Configuration virtualization

Installation manual

for system providers

9/8/2021

Product line *neo*, version 6.x

The described functions can be used with the following ASC products:

EVOIP*neo*

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at http://www.asctechnologies.com.

ASC Technologies AG - Seibelstr. 2-4 - 63768 Hösbach - Germany

Contents

1 General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at https://www.asctechnologies.com

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

2 Introduction

This document describes:

- The configuration in VMs in VMware
- The installation of a *neo* server by means of VMware templates
- The installation of a *neo* servers by means of Google templates
- The configuration of VMs in HyperV
- Further configurations required for the operation of the EVOIP*neo* software in virtualized environments

For information about the installation and configuration of Microsoft Windows refer to the respective installation manual for system providers *Configuration Windows Server 2012 R2*, *Configuration Windows Server 2016* or *Configuration Windows Server 2019*.

In virtual environments, you can exclusively use network drives for archiving, import, and export of data. Internal or USB drives are not supported as performance issues may occur when trying to access a drive that is no longer available.

3 System requirements

Exclusively install software approved by ASC!

For information about approved software refer to the current *neo Integration Overview* in the ASC Partner Portal.

To be able to configure the virtualization in the application System Configuration, the customer-specific license file must have been imported. For further information about licensing refer to the administration manual *System Configuration - License administration*.

Virtual machines must not be cloned.

The volume IDs of the drives in Windows must be unambiguous in a virtual *neo* system. This means that in a distributed *neo* system, the volume ID must not exist more than once. You can run a query of the volume IDs in the Windows command line prompt by entering the command *MOUNTVOL /L*.

ATTENTION!

neo is a near real-time application which cannot work with resource sharing. Therefore, all VMware resources must be assigned exclusively to the virtual *neo* machines and drives must be configured as *Thick* If this precondition is not fulfilled, loss of recordings is imminent!

For information about the system requirements for virtual environments refer to the installation manual *Installation requirements*.

4 VMware

For a virtualization, VMware Tools must be installed.

4.1 Compatible VMware features

VMware ESX/ESXi Server features	Compatibility
VM Templates (OVAs, OVFs)	Partially [3]
Copy Virtual Machine	Partially [4]
Restart Virtual Machine on Different ESXi Host	Yes [1]
Resize Virtual Machine	Yes [1, 2]
Multiple Physical NICs and vNICs	Yes
VMware High Availability (HA)	No
VMware vNetwork Distributed Switch	No
VMware vMotion	No
Long Distance vMotion	No
VMware Storage vMotion	No
VMware Consolidated Backup (VCB)	No
VMware Data Recovery (DR, VDR)	No
VMware Snapshots	Yes [1]
VMware Fault Tolerance (FT)	No
VMware vCenter Converter	Yes
VMware vShield	No
Virtual Appliance Packaging of UC apps	No
3rd-Party VM-based Backup Tools (e. g. Veeam, Viziocore, esXpress)	Yes [1]
3rd-Party Physical To Virtual (P2V) Migration Tools	Yes [1]
VMware Boot from SAN	Yes [1]
All not-listed	On request

[1] Downtimes are possible

[2] No downsizing possible

[3] Only for OVFs provided by ASC

[4] Cloning VM with Windows installation (without *neo*) allowed

4.2 Installation and configuration of a neo VM by means of a VMware template

The following recording architecture types may be installed and configured:

- *neo* VM with Core and DB
- *neo* VM with Core and external DB
- *neo* VM without Core and with DB
- *neo* VM without Core and without DB

For the installation and configuration, *vCenter* is used.

1. Open a browser and connect with the web interface of *vCenter*.
2. Click on *vSphere Client (HTML5) - partial functionality*.

Fig. 1: vSphere Client (HTML5) - partial functionality

3. In the entry field *User name*, enter your e-mail address.

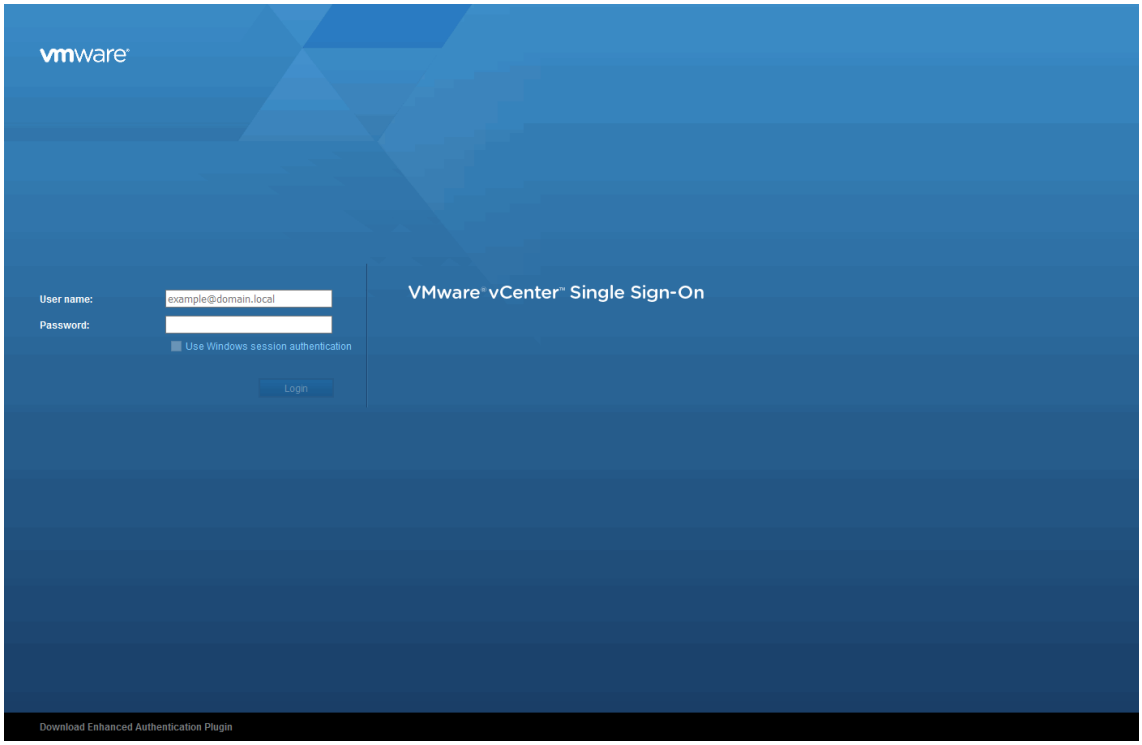

Fig. 2: Enter user name and password

4. In the entry field *Password*, enter your password.
5. Click on the button *Login*.
6. In the structure view, right-click on the directory where you would like to install your VM.
   ⇨ A context menu appears.
7. Click on the entry *Deploy OVF Template* in the context menu.

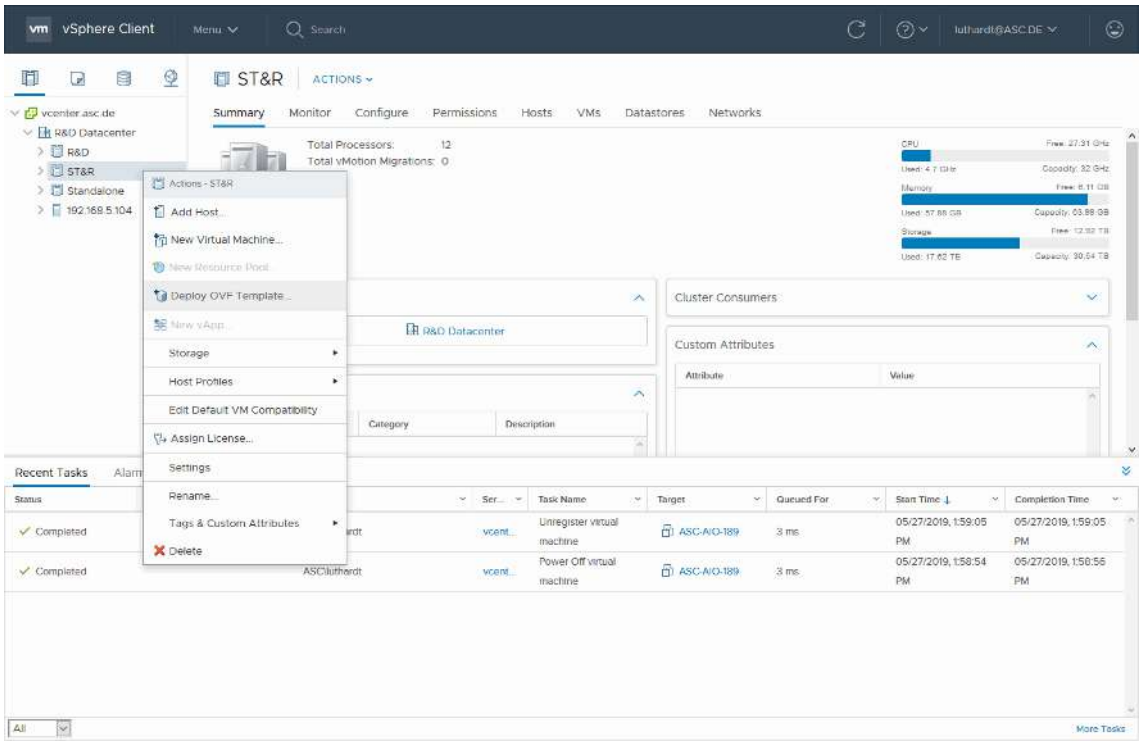

Fig. 3: Deploy OVF template

8. Activate the option *Local file*.

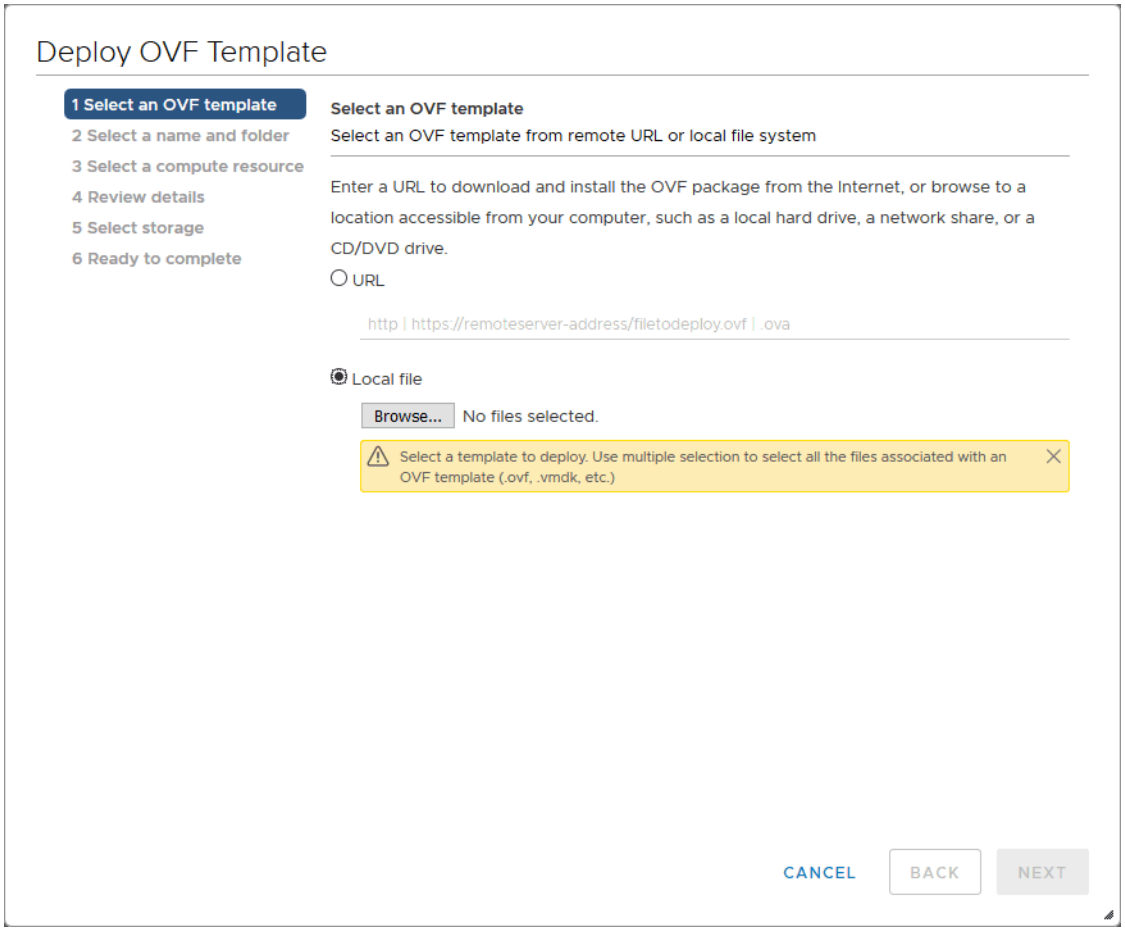

Fig. 4: Select OVF template

9. Click on the button *Browse*.
   ⇨ The following window appears:

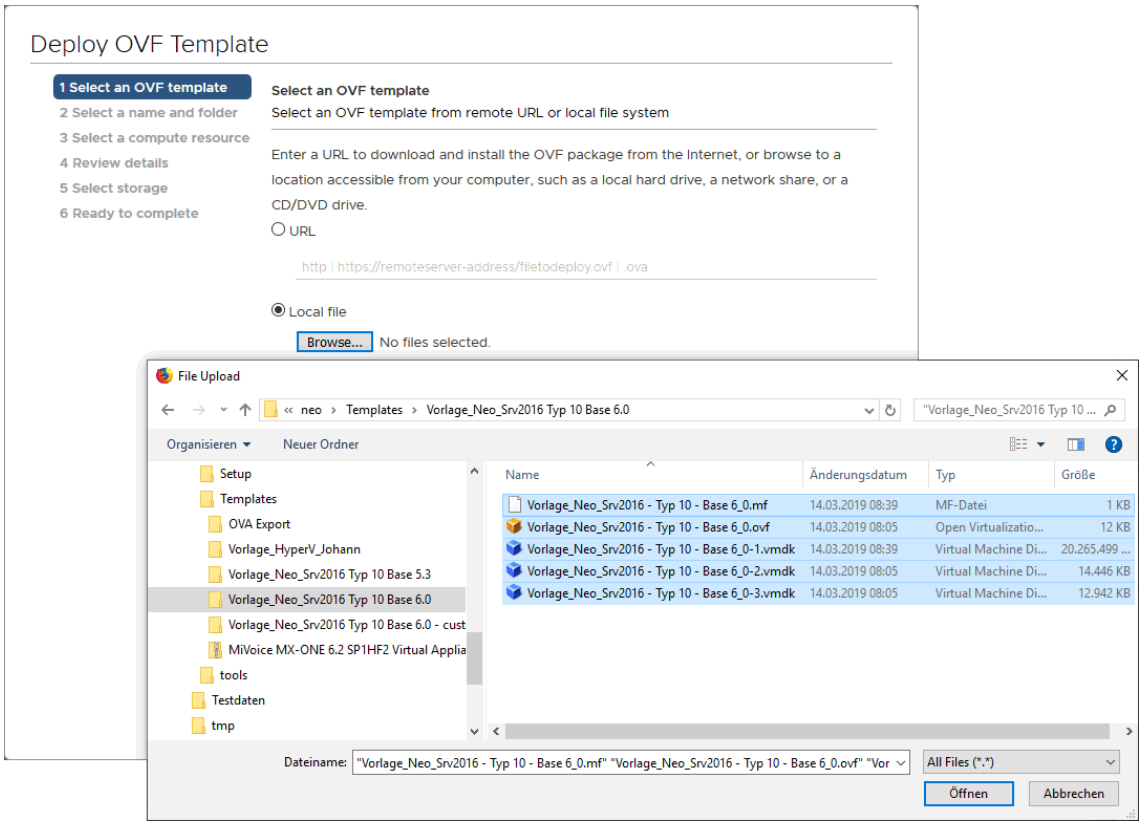

Fig. 5: Select OVF template

10. In the structure view, click on the directory with the *neo* installation files.
11. Select all files in the structure view.
12. Click on the button *Open*.
13. Click on the button *NEXT*.

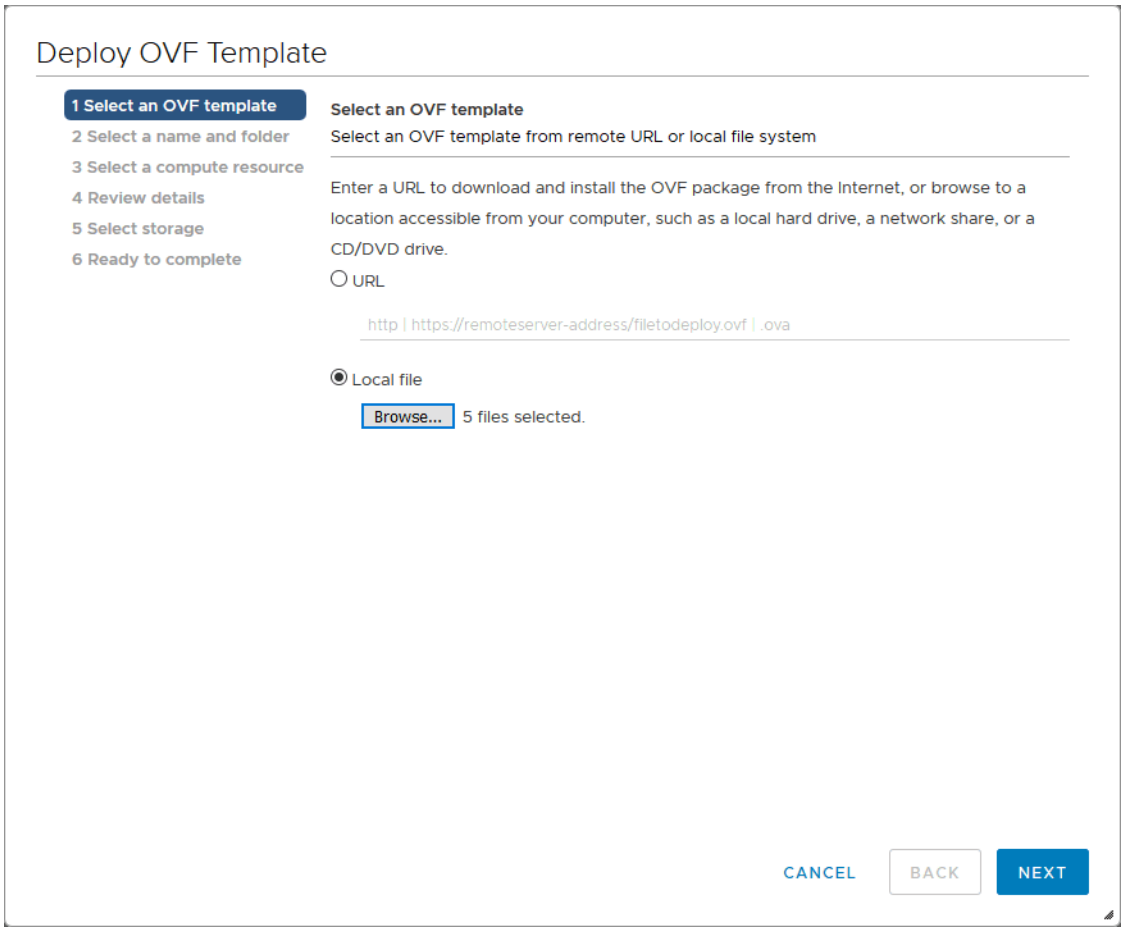

Fig. 6: Select OVF template

14. Enter a name in the entry field *Virtual machine name*.

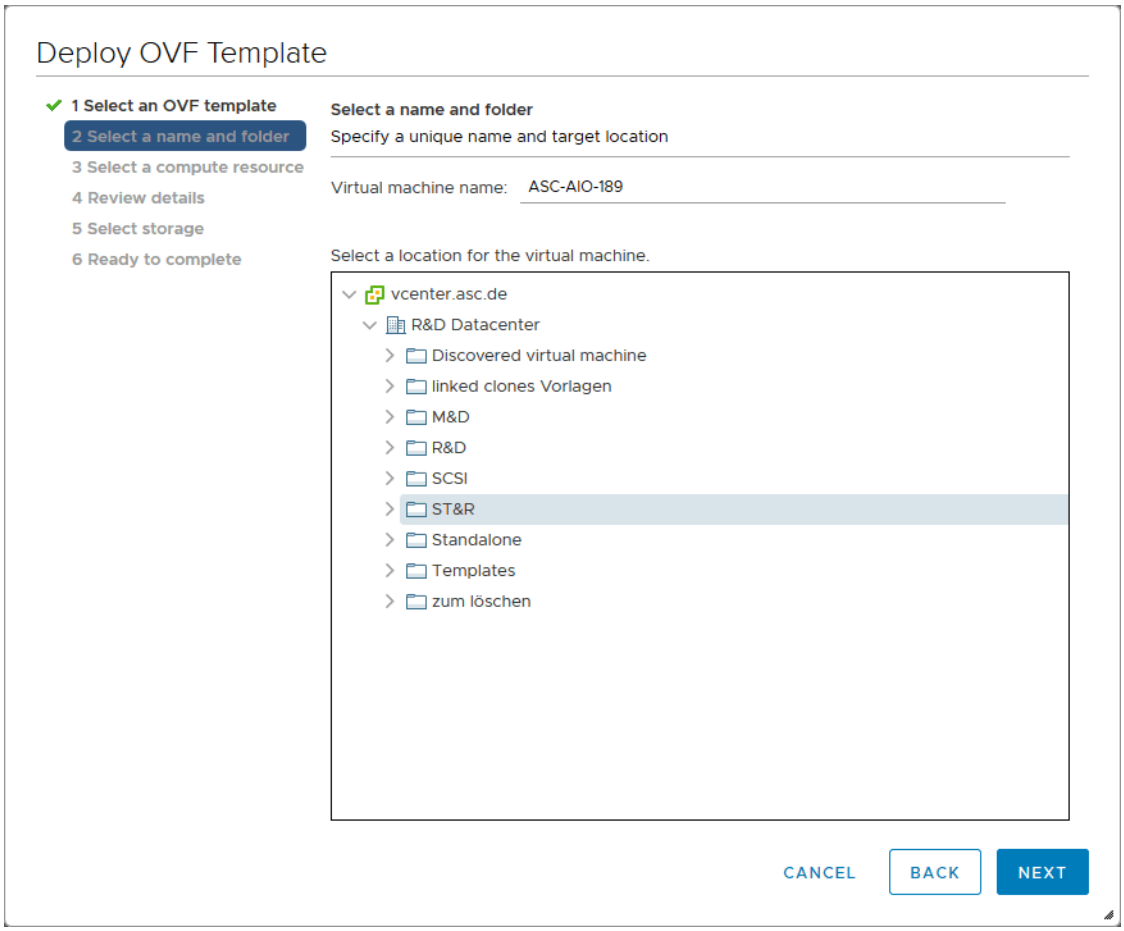

Fig. 7: Select name and folder

15. Select a storage location for the virtual machine.
16. Click on the button *NEXT*.
17. Select the computing resource.

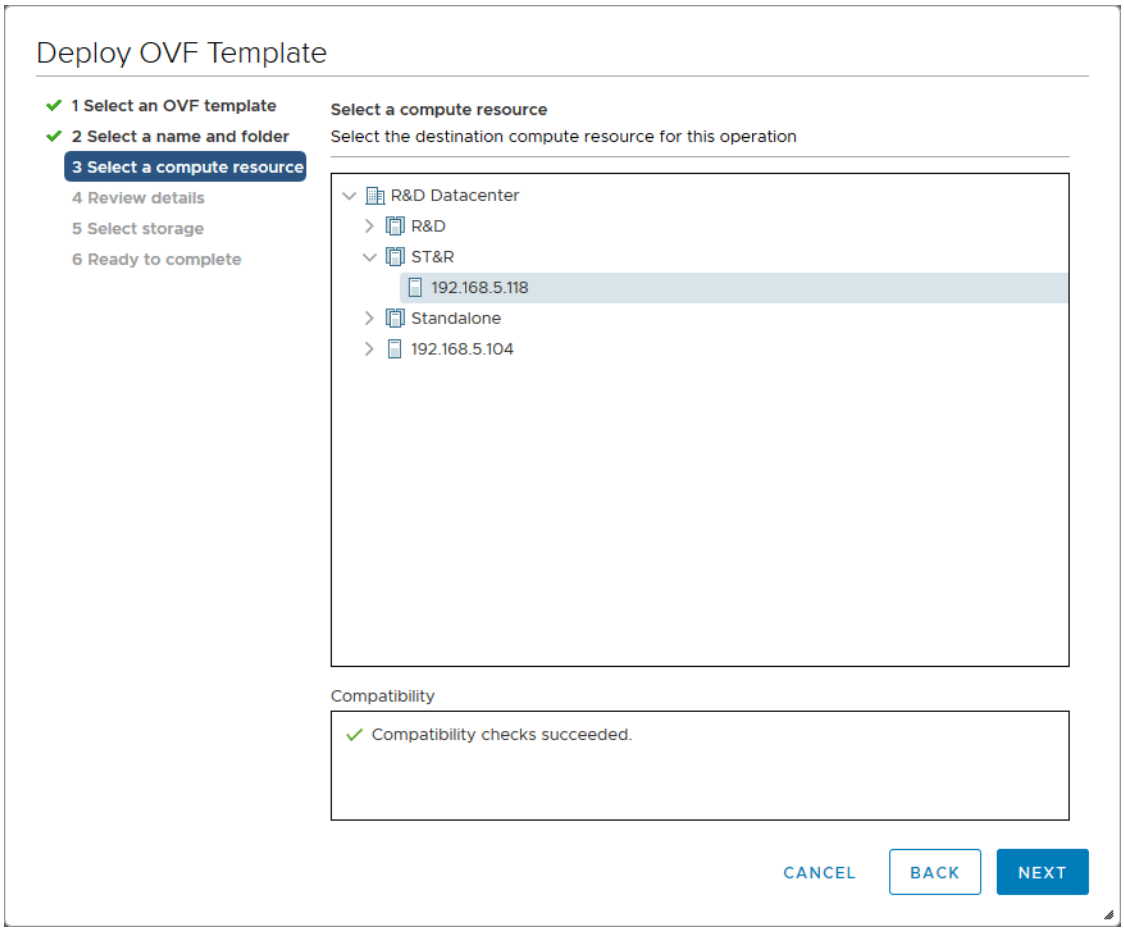

Fig. 8: Select computing resource

18. Click on the button *NEXT*.
19. Click on the button *NEXT*.

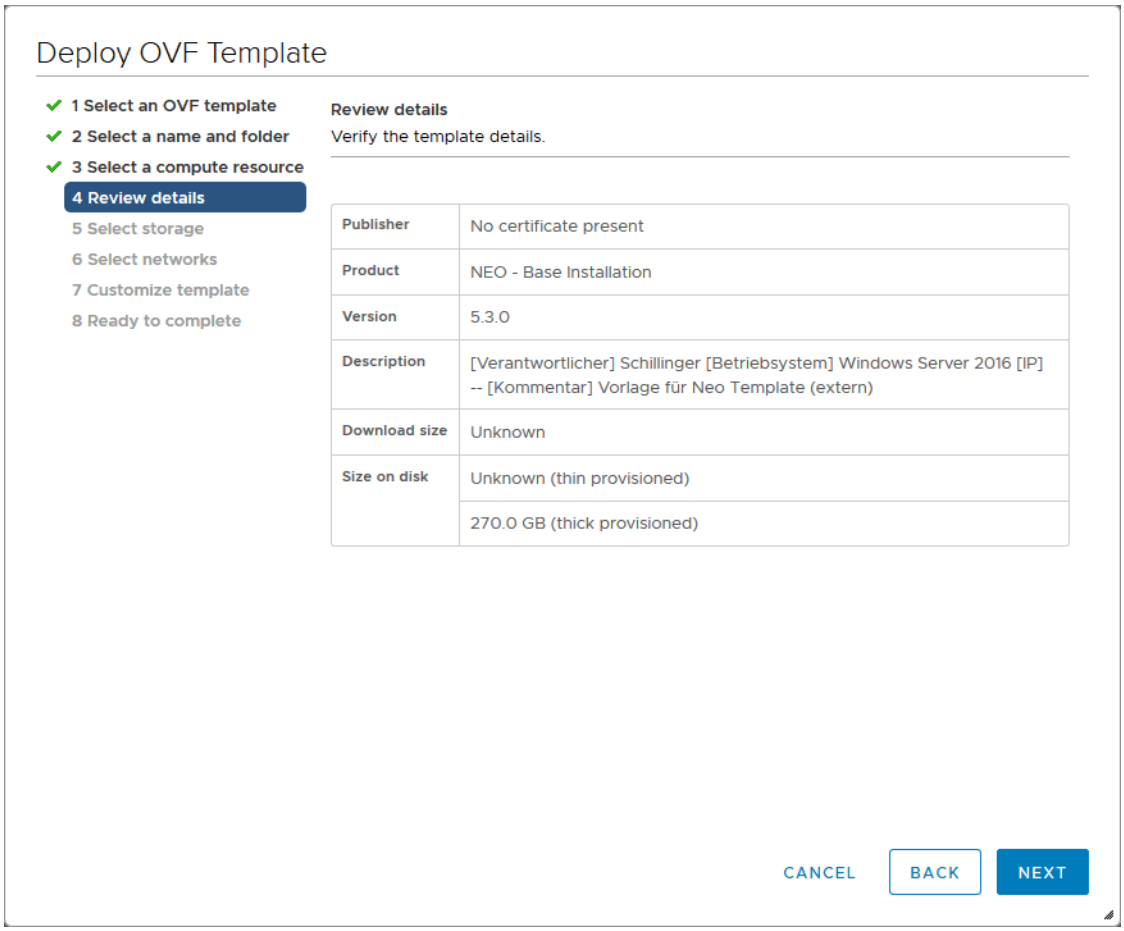

Fig. 9: Check details

20. For *Select virtual disk format*, select the required format for the VM from the drop-down list.

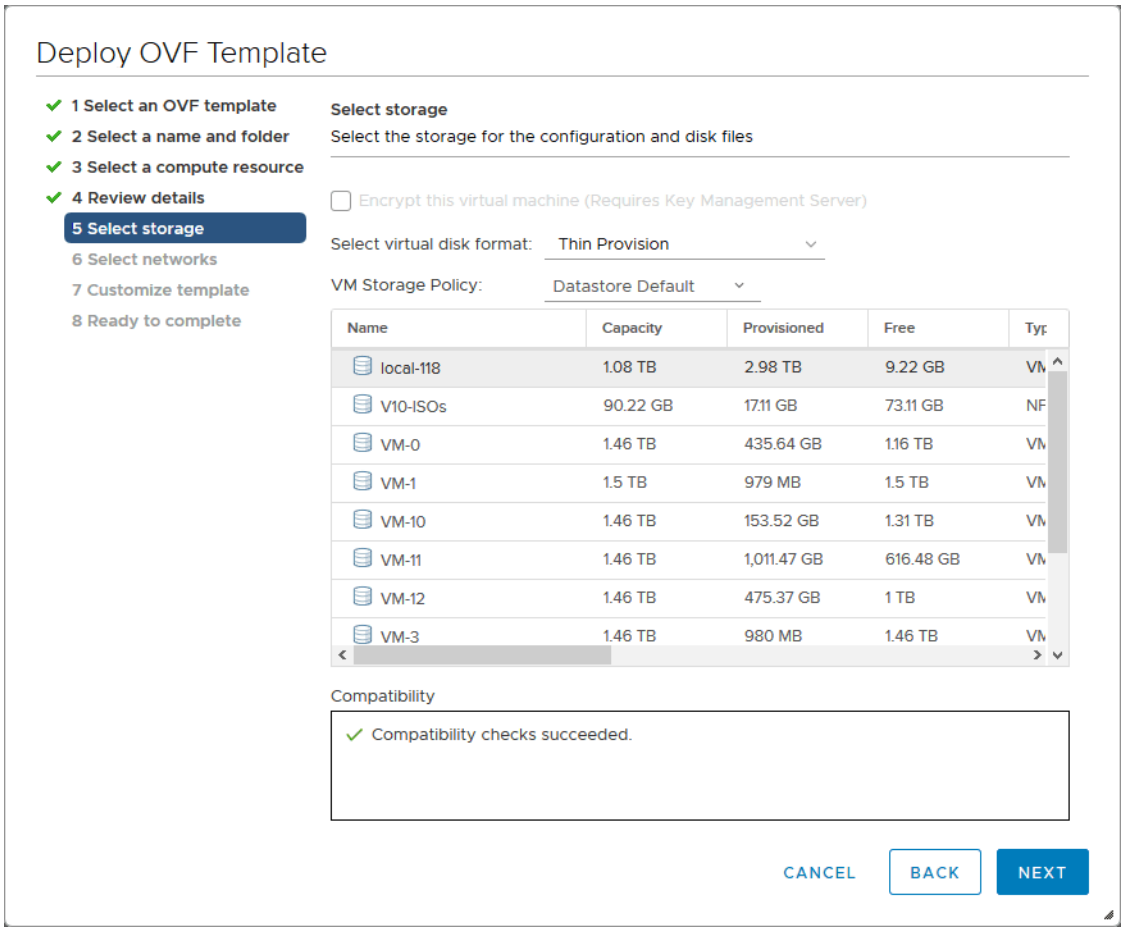

Fig. 10: Select storage location

21. Select the storage location for the VM storage policy.
22. Click on the button *NEXT*.
23. In the field *Destination Network*, select the required format for the DMZ2 network from the drop-down list.

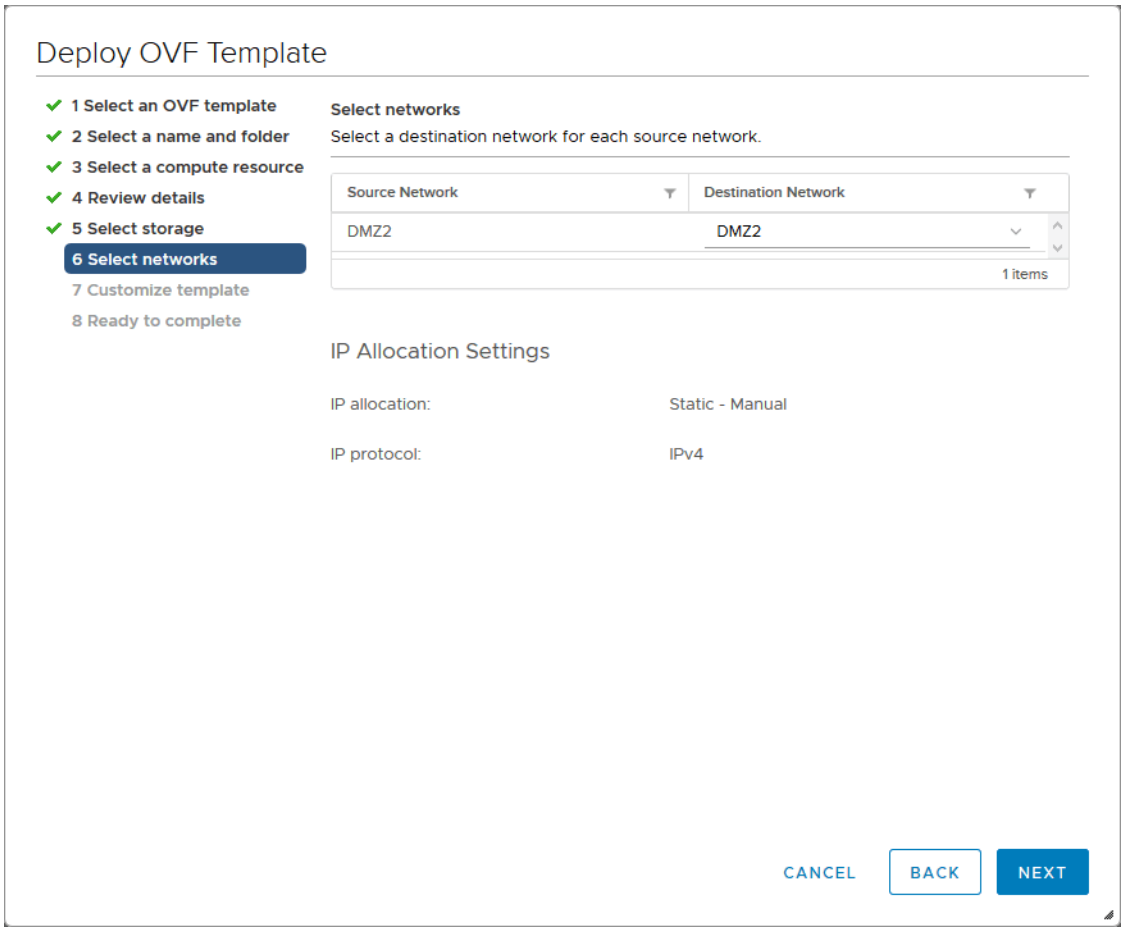

Fig. 11: Select networks

24. Click on the button *NEXT*.
25. Complete all required fields.

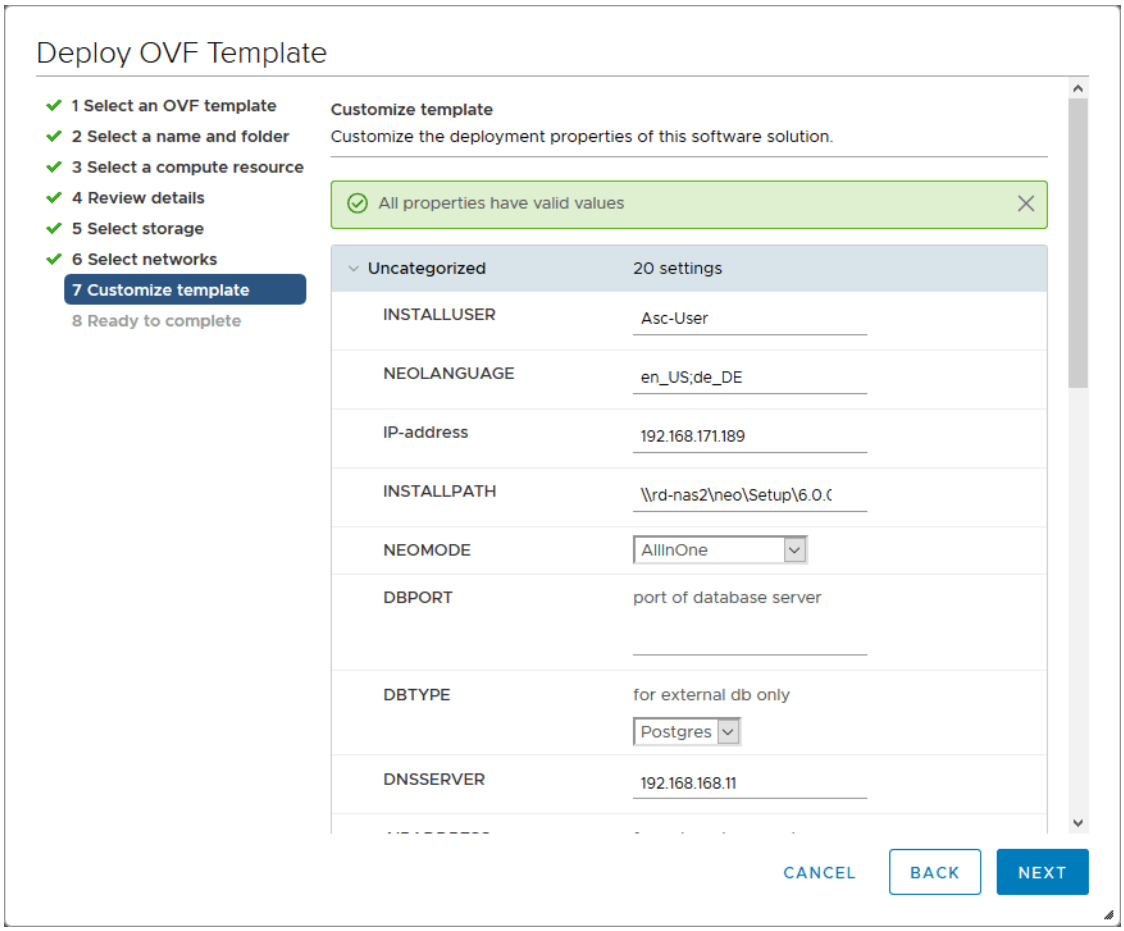

Fig. 12: Adjust template

The following parameters are available:

Parameter	Description
INSTALLUSER	Enter the user to access the installation path.
NEOLANGUAGE	Enter the languages to be installed for *neo*, *en_US;de_DE*.
IP-address	Enter the IP address of the network.
INSTALLPATH	Enter the path to the *neo* installation files. The path must not contain more than one ISO file. The ISO file is used automatically for the setup.
NEOMODE	From the drop-down list, select one of the following options: • *AllInOne* = *neo*-VM with Core and with DB • *external db* = *neo*-VM with Core and with external DB • *without core* = *neo*-VM without Core and with DB • *without core/db* = *neo*-VM without Core and without DB
DBPORT	Enter the value *1433* for MSSQL Standard. If a Named Instance is used, enter the differing port. Enter the value *5432* for POSTGRES. This information is not required for NEOMODE *AllInOne* or for *without core*.
DBTYPE	From the drop-down list, select one of the following options: • *Postgres* • *MSSQL* This information is not required for NEOMODE *AllInOne* or for *without core*.

Parameter	Description
DNSSERVER	Enter the IP address for the DNS network.
AIPADDRESS	Enter the IP address for the AIP (Core). This information is not required for NEOMODE *AllInOne* or for *external db*.
DBINSTANCE	If you use MSSQL and Named Instance, enter the name of the Named Instance. If no information is entered, the ASC default is entered. This information is not required for NEOMODE *AllInOne* or for *without core*.
POSTGRESHOST	Option: Enter the IP address for the DB which requires remote access (e. g. with remote recorder). You can create several IP/Netmasks separated by semicolons. The format IP/Netmask is mandatory.
INSTALLPASSWORD	Enter the password to access the installation path.
COMPUTERNAME	Option: Enter the computer name. Observe Microsoft's conventions!
DBUSER	Enter the external DB user. If no information is entered, the ASC default is entered. This information is not required for NEOMODE *AllInOne* or for *without core*.
DEFAULTNTP	Option: Enter the IP address for the NTP server of *neo*.
CLUSTERID	Option: Enter the cluster ID. The server name is entered as default ID here. For All-in-One systems you can apply this ID. If you set up a multi-server system with several application servers, you must replace the default ID for all application servers with another arbitrary cluster ID which is identical for all application servers.
DBIP	Enter the IP address for the external DB. This information is not required for NEOMODE *AllInOne* or for *without core*.
default gateway	Enter the IP address for the network.
netmask	Enter the IP address for the network mask.
DBPASSWORD	Enter the password for the external DB. If no information is entered, the ASC default is entered. This information is not required for NEOMODE *AllInOne* or for *without core*.

26. Click on the button *NEXT*.
27. Click on the button *FINISH*.

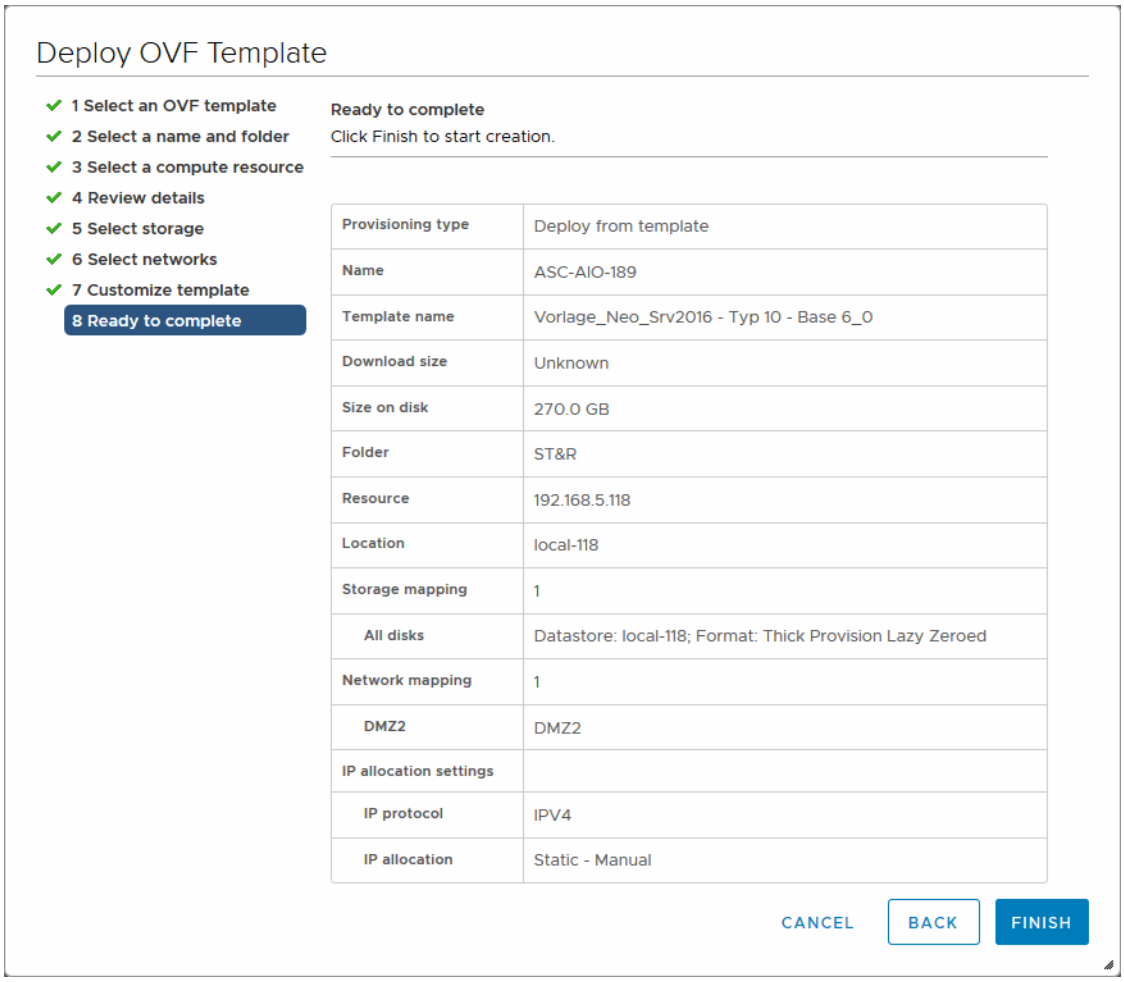

Fig. 13: Ready to finish

28. The successful completion of creating the VM is displayed in the table.

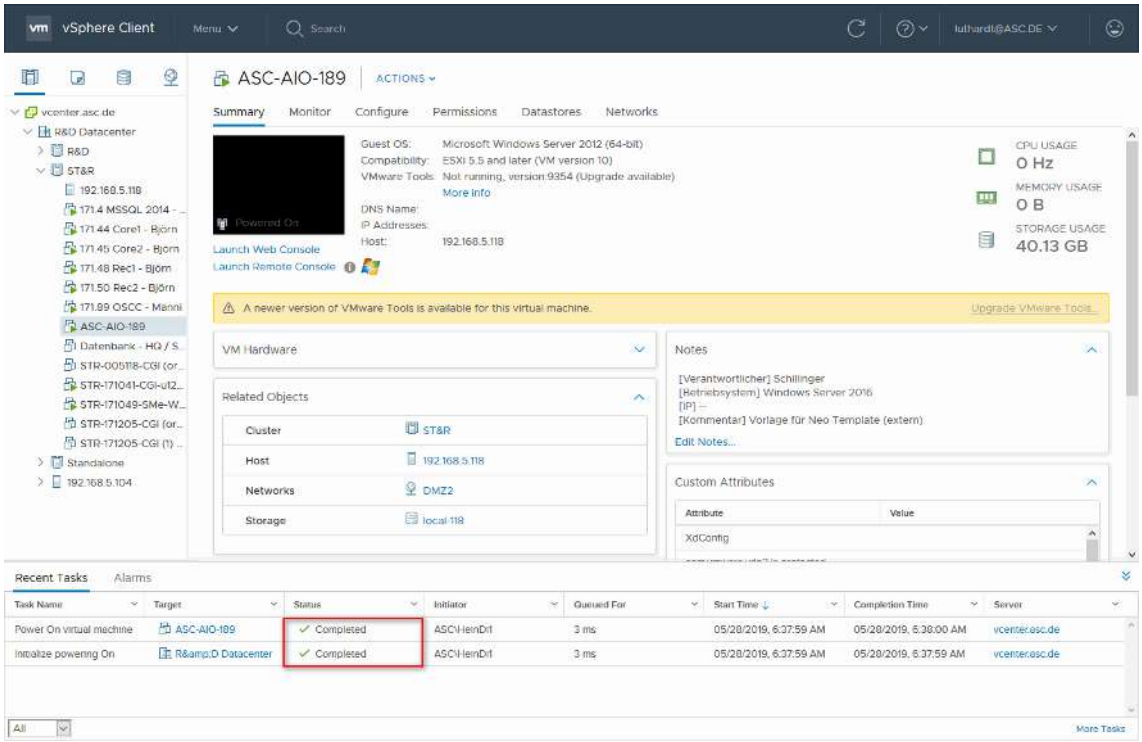

Fig. 14: VM creation completed

29. In the structure view, right-click on the directory where you have created the new VM.

⇨ A context menu appears.

30. Click on the entry *Power* > *Power On* in the context menu.

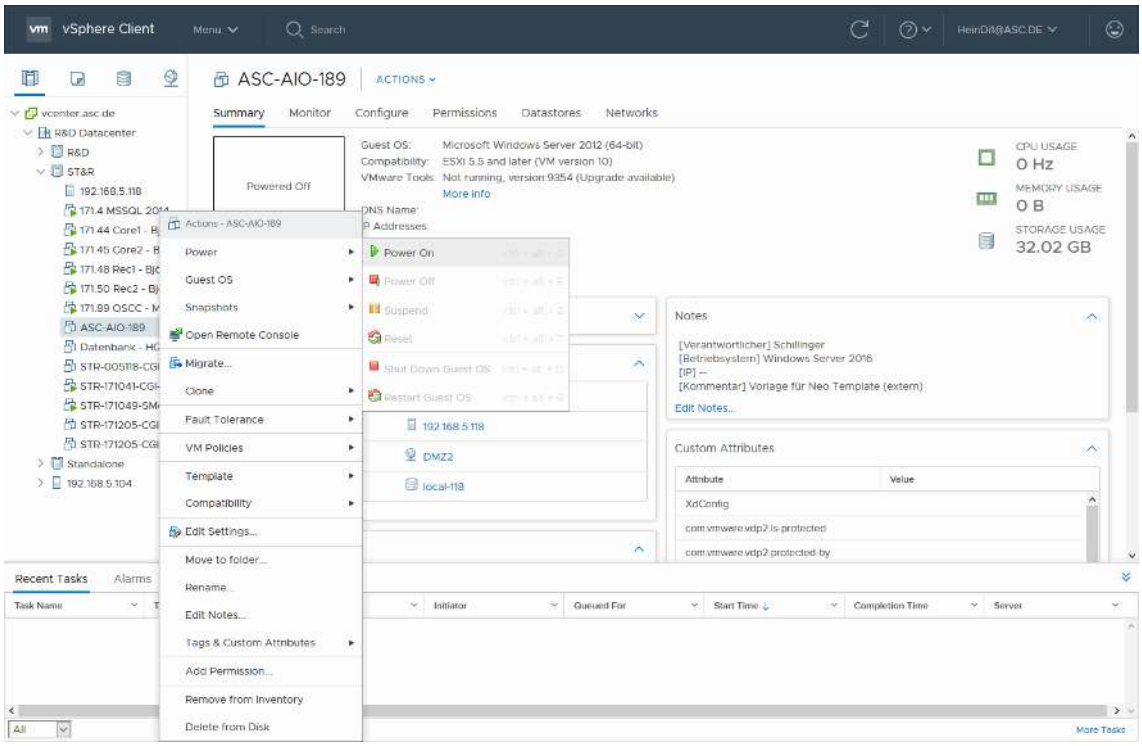

Fig. 15: Power on

31. The configurations script is started automatically.
32. Click on the small VM window to see the progress of the configuration.

⇨ The VM is displayed in a separate tab.

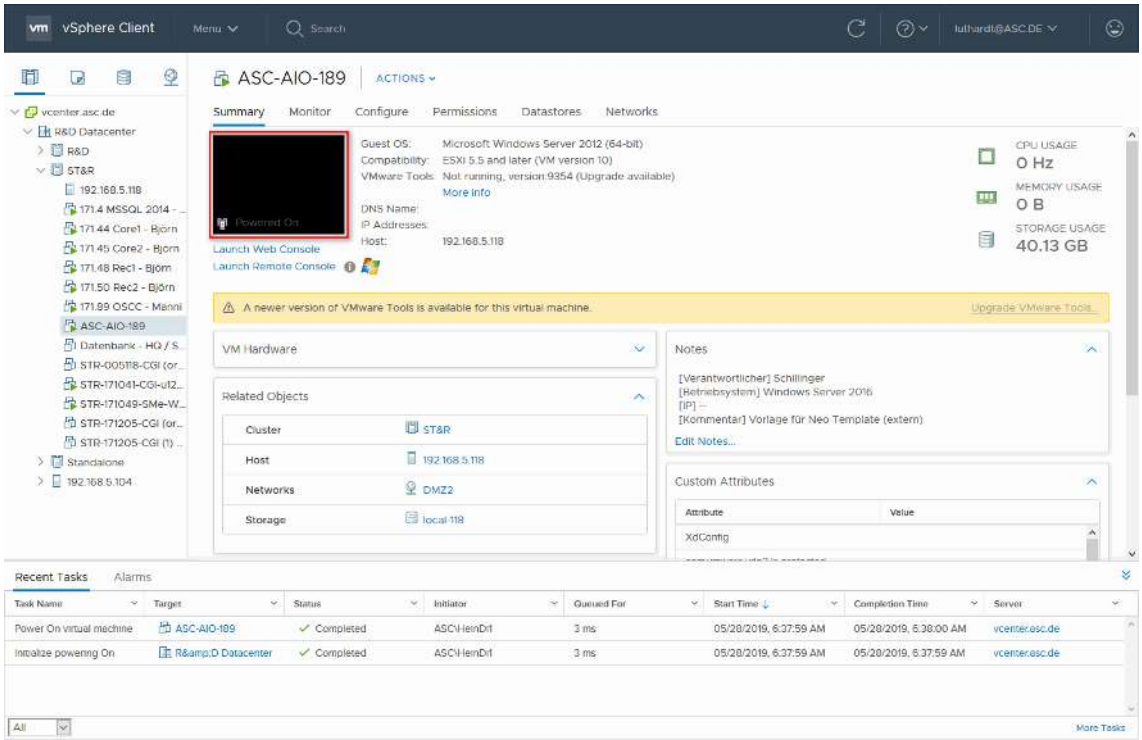

Fig. 16: Display VM in a separate tab of the browser

33. Change to the tab VM in the browser.
34. During the configuration, the VM is restarted several times automatically.

35. Upon completing the basic configuration, the VM is switched off automatically.

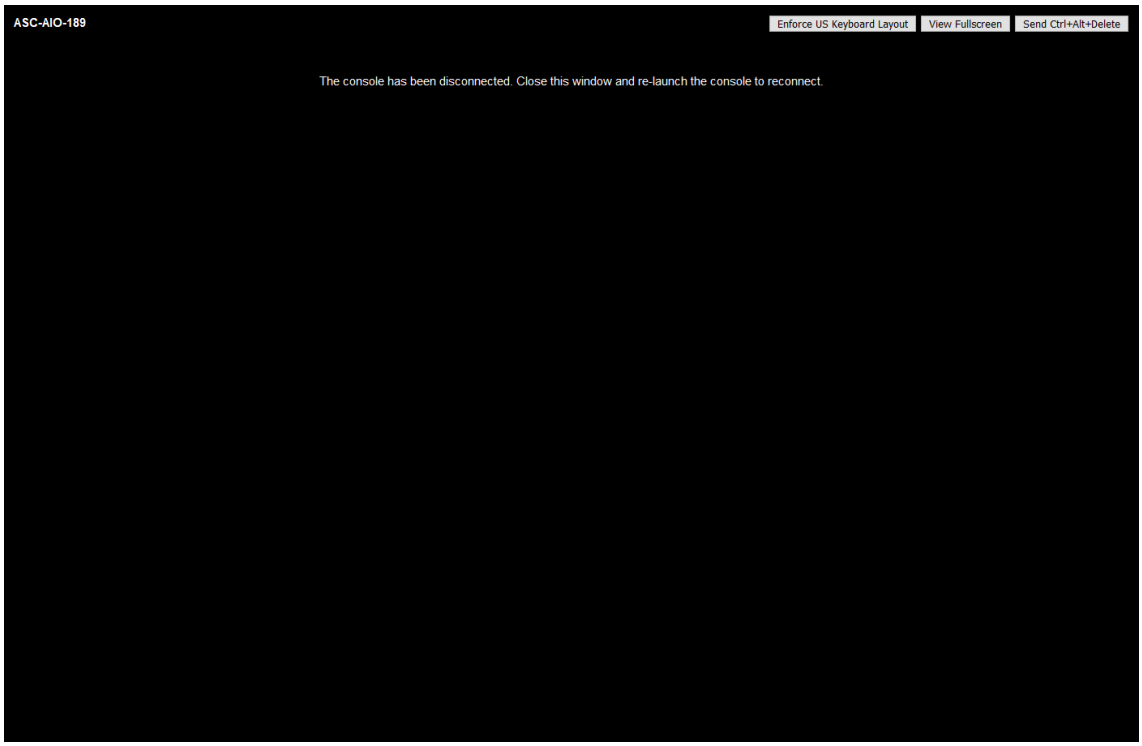

Fig. 17: VM switched off automatically

36. Close the tab VM.
37. In the structure view, right-click on the directory where you have created the new VM.
    ⇨ A context menu appears.
38. Click on the entry *Power* > *Power On* in the context menu.

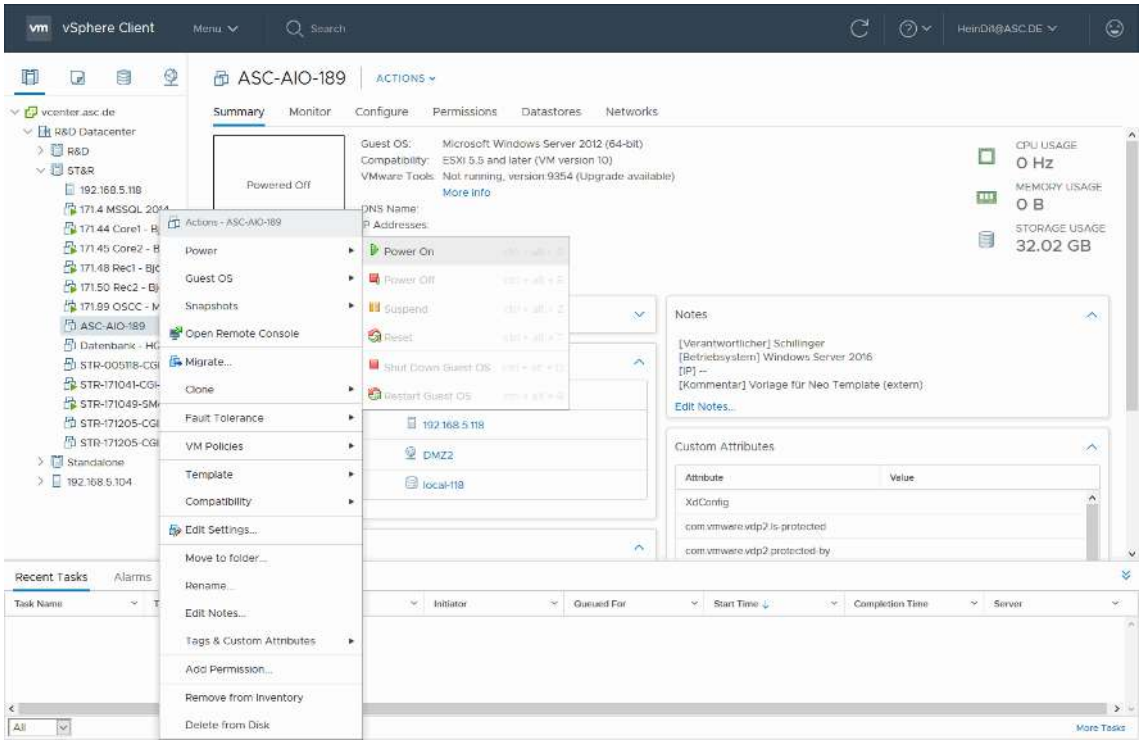

Fig. 18: Power on

39. Click on the small VM window.
    ⇨ The VM is displayed in a separate tab.

40. Change to the tab VM in the browser to configure Windows.
41. Select the respective language from the drop-down lists.

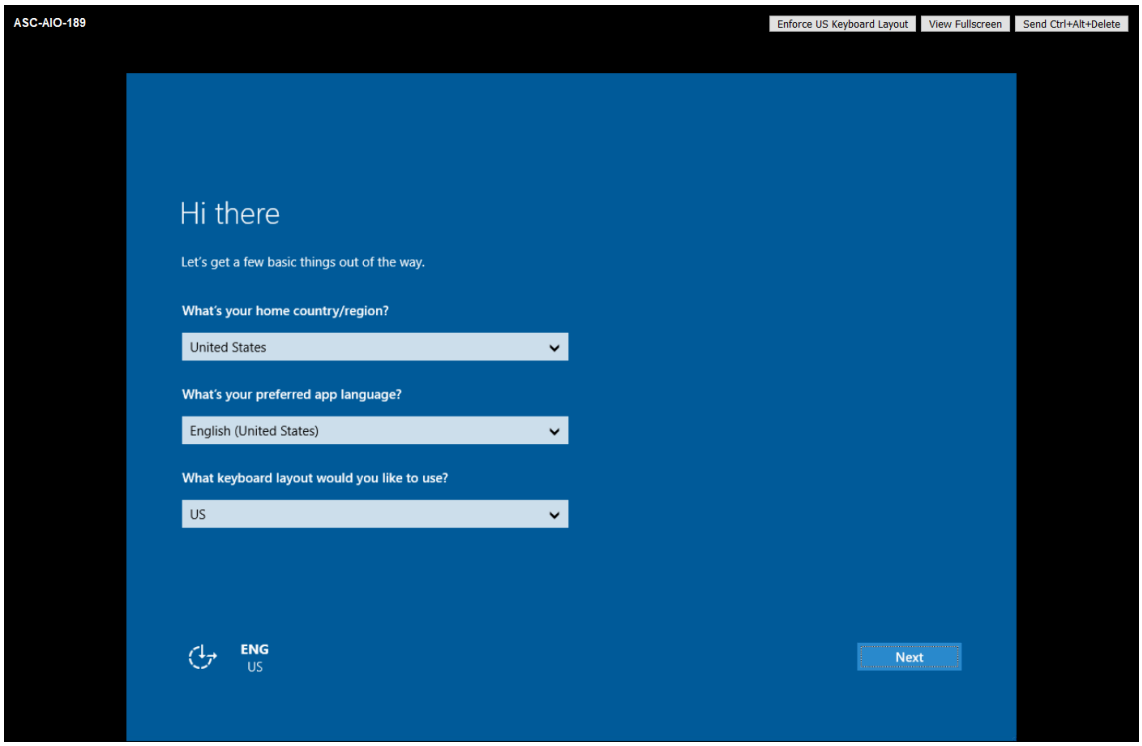

Fig. 19: Select language

42. Click on the button *NEXT*.
43. Enter the Windows product key.

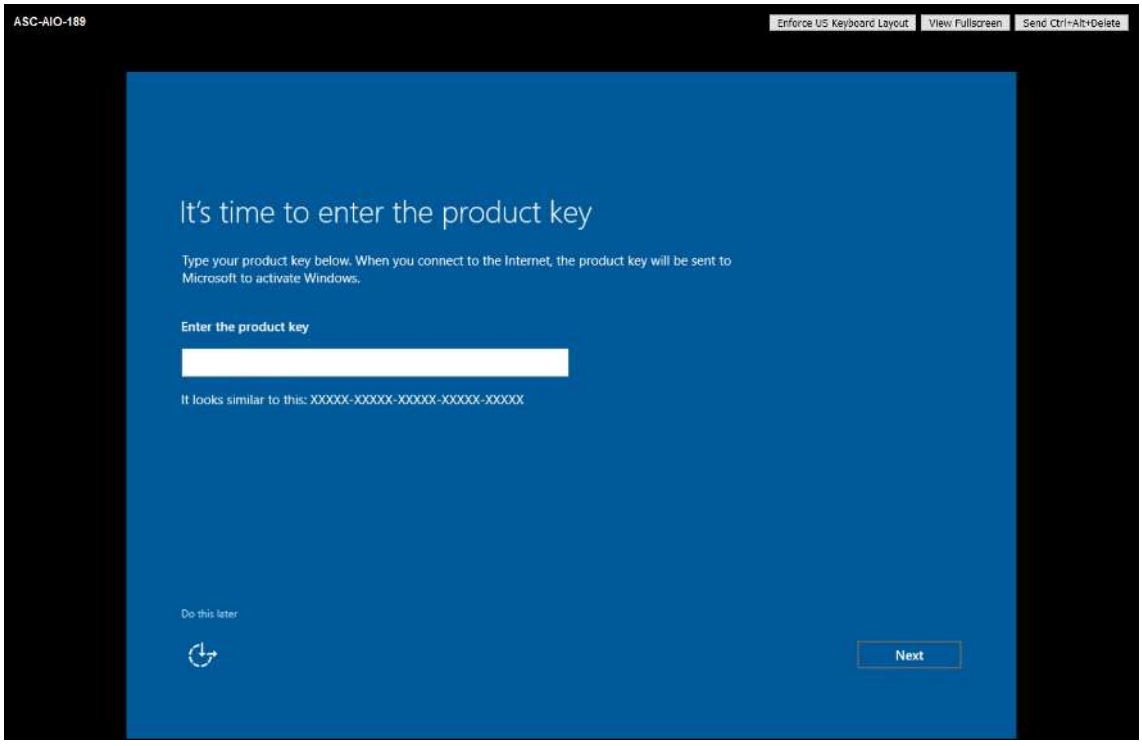

Fig. 20: Enter Windows product key

44. Click on the button *NEXT*.
45. Click on the button *Accept* to accept the license terms.

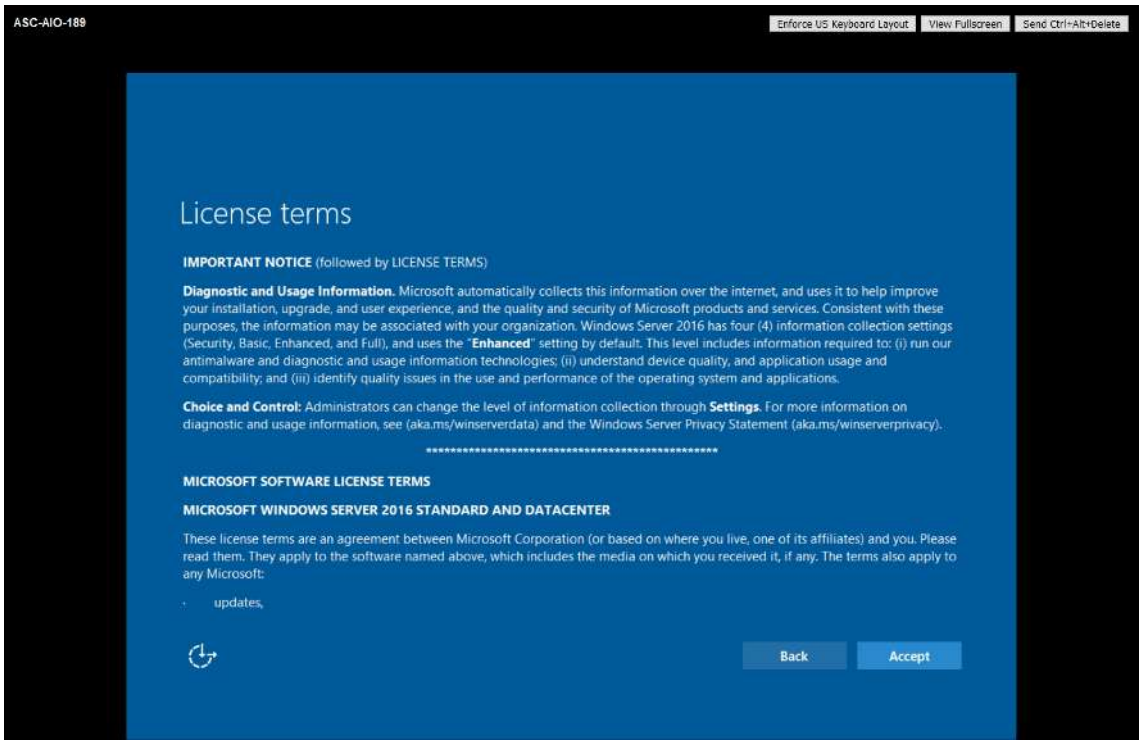

Fig. 21: Accept license terms

46. In the field *Password*, enter the password for the local administrator.
47. In the field *Reenter password*, enter the password again.

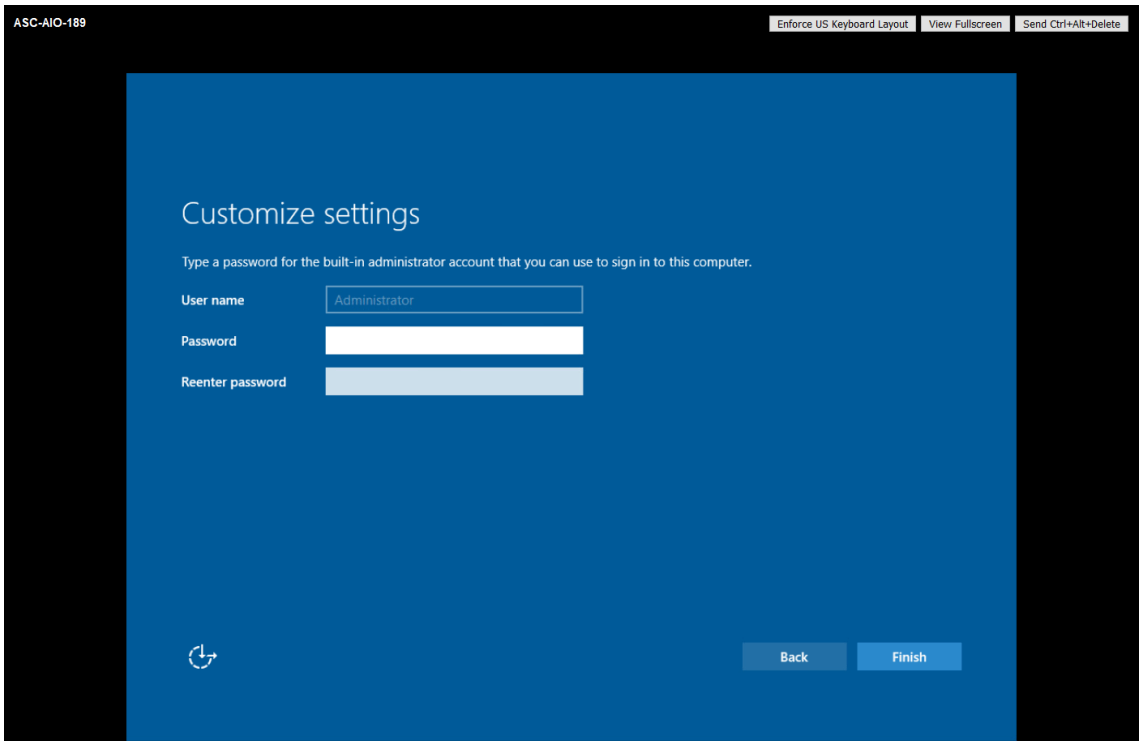

Fig. 22: Enter password for local administrator

48. Click on the button *Finish*.
49. Click on the button *Send Ctrl+Alt+Delete*.
50. Enter the password for the local administrator and press the Enter key.
    ⇨ The last adaptions are made before the window *Neo version installed successfully - press button for reboot* appears.

51. Click on the button *Reboot VM* to finish the configuration.

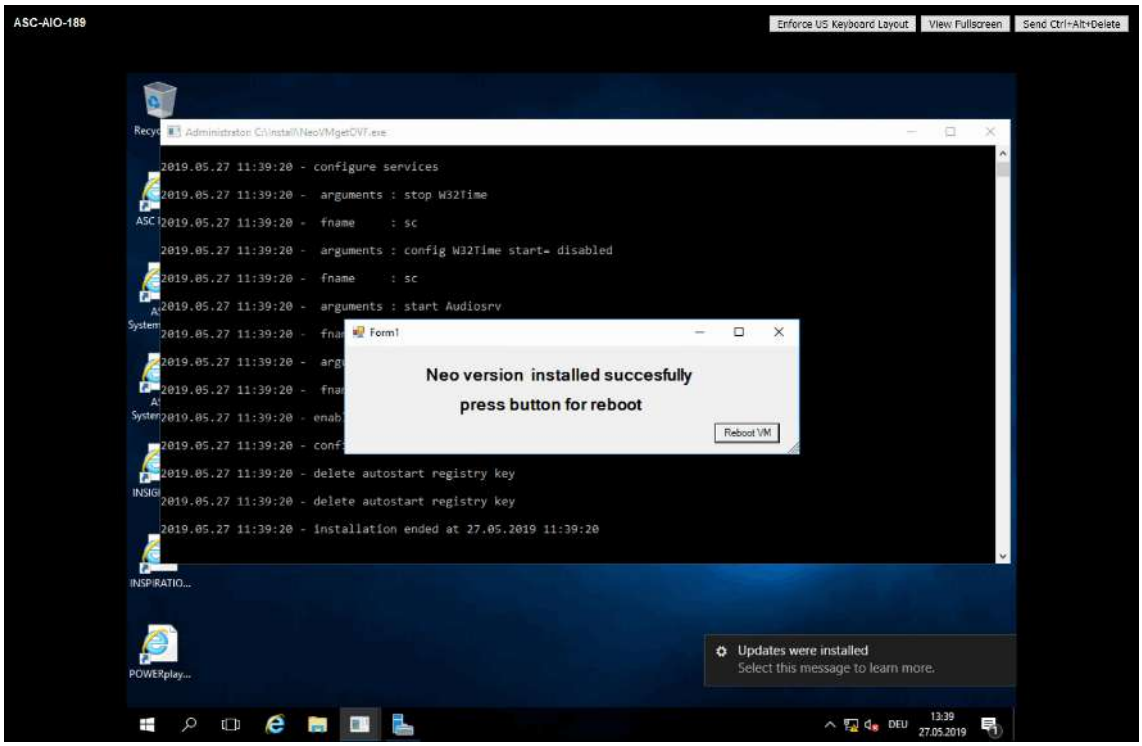

Fig. 23: neo version installed successfully

52. Close the tab VM.

4.3 Configuration vNetwork standard switches

The following chapters of this document describe the configuration of vSwitches for VMware ESXi servers by means of the VMware vSphere client or the VMware vCenter client. The configuration is necessary to guarantee that the ASC software functions correctly if it is supposed to be used in an ESXi-hosted virtual network.

This document merely covers the basic configuration of the vSwitches of the VMware ESXi software and not the basic installation or configuration of the VMware ESXi software in general. Neither the installation nor the configuration of the VMware vSphere Client and the VMware vCenter client are part of this document. This information can be found in the manufacturer documentation *Manual for the server configuration for ESXi*.

vNetwork standard switches are abstract network devices which fulfill the following tasks in a VMware ESXi-hosted virtual network:

- Control of the data traffic between virtual machines and external physical networks
- Control of the data traffic between virtual machines
- Combination of the bandwidth of several network adapters
- Distribution of the data traffic of several network adapters
- Mapping of failover scenarios in physical network adapters
- Substitution of a physical ethernet switch

When two or more virtual machines have been connected to the same vSwitch, the network data transfer between these virtual machines is controlled locally. When an uplink adapter is connected to the vSwitch, any virtual machine can access the external network that the adapter is connected to. In order to emulate the connection of the ASC software to a physical network best possible, two vSwitches have to be created. One for the administration of the ASC software and the ESXi server as well as another for the purpose of passive recording.

The following paragraphs of this chapter describe the setup of the vSwitches if the ASC software is supposed to be used in a VMware ESXi-hosted network.

For more information about the switch configuration refer to the administration manual *Configuration switch for passive VoIP recording*.

4.3.1 vSphere client

4.3.1.1 Create vSwitch for administration

For communication with the ASC software for configuration and maintenance purposes a separate vSwitch is required which is created as follows:

1. Log into the vSphere Client and click on the host in the inventory list window.
2. Click on the tab *Configuration*.

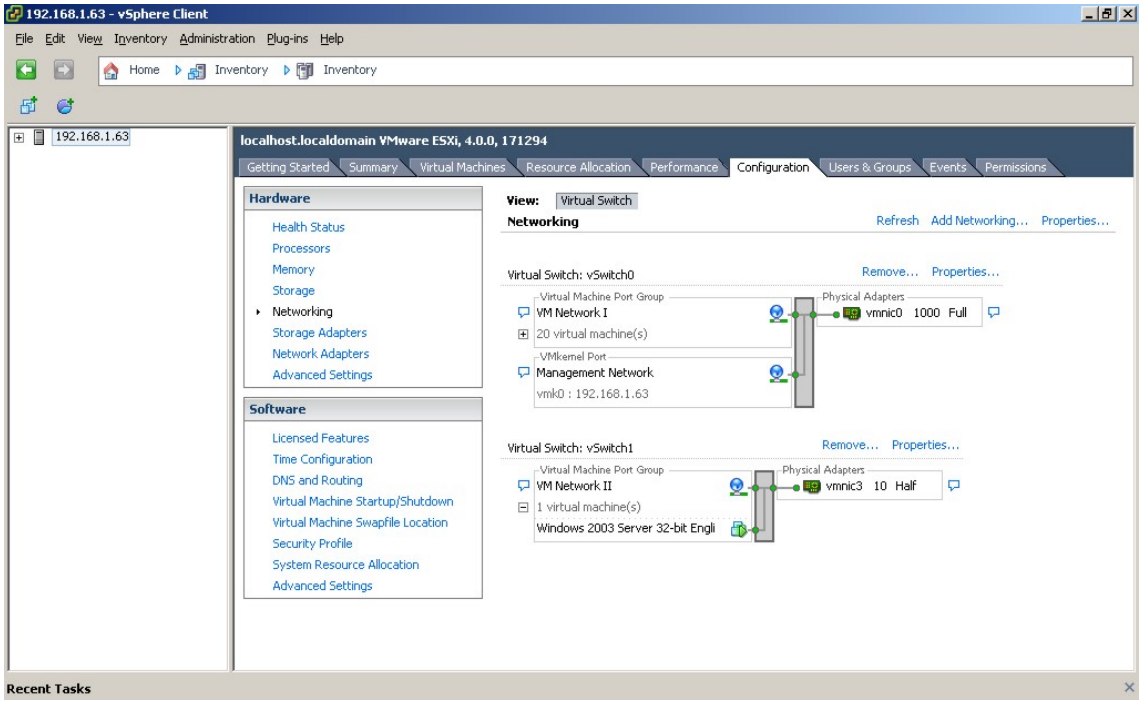

Fig. 24: vSphere Client (example)

3. Click on the menu item *Networking*.
4. Select the view *Virtual Switch*.
5. Click on *Add Networking*.
6. Accept the default connection type *Virtual Machine* and click on the button *Next*.

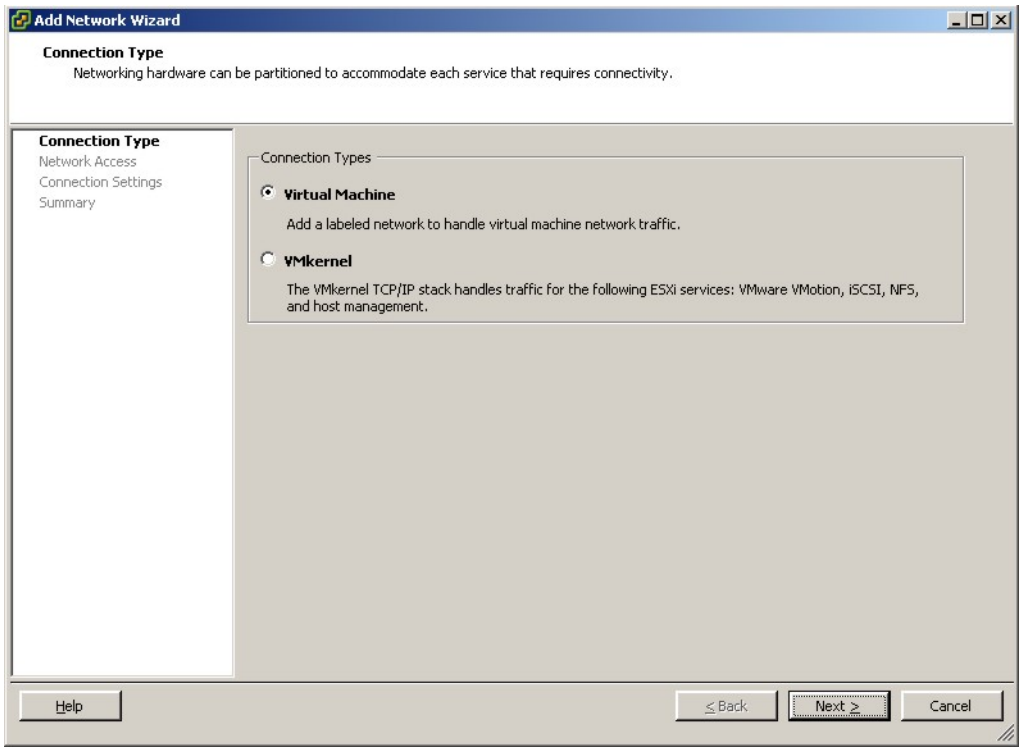

Fig. 25: Add virtual machine

7. Activate the option *Create a virtual switch* and the assigned physical adapters which are supposed to be connected to this vSwitch.

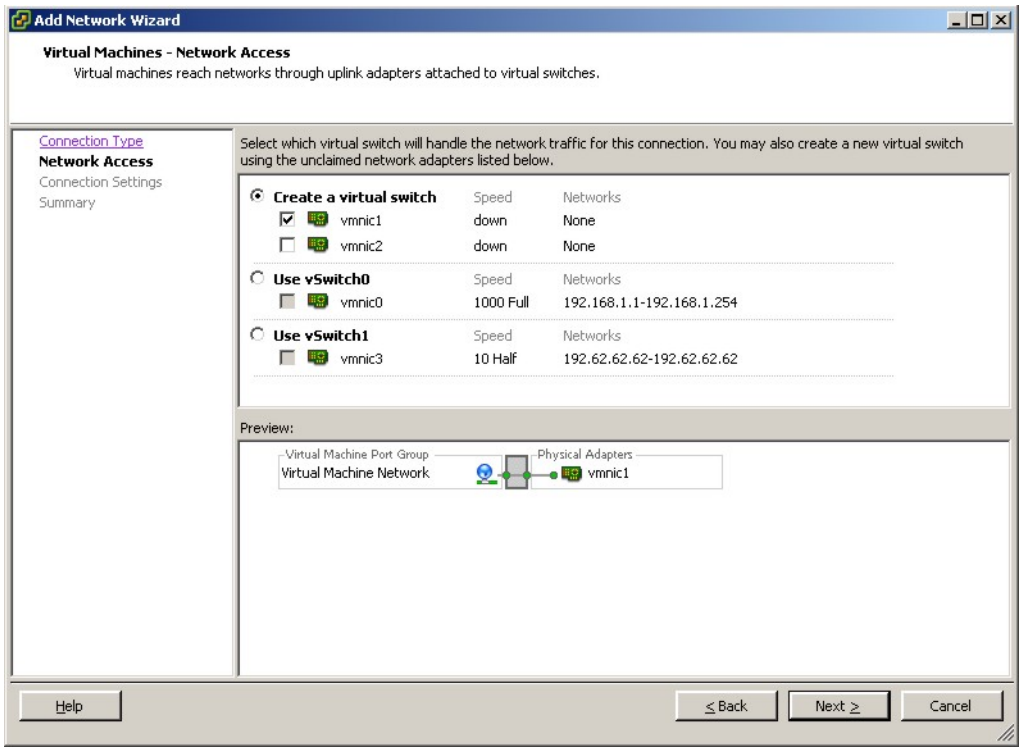

Fig. 26: Create a virtual switch (example)

8. Click on the button *Next*.
9. In the entry field *Network Label*, enter a term for the port group to be created (e. g. VM Network I).

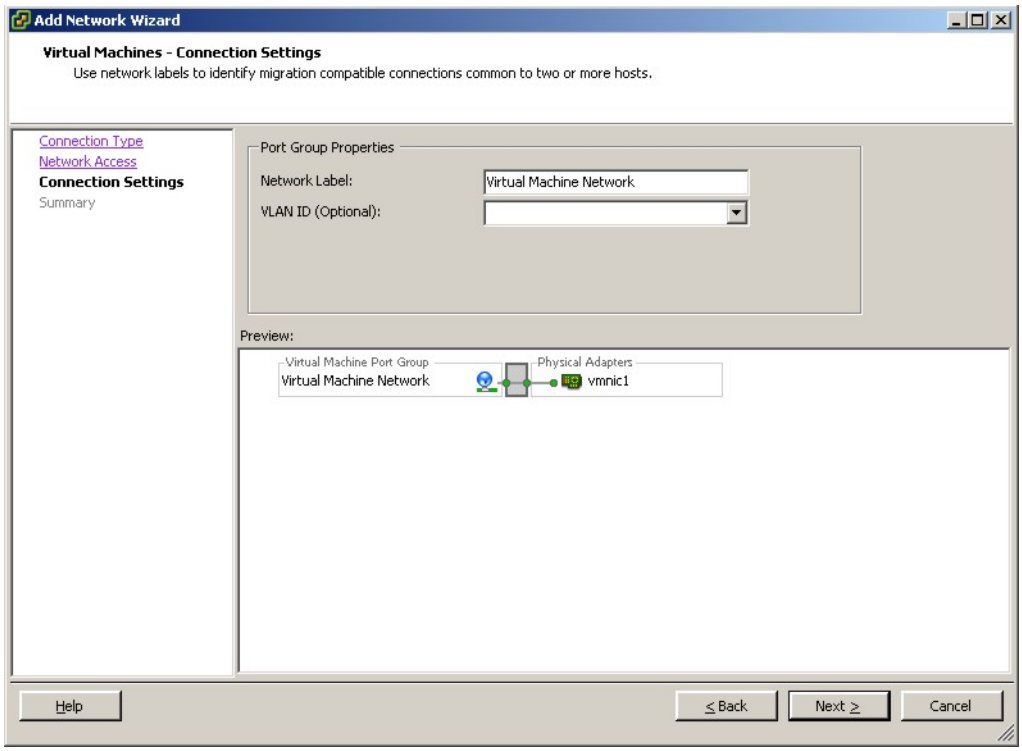

Fig. 27: Enter network label (example)

10. Click on the button *Next*.
11. Verify that the vSwitch has been configured properly.

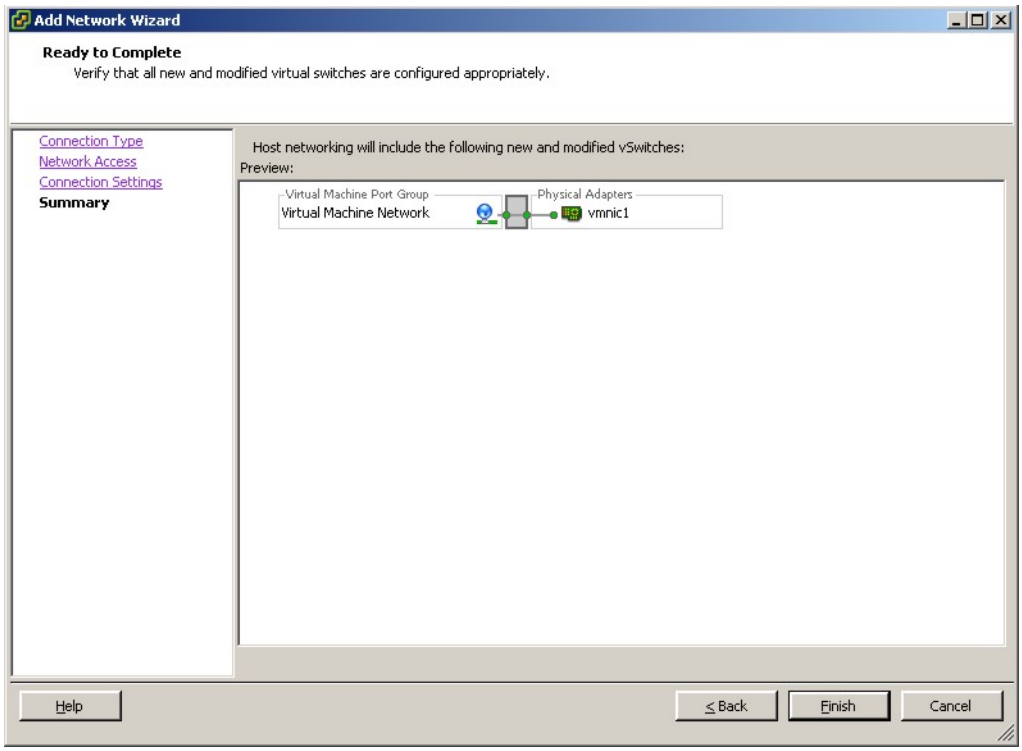

Fig. 28: Configuration ready to finalize (example)

12. Click on the button *Finish*.

When all configuration steps mentioned above have been concluded, the vSwitch has been created successfully and is ready for enhanced configuration.

4.3.1.2 Configure vSwitch for administration

For the new vSwitch for administration to be used with the ASC software, the following configuration steps have to be carried out:

1. Click on the *Properties* of the corresponding vSwitch.
2. Click on the configuration *vSwitch*.

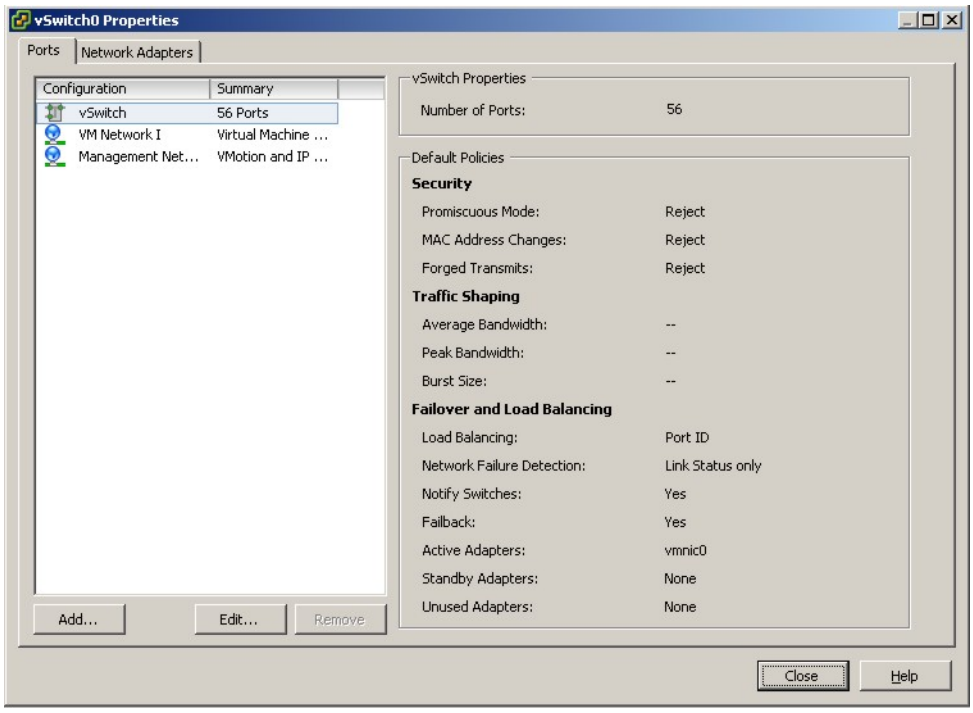

Fig. 29: Edit vSwitch (example)

3. Click on the button *Edit*.
4. Click on the tab *Security*.

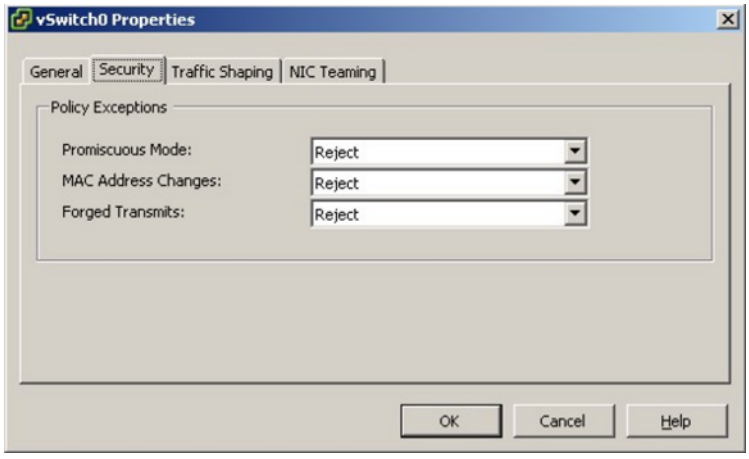

Fig. 30: Define policy exceptions

5. From the drop-down list, select the parameter *Reject* for the following options:
   - *Promiscuous Mode*
   - *MAC Address Changes*
   - *Forged Transmits*
6. Click on the button *OK*.
7. Verify the configuration.

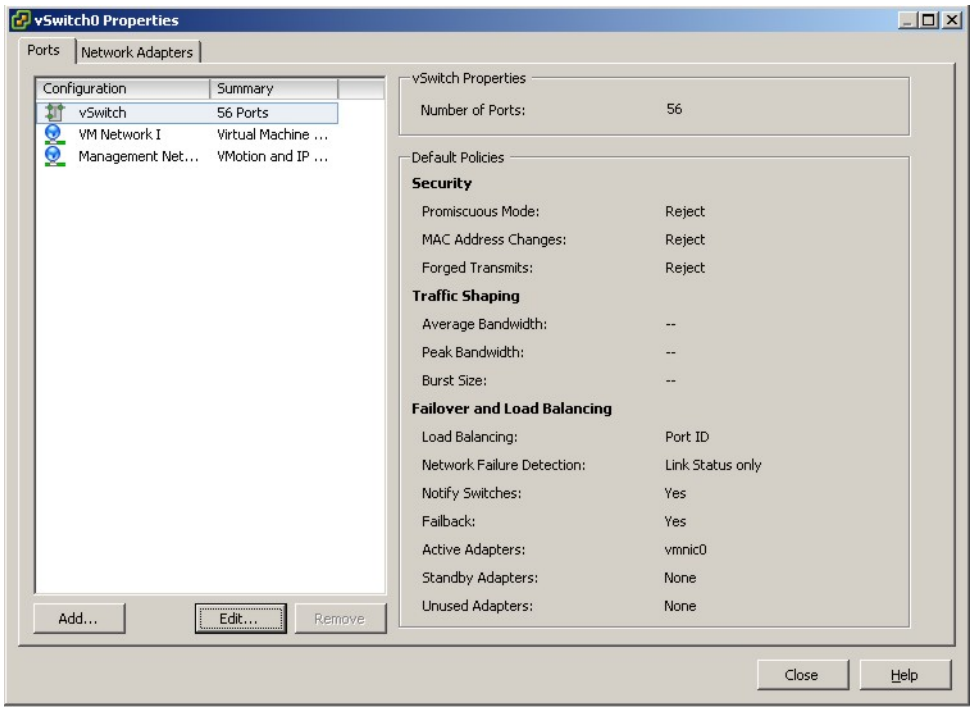

Fig. 31: Verify vSwitch configuration (example)

8. Select the respective virtual network which you have created in one of the previous configuration steps.

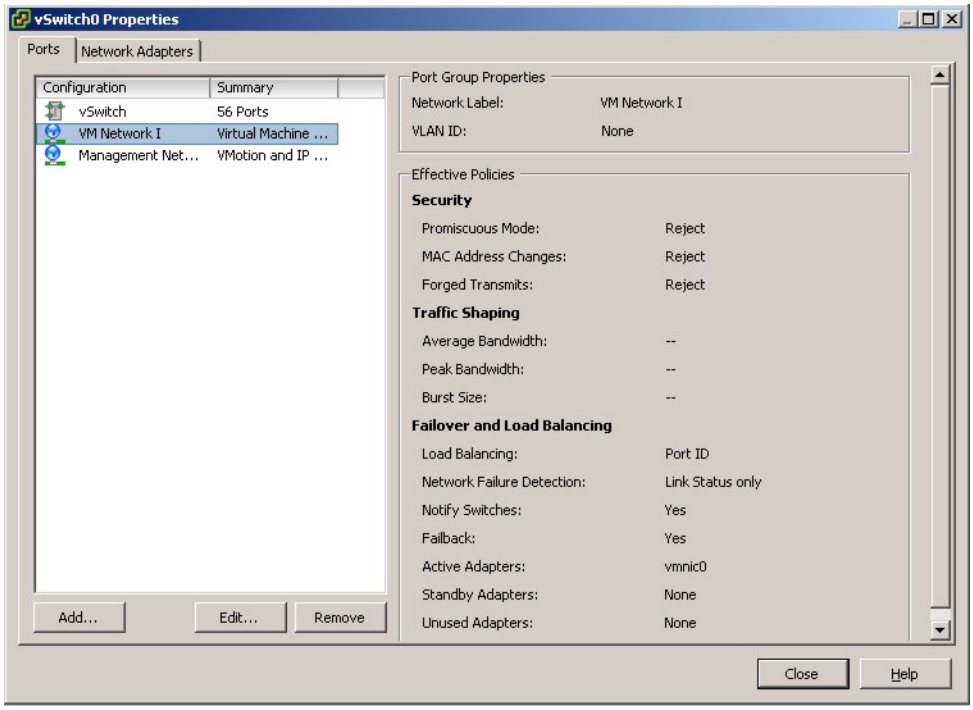

Fig. 32: Edit VM Network I (example)

9. Click on the button *Edit*.
10. Click on the tab *Security*.

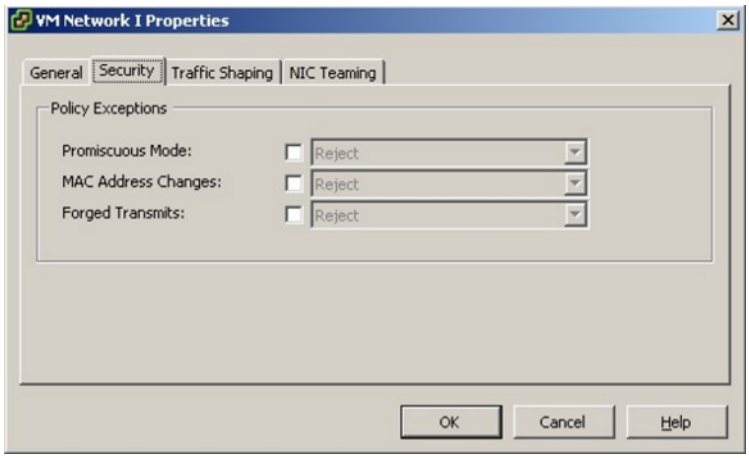

Fig. 33: Define policy exceptions

11. From the drop-down list, select the parameter *Reject* for the following options:
    - *Promiscuous Mode*
    - *MAC Address Changes*
    - *Forged Transmits*
12. Click on the button *OK*.

When all mentioned configuration steps have been carried out successfully, the ASC software can be configured via this interface.

4.3.1.3 Create vSwitch for passive recording

For passive recording by means of the ASC software, a separate vSwitch is required which is created as follows:

1. Log into the vSphere Client and click on the host in the inventory list window.
2. Click on the tab *Configuration*.

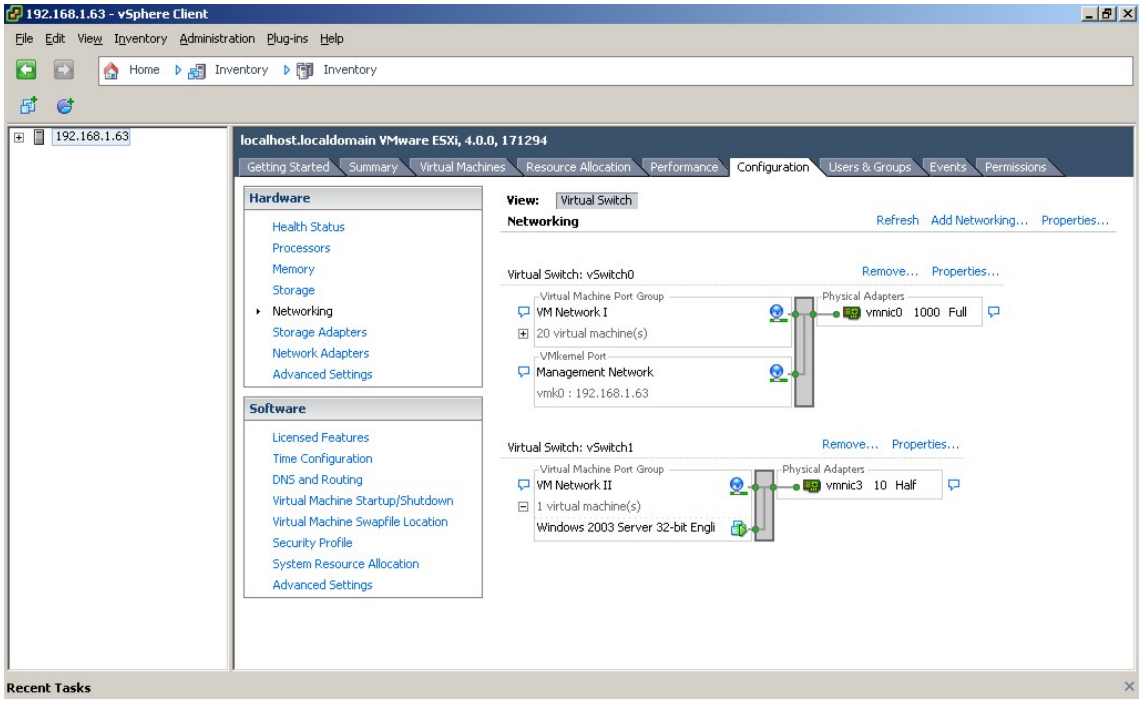

Fig. 34: vSphere Client (example)

3. Click on the menu item *Networking*.
4. Select the view *Virtual Switch*.

5. Click on *Add Networking*.
6. Accept the default connection type *Virtual Machine* and click on the button *Next*.

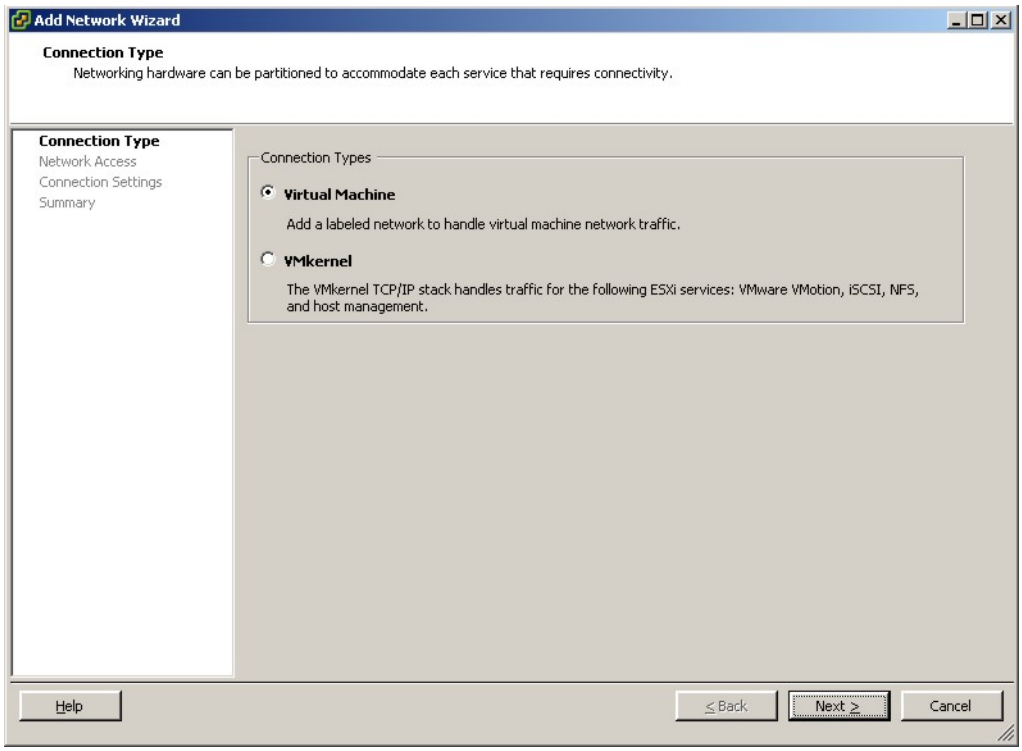

Fig. 35: Add virtual machine

7. Activate the option *Create a virtual switch* and the assigned physical adapters which are supposed to be connected to this vSwitch.

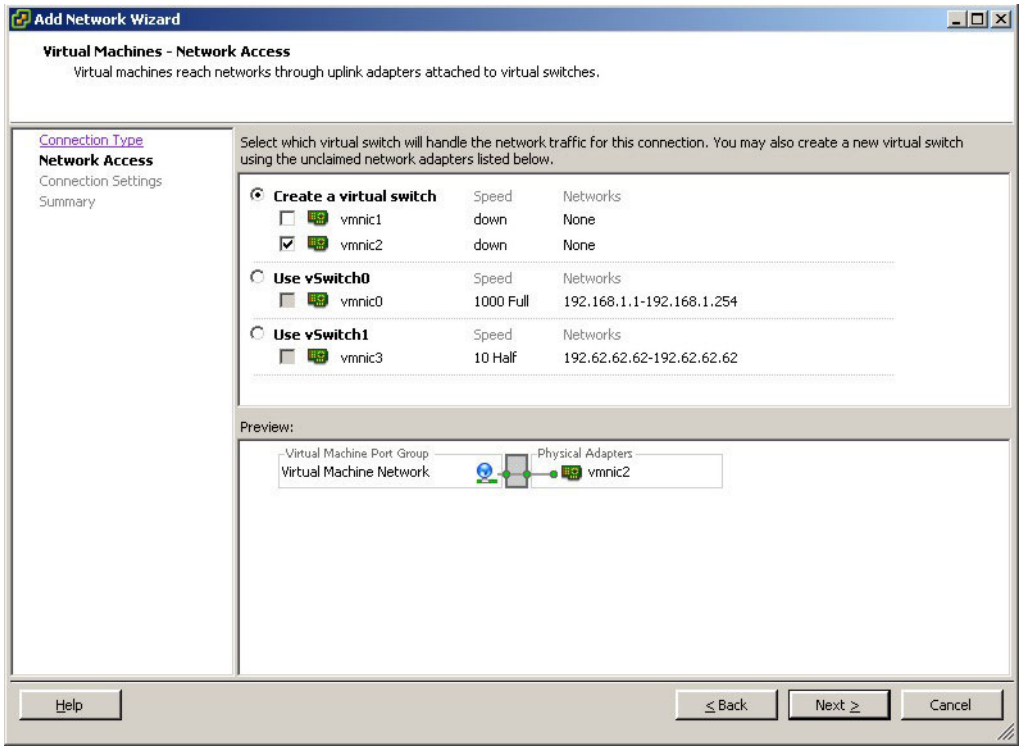

Fig. 36: Create a virtual switch (example)

8. Click on the button *Next*.
9. In the entry field *Network Label*, enter a description of the port group to be created (e. g. VM Network II).

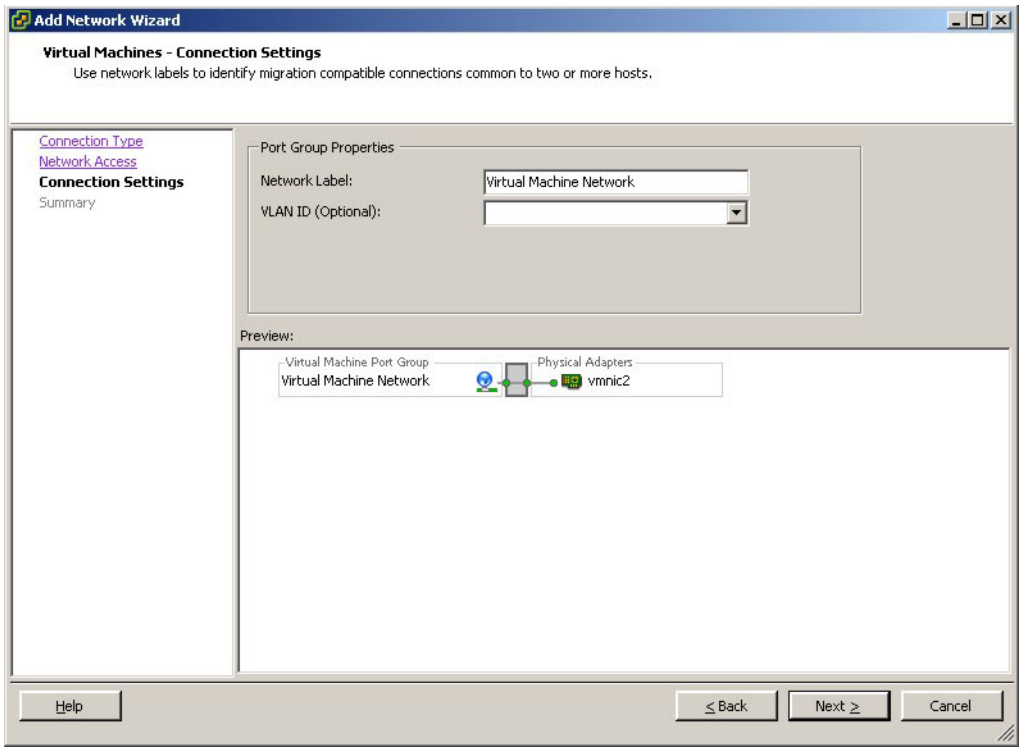

Fig. 37: Enter network label (example)

10. Click on the button *Next*.
11. Verify that the vSwitch has been configured properly.

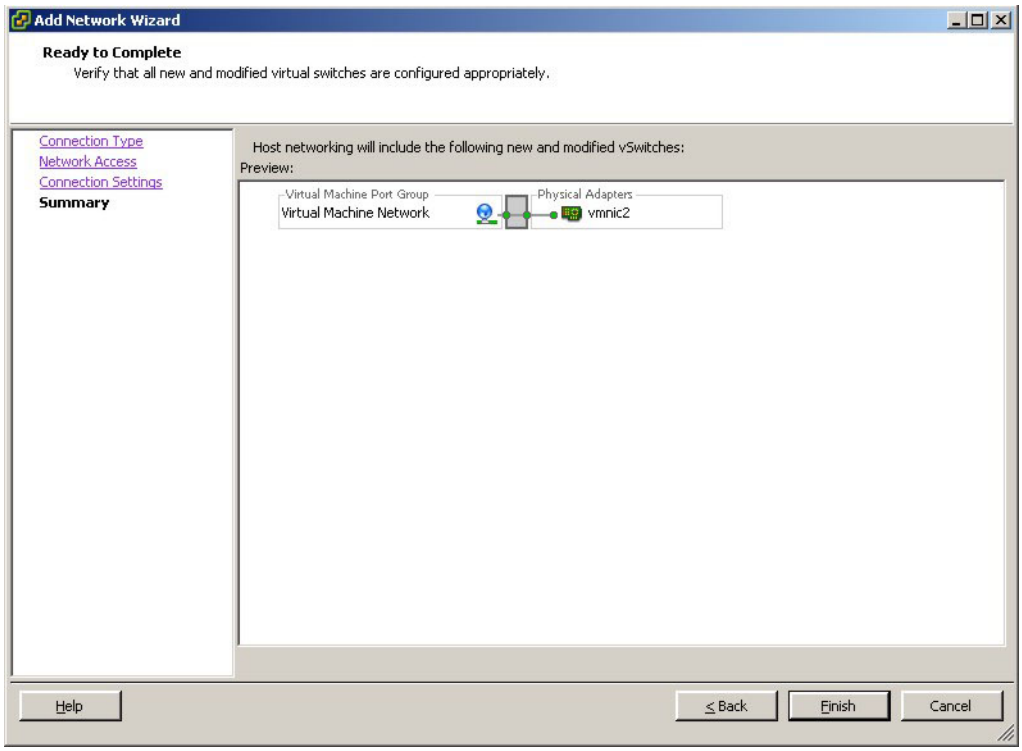

Fig. 38: Configuration ready to finalize (example)

12. Click on the button *Finish*.

When all configuration steps mentioned above have been concluded, the vSwitch has been created successfully and is ready for enhanced configuration.

4.3.1.4 Configure vSwitch for passive recording

For the new vSwitch for passive recording to be used with the ASC software, the following configuration steps have to be carried out:

1. Click on the *Properties* of the corresponding vSwitch.
2. Click on the configuration *vSwitch*.

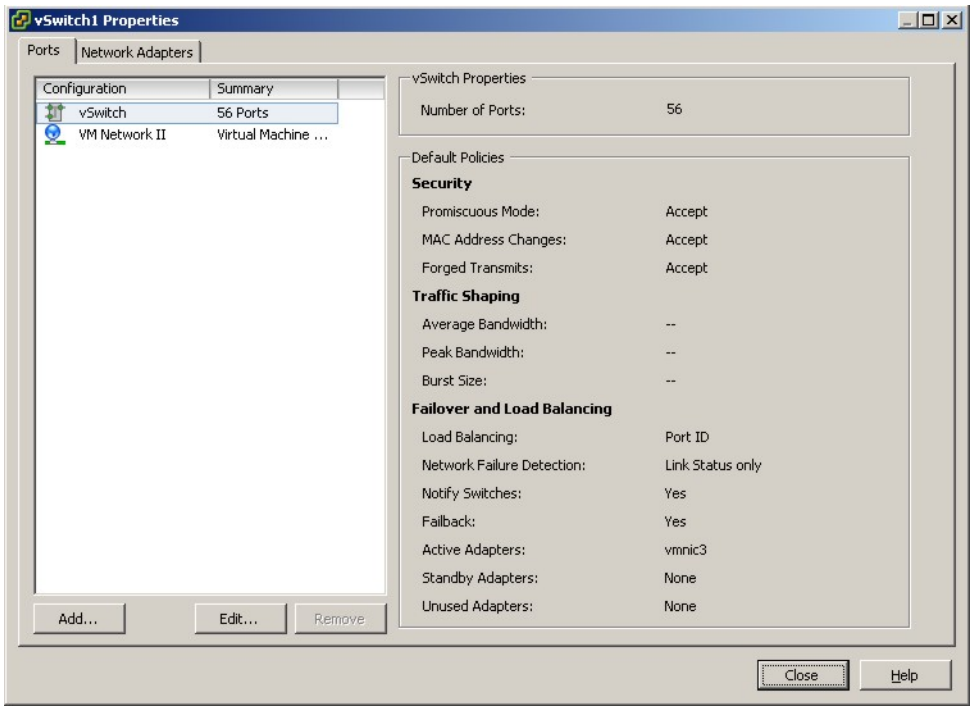

Fig. 39: Edit vSwitch (example)

3. Click on the button *Edit*.
4. Click on the tab *Security*.

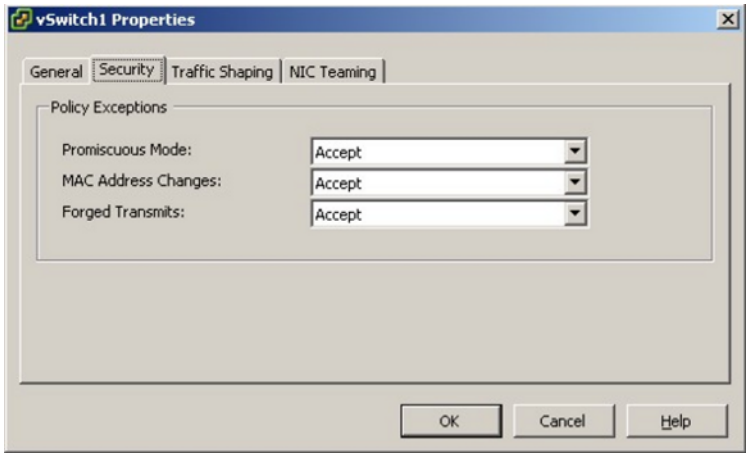

Fig. 40: Define policy exceptions

5. From the drop-down list, select the parameter *Accept* for the following options:
   - *Promiscuous Mode*
   - *MAC Address Changes*
   - *Forged Transmits*
6. Click on the button *OK*.
7. Verify the configuration.

8. Select the respective virtual network which you have created in one of the previous configuration steps.

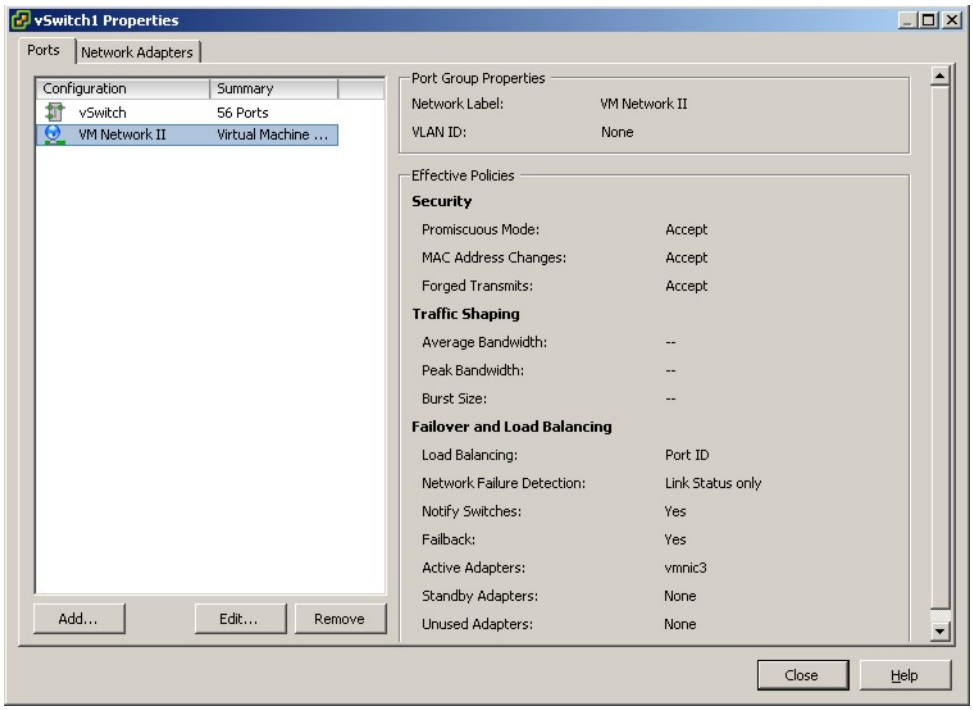

Fig. 41: Edit VM Network II (example)

9. Click on the button *Edit*.
10. Click on the tab *Security*.

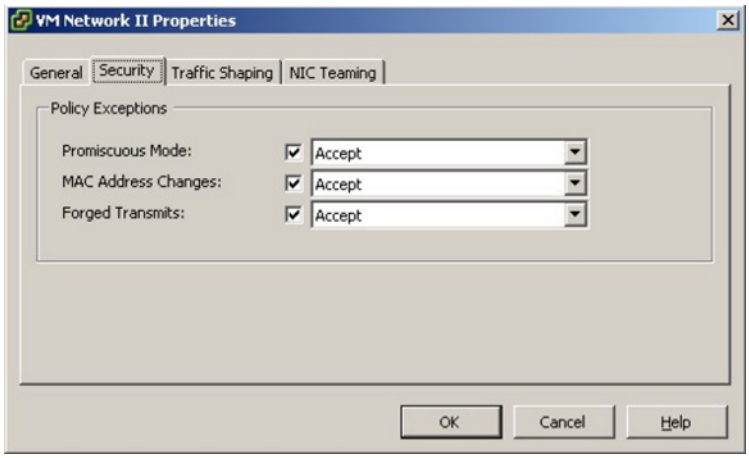

Fig. 42: Define policy exceptions

11. From the drop-down list, select the parameter *Accept* for the following options:
    - *Promiscuous Mode*
    - *MAC Address Changes*
    - *Forged Transmits*
12. Click on the button *OK*.

When all mentioned configuration steps have been carried out successfully, the ASC software can be used for passive recording via this interface.

4.3.2 vCenter client

4.3.2.1 Configuration vCenter standard switches

To communicate with the ASC software for configuration and maintenance purposes, a separate vSwitch is required which is created and configured as follows:

1. Log in to the vCenter client and click on the host in the inventory list window.
2. Click on the tab *Configure*.
3. Click on *Networking* > *Virtual switches*.
4. Open the virtual switch *Standard Switch: vSwitch8*.
5. Under the virtual switch *Standard Switch: vSwitch8*, click on the button *ADD NETWORKING*.

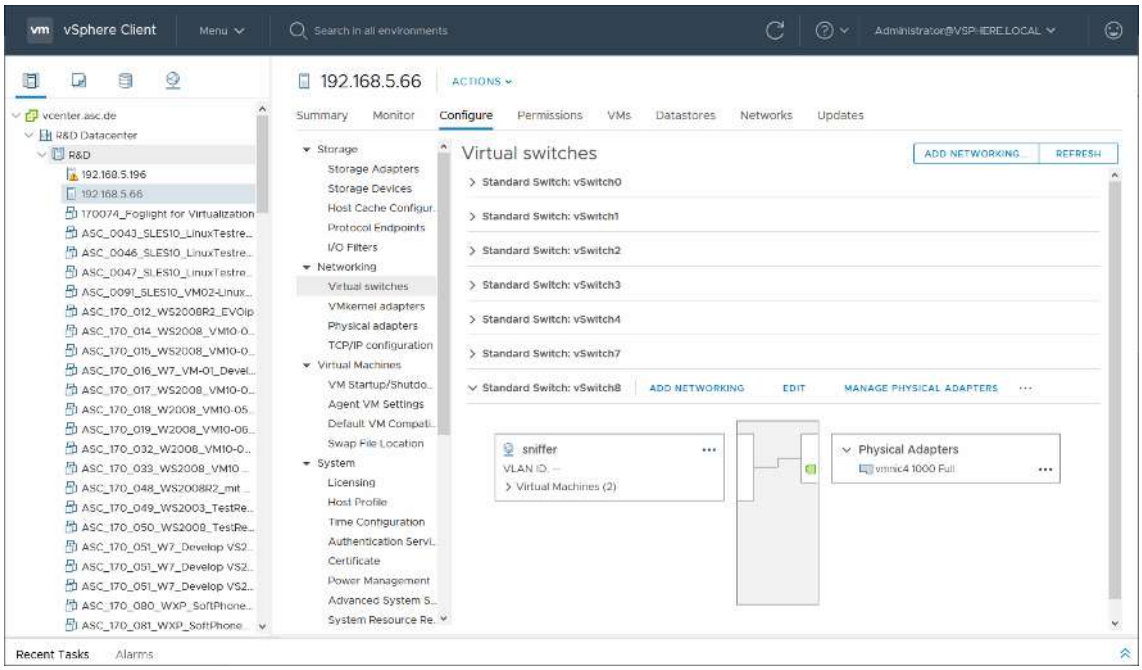

Fig. 43: Configure virtual switches (example)

6. Select the option *Virtual Machine Port Group for a Standard Switch* and click on the button *NEXT*.

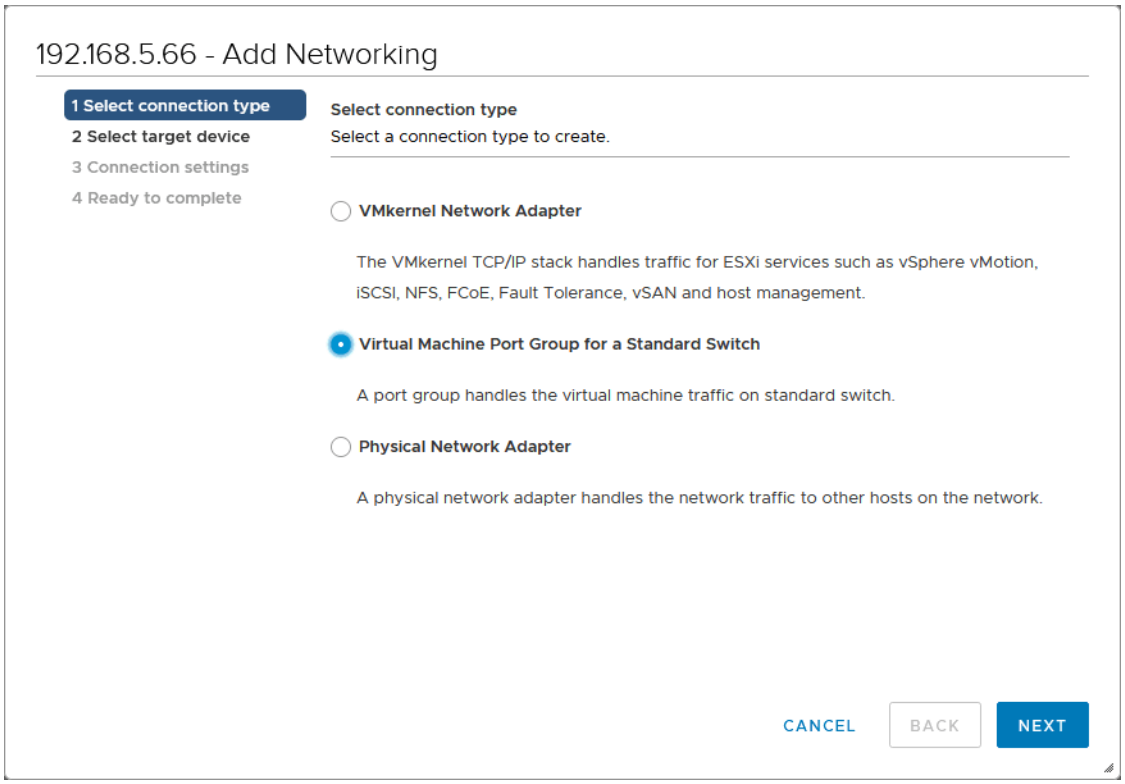

Fig. 44: Add networking (example)

Select either the option *Select an existing standard switch* or the option *New standard switch* as required.

Select an existing standard switch

1. Select the option *Select an existing standard switch*.
2. Click on the button *BROWSE*.

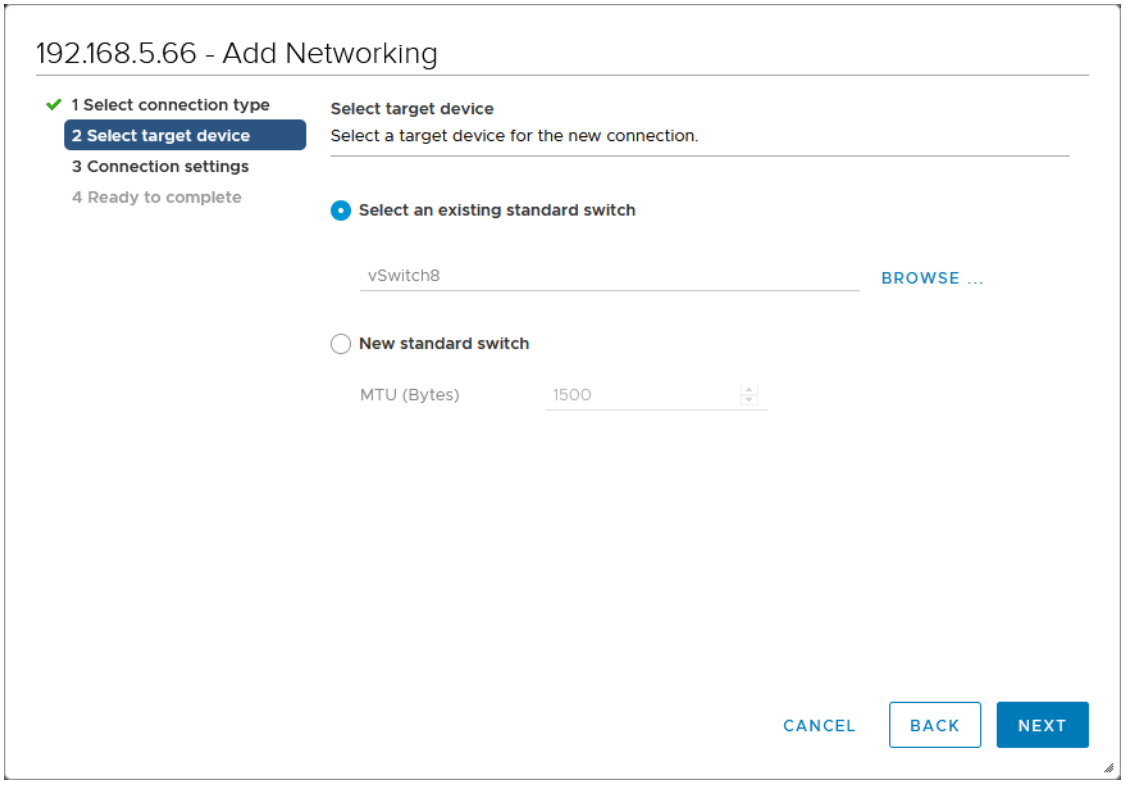

Fig. 45: Add networking (example)

3. Click on the required switch, e. g. *vSwitch8*.
4. Click on the button *OK*.

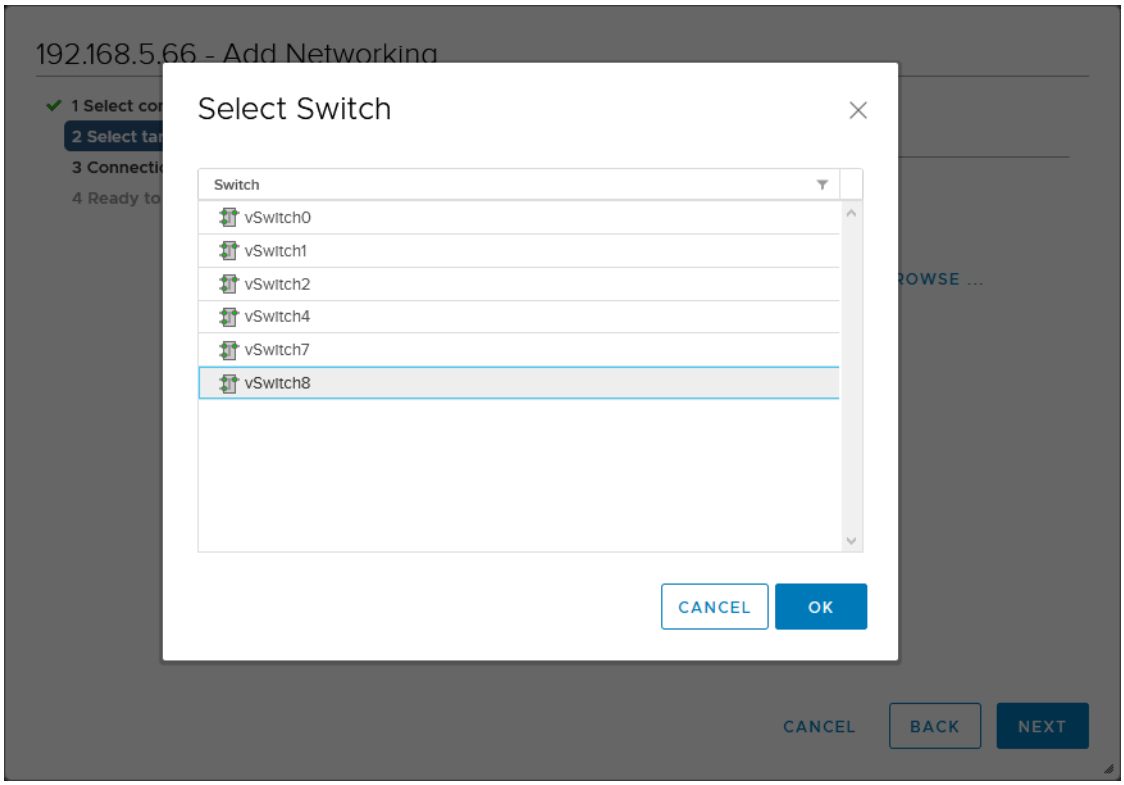

Fig. 46: Select switch (example)

5. Click on the button *NEXT*.
6. In the entry field *Network label*, enter a name for the network, e. g. *VM Network*.
7. Click on the button *NEXT*.

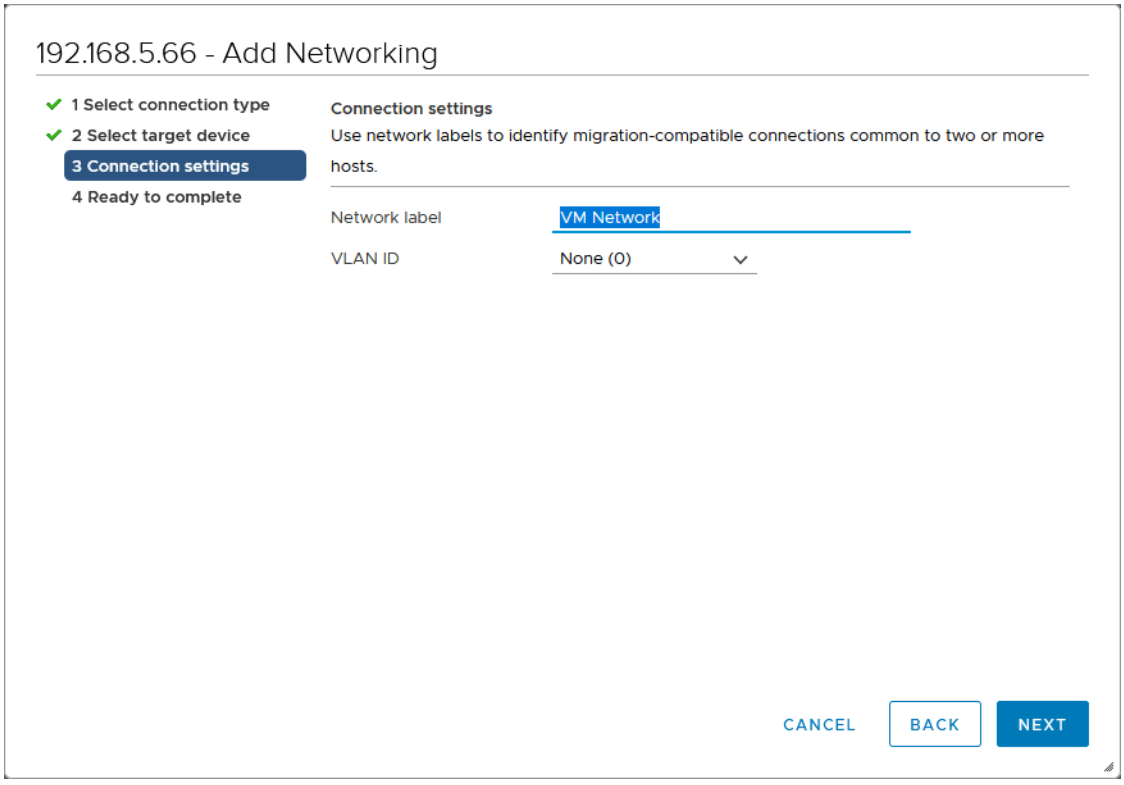

Fig. 47: Add networking (example)

8. Click on the button *FINISH*.

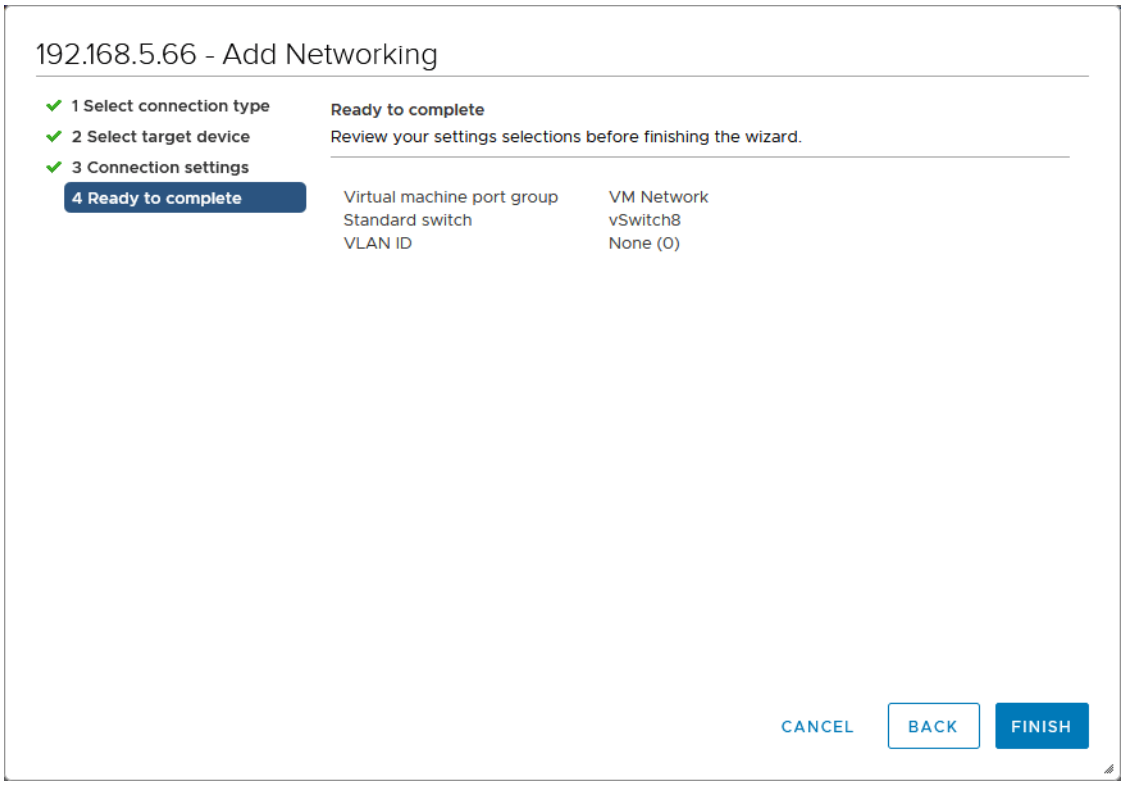

Fig. 48: Add networking (example)

New standard switch

1. Select the option *New standard switch* and click on the button *NEXT*.

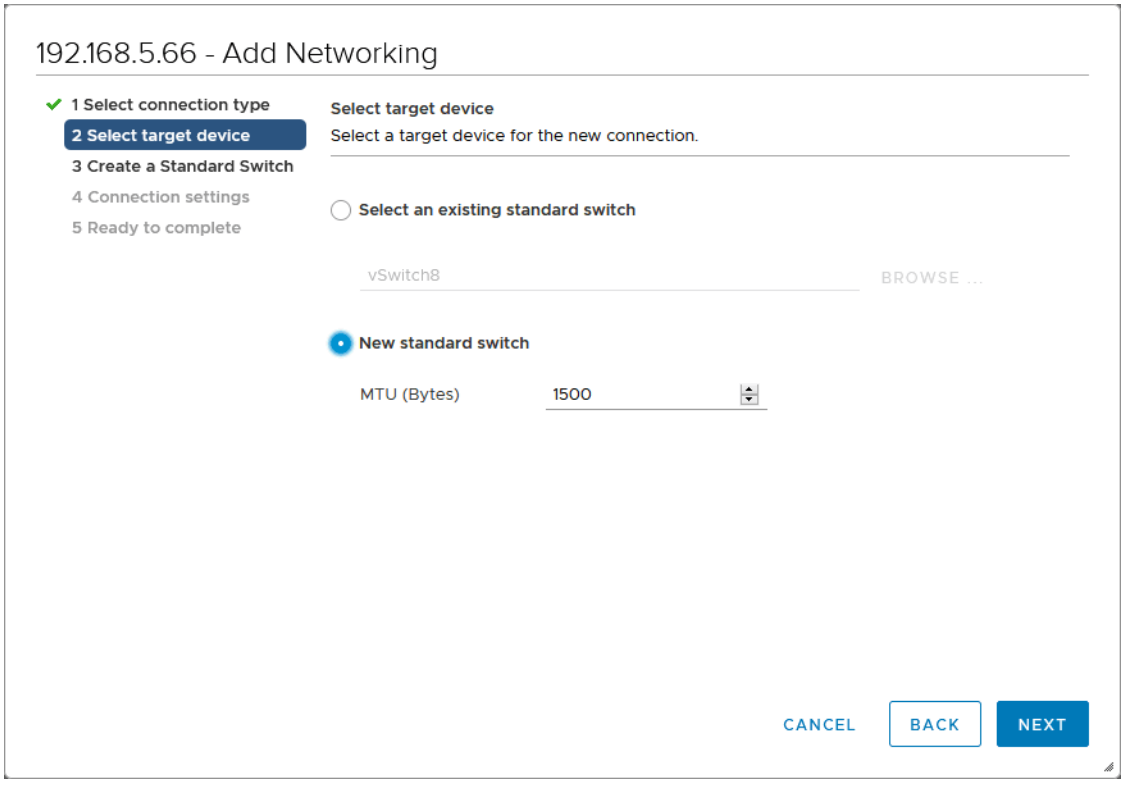

Fig. 49: Add networking (example)

2. Click on *Active adapters*.
3. Click on the icon ✚ *(Add adapter)*.

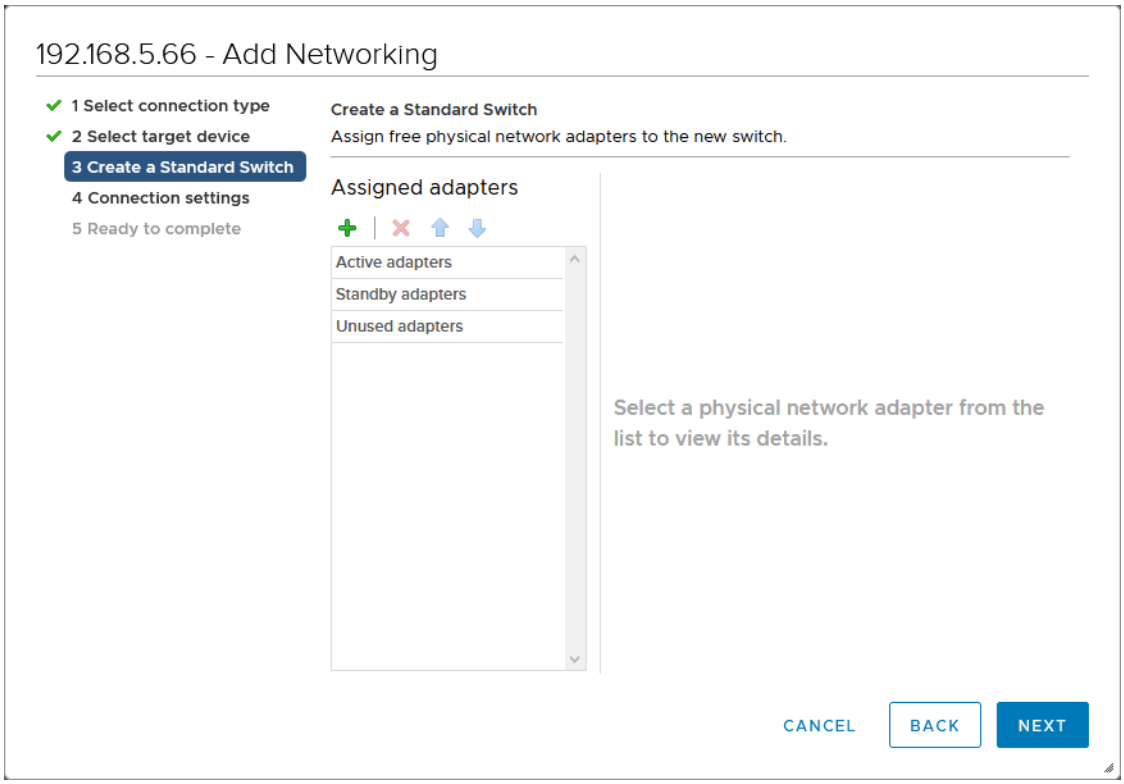

Fig. 50: Add networking (example)

4. Click on the respective network adapter, e. g. *vmnic5*.
5. Click on the button *OK*.

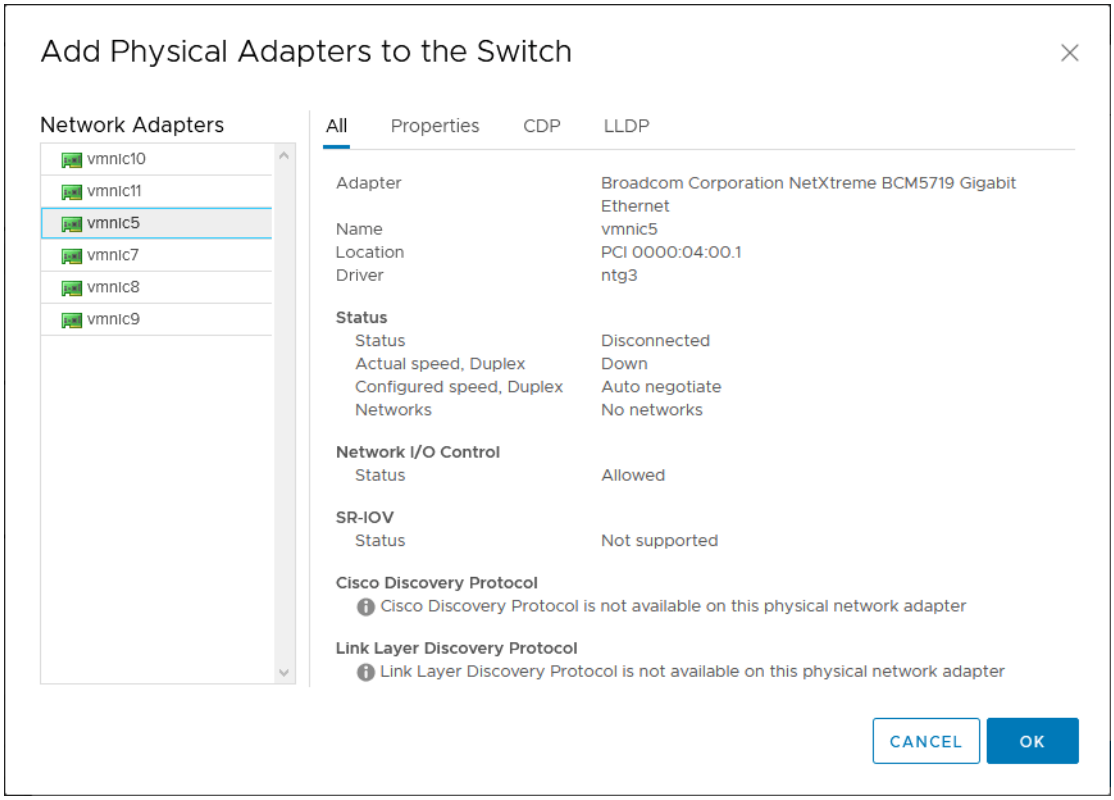

Fig. 51: Add Physical Adapters to the Switch (example)

6. Click on the button *NEXT*.

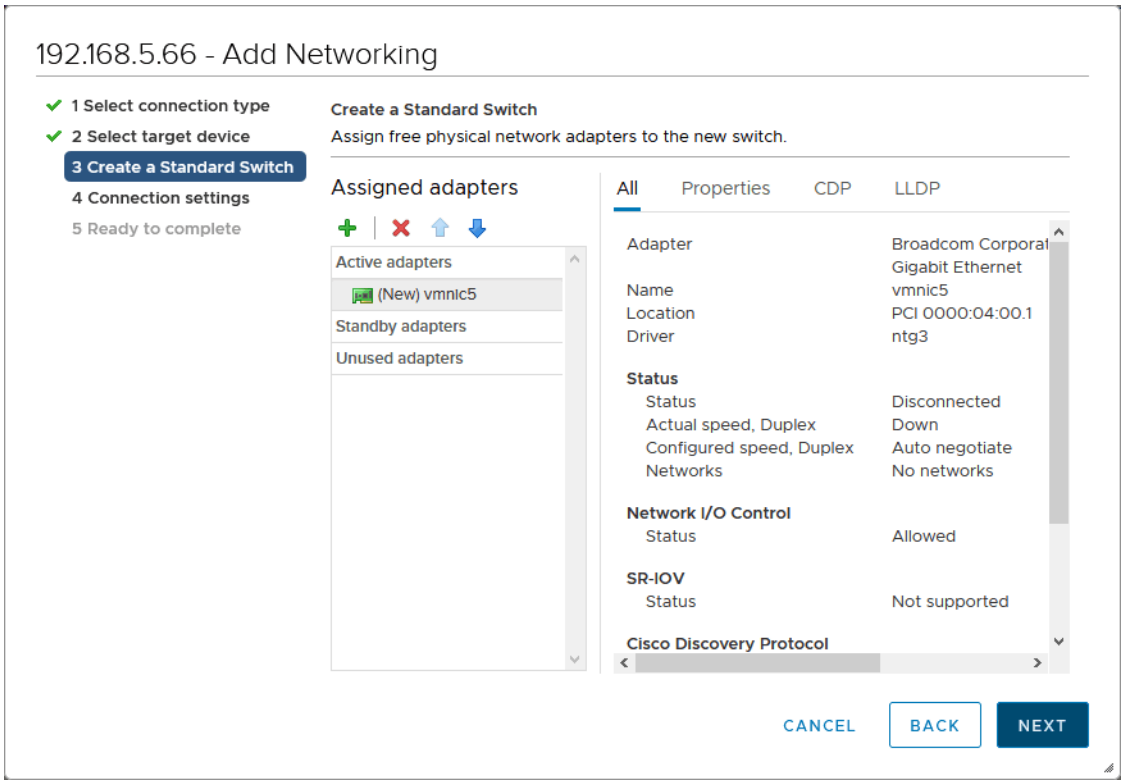

Fig. 52: Add networking (example)

7. Click on the button *OK*.

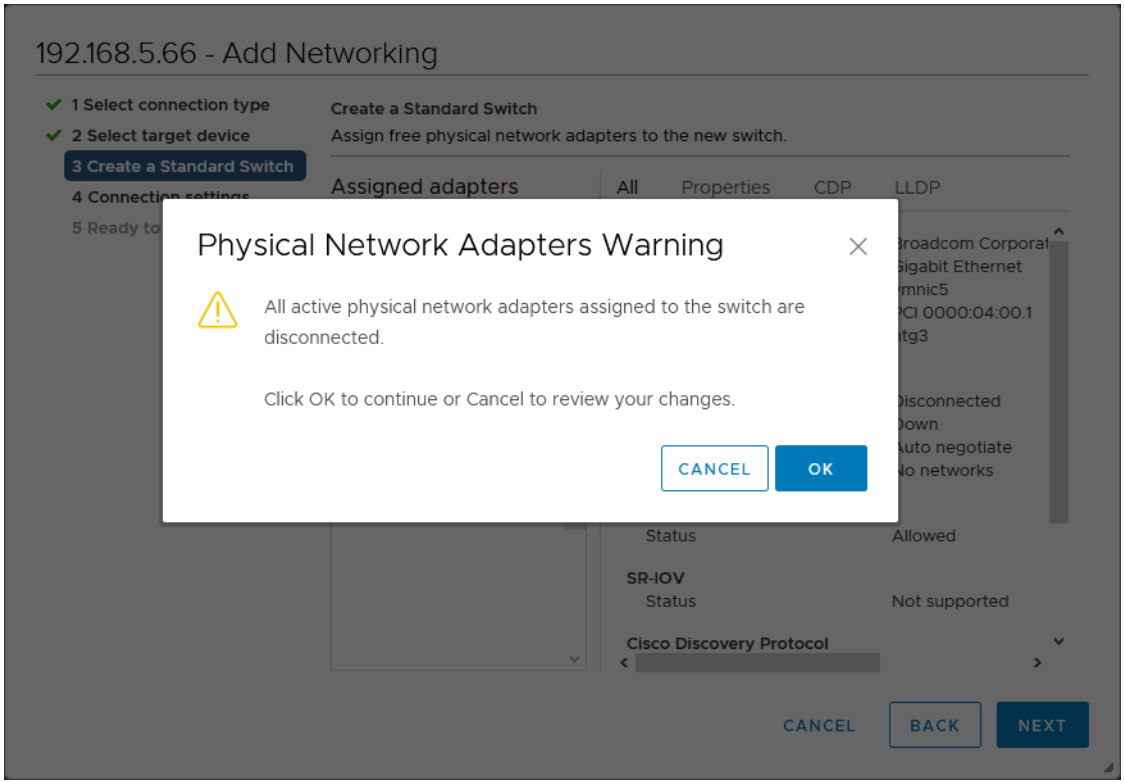

Fig. 53: Physical Network Adapters Warning

8. In the entry field *Network label*, enter a name for the network, e. g. *VM Network*.
9. Click on the button *NEXT*.

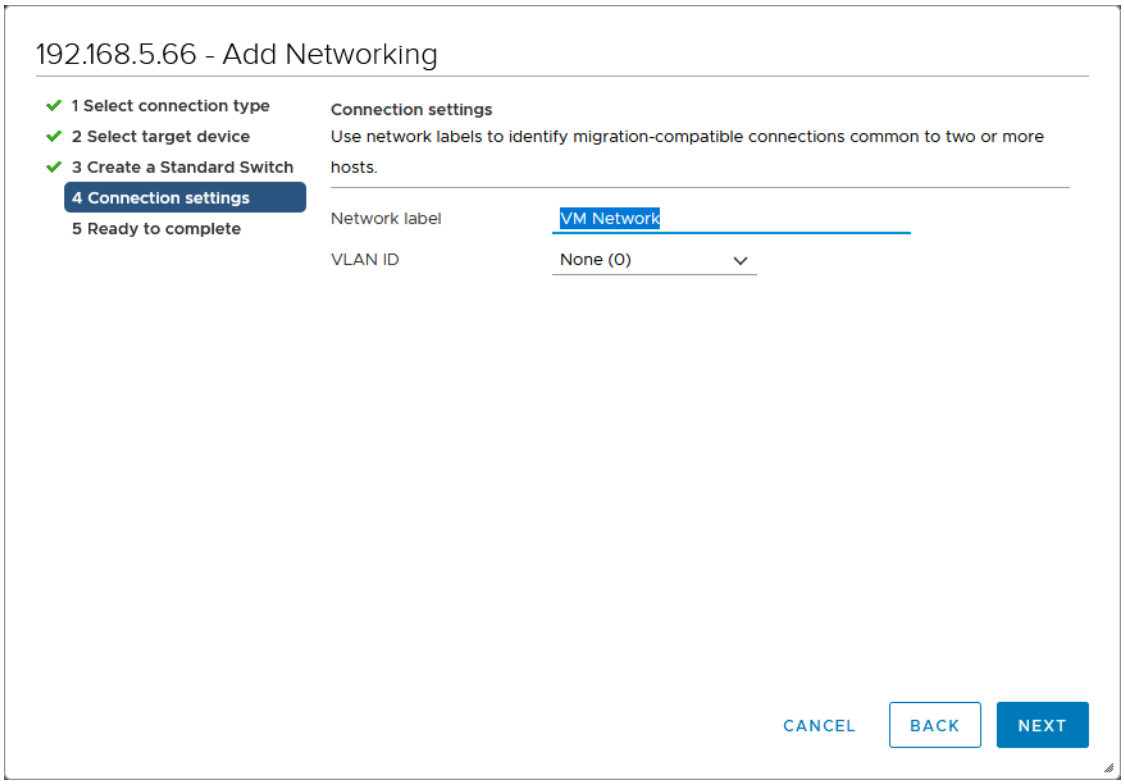

Fig. 54: Add networking (example)

10. Click on the button *FINISH*.

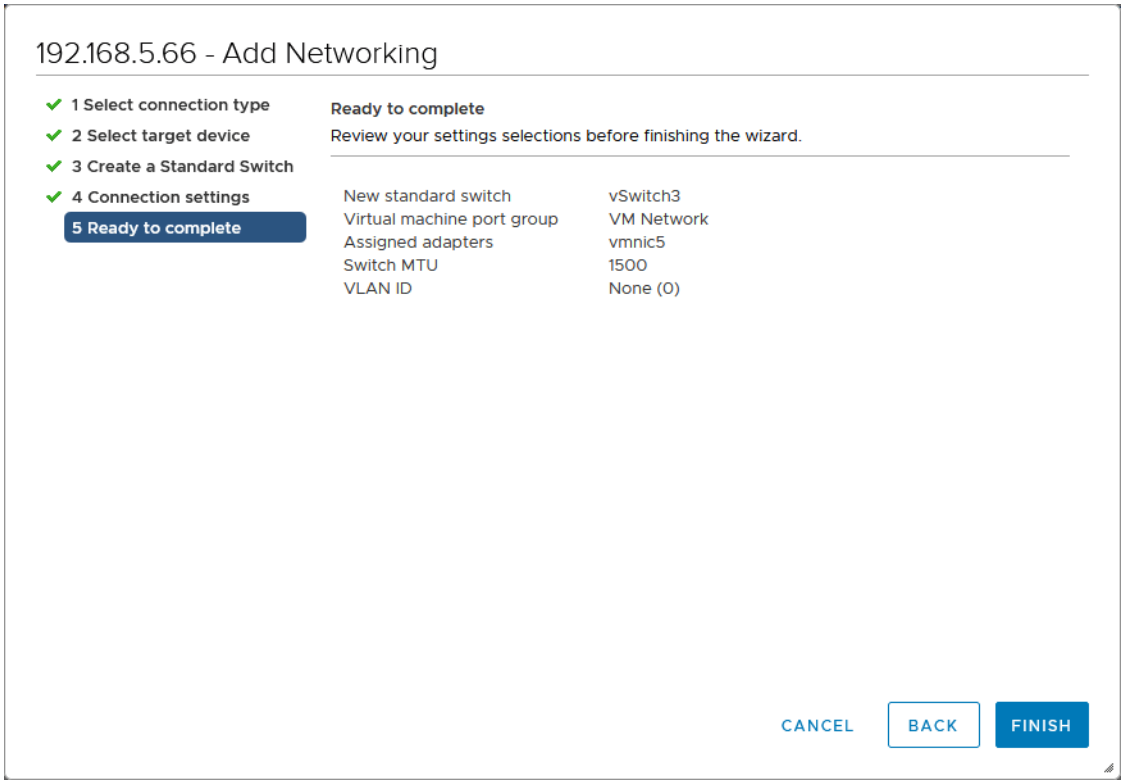

Fig. 55: Add networking (example)

Configure security settings

1. To configure security settings, click on the button *EDIT* under the virtual switch *Standard Switch: vSwitch8*.

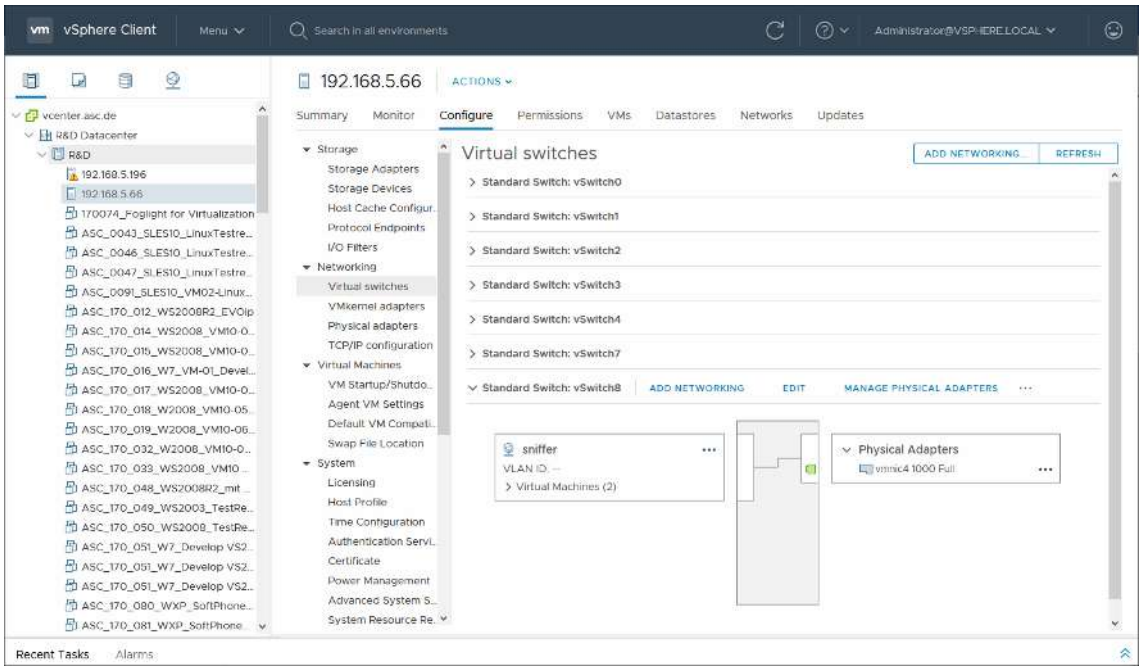

Fig. 56: Configure virtual switches (example)

2. Click on the menu item *Security*.

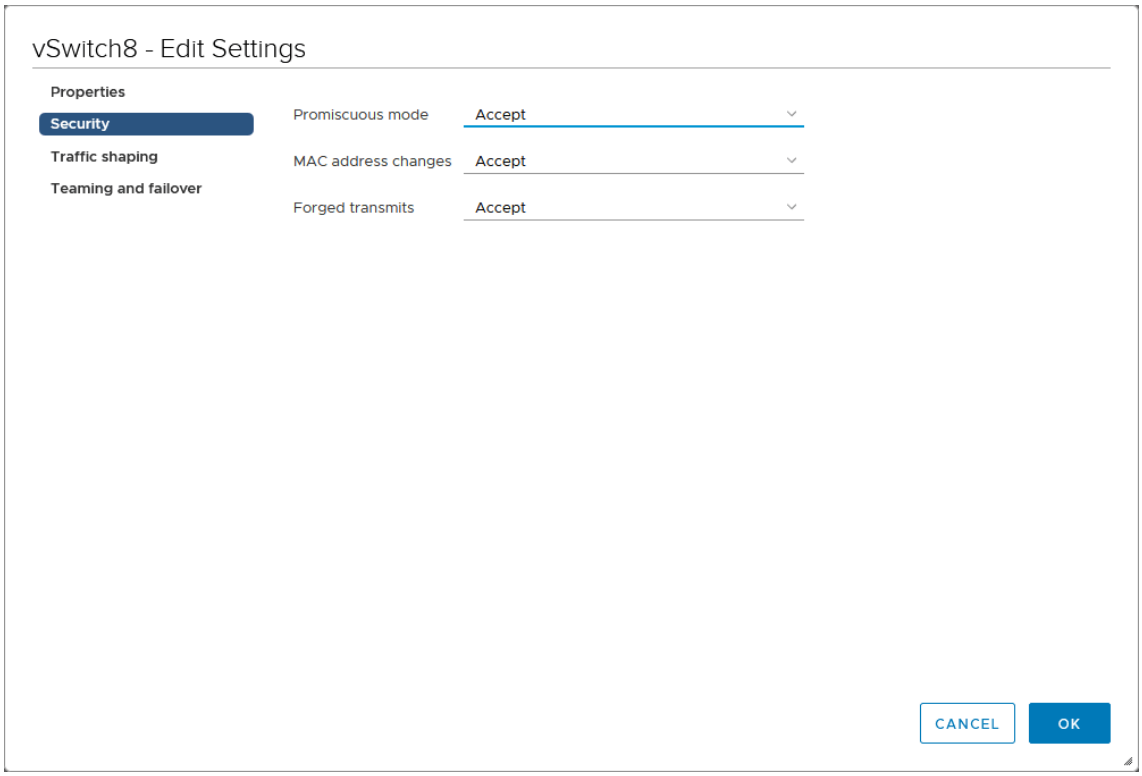

Fig. 57: Edit settings (example)

3. From the drop-down list, select the parameter *Accept* for the following options:
   - *Promiscuous mode*
   - *MAC address changes*
   - *Forged transmits*
4. Click on the button *OK*.

5 Installation and configuration of a neo VM in the Google Cloud by means of a template

The following recording architecture types may be installed and configured:

- *neo* VM with Core and DB
- *neo* VM with Core and external DB
- *neo* VM without Core and with DB
- *neo* VM without Core and without DB

For the installation and configuration, the application *Windows PowerShell ISE (x86)* and the gcloud command line tool are used.

The gcloud command line tool is part of Google Cloud SDK. You must download Google Cloud SDK and install and initialize it on your computer before you can use the gcloud command line tool.

To be able to copy templates from the ASC Google project, ASC must assign the respective rights and permissions to the service administrator in advance. Contact your local ASC support or call ASC support at +49 700 27278776 and transmit the e-mail address to be used for the service account.

Create script file

1. Open the Windows Explorer.
2. In the manual package, change to the directory *\4_Tools*.
3. Right-click on the script file *Example_CreateCore.ps1*.
   ⇨ The context menu appears.
4. Click on *Edit* in the context menu.
   ⇨ The script file *Example_CreateCore.ps1* is opened in the application *Windows PowerShell ISE (x86)*.

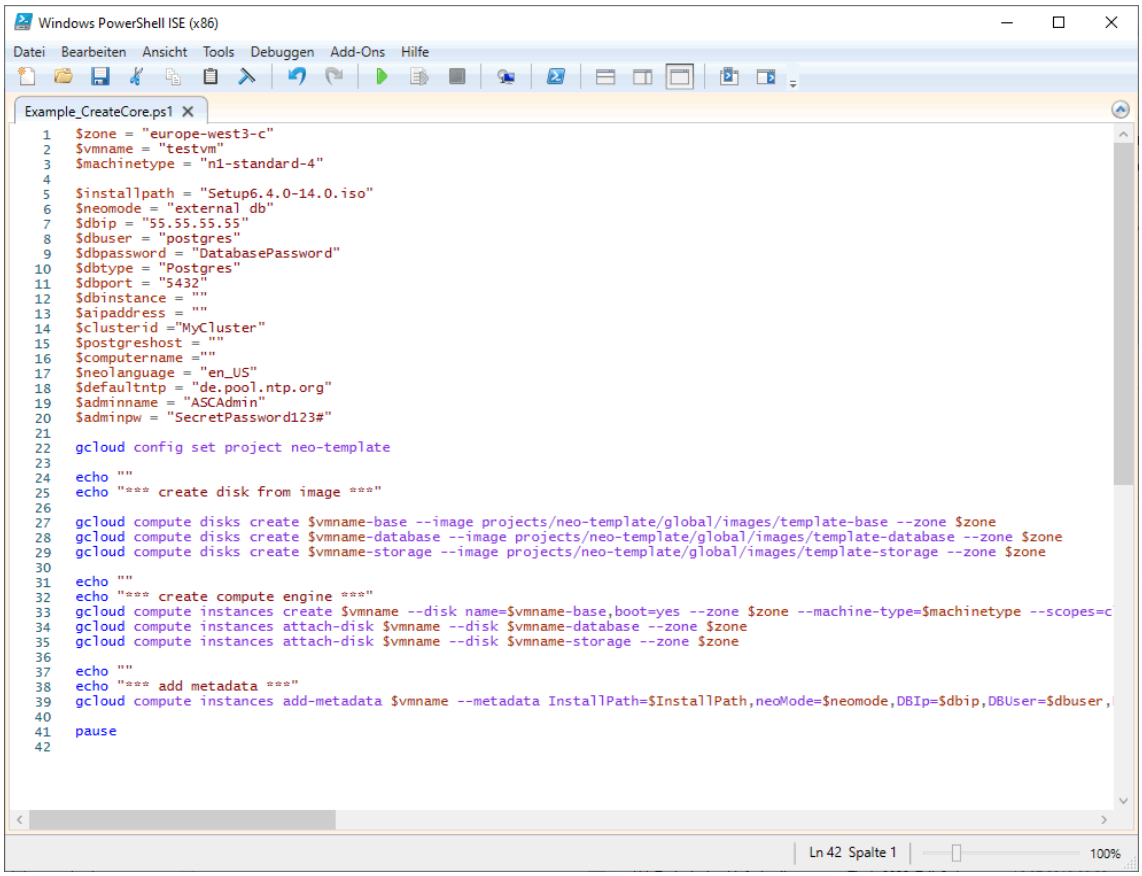

Fig. 58: Example of a script file (Example_CreateCore.ps1) to create an All-in-One *neo* system with external Postgres database

Explanation of the parameters in the script file

Rows 1-3:
Here, you define the zone in which the Google Cloud VM is supposed to be created as well as the name and the type of the VM.

Rows 5-20:
Here, you define the PowerShell variables with the necessary details of the installation. As depicted in the example, variables not relevant for the installation can be left out or defined as an empty string.
In case of the Google Cloud, the parameter *InstallPath* (see fig. row 5) must be filled with the name of the *neo* ISO image file. The respective names of the *neo* ISO image file are available at our website. Log in to ASC XCHANGE on our website https://www.asc.de/partner and open the respective directory in the area *Software Download* e. g. *neo suite* > *NEO 6.4* to view the respective *neo* ISO image file, e. g. *Setup6.4.0-13.0.iso*.

The following parameters are available:

Parameter	Description
installpath	Enter the name of the *neo* ISO image file. Example: "*Setup6.4.0-13.0.iso*"
neomode	Enter one of the following options: • *AllInOne* = *neo*-VM with Core and with DB • *external db* = *neo*-VM with Core and with external DB • *without core* = *neo*-VM without Core and with DB • *without core/db* = *neo*-VM without Core and without DB Example: "*external db*"

Parameter	Description
dbip	Enter the IP address for the external DB. This information is not required for NEOMODE *AllInOne* or for *without core*.
dbuser	Enter the external DB user. If no information is entered, the ASC default is entered. This information is not required for NEOMODE *AllInOne* or for *without core*.
dbpassword	Enter the password for the external DB. If no information is entered, the ASC default is entered. This information is not required for NEOMODE *AllInOne* or for *without core*.
dbtype	Enter one of the following options: • *Postgres* • *MSSQL* This information is not required for NEOMODE *AllInOne* or for *without core*.
dbport	Enter the value *1433* for MSSQL Standard. If a Named Instance is used, enter the differing port. Enter the value *5432* for POSTGRES. This information is not required for NEOMODE *AllInOne* or for *without core*.
dbinstance	If you use MSSQL and Named Instance, enter the name of the Named Instance. If no information is entered, the ASC default is entered. This information is not required for NEOMODE *AllInOne* or for *without core*.
aipaddress	Enter the IP address for the AIP (Core). This information is not required for NEOMODE *AllInOne* or for *external db*.
clusterid	Option: Enter the cluster ID. The server name is entered as default ID here. For All-in-One systems you can apply this ID. If you set up a multi-server system with several application servers, you must replace the default ID for all application servers with another arbitrary cluster ID which is identical for all application servers.
postgreshost	Option: Enter the IP address for the DB which requires remote access (e. g. with remote recorder). You can create several IP/Netmasks separated by semicolons. The format IP/Netmask is mandatory. Example: "*192.168.170.0/24*"
computername	Option: Enter the computer name. Observe Microsoft's conventions!
neolanguage	Enter the language to be installed for *neo*. Example: "*en_US;de_DE*"
defaultntp	Option: Enter the IP address for the NTP server of *neo*.
adminname	Enter the user name of the administrator.

Parameter	Description
adminpw	Enter the password of the administrator.
postbuildscript	Enter the PowerShell script file which is supposed to be executed after the installation.

Row 22:
The script changes to the target project. Enter the respective project of the GCP (Google Cloud Platform).

Rows 27-29:
The virtual hard disks of the VM are copied from the ASC template project.

Rows 33-35:
The virtual machine is created and the hard disks are attached.

Row 39:
Here, the metadata of the VM is filled with the installation parameters from rows 5-20.

5. Adjust the parameters in the script file according to your requirements.
6. Select the menu item *File* > *Save as*.
   ⇨ The window *Save As* appears.
7. Select a storage location and enter a file name for the script file, e. g. *C:\Install\Create-Core_neo.ps1*.
8. Click on the button *Save*.
   ⇨ The script file is saved and the window *Save As* is closed.

Execute script file

1. In the Windows Explorer, change to the storage location of the recently created script file, e. g. *C:\Install*.
2. Right-click on the recently created script file, e. g. *CreateCore_neo.ps1*.
3. Click on the menu item *Execute with PowerShell* in the context menu.
   ⇨ The VM is created. The preinstalled ASC tool *ImageMan* executes the *neo* installation and configuration with the transmitted parameters.
   ⇨ Log files of this process can be found on the VM in the path *C:\Install*.
4. During the configuration, the VM is restarted several times automatically. Do not start or stop the VM manually before the installation has been completed.

6 Configuration Hyper-V

Please be aware that *Hyper-V Live-Migration* is not supported.

Since *Hyper-V* works with its own NTP server, you have to use one of the following options to ensure an accurate time synchronization:

- The same *NTP* servers must have been configured for the recording system and for Hyper-V.
- Switch off the NTP server in the recording system.
- Remove the NTP server in the recording system.

For further information about the administration of the NTP servers of the recording system refer to the installation manual *Configuration of servers and recording architectures*.

When using passive recording solutions

To use *Hyper-V* in promiscuous mode to monitor external data traffic in virtual environments, enter the following commands with your configuration parameters in the Hyper-V console:

Examples:

```
Set-VMNetworkAdapter MyVM -PortMirroring Destination
```

```
Get-VMNetworkAdapter MyVM | ? MacAddress -eq 'xxxxxxxx' | Set-
VMNetworkAdapter MyVM -PortMirroring Destination
```

```
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName "Ethernet
Switch Port Security Settings"
```

```
# None = 0, Destination = 1, Source = 2
```

```
$portFeature.SettingData.MonitorMode = 2
```

```
Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName MySwitch -
VMSwitchExtensionFeature $portFeature
```

7 Installation and configuration Digi AnywhereUSB

For the operation of the ASC recording software in a virtual environment a permanent Internet connection to ASC or alternatively a USB dongle is required. The Digi AnywhereUSB box can be used to connect USB components such as a USB dongle.

The following chapter describes the installation and the configuration of the Digi AnywhereUSB box which is required for the operation in a virtual environment.

The Digi AnywhereUSB box can only be operated with one server at the same time.

7.1 Install drivers

1. Connect the Digi AnywhereUSB box to the power supply.
2. Connect the Digi AnywhereUSB box to your network.
3. Download the driver and, if required, the latest firmware from the homepage indicated below:
   https://www.digi.com/support/productdetail?pid=3747
4. Install the appropriate driver according to the setup instructions.
5. After the installation of the drivers, a CMD window is opened automatically. Verify that the message *System driver installed successfully!* is displayed.

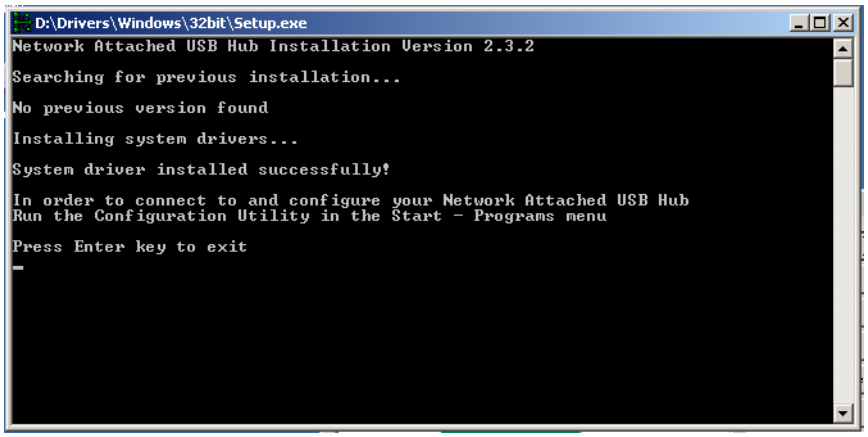

Fig. 59: Message informing about successful installation of driver

6. Press the [Enter] key to close the CMD window.

7.2 Configure Digi AnywhereUSB

7.2.1 Establish connection to the VMware server

1. Press the Windows key.
2. Click on the icon .
   ⇨ The installed apps are displayed.
3. Click on *AnywhereUSB Configuration Utility*.
   ⇨ The following window appears:

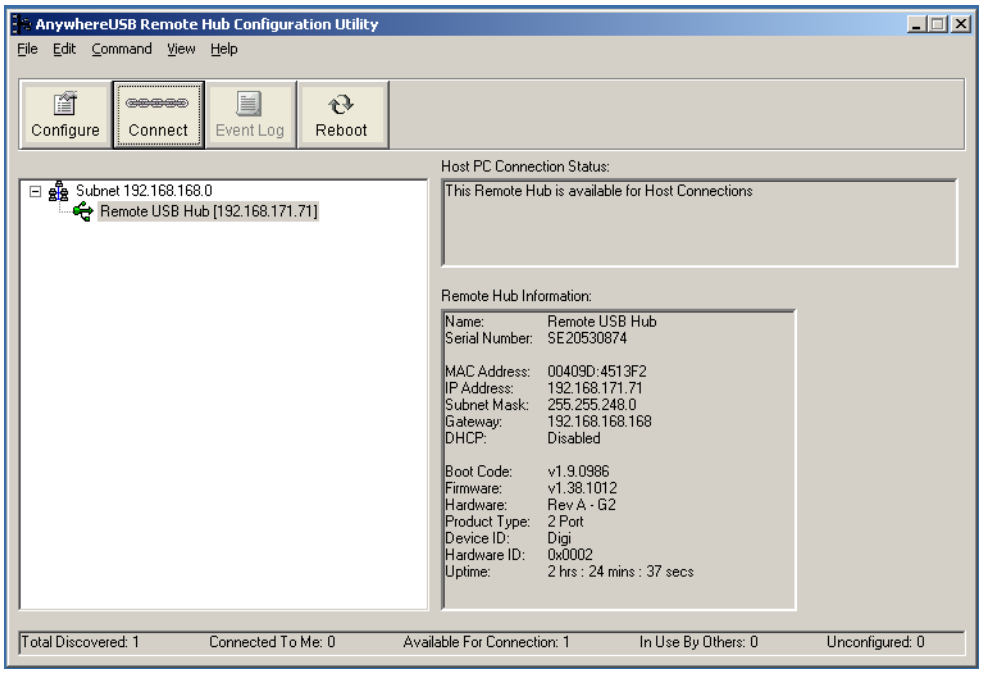

Fig. 60: Connect VMware server

4. Click on the button *Connect*.

7.2.2 Change connection to the VMware server

If the Digi AnywhereUSB box is supposed to be used on another VMware server, proceed as follows:

1. Press the Windows key.
2. Click on the icon .
   ⇨ The installed apps are displayed.
3. Click on *AnywhereUSB Configuration Utility*.
   ⇨ The following window appears:

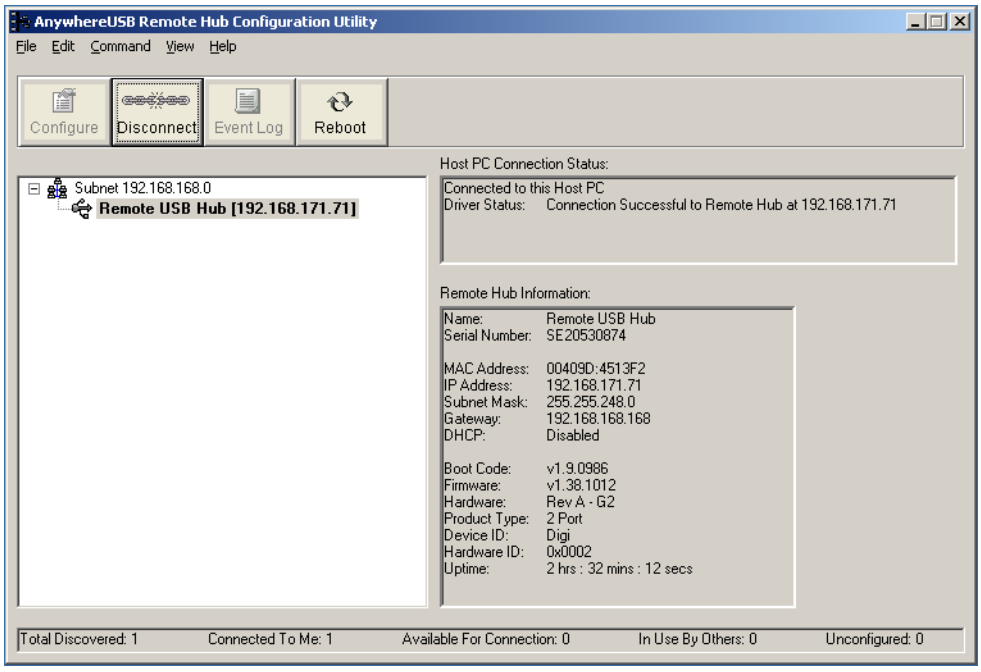

Fig. 61: Disconnect connection

4. Click on the button *Disconnect*.

5. Repeat all steps as described in chapter "Install drivers", p. 48.
6. Repeat all steps as described in chapter "Establish connection to the VMware server", p. 48.

7.2.3 Change IP address

By default, the Digi AnywhereUSB box has a DHCP network address. After the installation of the drivers, the Digi AnywhereUSB box is found automatically and the IP address of the VMware server is applied. This option has already been activated in the default setting.

To change the IP address, proceed as follows:

1. Start a browser.
2. Enter the IP address *https://192.168.175.20* in the address bar.
3. The configuration program *AnywhereUSB/2 Configuration and Management* is opened.

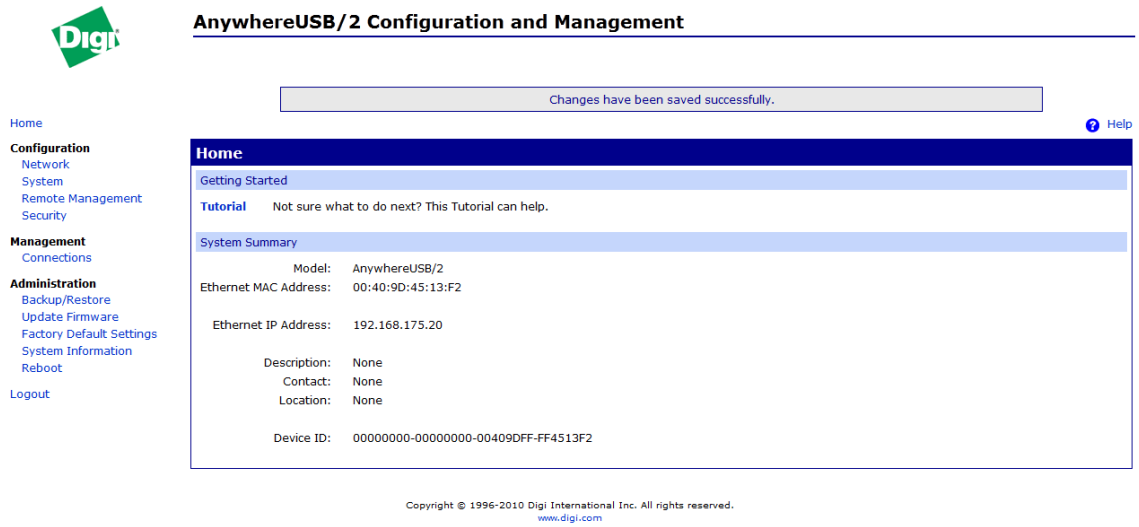

Fig. 62: Configuration program *AnywhereUSB/2 Configuration and Management*

4. Select the menu item *Configuration* > *Network* in the structure view.

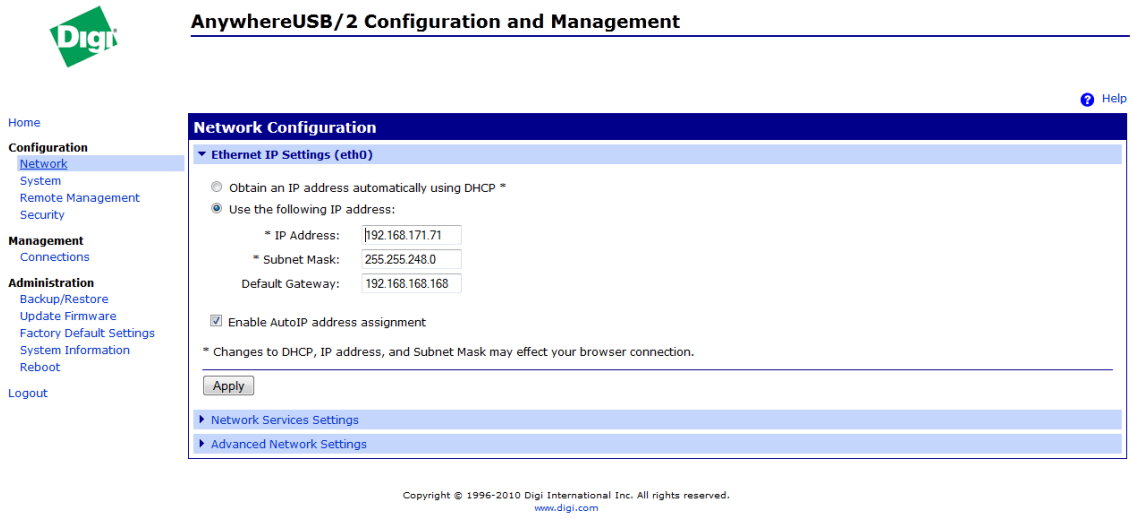

Fig. 63: Change IP address

5. In the field *Use the following IP address* > *IP Address*, enter the new IP address.
6. Click on the button *Apply*.
7. Confirm the security prompt with *Apply*.

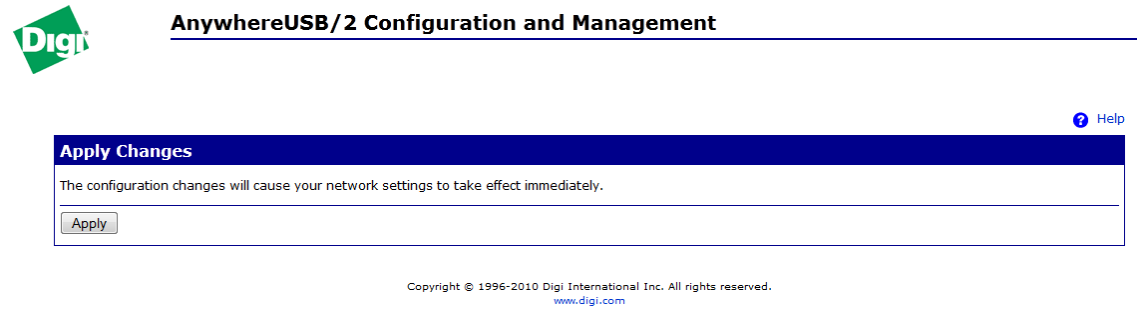

Fig. 64: Confirm change

8. The VMware server recognizes the change of the IP address automatically. The connection to the Digi AnywhereUSB box is reestablished.

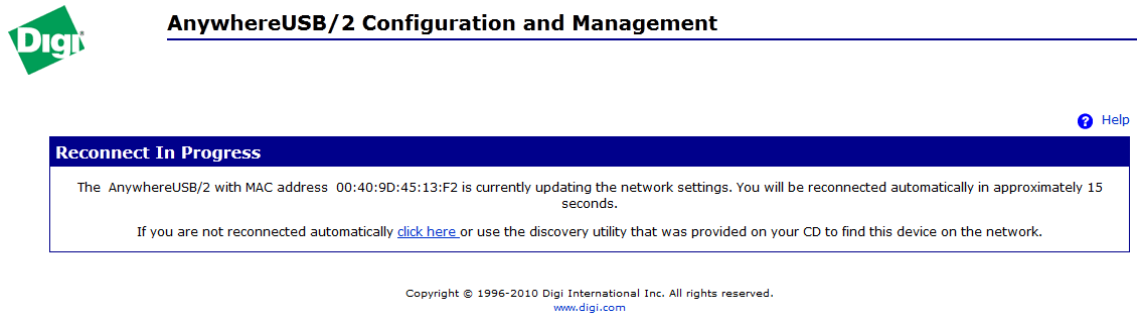

Fig. 65: Reconnect VMware server

9. In the configuration menu, the message *Changes have been saved successfully* appears.

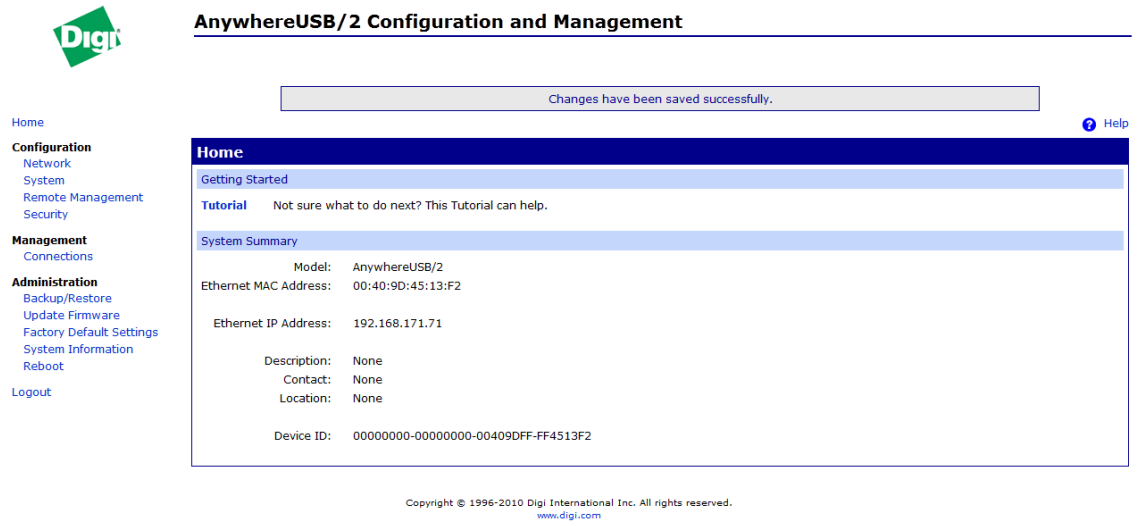

Fig. 66: Change of the IP address completed successfully

8 Configuration System Configuration

To be able to operate the recording system in a virtual environment, you have to adjust the following configurations in the Servers module of the application System Configuration:

1. Activate the VM support, see chapter "Tab Usage", p. 52.
2. Enter the connection data to the dongle, see chapter "Tab Keystore/Virtualization", p. 53.
3. To save the settings, click on the button *Save* in the detail view.

For information about starting and using the application System Configuration refer to the user manual *Usage System Configuration*.

8.1 Tab Usage

In this tab, you can configure the purpose of the selected server.

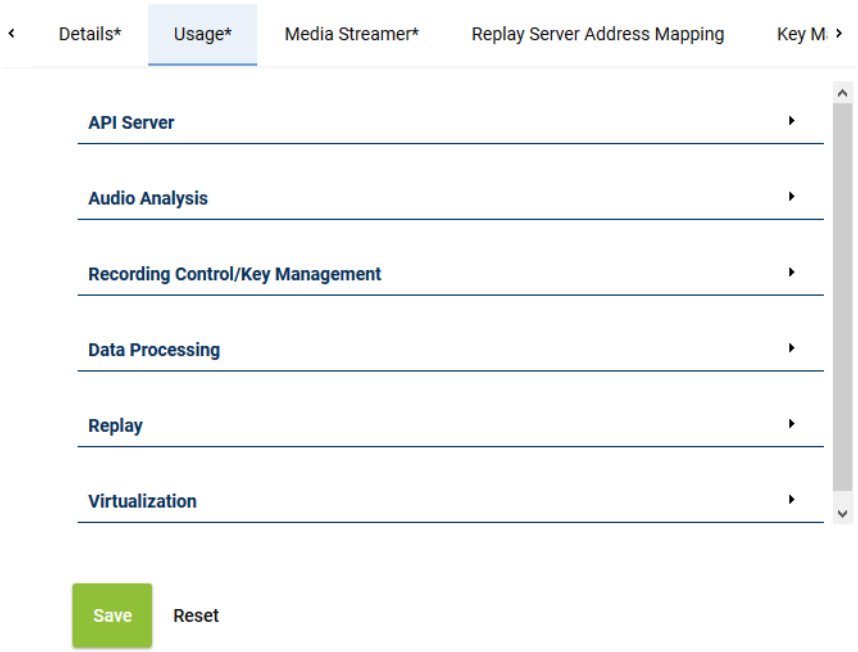

Fig. 67: Servers module - tab Usage

Group field Virtualization

1. Open the group field *Virtualization*.

Fig. 68: Group field Virtualization

2. Enter the following parameters:

VM without Trusted License	If the system runs in a virtual environment and if no *TRUSTED_VIRTUALIZATION* license has been installed, you must activate the function *VM without Trusted License*. ☑ = Function has been activated. ☐ = Function has not been activated. When activating this functionality, the Licensing module has to authenticate on one of the following instances: Dongle Manager or ASC License Management System

The system therefore requires a permanent connection either to the ASC License Management System at the ASC headquarters or to a dongle on one of the servers of the system. About the configuration of the connection data, see chapter "Tab Keystore/Virtualization", p. 53.

NOTICE! This functionality can only be activated on servers with an Enterprise Core.

NOTICE! This function can only be activated if the system has been installed in a virtual environment.

For *virtualization* without an Internet connection, a Trusted License is required.

8.2 Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data for the service *DongleMan* for the *neo* key management and for the authentication of the VM.

If your system has been installed in a virtualized environment and you are deploying a dongle, the port that the dongle has been plugged in to must have been assigned to the server that the application of the Dongle Manager has been installed on to enable access to the dongle.

For detailed information about neo key management refer to the administration manual *Encryption of recordings*.

For Keystore/Virtualization, the following constellations are possible:

- Hardware without dongle with key management

  In this case, the keystore, i. e. the Dongle Manager, must be configured.
- Hardware with dongle with key management

  In this case, the keystore, i. e. the Dongle Manager, must be configured.
- VM with dongle without key management

  In this case, the Dongle Manager must be configured.

  Only valid for inventory systems. No longer supplied.
- VM with connection to *licensing.asc.de* without key management

  The connection to *licensing.asc.de* must be configured.
- VM with *TRUSTED_VIRTUALIZATION* license with key management

  In this case, the Dongle Manager must be configured.

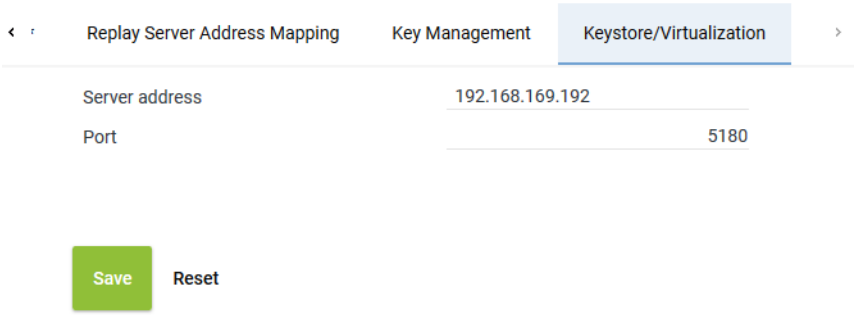

Fig. 69: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for the connection. • If you use the hardware with neo key management:

	IP address of the server where the service *DongleMan* has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM without neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: *licensing.asc.de* • If you use the VM with *TRUSTED_VIRTUALIZATION* license and neo key management: IP address of the server where the service *DongleMan* has been installed.
Port	Enter the port for the connection. *5180* = Dongle Manager *8181* = ASC License Management System

9 Quick guide

9.1 Create and configure vSwitch for administration

- Create vSwitch:

  Register vSphere Client **>** in the inventory window on host **> Configuration > Networking > Virtual Switch > Add Networking > Virtual Machine > Next > Create a virtual switch** and activate adapter **> Next >** Enter network label **> Next > Finish**.

- Configure vSwitch:

  Select vSwitch **> Properties > vSwitch > Edit > Security > Promiscuous Mode:** `Reject` **> MAC Address Changes:** `Reject` **> Forged Transmits:** `Reject` **> OK >** Click on previously created network **> Edit > Security > Promiscuous Mode:** `Reject` **> MAC Address Changes:** `Reject` **> Forged Transmits:** `Reject` **> OK**.

9.2 Create and configure vSwitch for passive recording

- Create vSwitch:

  Register vSphere Client **>** in the inventory window on host **> Configuration > Networking > Virtual Switch > Add Networking > Virtual Machine > Next > Create a virtual switch** and activate adapter **> Next >** Enter network label **> Next > Finish**.

- Configure vSwitch:

  Select vSwitch **> Properties > vSwitch > Edit > Security > Promiscuous Mode:** `Accept` **> MAC Address Changes:** `Accept` **> Forged Transmits:** `Accept` **> OK >** Click on previously created network **> Edit > Security > Promiscuous Mode:** `Accept` **> MAC Address Changes:** `Accept` **> Forged Transmits:** `Accept` **> OK**.

9.3 Install and configure Digi AnywhereUSB

- Install drivers:

  Download drivers from homepage and follow setup instructions.

- Establish connection to the VMware server:

  Windows key > icon **> AnywhereUSB Configuration Utility > Connect**.

- Change connection to the VMware server:

  Windows key > icon **> AnywhereUSB Configuration Utility > Disconnect >** follow setup instructions **> Install Drivers > Windows key >** icon **> AnywhereUSB Configuration Utility > Connect**.

9.4 Configure virtualization in System Configuration

- Activate VM without Trusted License:

  Servers module > Usage > Virtualization > Activate VM without Trusted License > Save

- Enter connection data for authentication:

  Servers module > Keystore/Virtualization > Server address: enter `licensing.asc.de` or IP address of the server with the dongle **> Port:** enter port (default: `5180`) **> Save**

List of figures

List of tables

Glossary

AIP

Asynchronous Integration Platform

DB

Database

DHCP

A Dynamic Host Configuration Protocol allows integrating computers into an existing network without configuring the network interface manually. Necessary information such as IP address, net mask, gateway, name server (DNS) and additionally required settings are distributed dynamically. (Source: Wikipedia 5th April 2017)

NTP

Network Time Protocol NTP is a standard for the synchronization of clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP. It has been developed with the objective to guarantee reliable time verification across networks with variable packet runtime. (Source: Wikipedia 12th June 2018)

USB

Universal Serial Bus

VM

Virtual machine