Configuration Microsoft Windows Server 2016

Installation manual

for system providers

11/5/2021

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 installation and configuration of Microsoft Windows Server 2016 for the EVOIP*neo* software.

3 System requirements

The system requirements are described in the installation manual *Installation requirements*.

Update operating system

Updates of the operating system are supported with the exception of complete service packs. The installation of new service packs has to be approved explicitly by ASC.

Deactivate the "Automatic update function" of the operating system and install necessary updates manually if required.

The service Windows Firewall has to be started **before** the installation of the *neo* software to guarantee the correct operation of the recording system (see chapter "Configure services", p. 14). ASC only supports the Windows Firewall.

The time zone must be set **before** the installation of the *neo* software.

File Access Auditing/File Access Log must not have been activated.

Exclusively install software approved by ASC!

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

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

4 Installation requirements

4.1 Virus protection

The installation of an antivirus software on a *neo* recording system lies within the responsibility of the customer.

The installation of an antivirus software does affect neither warranty nor maintenance contracts; however ASC does not assume any liability for consequential damages that may occur due to the use of the antivirus software.

Running an antivirus software may slow down the execution of the *neo* software during periods of high system utilization. Running an antivirus software has an impact on the execution of functions, too, which involve increased data exchange at the I/O interfaces (e. g. creating diagnostic data, statistics or updating configuration data) and may thus cause functional impairment.

For this reason, ASC recommends defining time intervals for scanning the entire system for viruses when system utilization and data transfer rates are low.

Antivirus programs tested by ASC and supported:

- Windows Defender (virus protection integrated into Windows operating systems)

Required settings of an antivirus software:

- On-access scanning must have been activated
- The following directories are mandatory to be excluded from the virus scan:
  - All directories on the database partition (ASCDB, replication, …)
  - Directory *ASCDATA*
  - Directory *ASC Product Suite*
- The following file is mandatory to be excluded from the virus scan:
  - File *C:\Program Files\PostgreSQL\9.5\bin\postgres.exe* or *C:\Program Files\PostgreSQL\12\bin\postgres.exe* (the path depends on the deployed PostgreSQL version.)

When installing and/or updating the *neo* software, on-access scanning must have been disabled.

Troubleshooting

If the antivirus software should cause errors in the *neo* software, proceed as follows:

1. Uninstall or deactivate the antivirus software to restore the flawless operation of the *neo* software.
2. Contact your local ASC support or +49 700 27278776 to coordinate the further course of action.

5 Installation Microsoft Windows Server 2016

Make sure that 3 partitions have been created and configured as follows:

For the partitions, the following variants are supported:

- 1 hard disk with 3 partitions
- 3 hard disks with 1 partition each

1. System partition

   The system partition should have a minimum of 60 GB.

   – 40 GB operating system

   – 20 GB *neo* software

2. Database partition

   NOTICE! The database partition is required if you install the PostgreSQL database on this server.

   – The size of the database depends on the number of recordings and on the retention period of recordings.

Information about how to calculate the size of the database partition can be found on the Manual Package in the file *Postgres_Callpool_Sizing* in folder *1_Sizing calculator*.

3. Data partition

   NOTICE! The data partition is required if you save the pool of data on this server.

   – The size of the data partition depends on the recording requirements.

   A minimum of 150 GB is mandatory.

Information about how to calculate the size of the data partition can be found on the Manual Package in the file *Postgres_Callpool_Sizing* in folder *1_Sizing calculator*.

Install the operating system Microsoft Windows Server 2016.

6 Configuration Microsoft Windows Server 2016

The following images refer to the display mode *View by Category* preset by default.

Configure the EVOIP*neo* software as follows to guarantee smooth operation:

- chapter "Configure Internet Explorer", p. 9
- chapter "Deactivate Internet Explorer Enhanced Security Configuration (IE ESC)", p. 9
- chapter "Network cards", p. 10
- chapter "Configure services", p. 14

6.1 Configure Internet Explorer

Follow the installation manual *Configuration Browser* to install the Internet Explorer.

6.2 Deactivate Internet Explorer Enhanced Security Configuration (IE ESC)

1. Open the *Server Manager* in the taskbar.
2. Select the menu item *Local Server* in the structure view.
3. Under *Internet Explorer Enhanced Security Configuration* select *Off*.

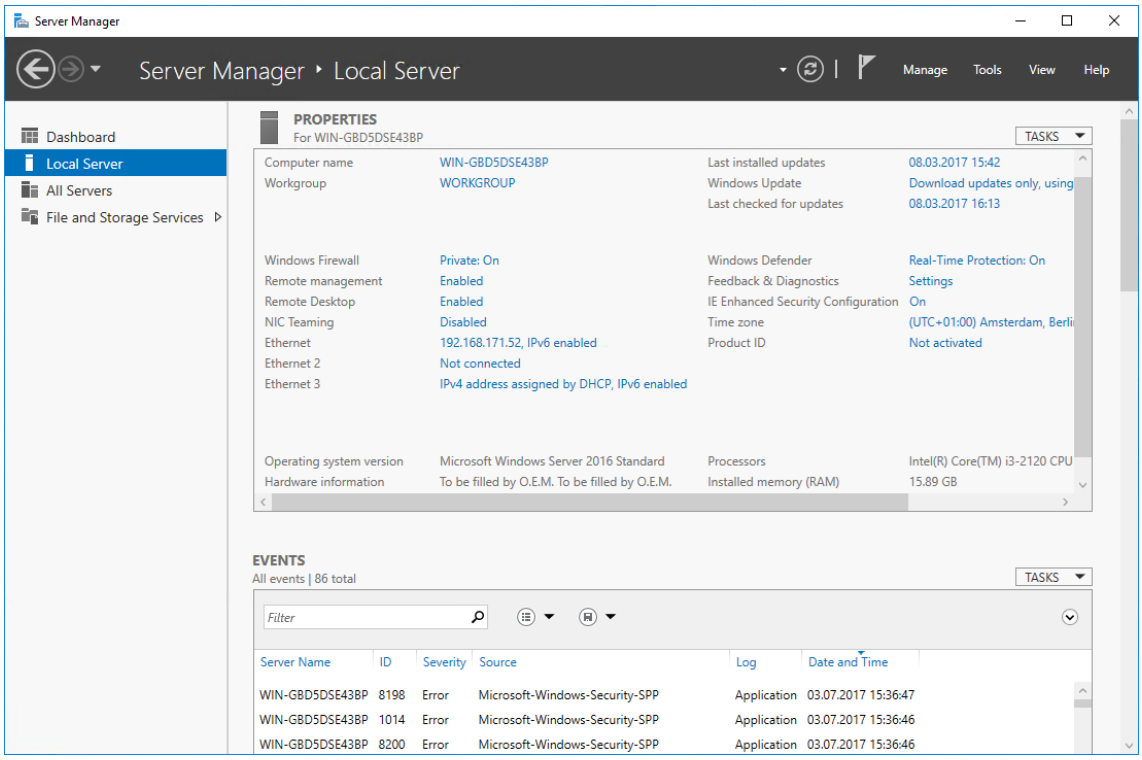

Fig. 1: Server Manager

4. Under *Administrators* and *Users*, activate the option *Off*.

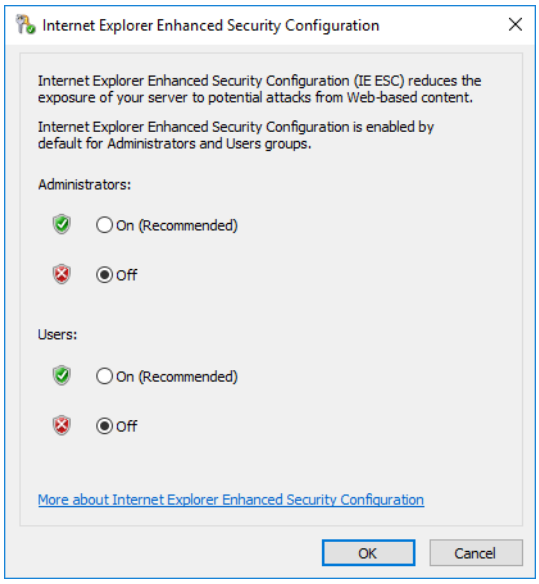

Fig. 2: IE ESC

5. Click on the button *OK* to save the settings and to close the window.

6.3 Network cards

Change IP address

The IP address should have been configured before the installation of the *neo* software.

Changing the IP address once the recorder application has been installed affects the certificates. For further information refer to the installation manual *Installation of the recording software of ASC*.

If you use a sniffer card, you have to enter an unambiguous IP address and a protocol version for this card, too.

An overview of the supported VoIP network cards can be found in the installation manual *Installation requirements*.

Check the network speed.

Autonegotiation has been set as default for network cards. As a consequence, the network cards agree on the same speed between switch and recorder.

ASC recommends a transmission speed of 1000 Mbit/s Full Duplex.

6.3.1 Configure network cards

1. Press the Windows key.
2. Open the window *Network and Sharing Center* (network connection) via *Control Panel* > *Network and Internet* > *Network and Sharing Center*.
3. Click on *Change adapter settings* on the left side.

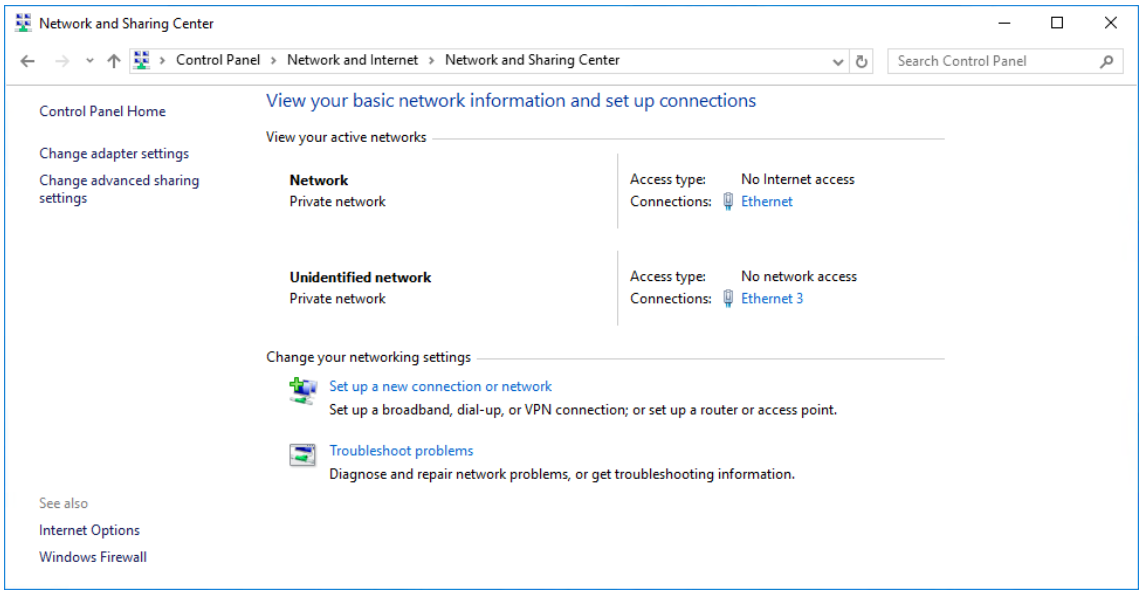

Fig. 3: Network and Sharing Center

4. Click on the inserted card.
5. Open the context menu with a right-click.
6. Select the menu item *Properties*.

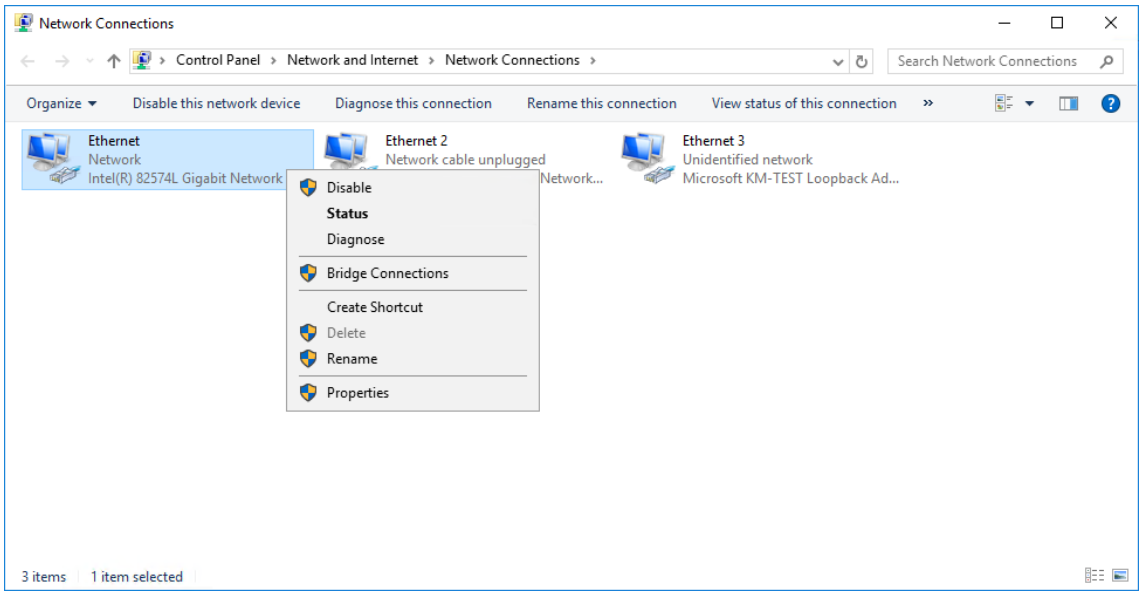

Fig. 4: Network Connections

7. Make sure that the option *File and Printer Sharing for Microsoft Networks* has been activated.
8. Click on *Internet Protocol, Version 4 (TCP/IPv4)*.

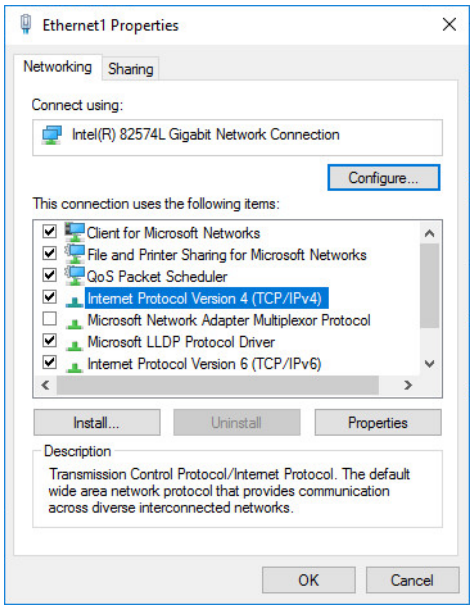

Fig. 5: Network connection properties

9. Click on the button *Properties*.
10. You have to assign a static IP address for the *neo* software. Select the option *Use the following IP address*.

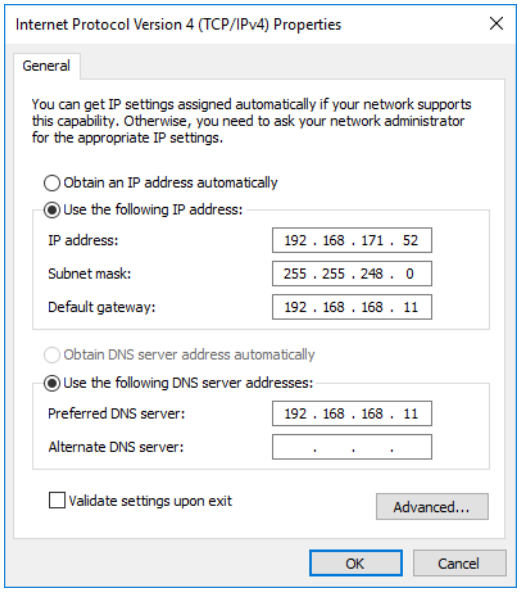

Fig. 6: Internet Protocol Version 4 (TCP/IPv4) Properties (example)

11. Enter the IP address, the subnet mask, and the default gateway.
12. Click on the button *OK* to save the settings and to close the window.
13. Click on the button *Configure*.

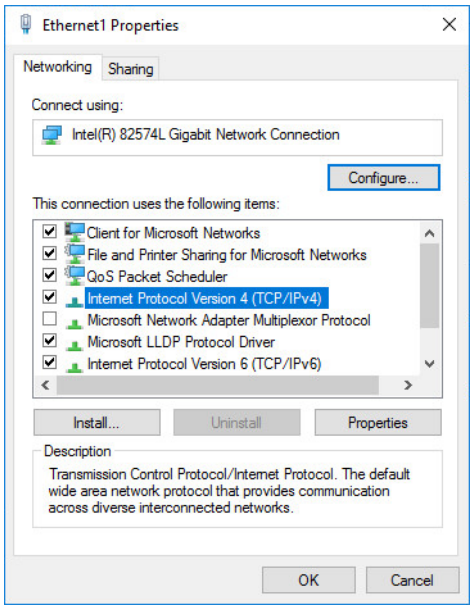

Fig. 7: Network connection properties

14. Click on the tab *Power Management*.

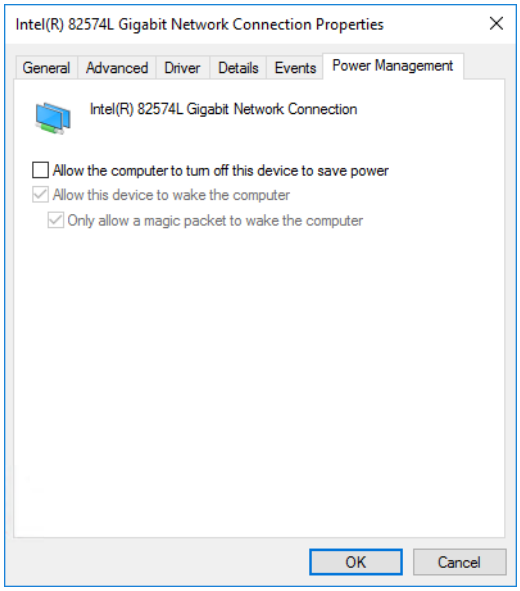

Fig. 8: Network connection energy options

15. Deactivate the check box *Allow the computer to turn off this device to save power*.
16. If you do not want to configure a sniffer card for the passive recording, click on the button *OK*. The settings are saved and the window is closed.
    If you would like to configure a sniffer card for the passive recording, proceed as follows:
17. Click on the tab *Advanced*.

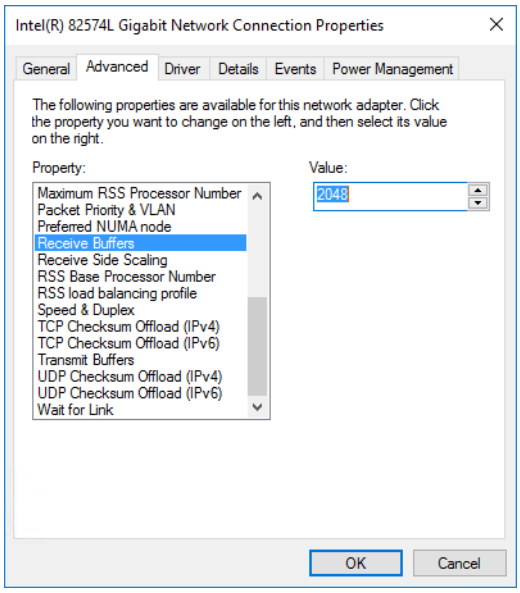

Fig. 9: Network connection advanced properties (example)

Depending on the network card, the following setting dialog may differ.

18. Select the option *Receive Buffers* or *Receive Descriptors* in the list.
19. Enter the maximum value in the field *Value*. Click on one of the arrows to increase or decrease the value.

Depending on the inserted card the maximum value lies between 1024 and 2048.

20. Click on the button *OK* to save the settings and to close the window.

6.4 Configure services

The recording system uses a native SNMP service for SNMPget requests. The SNMP service of the system is **not** used.

Use a different network port for the *neo* SNMP agent than the default SNMP port of the operating system or deactivate the SNMP service of the operating system if you do not need it for other applications.

1. Open the *Server Manager* in the taskbar.
2. Click on the menu item *Tools* > *Services*.

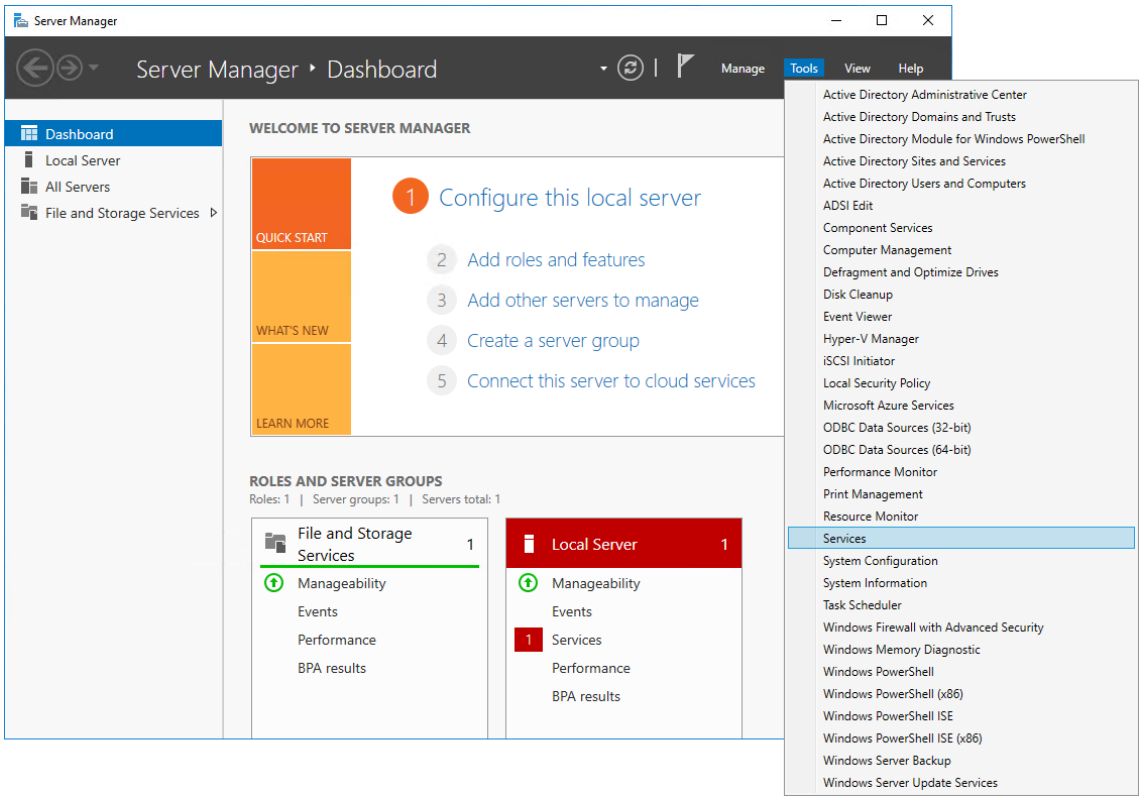

Fig. 10: Select services

During the *neo* setup the necessary port releases will be entered automatically if the firewall has been activated. For information about the communication matrix (port configuration) see installation manual *Installation requirements*.

Windows firewall

To start the service *Windows Firewall*, proceed as follows:

1. Right-click on the entry *Windows Firewall*.
   ⇨ A context menu appears.
2. Click on *Properties* in the context menu.

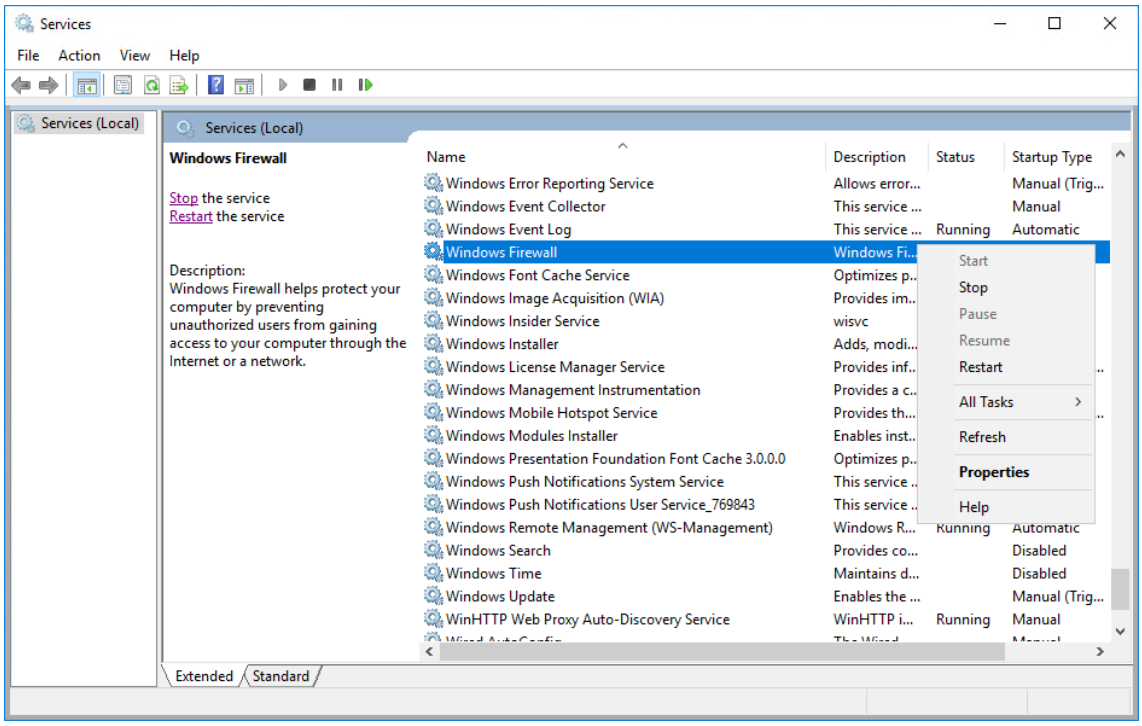

Fig. 11: Open window “Windows Firewall Properties”

3. Click on the tab *General*.
4. Click on the button *Start*.

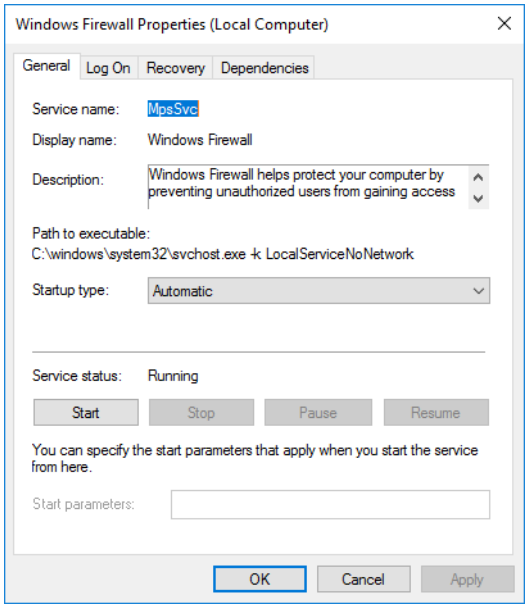

Fig. 12: Windows Firewall Properties

5. In the drop-down list *Startup type*, select the option *Automatic* if the service *Windows Firewall* is supposed to be started automatically upon starting Windows.
6. Click on the button *OK* to save the settings and to close the window.

Windows Audio

To allow a local replay on the server, the Windows Audio Service has to be enabled. Proceed as follows:

1. Right-click on the entry *Windows Audio*.
   ⇨ A context menu appears.

2. Click on *Properties* in the context menu.

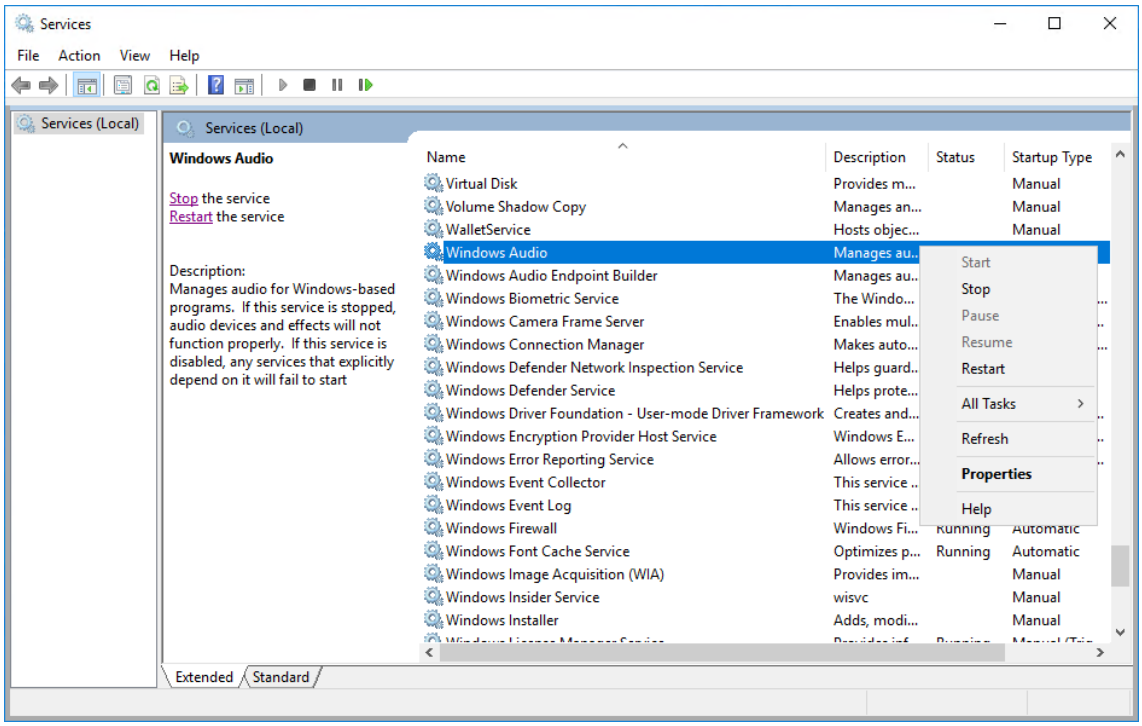

Fig. 13: Open the window "Windows Audio Properties"

3. Click on the tab *General*.
4. In the drop-down list *Startup type*, select the option *Automatic*.

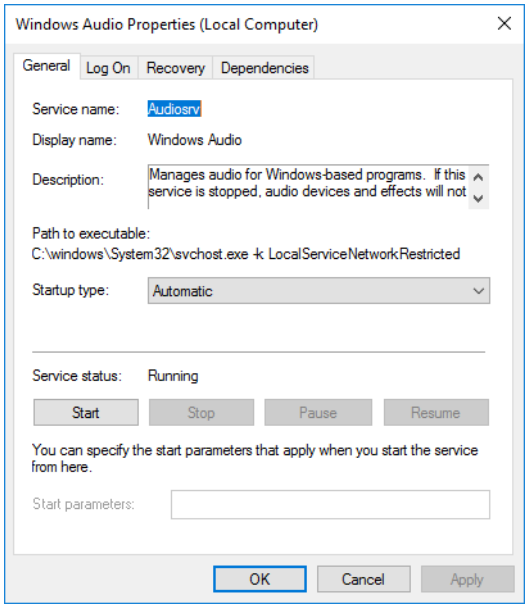

Fig. 14: Windows Audio Properties

5. Click on the button *OK* to save the settings and to close the window.

Windows Time

Since ASC uses a time emitter system based on NTP, the Windows time emitter service has to be deactivated. Proceed as follows:

1. Right-click on the entry *Windows Time*.
   ⇨ A context menu appears.
2. Click on *Properties* in the context menu.

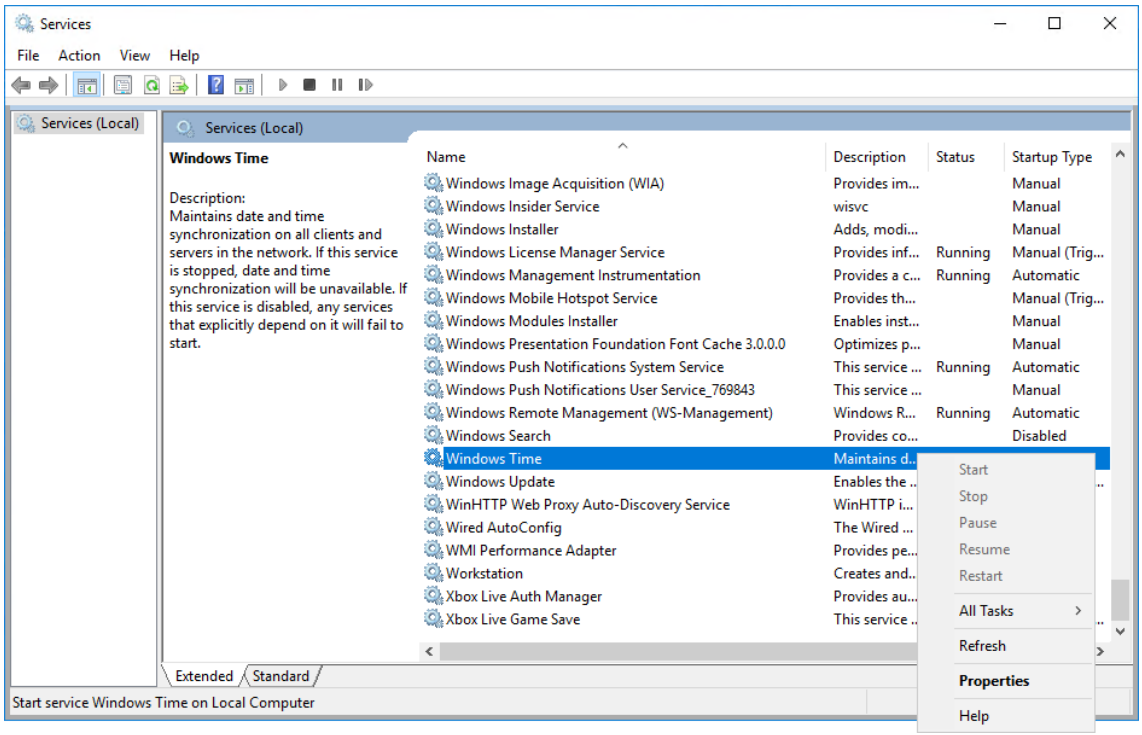

Fig. 15: Open window “Windows Time Properties”

3. Click on the tab *General*.
4. In the window *Windows Time Properties* under *Startup type*, select the option *Disabled*.
5. Check whether the *Service status* has been set to the mode *Stopped*. If this is not the case, stop the service by clicking on the button *Stop*.

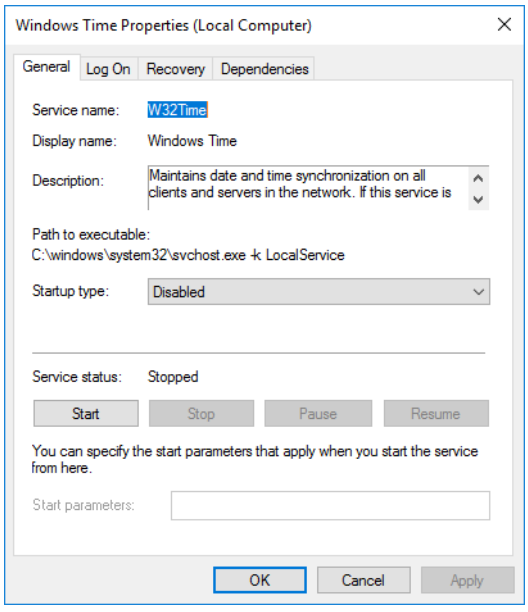

Fig. 16: Windows Time Properties

6. Click on the button *OK* to save the settings and to close the window.

6.5 Install .NET framework

1. Open the *Server Manager* in the taskbar.
   ⇨ The following window appears:

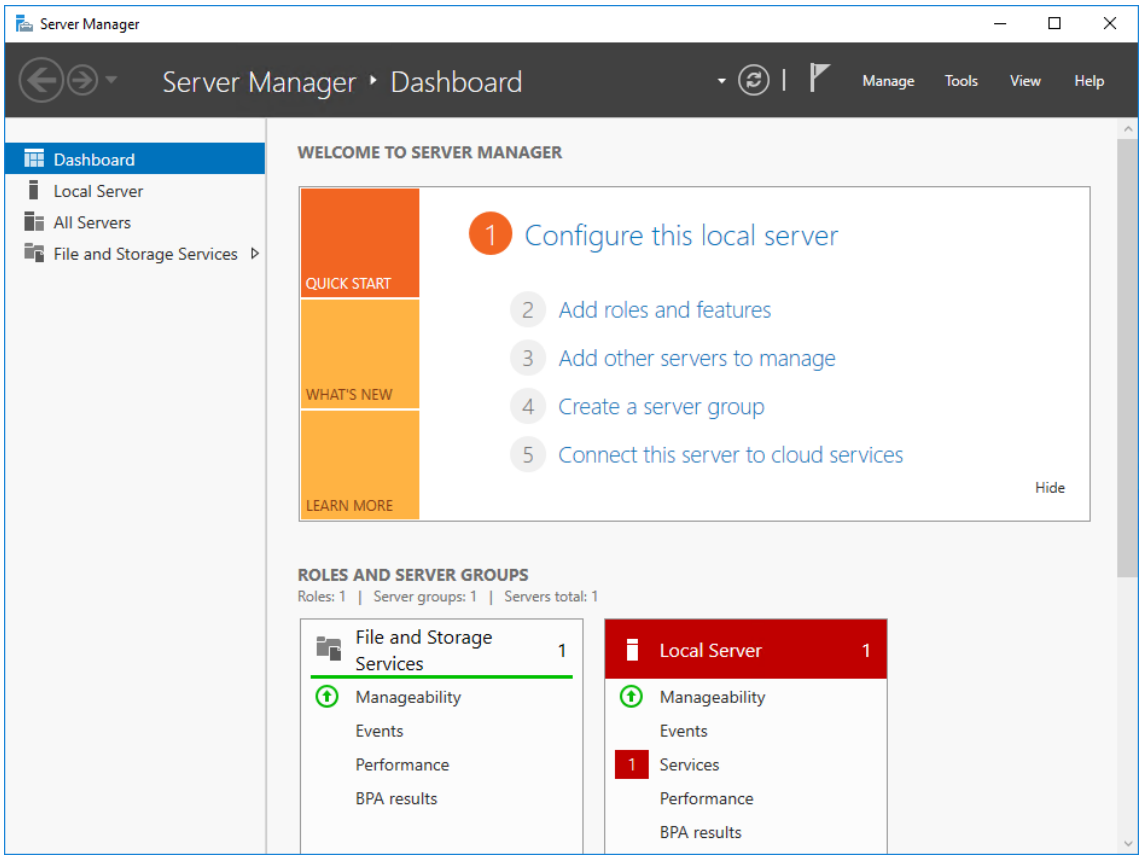

Fig. 17: Server Manager

2. Click on *Add roles and features*.
   ⇨ The following window appears:

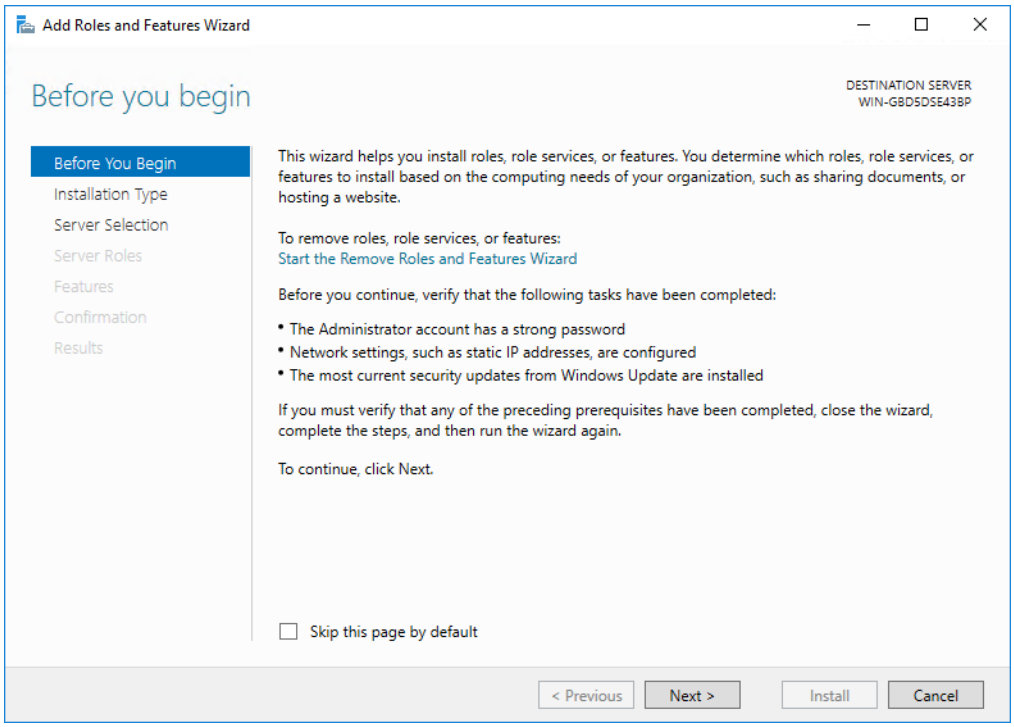

Fig. 18: Add Roles and Features Wizard

3. In the menu item *Installation Type*, click on the button *Next*.
4. In the menu item *Server Selection*, click on the button *Next*.
5. In the menu item *Server Roles*, click on the button *Next*.

6. In the menu item *Features*, click on the button *Next*.
7. Activate the check box *.NET Framework 3.5 Features*.
8. Click on the button *Next*.
   ⇨ The following window appears:

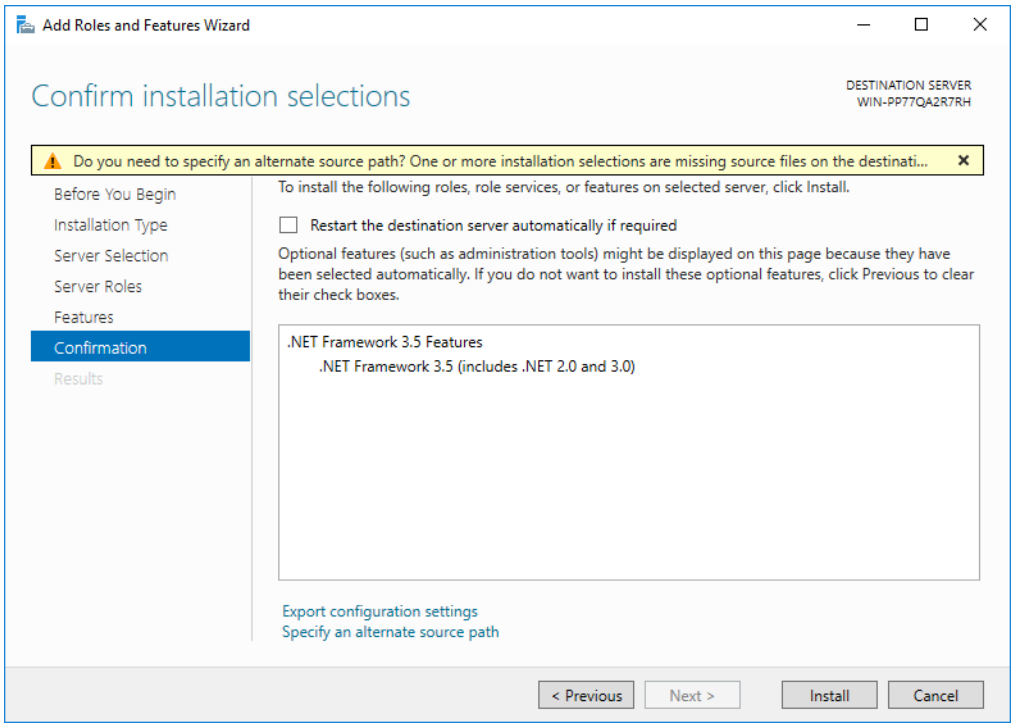

Fig. 19: Add Roles and Features Wizard

9. Open the *Windows Explorer* in the taskbar.
10. Click on the button *This PC*.
11. Right-click on the DVD drive.
    ⇨ A context menu appears.
12. Click on *Open* in the context menu.

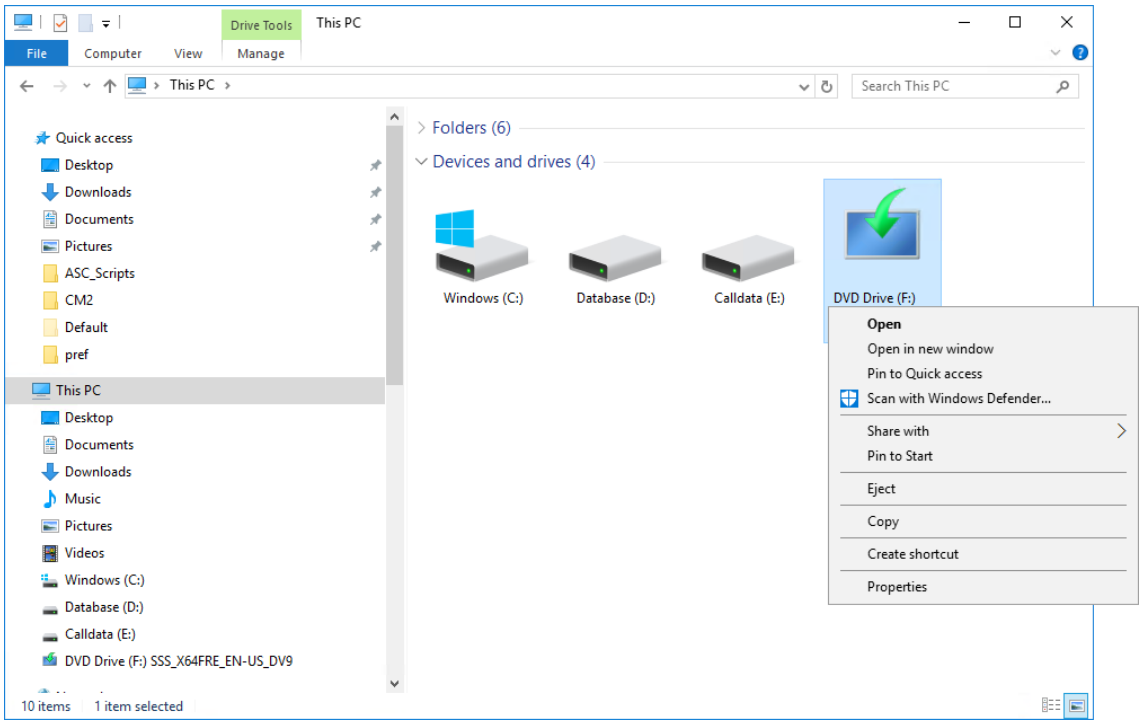

Fig. 20: Computer

13. Double-click on the folder *sources* in the structure view.
14. Click on the folder *sxs* in the structure view.
15. Left-click into the address bar at the top.
    ⇨ The folder path is selected.
16. Right-click into the address bar at the top.
    ⇨ A context menu appears.
17. Click on *Copy* in the context menu.

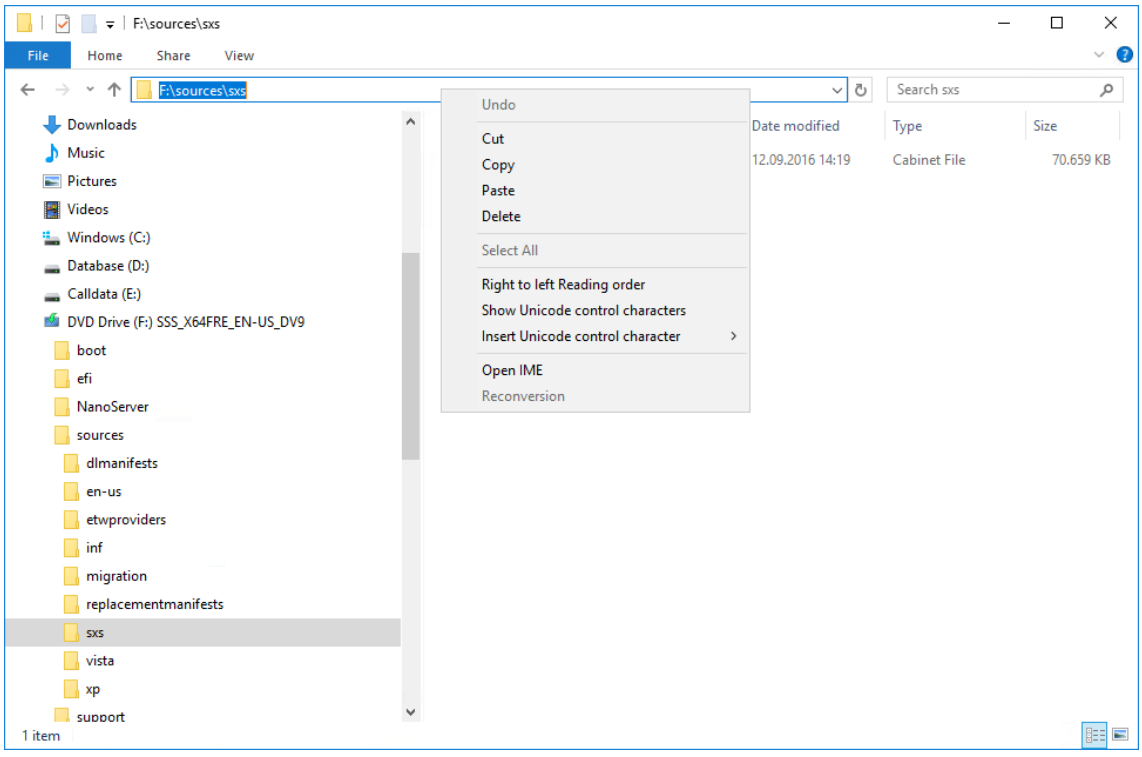

Fig. 21: Copy source path for configuration settings

18. Change to the window *Add Roles and Features Wizard*.
19. Click on *Specify an alternate source path*.

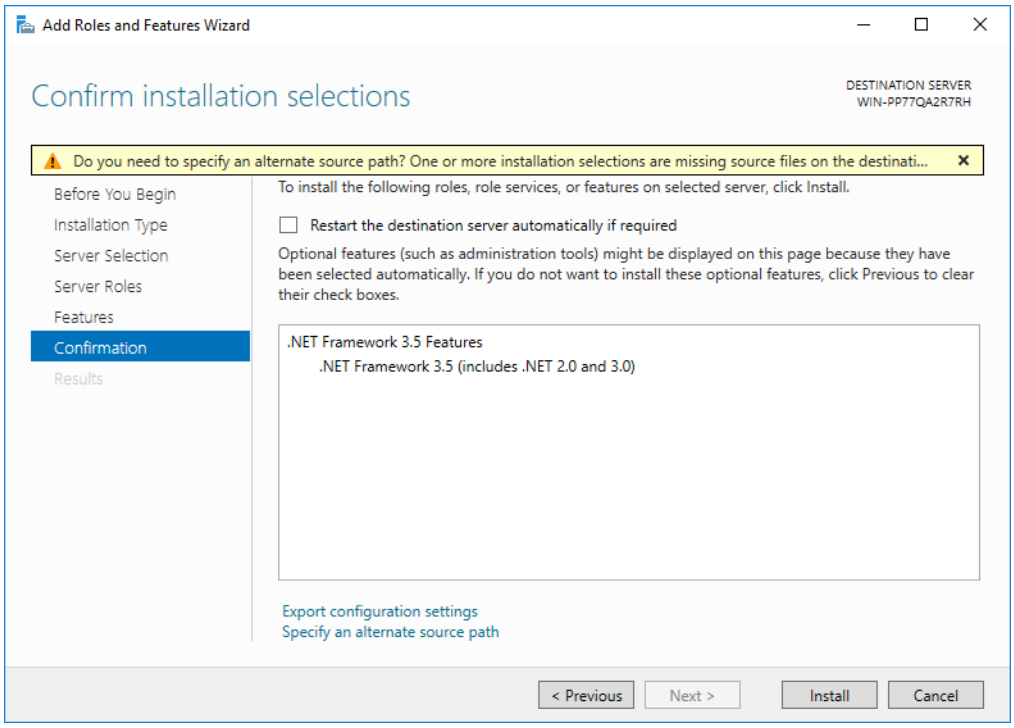

Fig. 22: Add Roles and Features Wizard

20. Right-click in the entry field *Path*.
    ⇨ A context menu appears.
21. Click on *Paste* in the context menu.
    ⇨ The path is pasted.

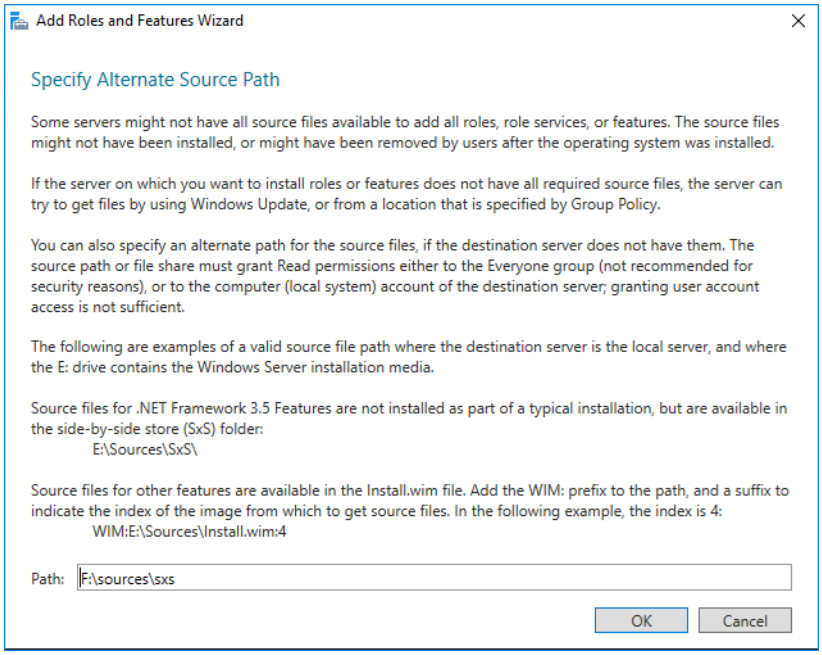

Fig. 23: Copy source path for configuration settings was pasted

22. Click on the button *OK* to save the settings and to close the window.
23. Click on the button *Install* to install the service.
24. Click on the button *Close* to close the window.

6.6 Install Media Foundation

1. Press the Windows key.
2. Open the Windows options by clicking on *Control Panel* > *Programs and Features*.
3. Click on the option *Turn Windows features on or off*.

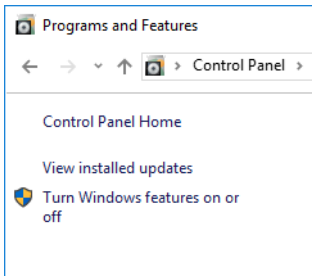

Fig. 24: Windows options

4. The following window appears:

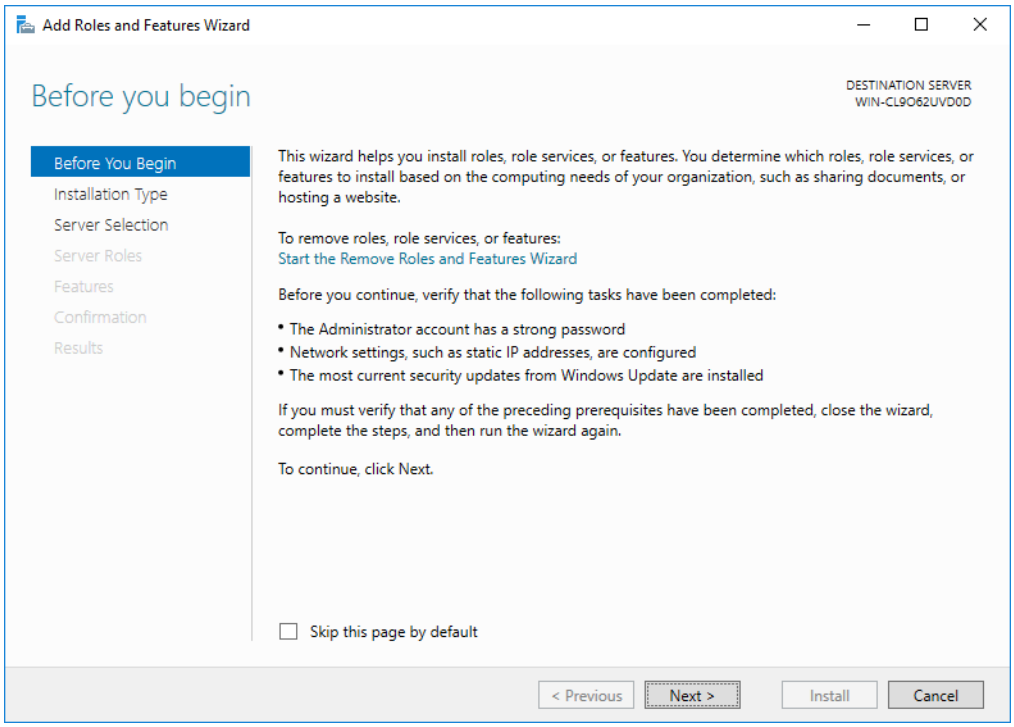

Fig. 25: Add Roles and Features Wizard

5. Click on the button *Next*.
6. Under *Installation Type*, activate the option *Role-based or feature-based installation*.

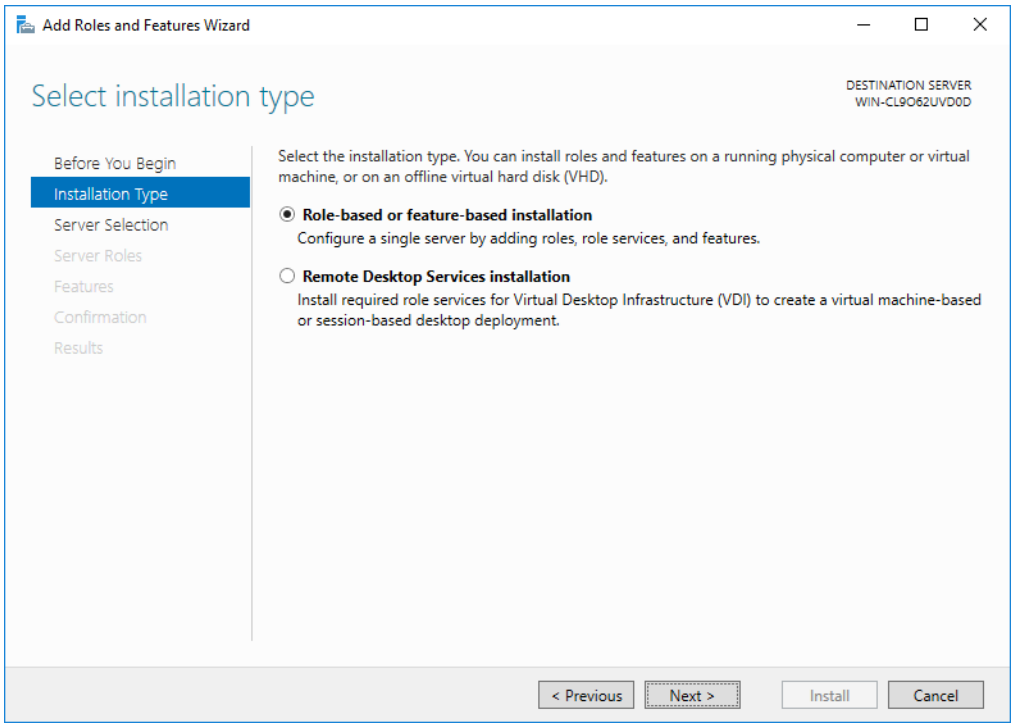

Fig. 26: Installation type

7. Click on the button *Next*.
   ⇨ The following window appears:

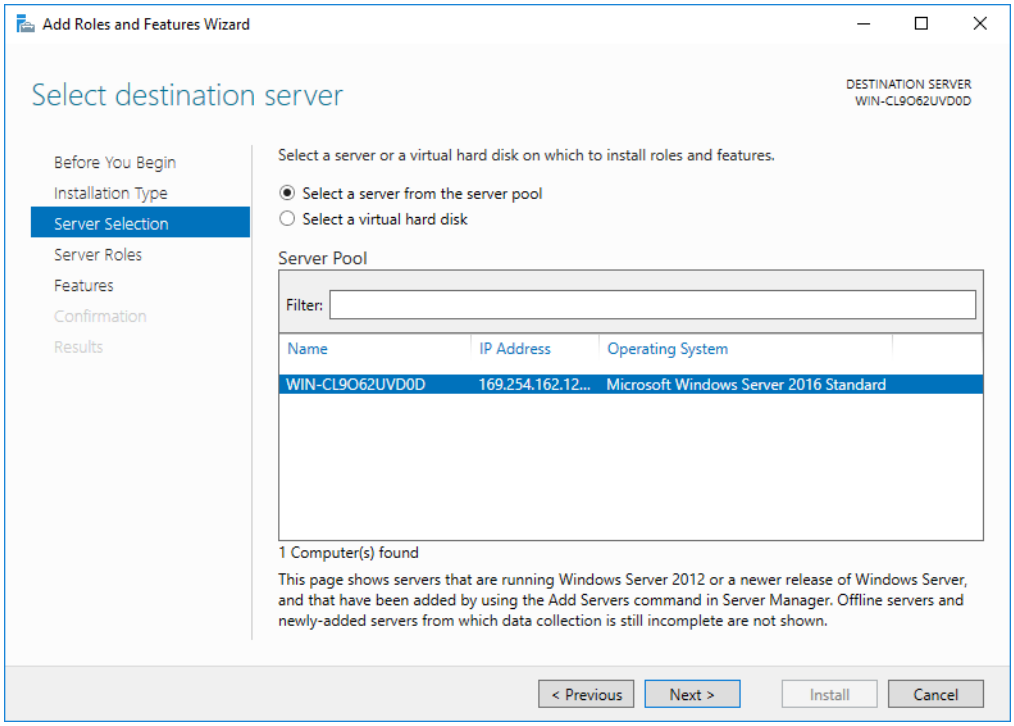

Fig. 27: Server selection

8. Under *Server Selection*, activate the option *Select a server from the server pool*.
9. Select your server from the pool of servers.
10. Click on the button *Next*.
    ⇨ The following window appears:

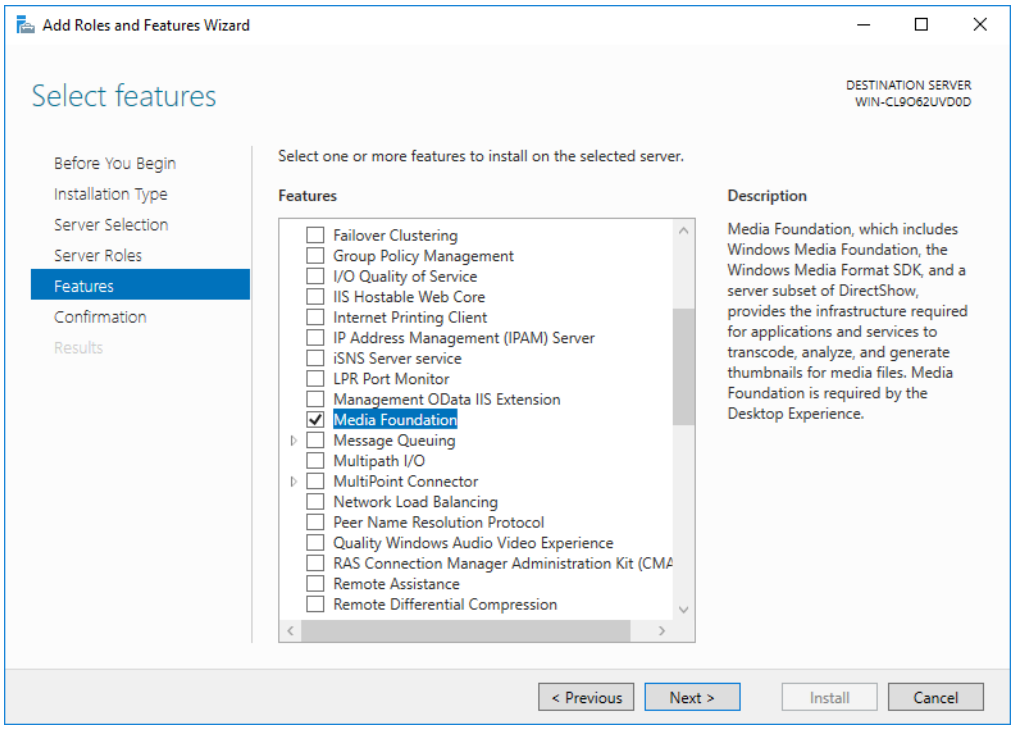

Fig. 28: Features

11. Under *Features*, activate the option *Media Foundation*.
12. Click on the button *Install* to install the service.
13. Restart the computer after the installation to apply the settings.

6.7 Enable script hosts

To check whether script hosts have been enabled and to configure scrip hosts if required, proceed as follows:

1. Press the Windows key.
2. Enter *regedit.exe*.
3. In the list of search results above, right-click on *regedit.exe*.
   ⇨ A context menu appears.
4. Click on *Run as administrator* in the context menu.
5. Change to the path *HKEY_LOCAL_MACHINE* > *Software* > *Microsoft* > *Windows Script Host* > *Settings*.
6. If the entry *Enabled* is not displayed in the main view, you do not have to continue the configuration of the script hosts.
   If the entry *Enabled* is displayed in the main view, proceed as follows:
7. Double-click on the entry *Enabled*.
8. In the entry field *Value Data*, enter the value *1*.

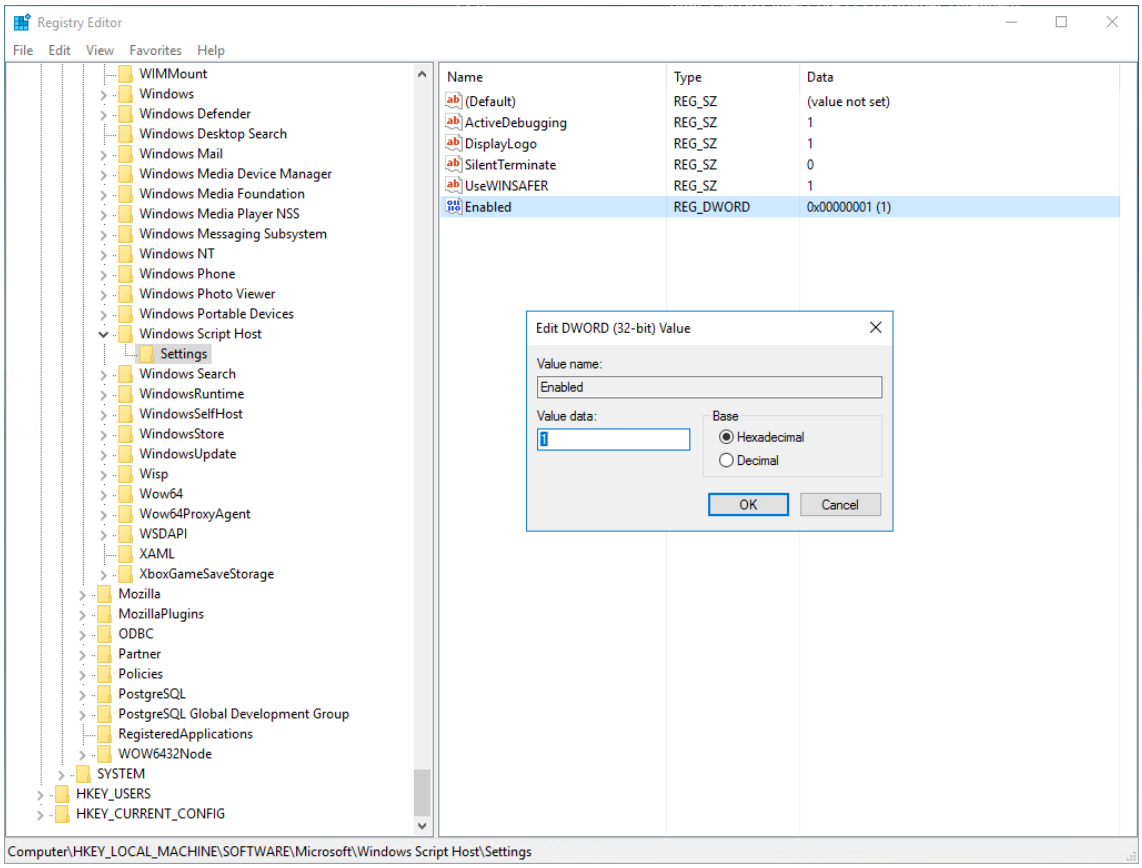

Fig. 29: Enable script hosts

9. Click on the button *OK* to save the entries and close the window.

6.8 Configure maximum password age

1. Press the Windows key.
2. Enter *gpedit.msc*.
3. In the list of search results above, right-click on *gpedit.msc*.
   ⇨ A context menu appears.
4. Click on *Run as administrator* in the context menu.
   ⇨ The window *Local Group Policy Editor* opens.
5. Change to the path *Computer Configuration* > *Windows Settings* > *Security Settings* > *Account Policies* > *Password Policy*.

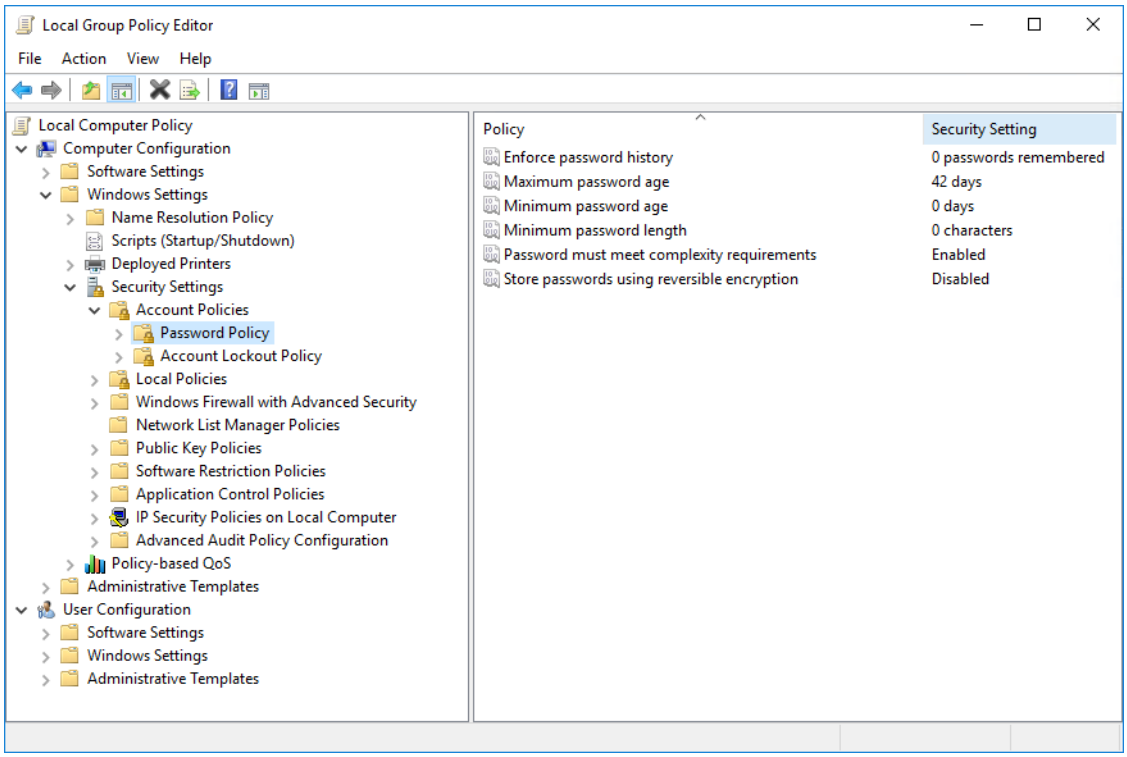

Fig. 30: Local Group Policy Editor

6. In the main view, right-click on *Maximum password age*.
   ⇨ A context menu appears.
7. Click on *Properties* in the context menu.
8. Under *Password will expire in* enter the value *0*.
   ⇨ The description now says *Password will not expire*.

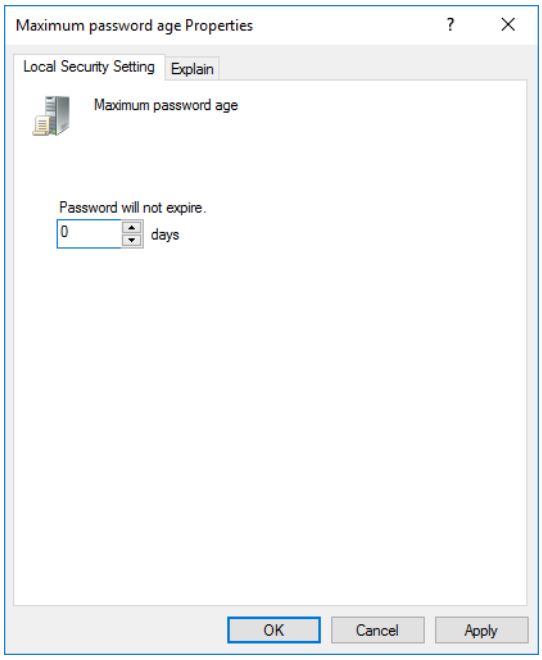

Fig. 31: Maximum password age Properties

9. Click on the button *OK* to save the entries and close the window.

6.9 Deactivate write cache for hard disk

1. Press the Windows key.

2. Open the system configuration by clicking on *Control Panel* > *All Control Panel Items* > *System*.
3. Click on the shortcut *Device Manager*.

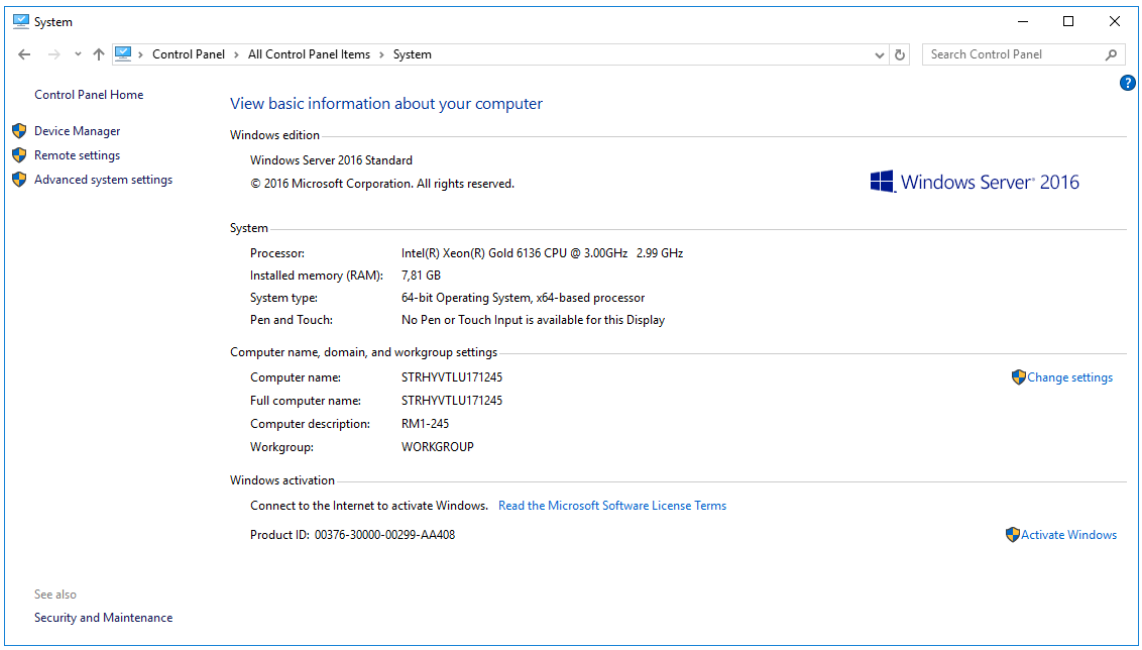

Fig. 32: System

4. Open the menu item *Disk drives* in the structure view.
5. Right-click on the hard disk where the database data has been saved.
   ⇨ A context menu appears.
6. Click on the menu item *Properties* in the context menu.

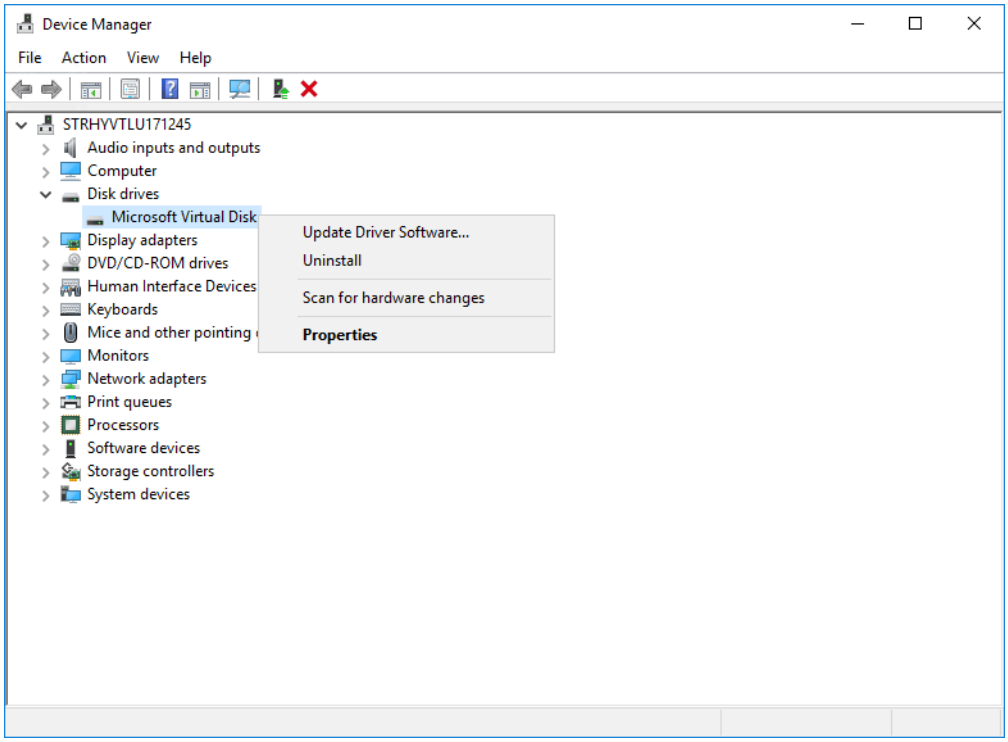

Fig. 33: Device Manager

7. Click on the tab *Policies*.
8. Deactivate the option *Enable write cache on the device*.

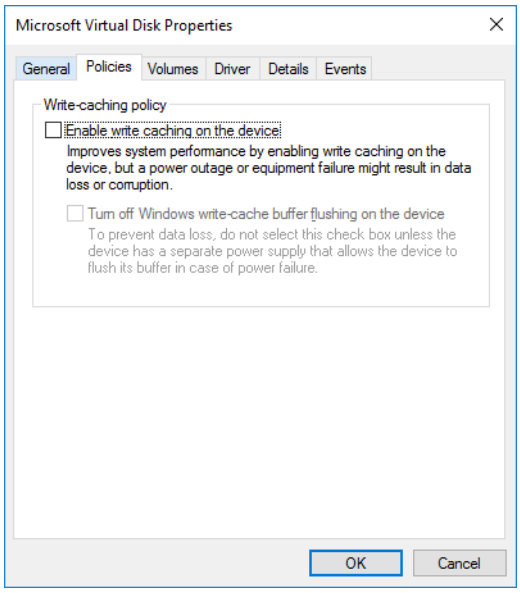

Fig. 34: Properties of hard disk

9. Click on the button *OK*.

7 Quick guide

7.1 General requirements

- 3 partitions:

  At least 60 GB for the system partition

  At least 40 GB for the database partition

  At least 150 GB for the data partition

7.2 Observe the following steps after the installation of Windows Server 2016

- Deactivate IE Enhanced Security Configuration (IE ESC):

  Server Manager > Local Server > IE Enhanced Security Configuration: Off > Administrators, Users: select `Off` respectively **> OK**.

- Configure network card:

  Windows key > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings > NIC > Internet Protocol, Version 4 (TCP/IPv4) **Properties:** `Use the following IP address` enter IP address, subnet mask, default gateway **> OK > Configure > Power Management:** deactivate `Allow the computer to turn off this device to save power`

  if no sniffer card **> OK**.

  Configure sniffer card for passive recording:

  > Advanced > Receive Buffers or **Receive Descriptors > Value:** enter maximum value: `1024-2048` (depending on the network card) **> OK**.

- Configure services:

  Server Manager > Tools > Services > Windows Firewall > Properties > General > Start > Startup type: `Automatic` **> OK > Windows Audio > Properties > General > Startup type:** `Automatic` **> OK > Windows Time > Properties > General > Startup type:** `Disabled` **> Stop > OK**.

- . Install .NET framework:

  Server Manager > Add roles and features > Next > Next > Next > Next > activate **.NET framework 3.5 Features > Next > Windows Explorer > This PC >** right-click to copy folder path **DVD > Open > \sources\sxs:** and change to the following window **Add Roles and Features Wizard > Specify an alternate source path > Path:** paste copied folder path **> OK > Install**.

- Install Media Foundation:

  Activate **Windows key > Control Panel > Programs and Features > Turn Windows features on or off > Next > Roles-based or feature-based installation** activate **> Next > Select a server from the server pool** and select your server **> Next >** activate **Media Foundation > Install** and reboot computer.

- Enable script hosts:

  Windows key > enter `regedit.exe` **>** right-click on search result **regedit.exe > Run as administrator >** select path **HKEY_LOCAL_MACHINE > Software > Microsoft > Windows Script Host > Settings**

  If the entry **Enabled** is not displayed in the main view, you do not have to continue the configuration of the script hosts.

  If the entry **Enabled** is displayed in the main view, proceed as follows: double-click **Enabled > Value Data** enter `1` **> OK**.

- Configure maximum password age:

Windows key > enter `gpedit.msc` **>** right-click on the search result **gpedit.msc > Run as administrator >** select path **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy >** right-click on **Maximum password age > Properties > Password will expire in:** enter value `0` **> OK**.

- Deactivate write cache for hard disk:

  Windows key > Control Panel > All Control Panel Items > System open **Device Manager** in the **Disk drives** structure view > right-click on the hard disk where database data has been saved, deactivate **> Properties > Policies > Enable write caching on the device > OK**.

List of figures

List of tables

Glossary

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)

Sniffer card

A sniffer card is a network card approved by ASC for passive VoIP recording.

SNMP

Simple Network Management Protocol is a network protocol and serves to monitor and manage network components. The protocol does not depend on the IP network protocol for the transport. It sends notifications (traps) about the activities on the network components on its own accord.

VoIP

Voice over IP