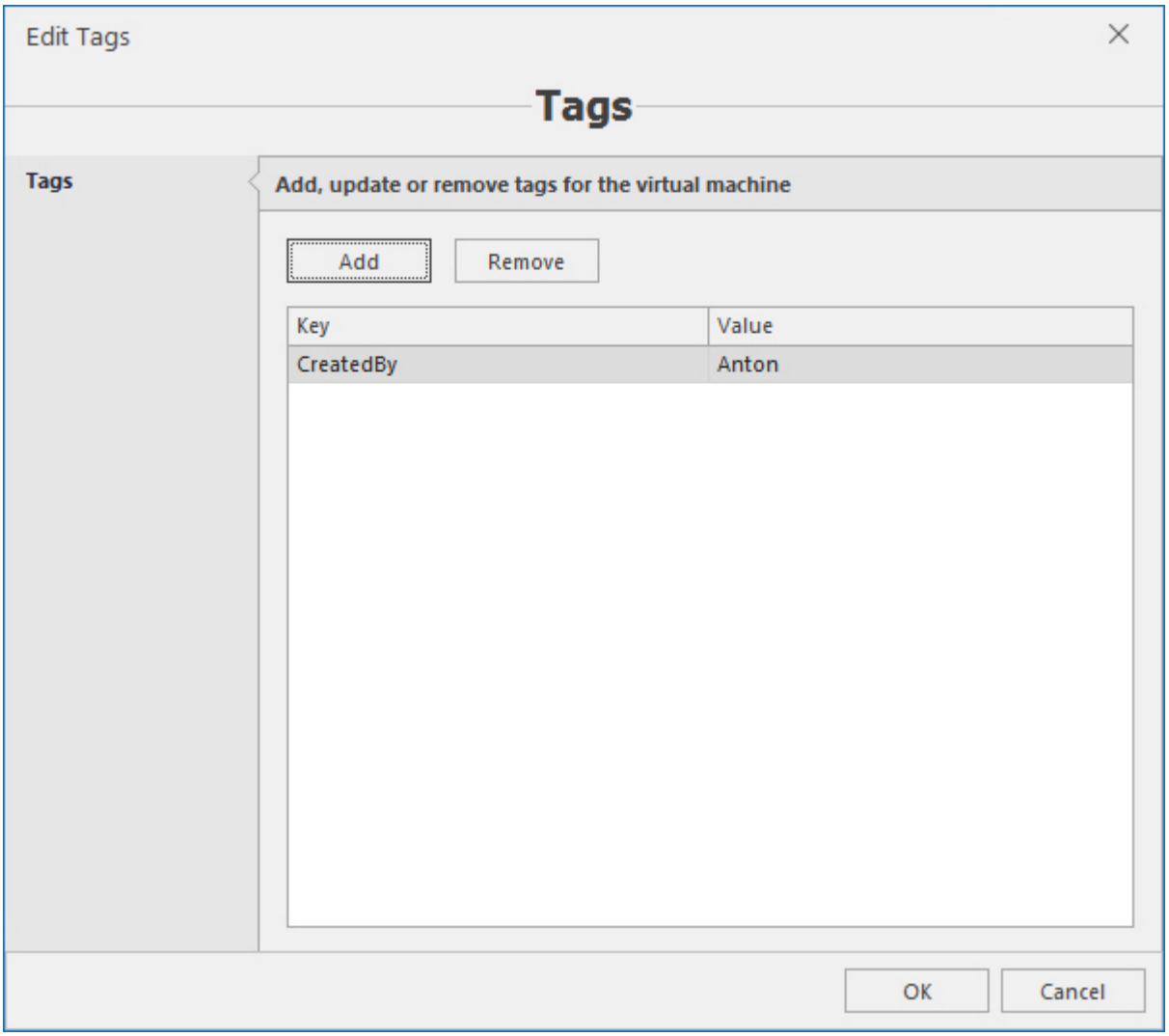
Tags, which are used in Microsoft Azure to categorize and logically order resources, can be edited using Acronis Cloud Manager GUI. To view and edit tags, select either the root branch of the object tree or the exact subscription to view Azure VM list:



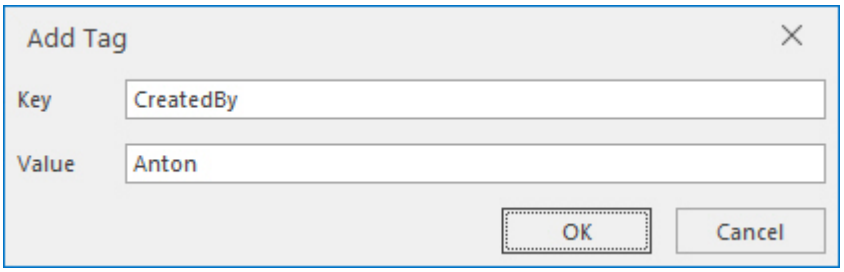
The **Tags** column shows tags for each object:



Click the button located to the right from each row to open the **Edit tags** dialog:



To add the new tag, click the **Add** button and type in its parameters, and then click **OK**:



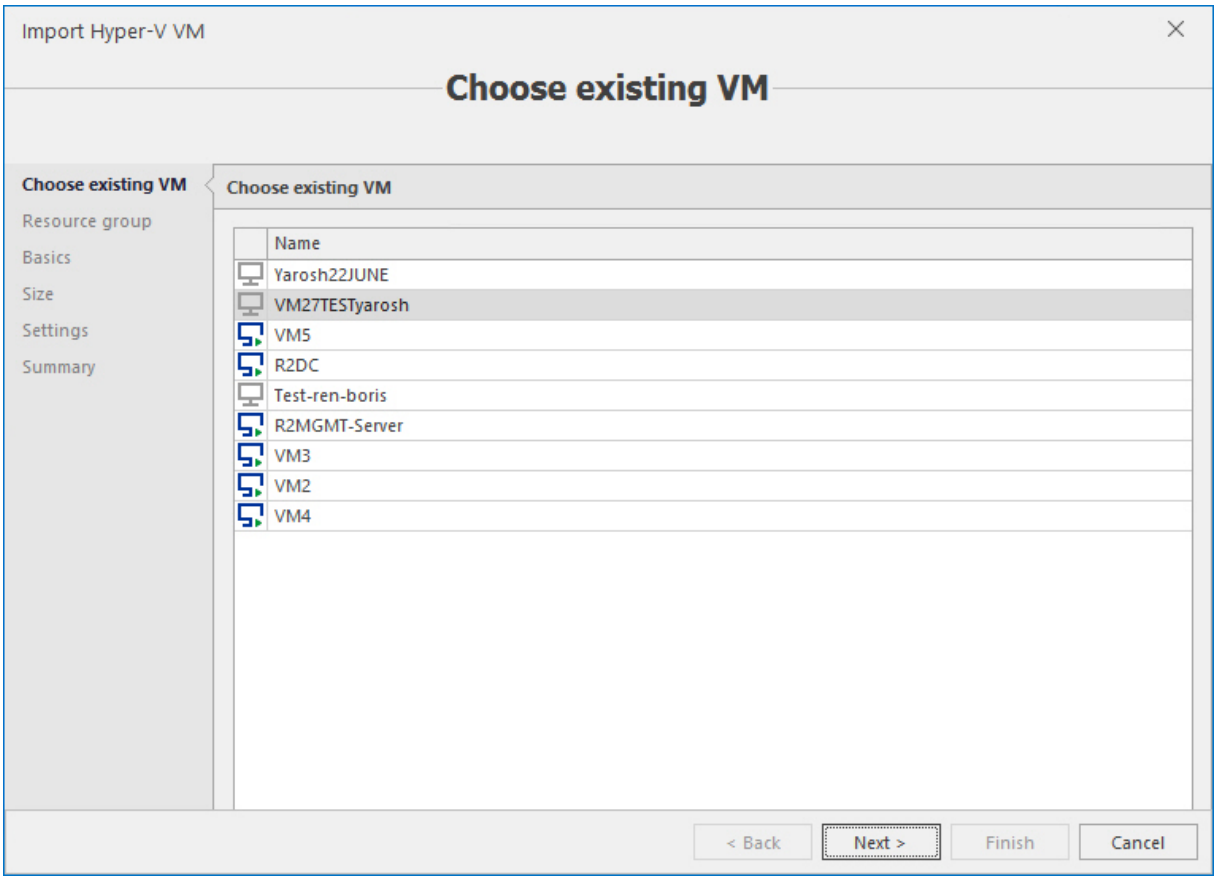
To remove the tag, select it and click the **Remove** button.

At the end, click **OK** in the **Edit tags** dialog to complete the operation.

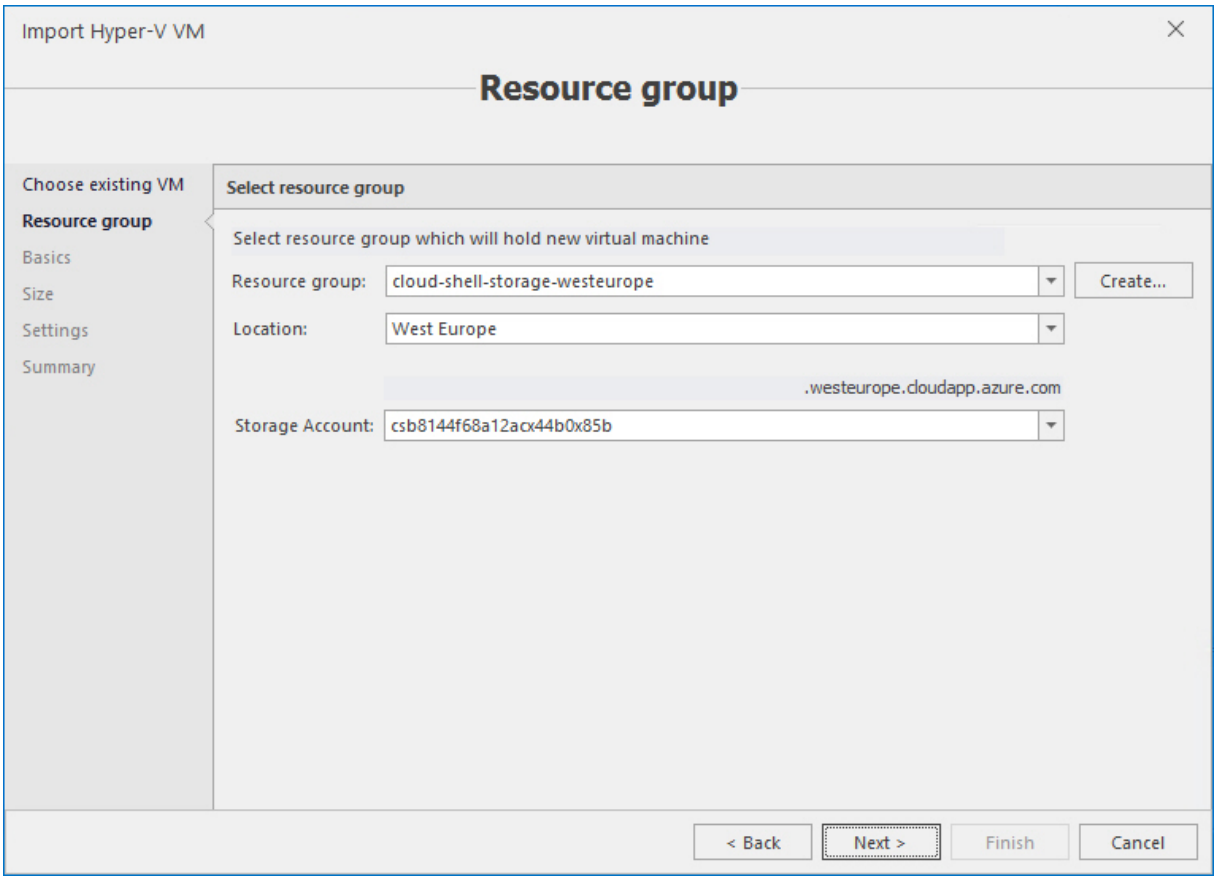
Importing Hyper-V VM into Azure

Note
Only stopped VM can be imported into Microsoft Azure.

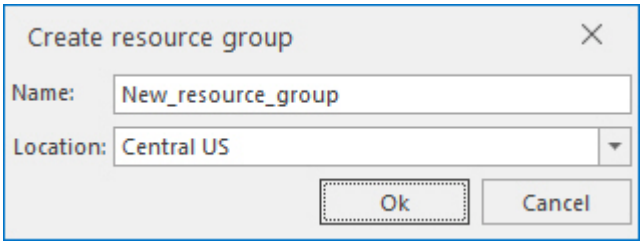
To import Hyper-V VM into Azure, select it, make sure it is in stopped state, and then click the **Import Hyper-V VM** button on the main ribbon. The **Import Hyper-V VM** wizard will be opened:



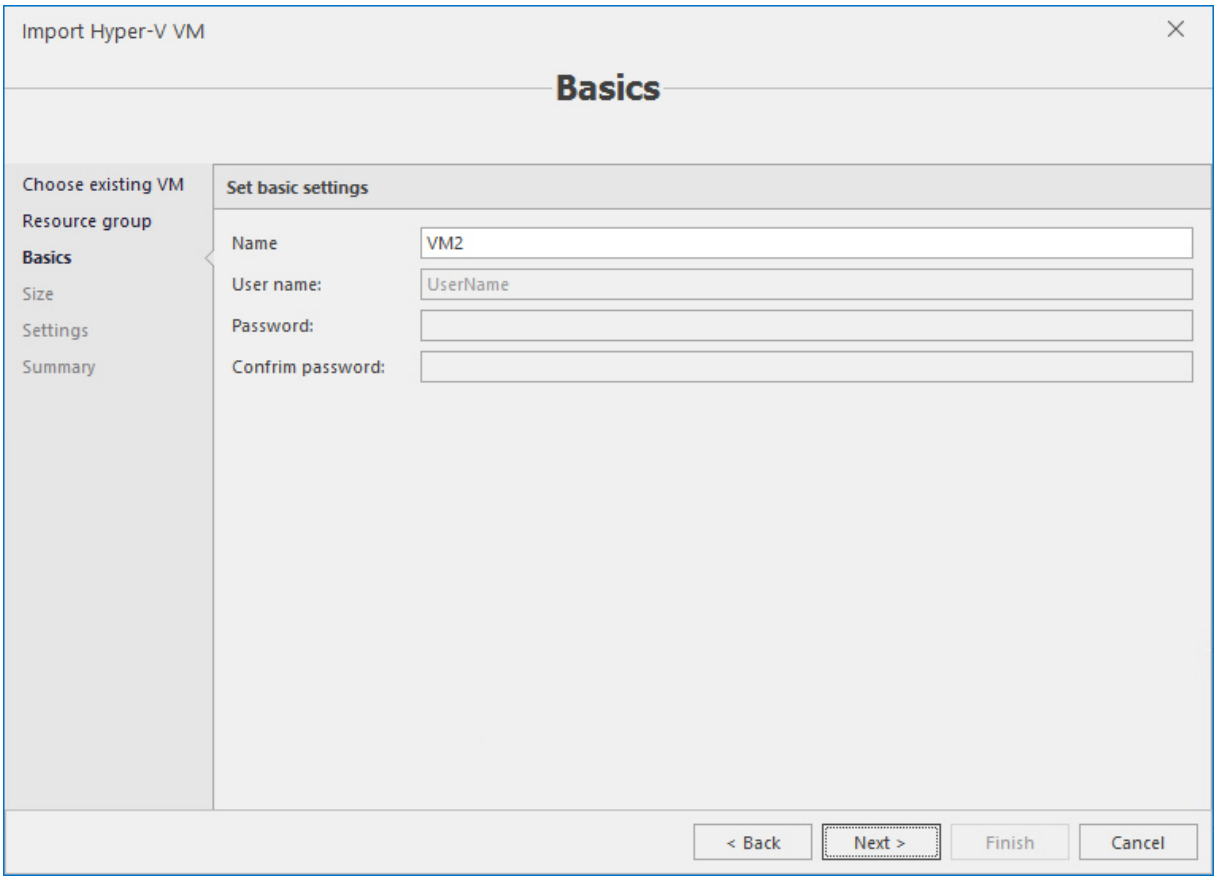
On the first screen, select VM that needs to be imported into Microsoft Azure. Click **Next**.



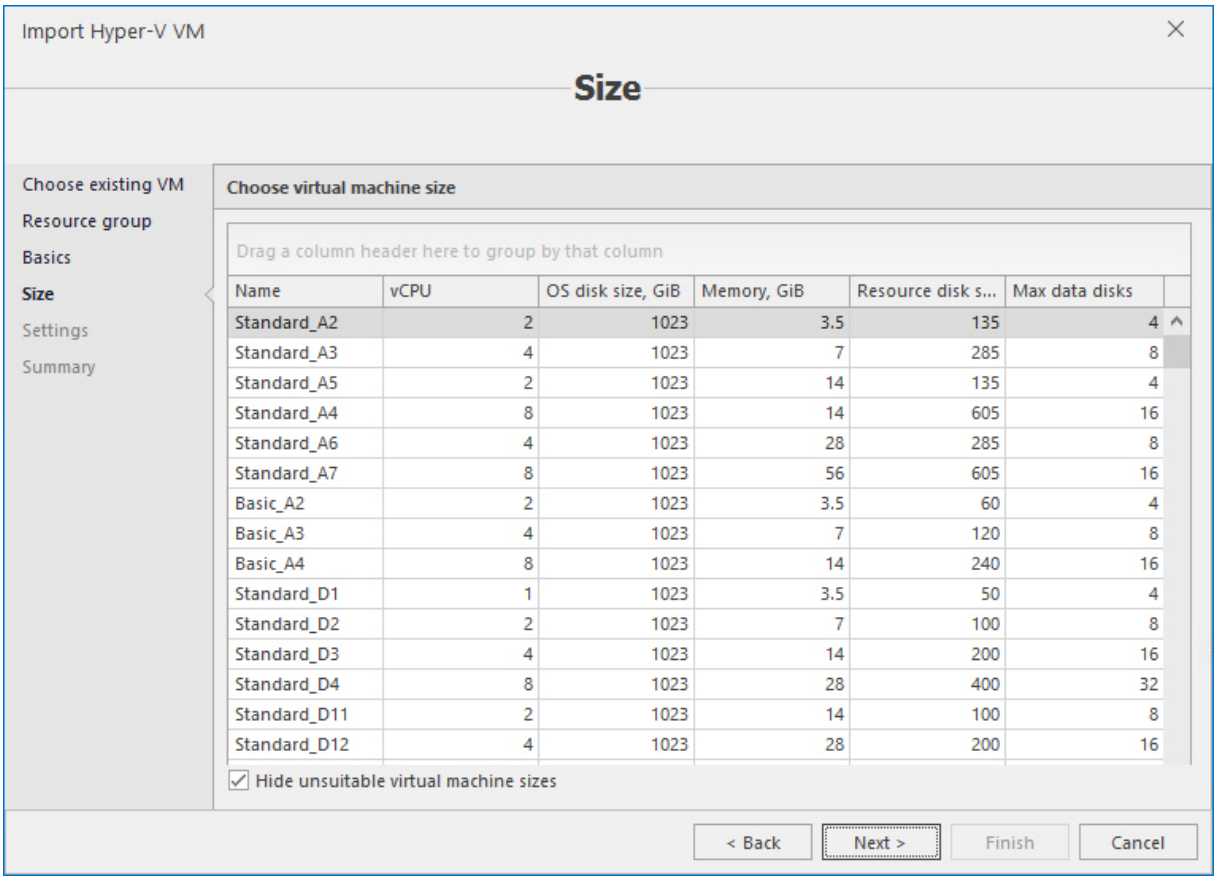
On the next screen, select resource group, location and storage account. To create the new resource group, click the **Create** button to the right from the **Resource group** field:



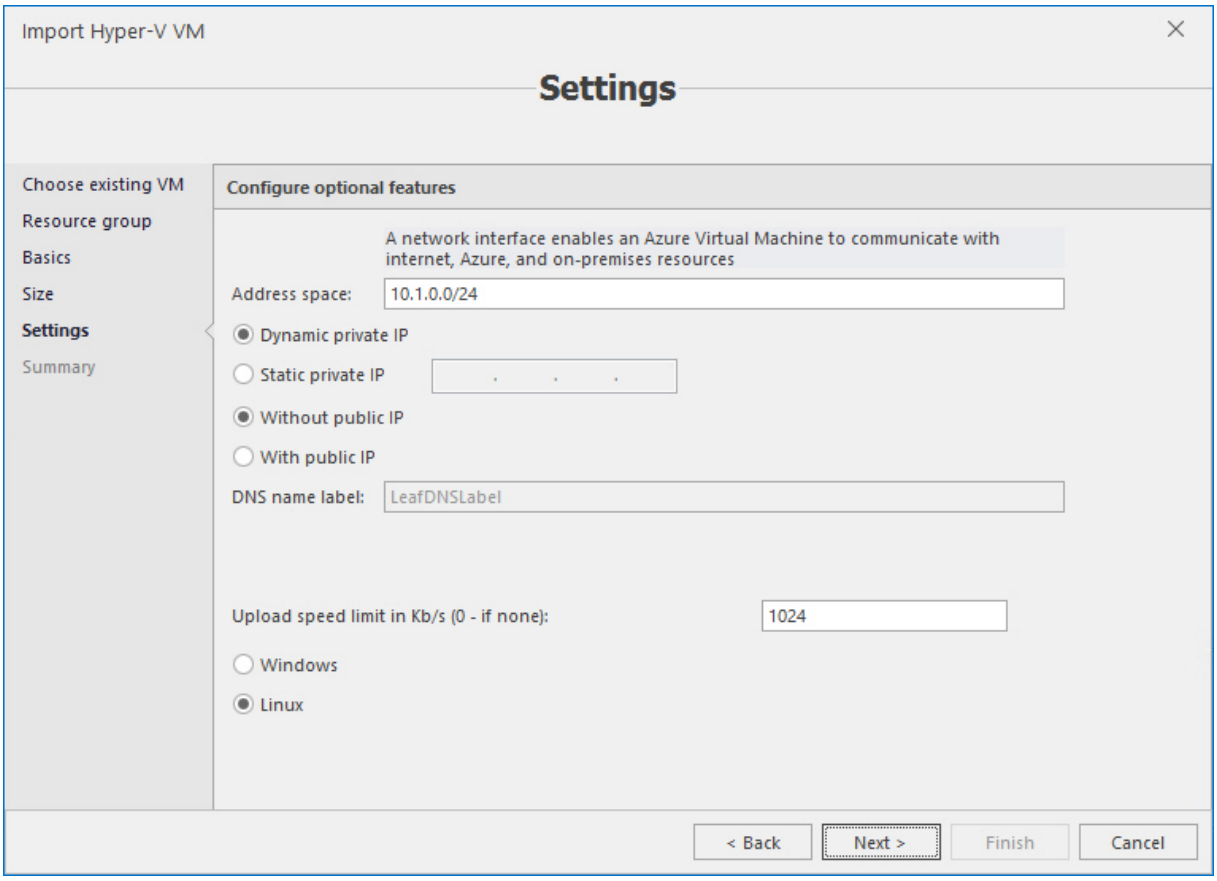
Enter the name for the new resource group and select the location. Click **OK**. Click **Next** in the main window.



On the next screen, edit the name for virtual machine as it will appear in Microsoft Azure. Only this parameter can be edited. Click **Next**.



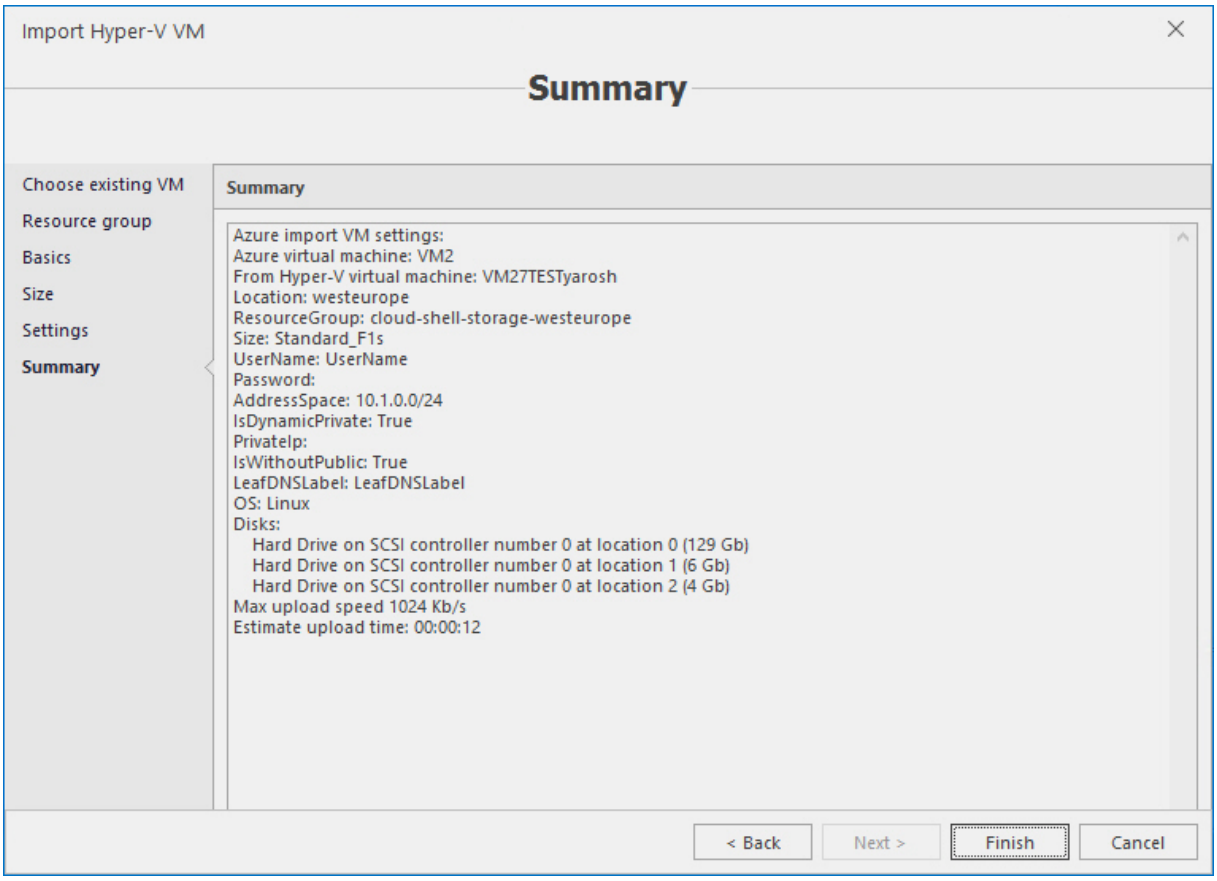
Select size for VM. Click **Next**.



Configure the following settings for VM:

- IP addresses;
- Upload speed limit in Kb/s (0 – if none);
- Guest OS type.

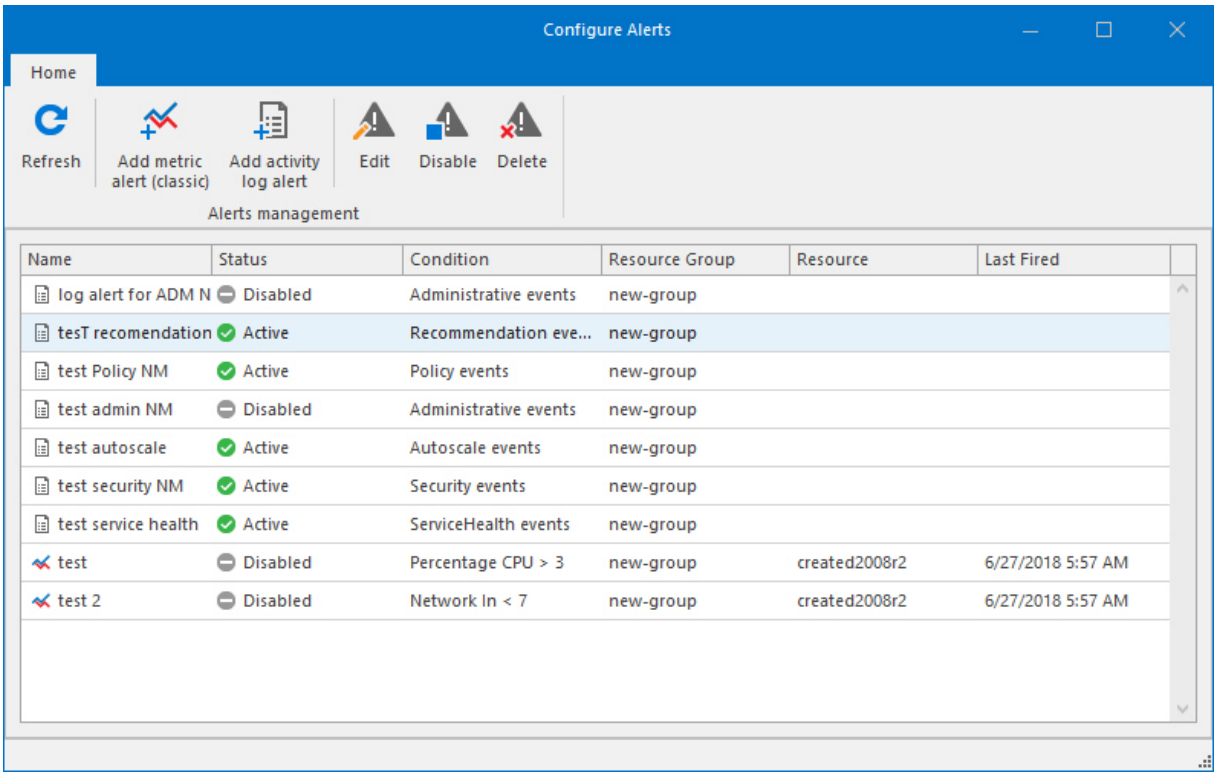
Click **Next**.



Review the summary and click **Finish**.

Configuring Azure monitoring alerts

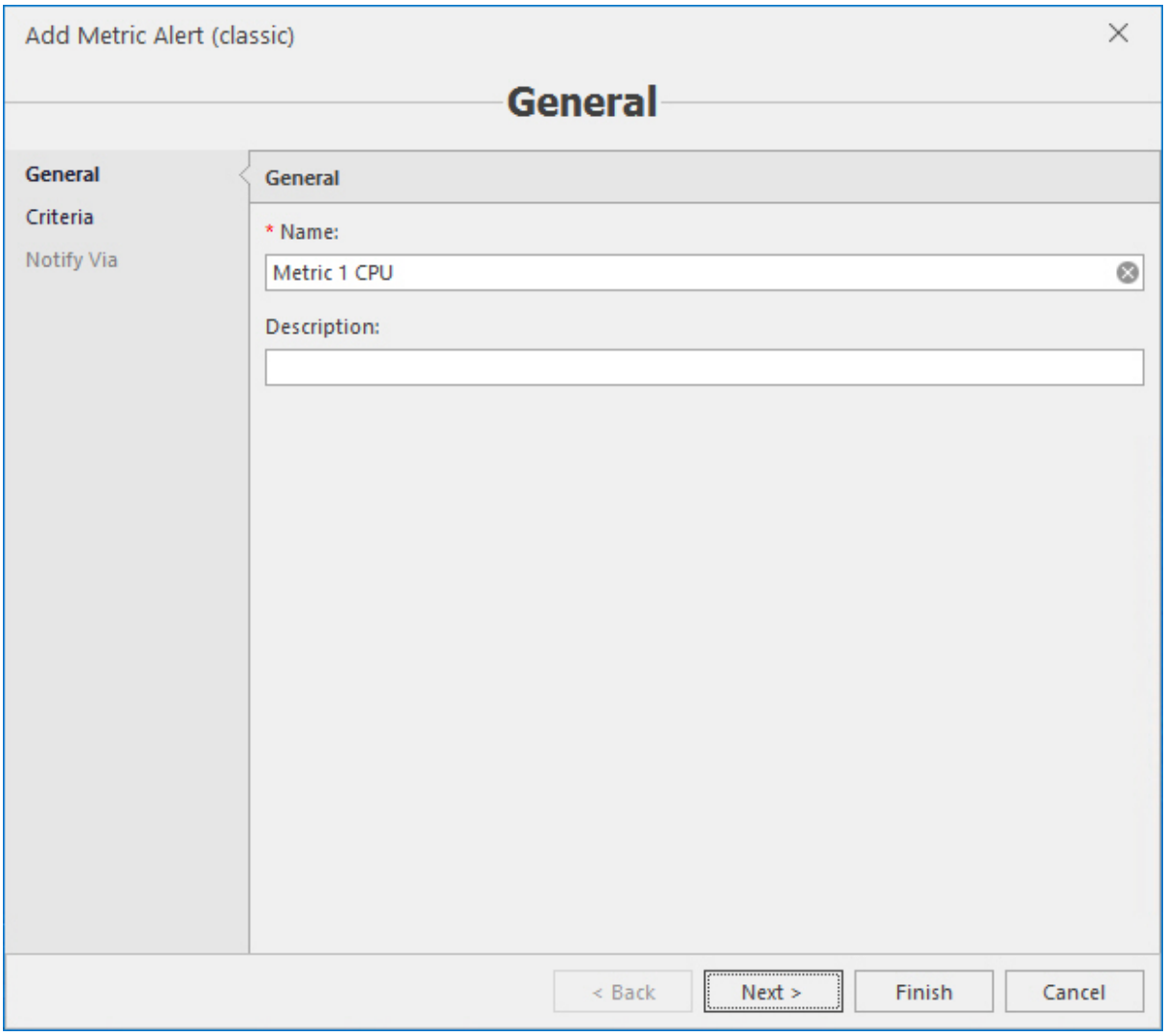
To configure Azure monitoring alerts, click the **Configure alerts** button on the main ribbon.



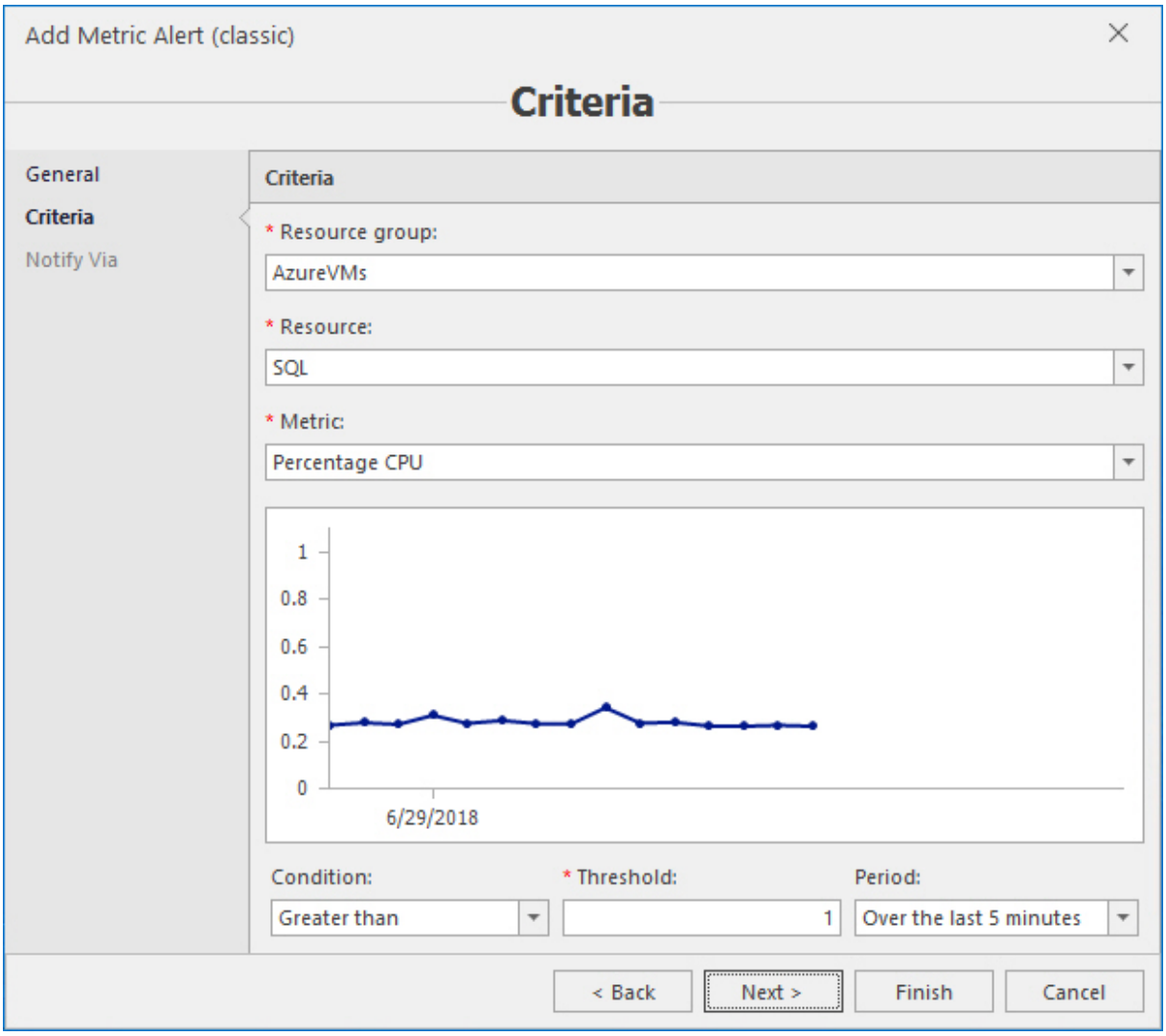
There are two types of alerts – metric alert (classic) and activity log alert. Metric alerts contain numerical data, such as, CPU percentage, disk write/read operations in bytes and sec, network performance etc. Activity log alerts contain information about various services, security issues and actions.

Configuring metric alerts

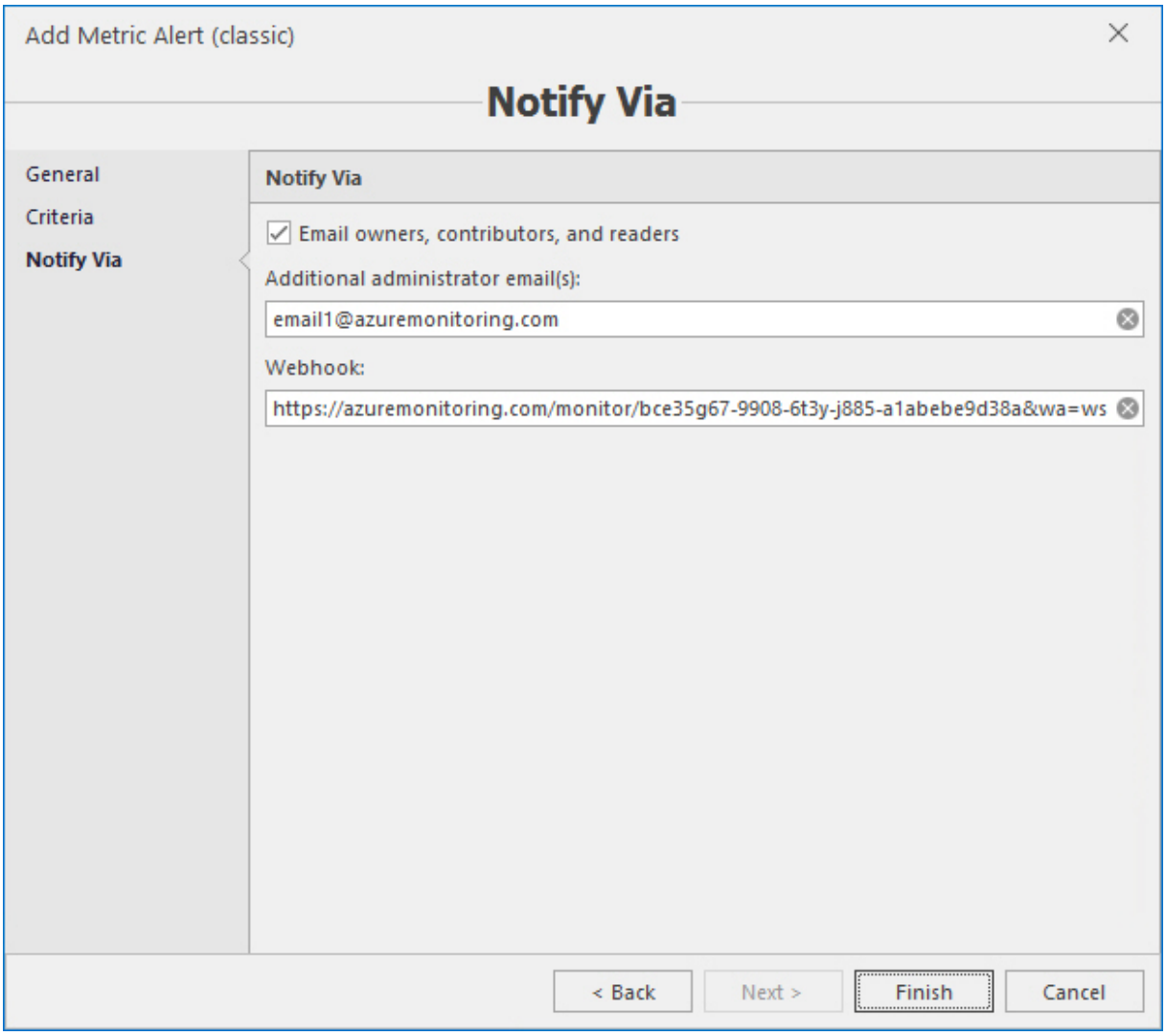
To add metric alert, click the **Add metric alert (classic)** button on the main ribbon. The **Add metric alert (classic)** wizard will be opened:



On the **General** screen type the name and description (if necessary) and click **Next**.



On the next screen, specify the criteria for the alert – resource group, resource, metric, condition, threshold and period. Click **Next**.

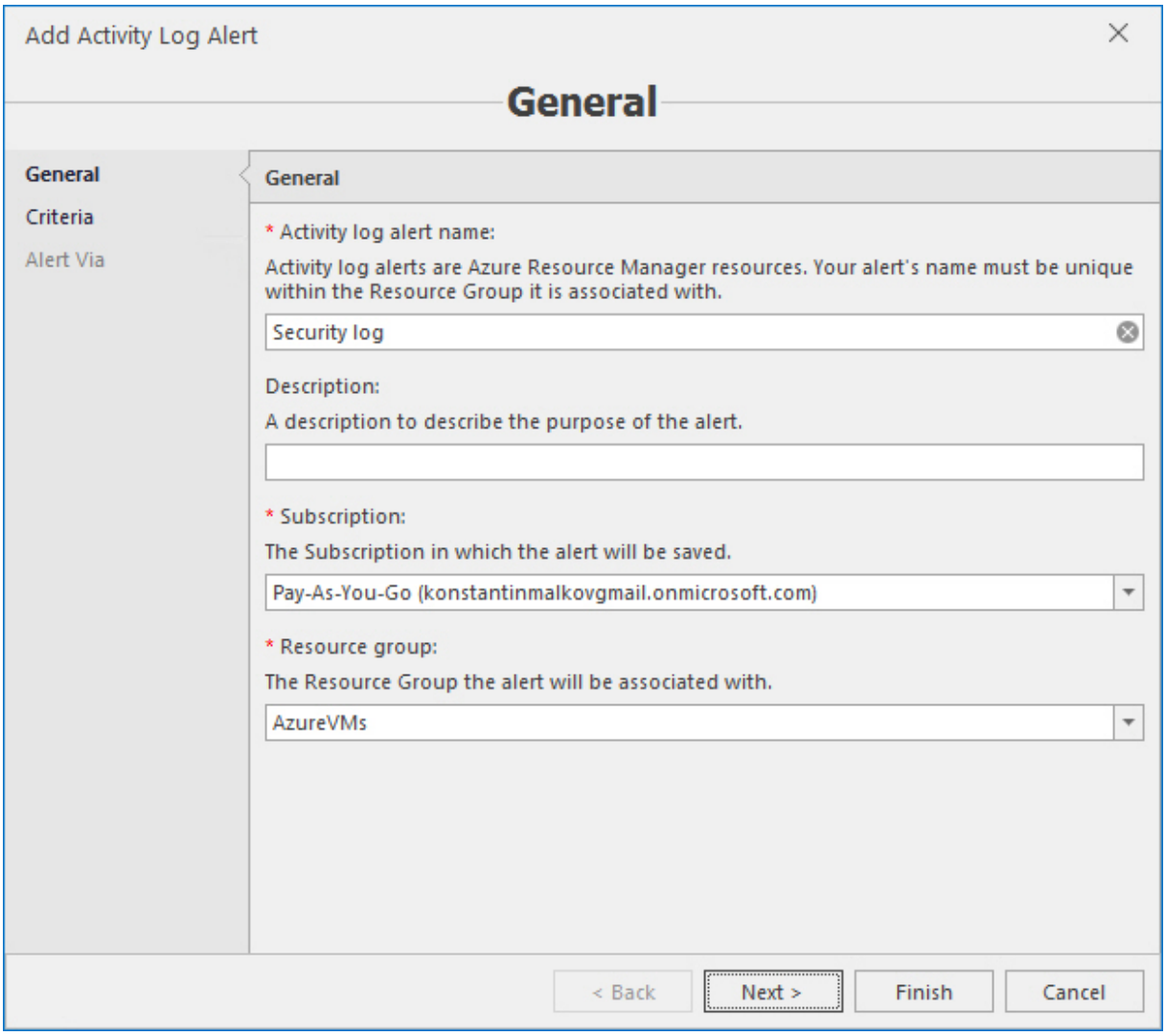


On the last screen determine, whether and who should be notified – email owners, contributors and readers associated with Microsoft Azure subscription and/or additional email addresses, and/or specific http/https endpoint, where the alerts should be sent. Click **Finish**.

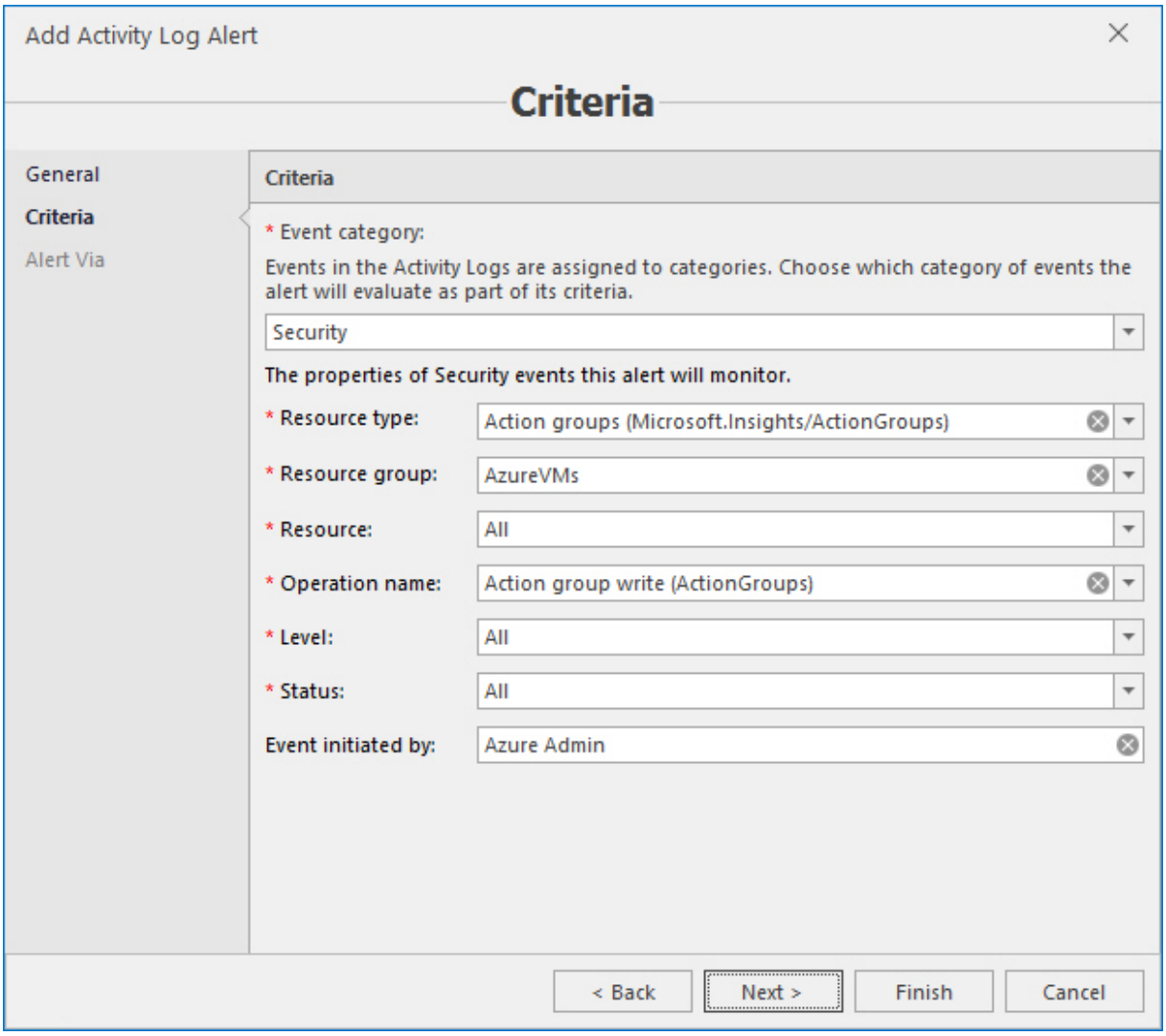
To edit the metric alert, select it in the **Configure alerts** window and click the **Edit** button on the main ribbon. Then repeat the same actions as when adding the alert – edit alert settings as required. To remove the metric alert, select it in the **Configure alerts** window and click the **Delete** button on the main ribbon.

Configuring activity log alert

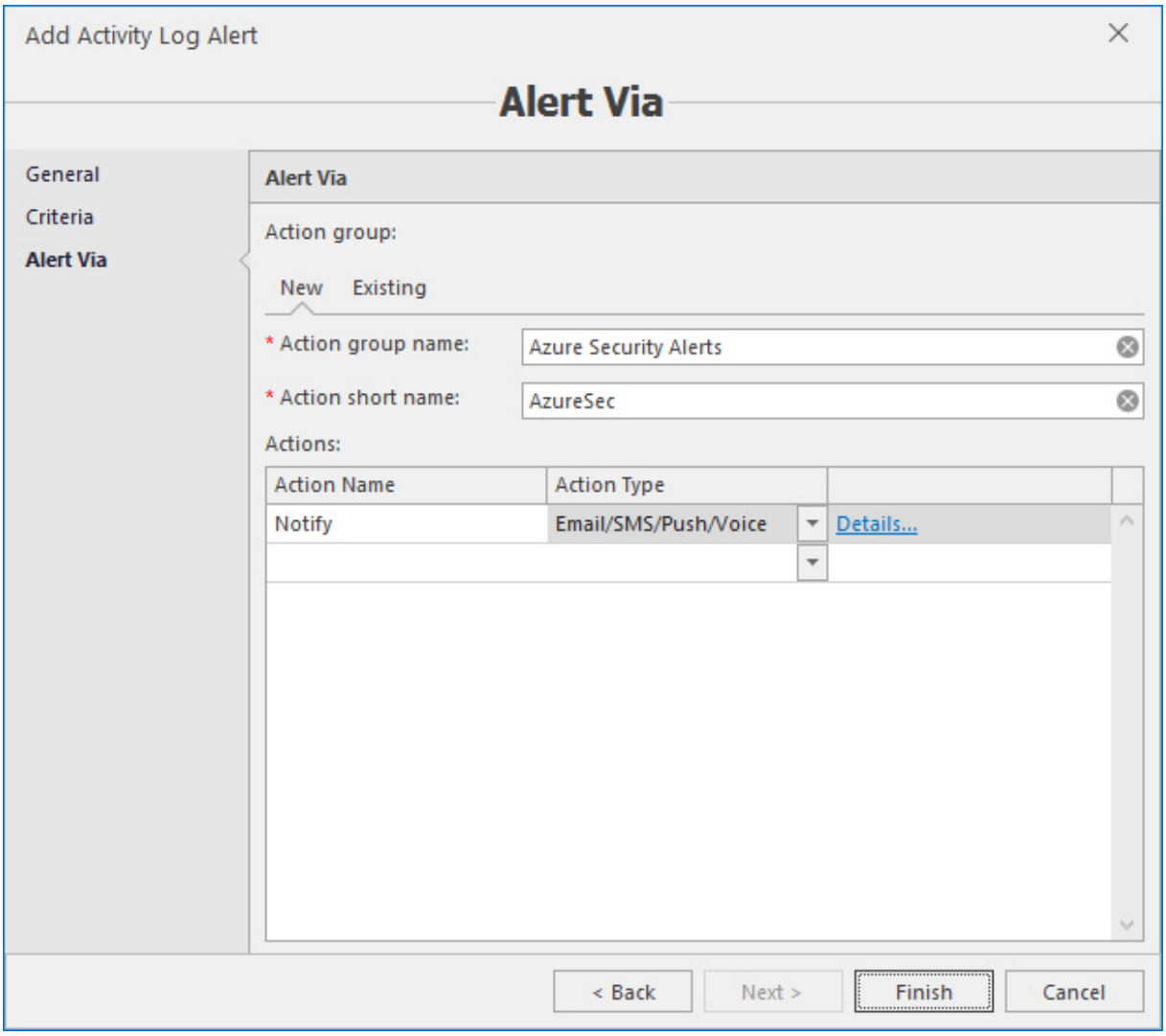
To add activity log alert, click the **Add activity log alert** button on the main ribbon. The **Add activity log alert** wizard will be opened:



On the **General** screen, specify the following parameters – activity log alert name, description (if necessary), Microsoft Azure subscription and resource group. Click **Next**.



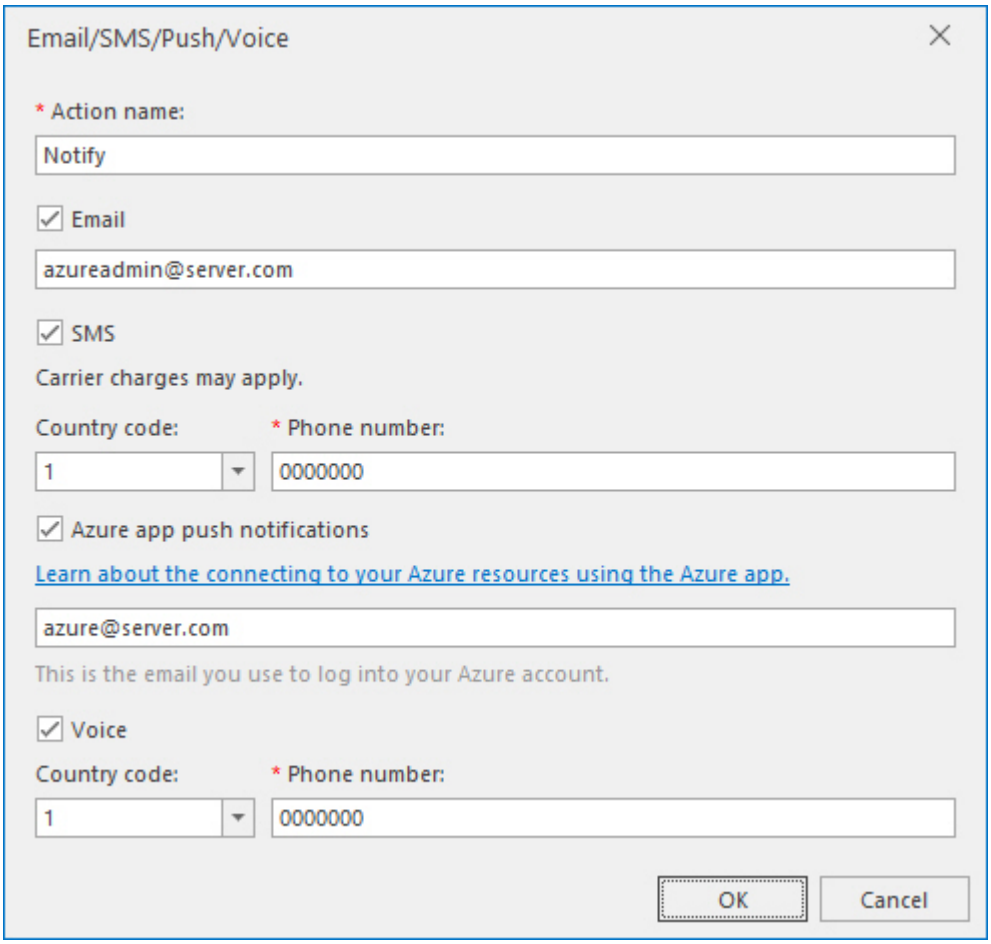
On the next screen, specify criteria for the activity log alert. Events in the activity logs are assigned to categories. First, select the required category, then select properties. The **All** value that is set by default will include all values in each property. Also, you may type the name or another ID of the person who created the alert, if required. Click **Next**.



On the last screen, specify notification actions associated with the alert. You can configure the new group or select the existing one.

To configure the new notification action group, stay on the **New** tab and enter full and short name for the new group. Then specify action name and type.

Click on **Details** link. The following dialog will be opened:



Fill up the parameters for notification methods as required – email, SMS, push and/or voice. Click **OK**. You may add several actions into the new group.

To select the existing action group, move to the **Existing** tab:

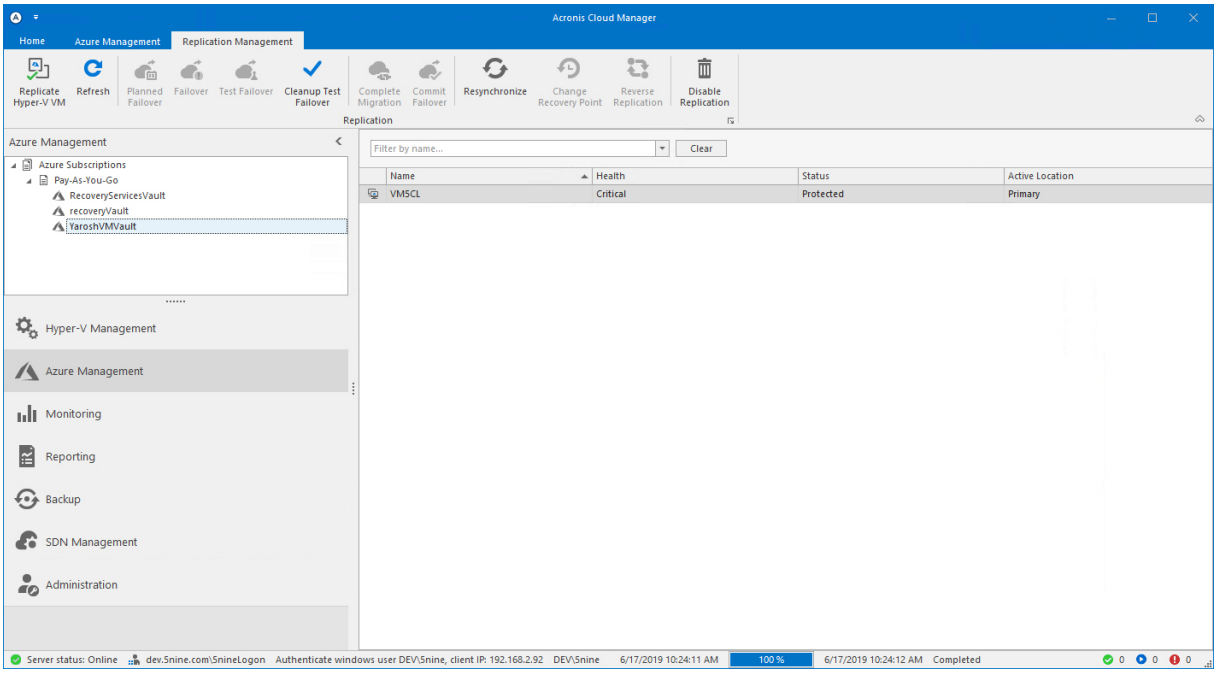
Select the required action group from the drop-down box.

Click **Finish** on the wizard when you complete the operation to add the new activity log alert.

To edit the activity log alert, select it in the **Configure alerts** window and click the **Edit** button on the main ribbon. Then repeat the same actions as when adding the alert – edit alert settings as required. To remove the activity log alert, select it in the **Configure alerts** window and click the **Delete** button on the main ribbon.

Hyper-V VM replication into Azure

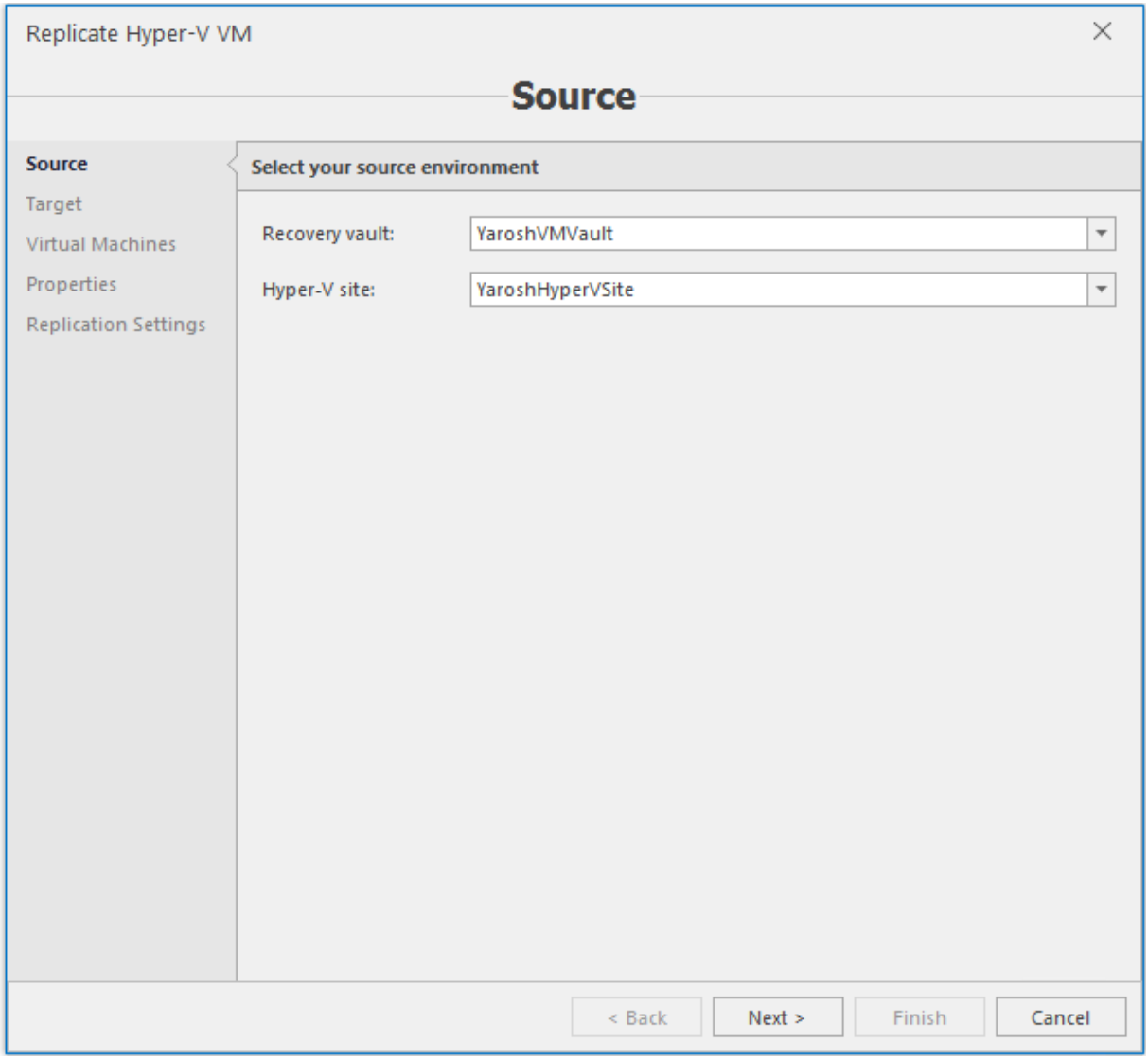
The **Azure management** plugin provides ability to replicate Hyper-V VMs into Azure, which acts as a replica server instead of the other Hyper-V server since that happens in the Hyper-V replication environment. This Acronis Cloud Manager feature is managed on the **Replication management** tab:



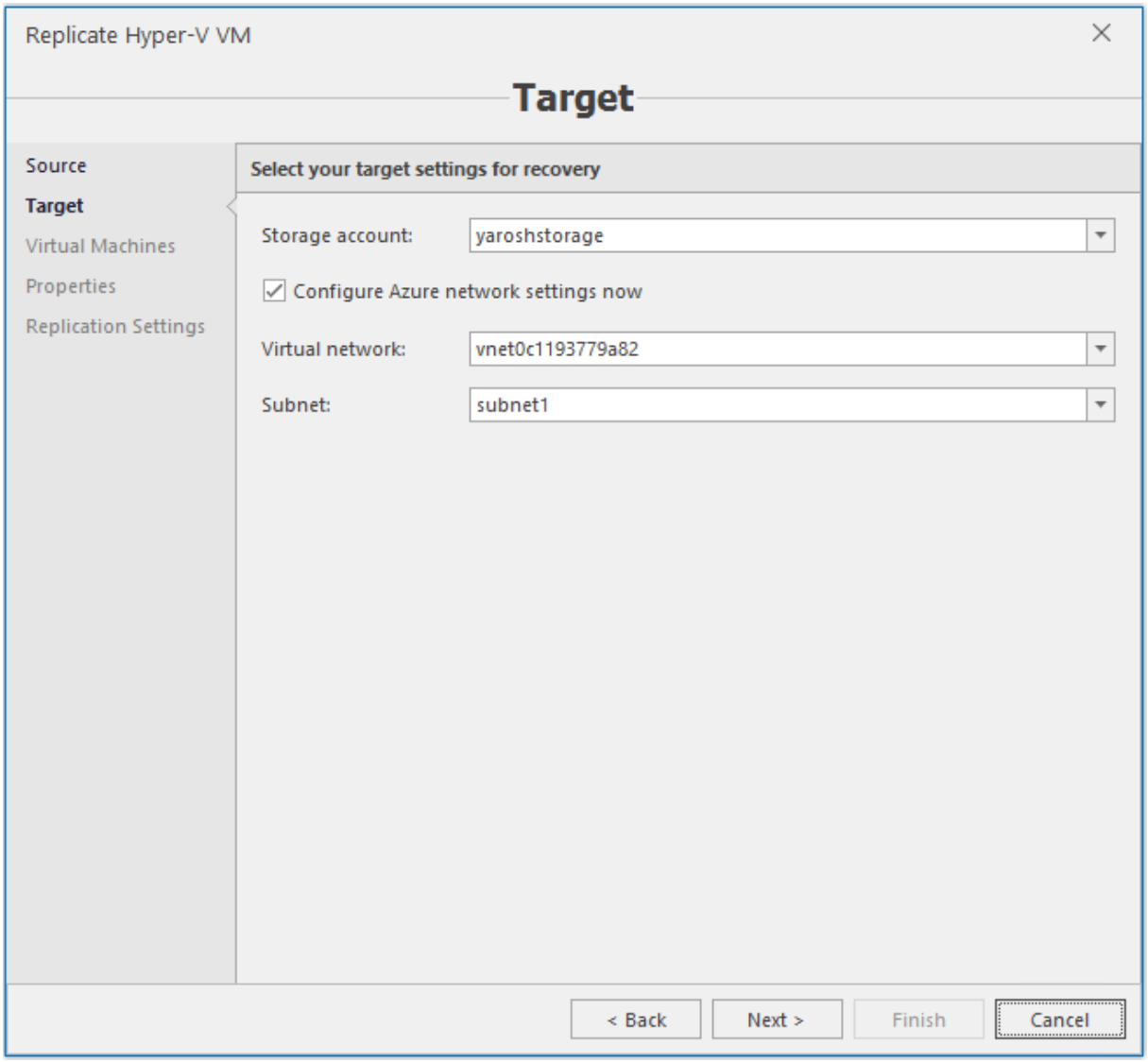
To start Hyper-V VM replication into Azure, first select the subscription to which VM will be replicated. To be able to start replication into Azure using Acronis Cloud Manager, the recovery vault with all necessary parameters must be configured on Azure portal for the selected subscription.

Click the **Replicate Hyper-V VM** button on the main ribbon.

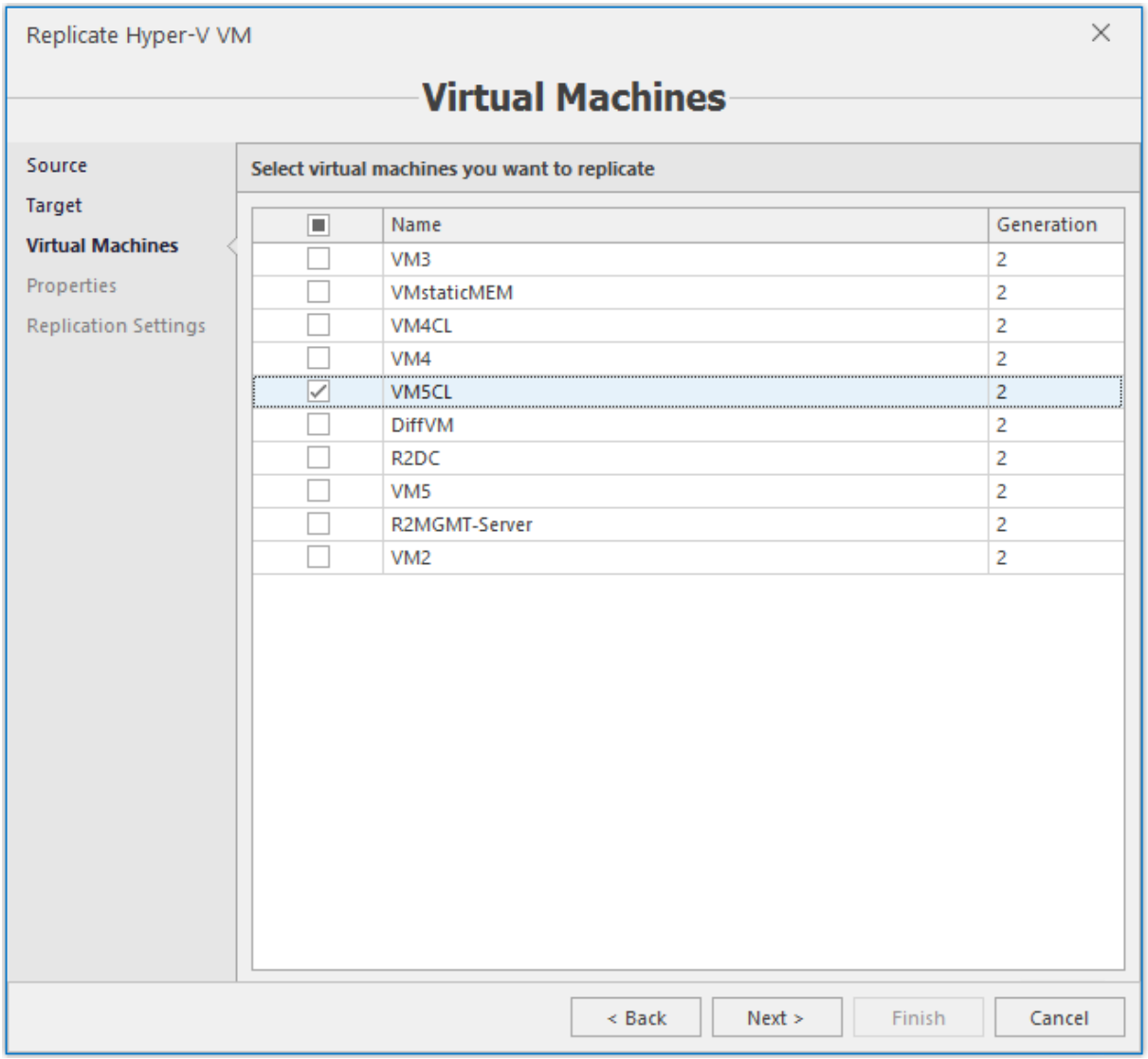
Configure replication parameters:



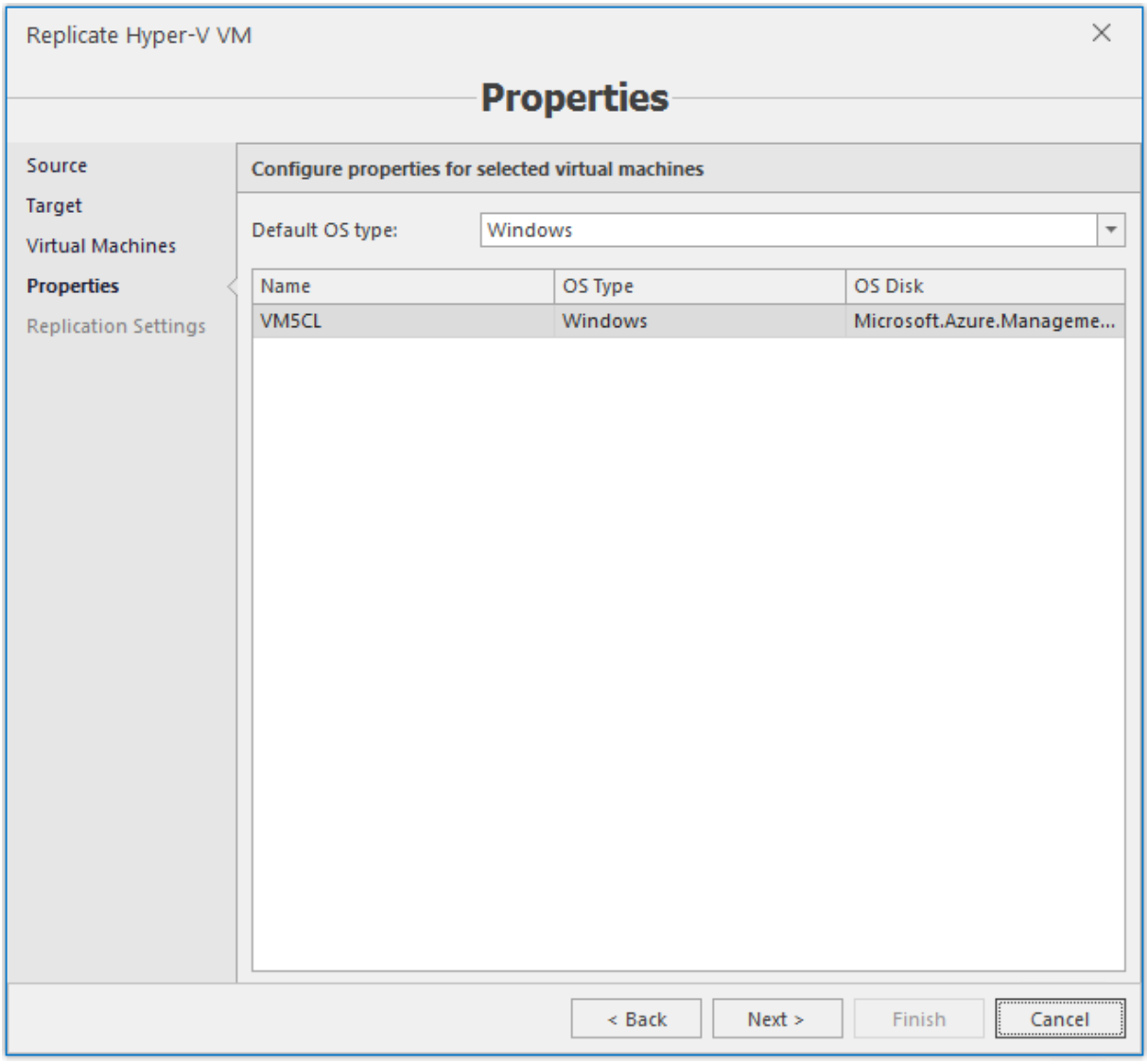
Select the recovery vault and Hyper-V site. These parameters must be configured on Azure portal in advance. Click **Next**.



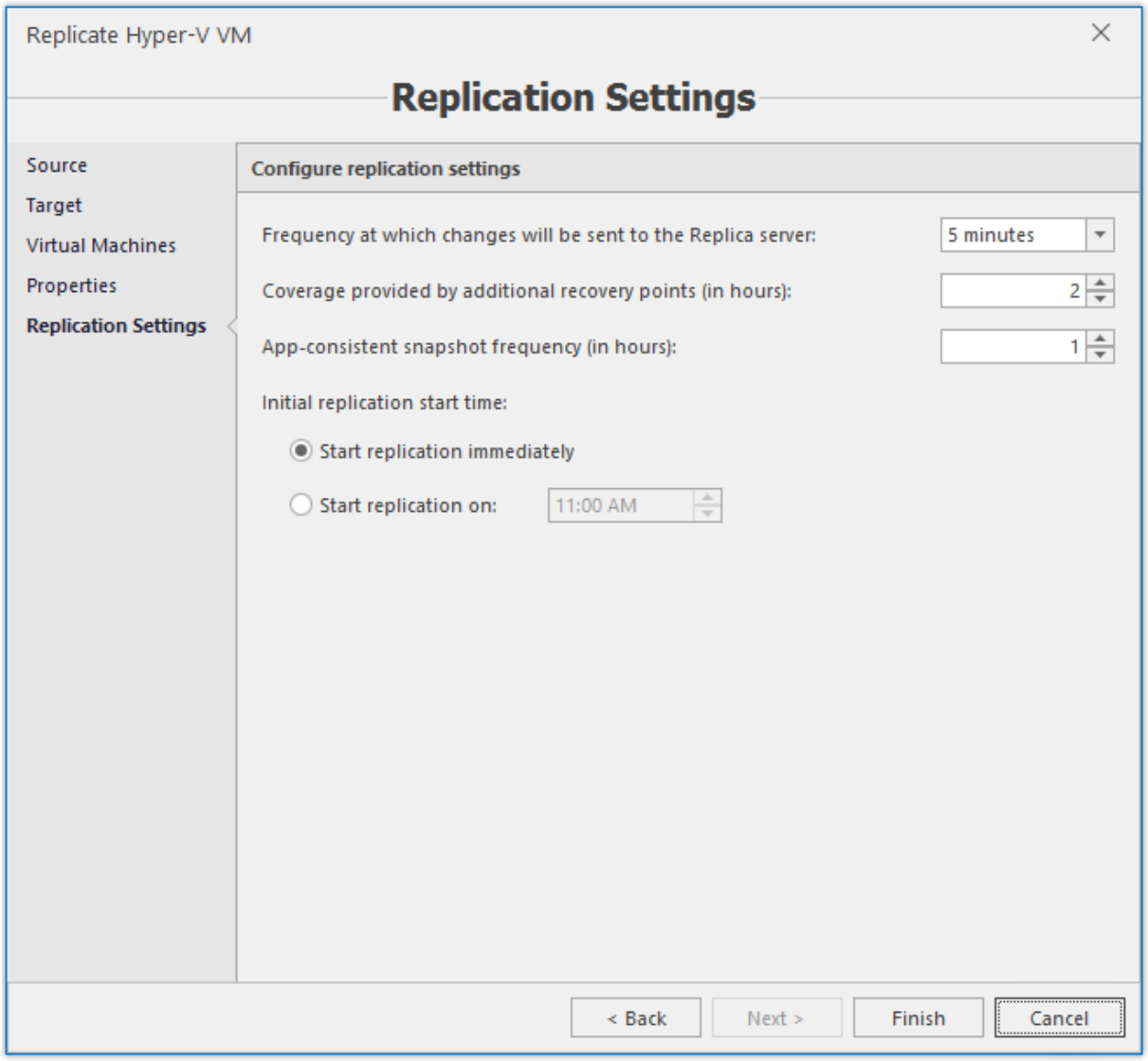
Configure the target settings for recovery – storage account, virtual network and subnet. Click **Next**.



Select virtual machines for replication. Click **Next**.



Select the operating system of the VM (Windows/Linux). Click **Next**.

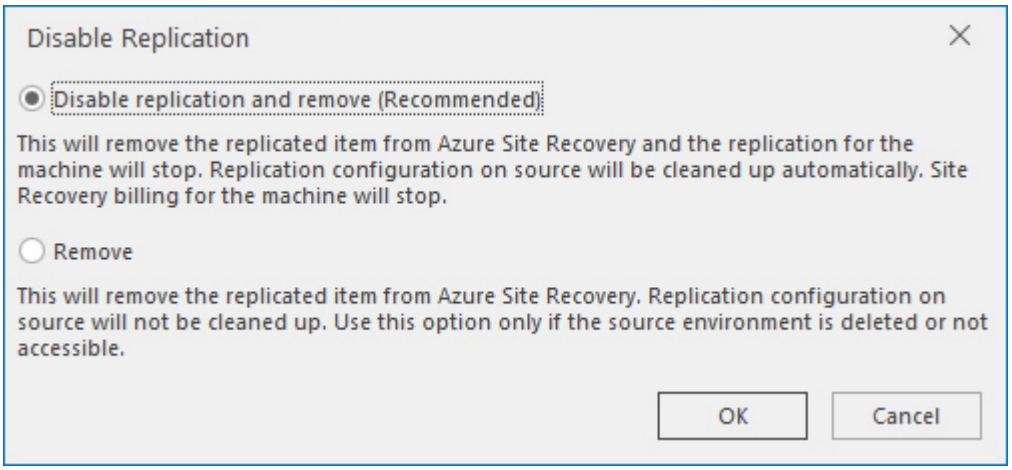


Configure the general replication settings:

- Frequency to send changes to the Replica server (Azure).
- Coverage period in hours, which additional recovery points provide.
- Application-consistent snapshot frequency in hours.
- Replication start time: immediately upon completing the replication configuration wizard or deferred start (at which moment in the future).

Click **Finish** to save replication configuration settings and start replication in accordance with the configured schedule.

Other replication operations available: failover, test failover, planned failover, commit failover, complete migration, resynchronize, change recovery point, reverse replication. Disabling replication into Azure will erase the replicated VM from Azure and, if configured, stop the replication on the VM:

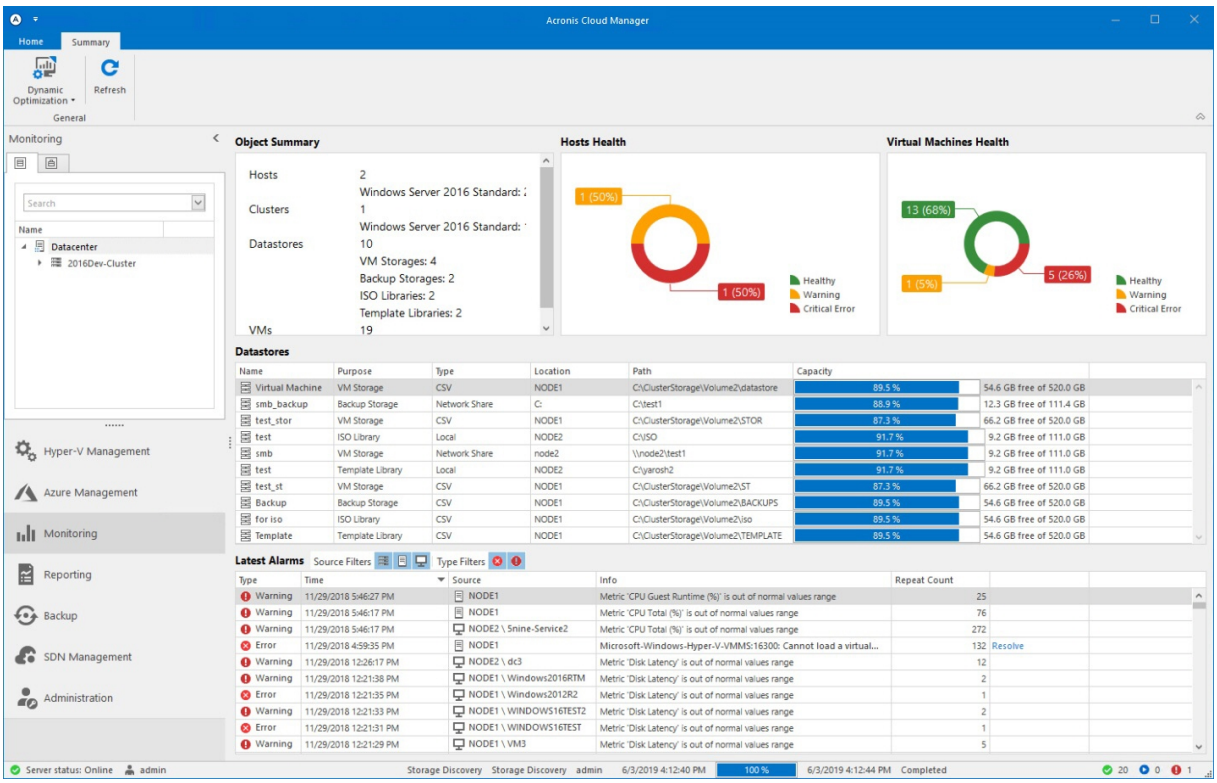


Hyper-V monitoring

Acronis Cloud Manager provides basic capabilities for cluster, host and VM monitoring. The **Datacenter** view provides consolidated data for the entire environment.

Datacenter monitoring

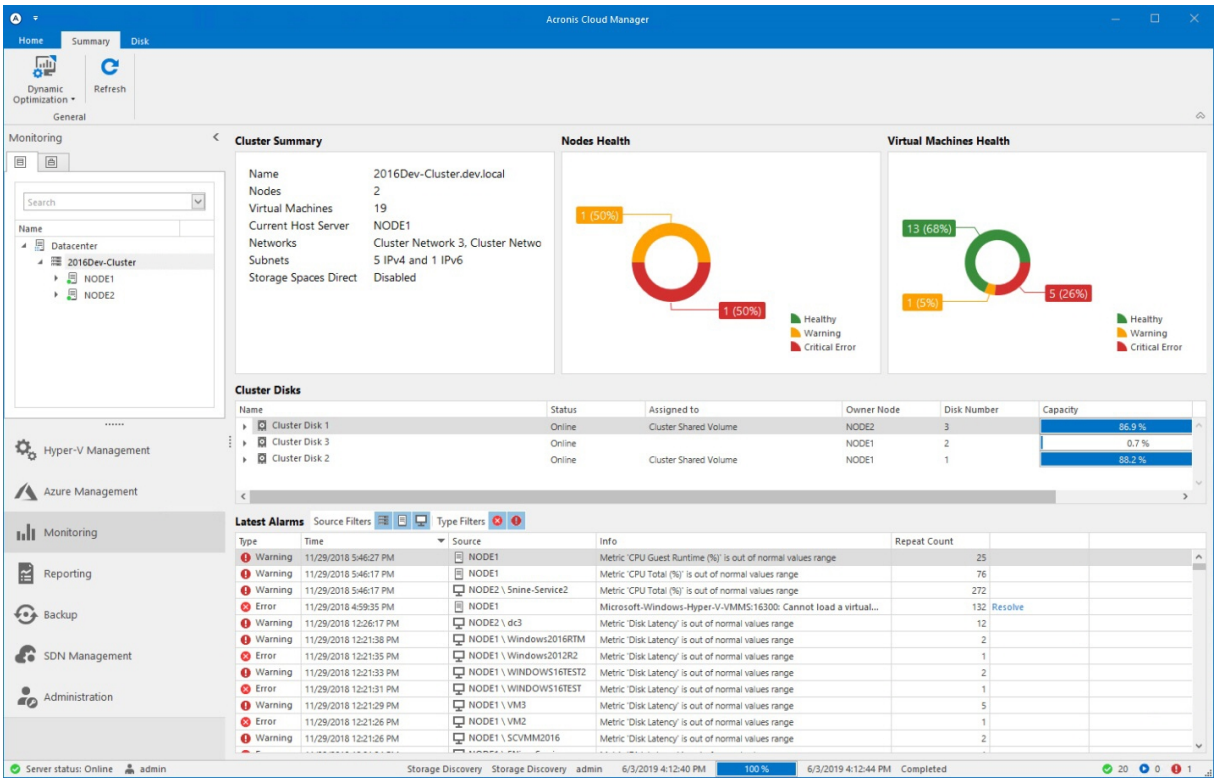
Datacenter monitoring contains consolidated data for all managed objects – clusters, hosts and virtual machines. It also displays datastore information and the list of latest alarms.



Cluster monitoring

Cluster monitoring has the following tabs containing information about cluster performance indicators:

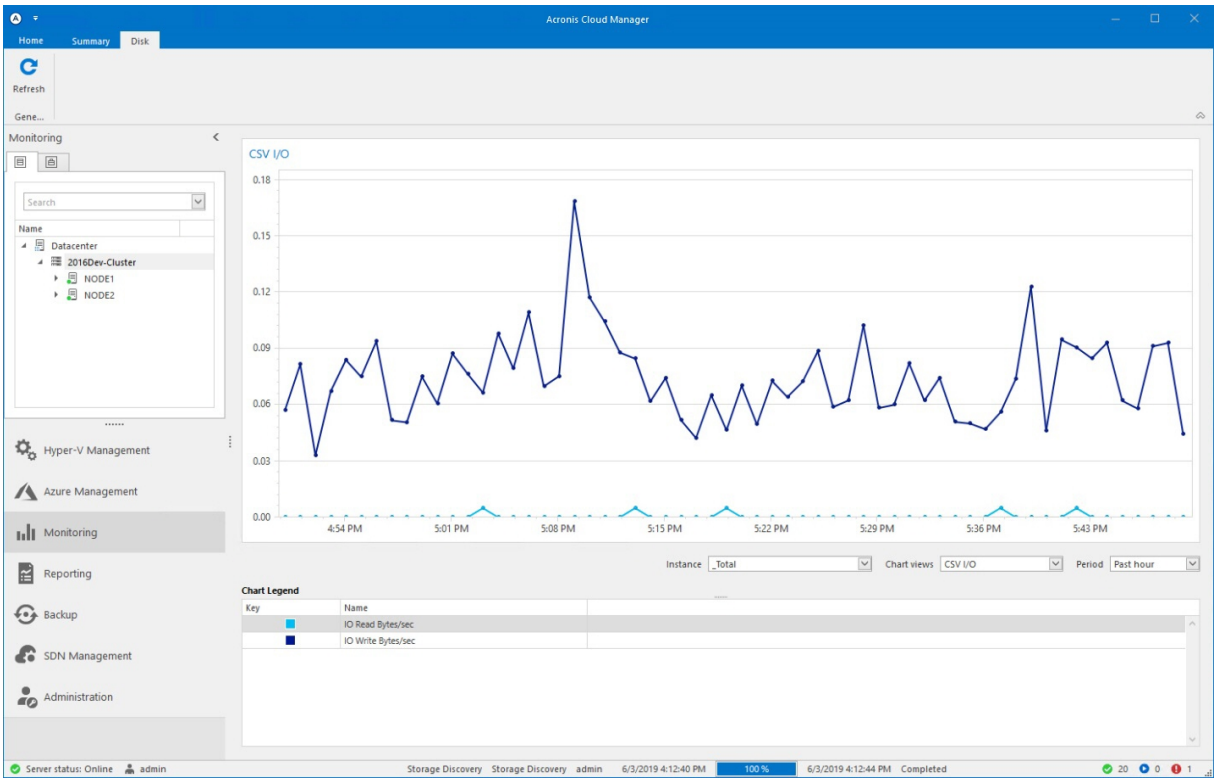
- **Summary**.
- **Disk**.



Note

Summary contains consolidated data for the cluster, overall nodes health diagram, overall VMs health diagram, cluster disks info and the list of latest alarms.

The **Disk** tab shows detailed diagram for CSV volumes I/O and historical data.

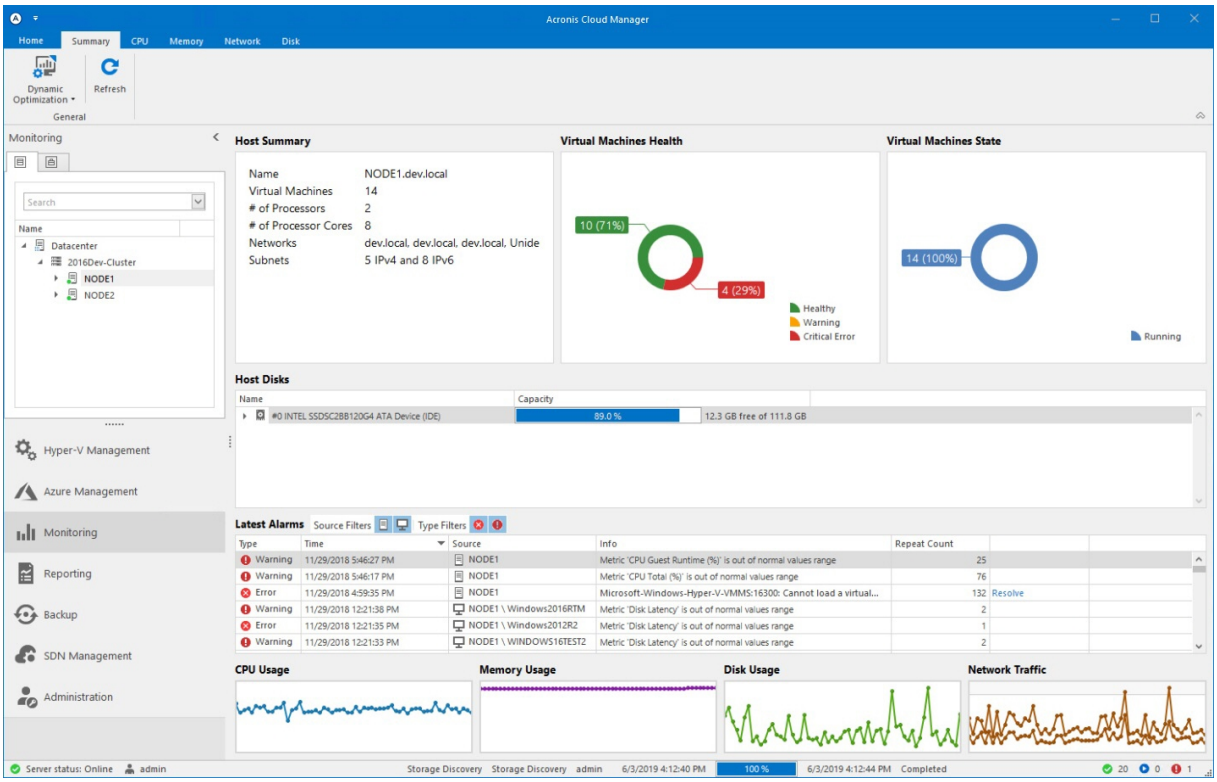


Host monitoring

Host monitoring has the following tabs containing information about host performance indicators:

- **Summary**.
- **CPU**.
- **Memory**.
- **Network**.
- **Disk**.

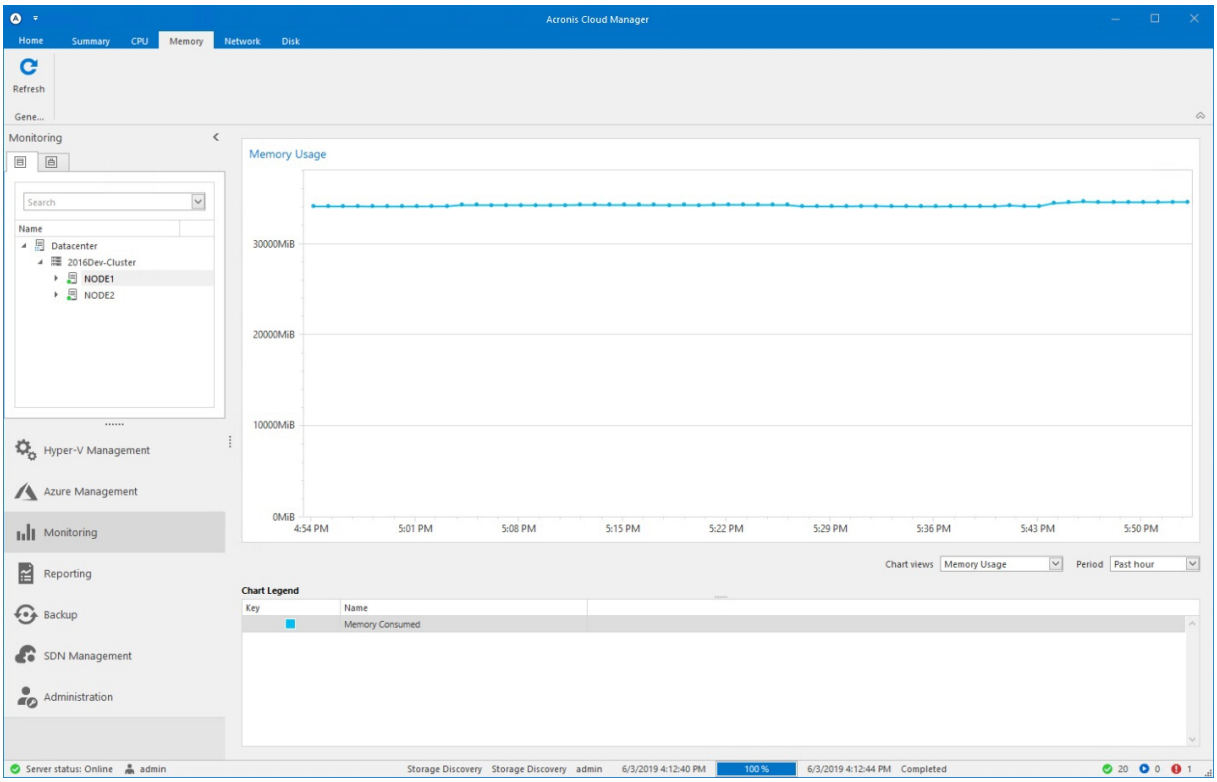
The **Summary** tab contains consolidated host information, VM states and health diagrams, host disks information, CPU total usage (%), memory consumption (Mb), disk read/write speed (MB/sec) and network in/out traffic (MB/sec) and the list of latest alarms.



Note

CPU, **Memory**, **Network** and **Disk** tabs show more indicators and historical data for the host.

E.g., the **Memory** tab displays the detailed information about the host memory consumption:

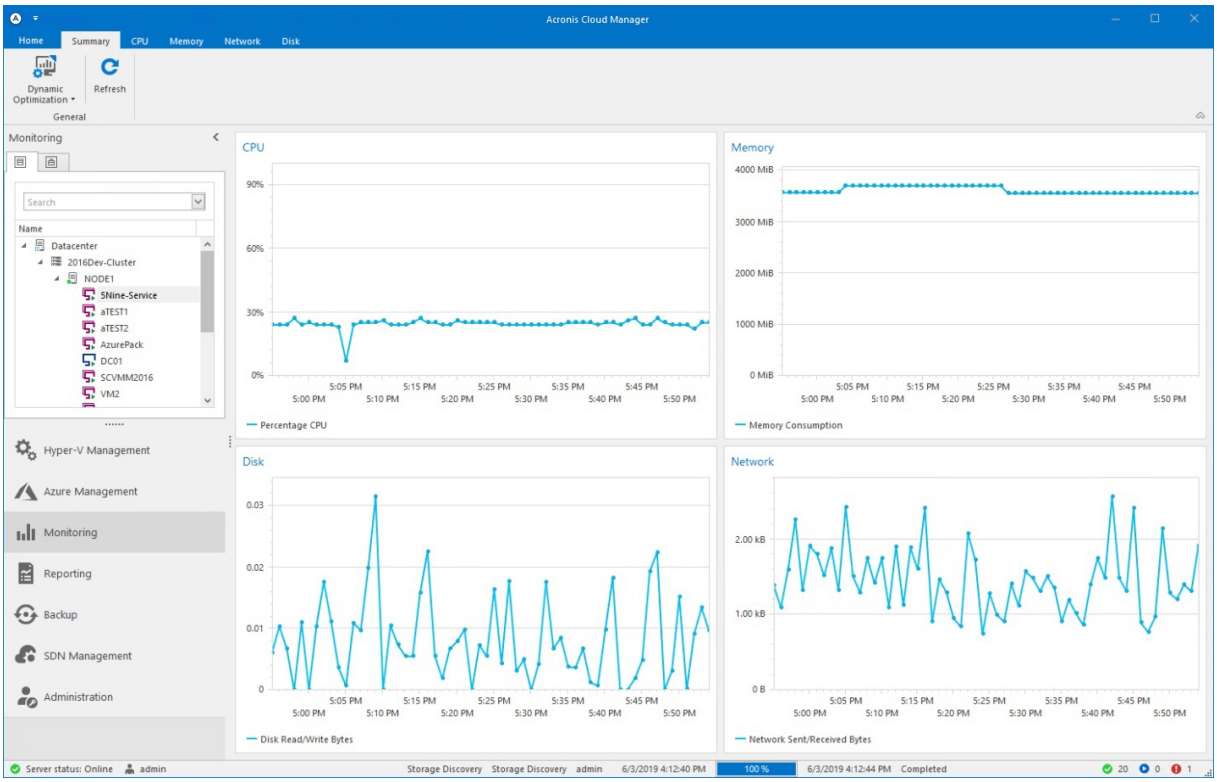


VM monitoring

VM monitoring has the following tabs containing information about VM performance indicators:

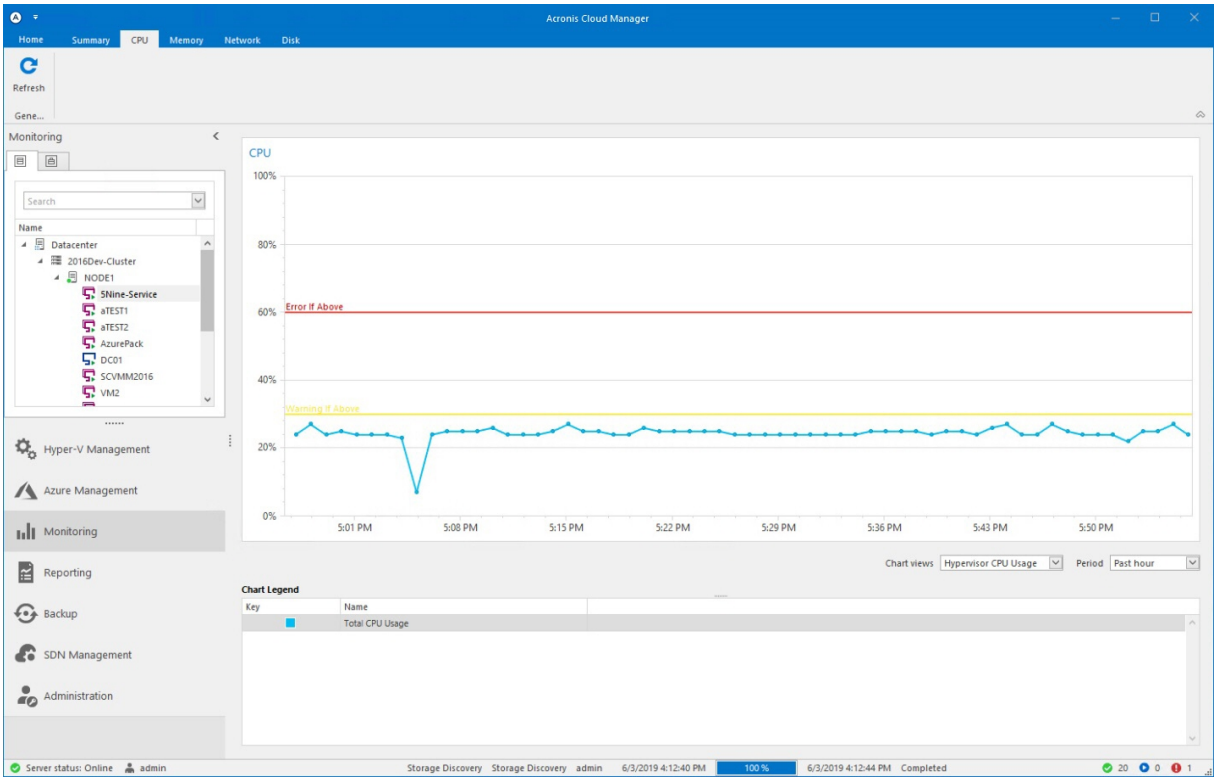
- **Summary**.
- **CPU**.
- **Memory**.
- **Network**.
- **Disk**.

The **Summary** tab contains VM CPU total usage (%), memory consumption (Mb), disk read/write speed (MB/sec) and network in/out traffic (MB/sec).



Note

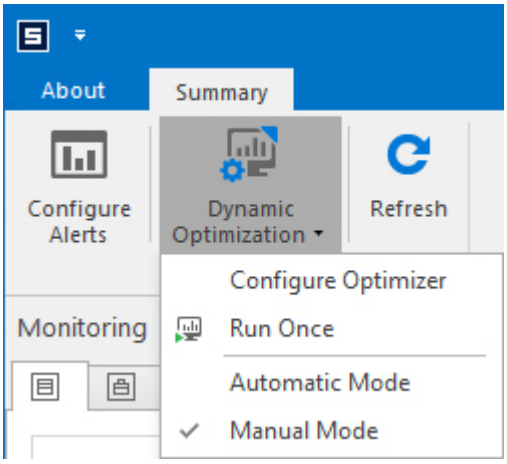
CPU, **Memory**, **Network** and **Disk** tabs show more indicators and historical data for the VM.



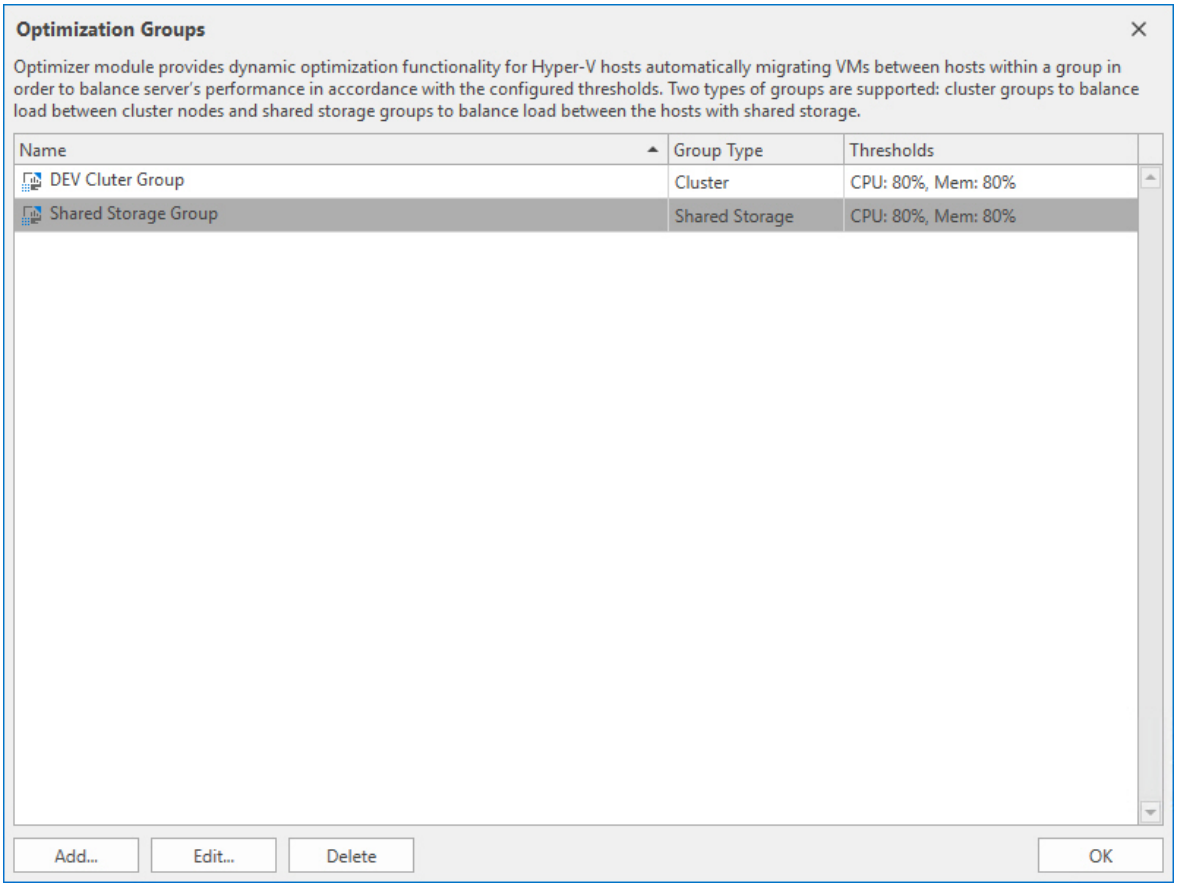
Optimizer

Optimizer is an active part of Acronis Cloud Manager monitoring feature. It provides dynamic optimization for Hyper-V servers' VM load based on the configured parameters and each server's performance. Selected VMs will be dynamically migrated to a less loaded Hyper-V host (cluster node) in accordance with the configured thresholds.

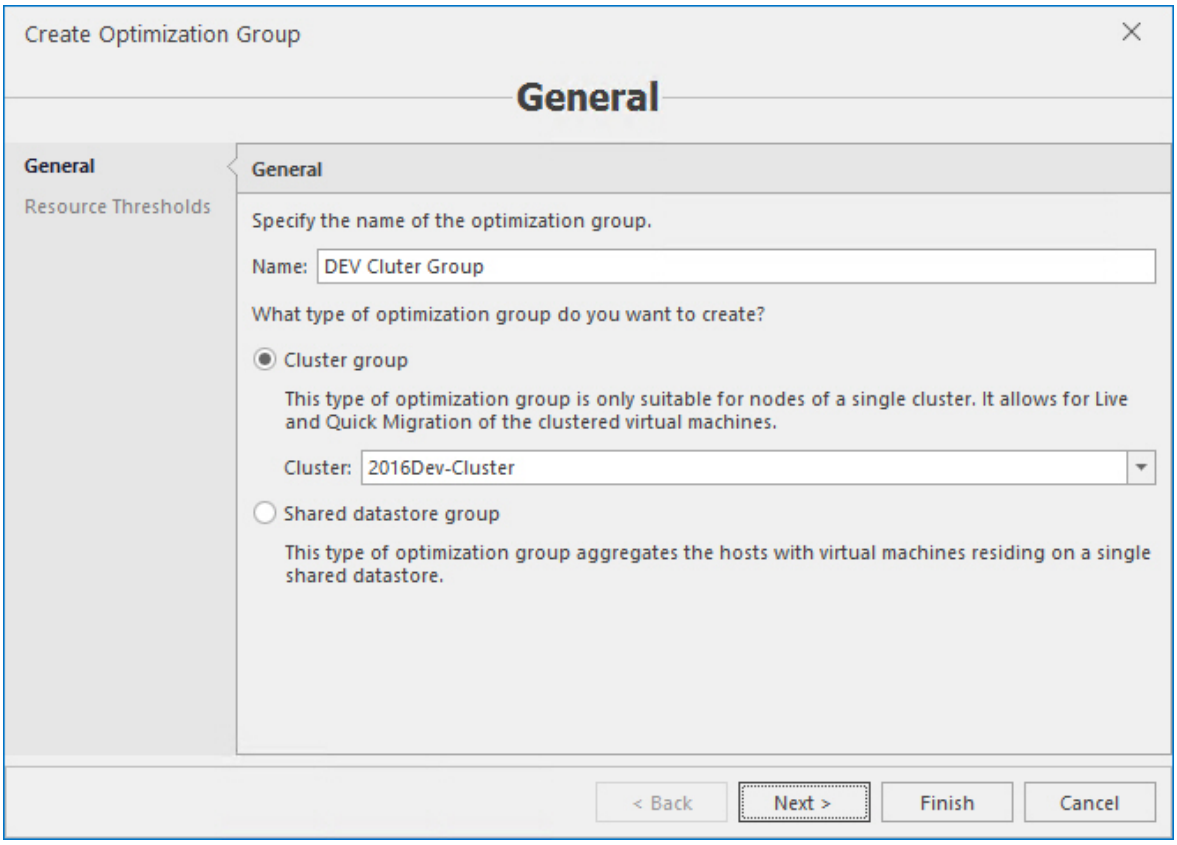
1. To configure optimizer, click the **Dynamic optimization** - **Configure optimizer** menu item on the main ribbon of the **Monitoring** plugin screen:



2. In the **Optimization groups** dialog window, you can add, edit and remove optimization groups.

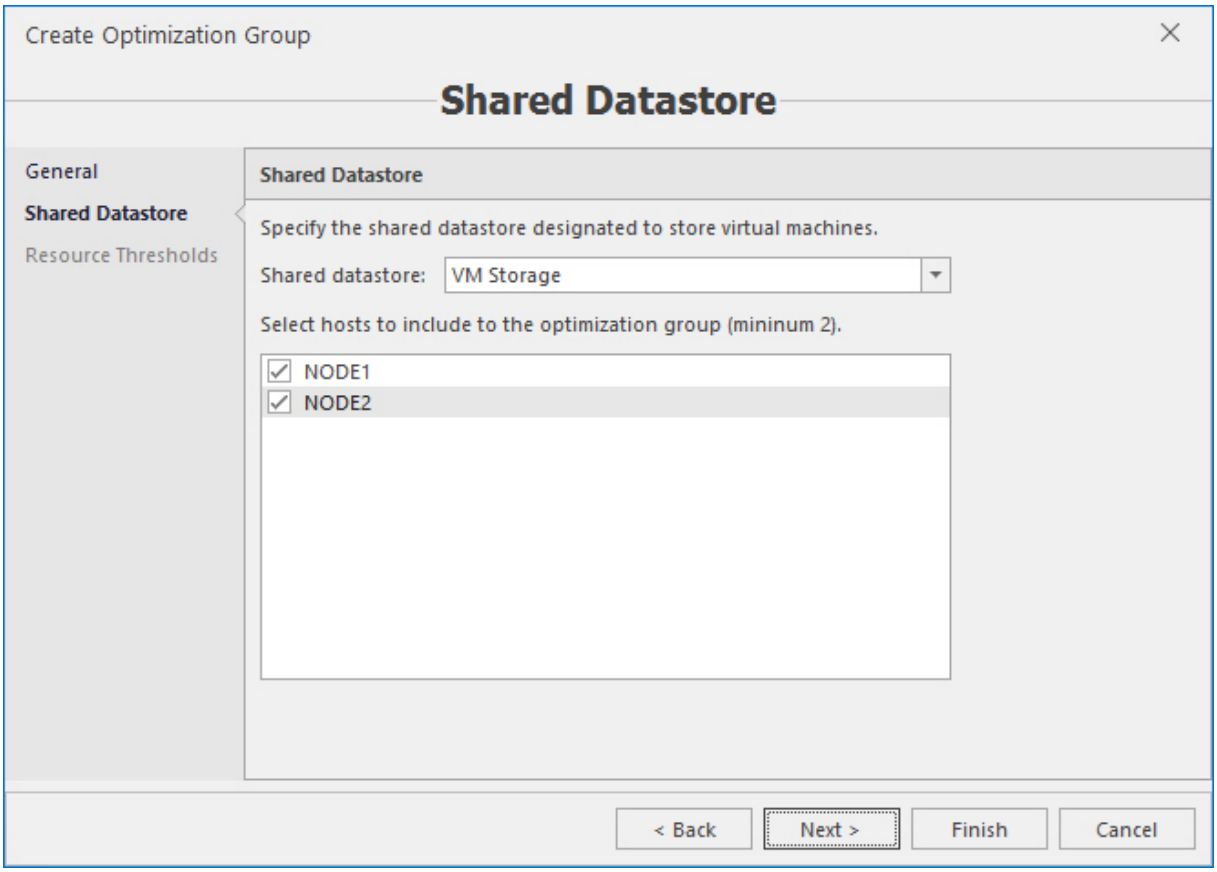


3. To add the new group, click **Add** to open the **Create optimization group** wizard.
4. Set the optimization group parameters: specify group name and choose the group type:

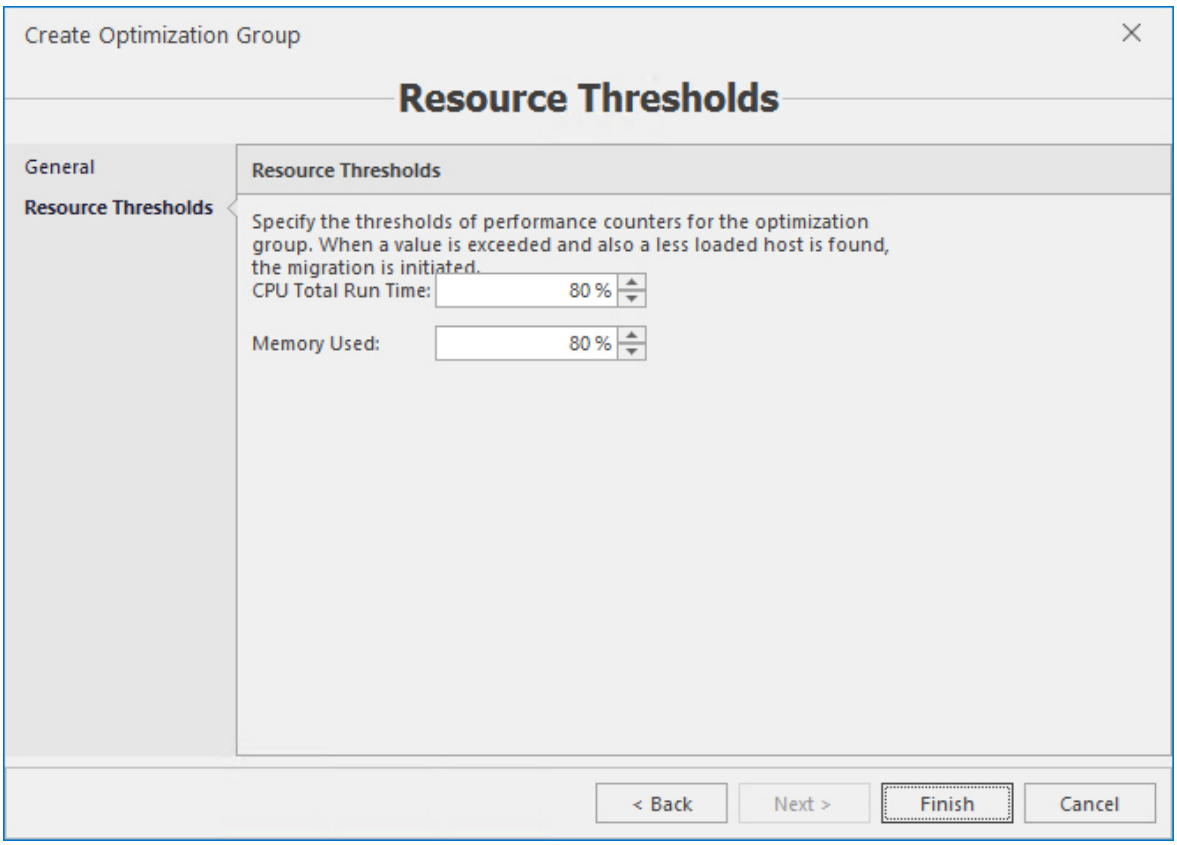


If the **Cluster group** type is selected, then choose the available cluster from the drop-down box.

If the **Shared datastore group** type is selected, then you will need to choose the datastore on the next screen:



5. Set the resource thresholds for Hyper-V server's CPU and memory consumption:



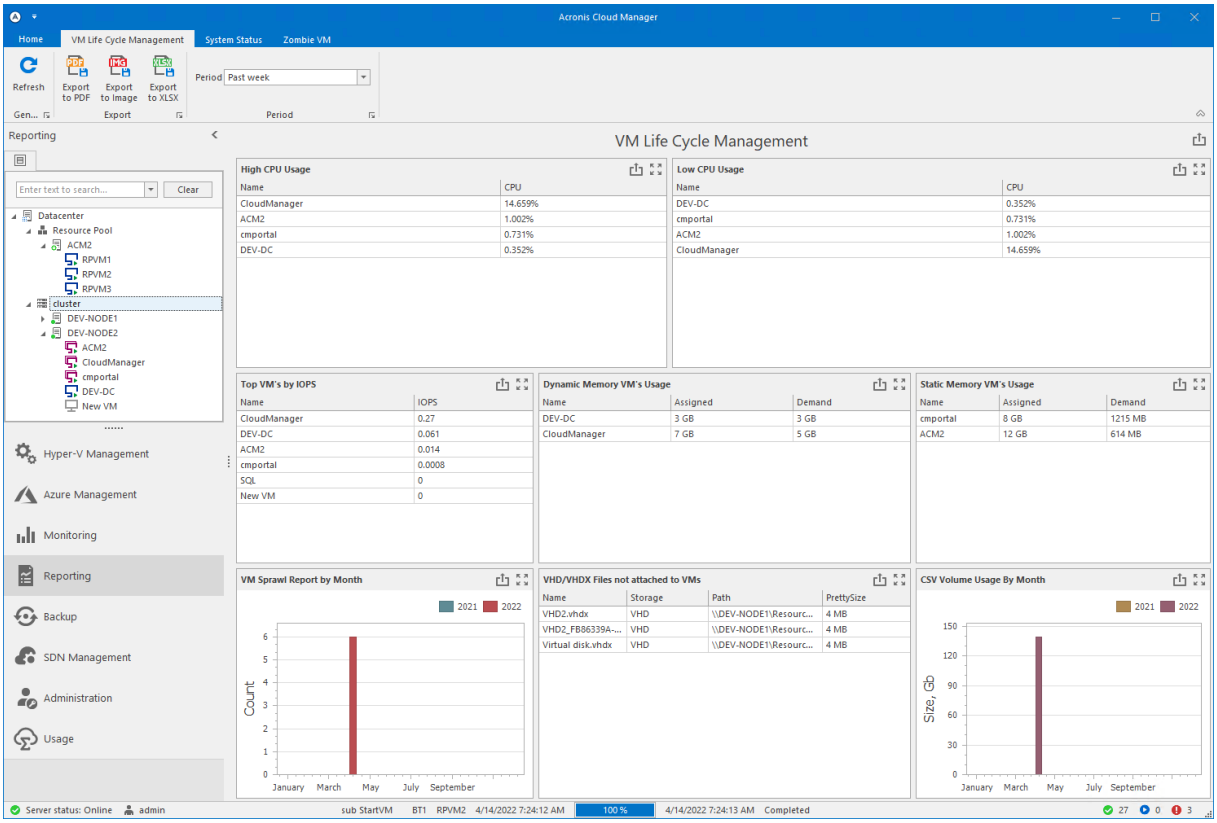
6. Click **Finish** when complete.
7. To choose automatic or manual optimizer mode, select the corresponding option in the **Dynamic optimization** menu on the main ribbon.
8. To run the optimizer once, click the **Run once** item in the **Dynamic optimization** menu on the main ribbon.

Reporting

The Acronis Cloud Manager **Reporting** plugin is designed to provide consolidated data about virtual machines. It consists of three tabs – **VM life cycle management**, **System status** and **Zombie VM**.

VM life cycle management

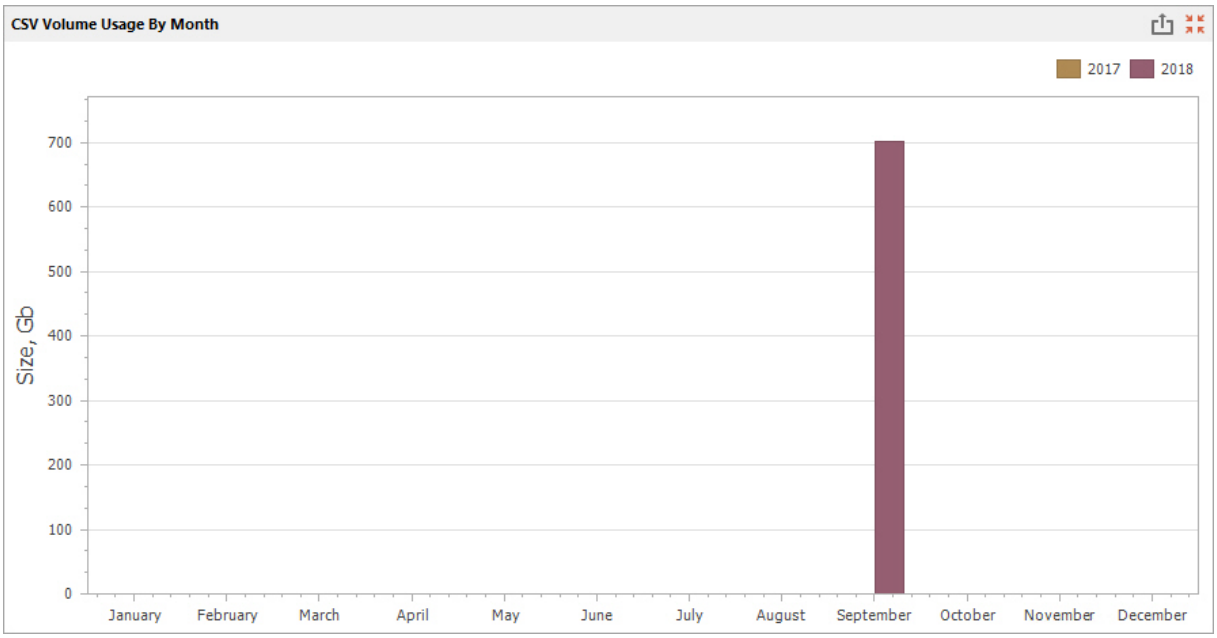
The **VM life cycle management** tab contains consolidated information about various resources utilization by virtual machines during the last week, last month or a period, specified by user.



The **VM life cycle management** tab represents the following data:

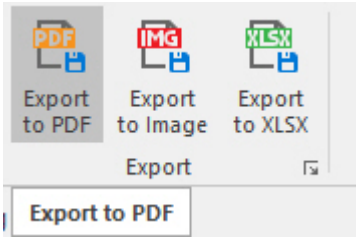
- High CPU usage;
- Low CPU usage;
- Top VMs by IOPS;
- Dynamic memory usage;
- Static memory usage;
- VM sprawl report;
- VHD/VHDX files not attached to VMs;
- CSV volume usage.

Each section can be maximized to the full window size:

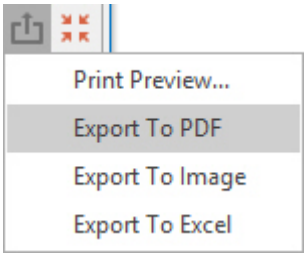


The whole report or just any single separate section (as needed) can be exported into different output formats – PDF file, PNG image, XLSX document or printed and print-previewed:

- By usage of the corresponding main ribbon buttons (for the whole report);

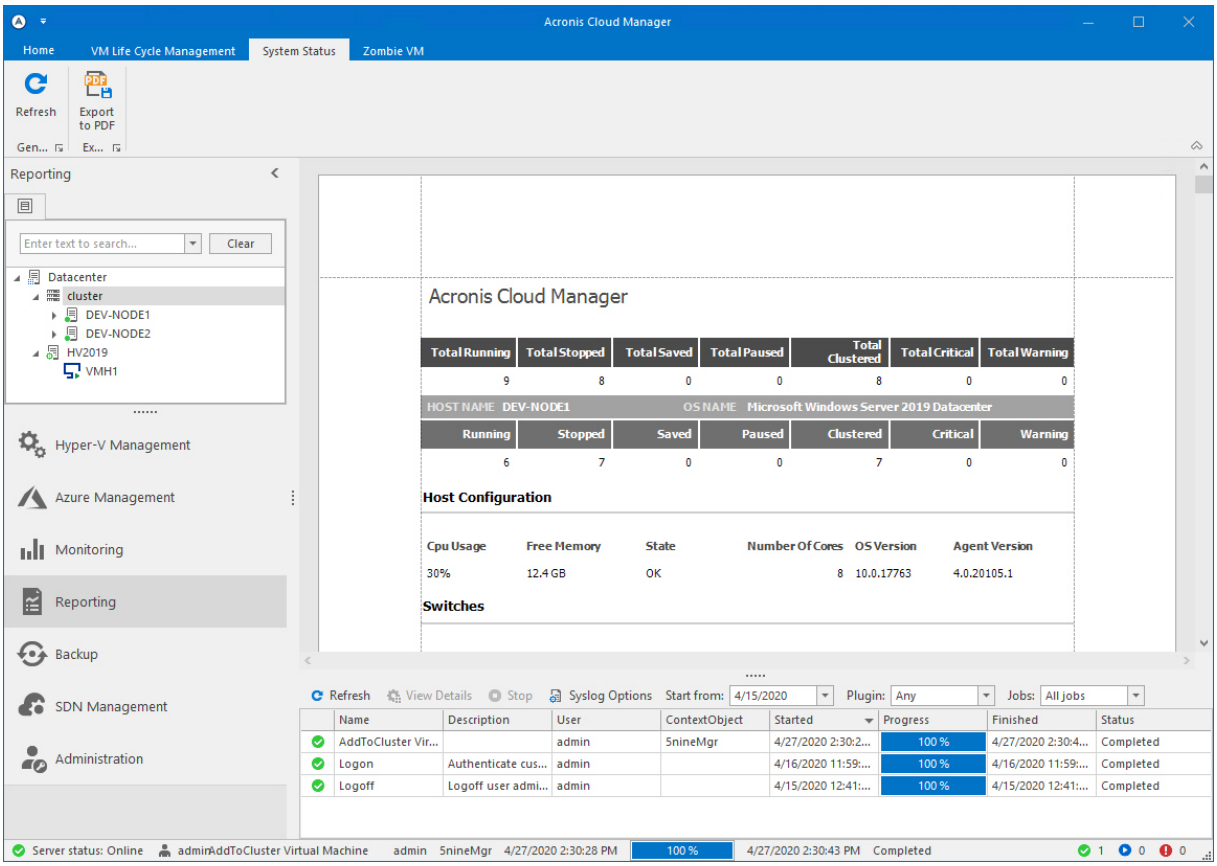


- By usage of the upper-right buttons for both whole report and a single section.

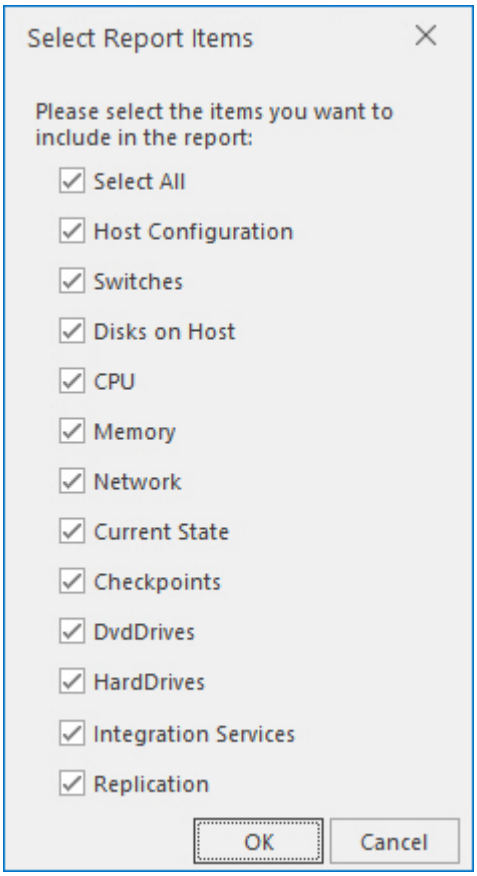


System status

The **System status** tab contains system status report in the table view. There are different parameters of Hyper-V hosts and virtual machines configuration – CPU, memory, physical/virtual disks, checkpoints and replication data.



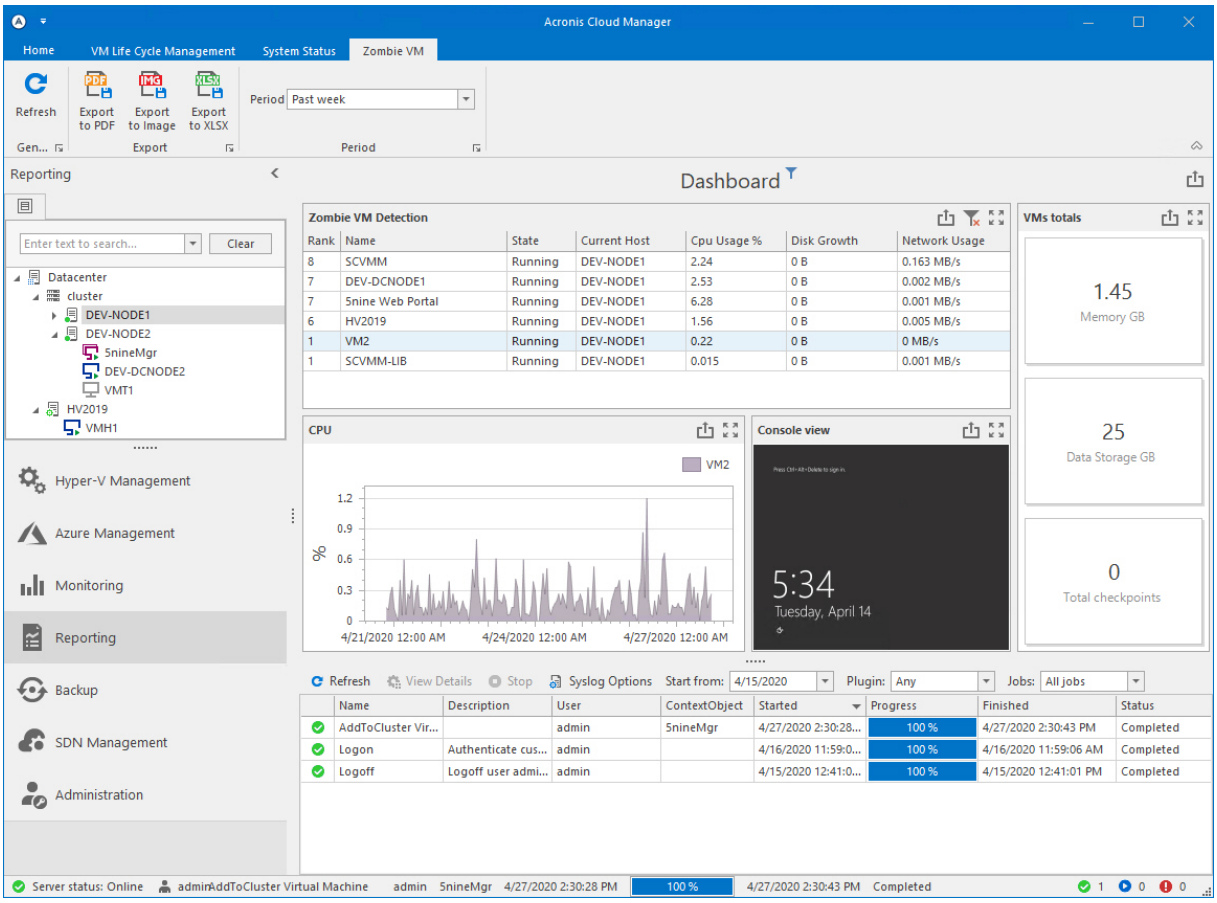
To generate system status report, after opening the System Status tab, click the Refresh button on the main ribbon and then select sections to show in the report:



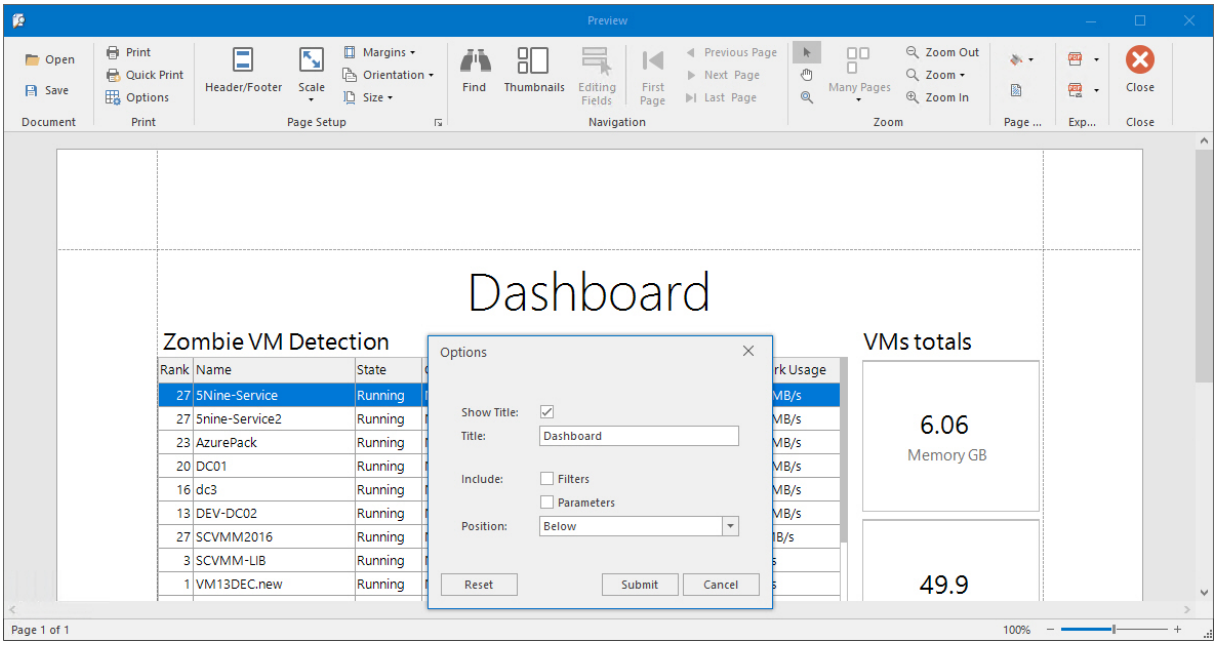
To export the report to pdf file, click “Export to PDF” button on the main ribbon.

Zombie VM

The **Zombie VM** tab displays all VMs by rank to identify VMs with very low CPU usage, network performance and virtual disk growth.

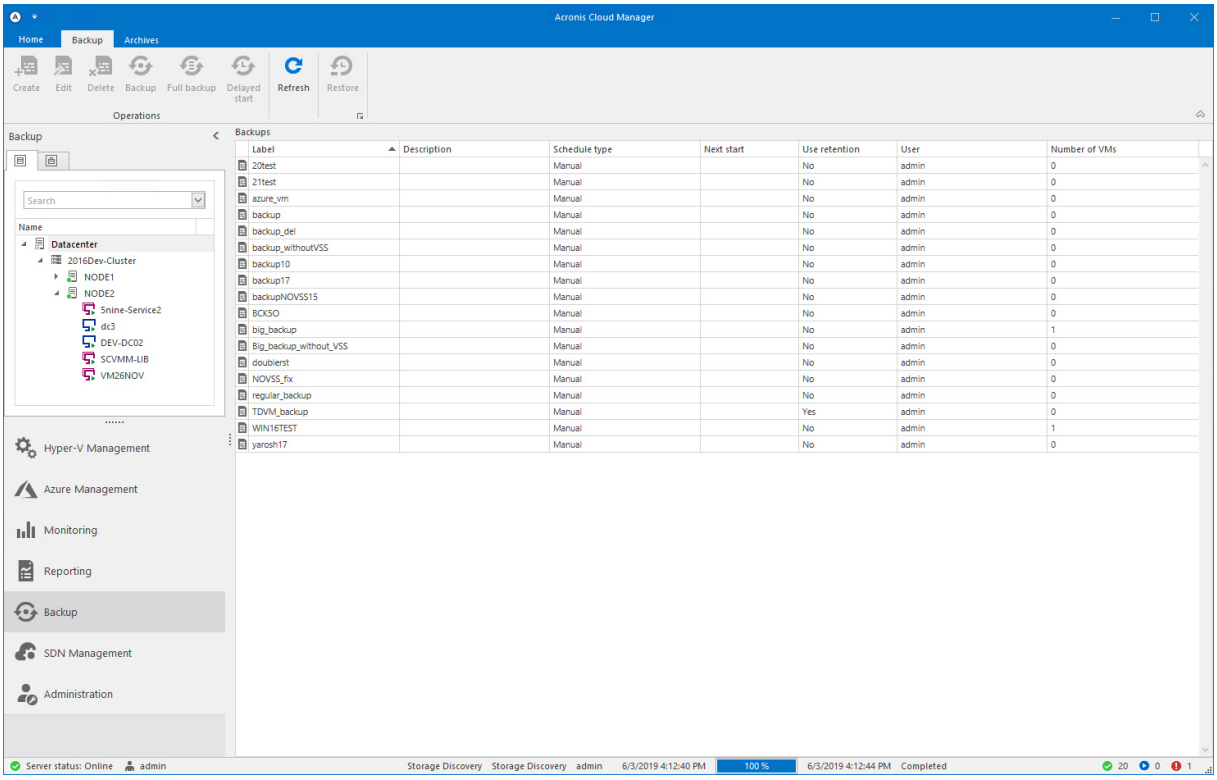


Any section can be exported into different output formats – PDF file, PNG image or XLSX document. Use the corresponding buttons on the main ribbon or the subsequent upper-right commands on each block. They also can be printed and print-previewed:



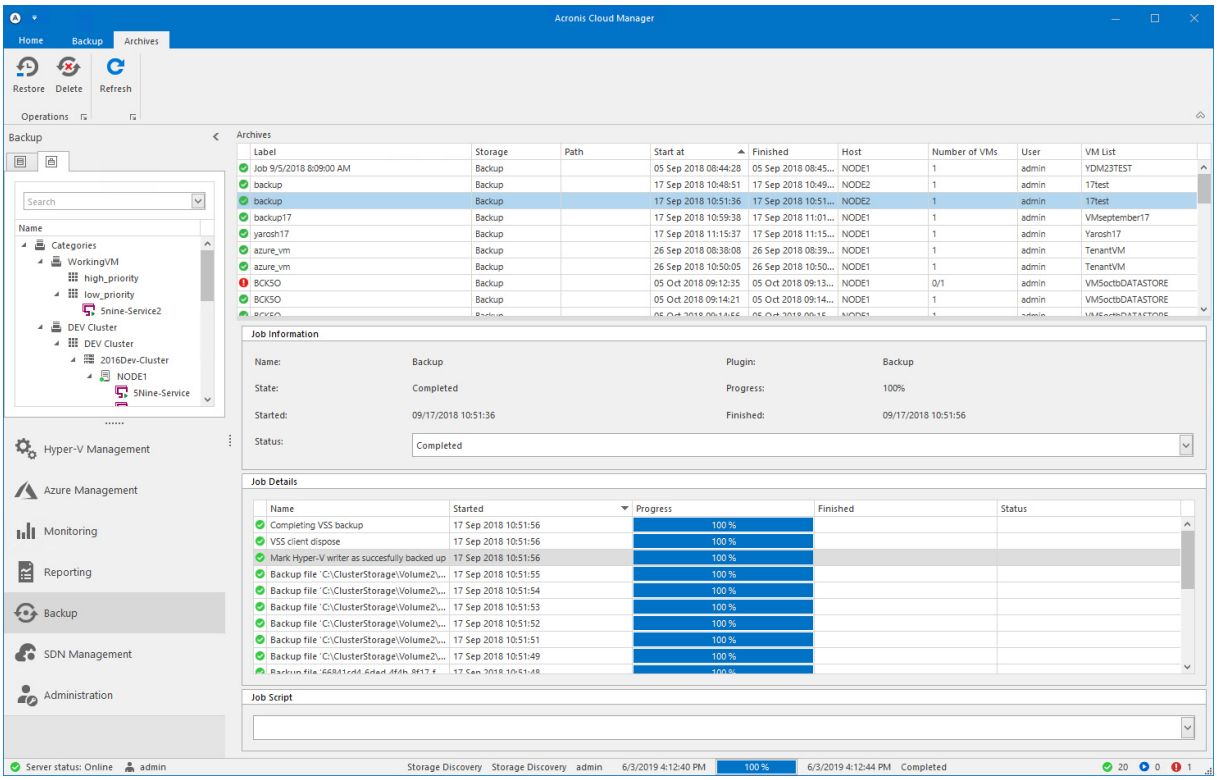
Hyper-V backup and restore

The Acronis Cloud Manager **Backup** plugin performs the entire VM backup on-demand immediately, with specified delay or by schedule. All backup jobs are started from job templates initially created by the user from the backup wizard. Job templates are kept for further usage, and the new jobs can be launched from them manually at any time. Recurrent and deferred backup jobs are launched automatically in accordance with the schedule configured in their job templates. The new WMI-based approach is implemented in the VM backup plugin - switched to Hyper-V RCT API from VSS volume snapshot (legacy), leaving the option to use the old approach for backward compatibility.
There is an option to perform the offsite backup copy to Microsoft Azure cloud and restore from it.



The **Backup** plugin consists of two tabs: **Backup** and **Archives**. On the **Backup** tab there are list of backup job templates and commands to work with them – create, delete, edit, start (full, incremental, delayed).

On the **Archives** tab there are list of backup jobs that are started, in progress and completed (both successful and failed ones) and commands to work with them – restore, delete, view job info.



There are different backup job types:

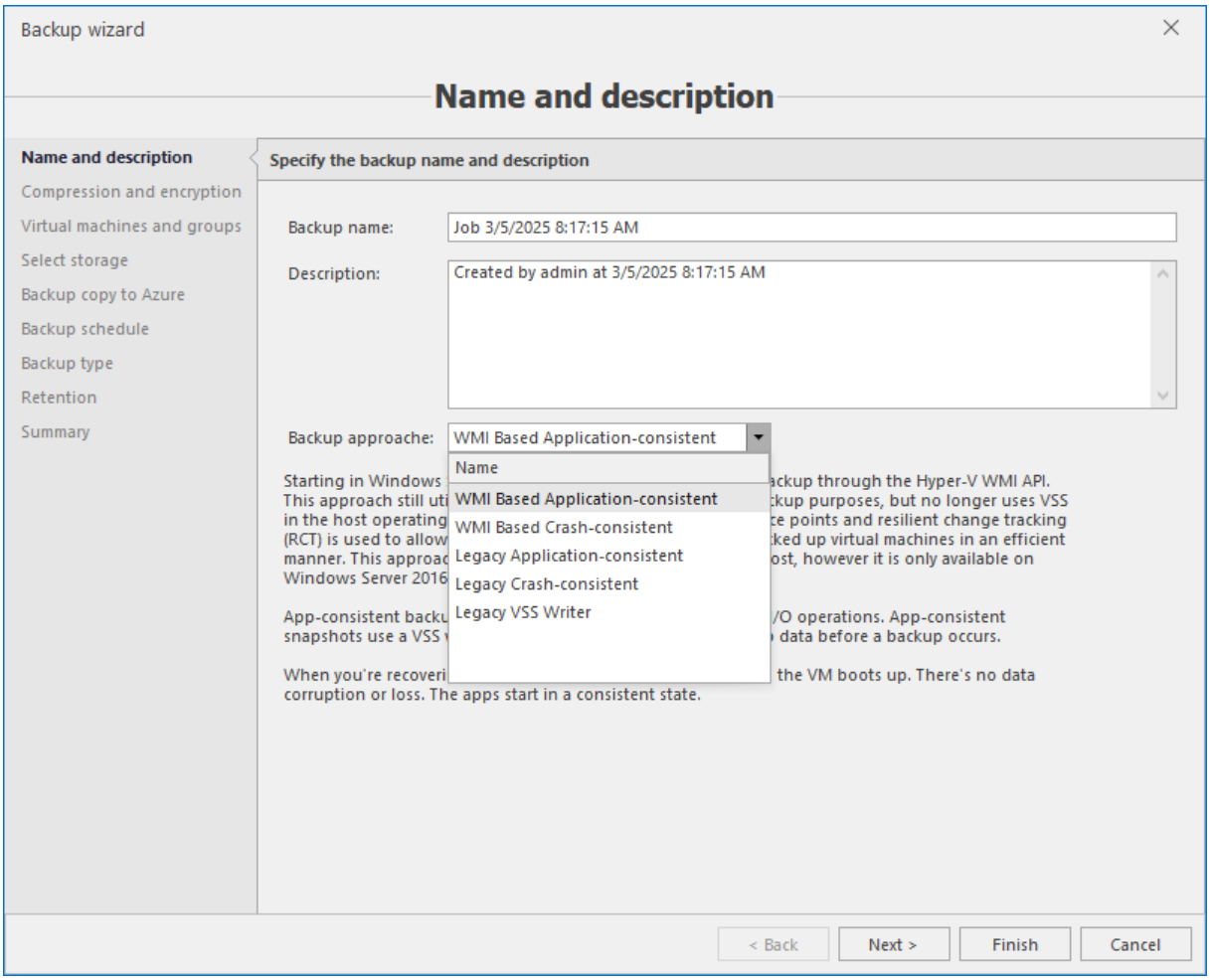
- *Full* – always performs the entire VM backup.
- *Incremental* – performs only first entire VM backup, then saves only changed virtual disks parts in subsequent backups. Normally, the scheduled jobs are used for incremental backup that allows additional saving of a storage disk space and ensure safety of data.

  To keep track of changing data blocks, Acronis Cloud Manager backup uses changed block tracking technology (CBT) for Hyper-V virtual disks (A)VHD(X).

The CBT is implemented as a file system filter driver to be installed on every Hyper-V host within Acronis Cloud Manager agent setup. The CBT driver keeps track of changed data blocks of virtual disks. Information on data blocks that have changed is registered in special files. When an incremental job is run, Acronis Cloud Manager uses these files to understand what blocks of data have changed since the last run of this incremental job, and copies only changed data blocks from the disk image.

Creating a backup job

1. To create a VM backup job, start the backup wizard by clicking **Create**. Specify the name of the backup job and provide the job description.

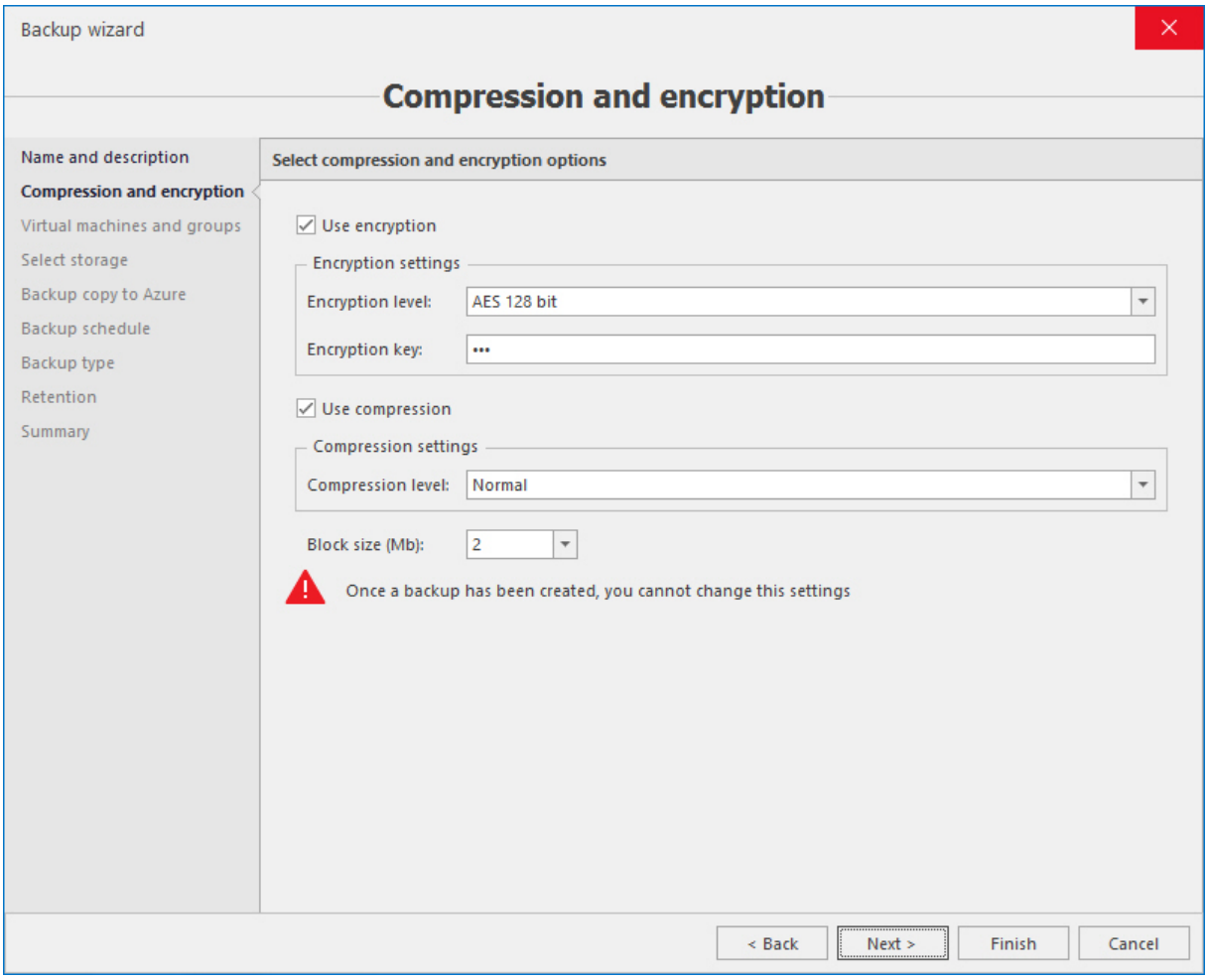


2. Select the approach option:
   - **WMI based application-consistent** - for Windows Server 2016 and later versions to use Hyper-V WMI API approach for backup instead of VSS. This approach still uses VSS inside the guest operating system, but does not use it in the host OS. Application-consistent backups capture memory content and pending I/O operations. Application-consistent snapshots use a VSS writer inside a guest OS to ensure the consistency of the application data before a backup occurs. There will be no data corruption or loss upon recovery, and the applications will start in a consistent state.
   - **WMI based crash-consistent** - for Windows Server 2016 and later versions to use Hyper-V WMI API approach for backup instead of VSS. Crash-consistent snapshots only capture the data that already exists on the disk at the time of the backup operation. Data in read/write host cache is not captured. When the recovery occurs, the disk is checked for corruption errors in order to fix them, and any data stored in memory or write operations that were not transferred to the disk before the crash are lost. Applications may implement their own data verification independently.
   - **Legacy application-consistent** - this option bypasses VSS writer in the host OS, and exists for backward compatibility to run application-consistent backups using the old approach.
   - **Legacy crash-consistent** - this option bypasses VSS writer in the host OS, and exists for backward compatibility to run crash-consistent backups using the old approach.

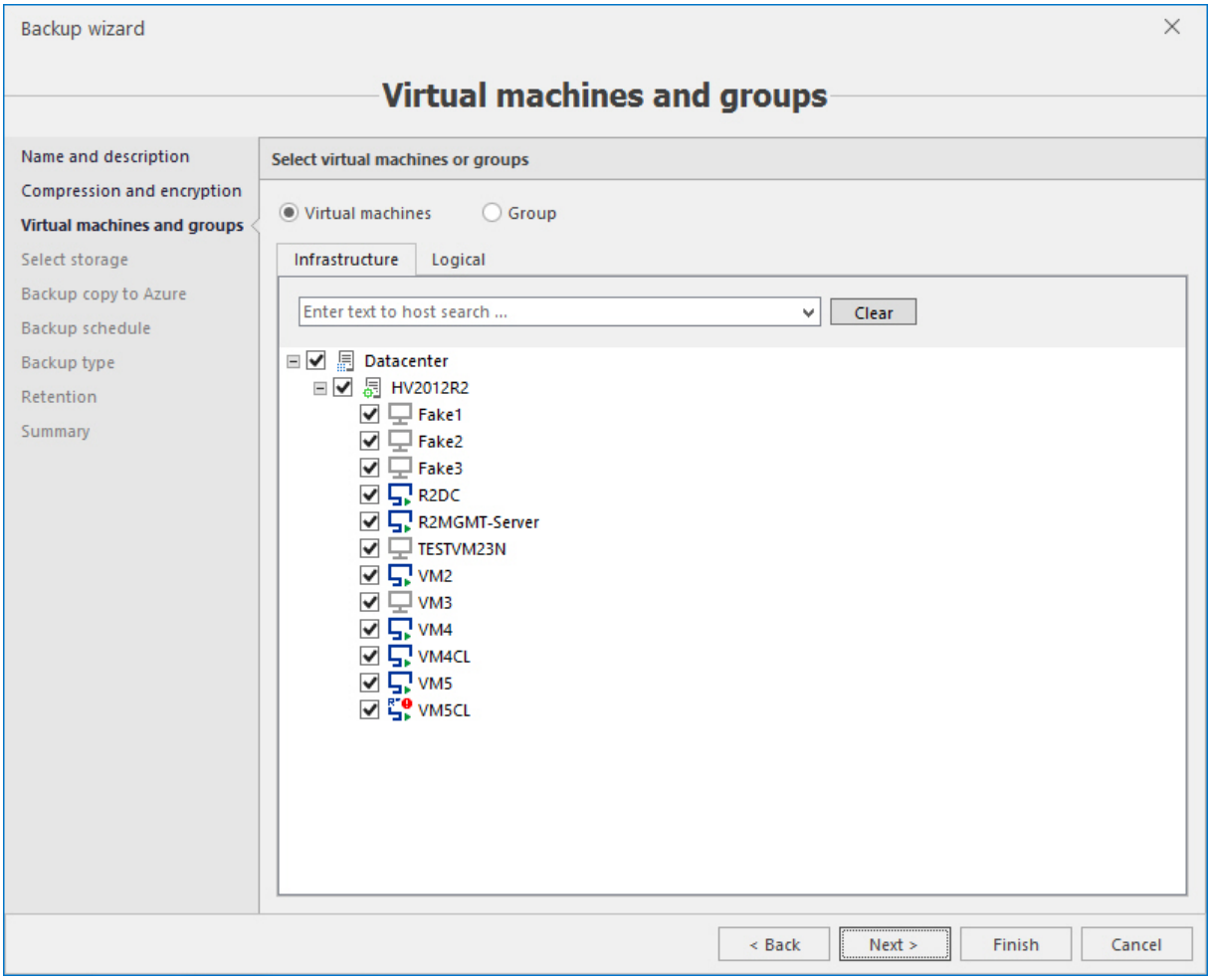
- **Legacy VSS-writer** - this is the classic backup option, available on all versions of Windows Server that support Hyper-V and exists for backward compatibility.

Click **Next**.

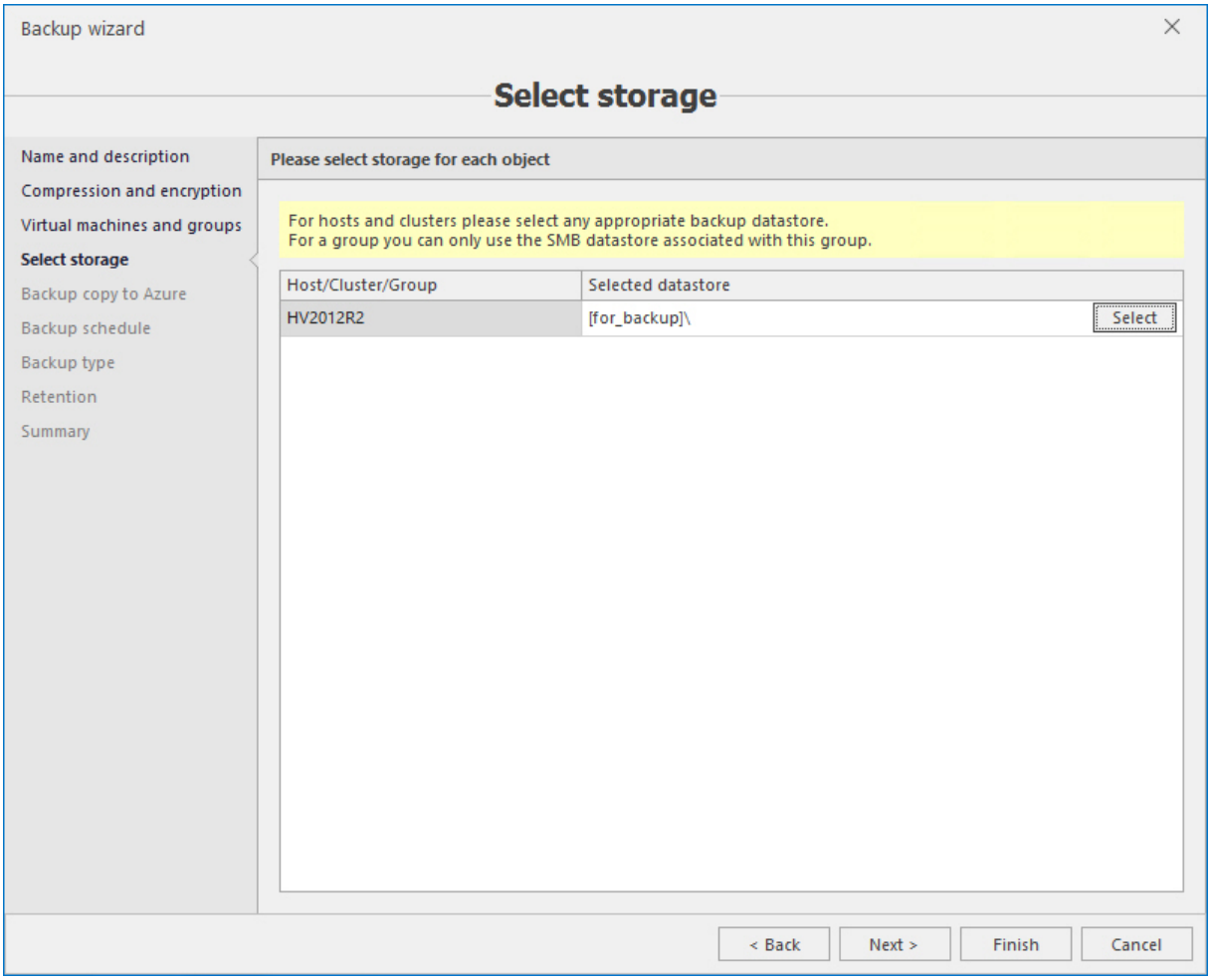
2. Define compression and encryption options.



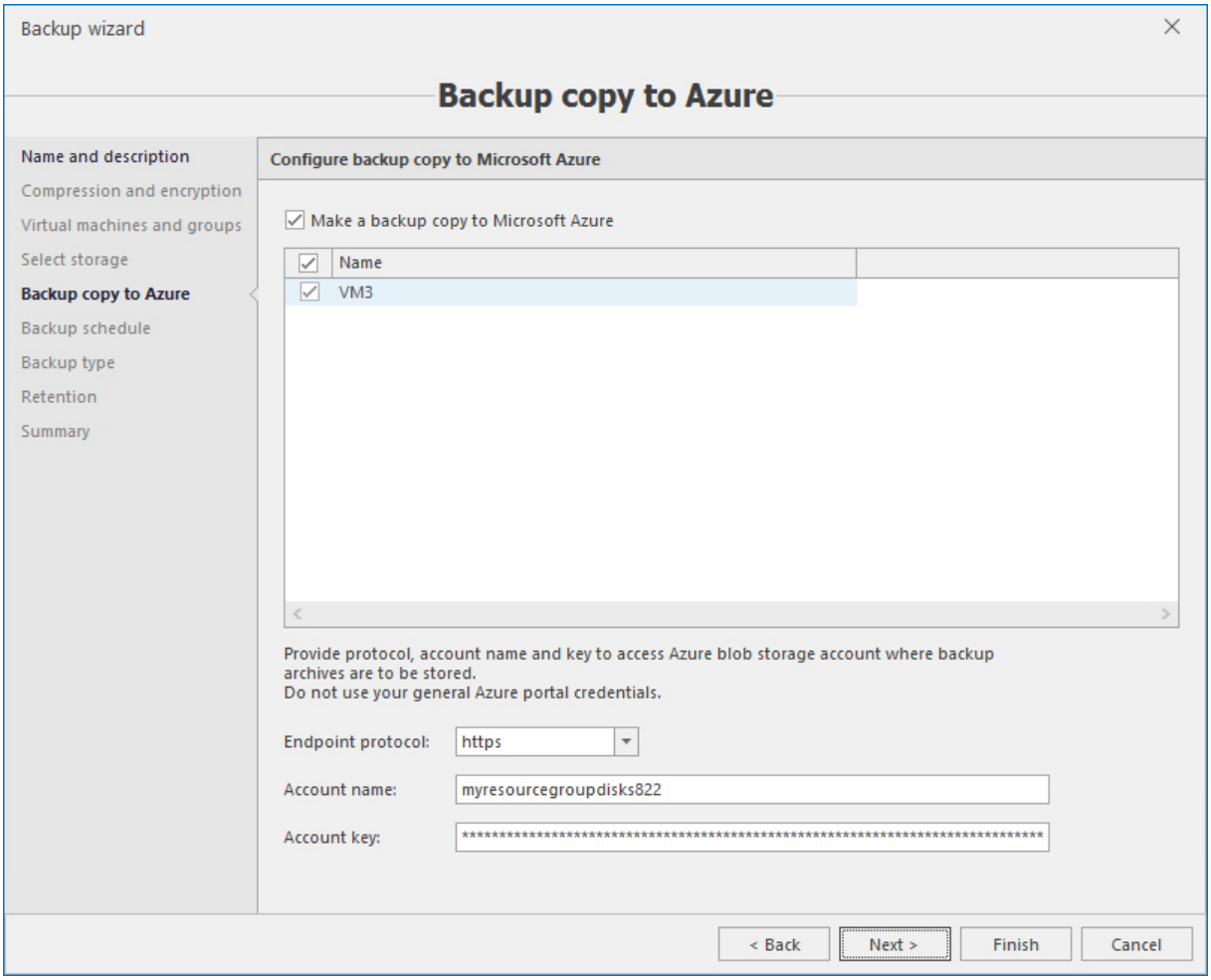
3. Select virtual machines or groups to be placed into backup job.



4. Select the storage and folder for each VM Hyper-V host where backup files will be placed.



5. Specify parameters to create an offsite backup copy to Microsoft Azure cloud, if necessary (skip this screen if an offsite backup copy to Microsoft Azure is not needed):

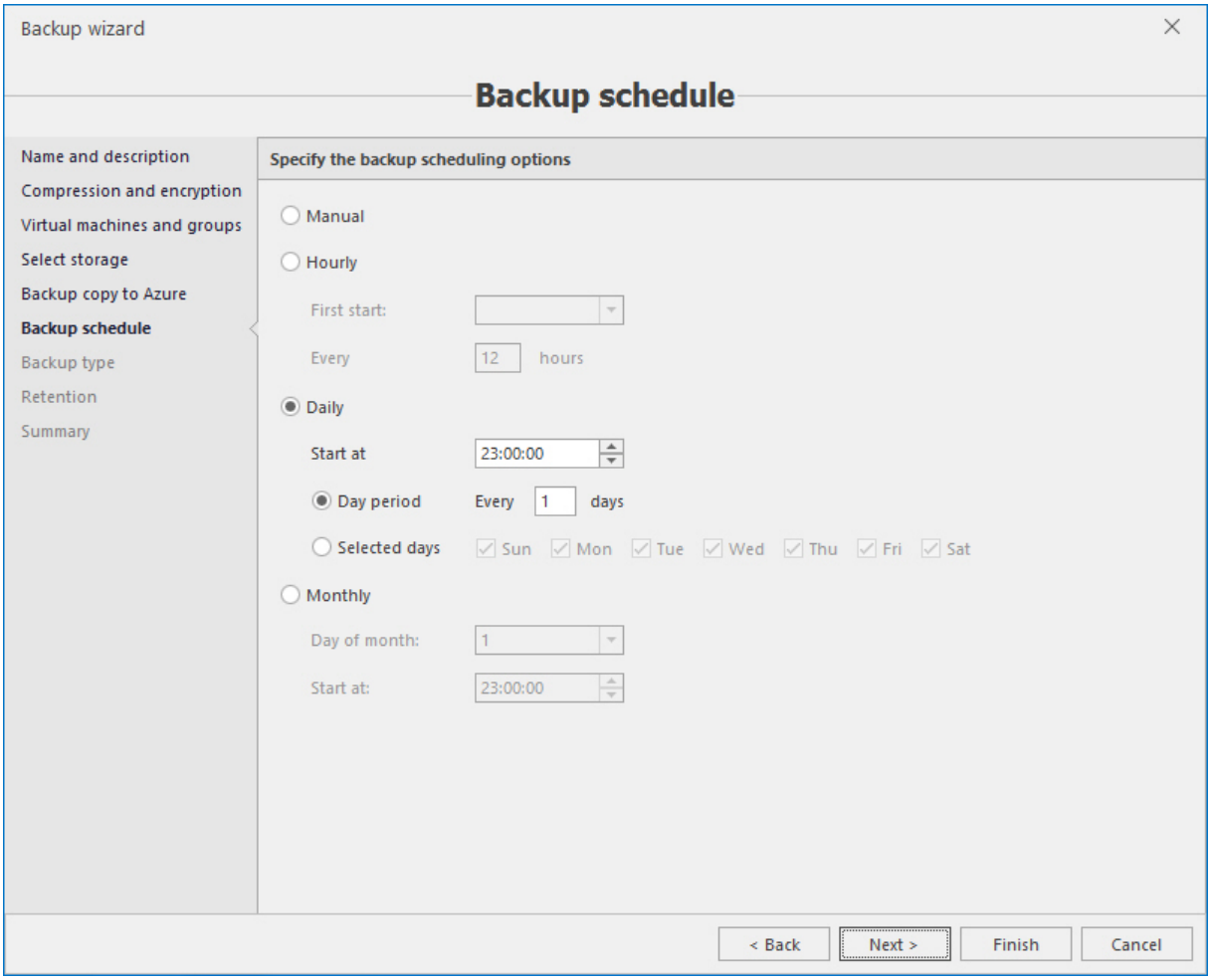


- Enable the checkbox for **Make a backup copy to Microsoft Azure** option.
- Select VMs to make backup copy to Microsoft Azure from the list of selected VMs into the backup job.
- Select endpoint protocol (http or https) and specify the storage account name and access key to access Microsoft Azure cloud.

Note

Storage account name and access key are different from your general Azure portal credentials, which will not be accepted! The proper parameters can be retrieved at the following address on the portal: **Home -> Storage accounts -> <your_storage_account_name> -> Access keys**. You may generate the new key (s) for the existing storage account in there and/or create the new storage account(s).

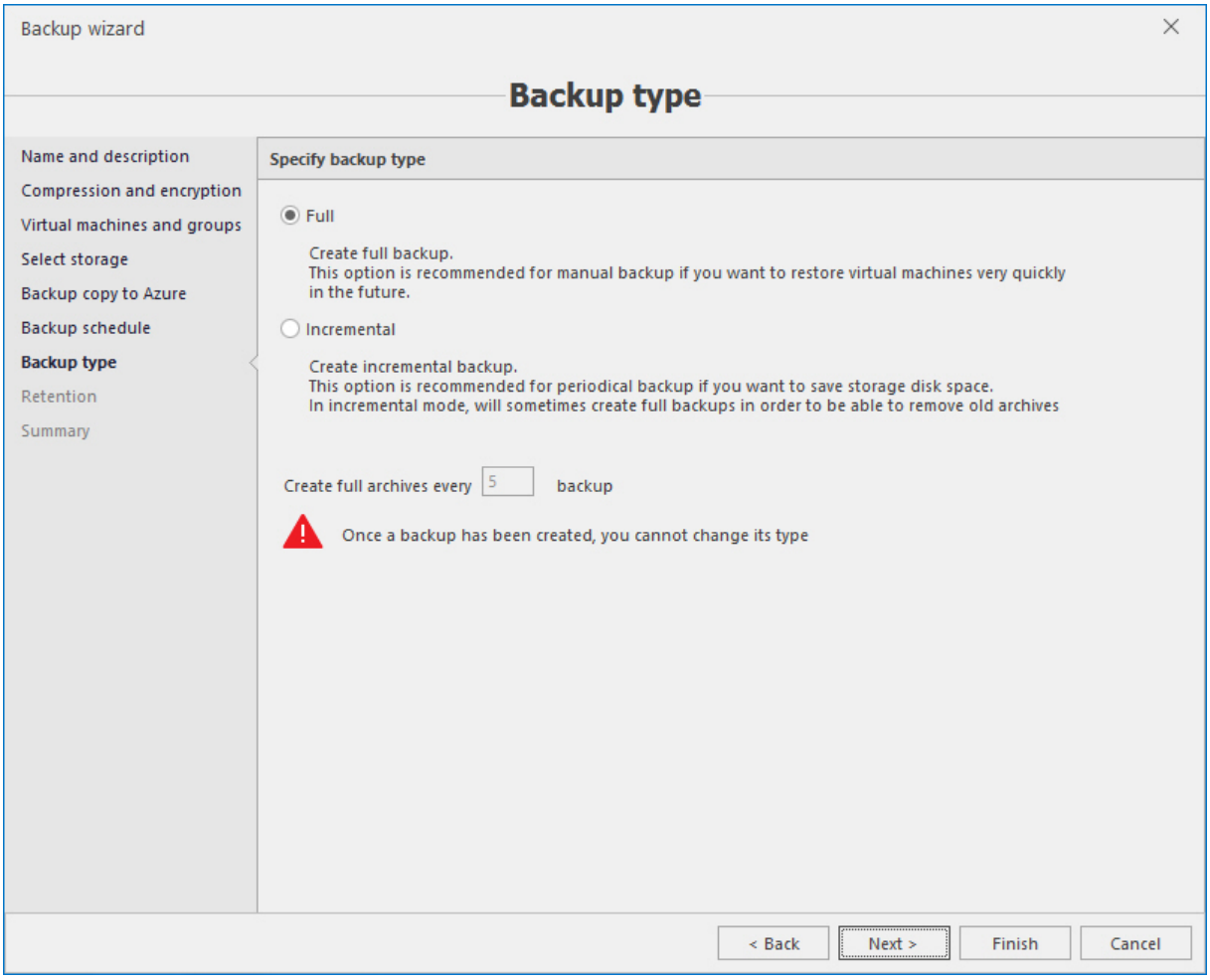
6. Configure backup job schedule:



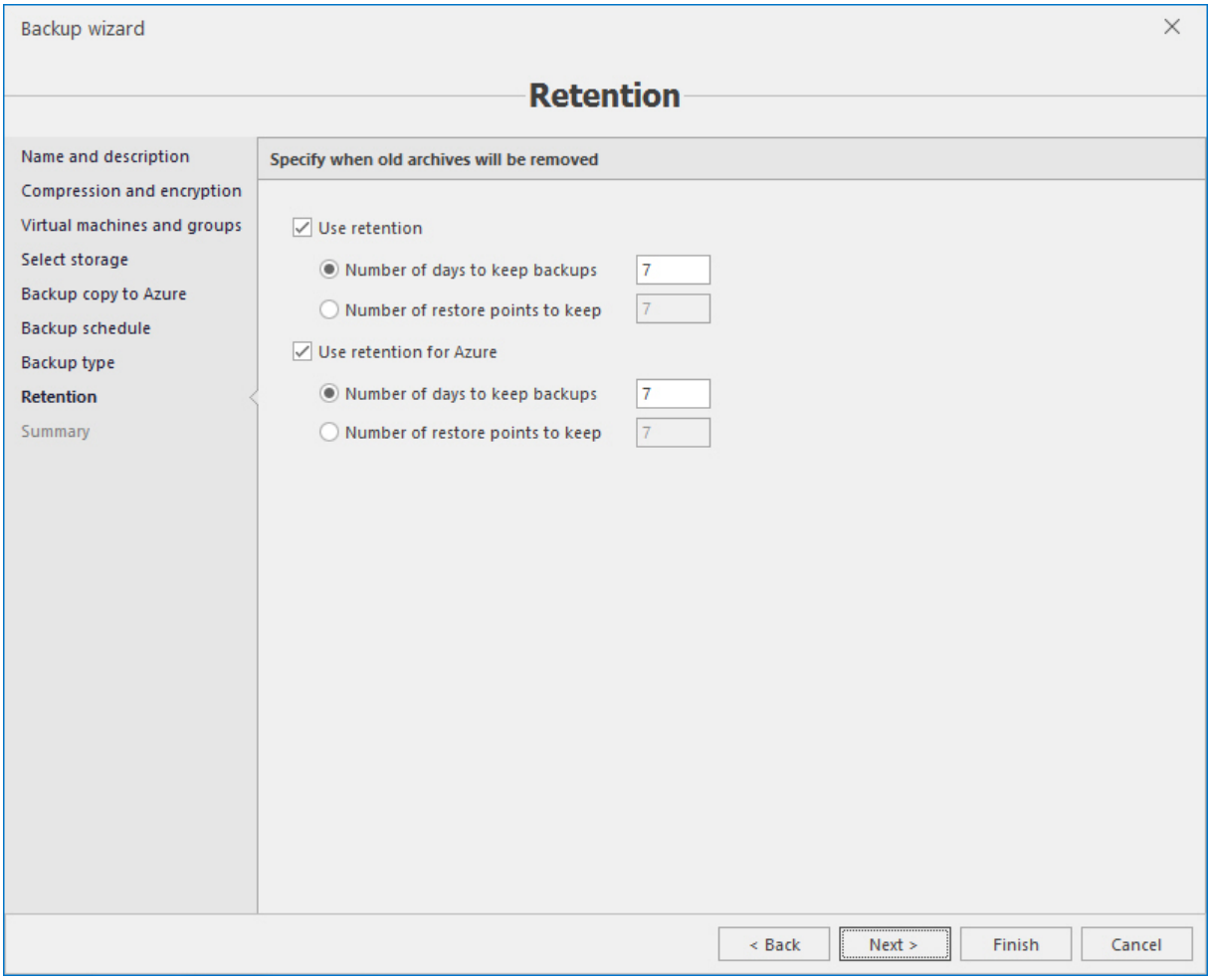
7. Select the backup job type.
   For incremental backup job you can determine the frequency of performing full backup job between incremental backup jobs.

Note

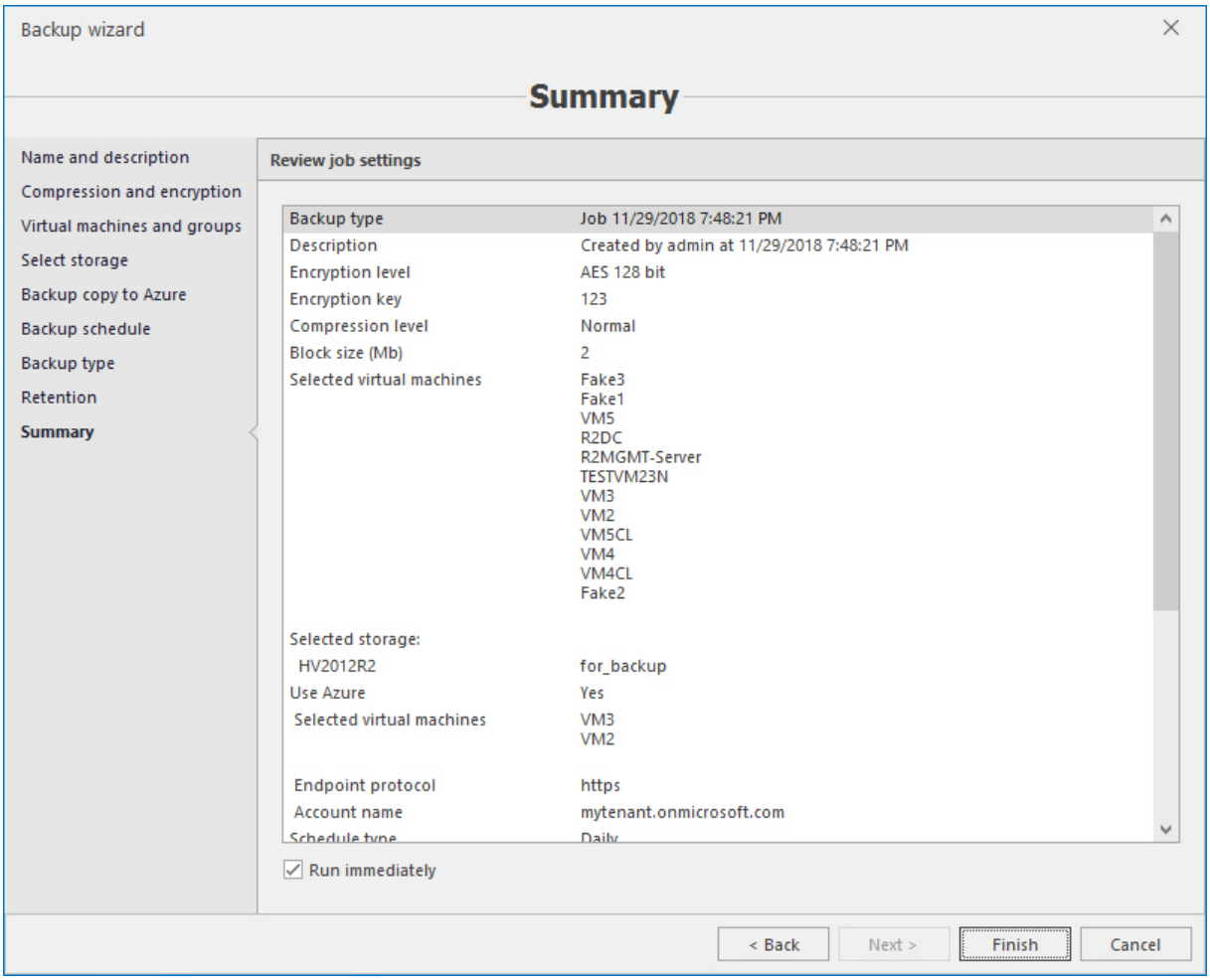
Cloud Manager does not allow to leave at “0”, some value must be configured for full backups. The number of incremental backups to perform before doing a full backup should balance between ease of restoration jobs due to the number of backup archives files and the speed of performing backups. This will vary widely between environments based on the frequency of backups and the rate of changes between them.



8. Review and set the retention parameters if necessary. It is disabled by default.



9. Check the summary information and if everything is correct. Check the **Run immediately** box if you need to launch the backup job right upon completing the backup wizard. Press the **Finish** button to create a backup job.

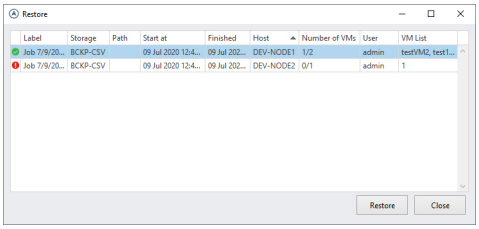


Restore

To restore a VM from backup, perform the following actions:

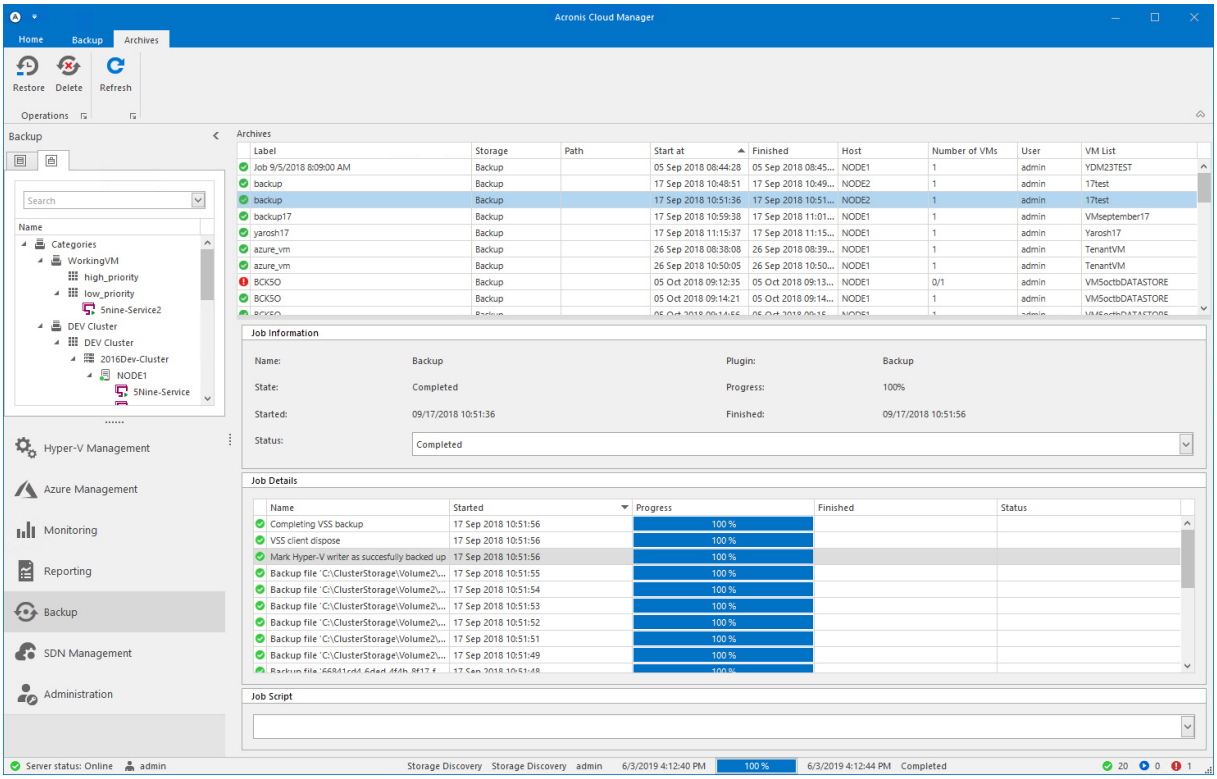
1. Select appropriate completed backup job on the **Backup** or **Archives** tab and start the **Restore** wizard by pressing the **Restore** button.

If you have chosen the job on the **Backup** tab, first the following dialog window will be opened:



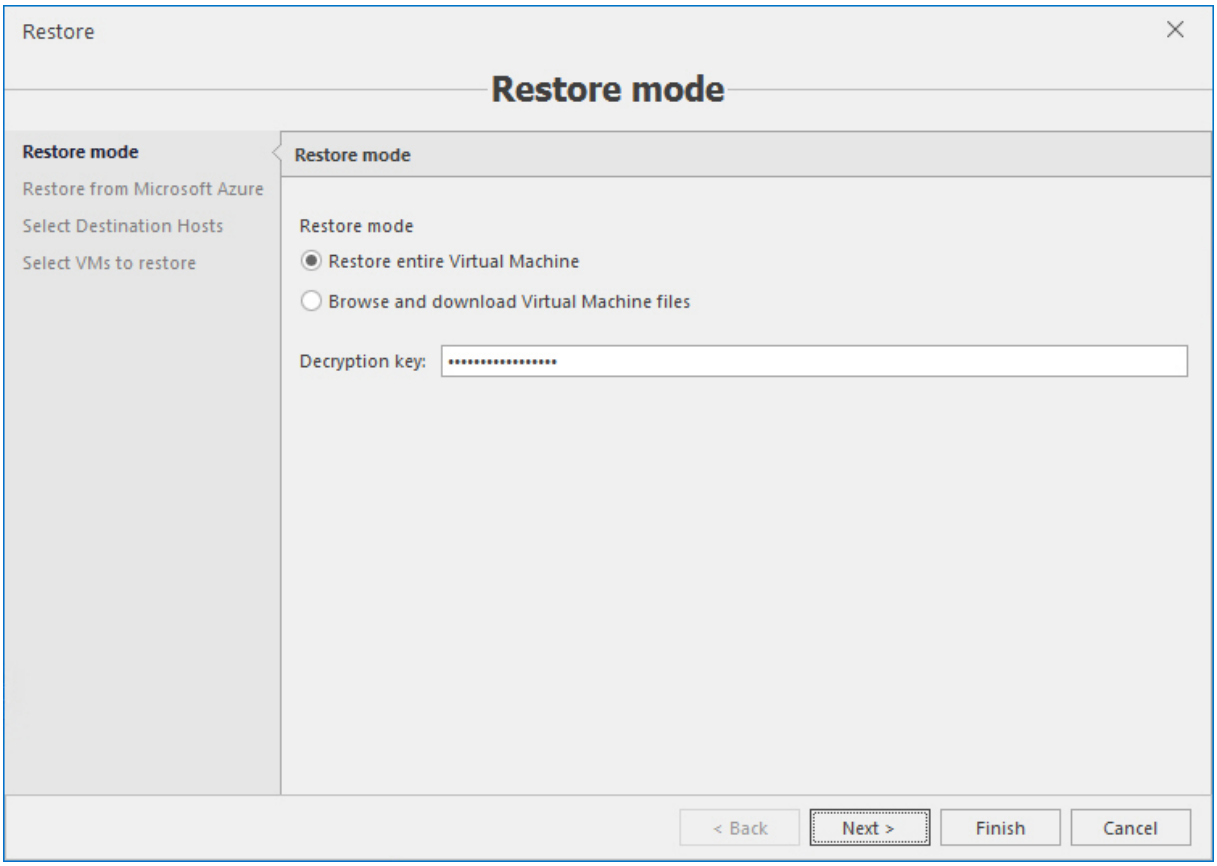
Select the required archive and click **Restore**.

If you are on the **Archives** tab, select the required archive form the list of archives and then click the **Restore** button on the main ribbon:

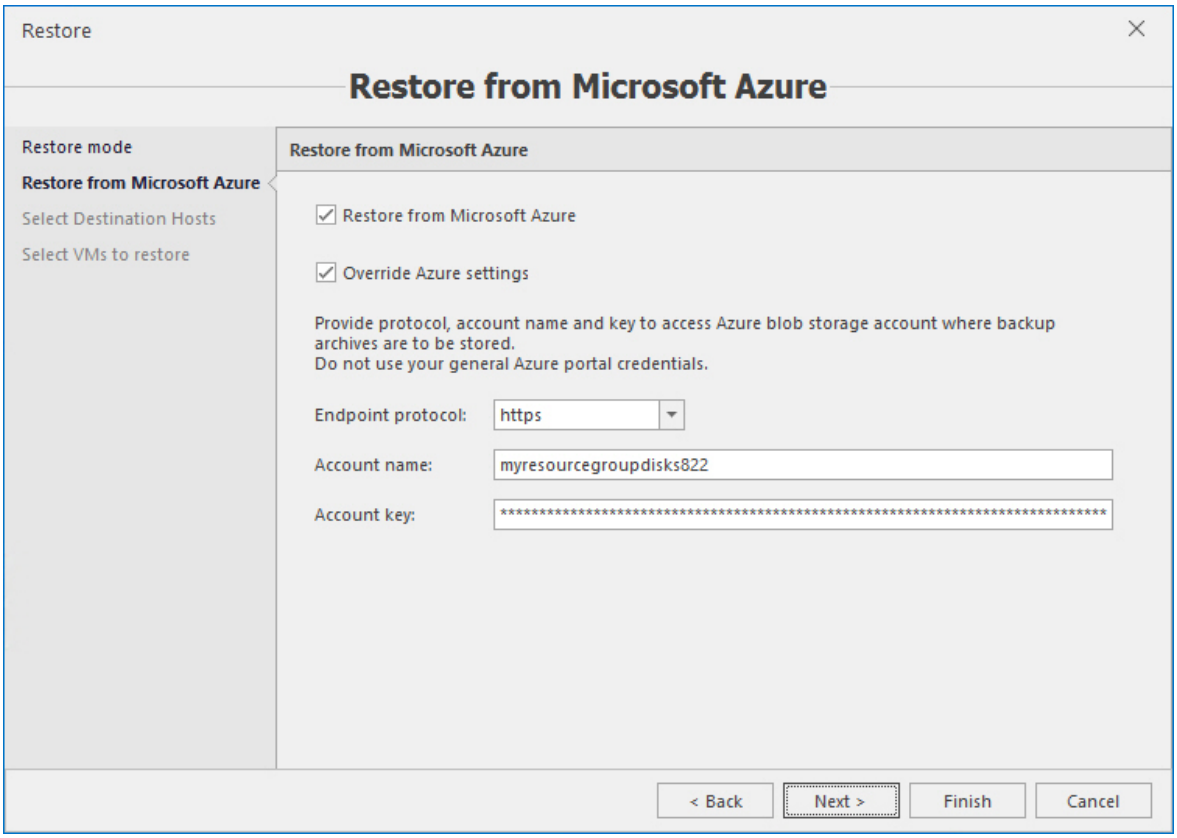


2. Select the restore mode:
   - **Restore entire virtual machine** – to restore the full copy of the VM.
   - **Browse and download virtual machine files** – to select and download the separate files from within the archived VM.

Specify the decryption key if encryption was used in the backup creation. If the decryption key was not specified, the field **Decryption key** will not appear. Click **Next**.

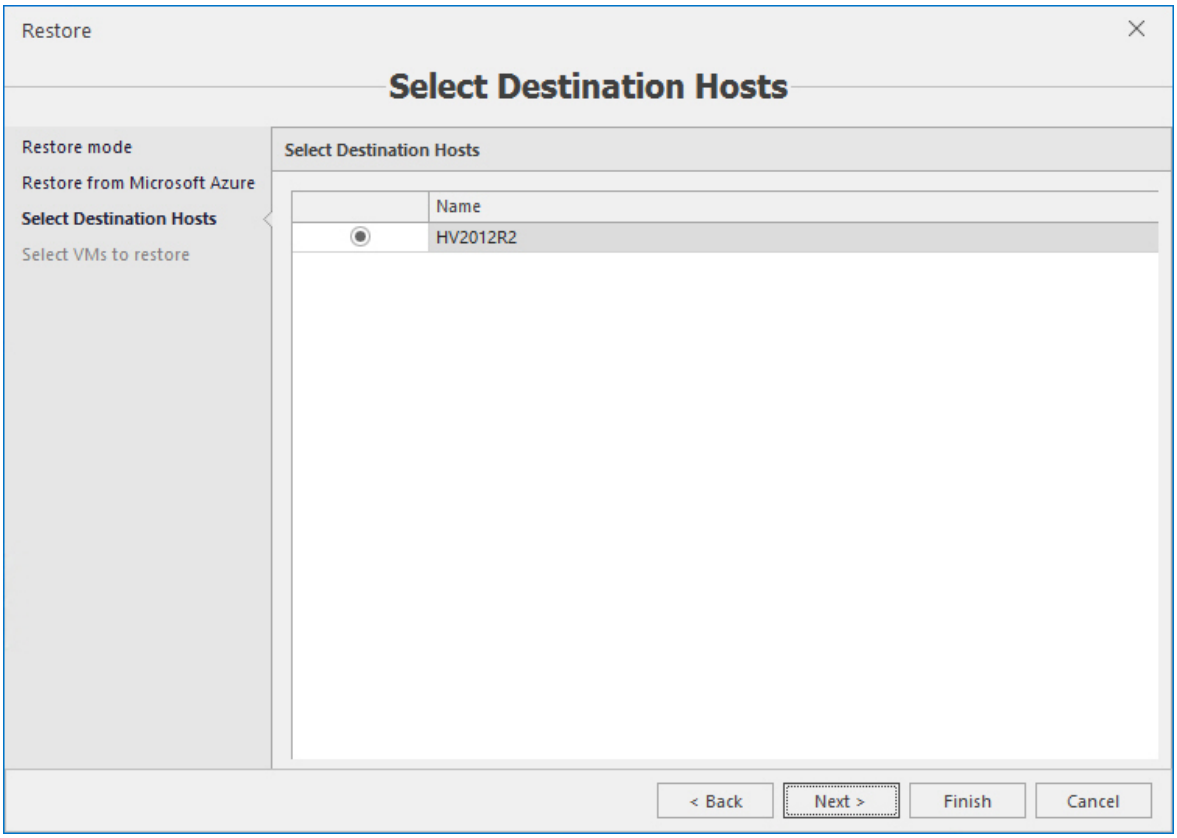


3. [Optional] The next page will appear only if in the corresponding backup job the **Make a backup copy to Microsoft Azure** option was enabled and on the first page of the **Restore** wizard the **Restore entire Virtual Machine** option was selected.

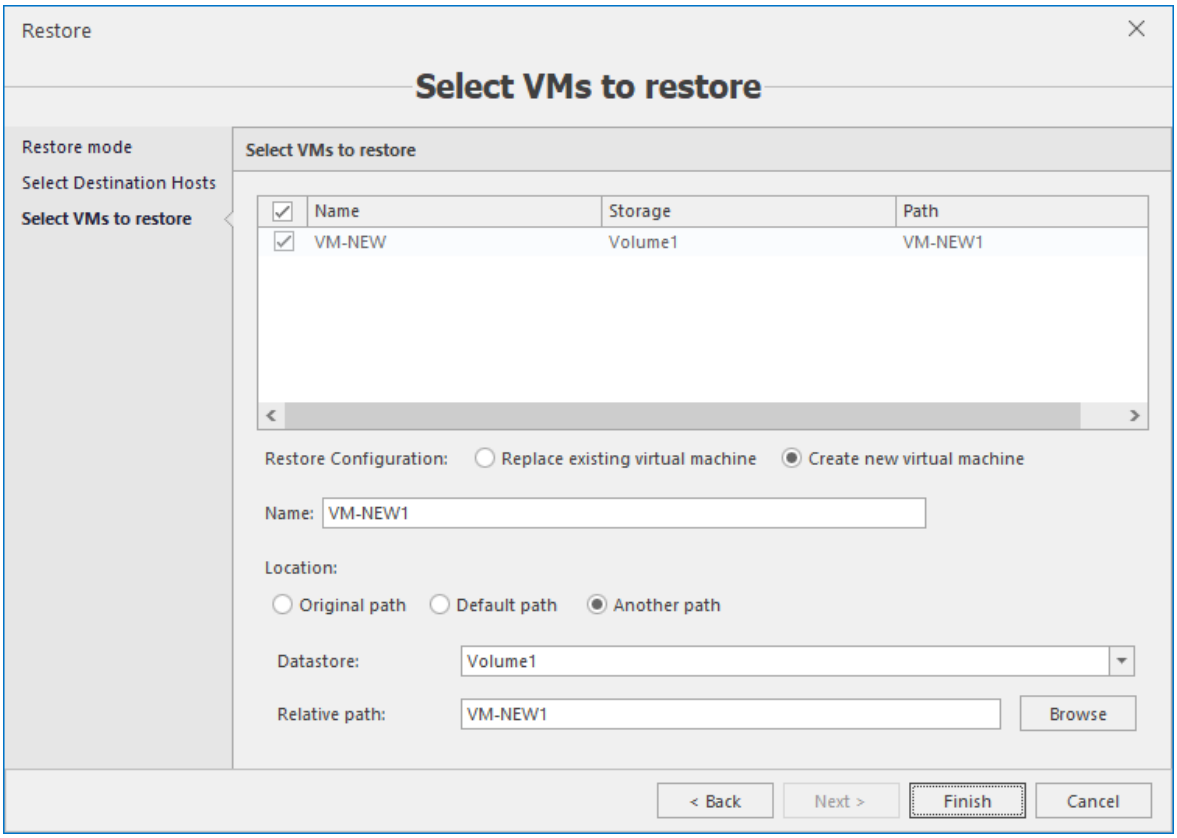


This step is optional and can be skipped. If you do not need to restore the VM from the Microsoft Azure off-site copy, just click **Next**. Otherwise, enable the **Restore from Microsoft Azure** option and specify the storage account settings to override the default ones if necessary, and then click **Next**.

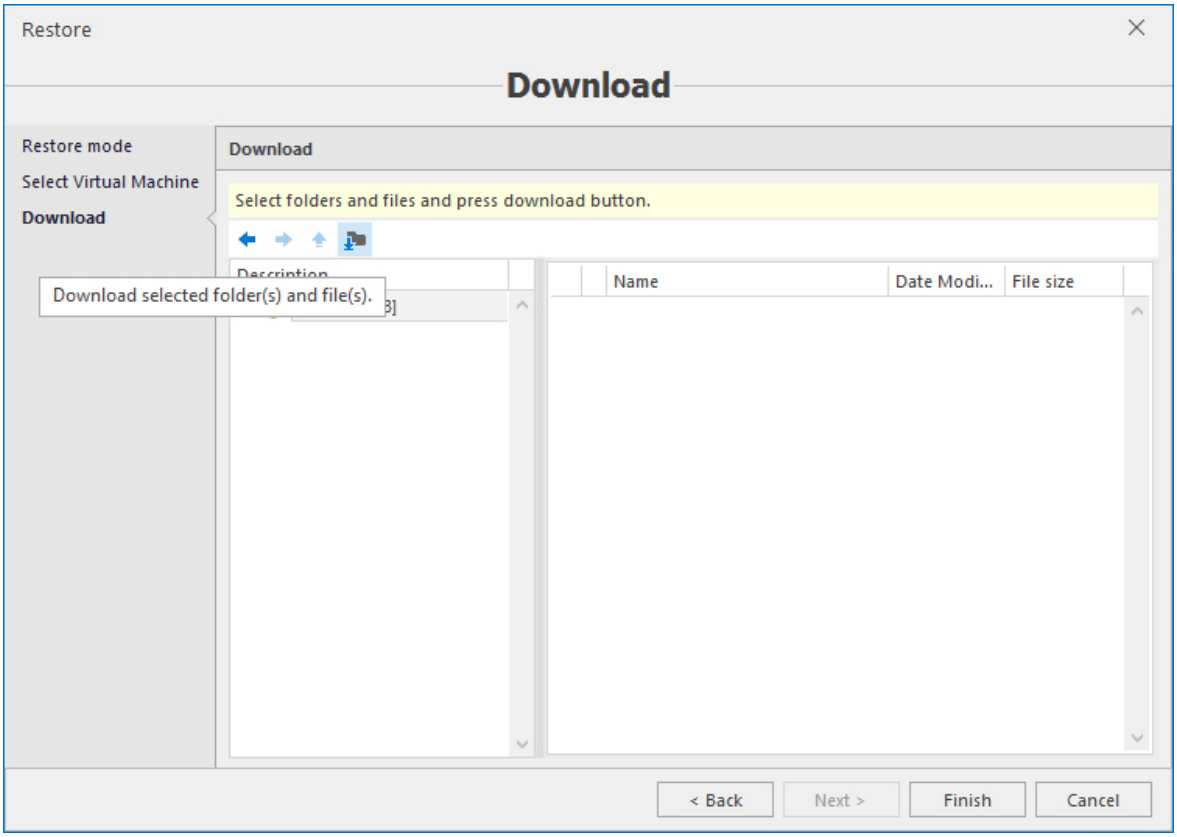
4. Select a host or a cluster where you need to restore a VM. This step applies for the restore of the entire VM.



5. Select the VMs you need to restore, and choose the configuration - whether to replace the existing VM (s) or create the VM with the new ID and keep the existing. Set the alternative path to store the VM files, if necessary. Original path will place files as they were stored previously, whereas default path will set the folders, configured in the host's Hyper-V settings. Click **Finish** to start the VM restore operation:



6. If you have selected to browse and download separate files from the archive, you will need to choose and download the required files:



7. When the files downloading is complete, press **Finish** or **Cancel** to exit the wizard.

SDN management

Software defined networking (SDN) provides a method to centrally configure and manage physical and virtual network devices such as routers, switches, and gateways in your datacenter.

For Hyper-V hosts and virtual machines (VMs) that run SDN infrastructure servers, such as network controller and software load balancing nodes, you must install Windows Server 2016 Datacenter edition or later. For Hyper-V hosts that contain only tenant workload VMs that are connected to SDN-controlled networks, you can run Windows Server 2016 Standard edition.

New in Windows Server 2016, the network controller provides a centralized, programmable point of automation to manage, configure, monitor, and troubleshoot both virtual and physical network infrastructure in your datacenter. Using network controller, you can automate the configuration of network infrastructure instead of performing manual configuration of network devices and services.

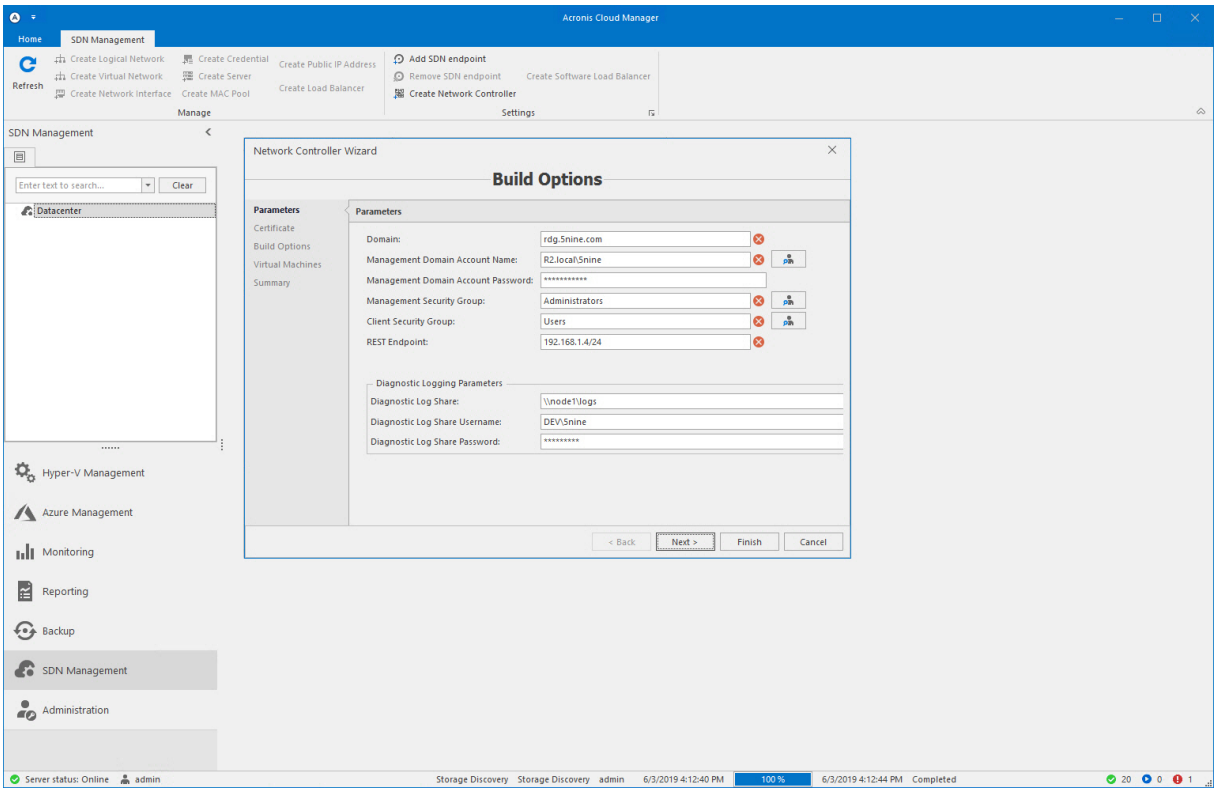
Network controller is a highly available and scalable server role and provides one application programming interface (API) - the *Southbound API* - that allows network controller to communicate with the network, and a second API - the *Northbound API* - that allows you to communicate with network controller.

Network controller provides Windows PowerShell and the representational state transfer (REST) API. Microsoft provides management APIs, Acronis Cloud Manager provides graphical user interface (GUI) to these APIs so that system administrator can easily work with SDN objects.

This GUI provides basic management features for the main SDN objects:

- Network controllers;
- Logical networks;
- Virtual machine networks;
- Logical switches;
- Network interfaces;
- Virtual switches;
- IP address pools.

Acronis Cloud Manager provides a graphical user interface for operations with all these objects via PS or REST interfaces of network controller.



Network controller deployment

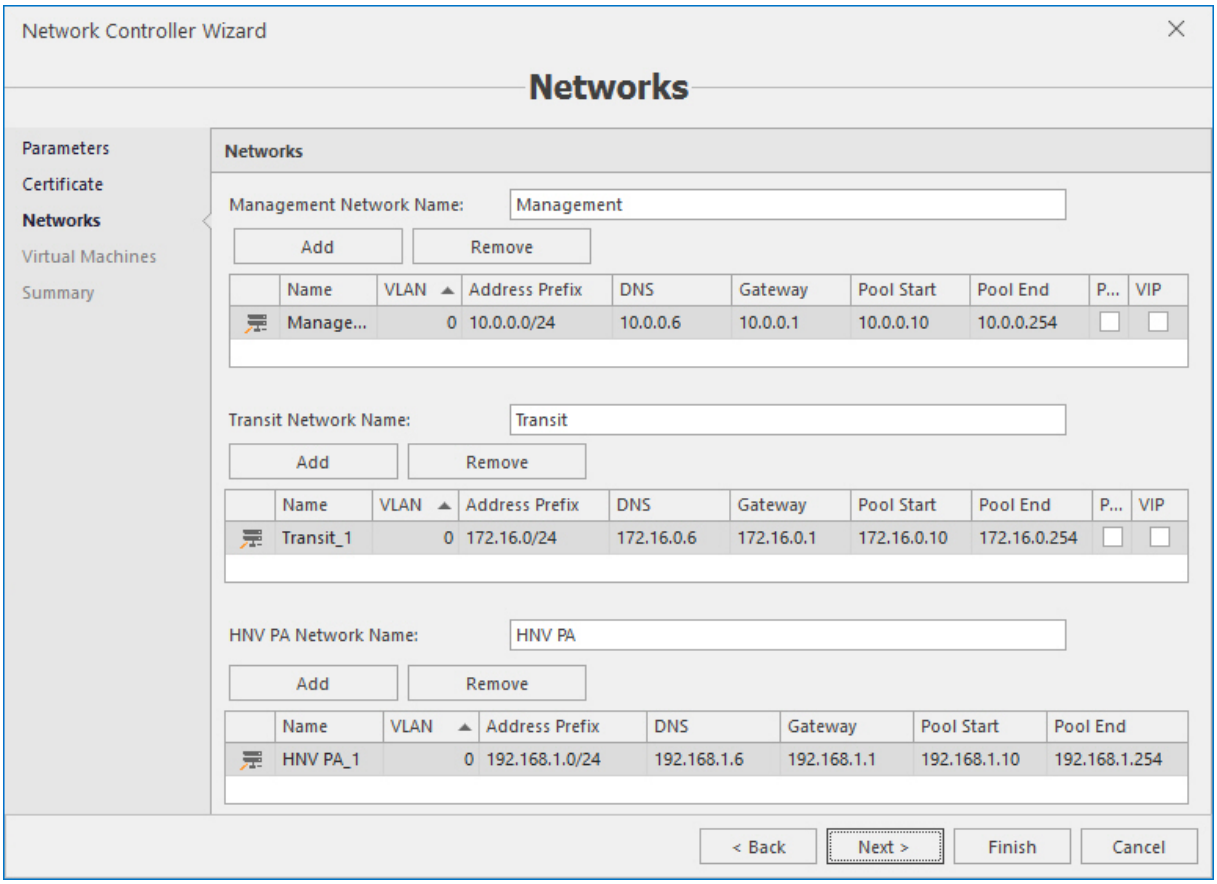
To start the network controller deployment, click the **Create network controller** button on the main ribbon:

Fill in parameters:

- **REST endpoint** – IP address or FQDN of northbound network controller interface (REST API). If FQDN is specified – *A* record must be created in DNS. If an IP address is used, it must be chosen from the vacant part of the pool. This IP address will be set for the NC cluster. It is not needed to create the cluster manually and set the IP in advance.
- **Domain** – active directory domain.
- **Management domain account name** – domain account used for network controller deployment. Will be added to local administrators group. Must be member of **Management Security Group** specified below.
- **Management domain account password** – password for domain account.
- **Local administrator password** – password assigned to local administrator account.
- **Management security group** – active directory security group. Members of this group will have full access to the network controller.
- **Client security group** – active directory security group. Members of this group will have read-only access to the network controller.
- **Diagnostic log share** – file share for storing logs of network controller and managed server. If not specified – logs will be stored locally on each NC node or managed server with retention 14 days.
- **Diagnostic log share username** – user name of the account, which have write access to logs file share.
- **Diagnostic log share password** – password of log share access account.

Click **Next**.

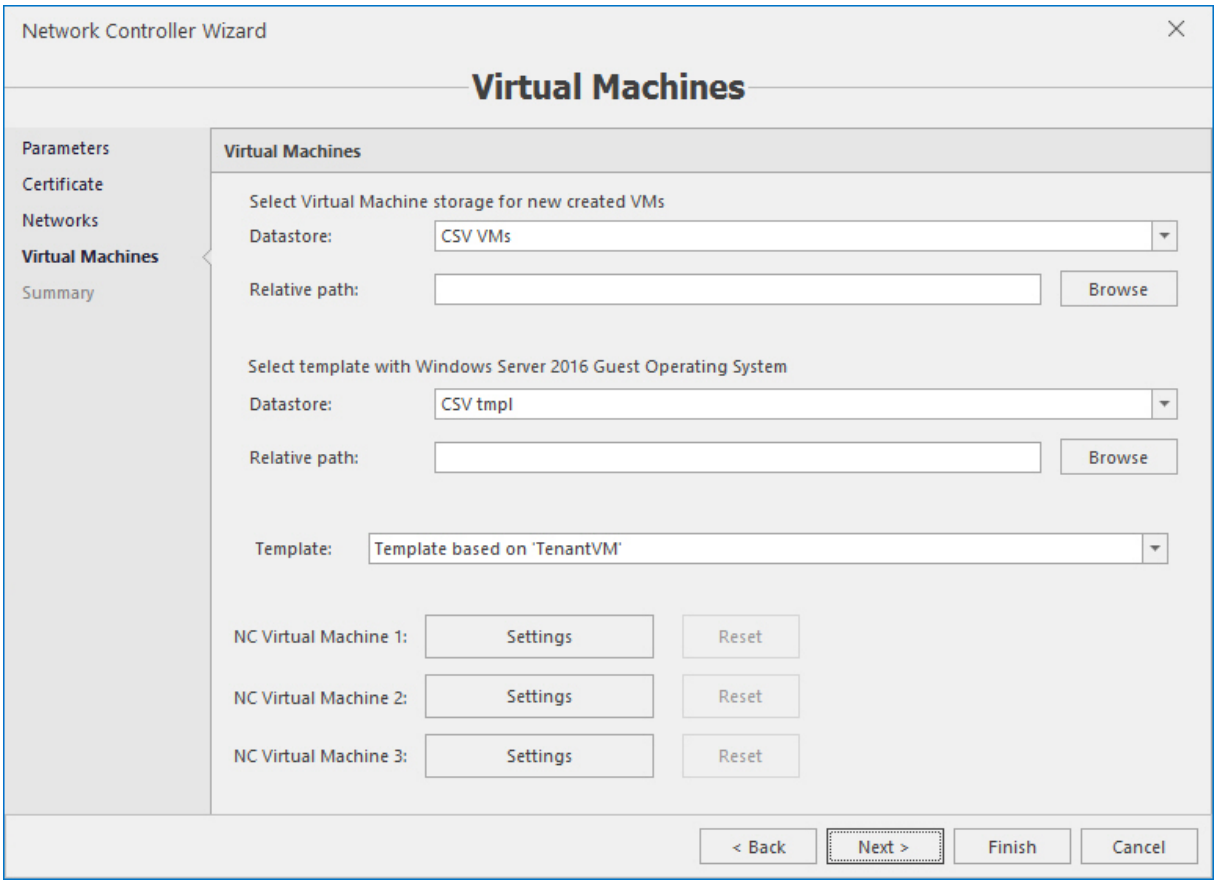
Set certificate. Network controller can be deployed with self-signed or CA certificate. Acronis Cloud Manager can work with both types of certificate. If you want to use CA certificate – you need to prepare certificate template with two **Enhance key usage** attributes – *server authentication* (1.3.6.1.5.5.7.3.1) and *client authentication* (1.3.6.1.5.5.7.3.2). Click **Next**.



Set networks:

- Management network – management network is used for communication between network controller, network controller service VMs (SLB, GW) and managed devices. Must be specified for use in feature deployment of NC services (SLB, GW).
- Transit network – transit network is used for communication between service VMs (SLB, GW) and BGP router(s).
- HNV PA network – HNV PA network is used for creation of virtualized (VXLAN) VM networks. Every Hyper-V host will acquire two addresses from this network pool. These addresses will be used to create tunnels between Hyper-V hosts.

Click **Next**.



Select virtual machines that will be used for network controller. The following parameters must be specified for VMs that will be used for network controller deployment – datastore on which NC VMs will be placed and template from which network controller nodes will be deployed. Template must be syspreped VM with Windows Server 2016 or higher. Click **Finish**.

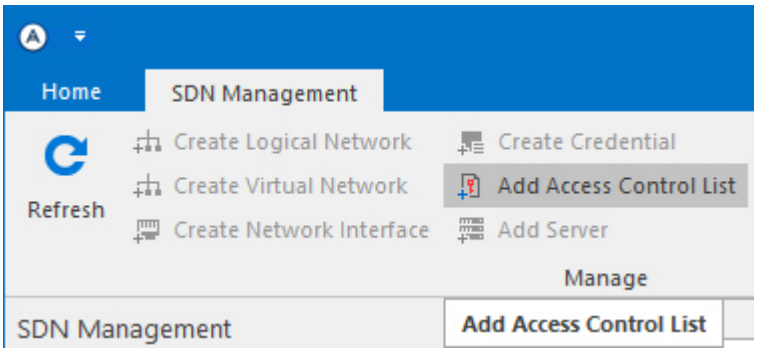
SDN management

SDN management includes the following operations:

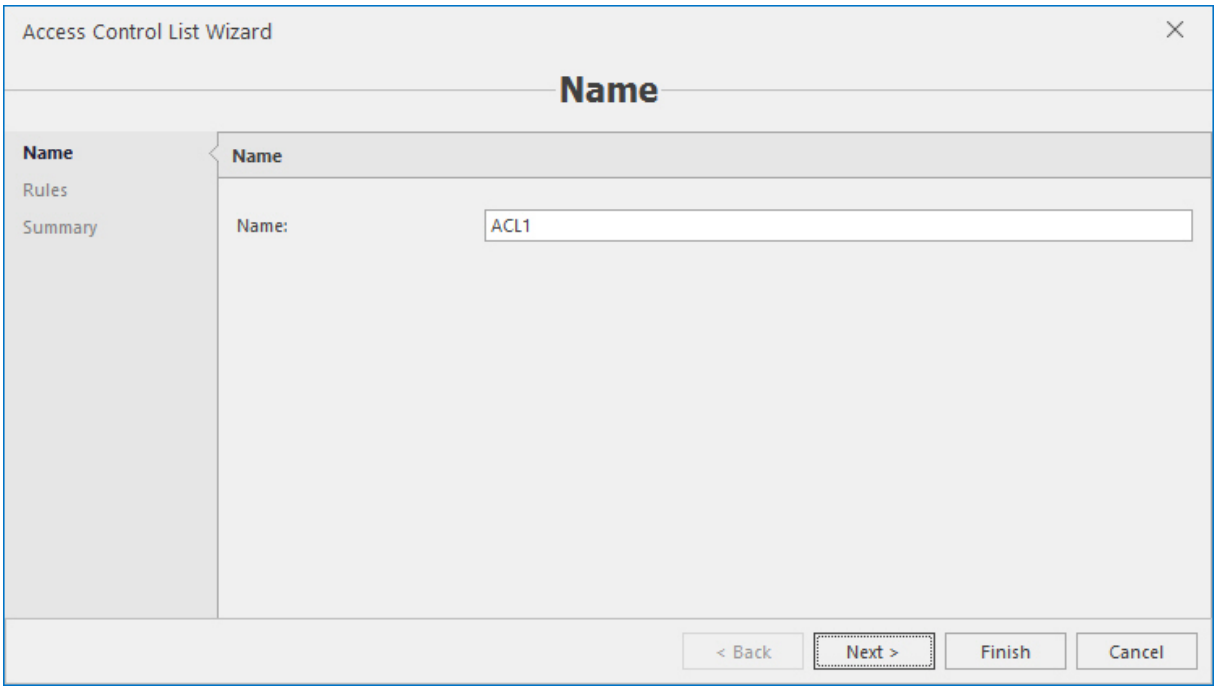
Access control list

Defines set of ACL for network interfaces – direction of flow (ingress/egress), range of source/destination ports and address prefix. After the network controller deployment Acronis Cloud Manager creates default rule which allows all inbound traffic.

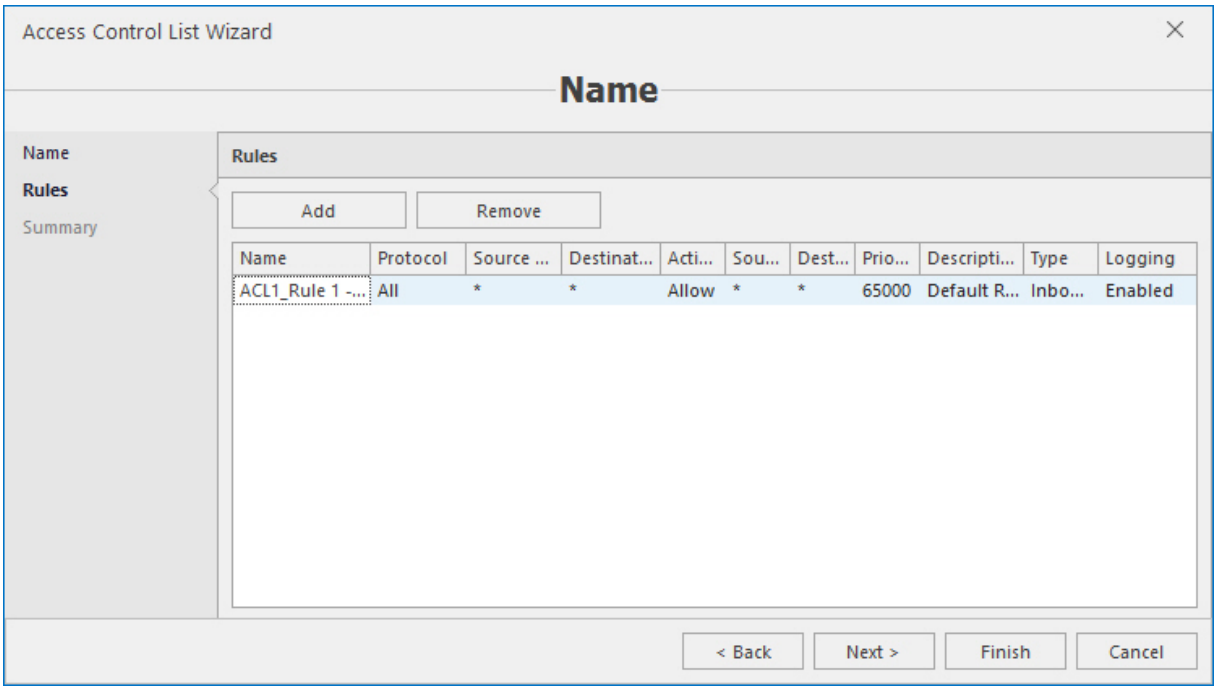
To add access control list, click the corresponding button on the main ribbon:



Specify name:



Specify rules:



Rule includes:

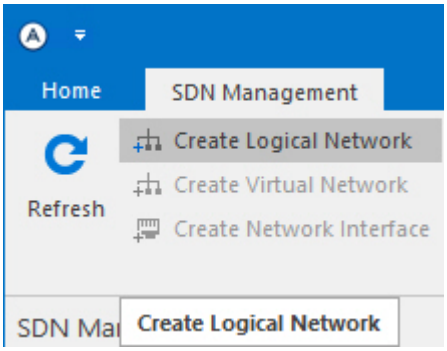
- Source/Destination port range.
- Action: (Allow/Deny).
- Source/Destination address prefix in CIDR (use /32 to specify one address).
- Priority from 100 to 65000 (rules with low priority have high precedence).
- Description.
- Type: Inbound/Outbound.
- Logging: Enabled/Disabled.

Click **Finish**.

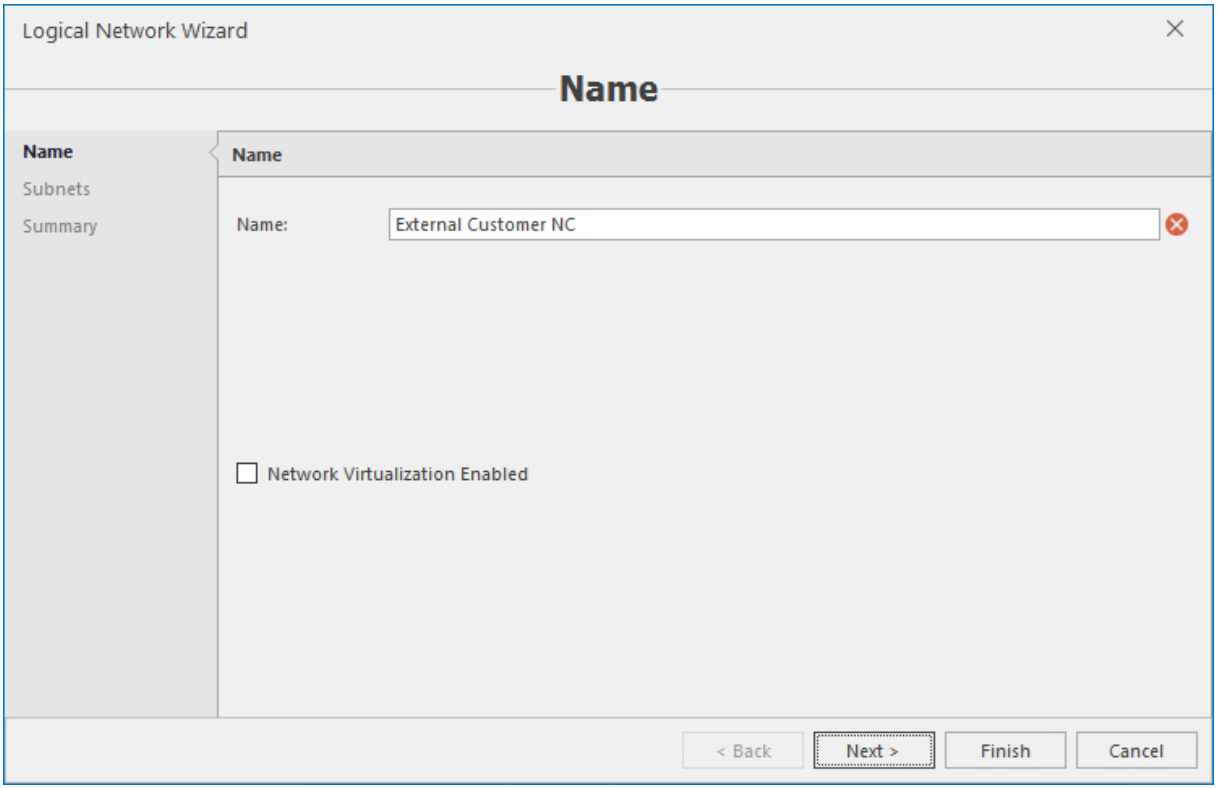
Logical network

Logical networks present abstraction of physical topology (i.e. provider addresses). After the network controller deployment, Acronis Cloud Manager creates PA network (used by host to build VXLAN tunnels), management network, and transit network (used for communication between SLB MUXes and BGP).

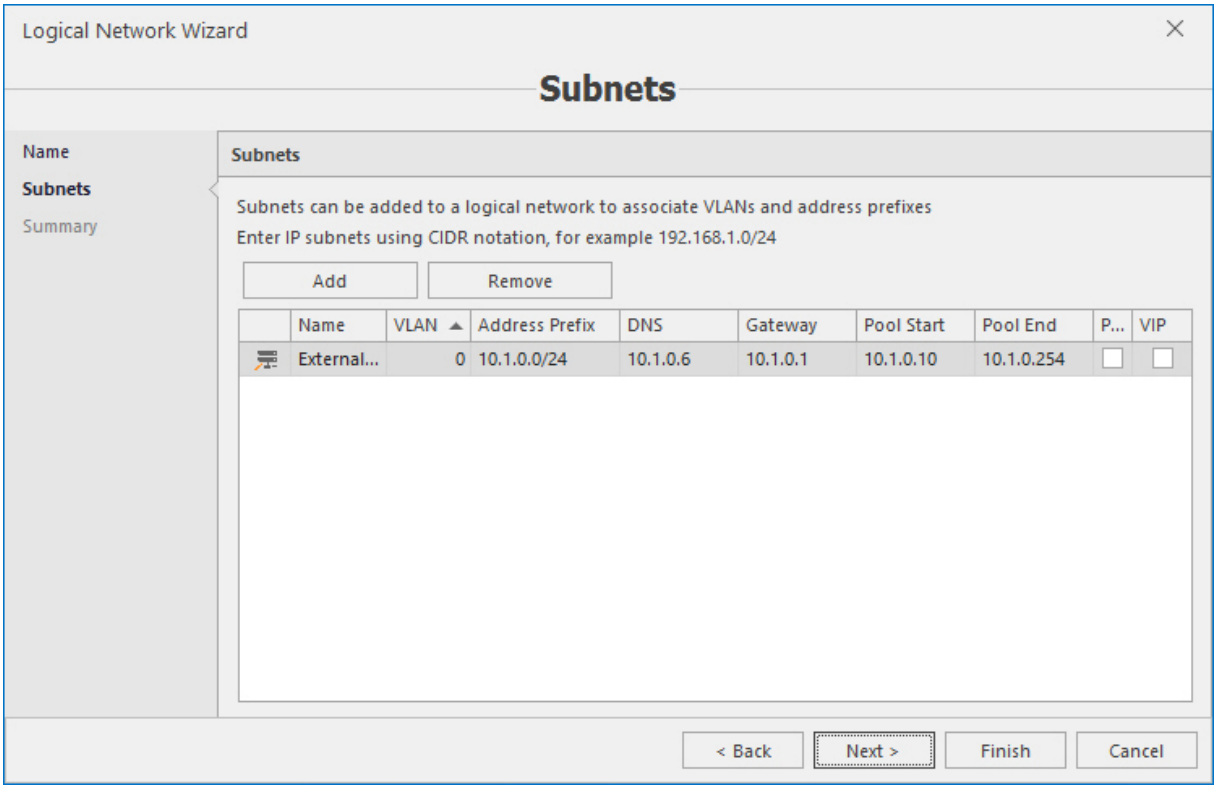
To add logical network click the corresponding button on the main ribbon:



Specify name:



Specify subnets:

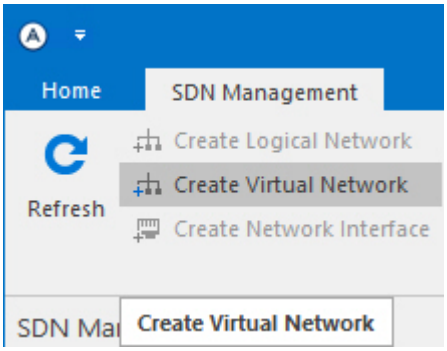


Subnet consist of VLAN ID, subnet address prefix, DNS server address, gateway address, IP range (must start from x.x.x.4, because first three addresses used internally by the network controller).

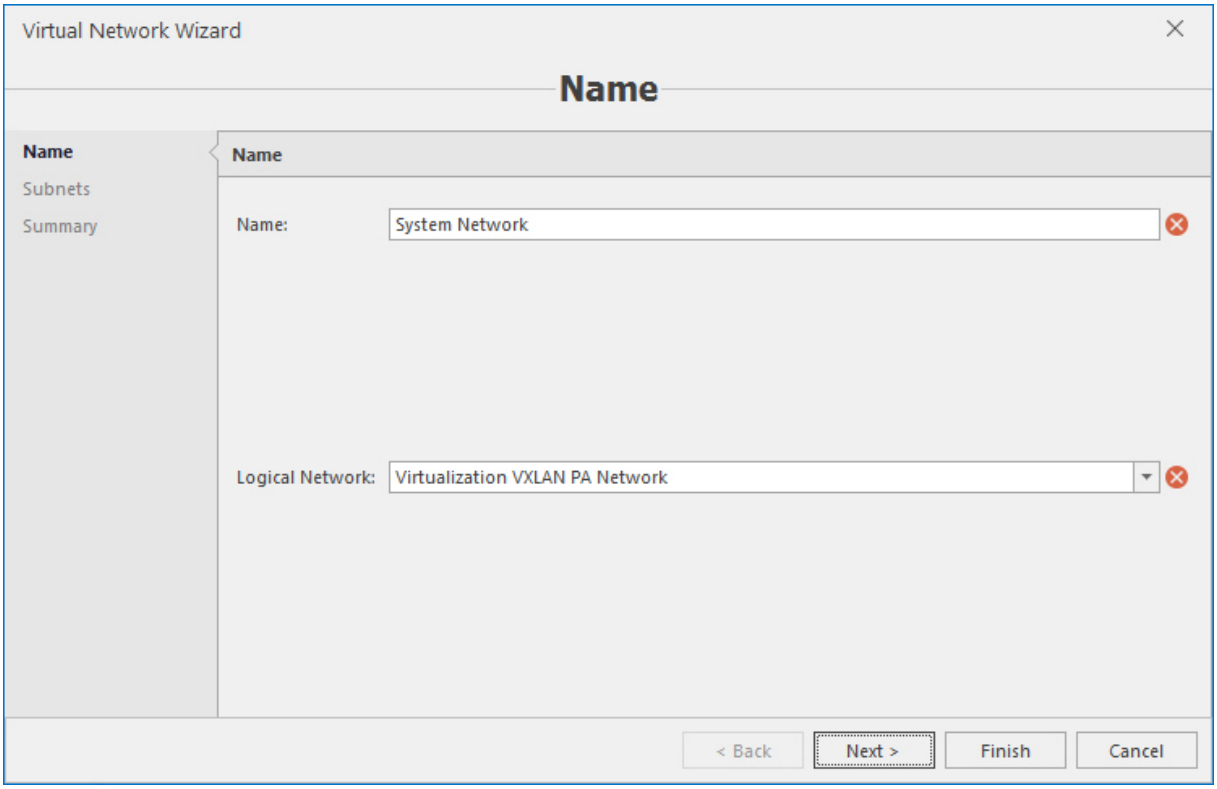
Virtual network

Virtual network is a network that virtualized using VXLAN. Virtual network must be created upon PA logical network.

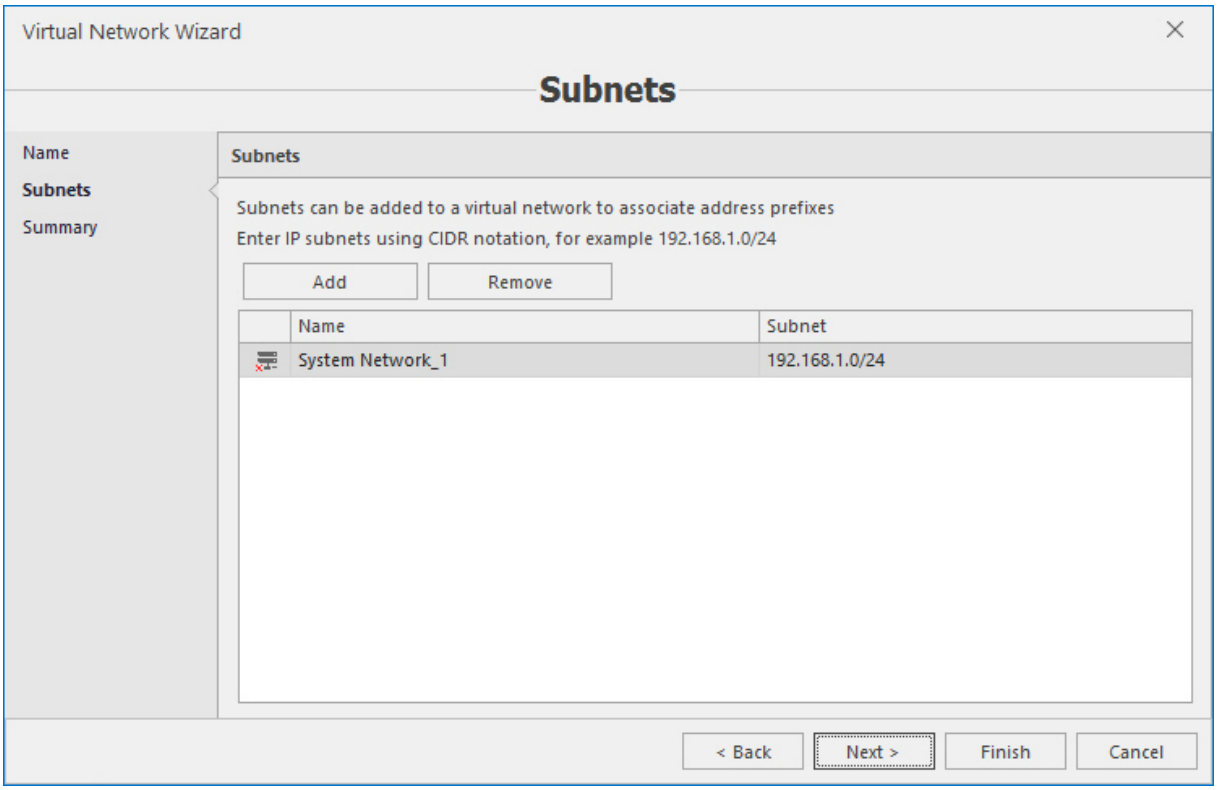
To add virtual network, click the corresponding button on the main ribbon:



Specify name:



Specify subnets:



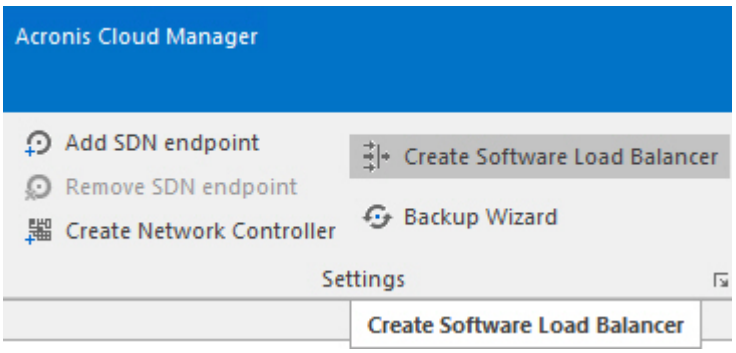
Subnet consists of subnet address prefix. x.x.x.1 assigned as subnet default gateway automatically. Network interfaces can use addresses from x.x.x.4.

Load balancer

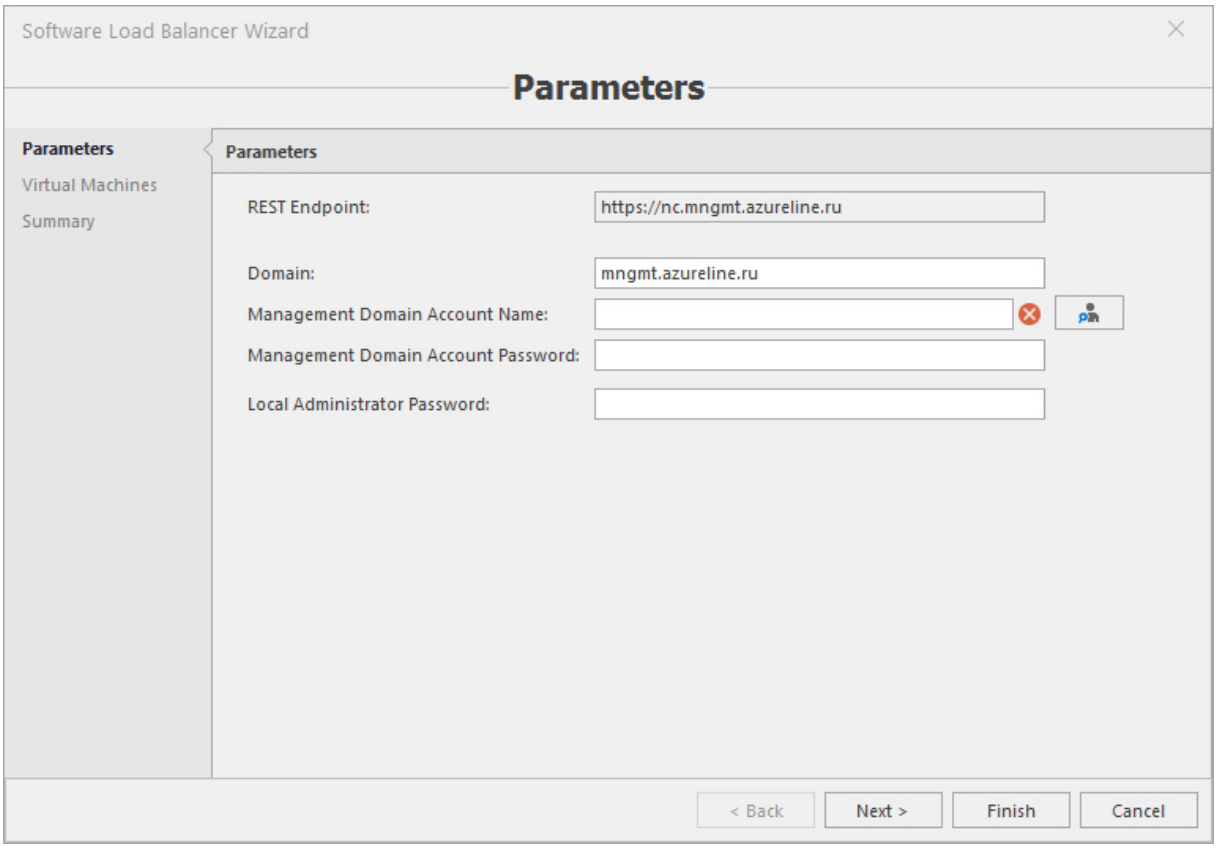
LB defines L4 load balancing for VMs: load balancer VIP, backend VMs.

Load balancer MUX - load balancer multiplexor is internally used by network controller. Network controller publishes load balancer VIPs to MUX, MUX publishes /32 route to BGP. Handles inbound traffic for load balancing.

To add MUXes, click the **Create software load balancer** button on the main ribbon:

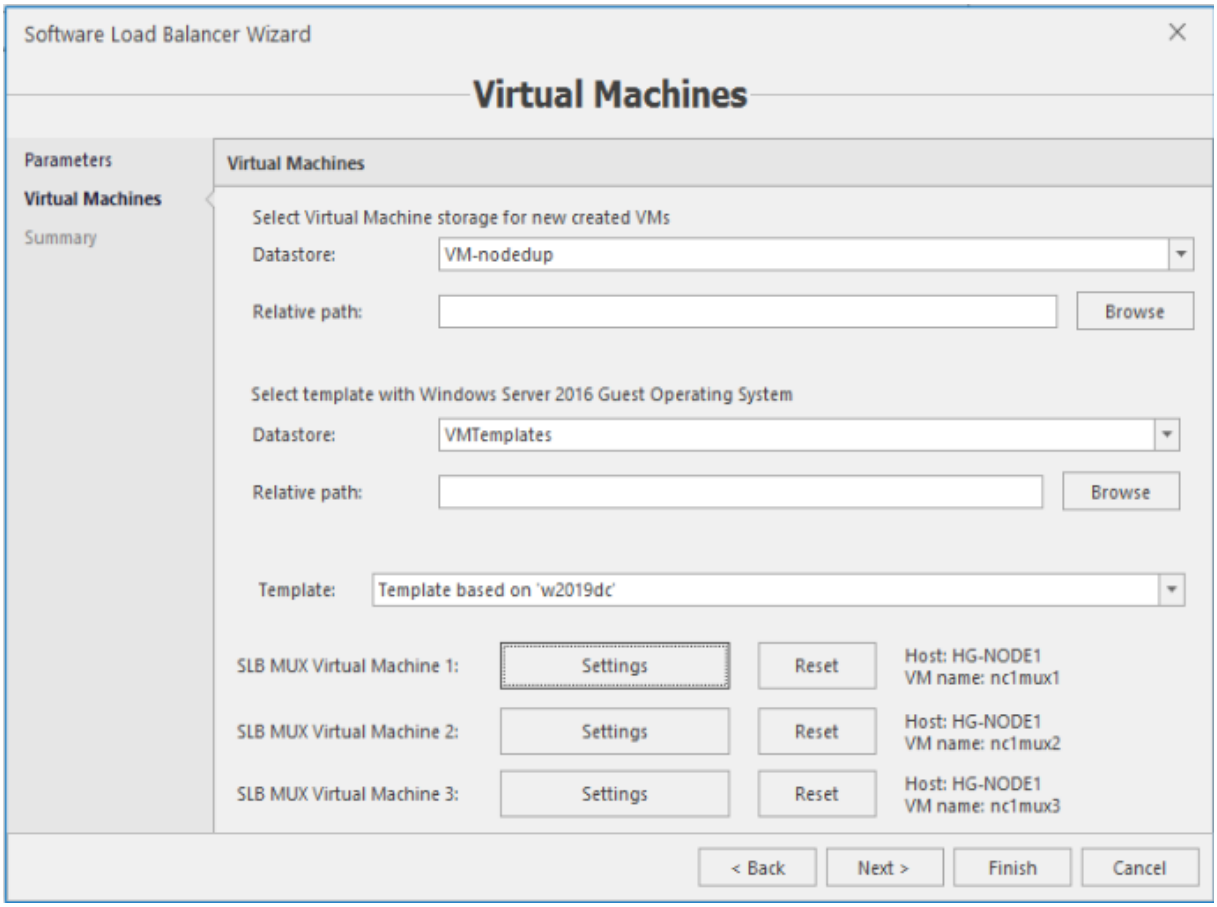


Specify parameters:



- **Domain** – domain to join SLB MUXes.
- **Management domain account name** – account used for add VM to domain, and configure MUXes in NC. Must be member of network controller management group.
- **Local administrator password** – password for local administrator account. Local administrator account used for install and configure necessary windows roles for SLB.

Specify parameters for VMs:

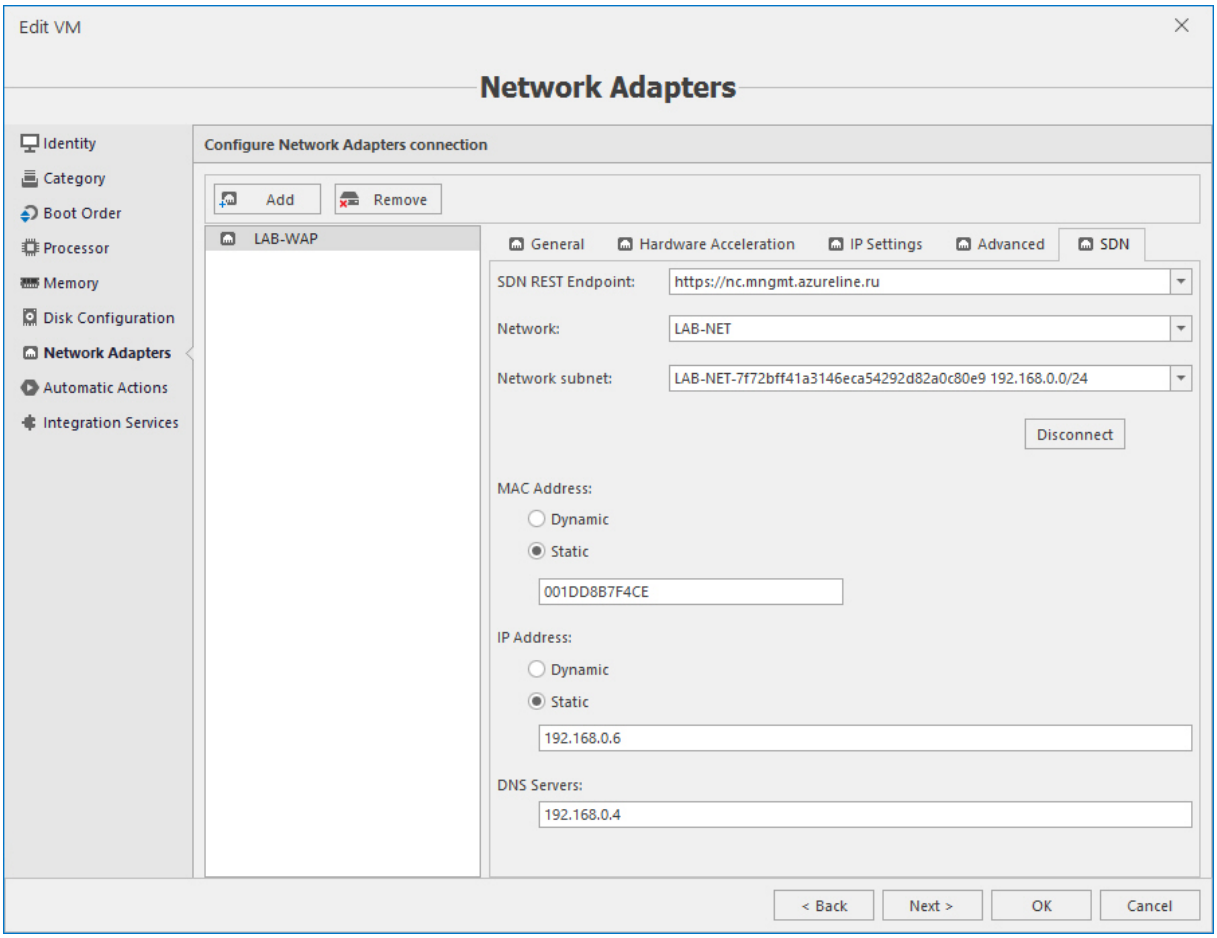


Datastore for VM placement. Datastore contains VM templates. Master automatically fills VM parameters upon clicking the **Settings** button. You can change VM name or CPU/memory configuration per VM If needed.

Network interface

List of VM network interfaces managed by the network controller.

To add managed VM interface, open VM properties, and navigate to the **Network adapters** page. Choose the appropriate network adapter and open the **SDN** tab:

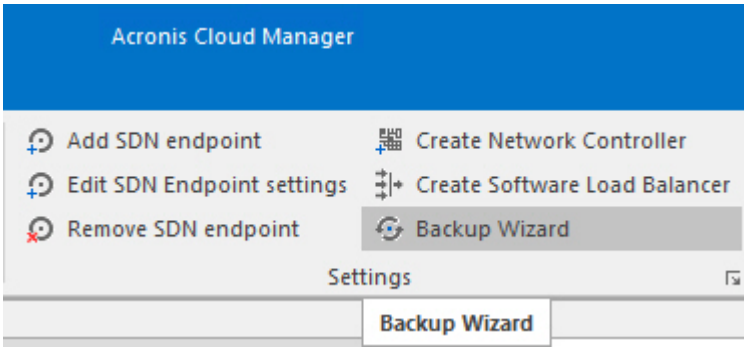


Choose the SDN REST endpoint of the appropriate network controller, network and network subnet. Configure MAC and IP addresses, and DNS servers as applicable. Click **OK** to save the configuration.

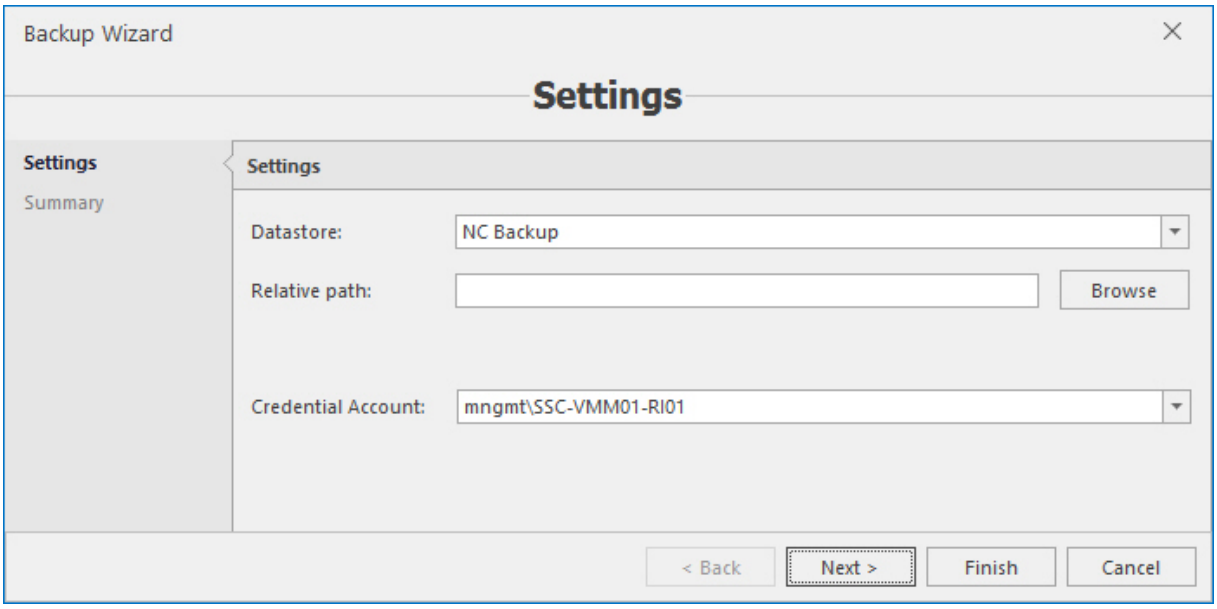
SDN backup

Acronis Cloud Manager provides ability to perform the network controller OVSDB backups.

To create manual backup, click the **Backup wizard** button on the main ribbon:



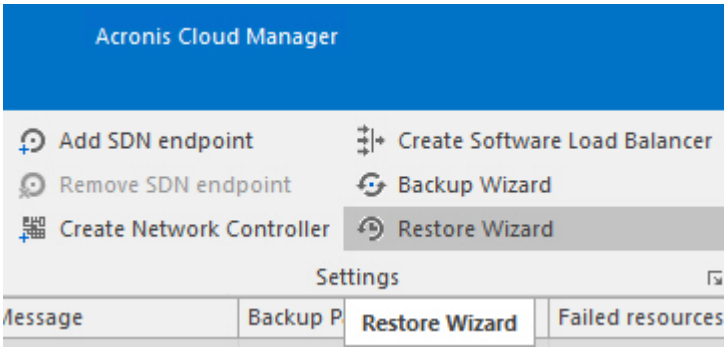
Specify the backup datastore parameters and click **Finish**:



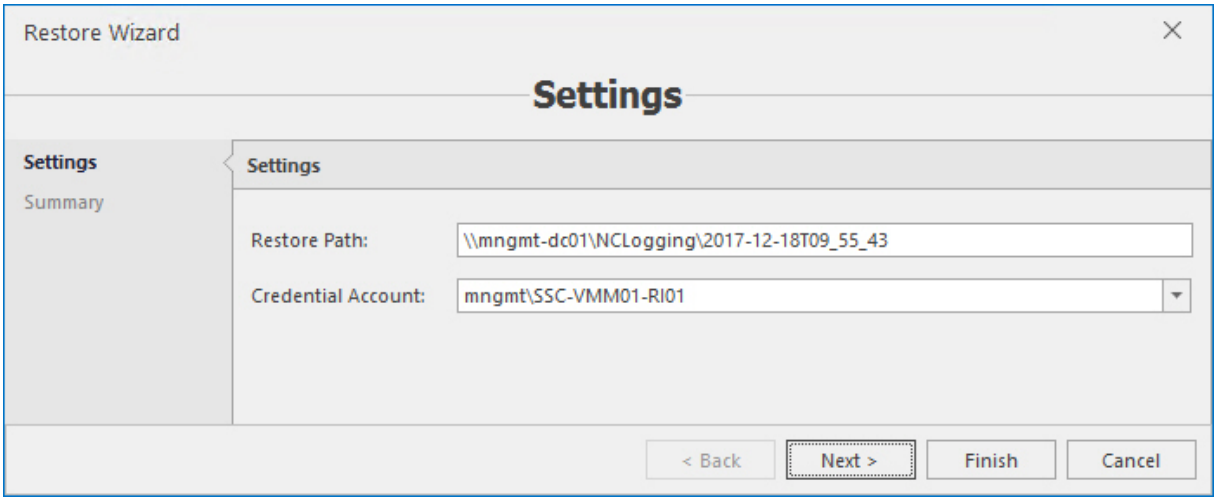
SDN restore

Acronis Cloud Manager provides ability to perform the network controller OVSDB restores.

To restore OVSDB, select backup and click the **Restore wizard** button on the main ribbon:



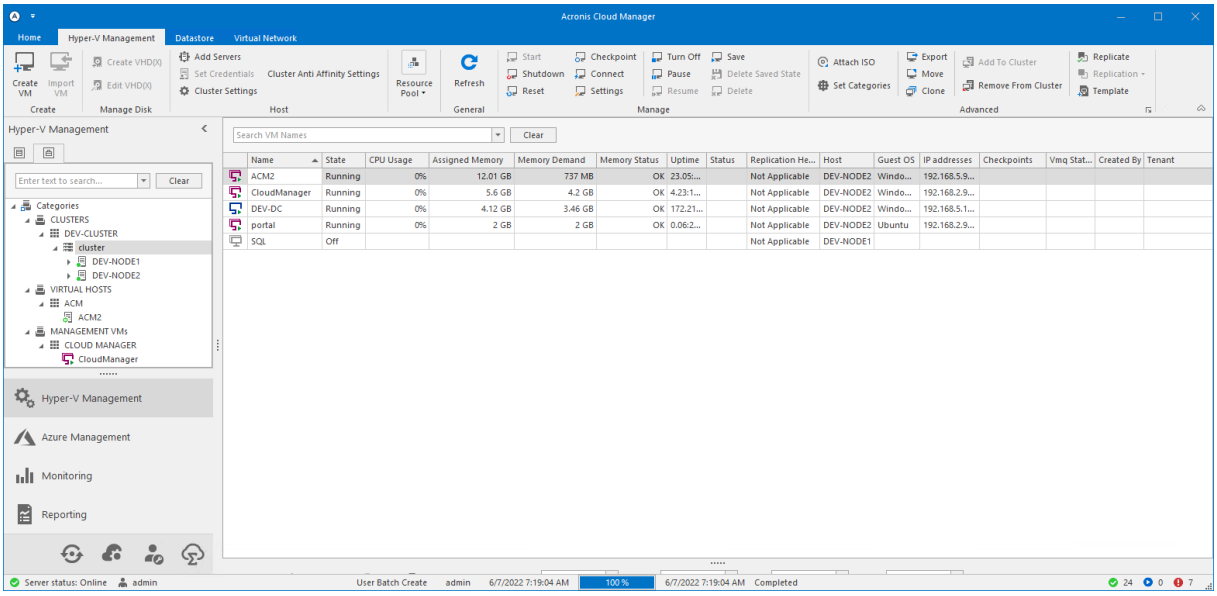
Review parameters, correct if required (they are filled in by default) and click **Finish**:



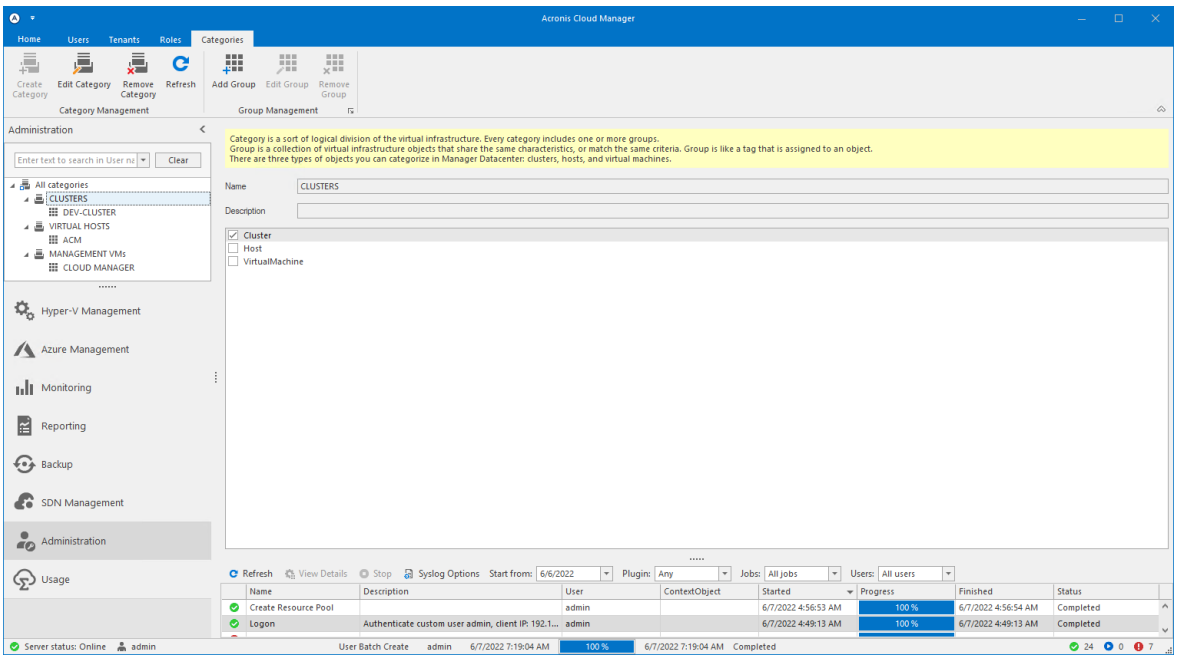
Logical view grouping

This feature allows administrators to combine multiple related resources into a single, logical tree through categorization and grouping. This new, customizable view has been added to the existing infrastructure view within the Hyper-V management console. A workload administrator, for example, can create a view of all relevant application VMs. Resource views can also be created to align with existing regional or functional administrative models.

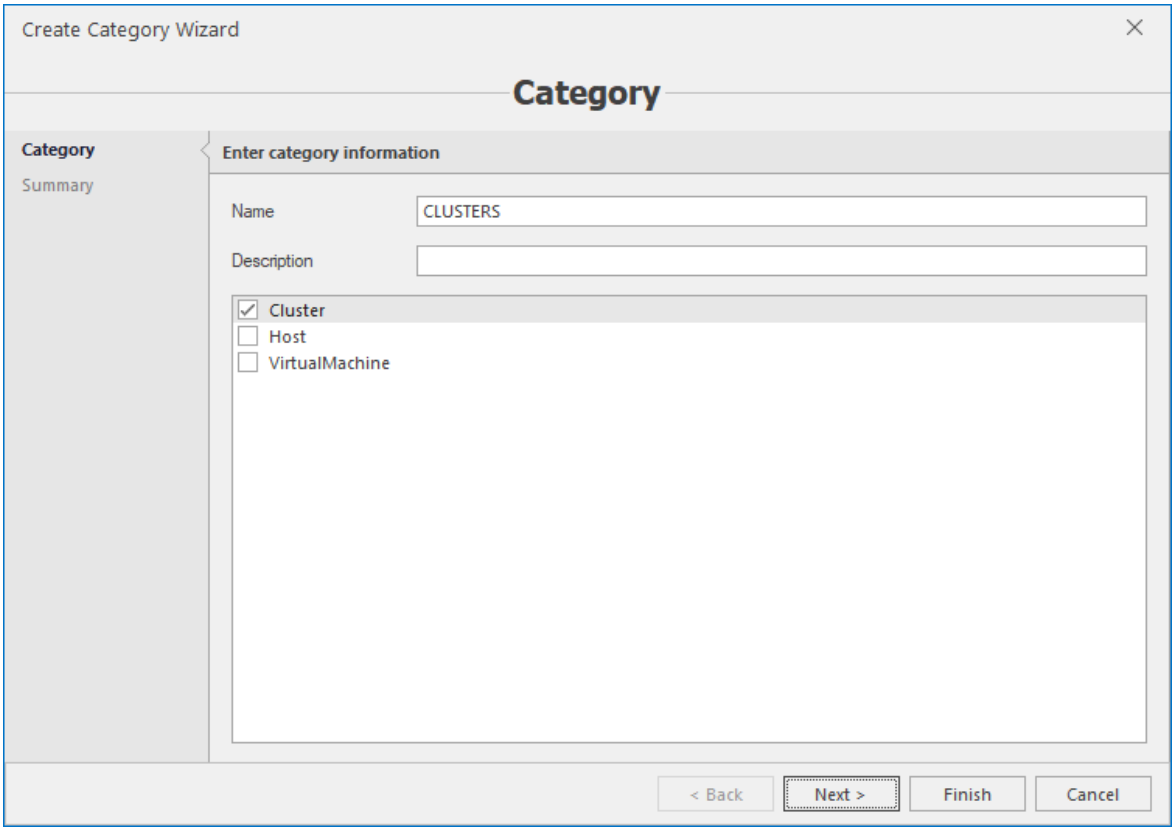
Logical view grouping allows administrators to more effectively manage, monitor and optimize operations by providing fast, easy access to relevant resources. It decreases the time and effort needed to sort through and find a resource or group of resources while maintaining strict role-based access controls.



1. First thing you need to do is create categories and groups using the **Administration** plugin – **Categories** tab:



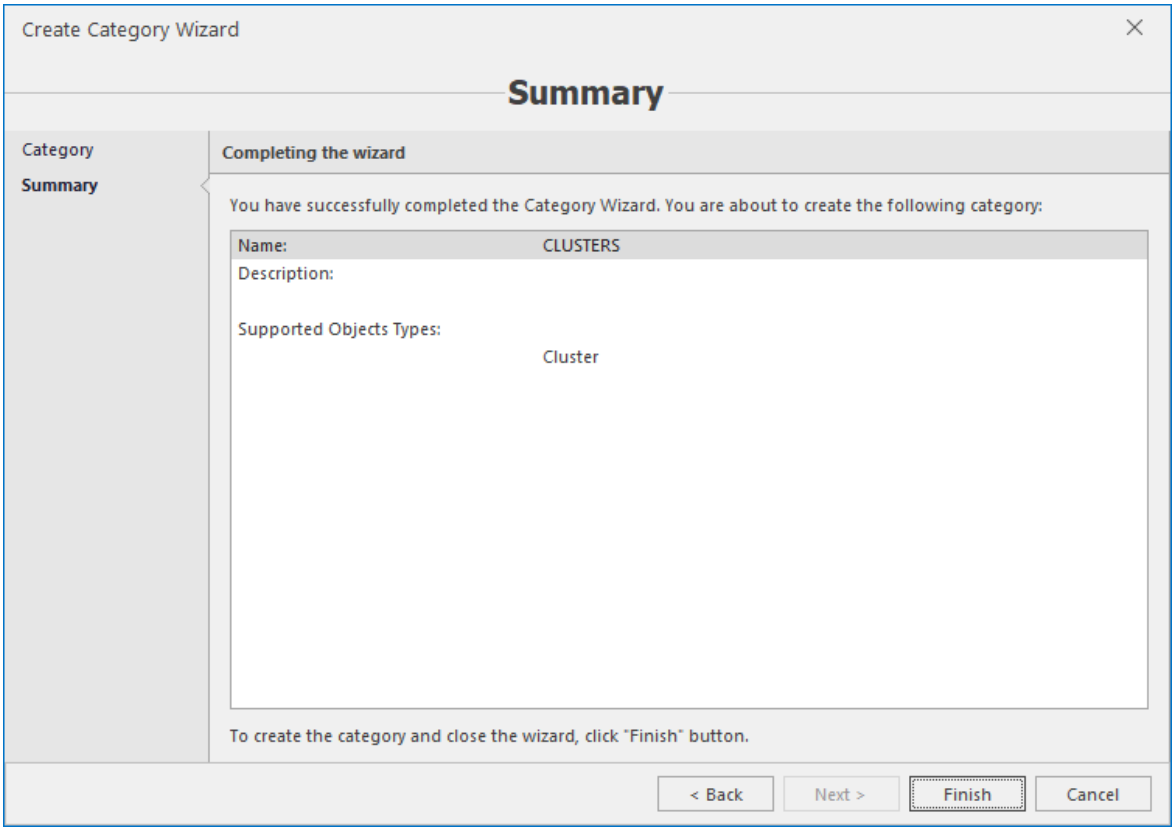
2. Click the **Create category** button on the left of the top bar and configure the new category parameters using the **Create category** wizard:



Note

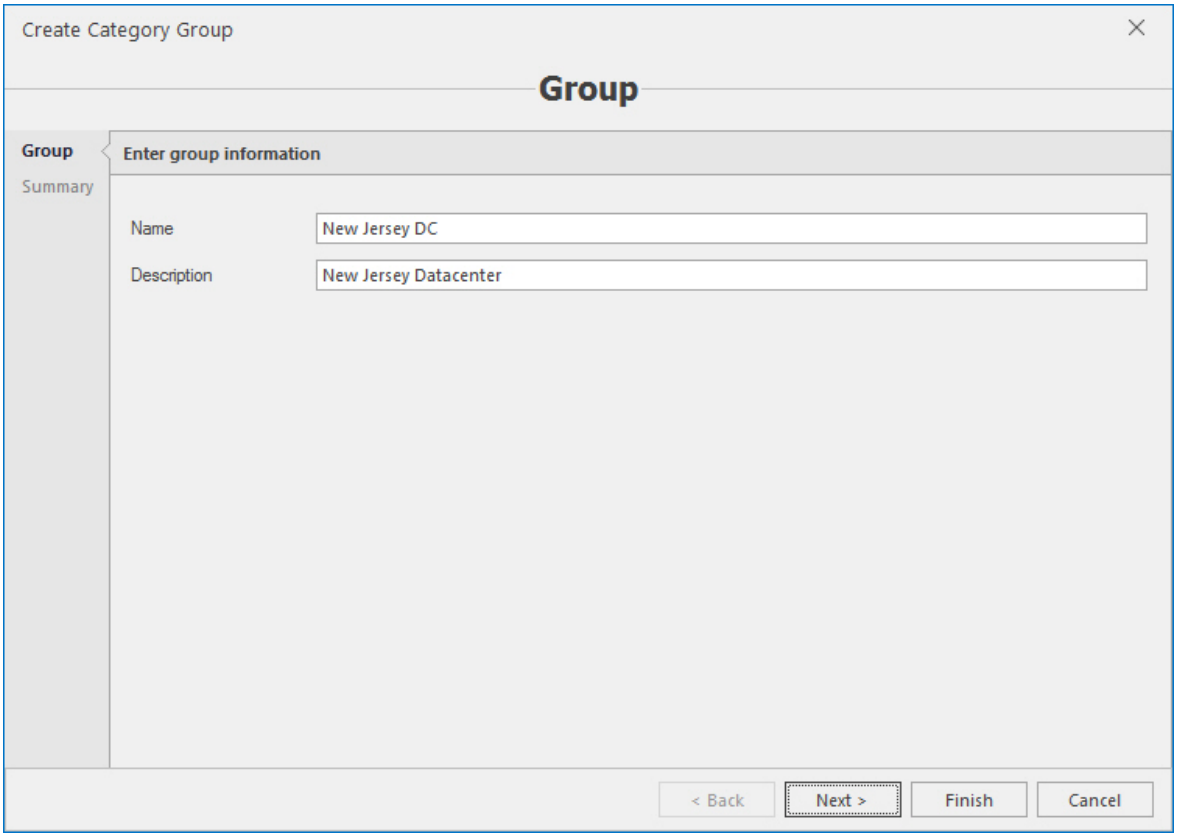
The main point is to enable certain object types that will be allowed to be associated with this category. There are three object types – cluster, host and virtual machine. It is up to you whether allow all of them or just some or one in any category. Category availability will be then appearing accordingly.

3. Click **Next**, review summary and click **Finish** to complete the wizard.



You will find your new category in the list then, where you will be able to alter it at any time.

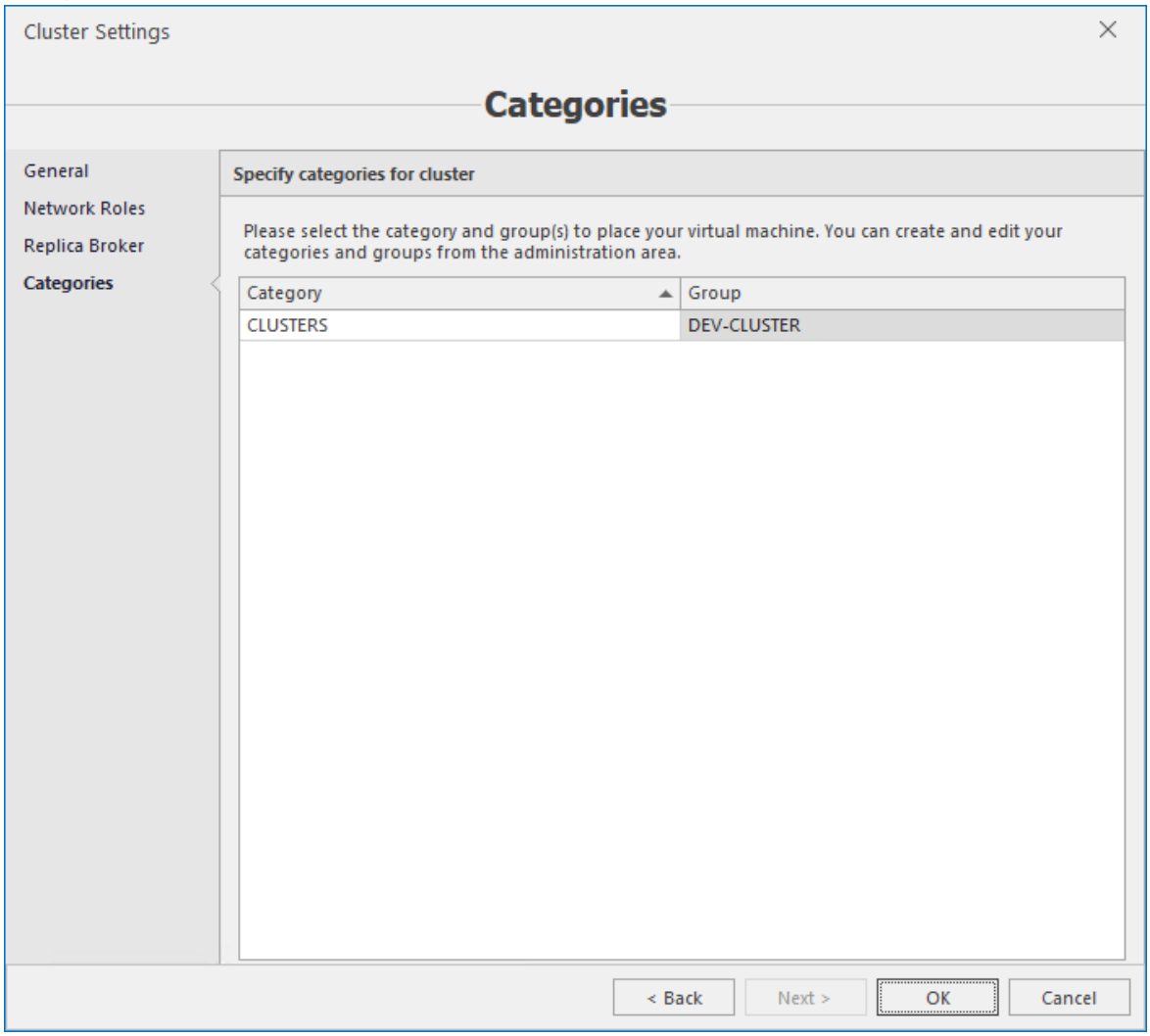
4. Next step is adding groups into categories. Select the category and click the **Add group** button.



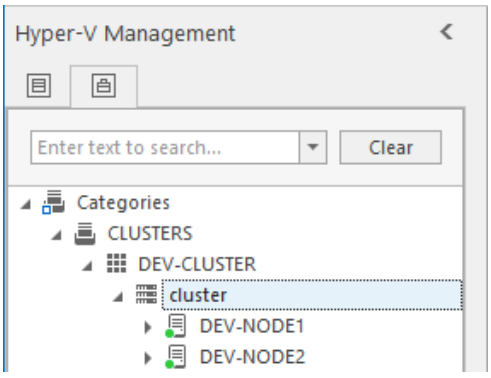
5. Specify the name for the group as will be displayed in your customized logical view. Click **Next**, review summary and click **Finish** to complete the wizard.

Note

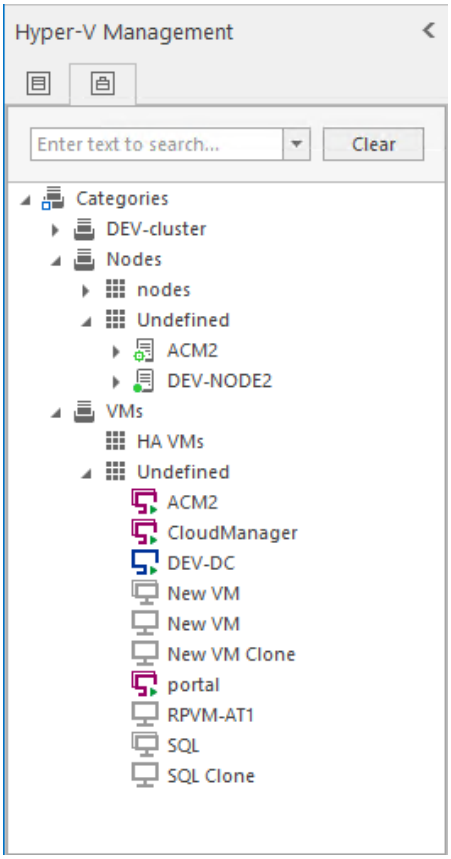
Now that you completed the above steps, you can assign objects to the group in accordance with its settings/availability (in the given example it is for cluster). This is done in the object's settings – **Categories** section, which appears in the same way in cluster, host and virtual machine settings:



Your object will appear in configured group in the logical view – open the **Hyper-V management** plugin and go to the right tab, where logical view is displayed:



Objects that are not joined into any category (group) will also be displayed in the logical view under the **Undefined** branch:

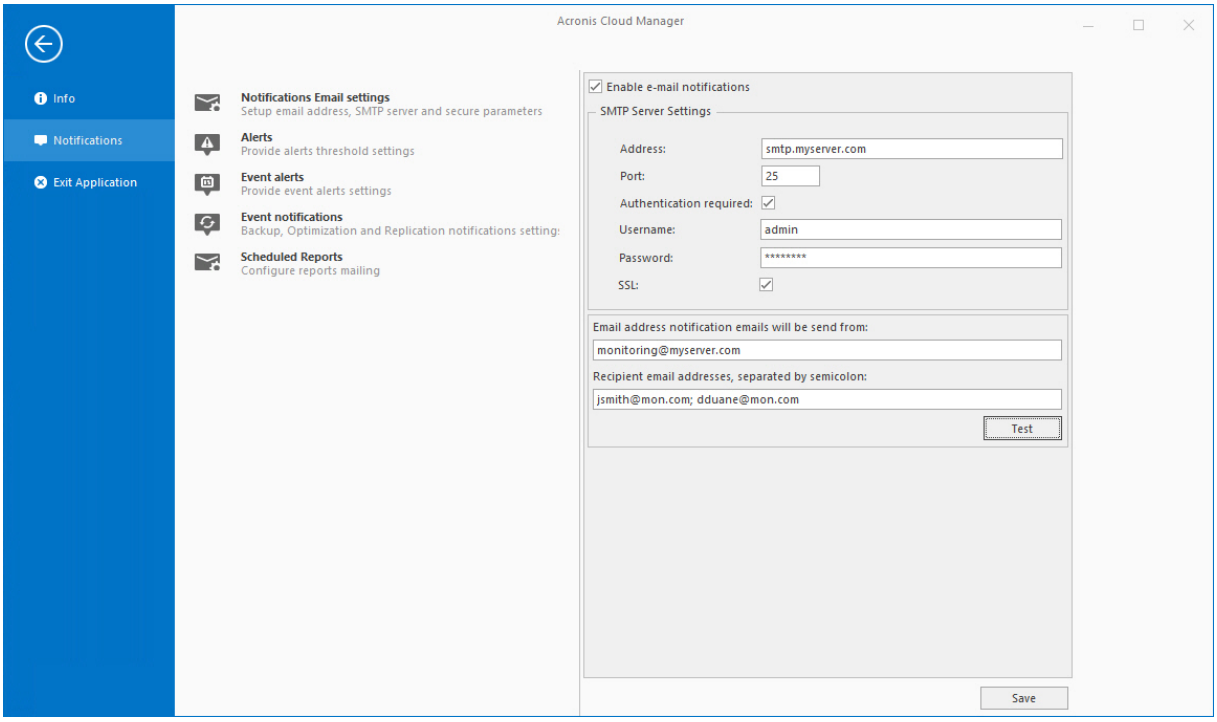


Notifications

Notifications are sent to configured email addresses and inform admin about various alerts – resource alerts, event alerts, backup & replication alerts and dynamic optimization alerts. There are also scheduled reports mailing settings for several types of data. Resource alerts work for physical/virtual performance parameters – CPU, memory, network and disk utilization; event alerts work for Microsoft Windows® clustering, HA, Hyper-V and security native events. Backup & replication alerts work for backup & replication successful/unsuccessful procedures. Dynamic optimization alerts are sent when VM migrations successfully completed. Scheduled reports are sent to configured emails – system status report, VM life cycle report and zombie VM report.

Email settings

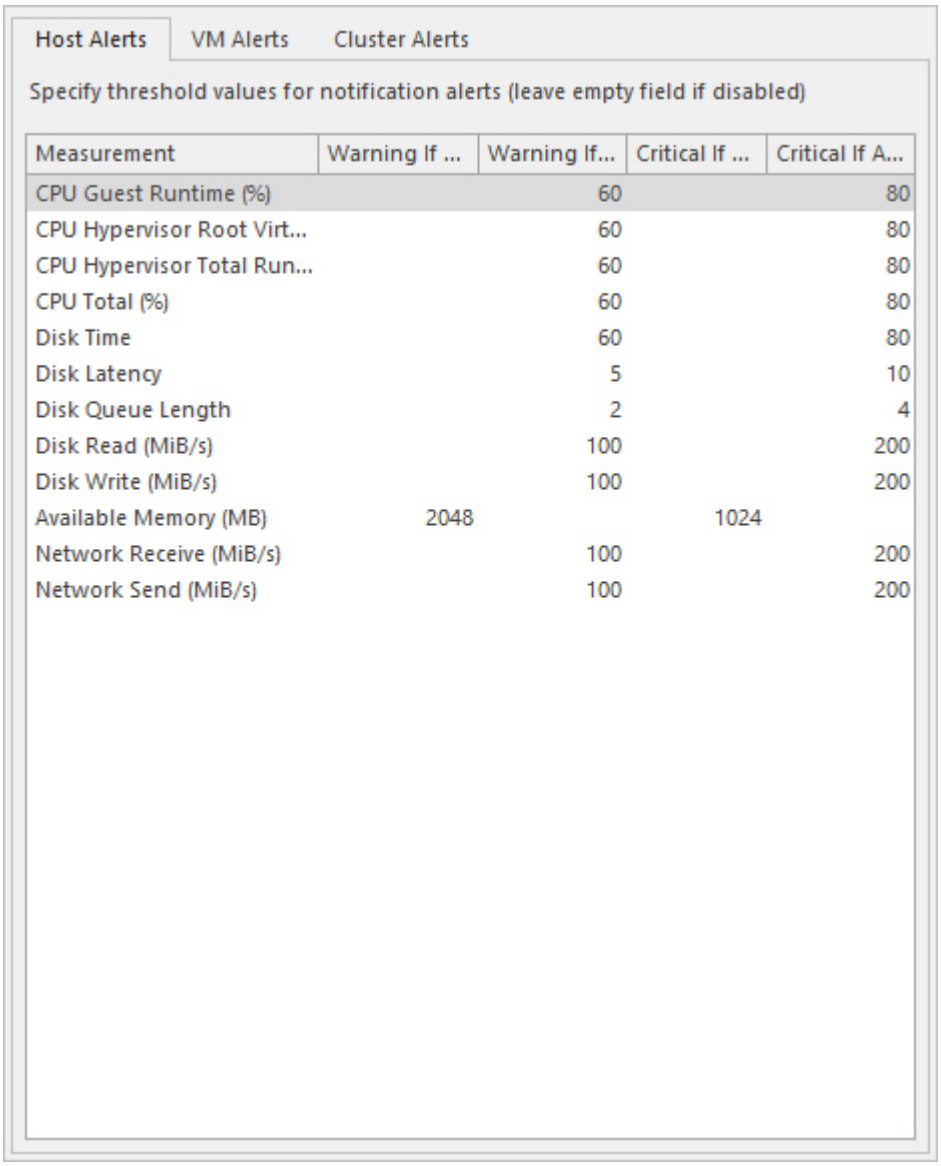
To configure notifications email settings, open the **Home** tab and then select **Notifications** – **Notifications email settings**:



Configure the email server with the TCP port and authentication credentials, and specify the recipients' emails. Notifications will be sent to the specified email addresses.

Resource alerts

To set thresholds for warning and critical alerting on performance counters open the **Home** tab and select **Notifications** – **Alerts**.



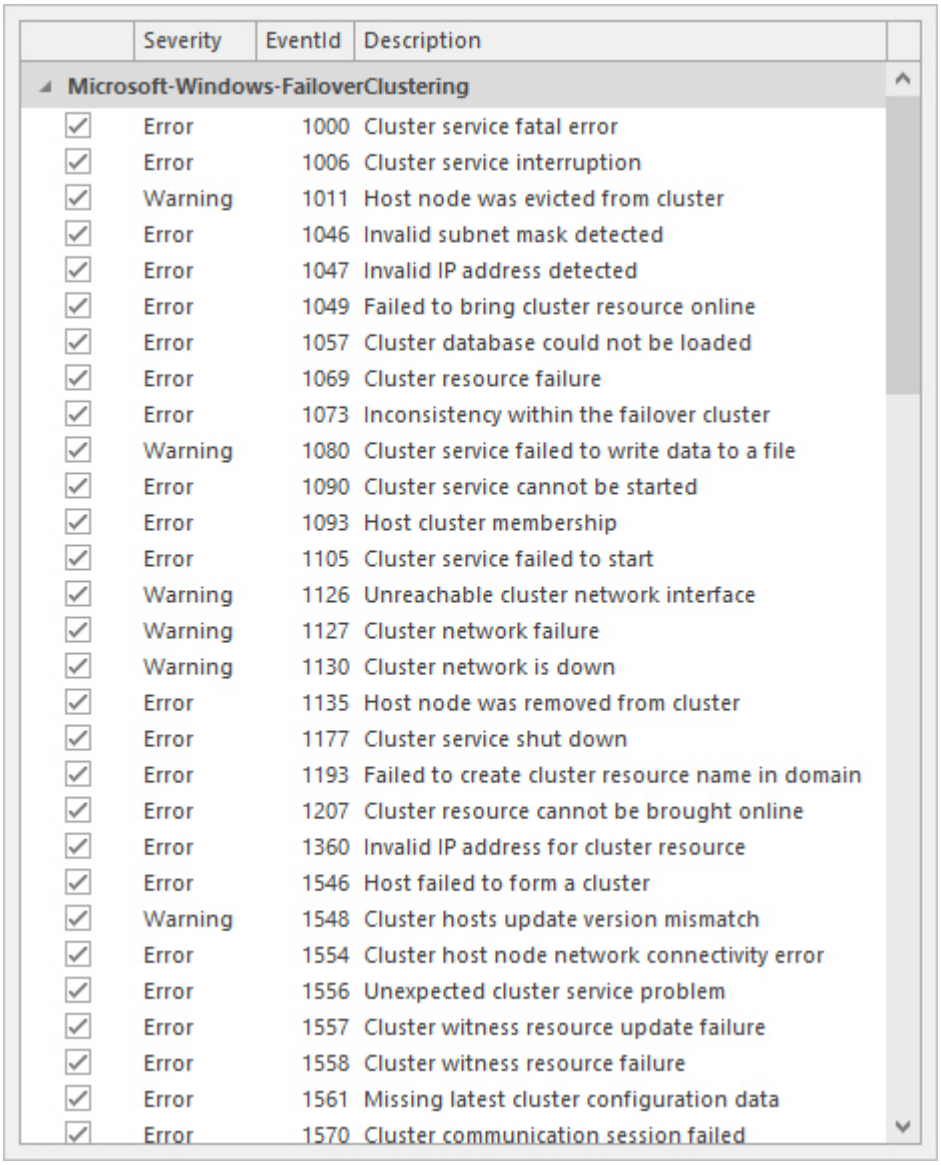
Note

There are separate sections for host, VM and cluster counters.

Values that are set to **0** mean they are disabled. Warning and error thresholds values can be set to trigger alerts when a value either falls below or above the setting.

Event alerts

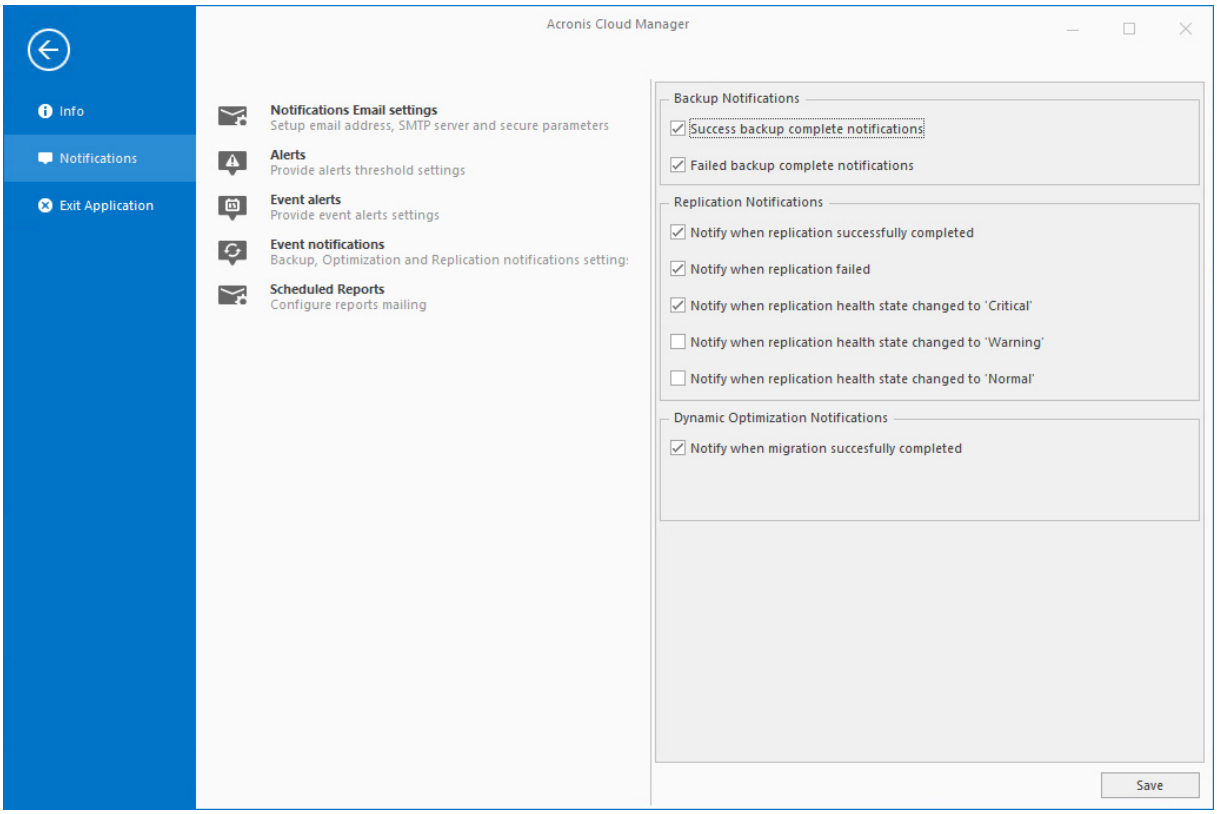
Event alerts are configured to transfer native Microsoft events into the Acronis Cloud Manager **Monitoring** plugin. To configure event alerts, select **Notifications** - **Event alerts**. Select checkboxes for the desired events to enable alerting for that event:



	Severity	EventId	Description
Microsoft-Windows-FailoverClustering			
☑	Error	1000	Cluster service fatal error
☑	Error	1006	Cluster service interruption
☑	Warning	1011	Host node was evicted from cluster
☑	Error	1046	Invalid subnet mask detected
☑	Error	1047	Invalid IP address detected
☑	Error	1049	Failed to bring cluster resource online
☑	Error	1057	Cluster database could not be loaded
☑	Error	1069	Cluster resource failure
☑	Error	1073	Inconsistency within the failover cluster
☑	Warning	1080	Cluster service failed to write data to a file
☑	Error	1090	Cluster service cannot be started
☑	Error	1093	Host cluster membership
☑	Error	1105	Cluster service failed to start
☑	Warning	1126	Unreachable cluster network interface
☑	Warning	1127	Cluster network failure
☑	Warning	1130	Cluster network is down
☑	Error	1135	Host node was removed from cluster
☑	Error	1177	Cluster service shut down
☑	Error	1193	Failed to create cluster resource name in domain
☑	Error	1207	Cluster resource cannot be brought online
☑	Error	1360	Invalid IP address for cluster resource
☑	Error	1546	Host failed to form a cluster
☑	Warning	1548	Cluster hosts update version mismatch
☑	Error	1554	Cluster host node network connectivity error
☑	Error	1556	Unexpected cluster service problem
☑	Error	1557	Cluster witness resource update failure
☑	Error	1558	Cluster witness resource failure
☑	Error	1561	Missing latest cluster configuration data
☑	Error	1570	Cluster communication session failed

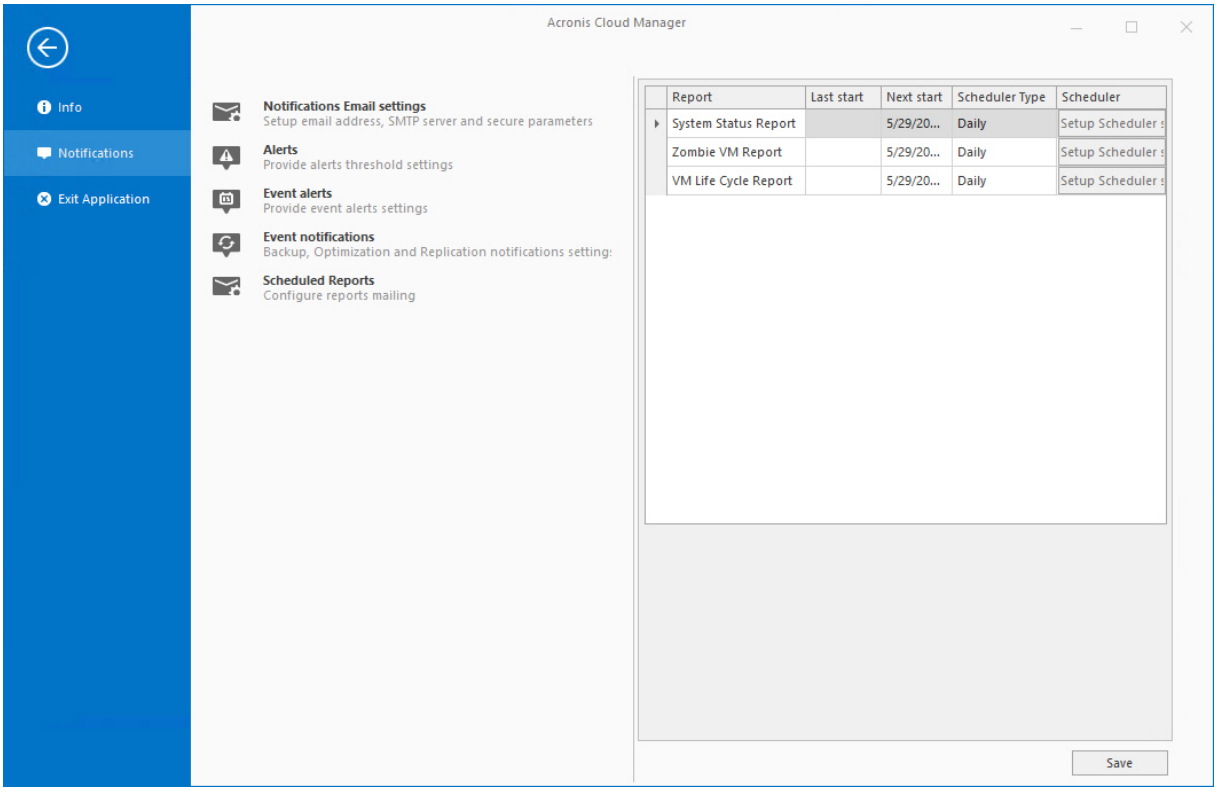
Backup, replication and dynamic optimization alerts

To configure backup, replication and dynamic optimization alerts, select **Notifications** – **Event notifications**. Select checkboxes for the desired events to enable notifications for that event:

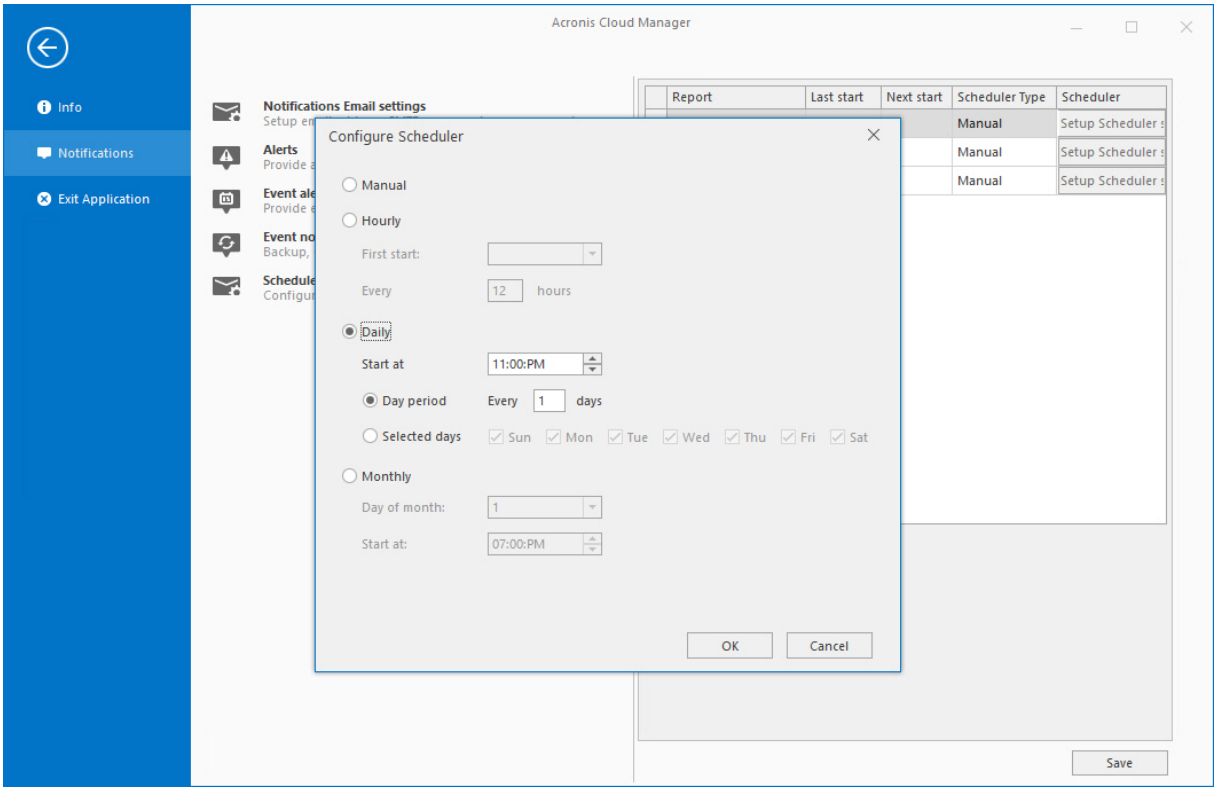


Scheduled reports

To configure scheduled reports mailing, select **Notifications** - **Scheduled reports**.



Under the **Scheduler** column, click the **Setup scheduler settings** button on the corresponding row to open the scheduler configuration dialog:



When all settings are done, click **Save** at the bottom of the window on the right side.

Note

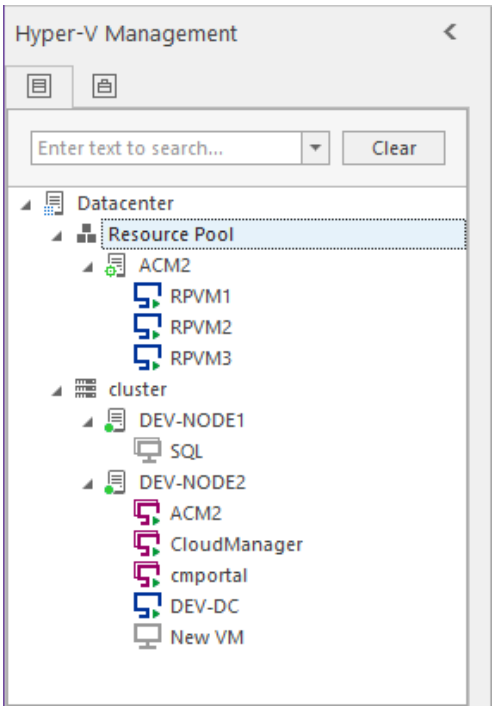
These reports can be viewed in the **Reporting** plugin of Cloud Manager (refer to the "Reporting" (p. 196) section above).

Resource pools, quotas and usage

Resource pools, quotas and usage features are designed to implement self-service Cloud Manager web portal. These features secure tenants isolation from physical layer when providing resources to them, managing resources allocation and keeping record of resources utilization.

Resource pools

Resource pool is a logical entity designed to isolate customers (tenant users) from physical layer: clusters, hosts, storages, network switches. To create VM user should select the resource pool, set CPU count, memory size, number of network adapters, number and size of disks without using any host specific information. At final VM will be created on the most appropriate host or cluster node. Resource pool contains a number of resource pool items: clusters (all nodes) and hosts:

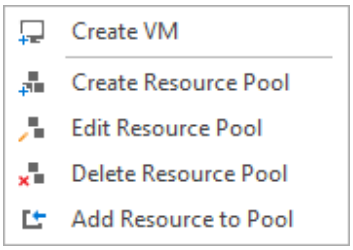


Physical host or cluster can belong only to one resource pool. Resource pool is an exclusive owner of resource pool items. So, hosts/clusters added to resource pool became not available as standalone resource for setting permissions. That way we have the principally new conception of resource utilization and control using resource pools. Hyper-V objects can be managed either using traditional method of straight control or using the new resource pool conception.

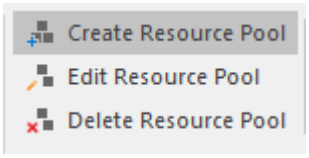
Creating, editing and deleting resource pool

To start creating the new resource pool either:

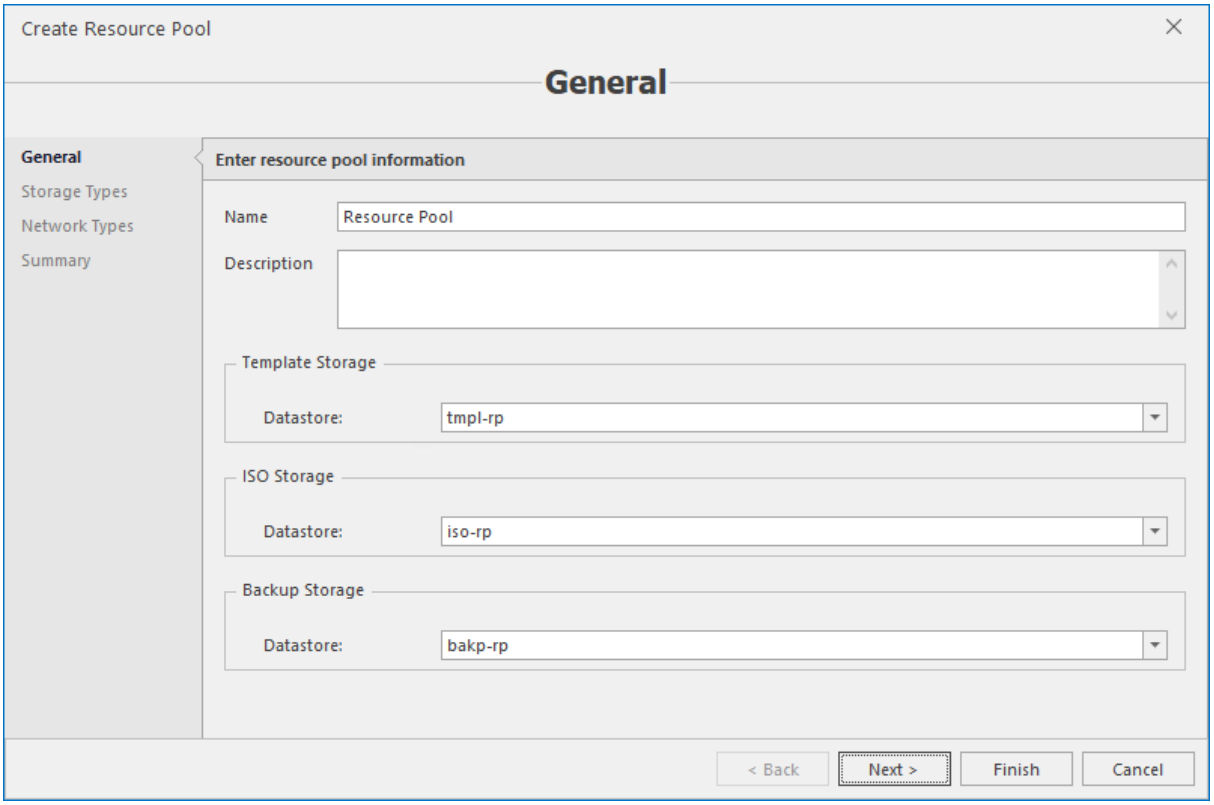
- In the **Hyper-V Management** plugin of Acronis Cloud Manager console press the **Create resource pool** button on the main ribbon:



- Right-click the existing resource pool (if it's been already created earlier) in the object tree and press the **Create resource pool** context menu item:



The **Create resource pool** wizard will be opened.



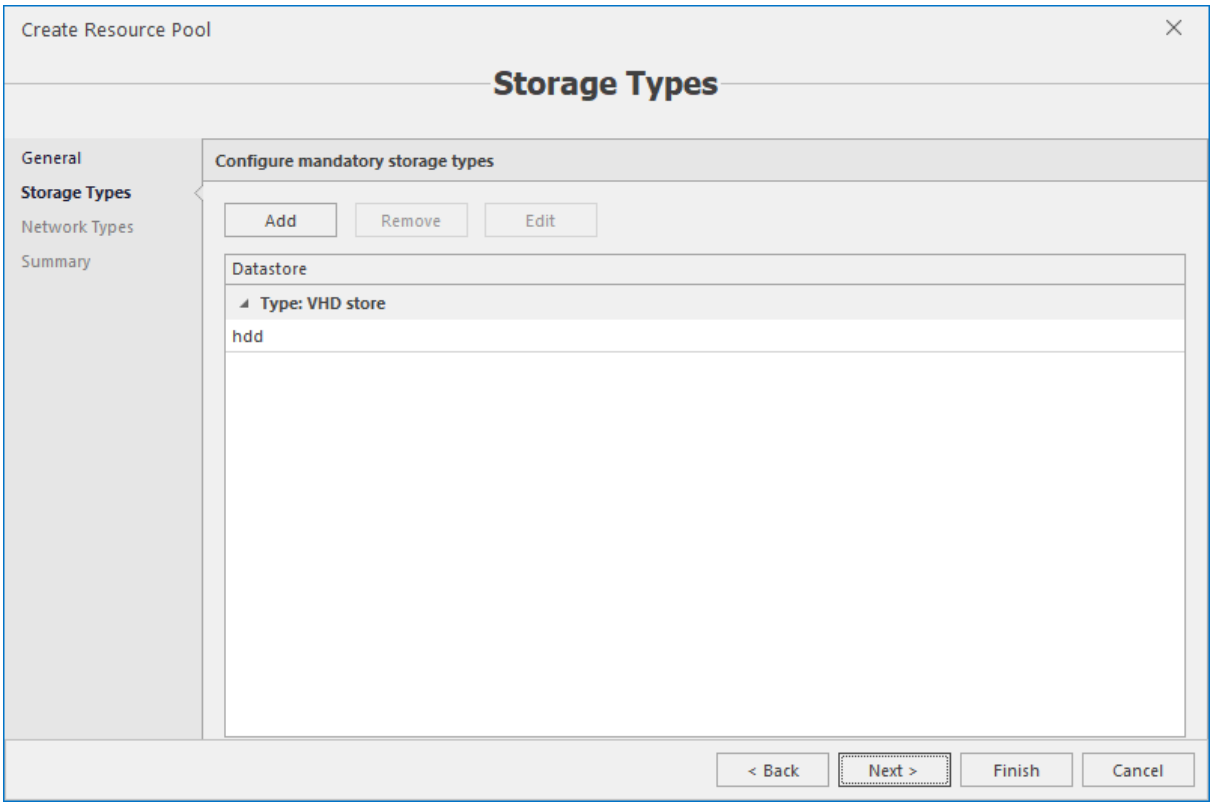
On the first page type the resource pool name, description (optional), and select storages for templates, ISO and backup files. Standard wizard to add the new datastore is available from drop down menu, if necessary.

Important

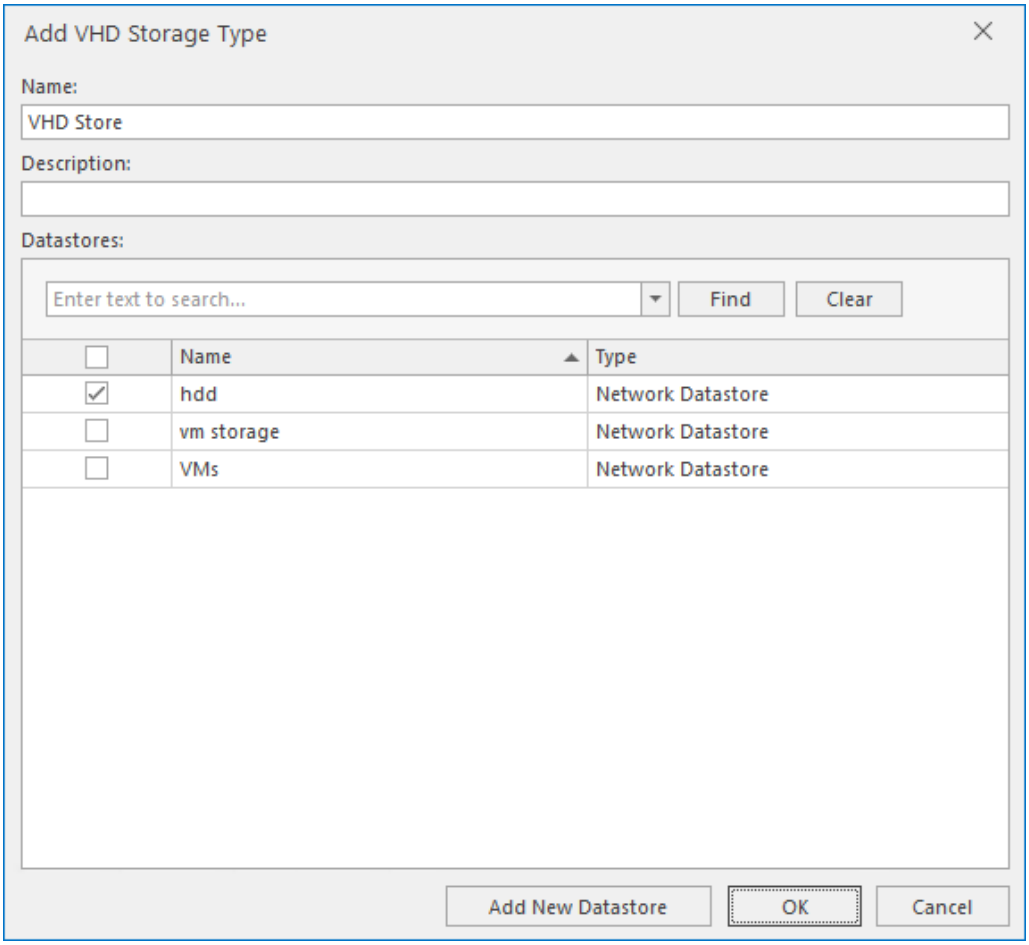
All resource pool storages must be registered as SMB type.

Click **Next**.

On the next page add the mandatory storage types:



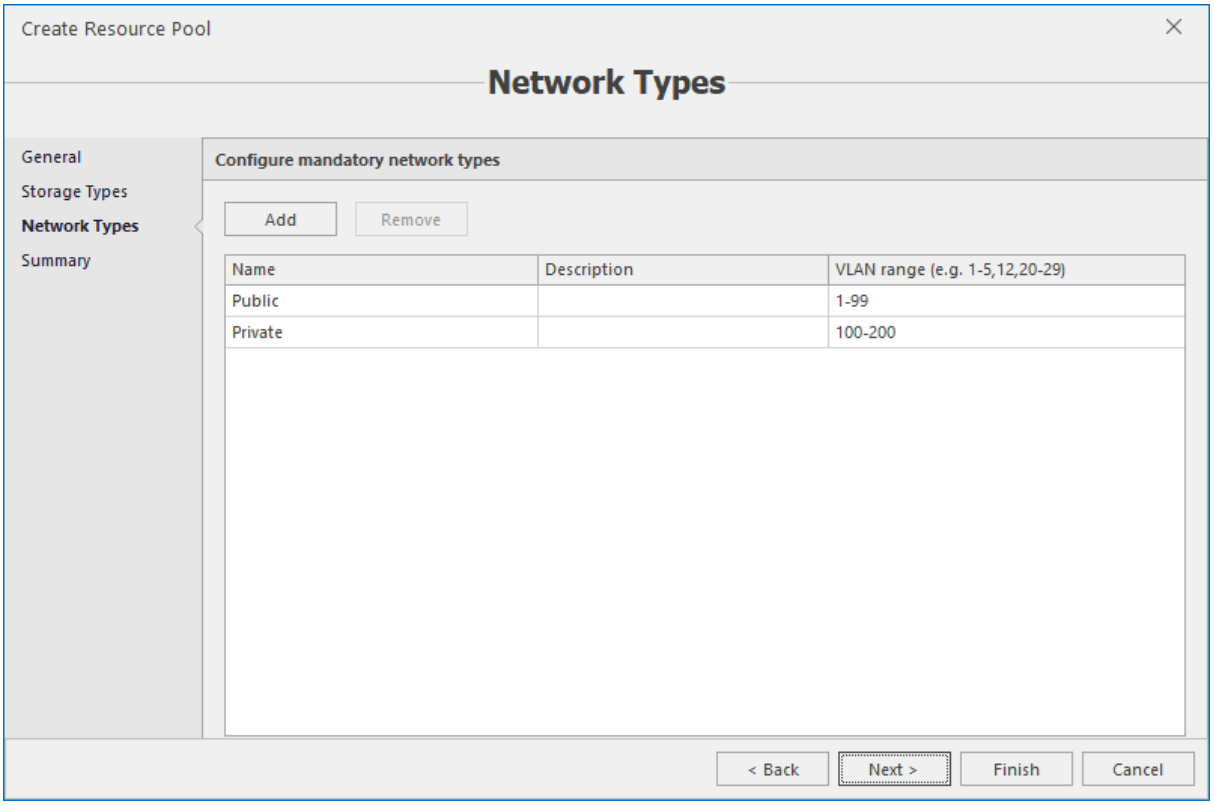
- Click the **Add** button. The **Add VHD storage type** dialog will be opened.



- Enter the name and, optionally, the decription for the storage type.
- Check the box(es) on the left side to select the required datastores from the list. Use the search filter for convenience on the large list.
- To add the new datastore, click the **Add new datastore** button to open the standard **Create virtual machine storage** wizard and then register the new storage there (please refer to the "Adding datastore" (p. 67) section above).
- Click **OK** to add the storage type.

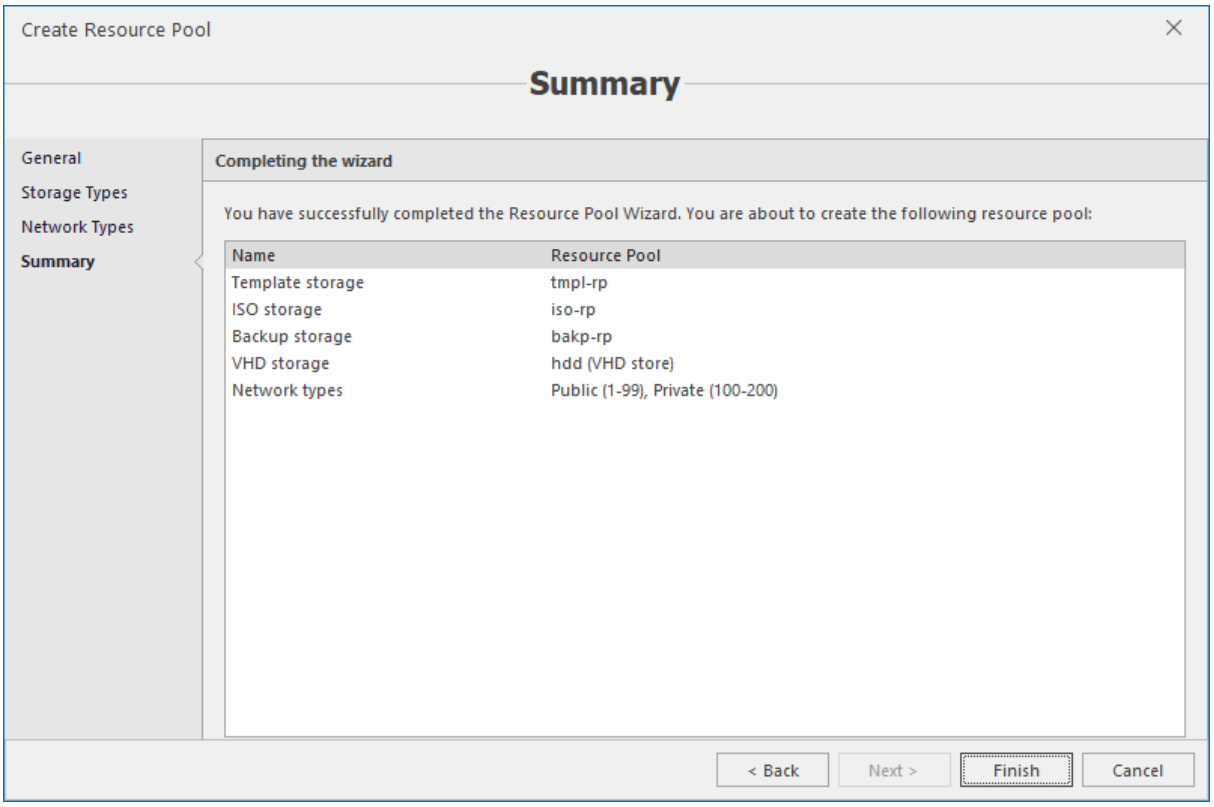
Click **Next**.

On the next page configure the mandatory network types:



- Click **Add** button to add the new network type.
- Type the network type name, description (optionally) and VLAN range (e.g. 1-5, 12, 20-29).
- To remove the network type, select it and click the **Remove** button.

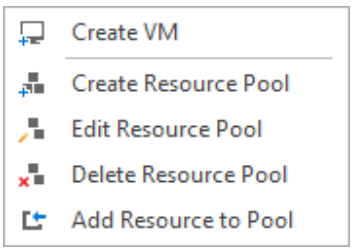
Click **Next**.



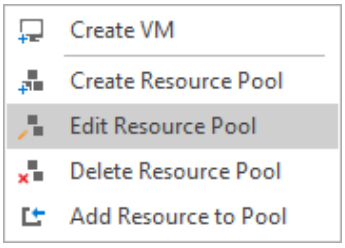
Review the summary and click **Finish**.

To edit the resource pool select it in the object tree and then either:

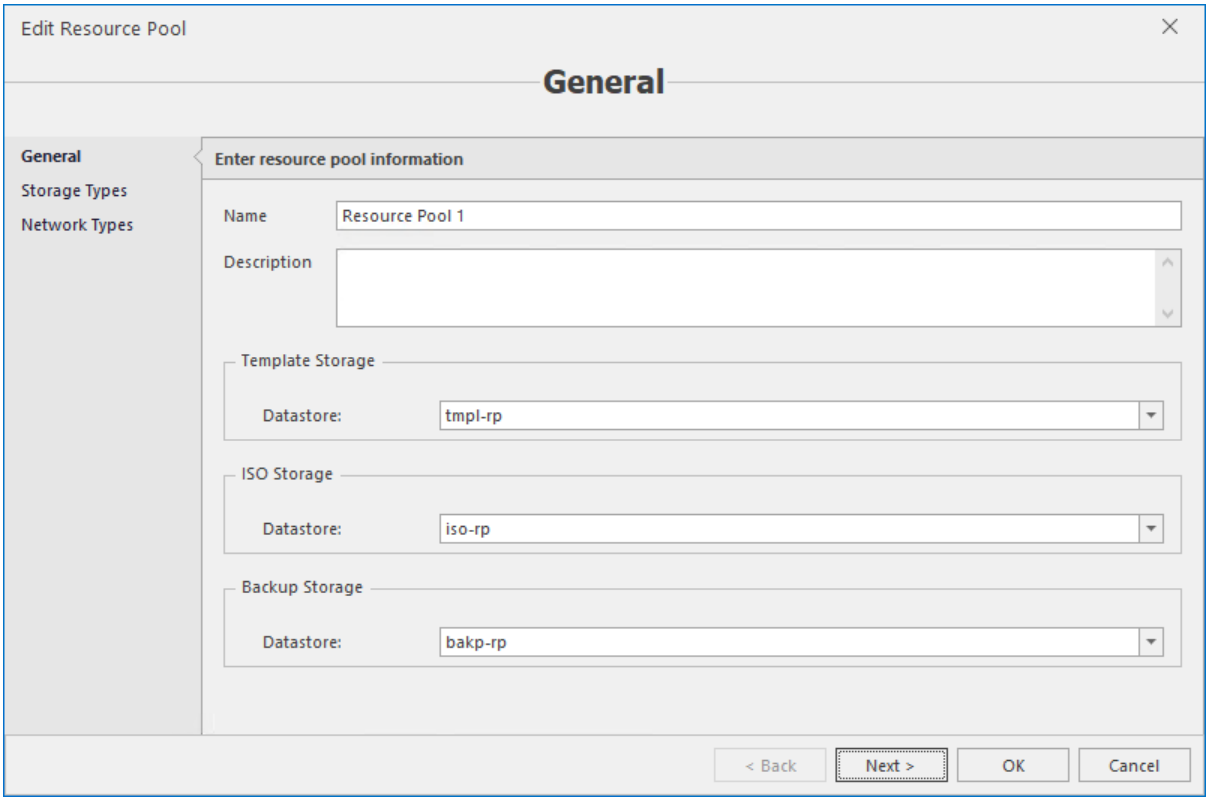
- Press the **Edit resource pool** button on the main ribbon:



- Right-click the resource pool and press the **Edit resource pool** context menu item:

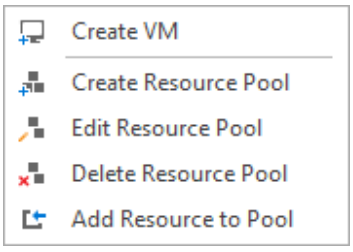


Edit resource pool parameters as required just like when you create it:

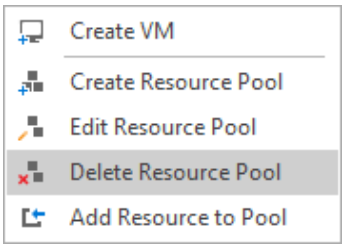


To delete resource pool select it in the object tree and then either:

- In the **Hyper-V Management** plugin of Acronis Cloud Manager console press the **Delete resource pool** button on the main ribbon:



- Right-click the existing resource pool (if it's been already created earlier) in the object tree and press the **Delete resource pool** context menu item:



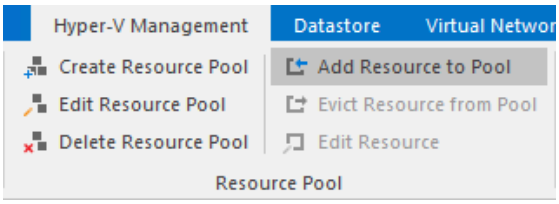
Note

Resource pool that contains resources cannot be deleted.

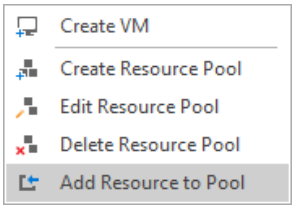
Adding and evicting resource to/from pool

To add resource to pool either:

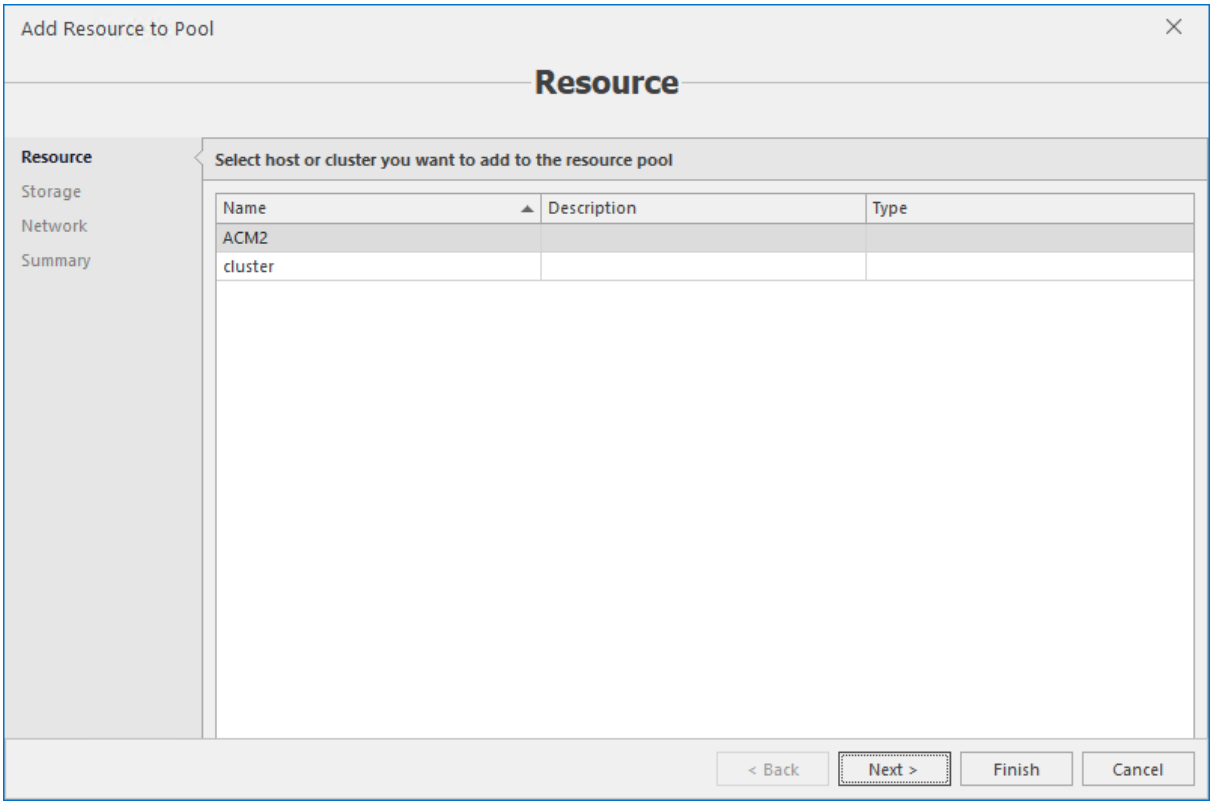
- In the **Hyper-V Management** plugin of Acronis Cloud Manager console select the target resource pool and press the **Add resource to pool** button on the main ribbon:



- Right-click the target resource pool in the object tree and press the **Add resource to pool** context menu item:

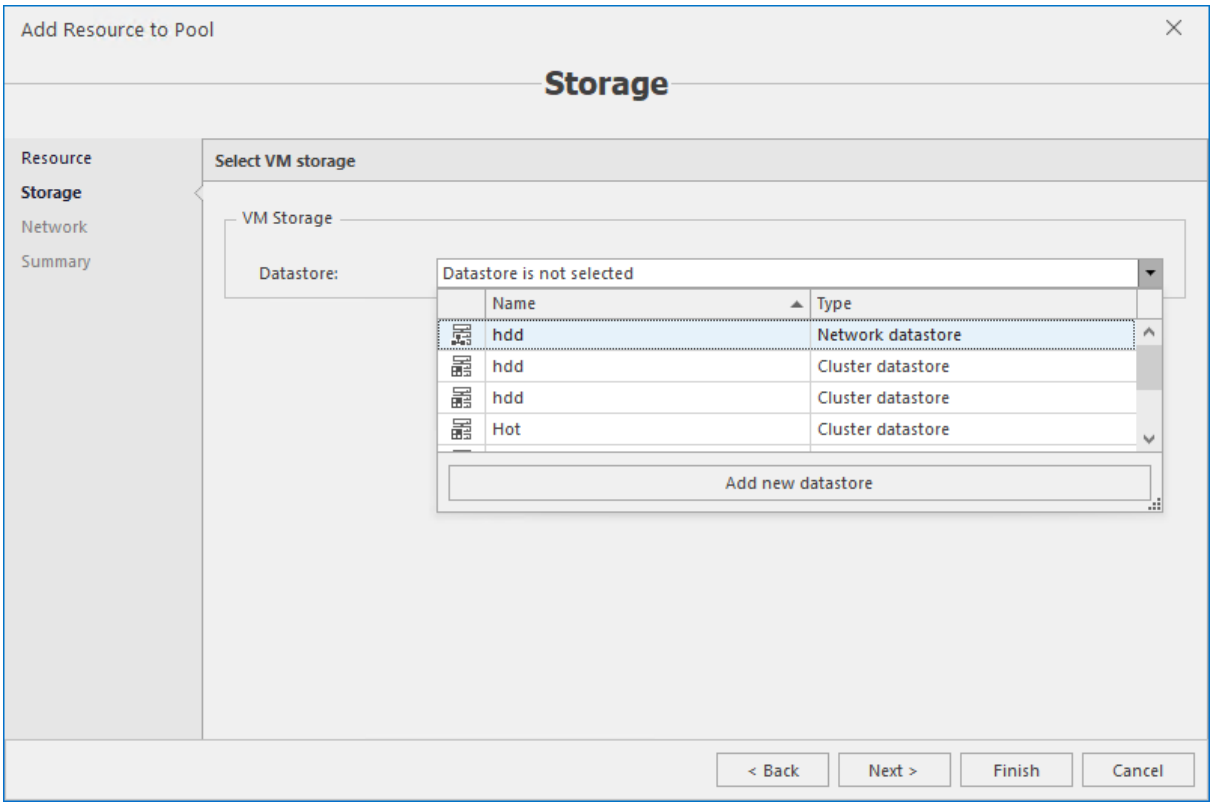


The **Add resource to pool** wizard will be opened.

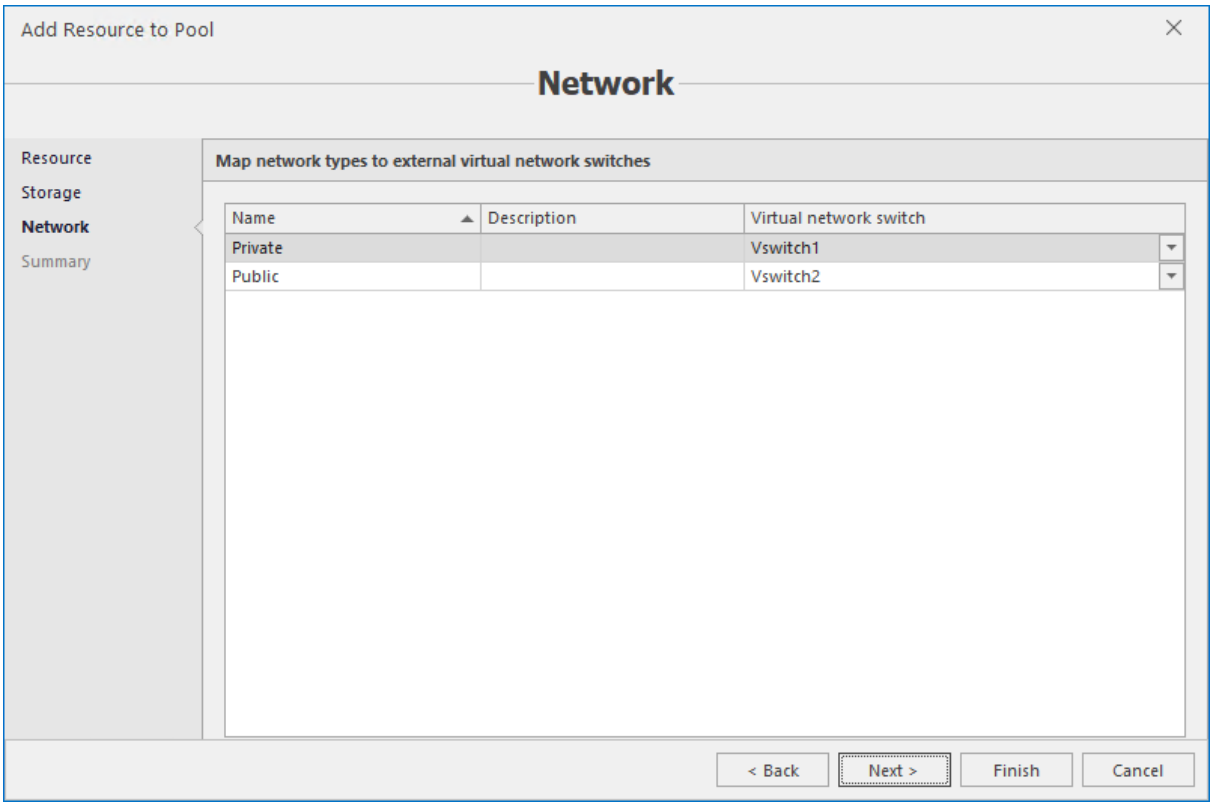


On the first page select the resource from the list of available objects, enter description (optional), and click **Next**.

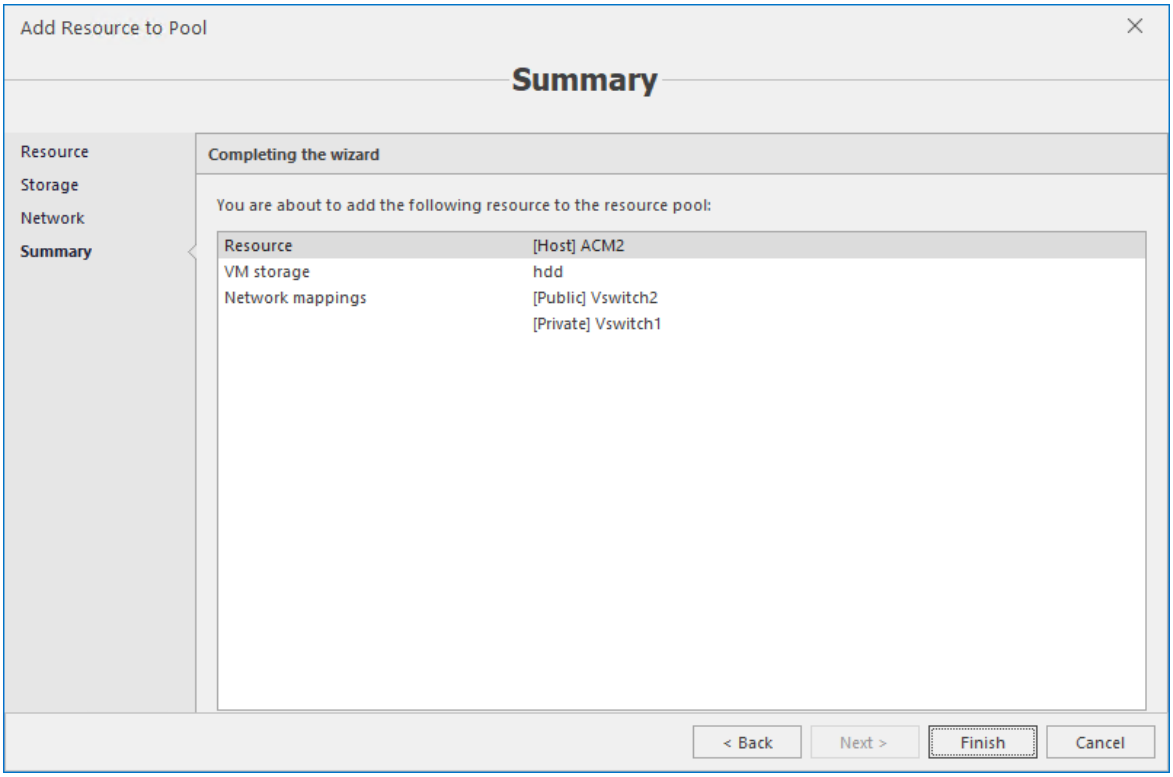
On the **Storage** page select the datastore form the drop-down list or add the new datastore, using standard wizard that can be called with the **Add new datastore** button at the bottom of the drop-down menu. Click **Next**.



On the **Network** page type the names and, optionally, descriptions for mandatory virtual networks and select the external virtual switches from the drop-down menu to map them to these virtual networks. Click **Next**.

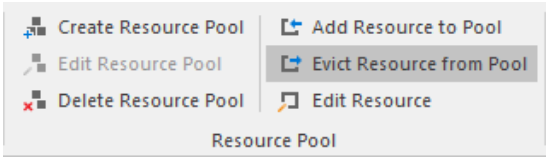


Review the summary and click **Finish**.

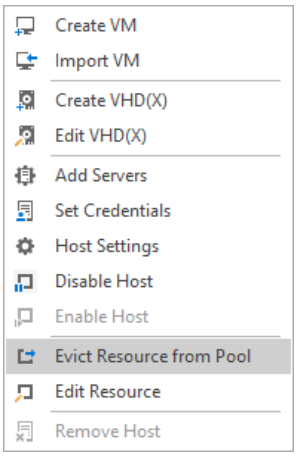


To evict the resource from pool, select it in the object tree and then either:

- Press the **Evict resource from pool** button on the main ribbon.



- Right-click the target resource and press the **Evict resource from pool** context menu item.



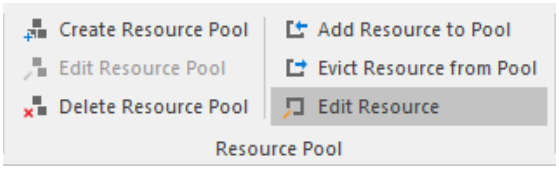
Note

Resource that is assigned to a tenant cannot be evicted from the pool.

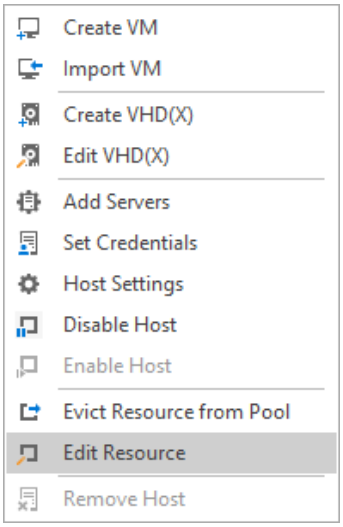
Editing resource

To edit the resource, select it in the object tree and then either:

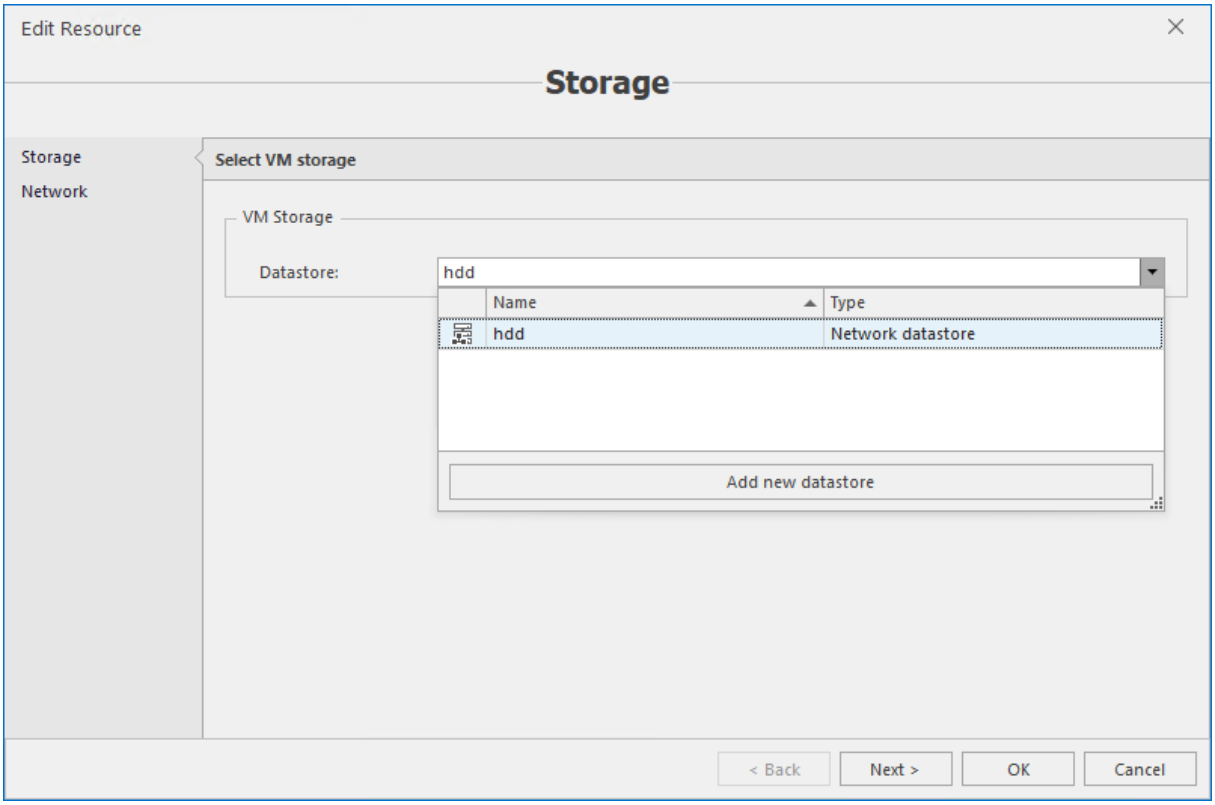
- Press the **Edit resource** button on the main ribbon:



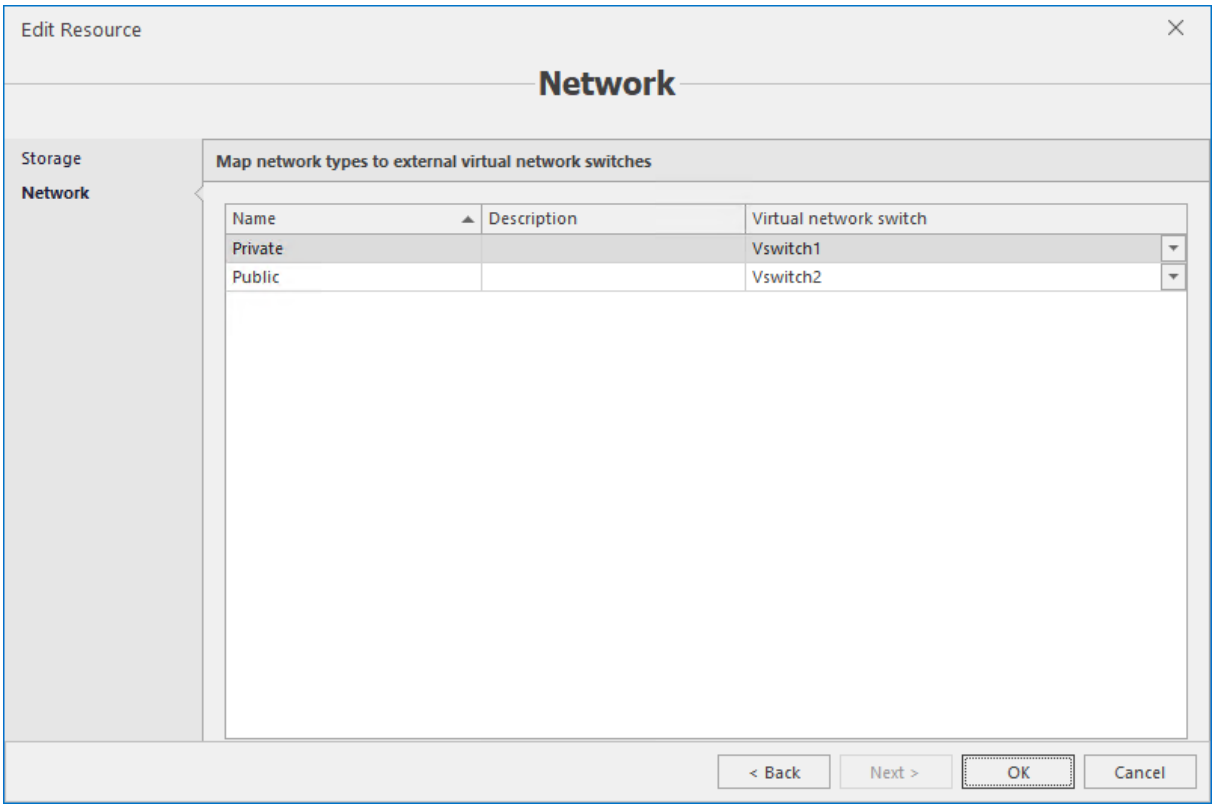
- Right-click the target resource and press the **Edit resource** context menu item:



The **Edit resource** wizard will be opened.



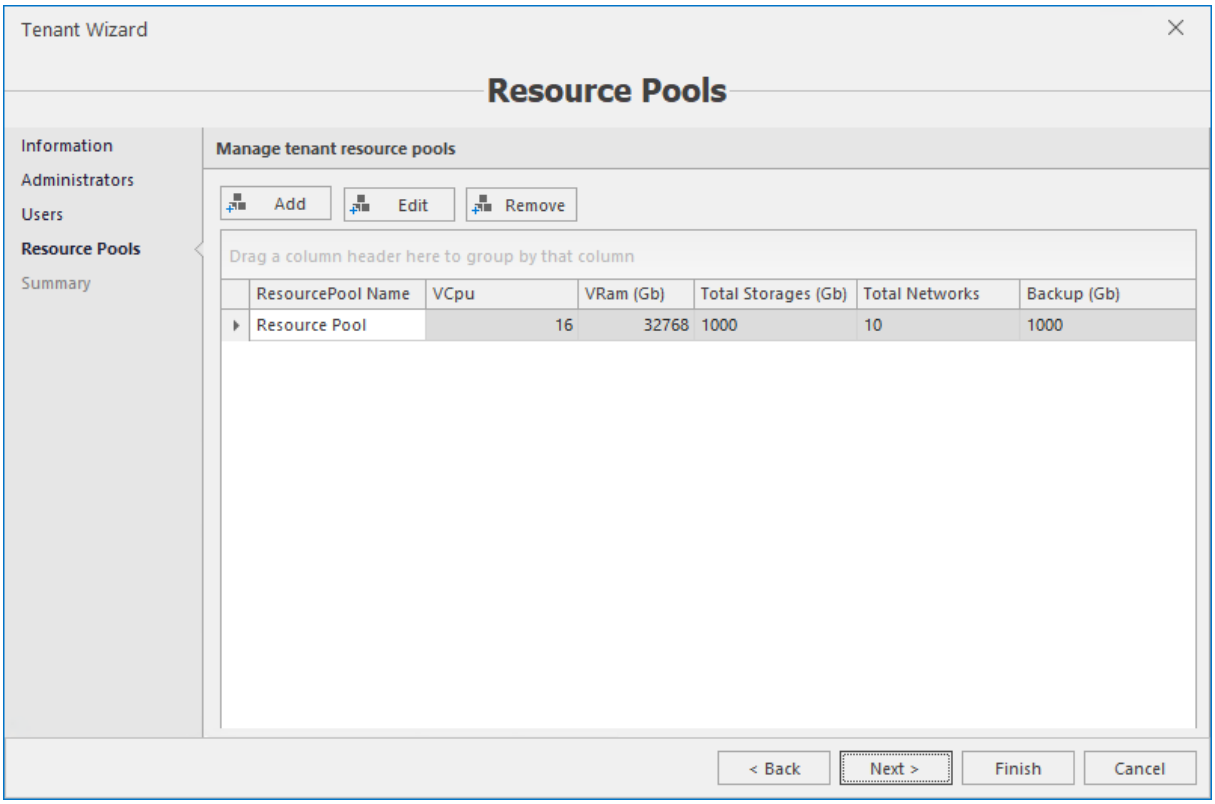
On the **Storage** page select the datastore form the drop-down list or add the new datastore, using standard wizard that can be called with the **Add new datastore** button at the bottom of the drop-down menu. Click **Next**.



On the **Network** page select the external virtual switches from the drop-down menu to re-map them to the virtual networks. Click **OK**.

Allocating resource pool to a tenant

Resource pool allocation to tenants is done in the standard way just like traditional resources allocation when the tenant is created or edited using the **Tenant** wizard in the **Administration** plugin.



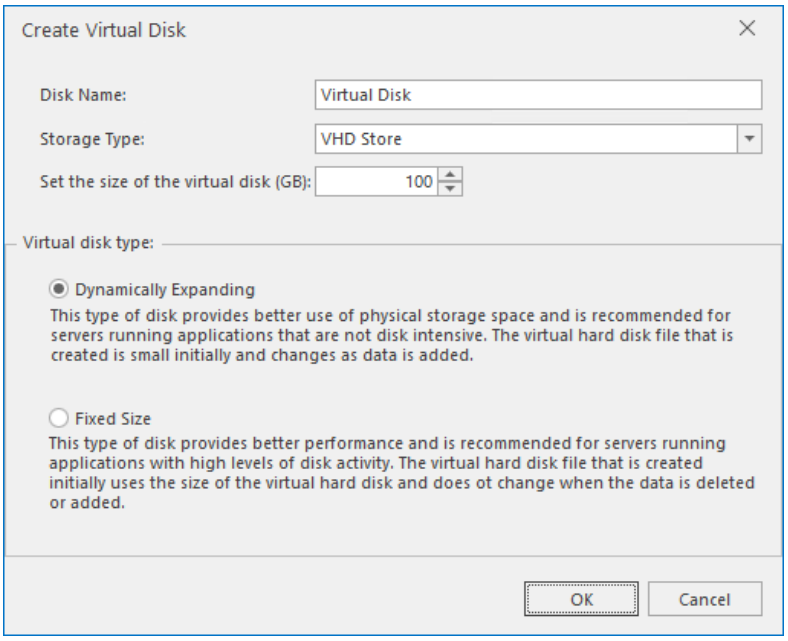
Please refer to the "Tenants" (p. 51) section above for details.

Operations in the resource pool

Operations in the resource pool include creating, editing and removing virtual disks, virtual networks and virtual machines. These operations are performed in the **Hyper-V management** plugin and can be done by both global users (admins) and tenant users (admins), who have rights to access the resource pool.

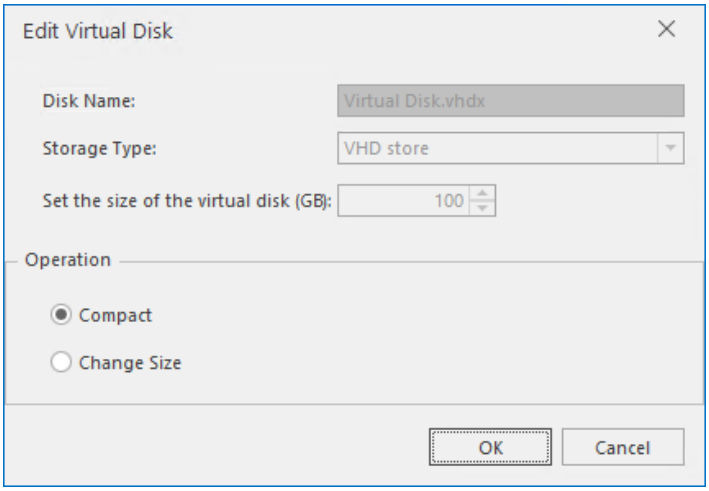
To create VHD(x) in the resource pool:

1. In the **Datastore** tab select the resource pool (or exact datastore) in the object tree and click the **Create virtual disk** button on the main ribbon.
2. Configure parameters for the VHD(x):



3. Type the VHD(x) name, select the storage type, set the VHD(x) size and type. Click **OK**.

To edit VHD(x) in the resource pool, select it and click the **Edit virtual disk** button. Then alter the VHD(x) parameters in the **Edit virtual disk** dialog:

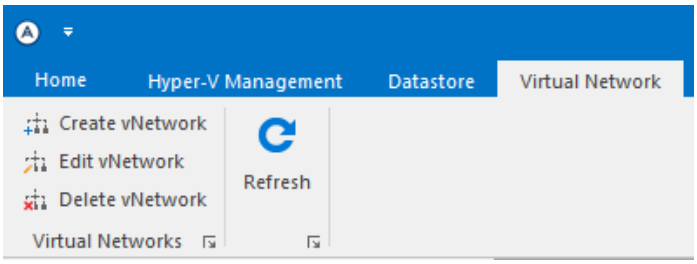


- Choose the operation: **Compact** or **Change size**.
- If the **Change size** operation is selected, set the new size of the VHD above.
- Click **OK**.

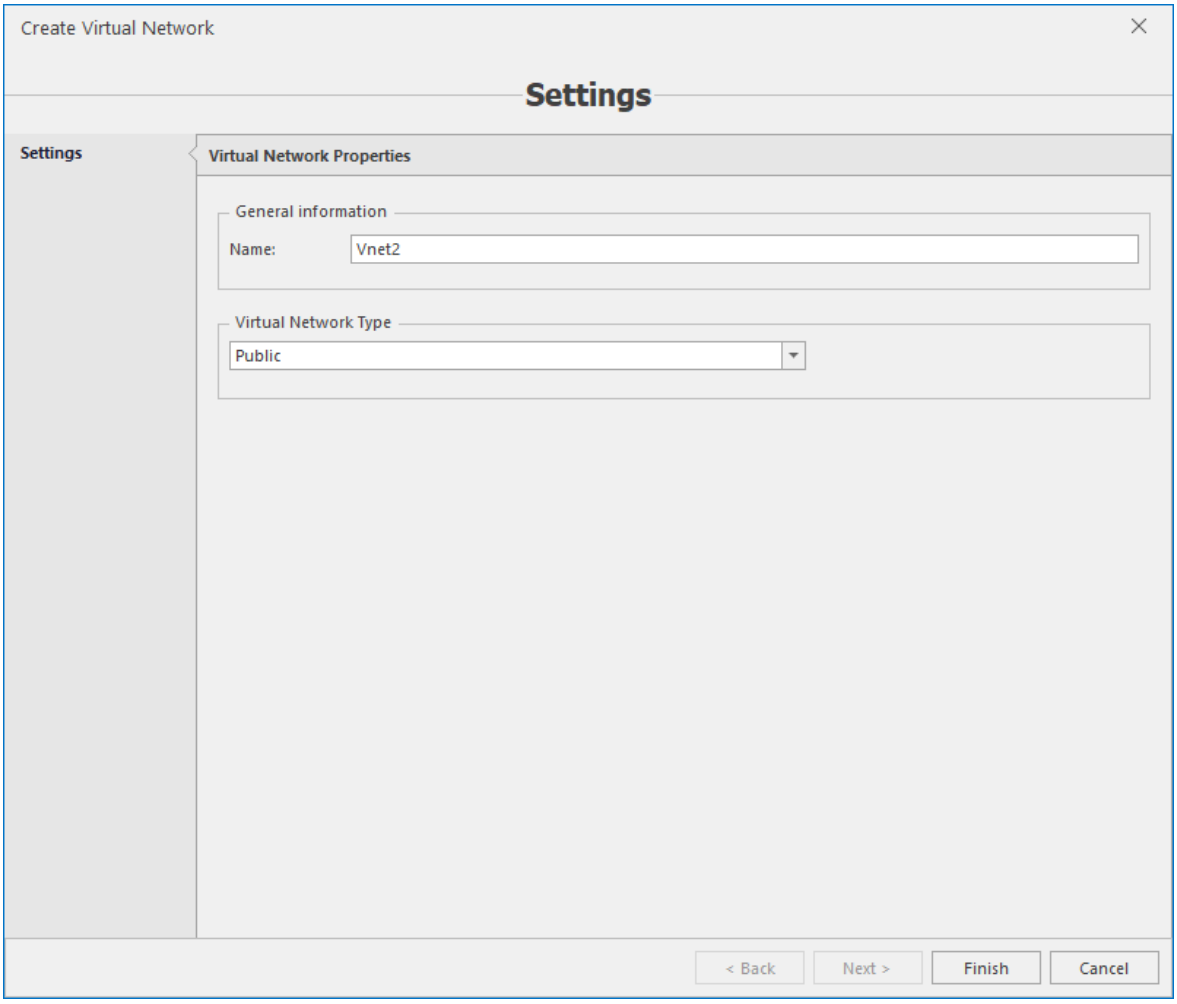
To delete VHD(x) select it and click the **Delete virtual disk** button. Confirm the operation.

To create the virtual network in the resource pool:

1. In the **Virtual network** tab select the resource pool in the object tree and click the **Create vNetwork** button on the main ribbon:



2. Configure parameters for the new virtual network in the **Create virtual network** wizard:



   - Type the vnet name.
   - Select the vnet type from the drop down menu.
3. Click **Finish**.

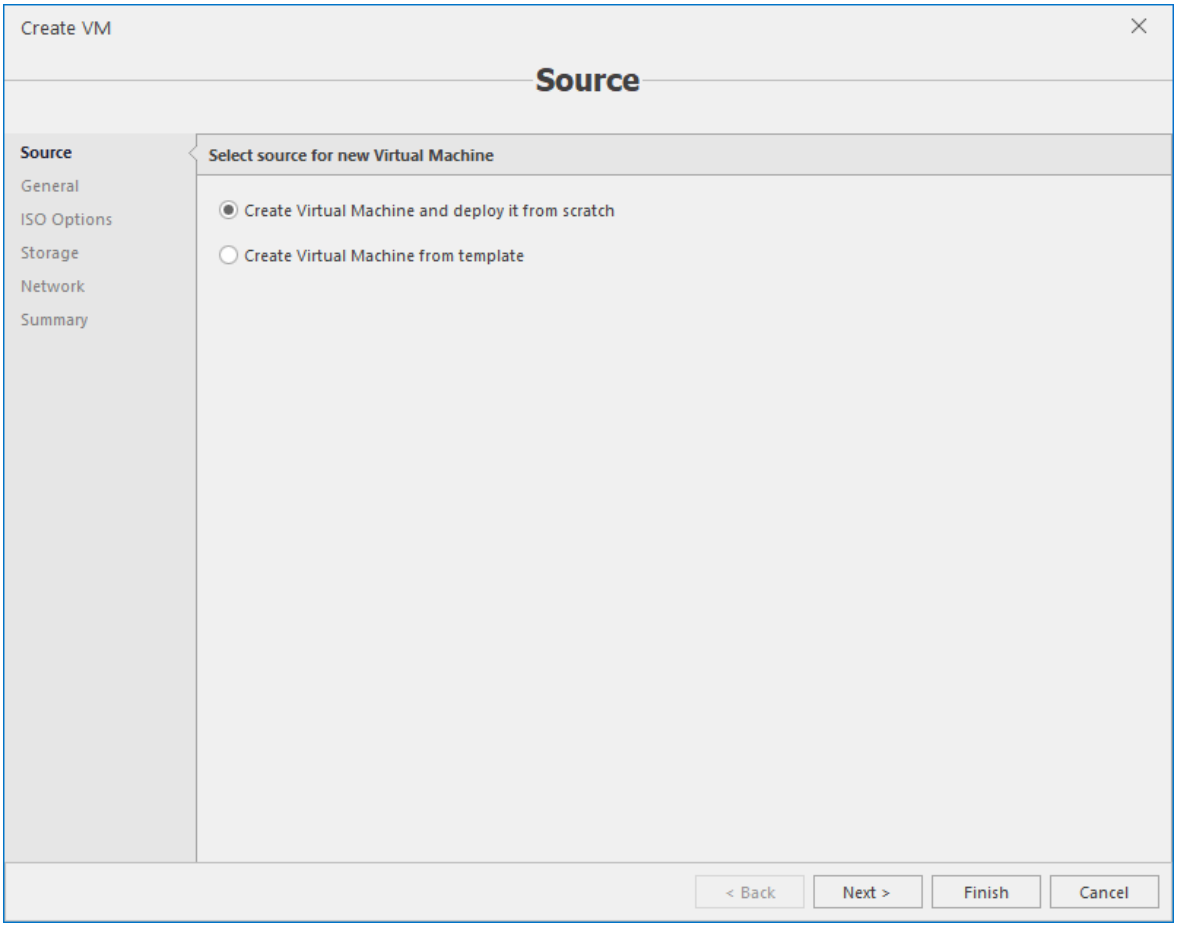
To edit the virtual network, select it and click the **Edit vNetwork** button. Then alter the vnet parameters just like you done when creating virtual network.

To delete the virtual network, select it and click the **Delete vNetwork** button. Confirm the operation.

To create the new resource pool VM:

1. In the **Hyper-V management** tab select the resource pool in the objet tree and click the **Create VM** button on the main ribbon or the corresponding context menu command.

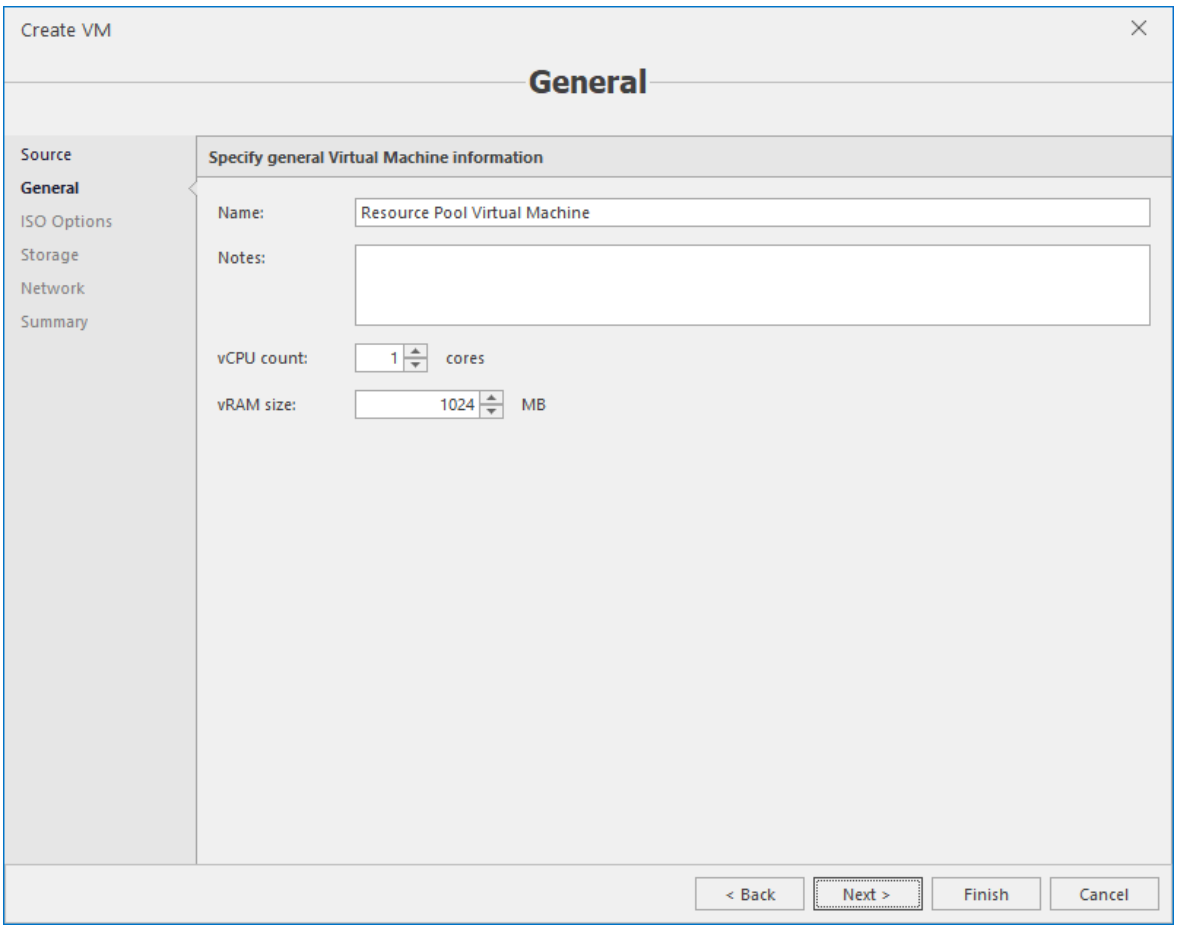
2. On the first page of the **Create VM** wizard select the source for the new virtual machine:



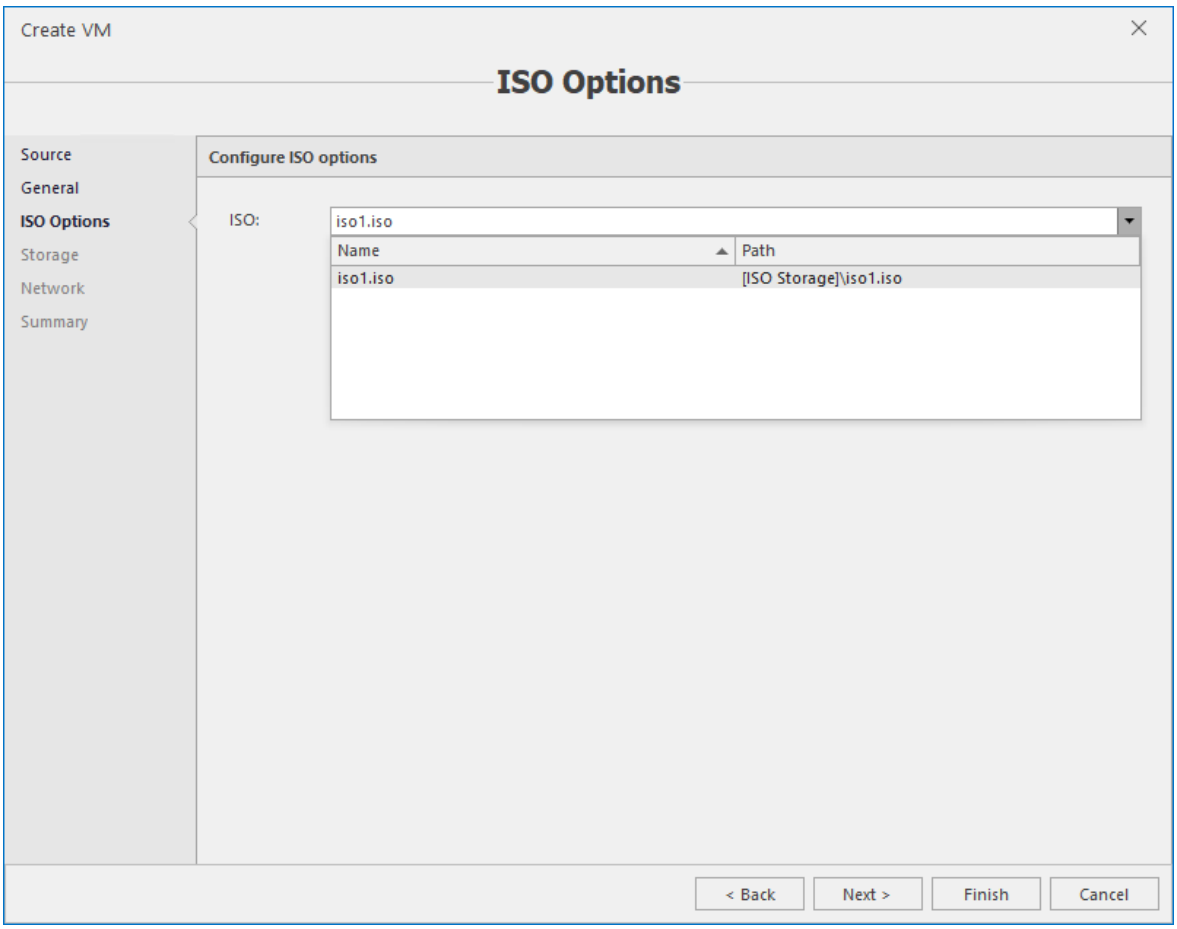
- **Create virtual machine and deploy it from scratch** - to create the new VM with your own parameters.
- **Create virtual machine from template** - to create the new VM using stored VM template.

Click **Next**.

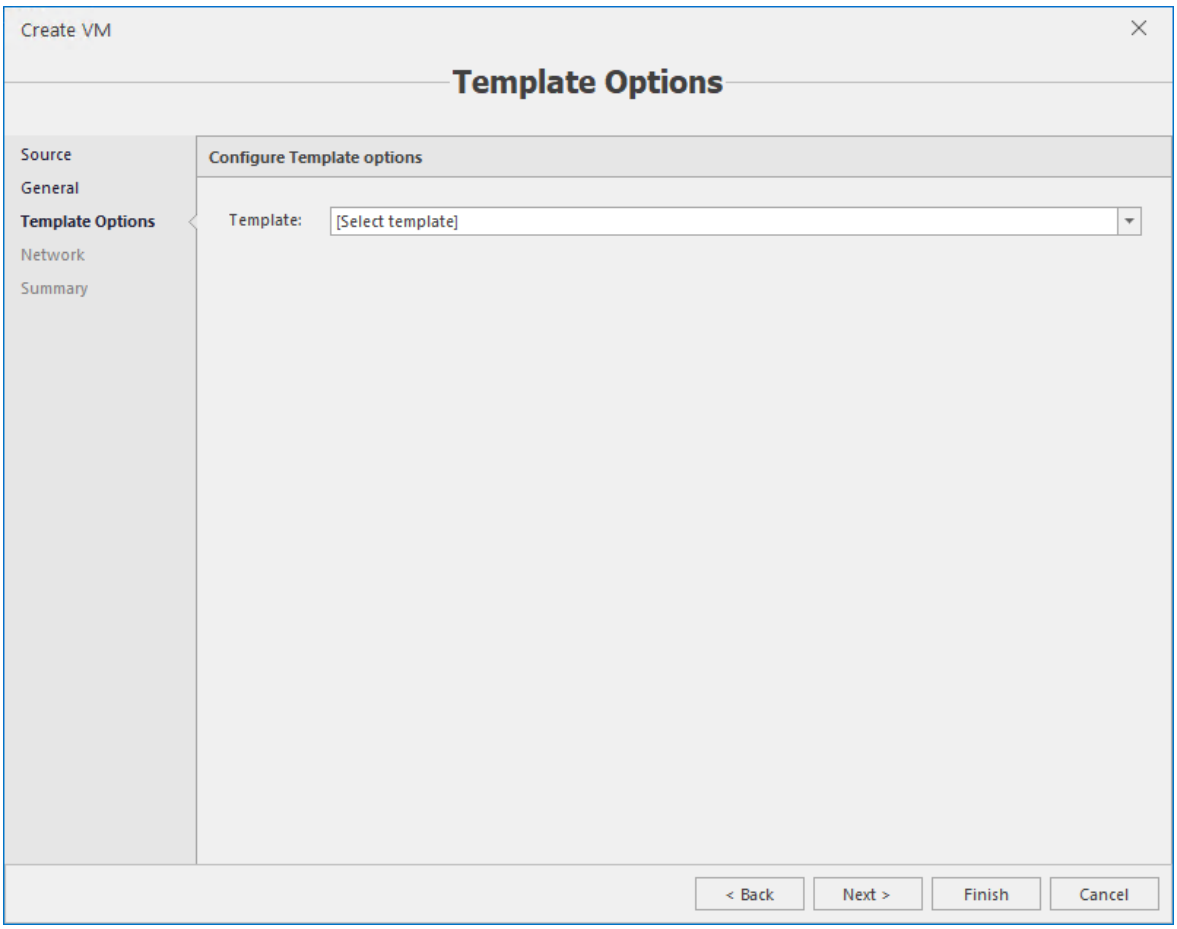
3. On the **General** page specify common VM information: name, notes (optionally), set vCPU cores count and vRAM size in MB. Clik **Next**.



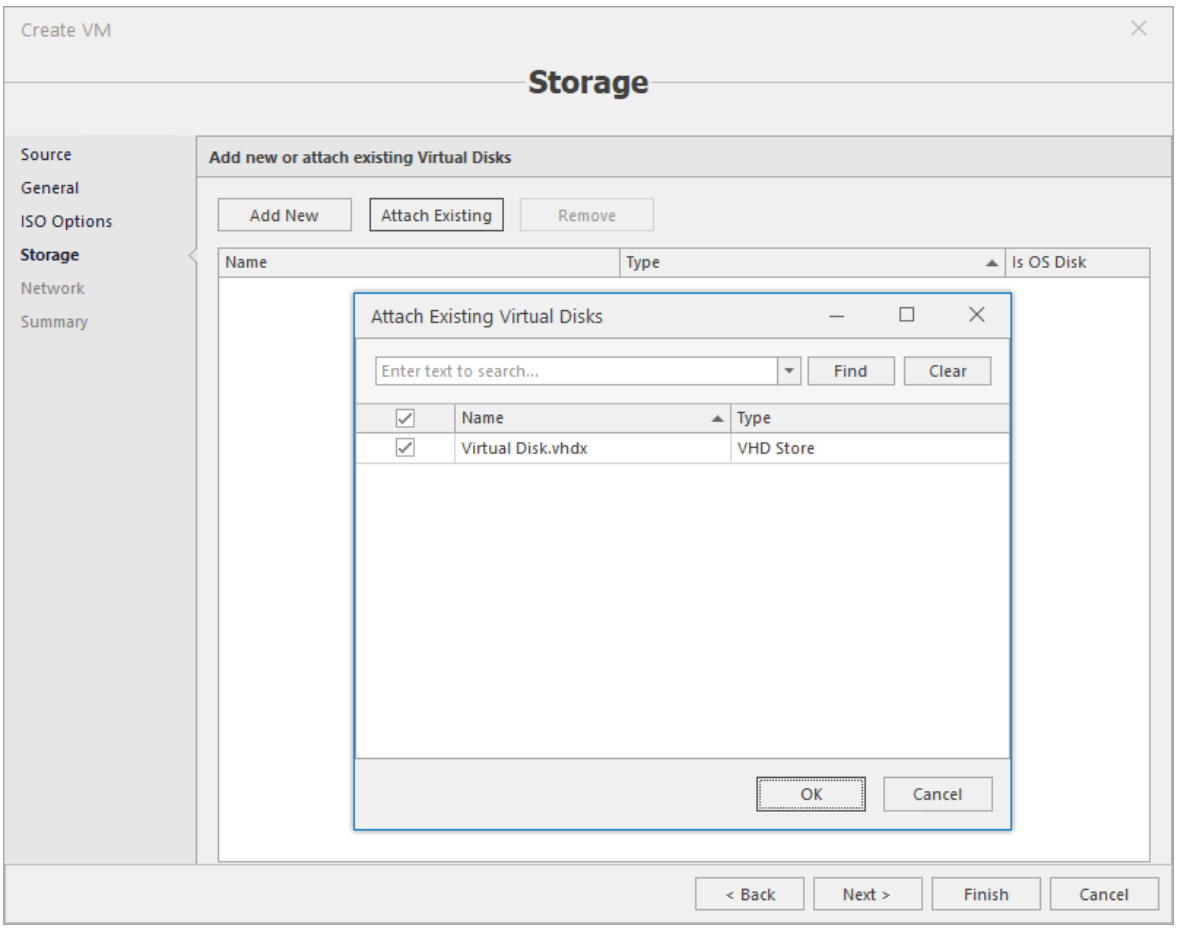
4. [If creating VM from scratch] On the **ISO options** page select the ISO from the drop-down list. It should be placed into the configured resource pool ISO storage in advance. Click **Next**.



5. [If creating VM from template] On the **Template options** page select the template from the drop-down list. It should be placed into the configured resource pool template storage in advance. Click **Next**.

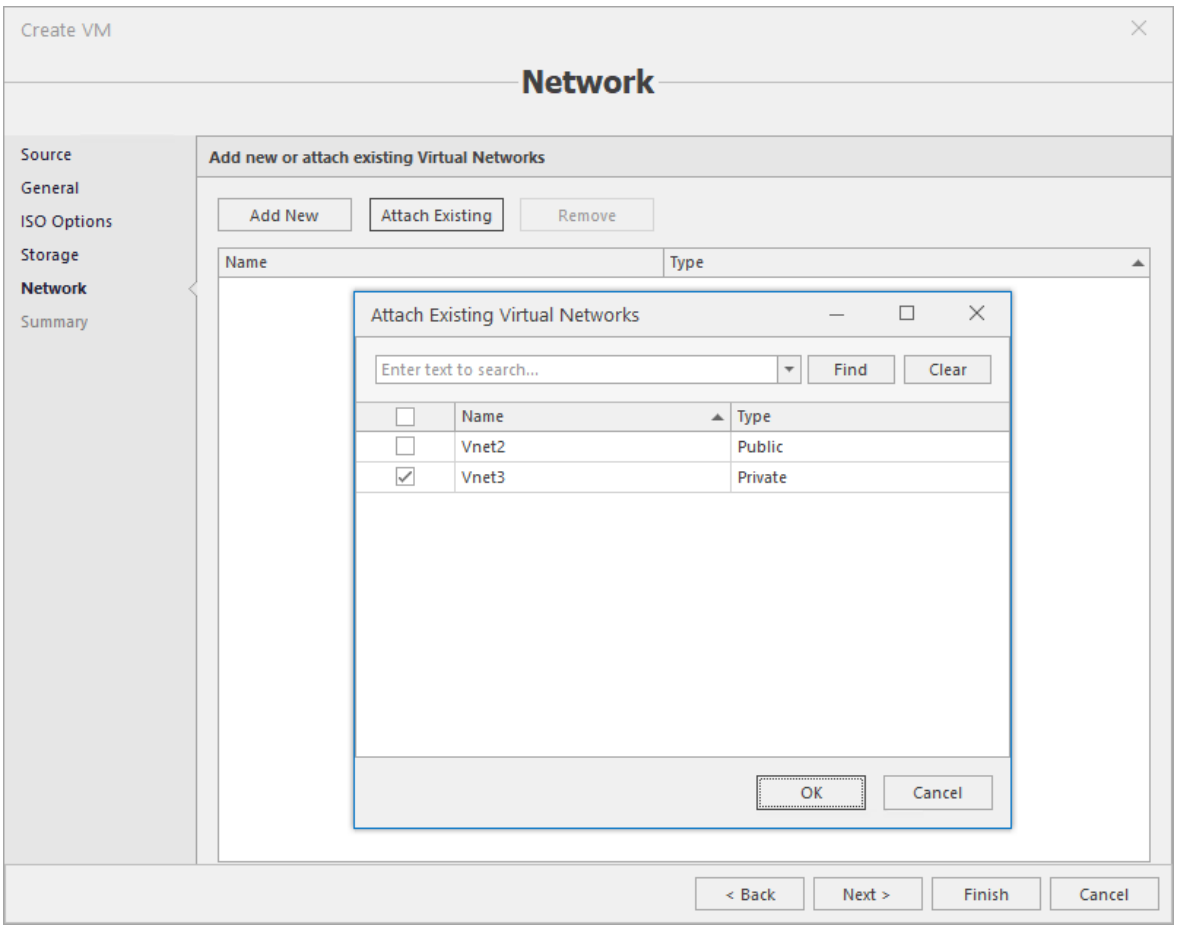


6. [If creating VM from scratch] On the **Storage** page add VM disks. You may both create new disk(s) or select and attach existing one(s):



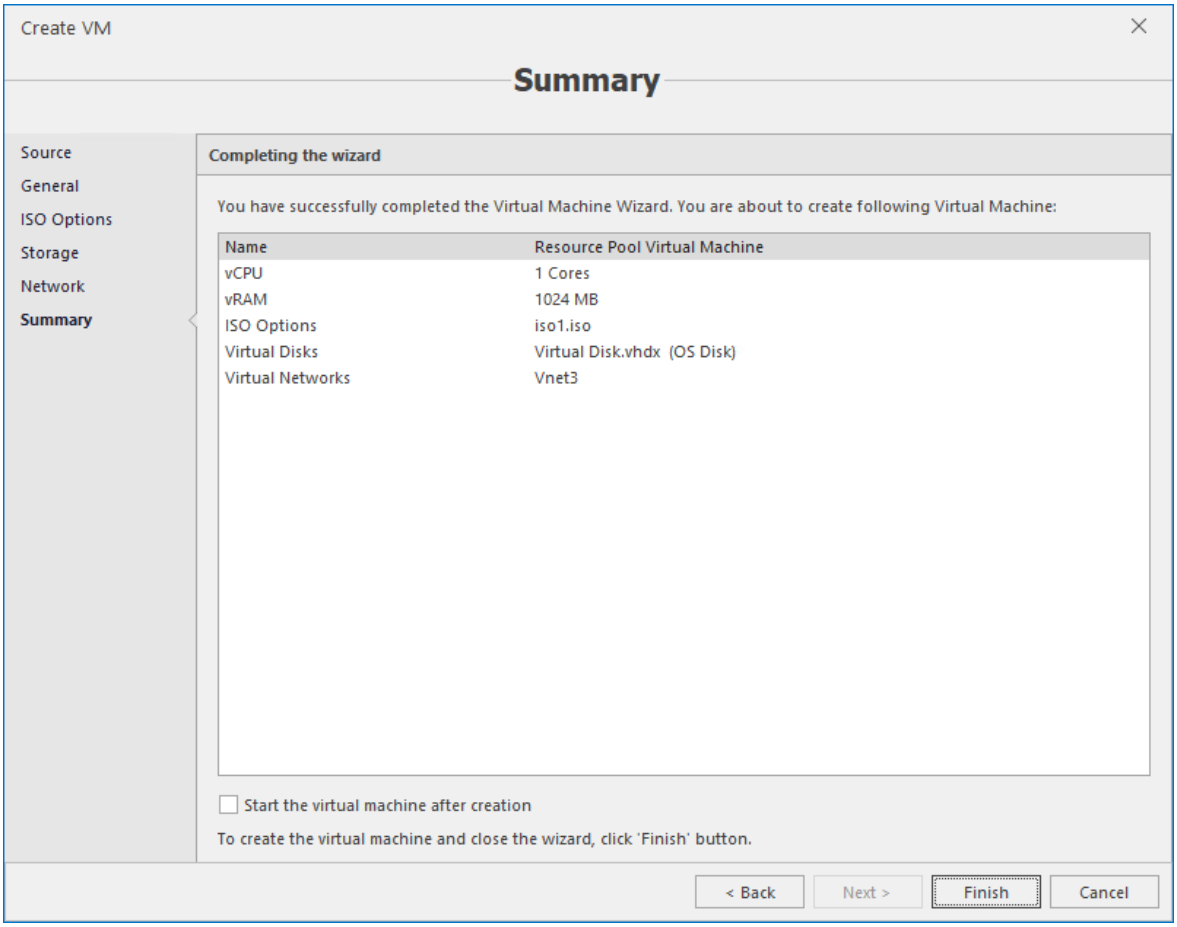
If you add several disks, set one of them as OS disk in the **Is OS disk** column. Click **Next**.

7. On the **Network** page set VM network connections - add virtual network adapters. You may both create new network(s) or select and attach existing one(s):



Click **Next**.

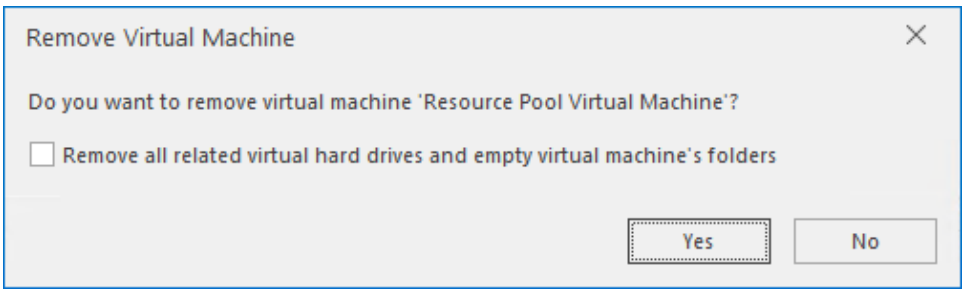
8. Review the summary:



If you would like VM to be started after the creation, enable the corresponding check box in the lower part of the page. Click **Finish**.

To edit VM settings, select it in the objet tree and click the **Settings** button on the main ribbon or the corresponding context menu command. Then edit VM parameters as required in the similar wizard as described above.

To delete VM, select it in the object tree and click the **Delete** button on the main ribbon or the corresponding context menu command. Then confirm the operation and, if you would like to delete all VM configuration files and disks, enable the corresponding option:

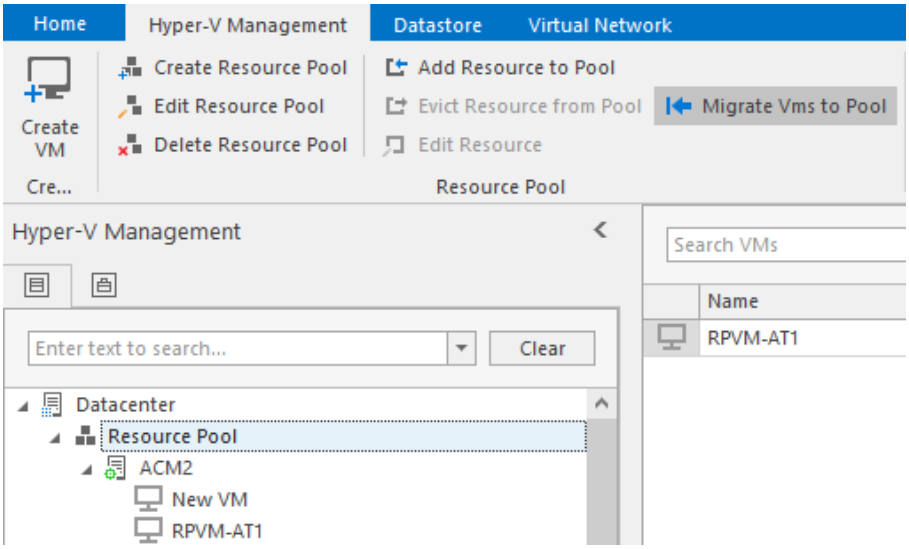


Migrating VMs to pool

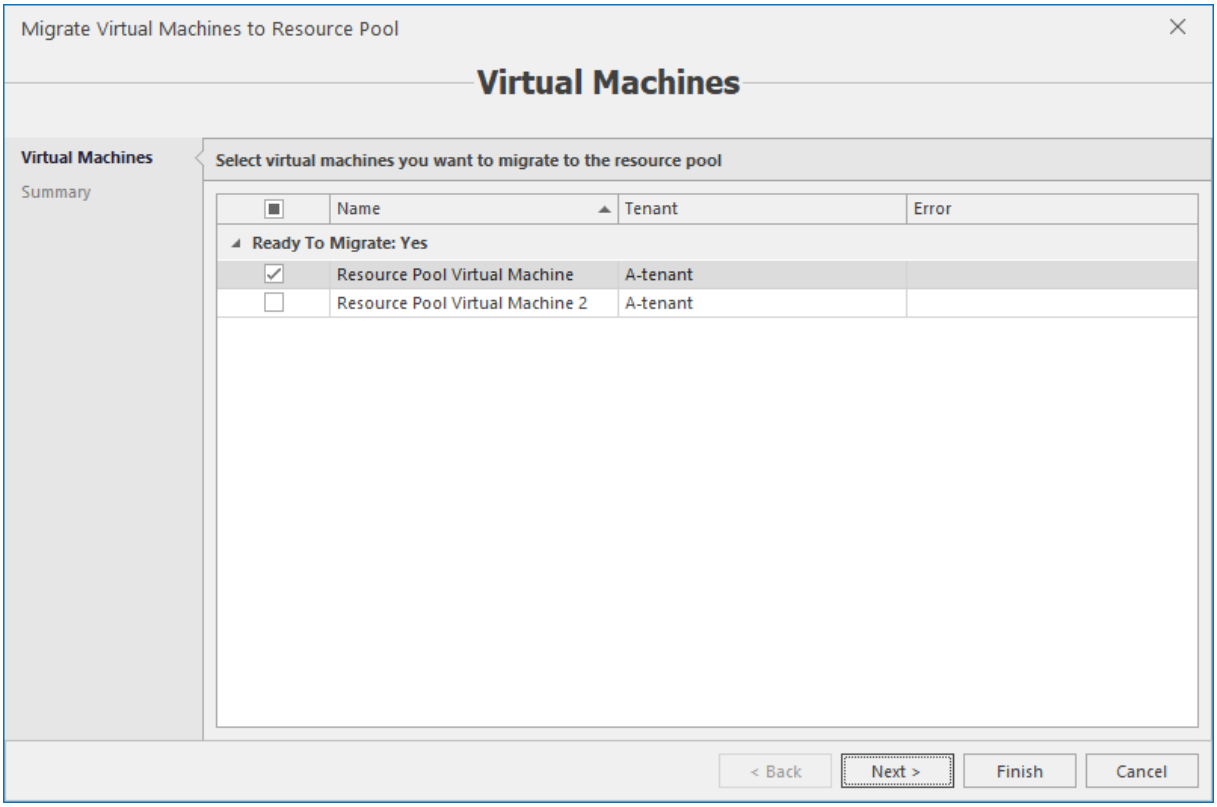
Migrating VMs to the resource pool is intended to provide the ability for enterprises to migrate the existing tenant VMs to the new resource management scheme, which were managed by the classic resource management mechanism before the new resource pool conception had been introduced in the product. It is possible on the following conditions:

- Target VM should be assigned to the tenant.
- Target resource pool should be assigned to tenant (with the set quota).
- VM should reside on the host or cluster, added to the target resource pool.
- VM configuration files and VHD(s) should be placed in the resource pool storage.

To migrate VMs to the resource pool, select the target resource pool or a host/cluster in the object tree and then press the **Migrate VMs to pool** button on the main ribbon:

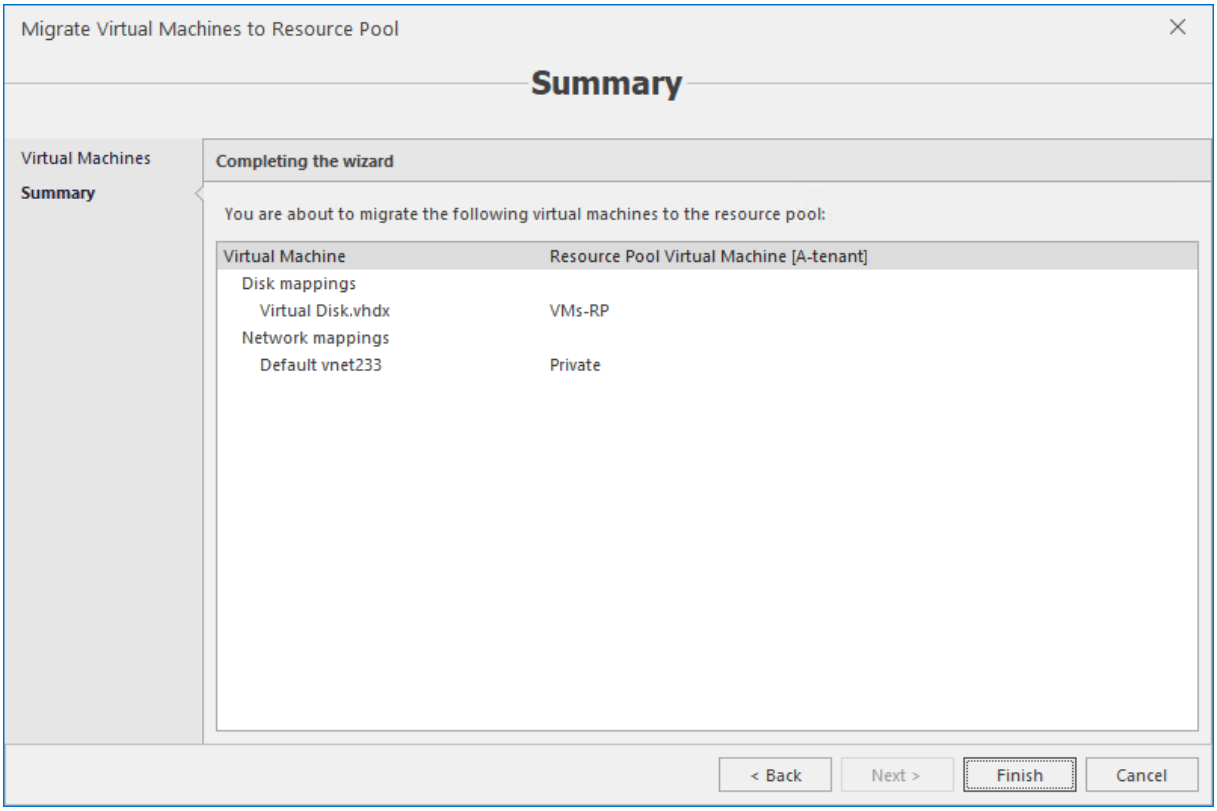


On the **Virtual machines** page of the **Migrate virtual machines to resource pool** wizard select the VMs, which you need to migrate to the resource pool:



Click **Next**.

Review the summary and click **Finish**:

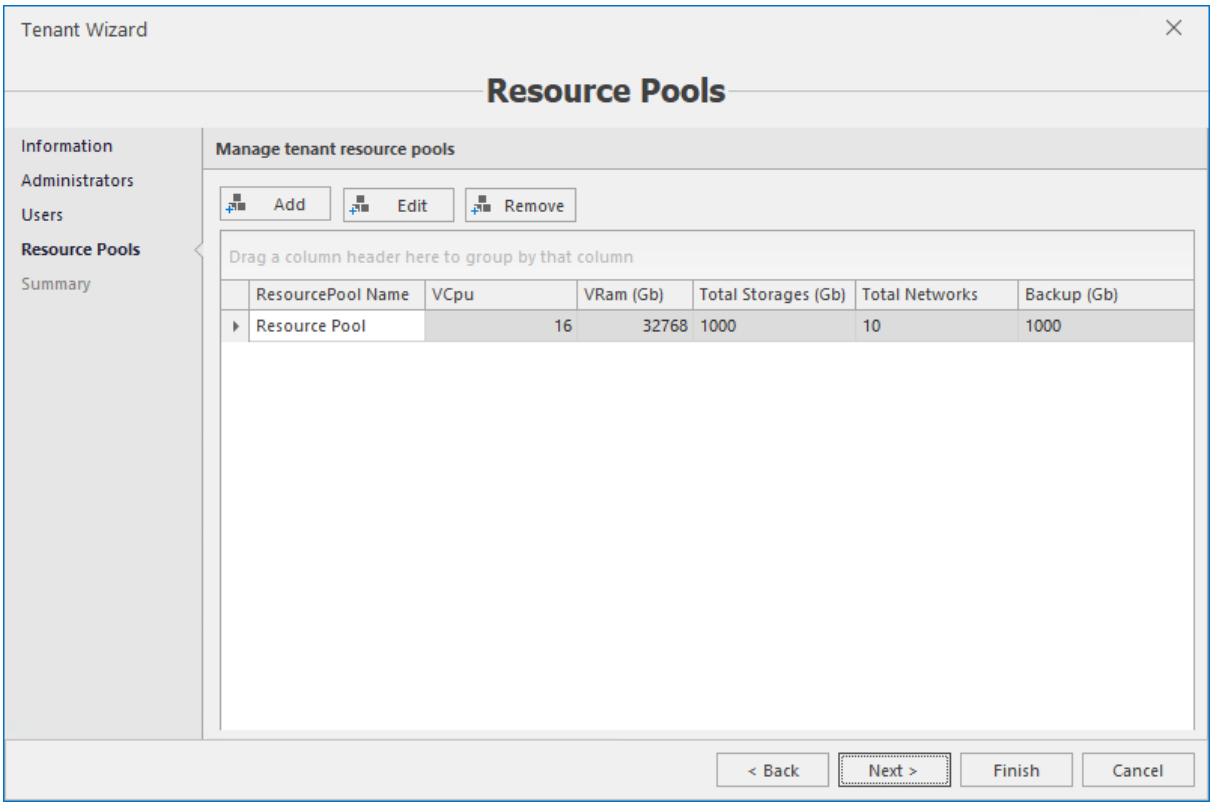


Quotas

Quotas are tenant specific settings determining how many resources can be allocated for the tenant per assigned resource pool. Also quotas are used in capacity planning of resource pools.

Setting quotas

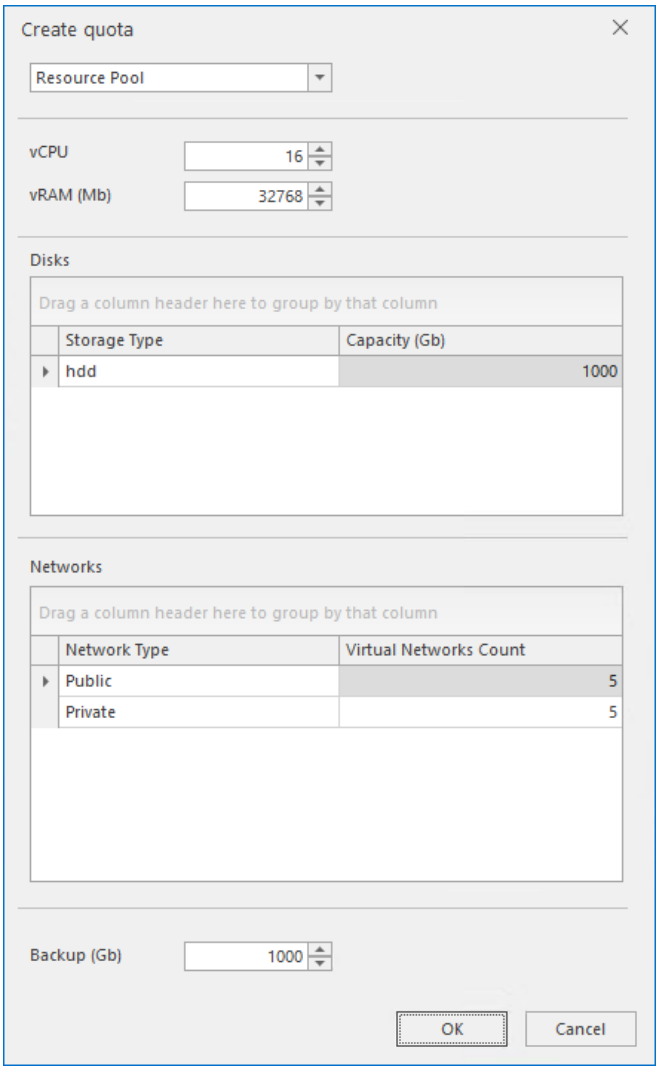
Administrator can set quotas on the **Resource pools** page of the **Tenant** wizard when adding the resource pool to the tenant:



Each selected resource pool are configured with its own quota settings:

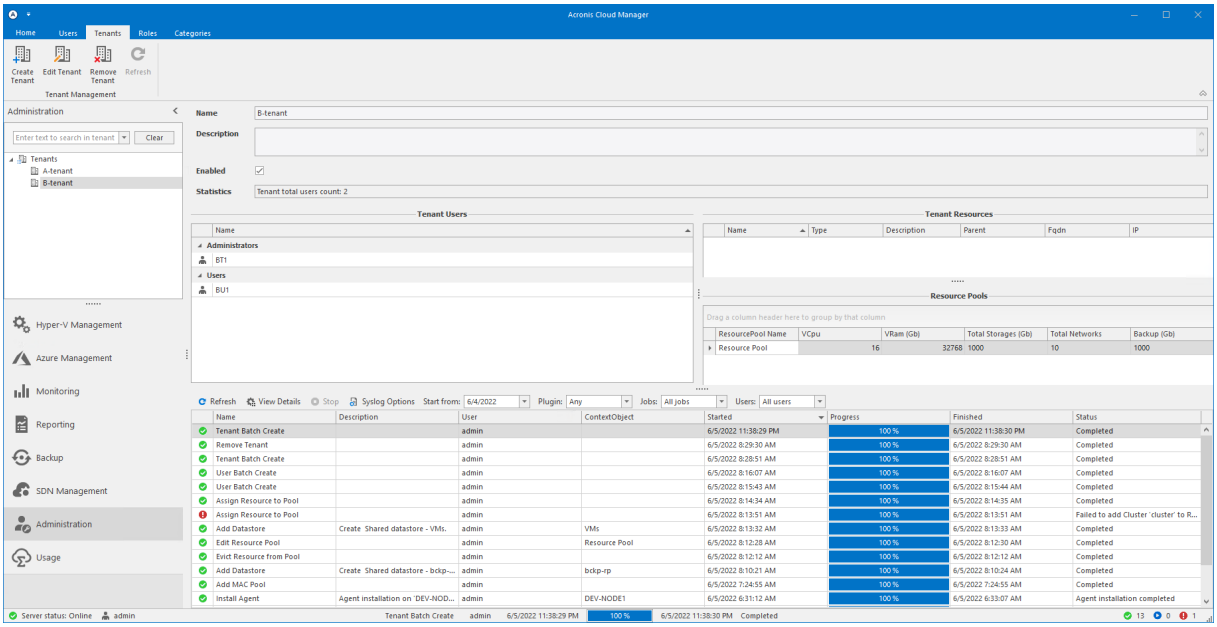
- vCPU (Gb).
- vRAM (Mb).
- Total disk capacity per each storage type (Gb).
- Number of virtual networks per each network type.
- Total backup storage capacity (Gb).

Quota settings are validated for consistence with current allocated resources: decreasing lower than already allocated resources and exceeding capacity of resource pool are denied. The warning with details appears if these constraints are violated.

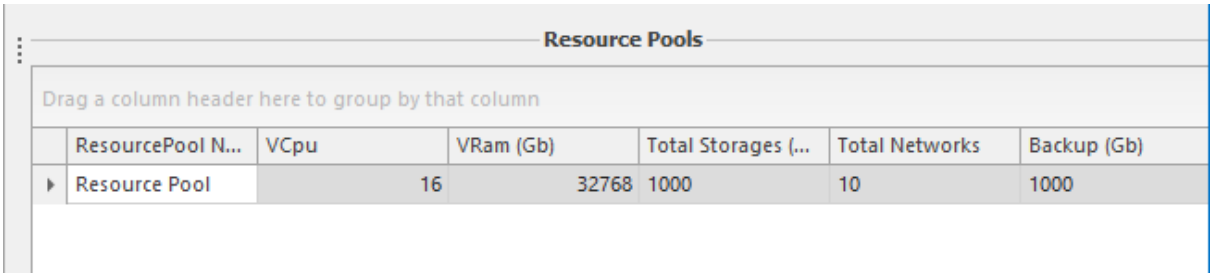


Displaying quotas

To view quotas, assigned to the tenant, go to the **Administration** plugin and open the **Tenants** tab, then select the required tenant:



Quotas are displayed on the **Resource pools** pane on the right hand side:



Usage

Usage is the feature that collects, displays and exports data on all resources allocated to tenants. These data are used for billing and can be imported into external billing systems.

Collecting usage statistics

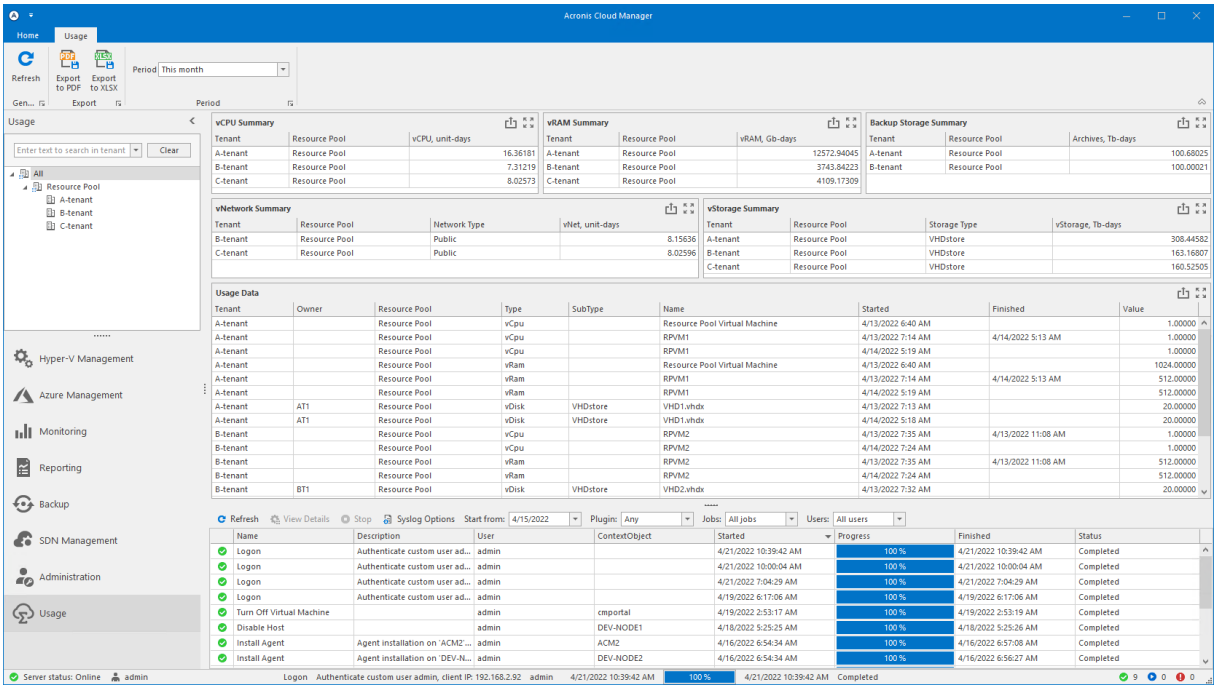
Statistics is collected on allocated resources:

- VMs - vCPU (periods when VM is running) and vRAM (periods when VM is running and paused).
- Virtual disks per disk type - total size.
- Virtual networks - per network type.
- Backup storage capacity used.

Taking into account that settings of each entity can be changed during a period, the start and end date/time of usage are stored for each specific configuration item in the detailed usage data description.

Displaying usage statistics

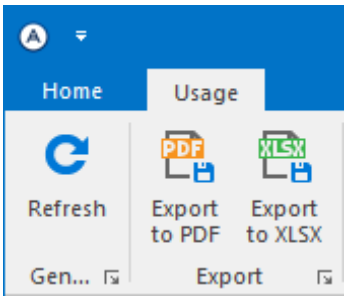
Usage statistics is displayed in the **Usage** plugin:



- User can see usage statistics across only own resources.
- Tenant admin can see overall tenant statistics and on per-user basis.
- Global admin can see statistics global, per-tenant, and per-user basis.
- User can set any date/time range to generate report using the **Refresh** button. The default is per-month view.
- Summary data is available in form: vCPU units, vRAM units, Size units per disk type, virtual network units.
- 1 Unit is equal to 1 day using of 1 unit of measurement. E.g., if 1 vCPU VM was running for a half of a day, it will be counted as 0.5 vCPU units.
- Physical resources (clusters, hosts) are measured by resource itself. 1 Unit is one day of this host/cluster being online. Physical host characteristics are displayed just for reference/additional details.

Exporting usage statistics

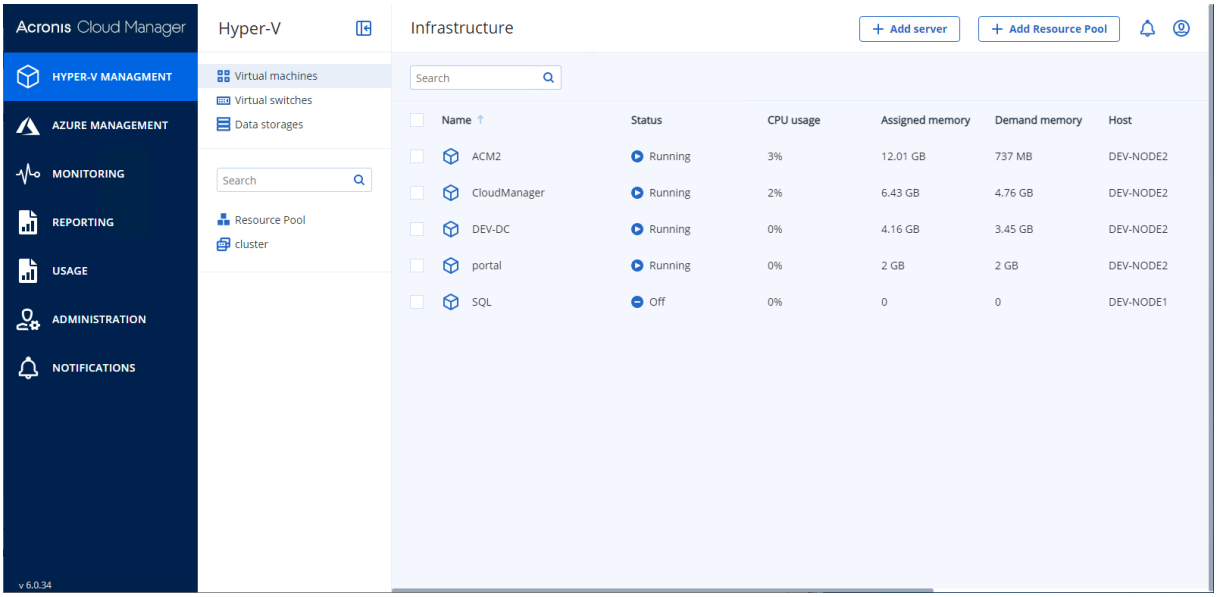
Usage statistics can be exported into PDF or XLSX file formats. The corresponding buttons are located on the main ribbon:



Click the required button and select the location where the corresponding file should be saved.

Web management console

Web management console is a web-based interface of Acronis Cloud Manager, which provides users with an access to all application's features through the web browser.



There are the following main parts of web console interface:

- Main navigation pane.

  Main navigation pane appears on the left side of the browser and contains the list of available plugins. You need to select the necessary plugin to open its content in the main browser's window to the right from the main navigation pain.
- Middle navigation pane.

  Middle navigation pane appears to the right from the main navigation pain and contains sub-menu with the selection of the objects and/or sections, applicable for the currently selected plugin.
- Data area.

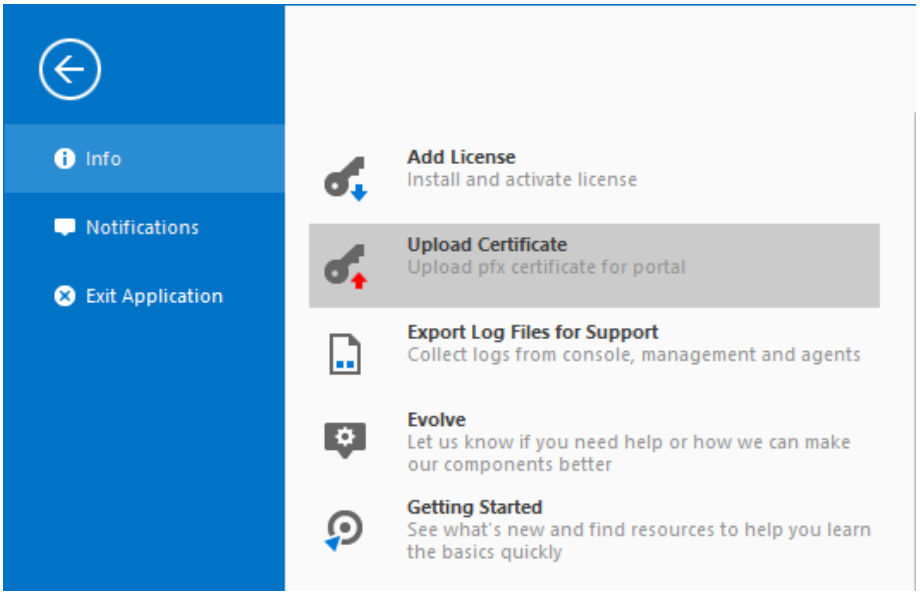
  Data area appears in the main part of the browser's window and shows text and/or graphical information about objects. It also contains applicable buttons and controls to perform operations with the objects and initiate various procedures. Context menu commands are also available for the objects where applicable.

Web management console installation

Web management console arrives along with the main setup archive of the product as a pre-configured .vhd file. It already contains all necessary software and required OS (Ubuntu Linux 18.04). All you need to do is prepare in advance generation 1 Hyper-V virtual machine, in accordance with system requirements and attach that vhd to this machine. Then review and configure a few settings inside the created virtual machine and on the management server side as described below.

To install web management portal:

1. Create generation 1 Hyper-V virtual machine in your environment that Acronis Cloud Manager is supposed to work in. This virtual machine must be connected to the external virtual switch and has the access to the management network, where the main application components will be working. Requirements to the machine you can find in the "Deployment and configuration" (p. 15) - "Acronis Cloud Manager web portal" (p. 17) section above.
2. Attach vhd disk that arrived with the installation package to the created VM.
3. Make sure you have at least one custom user with global admin rights created in Cloud Manager (**Administration** plugin). Please refer to the "Users" (p. 59)
4. Make sure you have SQL server user (sa) with sysadmin rights and remote connections enabled on your SQL server. Contact your DBA in case the assistance is required.
5. To use SSL/TLS connection to the management service you need to have a valid certificate for management server installed – self signed certificate will not work. Installing pfx for management server is available only within the management service installation wizard and should be done at that step. Please refer to the "Management service setup" (p. 19) section above.
6. Upload your own certificate for the web portal appliance via the Cloud Manager desktop console:



   Go to the **Home** tab and press the **Upload certificate** command. Then locate and select your certificate pfx file in the Windows explorer and click **Open**.
7. Start portal VM, open the guest console and, after the initial loading of the OS is finished, login into the system:

   login: **acronis**

   password: **CloudManager5**
8. Execute the following commands (substitute the fake data, shown in the snippet below - IP addresses, domain, URL etc, with yours):

```
aronis@cmportal:~$ sudo ./initsettings.sh
Current Ip is:
0.0.0.0
...Enter IP address with mask. Example: 192.168.1.1/16 :
192.168.1.3/24
Enter gateway:
192.168.1.1
Enter domain:
mydomain.com
Enter your DNS servers:
192.168.1.1,192.168.1.2
Enter URI:
https://192.168.1.4:16080/
Enter Acronis Cloud Manager User Name:
admin
Enter Aronis Cloud Manager User Password: admin
Enter ssl certificate password: <enter password>
Enter MS SQL Server address:
192.168.1.5
Enter MS SQL Server port:
1433
Enter MS SQL admin (sa):
sa
Enter MS SQL admin password: <enter password>
**now reboot the system**
sudo reboot
```

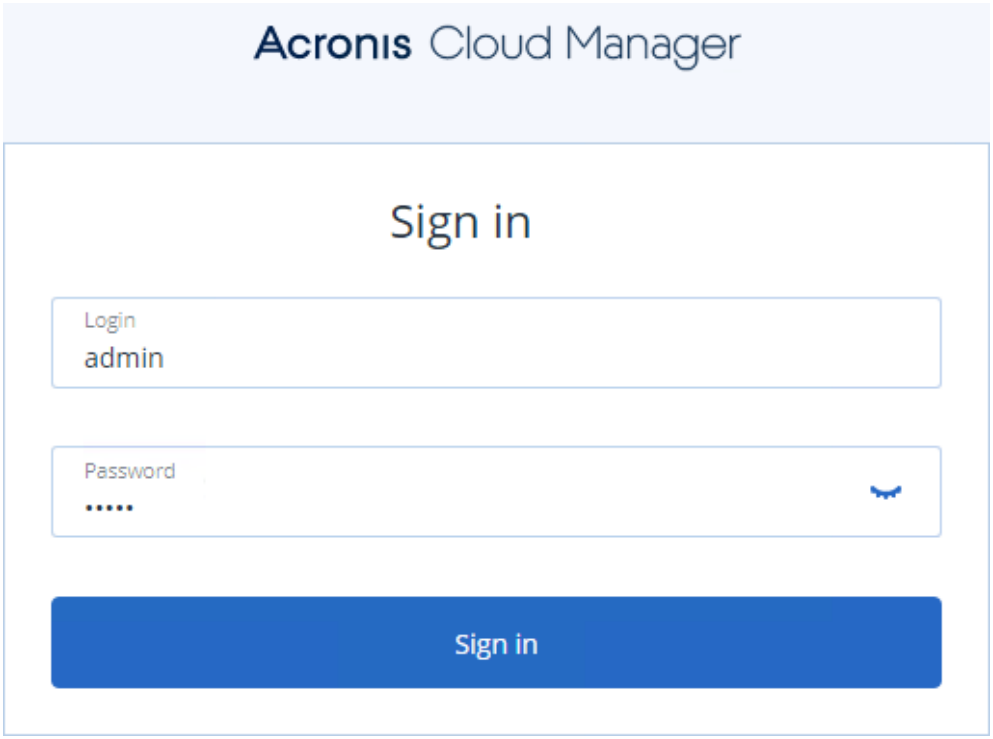
Note

If you use SQLEXPRESS version of MS SQL Server database, then you need to enable remote access and setup remote connection in the SQL Server Configuration Manager (enable browsing, TCP/IP connection and set up the port), which is disabled by default in this version. It is done on MS SQL server's side in accordance with Microsoft procedure. Contact your database admin if the assistance is required.

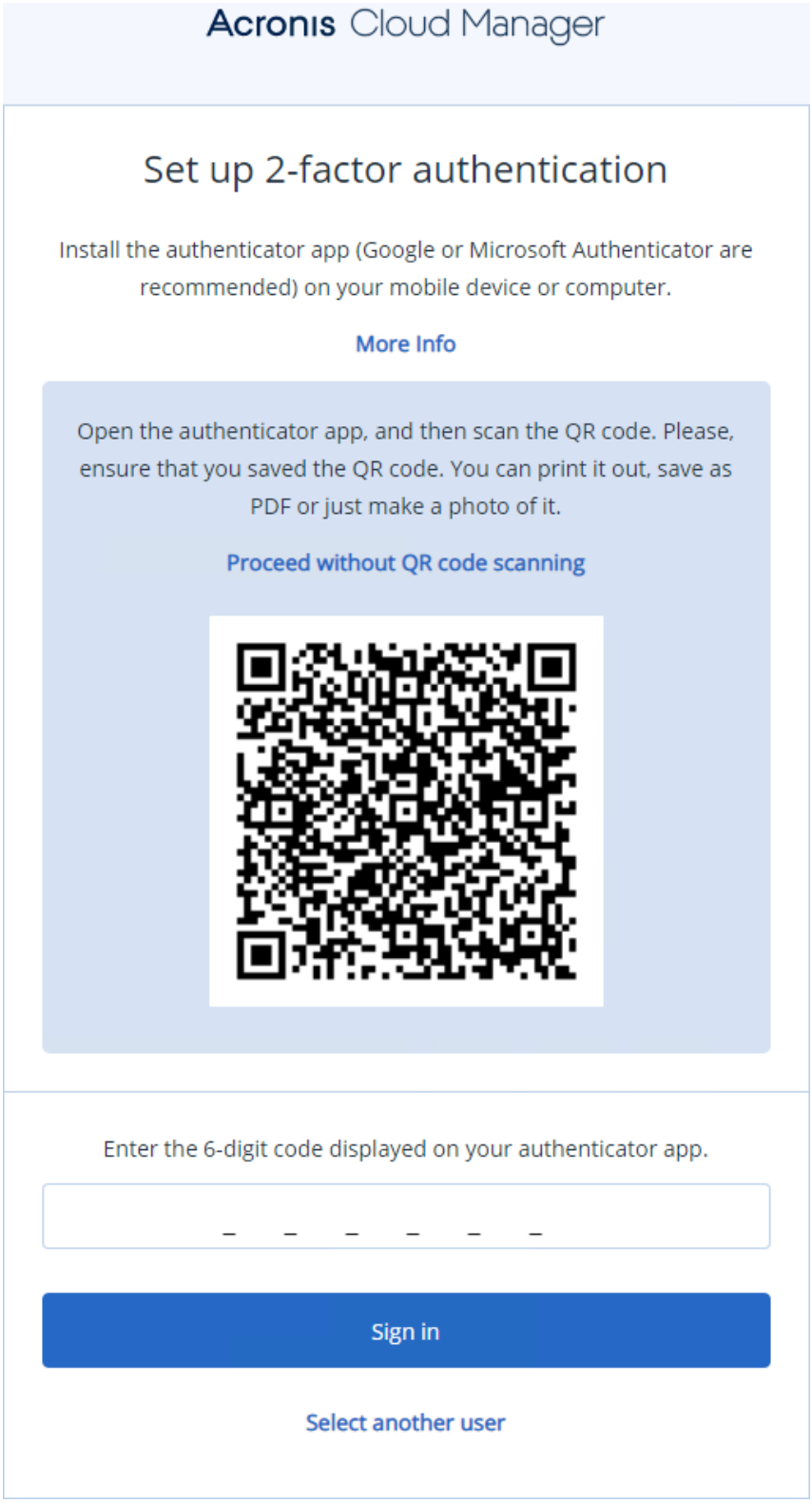
Login to the web management console

To login to the Acronis Cloud Manager web management console:

- Open the web portal appliance address in a browser, e.g. **https://192.168.1.5/**.
- Enter the Cloud Manager custom user login and password, then click **Sign in**:

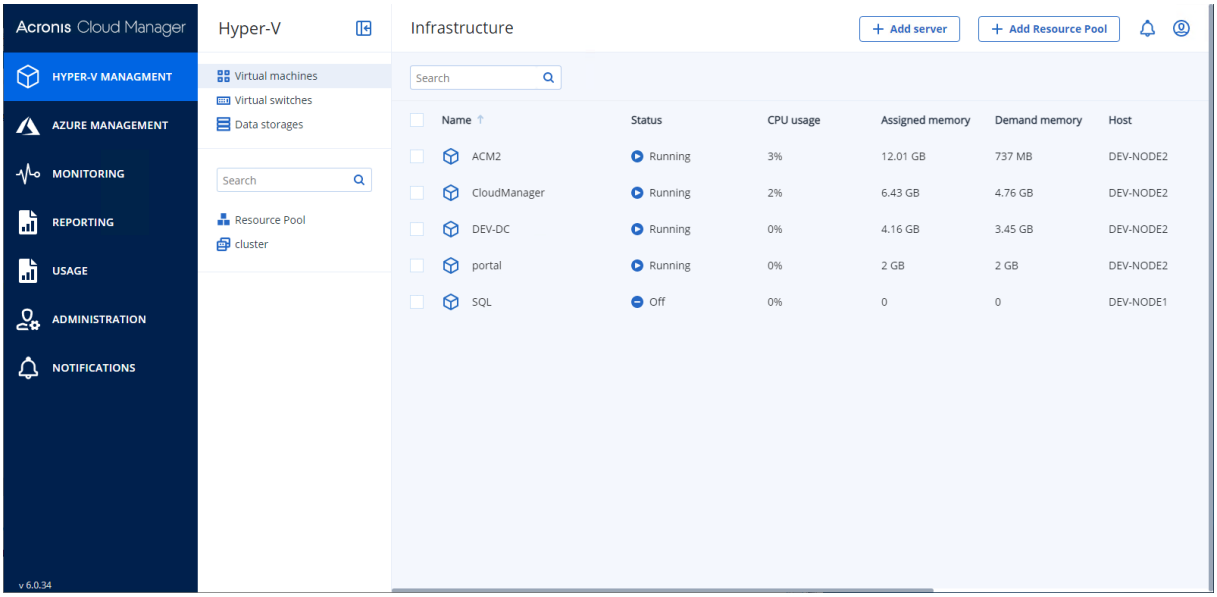


- In the case the two-factor authentication is enabled, the system will ask you to configure the Google authenticator (for the first time) and enter the one-time password generated by it, or just enter the one-time password (for subsequent login attempts):



Please, refer to the "Login to console" (p. 40) section above for more information about 2FA.

If the credentials (and the 2FA one-time password, if applicable) are correct and login is successful you will see the main screen in your browser:



Web management console operations

In current release there are the following features implemented in Acronis Cloud Manager web management console:

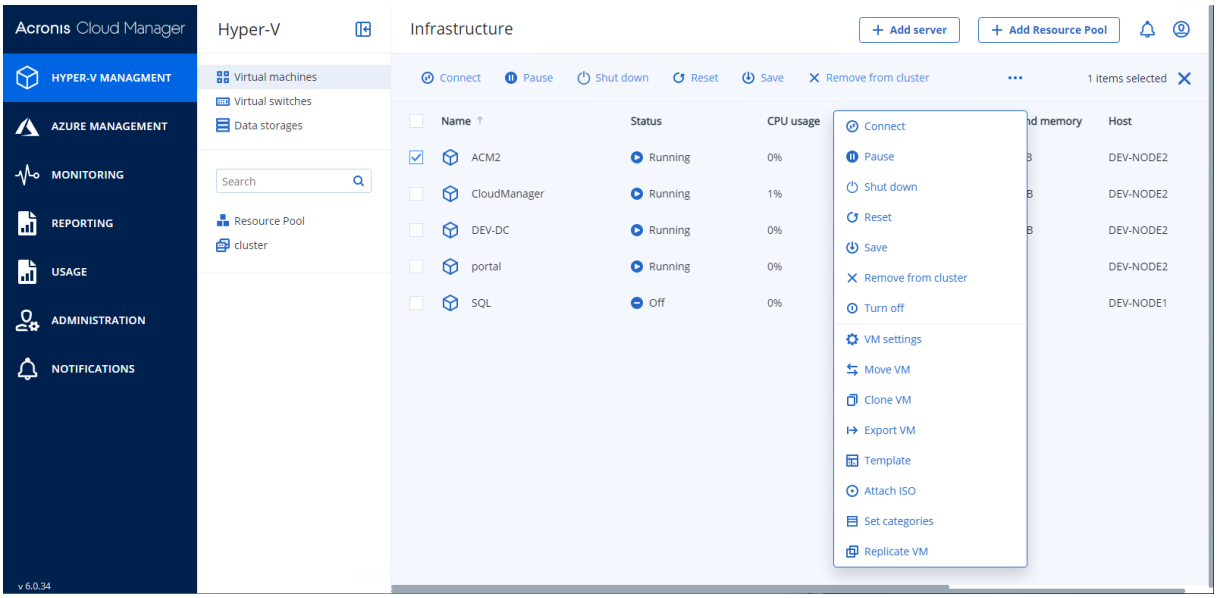
- Hyper-V management: all operations with VMs, virtual switches and datastores.
- Guest console VM connection: access VM directly from the web portal via guest console.
- Hyper-V monitoring: various performance indicators and alerts for Hyper-V objects.
- Azure management: operations with Microsoft Azure subscriptions.
- Administration: operations with users, tenants, roles and permissions.
- Reporting: creating various reports for Hyper-V environment/resources.
- New self-service tenant portal, based on the new features – resource pools, quotas and usage.

Next release will include other features:

- Hyper-V backup & replication.

Hyper-V management

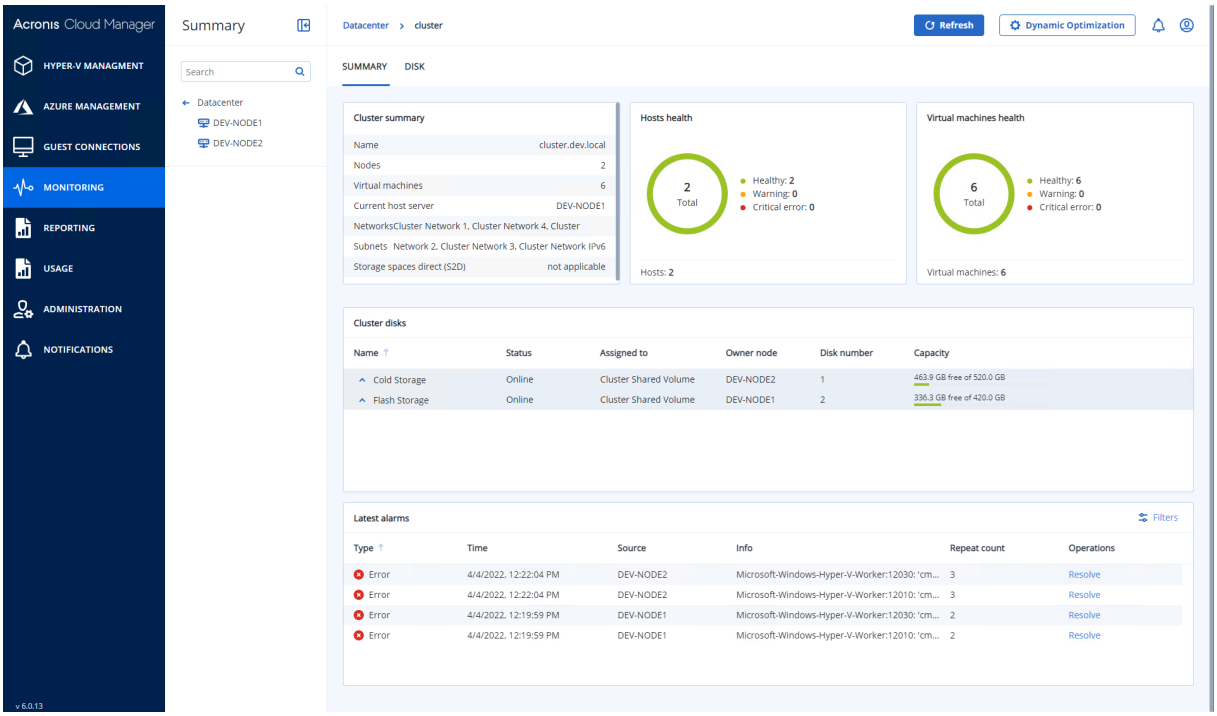
Hyper-V management plugin has the same features as desktop console including operations with VMs, virtual switches, resource pools and datastores. The submenu appears on the middle pane to open the necessary section: Virtual Machines, Virtual Switches and Data Storages.



Guest connection view is implemented via Guacamole remote desktop gateway (see https://guacamole.apache.org/).

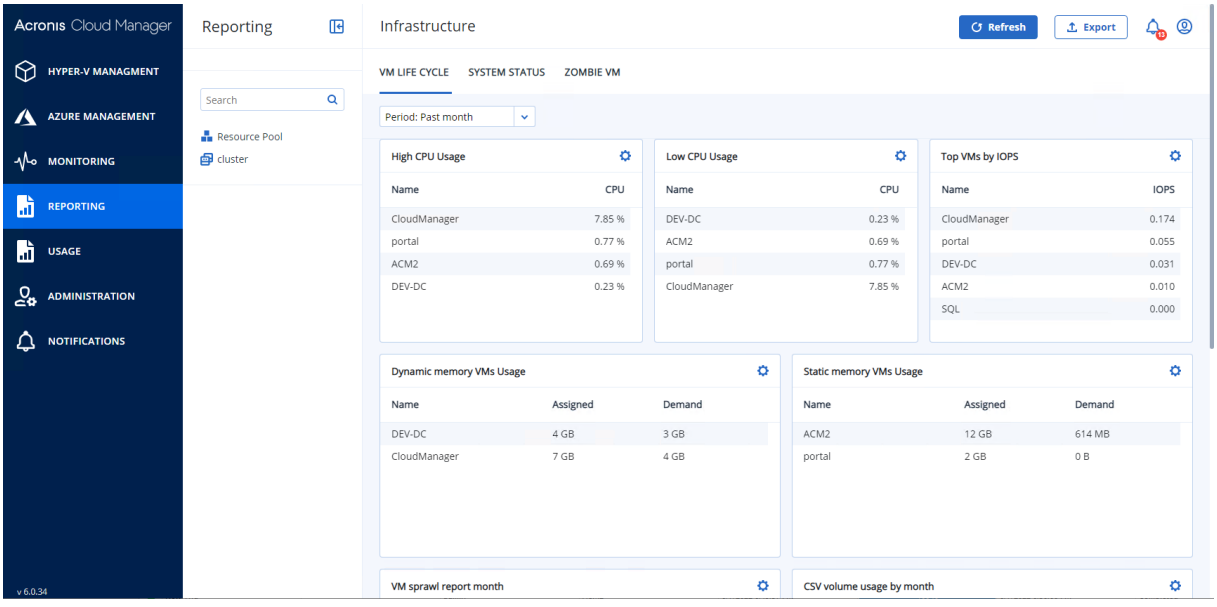
Hyper-V monitoring

Hyper-V monitoring plugin has the same features as desktop console including various performance graphs and alerts for Hyper-V hosts and VMs.



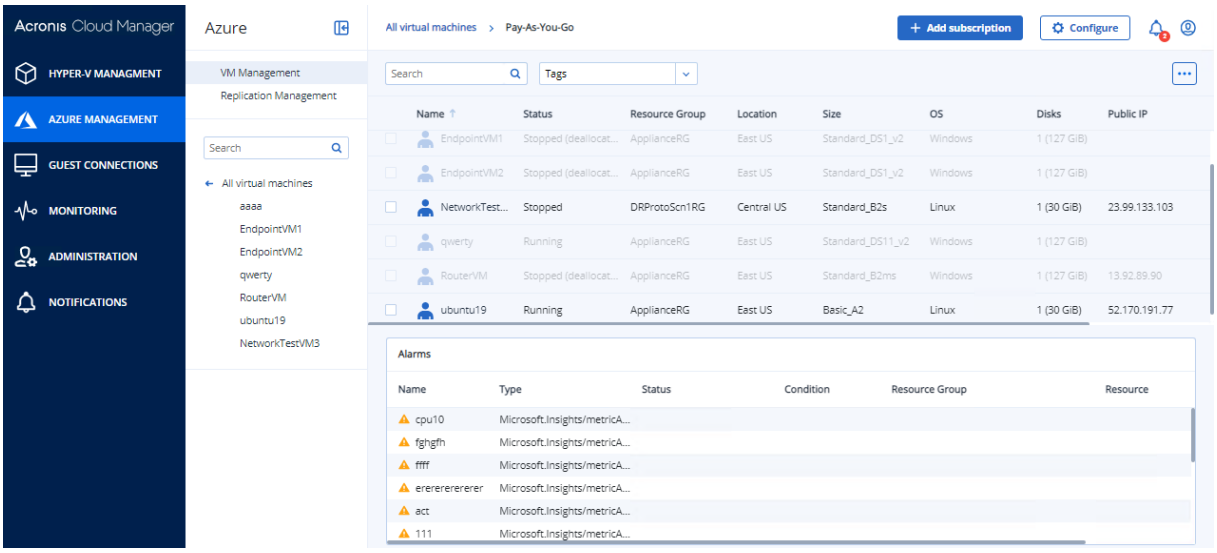
Hyper-V reporting

Hyper-V reporting plugin has the same features as desktop console and is designed to provide consolidated data about virtual machines. It consists of three tabs – **VM life cycle**, **System status** and **Zombie VM**.



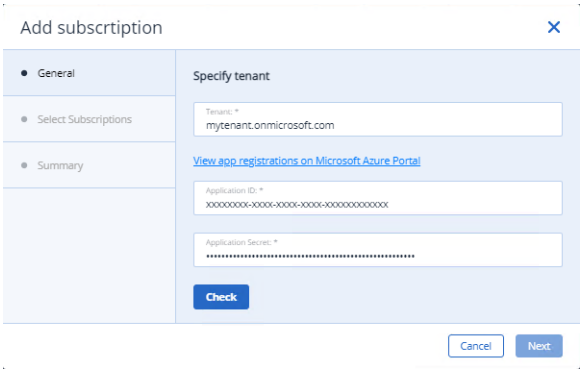
Azure management

Azure management plugin represents features to control Microsoft Azure subscriptions from Acronis Cloud Manager web console as it's done in the desktop application. It allows adding and removing subscriptions, control Azure VMs and, also, VM replication.

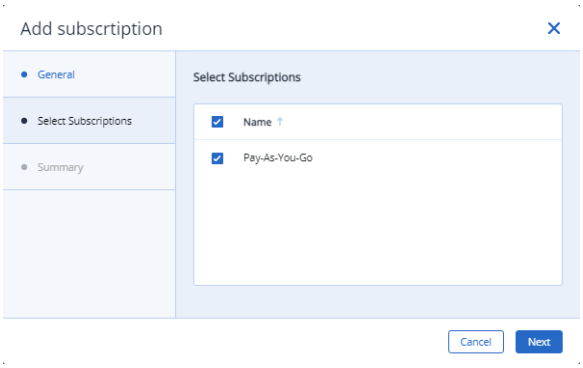


Adding subscription

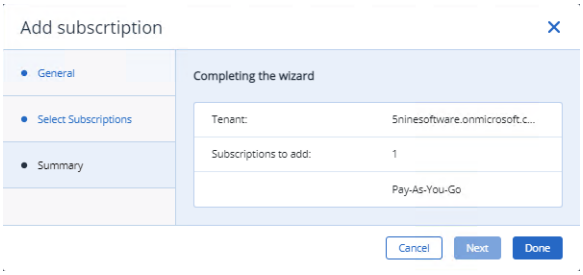
To add Microsoft Azure subscriptions click the **Add subscription** button on the main panel of the web portal. Then enter the credentials, click **Check** and, if everything is correct, click **Next**:



Select the subscriptions and click **Next**:

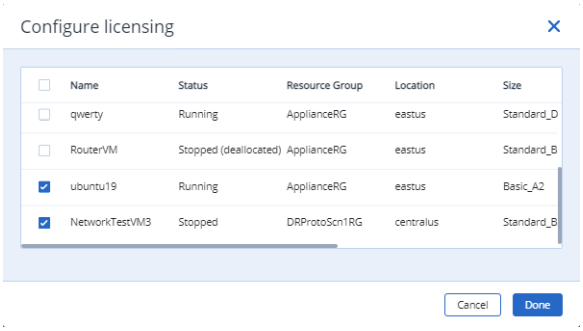


Review the summary and click **Done**:



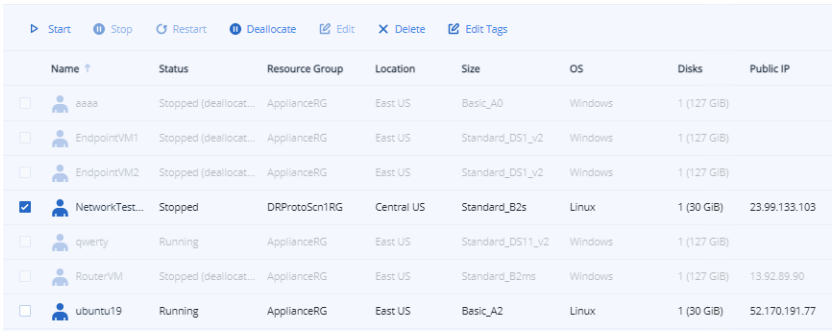
Configuring licensing

Before you are able to do any actions with Azure VMs, you have to configure licensing. The amount of VMs that will be operable in the portal can be configured within the limit of your purchased license. To configure licensing, select the subscription and click the **Configure licensing** button on the main panel of the web portal. Then select the VMs and click **Done**:



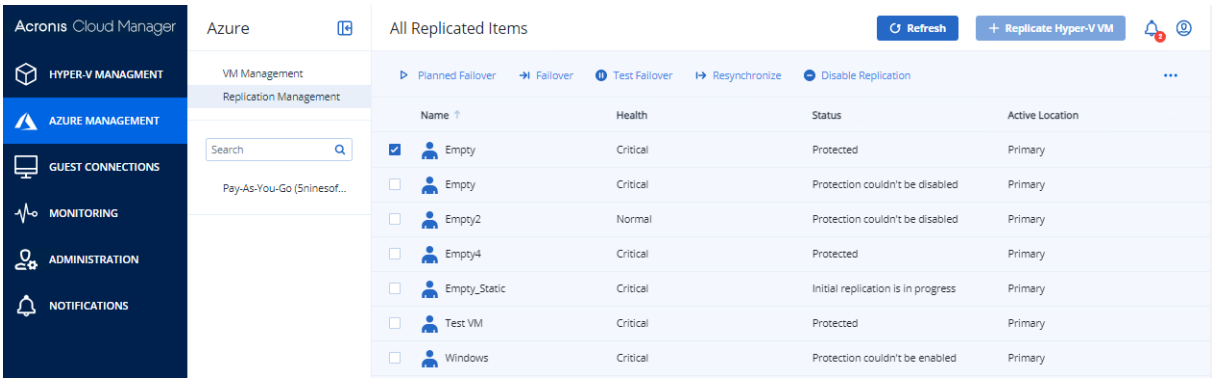
VM management

To do any action with Azure VM, open the **VM management** view on the left side of the **Azure management** plugin. Select the subscription and operable VM in the list from those you have configured in the license previously. Then select the required command on the subpanel:

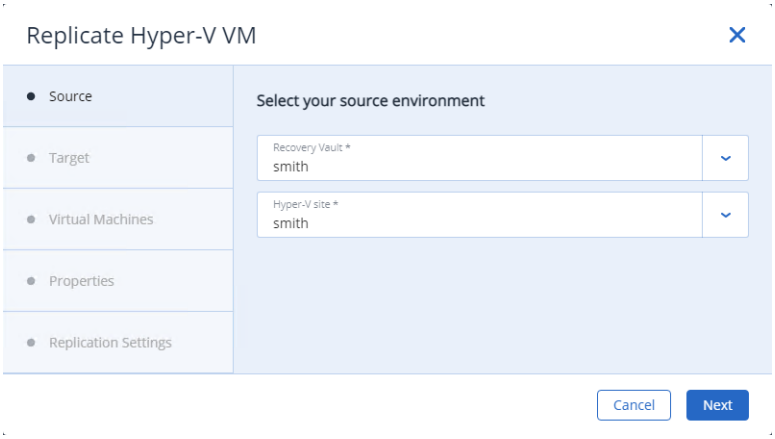


Replication management

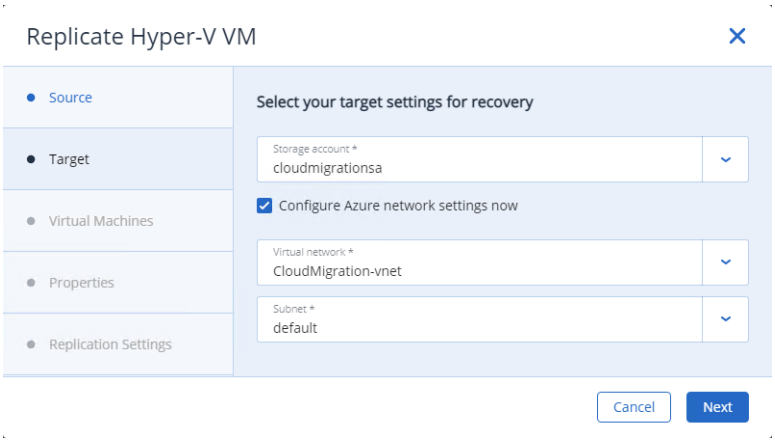
To manage VM replications open the **Replication management** view on the left side of the **Azure management** plugin. Select the subscription and the replicated VM in the list. Then select the required command on the subpanel:



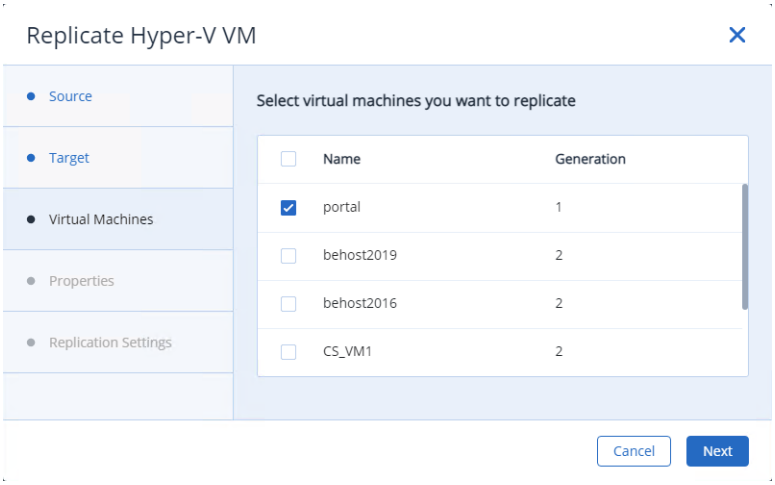
To replicate the new Hyper-V VM into Azure, select the subscription and click the **Replicate Hyper-V VM** button on the main panel. Select the source environment on the first screen of the **Replicate Hyper-V VM** wizard and click **Next**:



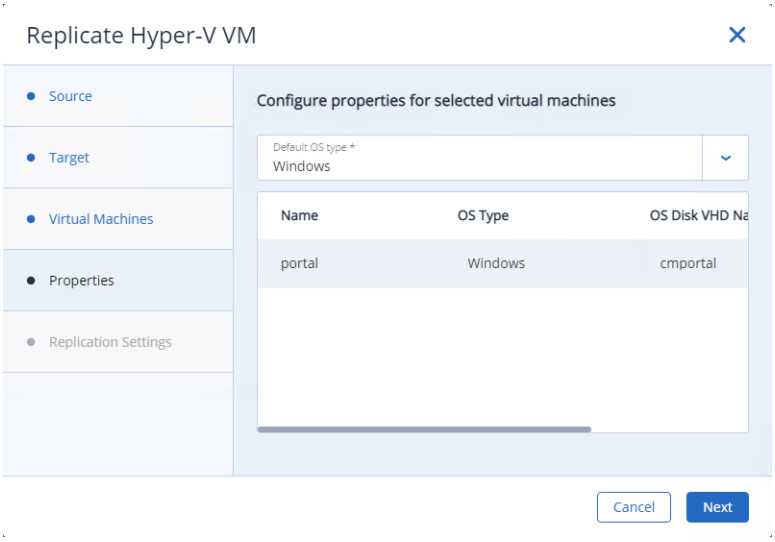
Select the target and click **Next**:



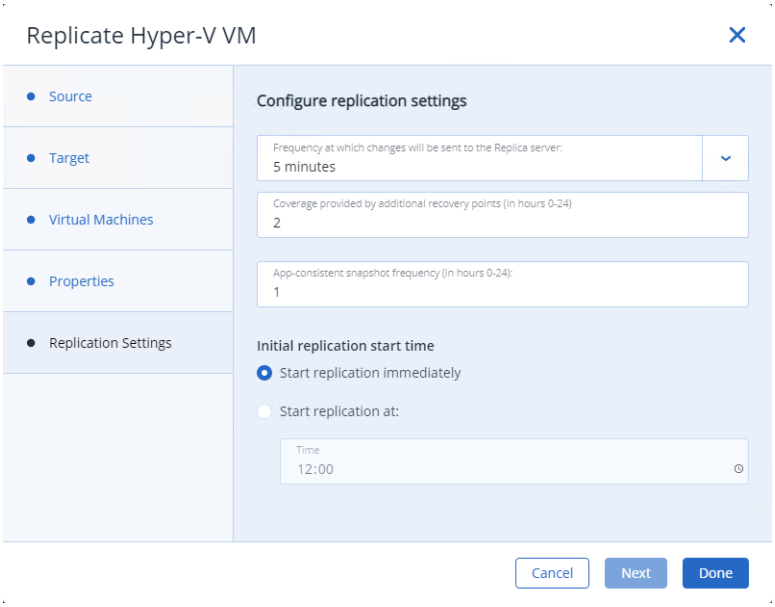
Select the VMs and click **Next**:



Configure the VM properties and click **Next**:

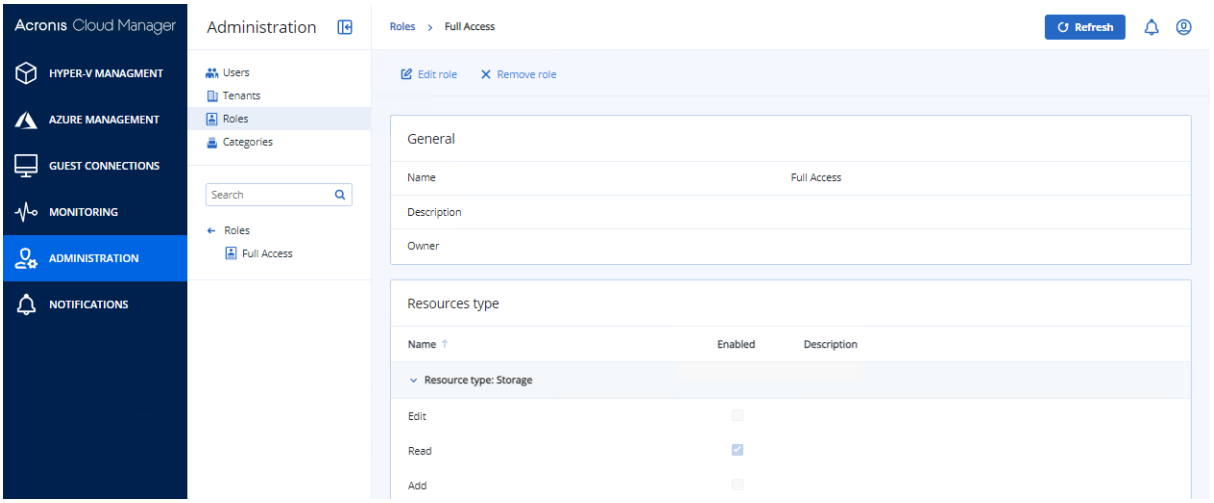


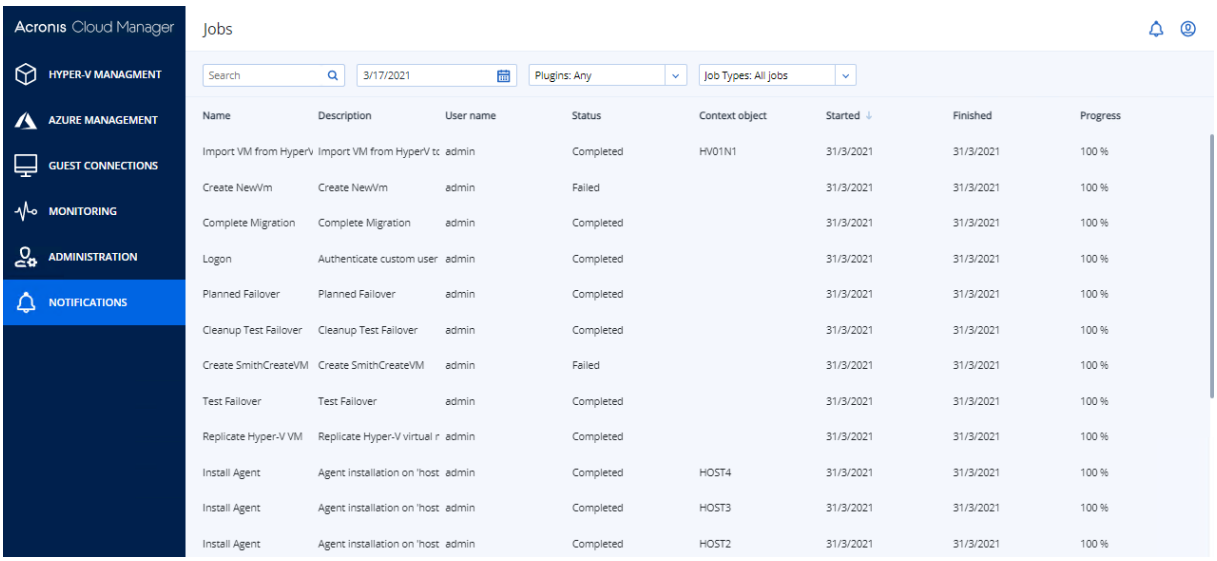
Configure replication settings and click **Done**:



Administration

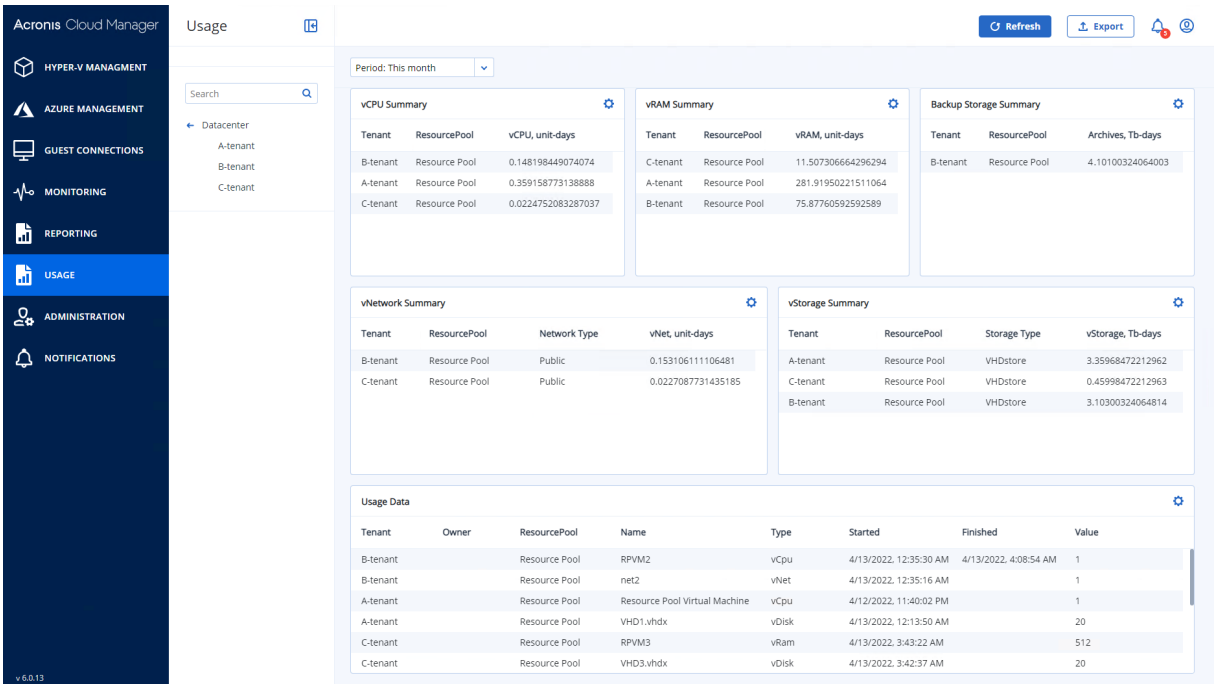
Administration plugin has the same features as desktop console including all operations with tenants, users and roles within the role-based access model and jobs management.





Usage

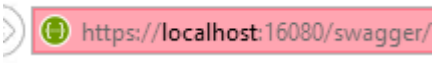
The **Usage** plugin in the web console has the same features as in desktop version to collect, display and export data on all resources allocated to tenants. Usage statistics is displayed on the **Usage** page of the portal:



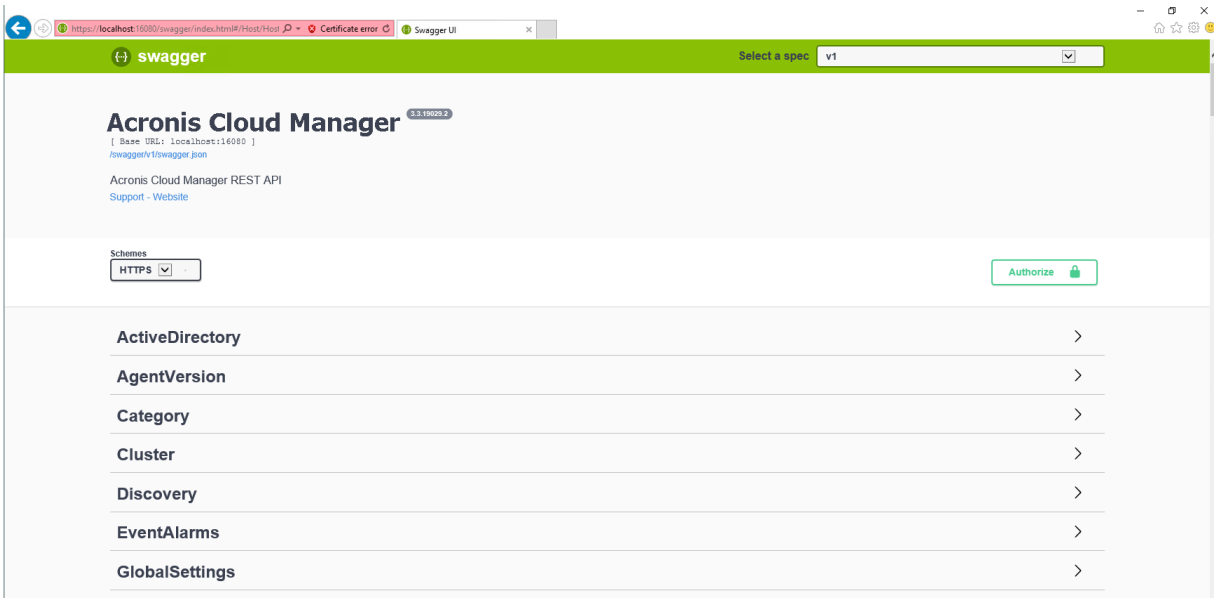
You can set the required period to collect data, reload the information using the **Refresh** button and export data into PDF or XLSX file formats using the **Export** button, located in the right-upper corner of the web page.

REST API

On the Acronis Management server, open a web browser to https://localhost:16080/Swagger

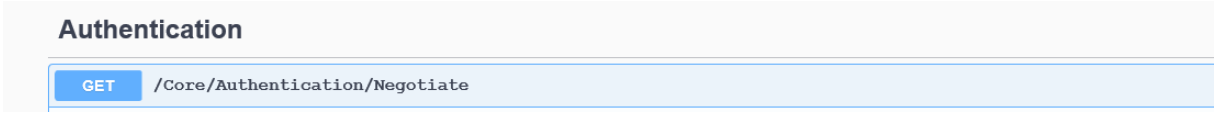


This will open the Acronis swagger API interface

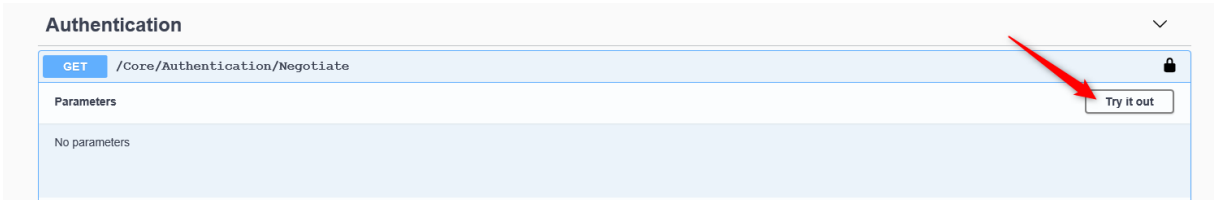


Navigate to authentication to generate an API key for testing

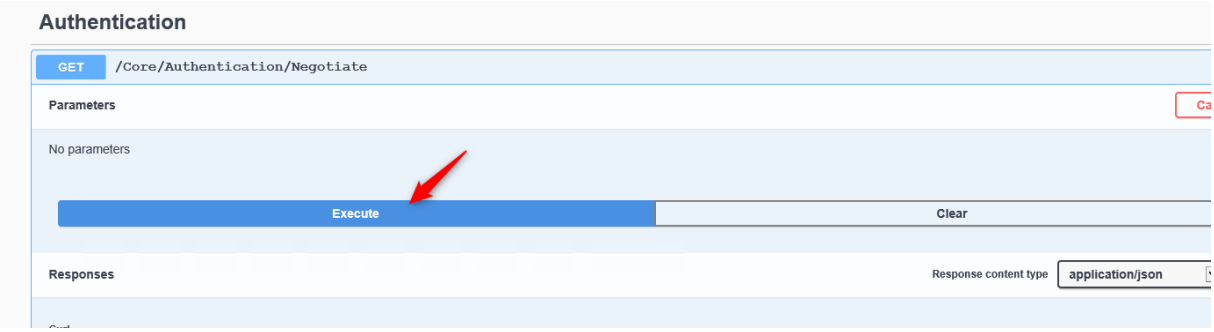
Select the **/core/authentication/negotiate**



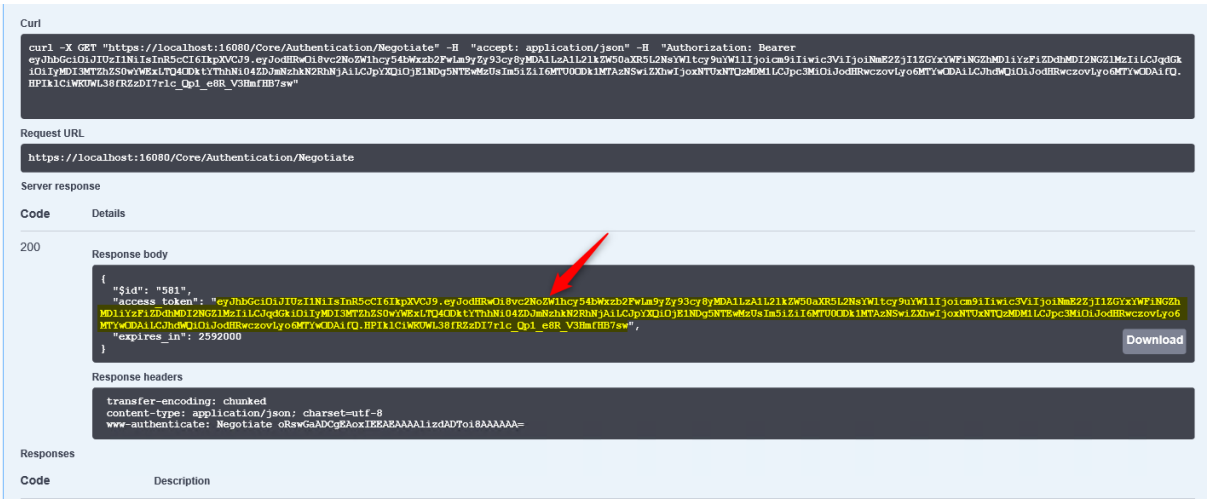
Execute the API call: select **Try it out**



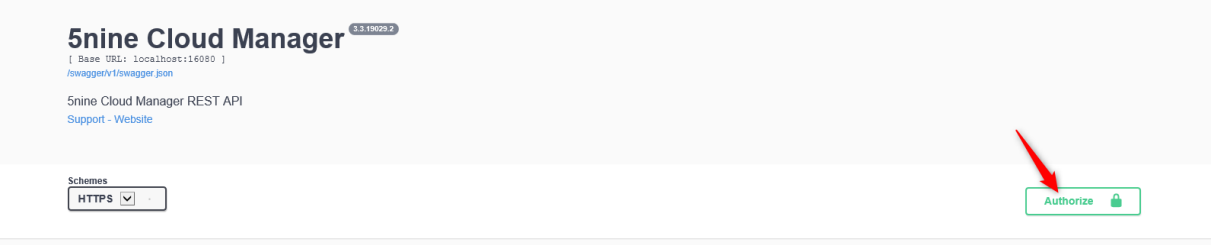
Next, select **Execute**



Copy generated access token without the quotes:



Browse back to top of the swagger API Screen and select **Authorize**



Enter the access token into the **Value** field,

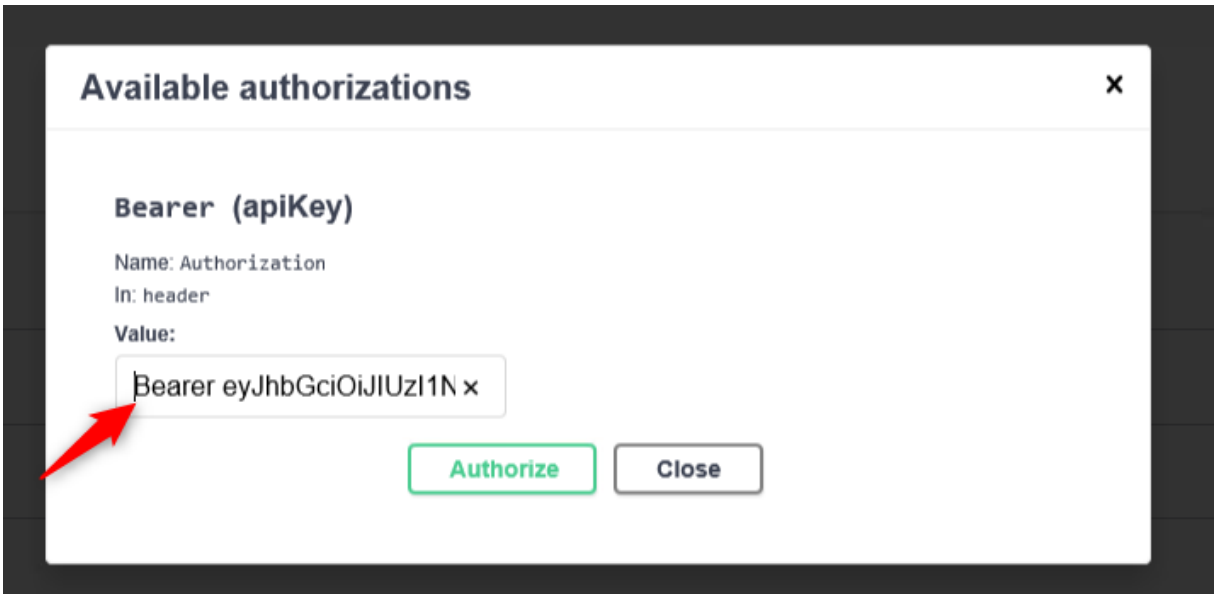
Note

You will need to add the word *bearer* before the access token, using the above access token.

The example entry would look like this:

Bearer

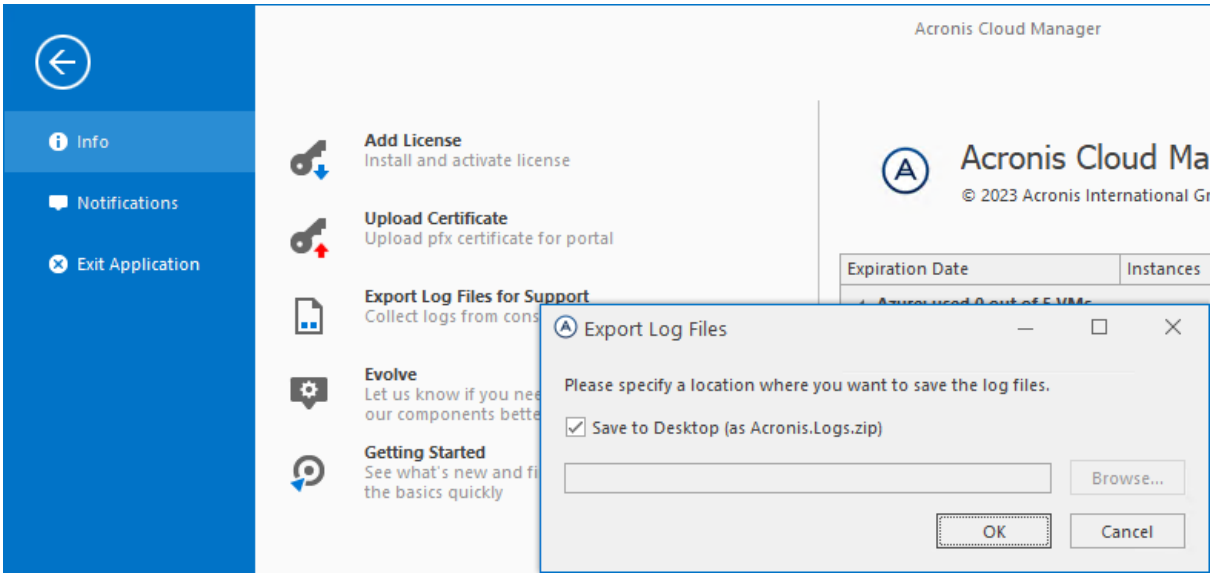
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJodHRwOi8vc2NoZW1hcy54bWxzb2FwLm9yZy93cy8yMDA1LzA1L2lkZW50aXR5L2NsYWltcy9uYW1lIjoicm9iIiwic3ViIjoiNmE2ZjI1ZGYxYWFiNGZhMDliYzFiZDdhMDI2NGZlMzIiLCJqdGkiOiIyMDI3MTZhZS0wYWExLTQ4ODktYThhNi04ZDJmNzhkN2RhNjAiLCJpYXQiOjE1NDg5NTEwMzUsIm5iZiI6MTU0ODk1MTAzNSwiZXhwIjoxNTUxNTQzMDM1LCJpc3MiOiJodHRwczovLyo6MTYwODAiLCJhdWQiOiJodHRwczovLyo6MTYwODAifQ.HPIklCiWKUWL38fRZzDI7rlc_Qp1_e8R_V3HmfHB7sw



Select **Authorize**, at this point, you should be authenticated to the API, You can now run and test other fuctions of the API. For more details about the API including examples please review https://www.acronis.com/en-us/support/.

Support information

To ease the communication process with Acronis technical support in the case of any questions regarding product function or if an investigation is required, automatic support information collection of logs is available in the Acronis Cloud Manager console. To get the support information archive, go to the **Home** tab – **Info** – **Export log files for support**. You will be offered to save the archive either directly on your desktop (by default) or any other place of your choice:



Please attach the collected archive to your request or send it to 5ninesupport@acronis.com or the Acronis representative that you are in contact with.

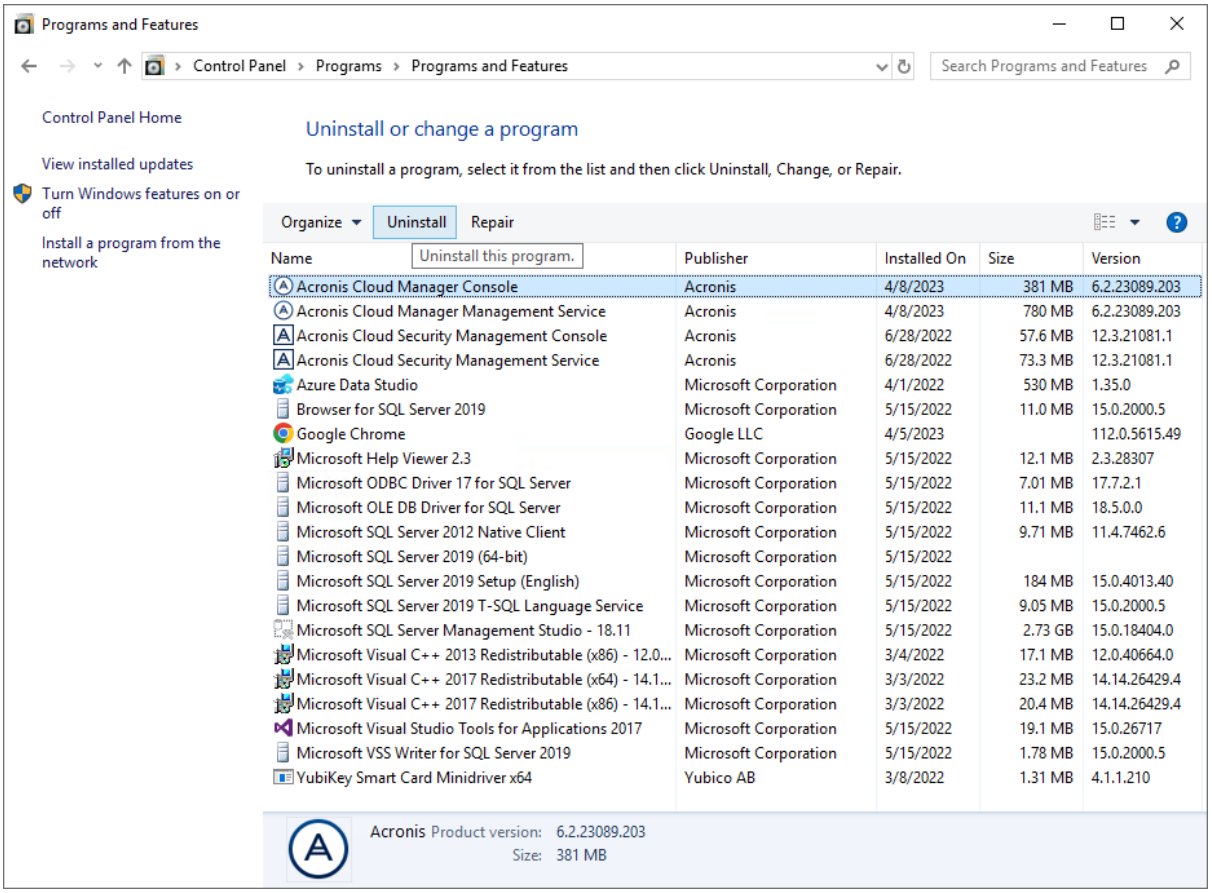
Also, refer to the following product support page at Acronis website: https://www.acronis.com/en-us/support/5nine/cloud-manager/ .

Uninstalling Acronis Cloud Manager

1. To uninstall Acronis Cloud Manager, you can use the same bootstrap application:

2. Select the component you need to uninstall and click on it to run uninstallation process.

Or you can open the **Start** menu, go to **Control Panel > Add or Remove Programs**, choose Acronis Cloud Manager components you want to uninstall and click **Uninstall**.



Repeat this procedure on every machine where the Acronis Cloud Manager components are installed.

Note

Acronis Cloud Manager database and its data is retained until you manually remove the database.

Index