

Siemens
Industry
Online
Support

PCS 7 Virtualization - Project Engineering and Configuration

SIMATIC PCS 7 V10.0 SP1

SIEMENS

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.



DANGER

indicates that death or severe personal injury will result if proper precautions are not taken.



WARNING

indicates that death or severe personal injury may result if proper precautions are not taken.



CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:



WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial cybersecurity measures that may be implemented, please visit https://www.siemens.com/cybersecurity-industry.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://new.siemens.com/cert.

Industrial Security

This product is a part of SIMATIC PCS 7 and integrated into the overall plant security concept. Siemens strongly recommends setting up, operating, maintaining, and decommissioning the plant environment according to the SIMATIC PCS 7 Compendium Part F – Industrial Security: Technical documentation SIMATIC PCS 7 (https://support.industry.siemens.com/cs/ww/en/view/109815443).

© Siemens 2025

Table of contents

1. Foreword 6

2. Automation task 7

2.1. Overview 7
2.2. Requirements for virtualization 7
2.3. Application areas for virtualization 7

3. Automation solution 8

3.1. SIMATIC PCS 7 system architecture in a virtual environment 8
3.2. What is virtualization? 9
3.2.1. Definition 9
3.2.2. Server-based virtualization (Type 1: Native) 11
3.2.3. Client-based virtualization (Type 2: Hosted) 12
3.2.4. Summary of server-based and client-based virtualization 13
3.2.5. Advantages and disadvantages of virtualization 14
3.2.6. Support for SIMATIC PCS 7 in virtual environments 15
3.3. SIMATIC PCS 7, SIMATIC WinCC and SIMATIC NET 16
3.4. SIMATIC Virtualization as a Service 17
3.5. SIMATIC IPC with Microsoft Hyper-V 18
3.5.1. Basic principle 18
3.5.2. Basic procedure 18

4. Configuration 19

4.1. Configuration of the host systems 19
4.1.1. Recommended Hardware 19
4.1.2. Hardware for Microsoft Hyper-V on Basis IPC 20
4.1.3. Microsoft Hyper-V: Create the VHDX files for the VMs 21
4.1.4. Installation and configuration of the host for Microsoft Hyper-V 22
4.1.5. Network 27
4.1.6. Time synchronization 30
4.2. Configuration of the guest systems 33
4.2.1. General information 33
4.2.2. Special features for VMware by Broadcom ESXi 34
4.2.3. Create and commission the VMs for Microsoft Hyper-V 35
4.2.4. Configuration of the network adapters 42
4.2.5. Licensing 45
4.3. Configuration examples for ESXi 46
4.3.1. Configuration of the VMs 46
4.3.2. Configuration 1 48

 © Siemens 2025

4.3.3. Configuration 2 ... 49
4.3.4. Configuration 3 ... 50
4.4. Remote access ... 51
4.5. Communication ... 52
4.5.1. Name resolution ... 52
4.5.2. VLANs ... 52
4.5.3. Redundancy connection between servers ... 52
4.5.4. Communication over multiple subnets (Terminal bus) ... 53
4.5.5. Communication with the AS ... 53
4.5.6. Redundant, fault-tolerant plant bus only with ESXi ... 55
4.5.7. Redundant terminal bus ... 56

5. User scenarios ... 58
5.1. Engineering functions ... 58
5.2. Process mode ... 60
5.3. Maintenance Server and Maintenance Client ... 60
5.4. SIMATIC Management Console (SMMC) ... 62

6. Notes / constraints ... 63
6.1. SIMATIC BATCH ... 63
6.2. Special hardware ... 63
6.3. New VMs/templates/clones with VMware by Broadcom ESXi ... 63
6.4. Dual monitors ... 65
6.5. Chip card reader ... 65
6.5.1. Configuration of users and groups for login ... 66
6.5.2. Configuration in the WinCC User Administrator of an OS Client ... 67
6.5.3. Connecting the smart card reader to a USB port on the thin client ... 68
6.5.4. Configuring SIMATIC Logon on the OS Client ... 69
6.5.5. Editing the chip card ... 71
6.5.6. Logging in to OS Runtime with Smart Card ... 72
6.6. S7 F/FH systems ... 74
6.7. Diagnostics with VMware by Broadcom ESXi ... 74

7. Glossary ... 78

8. Appendix ... 79
8.1. Service and support ... 79
8.2. Links and literature ... 80

© Siemens 2025

1. Foreword

Purpose of this document

This document will give you an overview for operating SIMATIC PCS 7 in a virtual environment. It describes typical configurations and features that should be borne in mind if stable and tested operation is desired.

Key content

This document deals with the following key topics:

- Typical configuration highlights
- Typical feature highlights
- Experiences from the practical operation of PCS 7 in a virtual environment.

Scope of validity

This document applies to PCS 7 V10.0 SP1.

NOTE Observe the information and notes in the entry "OS client, Batch client, Route Control client with SIMATIC PCS 7 V10.0 SP1 released for virtual operating environments"

© Siemens 2025

2. Automation task

2.1. Overview

The virtualization of systems has already achieved great importance in information technology. Even users of automation technology (e.g. SIMATIC PCS 7) have recognized the benefits of virtualization and are applying it increasingly.

This application example includes the following information:

- Virtualization of typical SIMATIC PCS 7 system configurations
- Which infrastructure is required for the virtualization of SIMATIC PCS 7 systems?
- What should I consider when running SIMATIC PCS 7 in virtual operating environments?

2.2. Requirements for virtualization

The availability of the system and the automation technology has the highest priority. This also applies to systems with real computers and for systems running in a virtual environment.

When running systems in a virtual environment, there should be no difference from real computers.

2.3. Application areas for virtualization

Various types of hardware and software for virtualization solutions can be used depending on the application area.

Use	Virtualization solution
Presentations and short tests	VMware by Broadcom Workstation Player, VMware by Broadcom Workstation Pro, ... VMware by Broadcom ESXi, Microsoft Hyper-V
Production plants	VMware by Broadcom ESXi, Microsoft Hyper-V

NOTICE

Approval of the virtualization software

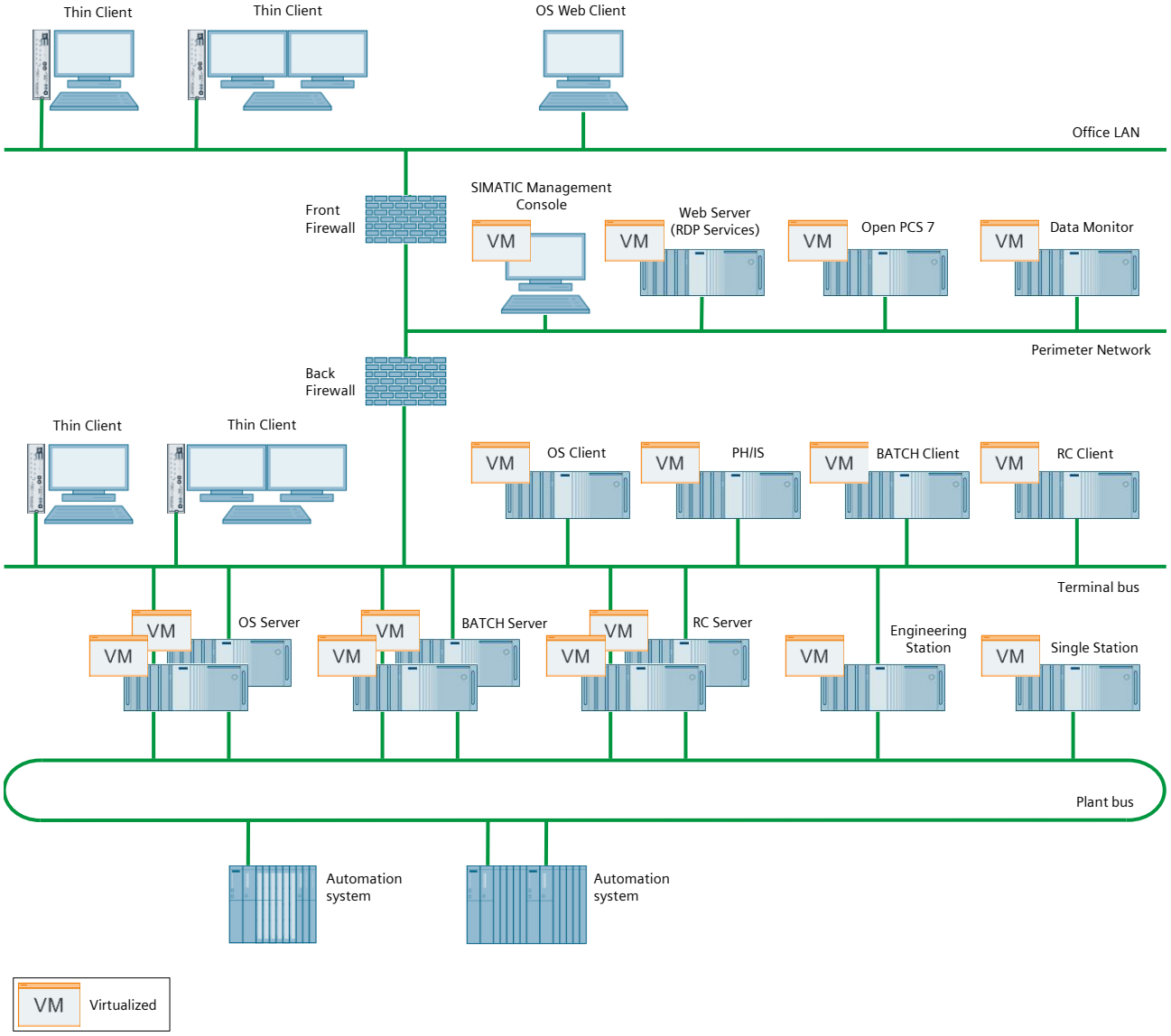
SIMATIC PCS 7 is approved for VMware by Broadcom ESXi. The approved version of VMware ESXi or Microsoft Hyper-V are included in the Compatibility tool. Possible configurations for Microsoft Hyper V on IPCs are listed in chap. 4.2.3.

© Siemens 2025

3. Automation solution

3.1. SIMATIC PCS 7 system architecture in a virtual environment

The SIMATIC PCS 7 systems marked "VM" in the following figure can be virtualized with VMware by Broadcom ESXi.



© Siemens 2025

3.2. What is virtualization?

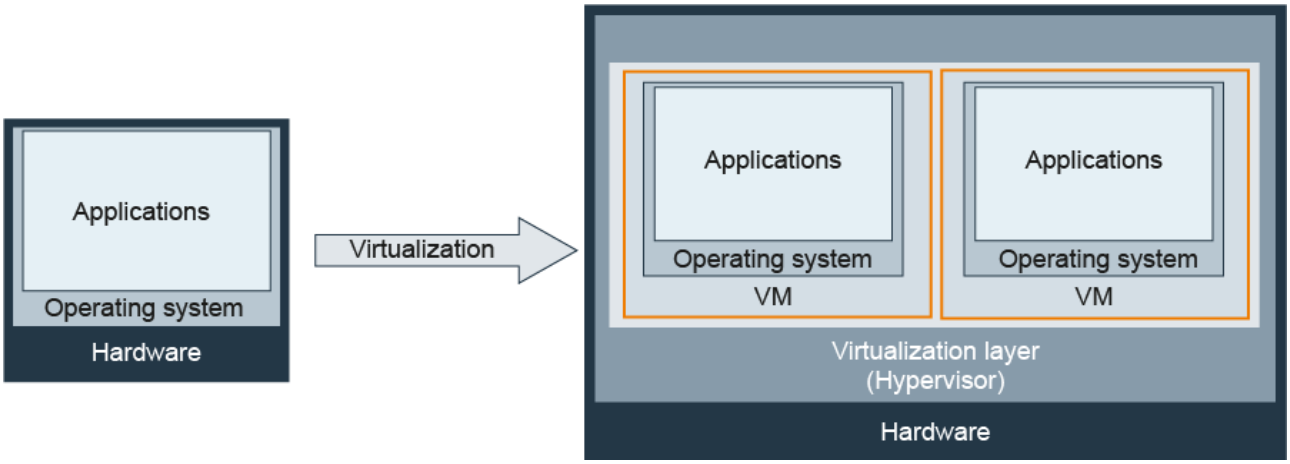
3.2.1. Definition

Virtualization

Virtualization refers to the abstraction of the physical hardware from the operating system. To achieve this, a special virtualization layer (so-called hypervisor) is installed in a real PC.

This makes it possible to implement several virtual machines (VM) isolated from each other on a real, physical computer (host system), each with its own virtual hardware components. They behave like real computers and can run their own applications independently.

Diagram about Virtualization



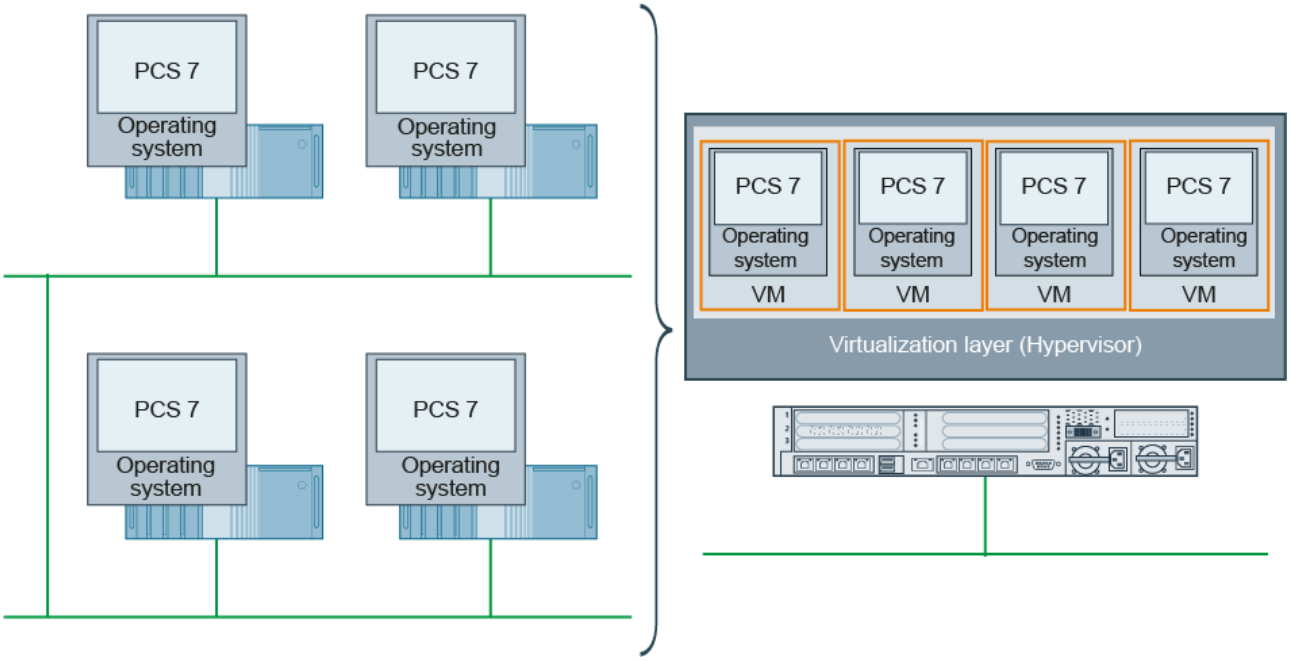
© Siemens 2025

Tasks of the hypervisor

Hypervisor tasks include the following:

- The hypervisor is the virtualization layer on top of which the VMs run.
- The hypervisor manages the resource allocation of existing real hardware on the VMs and the execution of the VMs.
- The hypervisor is also called VMM (Virtual Machine Manager or Monitor).

Physical and virtual design



Versions

There are basically two different types of virtualization which differ in their design and structure:

- Server-based virtualization (Type 1: Native)
- Client-based virtualization (Type 2: Hosted)

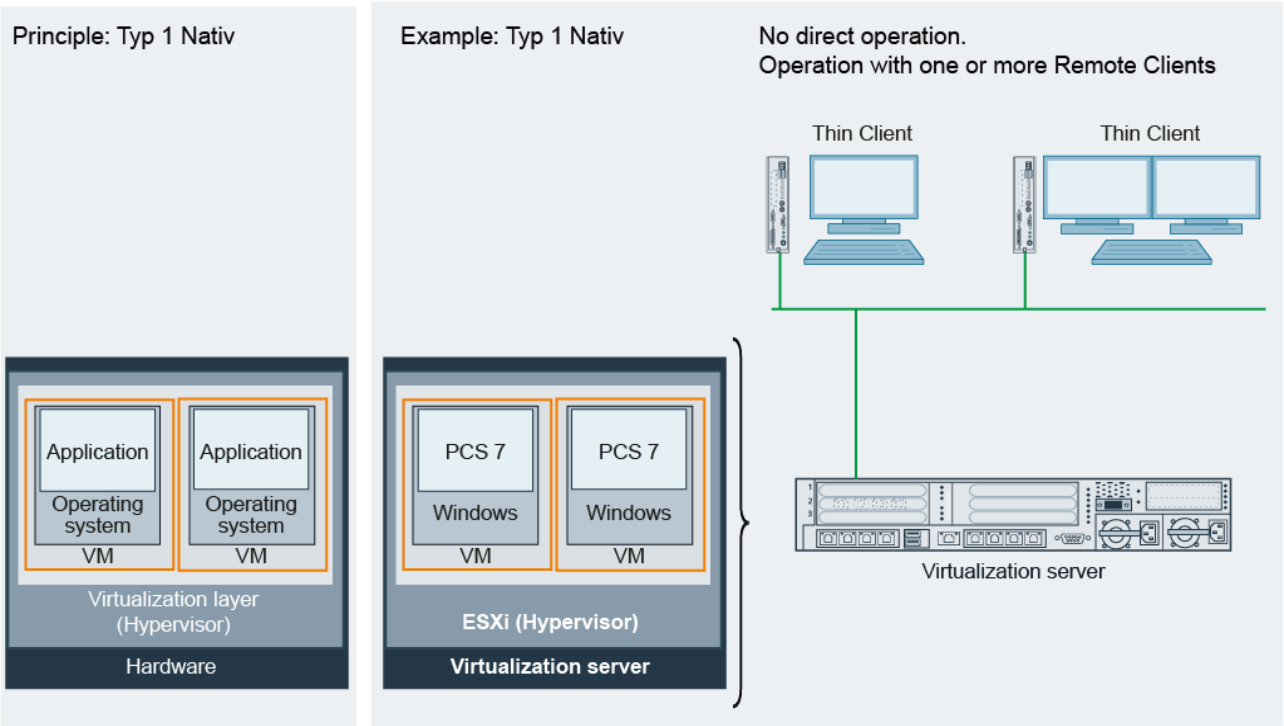
© Siemens 2025

3.2.2. Server-based virtualization (Type 1: Native)

This virtualization type is characterized by the following features:

- The hypervisor runs directly on the hardware of the host and is therefore more efficient. It requires fewer resources, but must provide all the necessary drivers.
- No direct operation: The VMs are operated via remote clients.
- Areas of application include data centers and production plants. This virtualization type can also be used for presentations and short tests.

Example



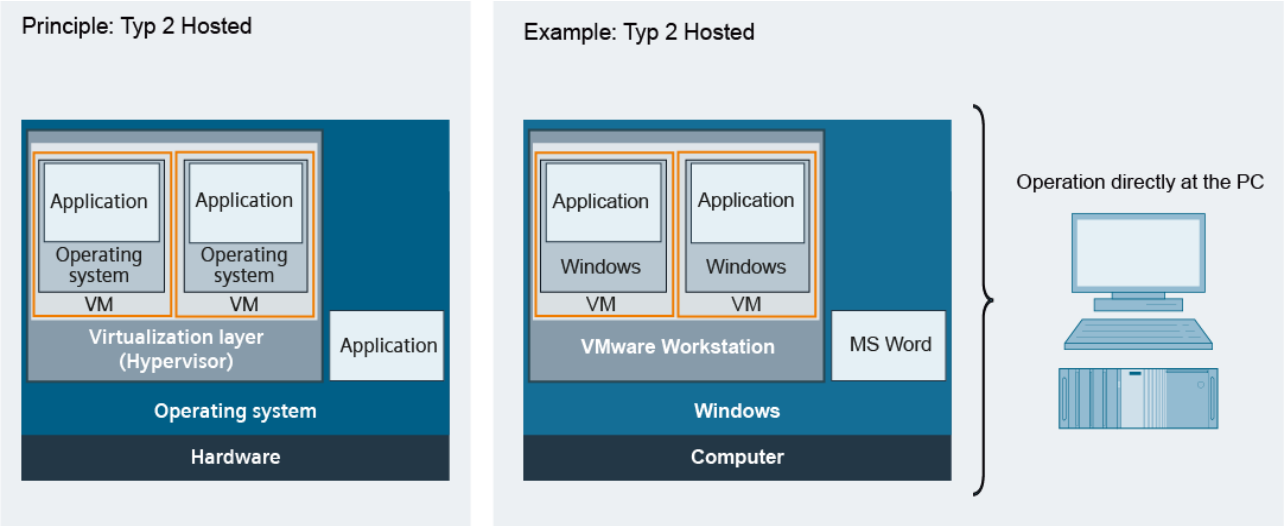
© Siemens 2025

3.2.3. Client-based virtualization (Type 2: Hosted)

This virtualization type is characterized by the following features:

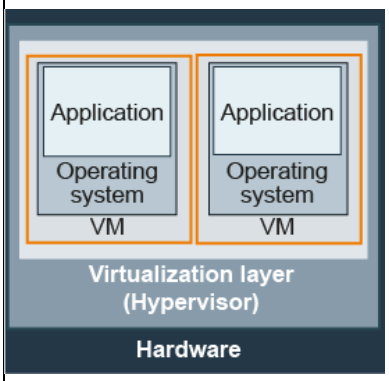
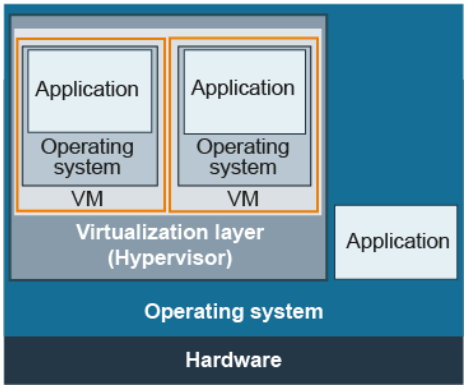
- The hypervisor is based on a full-fledged operating system (e.g. Windows) and uses the device drivers of the operating system.
- Direct operation: The VMs are operated directly from the PC via video card and monitor.
- Main application areas include presentations and short tests.

Example



© Siemens 2025

3.2.4. Summary of server-based and client-based virtualization

Server-based virtualization (Type 1 Native)	Client-based virtualization (Type 2 Hosted)
	
• The hypervisor runs directly on the hardware of the host and is therefore more efficient. It requires fewer resources, but must provide all the necessary drivers.	• The hypervisor is based on a full-fledged operating system (e.g. Windows) and uses the device drivers of the operating system.
• No direct operation: The VMs are operated via remote clients.	• Direct operation: The VMs are operated directly from the PC via video card and monitor
• Areas of application: Data centers and production plants	• Areas of application: Presentations and short tests

© Siemens 2025

3.2.5. Advantages and disadvantages of virtualization

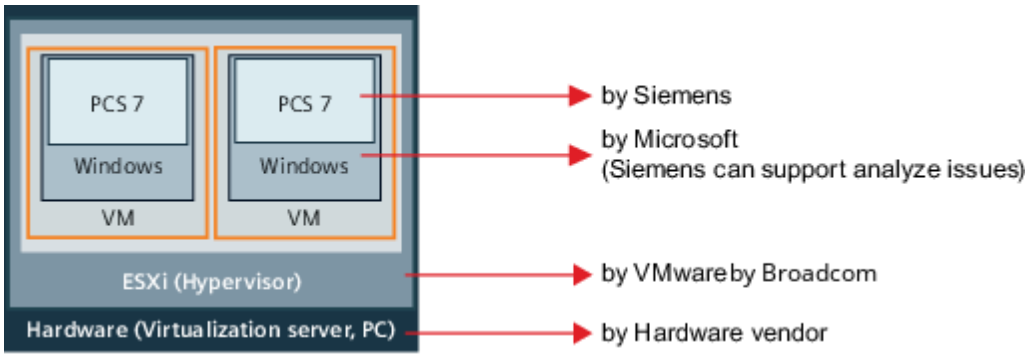
	Advantages	Disadvantages
Costs	Reduced costs • Consolidation of physical computers, cables, switches, etc. • Reduction of energy consumption • Footprint reduction • Cheaper hardware can be used for clients (so-called Thin Client solutions)	• Additional license fees may apply for virtualization depending on the scope of functions
Security	Increased security • Increased security via remote access and centralized rights management • Reduced attack possibilities with Thin Clients; central protection on the host for the virtual machines	• Possible increase in security-related expenses (additional layer, data security)
Availability	Increase of availability • Virtual machines running on the host can be easily replaced	• Danger of a "single point of failure" • Support may not be from one source
Flexibility	Increased flexibility • Hardware independence of virtual machines • Virtual machines running different operating systems on one host • Possibility of adding virtual machines by starting another VMware session	
System complexity		• Significant increase of system complexity • Higher administration costs

© Siemens 2025

3.2.6. Support for SIMATIC PCS 7 in virtual environments

3.2.6.1. Support for VMs based on VMware by Broadcom ESXi

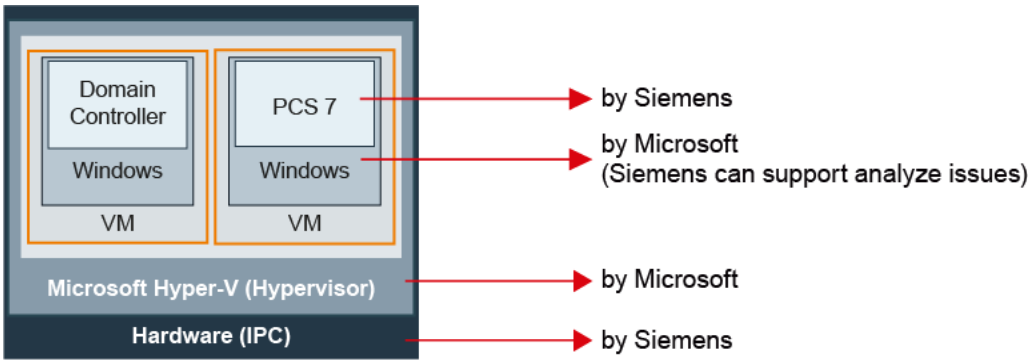
If a problem occurs when operating a virtual machine, the necessary support can be laborious. In this instance, responsibility must be first clarified as shown in the following picture.



NOTE When using SIMATIC Virtualization as a Service (see chapter 3.4), you not only get preinstalled and preconfigured ESXi Servers including SIMATIC PCS 7 installations in the form of VMs, you also get the service for these complete systems from a single source.

NOTE You can use a support request to determine the performance requirements of a virtualized SIMATIC PCS 7 / WinCC system.
Further information on this is available in the following FAQ:
"Technical support for the design of a virtual SIMATIC PCS 7 / WinCC system

3.2.6.2. Support for VMs based on IPC and Microsoft Hyper-V



The necessary support is simpler because the responsibility in the event of a support case is limited to either Siemens or Microsoft.

© Siemens 2025

3.3. SIMATIC PCS 7, SIMATIC WinCC and SIMATIC NET

Apart from this document, you can find further information and notes on how to operate SIMATIC PCS 7 in a virtual environment in the entry "OS client, Batch client, Route Control client with SIMATIC PCS 7 SP1 V10.0 released for virtual operating environments".

SIMATIC WinCC and SIMATIC NET are two essential components of SIMATIC PCS 7. There are therefore plenty of similarities, but also differences. You can find more information at:

- WinCC Virtualization
- Sales/delivery release of SIMATIC NET Software V18
- Quantity structures and performance data of the individual SIMATIC NET products

© Siemens 2025

3.4. SIMATIC Virtualization as a Service

SIMATIC Virtualization as a Service is a preconfigured, ready-to-use virtualization system based on VMware by Broadcom ESXi and Microsoft Hyper-V for the implementation of efficient automation solutions for SIMATIC systems.



A hypervisor is installed on a powerful server in order to manage hardware resources and share them dynamically across virtual machines. A management console serves for central administration, configuration and maintenance of the virtual machines and virtualization server.

The virtual machines are equipped with SIMATIC PCS 7 or SIMATIC WinCC installations and come preconfigured for their particular automation task
(e.g. PCS 7 ES/Client, WinCC Server).

The virtualization system can be extended easily and efficiently using preconfigured virtual machines and is therefore scalable to different system sizes. A fault-tolerant system can be realized by using additional virtualization servers.

You will find further information on SIMATIC Virtualization as a Service at:

- http://www.siemens.com/sivaas

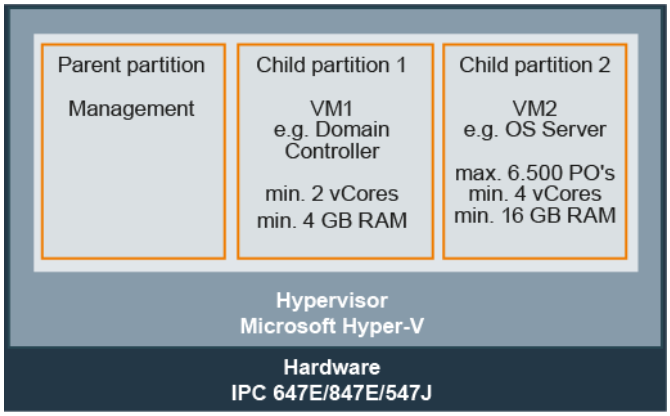
© Siemens 2025

3.5. SIMATIC IPC with Microsoft Hyper-V

IPCs with two virtual machines based on Microsoft Hyper-V have been approved for the first time with SIMATIC PCS 7 V9.1.

3.5.1. Basic principle

The special feature of Hyper-V is the so-called "parent partition", which is used exclusively for management.



NOTE Microsoft Windows for the virtual machines must be manually activated with the activation key listed on the COA sticker.

NOTE If more than two VMs are to be operated, additional CoA licenses must be purchased by article number

NOTE When allocating resources, make sure the minimum requirements are met; do not exceed the available resources of the virtualization host you are using.

NOTE If the host needs to be restarted, the VMs have to be terminated/stopped beforehand.

3.5.2. Basic procedure

1. Create the VHDX files for the VMs chapter 4.1.3
2. Install/configure the host with Hyper-V chapter 4.1.4
3. Create and commission the VMs chapter 4.2.3

© Siemens 2025

4. Configuration

4.1. Configuration of the host systems

NOTICE **Performance**

The host systems must be configured in such a way that sufficient resources can be assigned to them during periods of increased performance requirements.

4.1.1. Recommended Hardware

The following recommendations are proven based on practical experience:

- The configured main memory (RAM) for all concurrent VMs must not exceed 90% of the available physical RAM.
- The 2:1 ratio of the virtually configured CPU cores for all concurrent VMs to the physically available CPU cores should not be exceeded.

  The following table shows an example of a possible allocation:

Hardware	Quantity	Use	
Intel® Xeon® Gold 6444Y Grundtakt: 3,46 GHz	16 Cores 32 Threads	Host	1 Core = 2 vCores
		2x ES 1x OS Server 1x SB Server 9x OS Client	8 vCores 2 vCores 2 vCores 18 vCores

- The best read-write performance can be achieved by implementing a RAID 10 system for the data stores.
- Better performance can be achieved from SIMATIC PCS 7 by preferring a CPU with fewer cores and a higher base frequency to a CPU with more cores and a lower base frequency.
  The deciding factor is a higher value of the "Single Thread Rating" parameter.

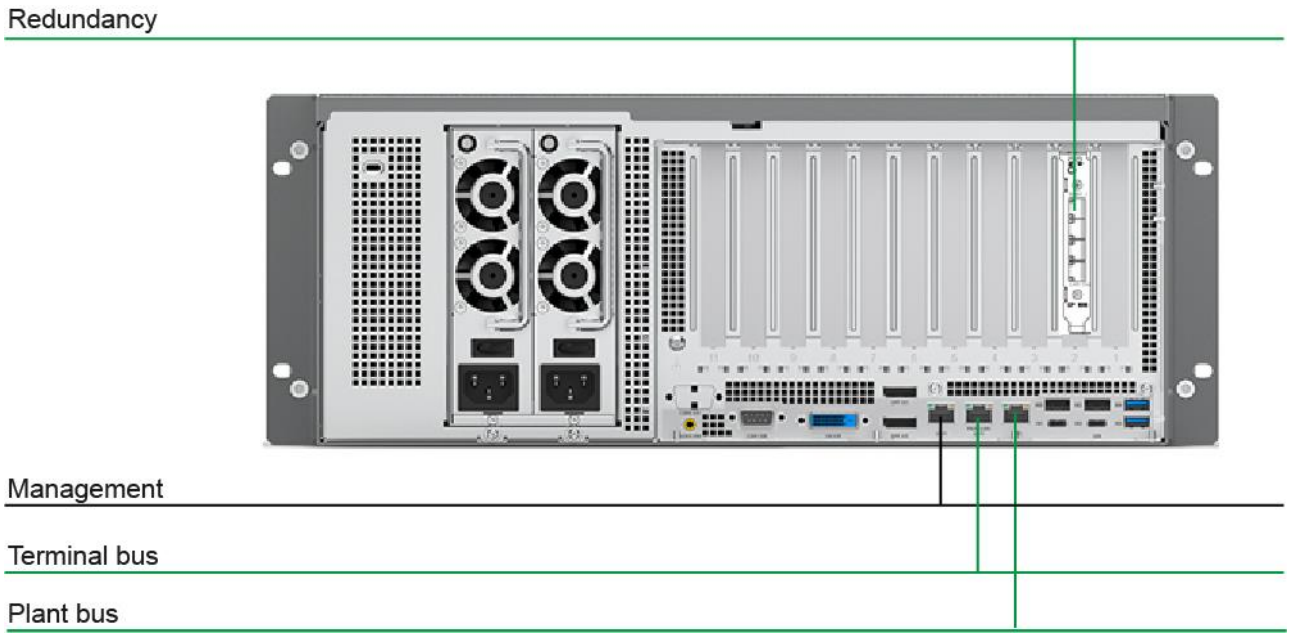
© Siemens 2025

4.1.2. Hardware for Microsoft Hyper-V on Basis IPC

To obtain the restore medium needed for the installation, use a PCS 7 OS Server Bundle BCE based on a IPC647E (6ES7661-0*), IPC847E (6ES7661-1*) or IPC547J (6ES7660-8*) in one of the following configurations:

- RACK PC, 19", 4 or 2 HE
- IPC647E/847E:
  Intel Xeon E-2176G (6C/12T, 3.7 (4.7) GHz, 12 MB Cache, TB, AMT)
  Intel Xeon E-2278GE (8C/16T, 3.3 (4.7) GHz, 16 MB Cache, TB, AMT)
- IPC547J:
  Intel Xeon W-1270E (8C/16T, 3.4 (4.8) GHz, 16 MB Cache)
- >=64 GB DDR4 SDRAM, with or without ECC
- >=512 GB SSD M.2 NVMe
- >=RAID1, 2x 960 GB SSD 2.5" SATA or
- >=RAID5, approx. 3.8 TB (3 x 1920 GB SSD 2.5" SATA); (only with IPC847E)
- 3x Ethernet interface onboard
- 1x Intel® Gigabit Network Adapter
- Microsoft Windows Server 2019 Standard or Microsoft Windows Server 2022 Standard

Example of a IPC847E:



© Siemens 2025

4.1.3. Microsoft Hyper-V: Create the VHDX files for the VMs

1. Start up the IPC from the included USB flash drive and perform a restore, e. g. of the OS Server image. For details on this procedure, please refer to the product information included with the device.

NOTICE **Terminating the restore environment with "Shutdown"**

Do not start the restore process for the image! Terminate the restore environment with the "Shutdown" menu.

2. Start the system with the SIMATIC IPC Image & Partition Creator and create a VHDX file of the system partition.
3. Repeat these steps for the operating system image "Windows (only)".

Result:

Two VHDX files have been created under the selected name.

© Siemens 2025

4.1.4. Installation and configuration of the host for Microsoft Hyper-V

Because the operating system image "Windows (only)" was restored recently (see previous chapter), now perform the commissioning. For details on this procedure, please refer to the product information included with the device.

Result:

The IPC has been installed with Windows Server 2019 Standard or Windows Server 2022 Standard.

4.1.4.1. Installation of Mircosoft Hyper-V

1. In "Server Manager", click "Manage" in the command line and select "Add Roles and Features". Keep the default settings in the subsequent dialogs.
2. Select the role "Hyper-V".
3. Install the necessary features by clicking "Add Features".
4. Do not create a virtual switch yet.
5. Select two storage locations, "Default location for virtual hard disk files:" und "Default location for virtual machine configuration files:" on drive E:, for example "E:\Hyper-V".
6. Tick the checkbox "Restart the destination server automatically if required".
7. Start the installation by clicking "Install".
   The Hyper-V role will now be installed and the host may restart if necessary. After the restart, the installation will continue automatically.
8. Finish the installation by clicking "Close".

Result:

Installation of the Hyper-V role is complete.

© Siemens 2025

4.1.4.2. Configuring the Microsoft Hyper-V settings for the host

In the next steps, verify and/or configure the Hyper-V settings for the host.

1. In "Server Manager", click on "Tools" in the command line and start the "Hyper-V Manager".
2. In the Hyper-V Manager, open "Hyper-V Settings..." from the context menu or with the actions of the virtualization host.
   Verify that the following settings have been made, or make them yourself:

Server settings

Name	Value	Description
Virtual Hard Disks	E:\Hyper-V	Specify the default folder to store virtual hard disk files
Virtual Machines	E:\Hyper-V	Specify the default folder to store virtual machine configuration files
NUMA Spanning	Enabled	Allow virtual machines to span physical NUMA Nodes
Live Migrations	Disabled	Enable incoming and outgoing live migrations
Storage Migrations	2	Simultaneous storage migrations
Enhanced Session Mode Policy	Disabled	Allow enhanced session mode
Replication Configuration	Disabled	Enable this computer as a Replica server.

User settings

Name	Value	Description
Keyboard	Enabled	Use on the virtual machine
Mouse Release Key	CTRL+ALT+LEFT ARROW	Release key
Enhanced Session Mode	enabled	Use enhanced session mode

3. Apply the settings by clicking "OK".

NOTE Virtual Machine Connection (VMConnect) is used for access to the VMs.

- VM Autologin for Windows can only be used in this mode.
- An RDP connection during the runtime to the OS Server in Enhanced Session Mode is not permitted.

The "Enhanced Session Mode Policy" setting is disabled for this reason.

4. In the Hyper-V Manager, open the "Virtual Switch Manager..." from the context menu or with the actions of the virtualization host.
   Add the following virtual switches:

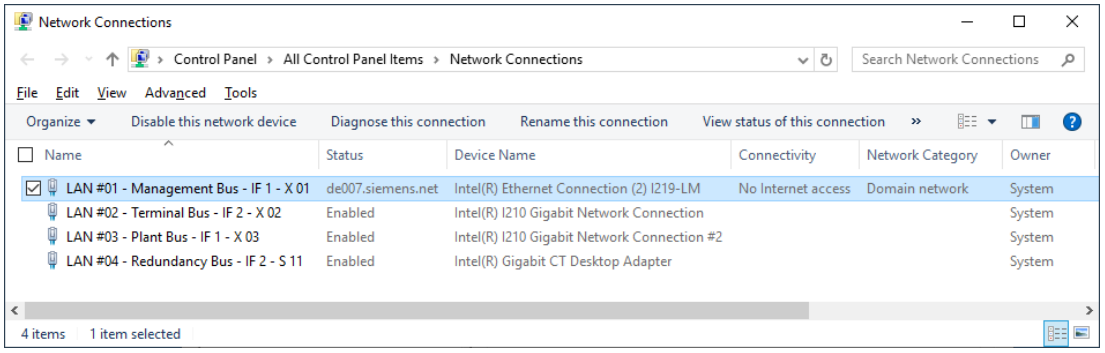
© Siemens 2025

Virtual switches

Name	Type	Selection
Virtual network switch LAN #02 - Terminal Bus - IF 2 – X 02	External network	Intel® I210 Gigabit Network Connection
Virtual network switch LAN #03 - Plant Bus - IF 1 – X 03	External network	Intel® I210 Gigabit Network Connection #2
Virtual network switch LAN #04 – Redundancy Bus IF 2 – S 11	External network	Intel® Gigabit CT Desktop Adapter

NOTE The option "Allow management operating system to share this network adapter" must not be enabled.

5. Apply the settings by clicking "OK".
6. In the Network & Sharing Center, rename the first network adapter "LAN #01" to "Management network".



NOTE Microsoft Hyper-V Replica and Live Migration are not supported.

Result:

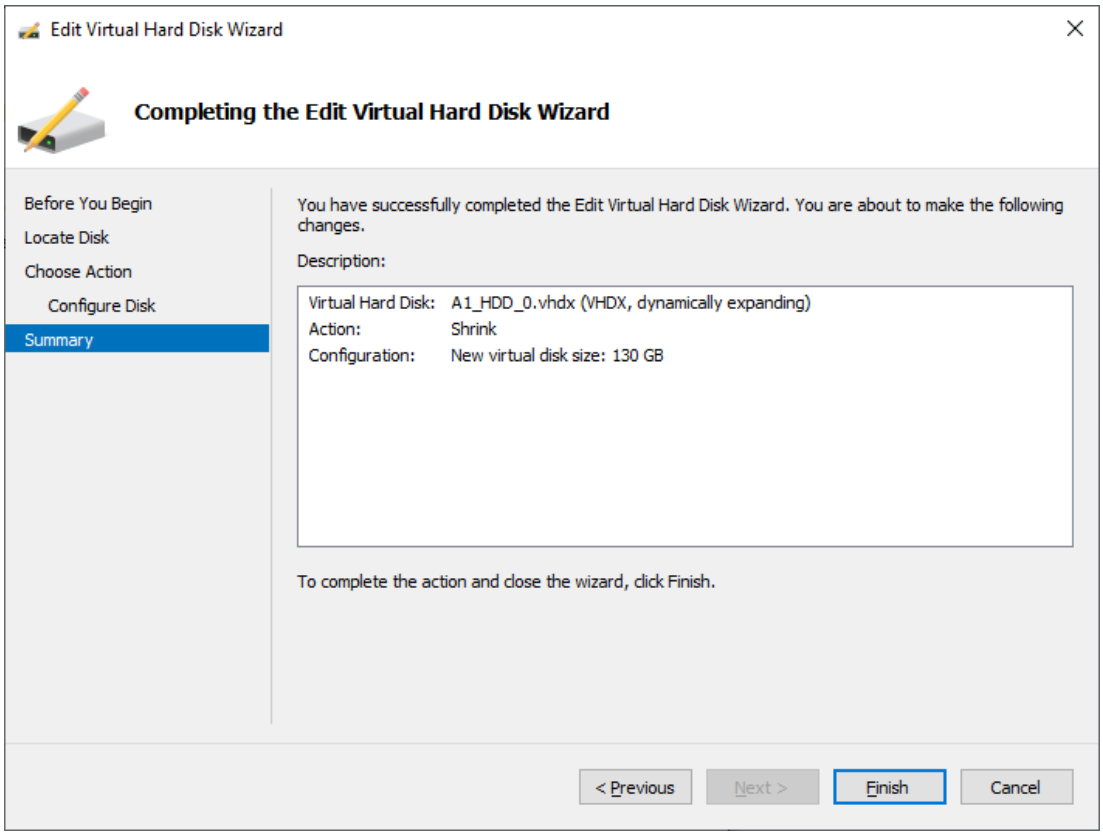
Microsoft Hyper-V, along with the necessary networks, is configured on the host.

© Siemens 2025

4.1.4.3. Configuring the VHDX files

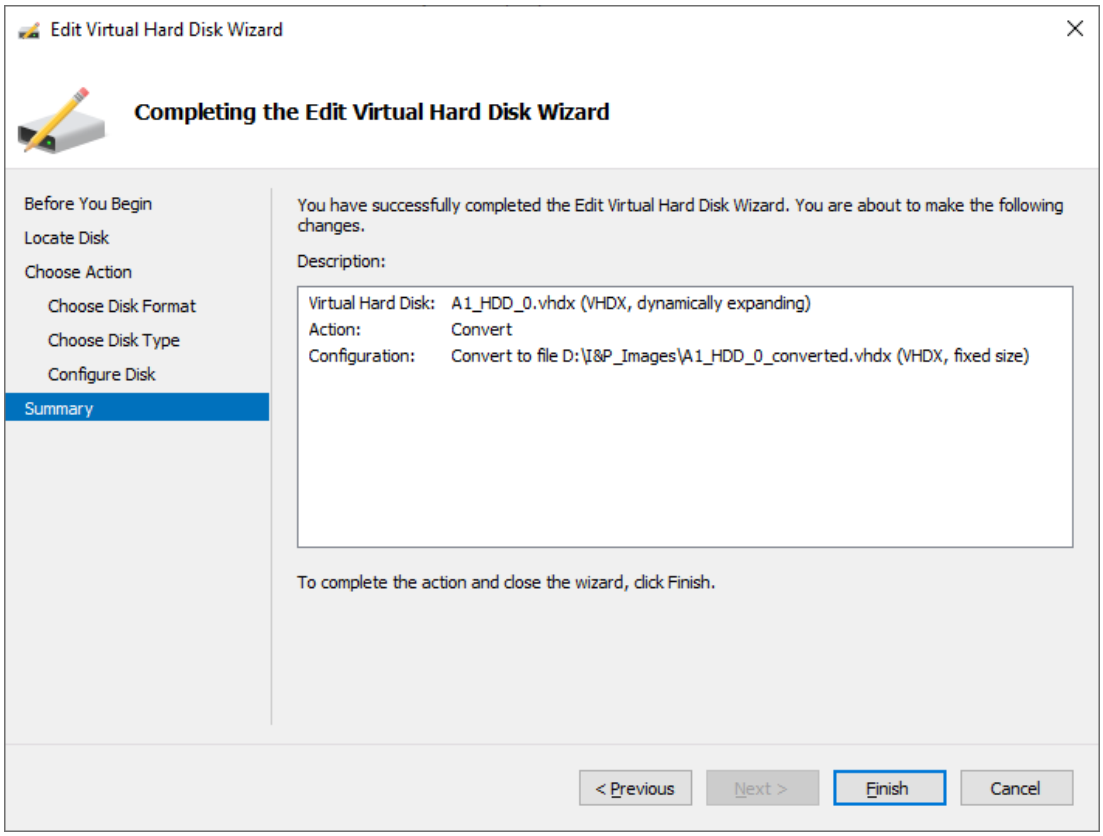
Before the VHDX files can be used in the VMs, they must first be modified:

7. In the Hyper-V Manager, open "Edit Disk..." from the context menu or with the actions of the virtualization host.
   - Choose Action: shrink
   - Configure disk: disk size 130 GB



8. Click "Finish" to close the "Edit Virtual Hard Disk Wizard".

9. In the Hyper-V Manager, open "Edit Disk..." from the context menu or with the actions of the virtualization host.
   - Choose Action: Convert
   - Choose Disk Format: VHDX
   - Choose Disk Type: Fixed Size
   - Configure Disk: <new name>



10. Click "Finish" to close the "Edit Virtual Hard Disk Wizard".
11. Repeat these steps for the second VHDX file.

Result:

Two VHDX files with a fixed size of 130 GB have been created under the selected name.

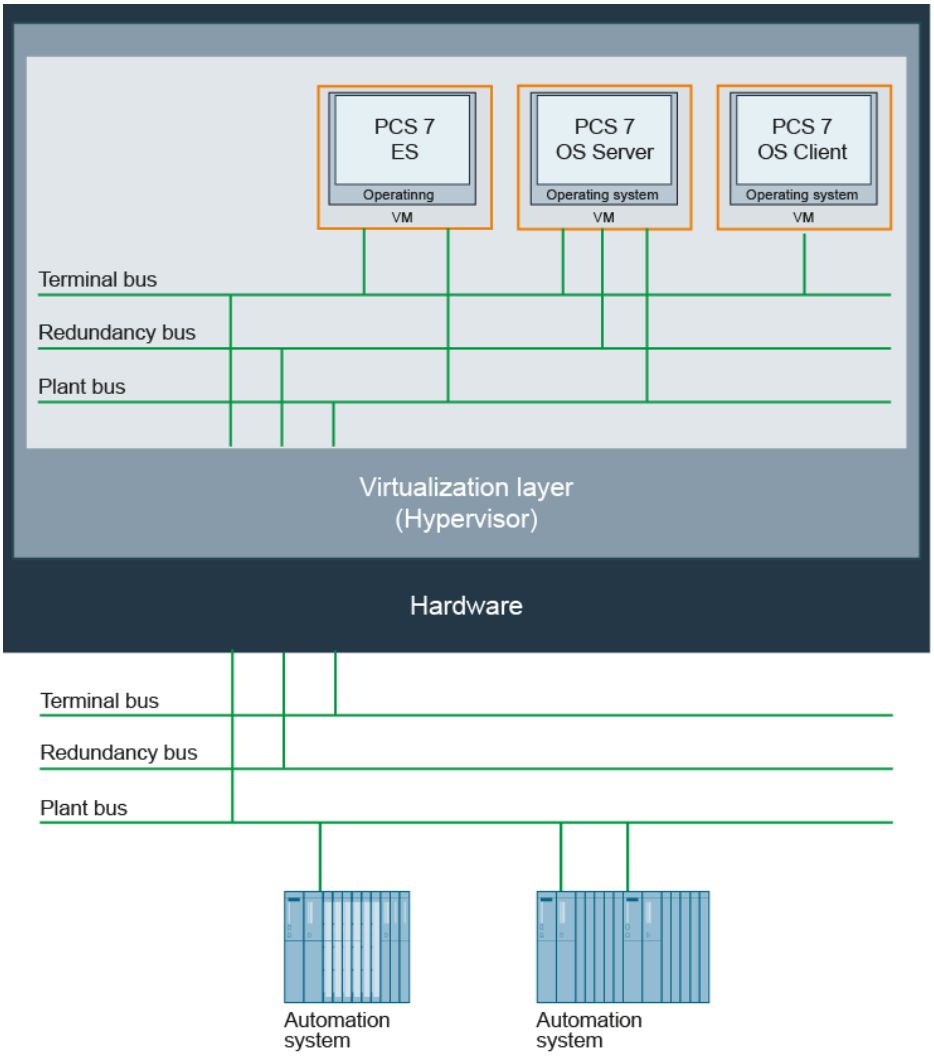
© Siemens 2025

4.1.5. Network

Principle

The following figure illustrates the communication principle of a virtualization system:

- The internal communication between ES, OS Server and OS Client.
- The outward communication of ES, OS Server and OS Client, e.g. to the AS via the physical network adapters of the host.



NOTE The type of VMs possible can vary depending on the type of hypervisor used.

NOTE For the terminal bus, system bus and redundancy bus, it is recommended to use a dedicated network adapter on the host. To connect the ES to the fieldbus (PROFINET), a dedicated network adapter must be used for commissioning and diagnostics.

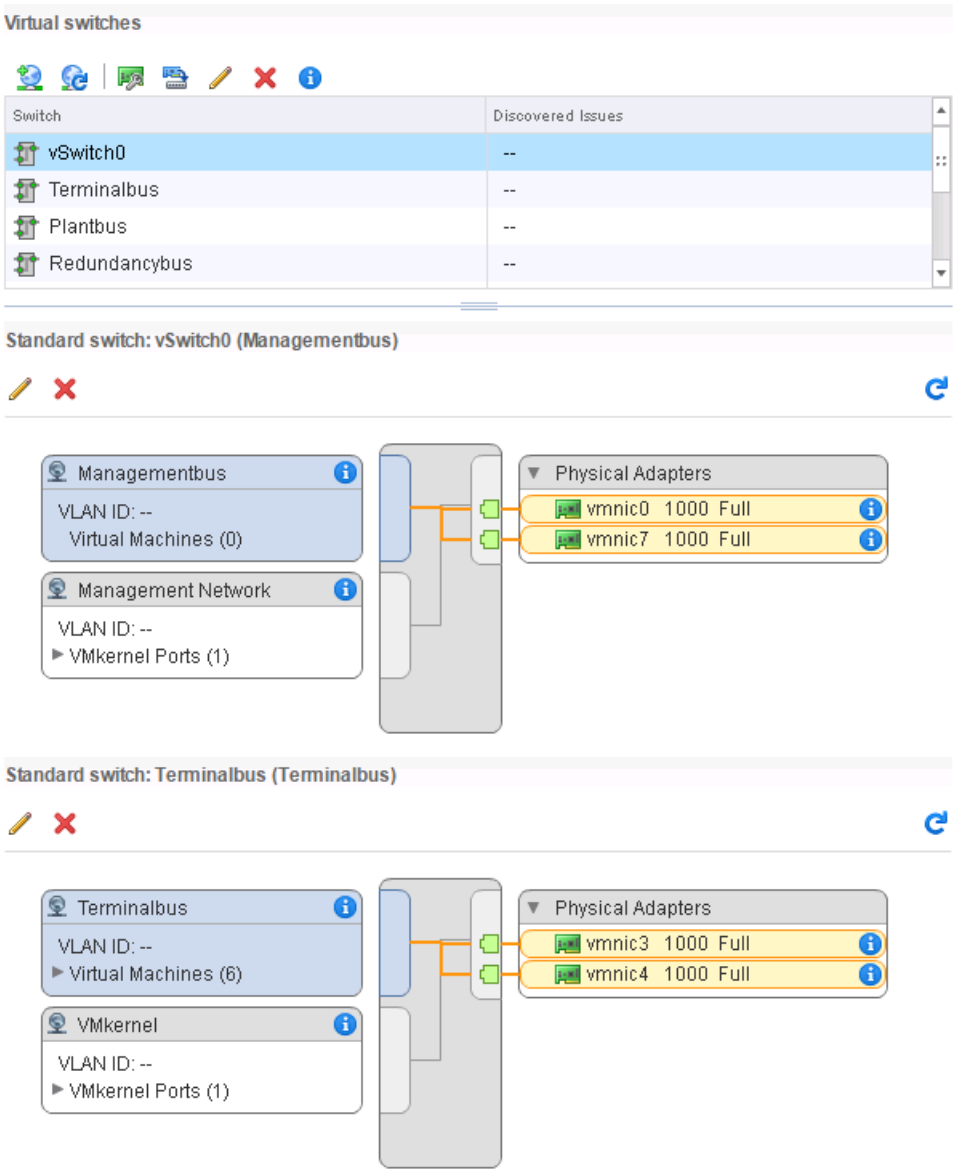
Further information is available in the entry "Service Bridge – Setup and Configuration".

© Siemens 2025

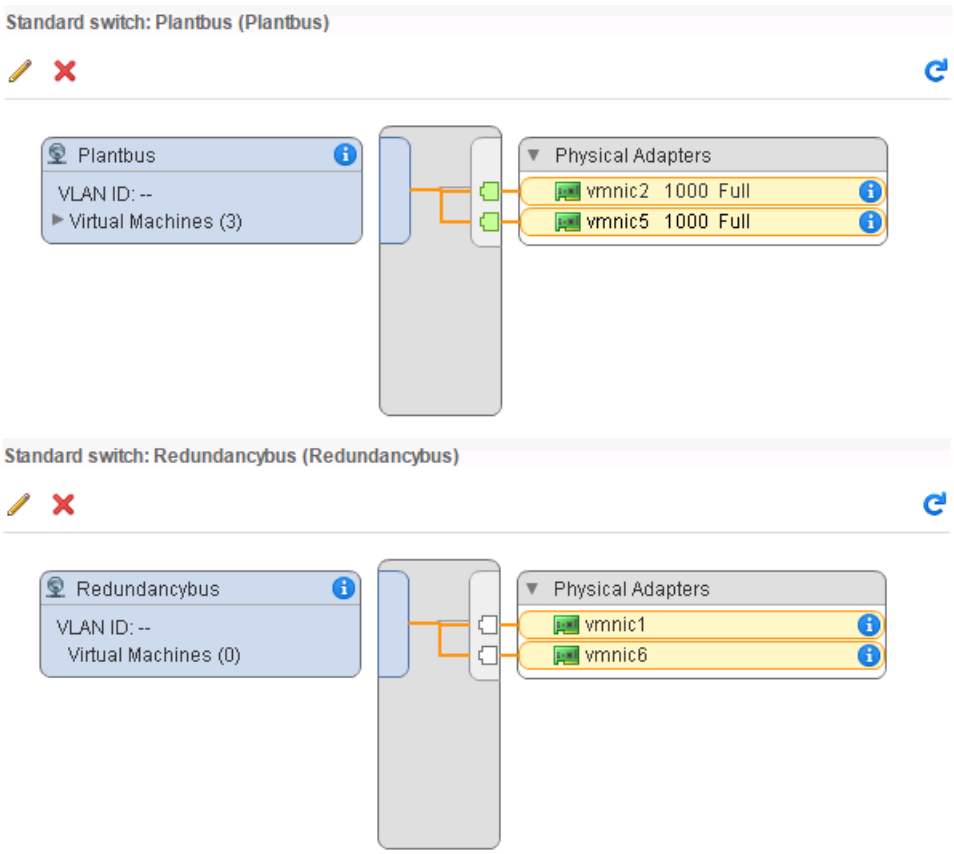
Network for VMware by Broadcom ESXi

The following figures show:

- The management network, the terminal bus, system bus and redundancy bus are connected with physical networks via dedicated physical network adapters (vmnic0 ... vmnic7, redundant).
- The virtual standard switch (vSS) is used.
- No VLANs are used.



© Siemens 2025



NOTE For reasons of performance and availability, it is generally recommended to use two physical network adapters for each network.

Network for Hyper-V

The network has already been set up in chapter "Configuring the Microsoft Hyper-V settings for the host".

© Siemens 2025

4.1.6. Time synchronization

NOTICE

Time synchronization

Except for the guest systems, in a virtual environment the host must also be synchronized. The host/hosts must have the same time source as the guest systems. This is important because when starting a VM, the time of the host is first set in the VM by default.

For the central time synchronization, the use of a system central clock is recommended, modules released for this purpose can be found in the document "SIMATIC Process Control System PCS 7 Released Modules (V10.0 SP1)".

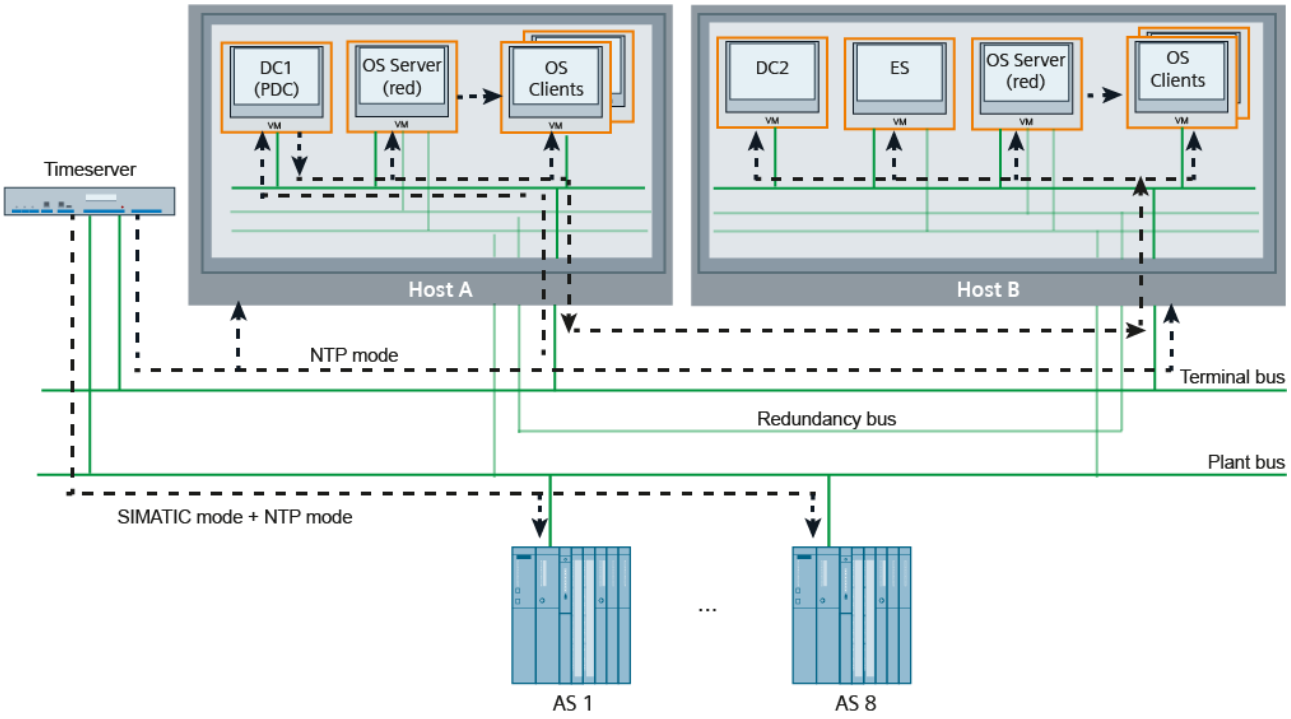
The following two scenarios are examples of the time synchronization of a virtual PCS 7 environment. For further information and options on time synchronization of a PCS 7 system, refer to the manual "SIMATIC Process control system PCS 7 Time Synchronization (V10.0)"

Time synchronization in a domain

The time synchronization in a domain proceeds as follows:

- Time synchronization on the terminal bus
  The domain controller (PDC emulator) and the hosts (ESXi Servers) are synchronized directly from the central plant clock via the NTP process.
  The domain controllers synchronize all domain members.
- Time synchronization on the plant bus
  The automation systems on the plant bus are synchronized via the central plant clock. The synchronization processes depend on the type of CPU or CP used and the network configuration.

The following figure illustrates an example of a virtual configuration for a network environment in a domain. This example is based on chapter 4.8.2 "Network environment within a domain" in the manual SIMATIC Process control system PCS 7 Time Synchronization (V10.0)"



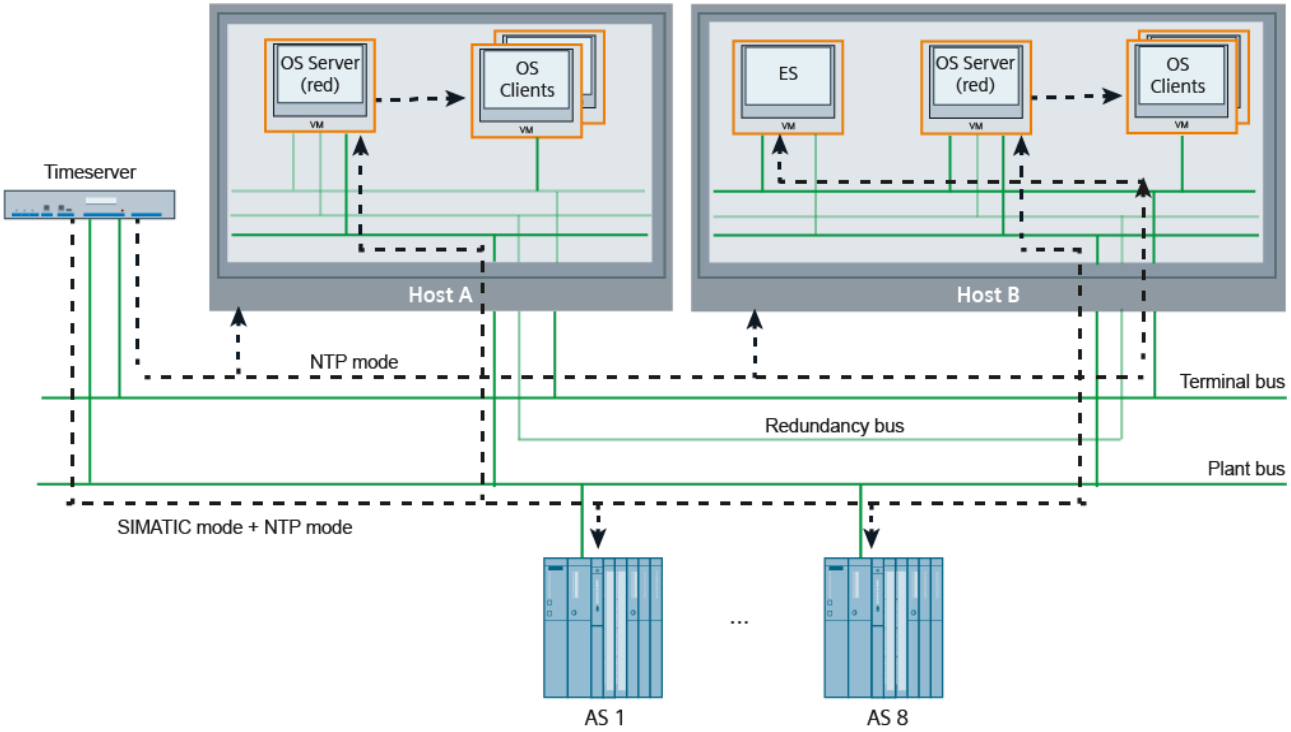
© Siemens 2025

Time synchronization in a workgroup

Time synchronization in a workgroup proceeds as follows:

- Time synchronization on the terminal bus
  The ES and the hosts (ESXi Servers) are synchronized by the central plant clock via the NTP process.
  The OS Clients receive the clock time from an OS Server, from which they have loaded the server data.
- Time synchronization on the plant bus
  The systems on the plant bus are synchronized via the central plant clock. The synchronization processes depend on the type of CPU or CP of the automation systems and the network configuration.

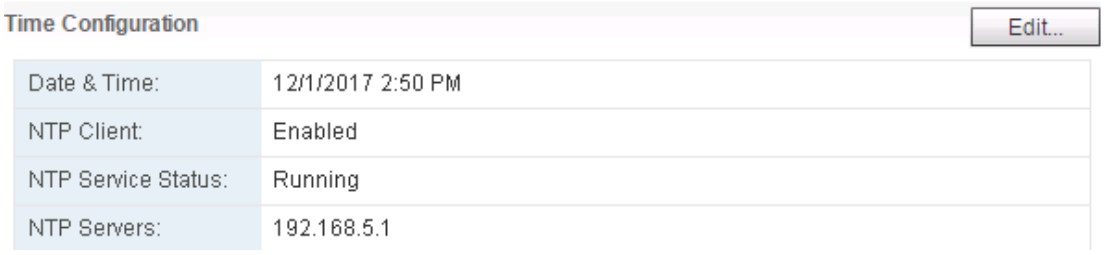
The following figure illustrates an example of a virtual configuration for a network environment in a workgroup. This example is based on chapter 4.8.3 "Network environment in a workgroup" in the manual
SIMATIC Process control system PCS 7 Time Synchronization (V10.0)"



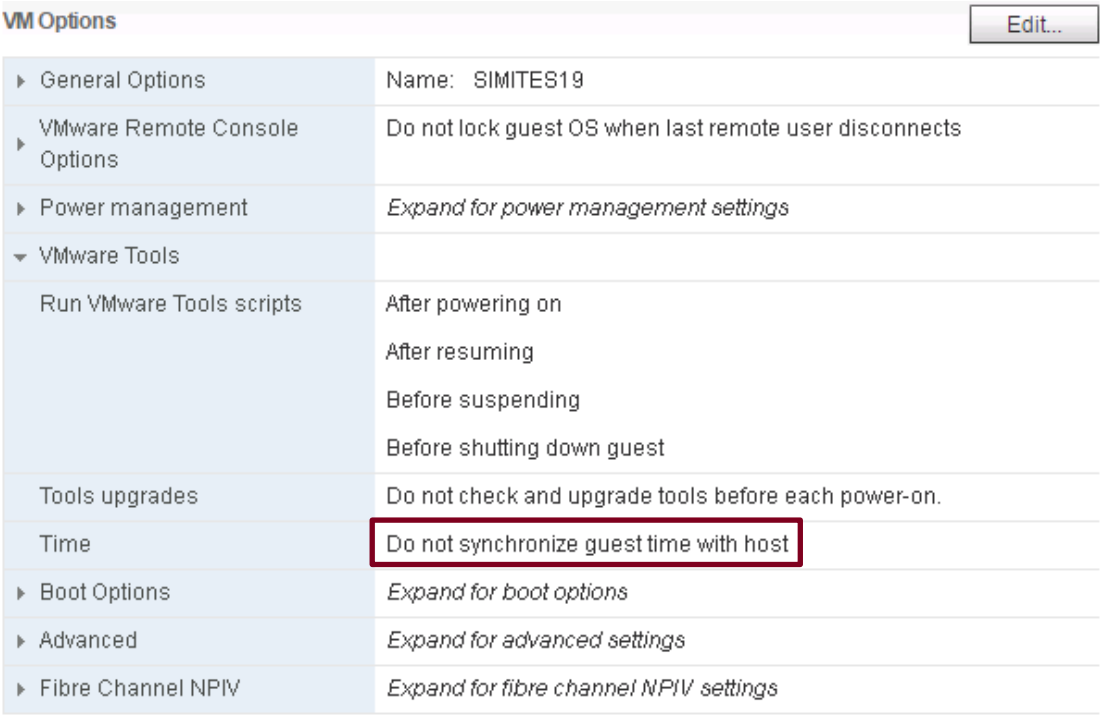
© Siemens 2025

Time synchronization for VMware by Broadcom ESXi

The following figure illustrates the configured time synchronization of an ESXi Server:



The following figure illustrates the configured time synchronization of a VM: The VM is not synchronized by the host.



NOTE To achieve a correct time synchronization, there should be no conflicts with other time synchronization methods. Therefore, the time synchronization of the VMs with the ESXi Server must be deactivated.

© Siemens 2025

4.2. Configuration of the guest systems

4.2.1. General information

Properties	Requirements
Virtual network modules	There are as many network adapters to be configured as if you were using real PCS 7 stations. A redundant OS Server would therefore have three virtual network adapters.
Disconnection of networks	It is recommended to virtually/physically disconnect the terminal bus, system bus and redundancy bus and to refrain from using any VLANs. The IP addresses of the terminal bus, system bus and redundancy bus must be located in different subnets.
Network adapters	All network adapters are assigned to the "Private" network profile via Group Policy within Windows.
CPU load	The CPU continuous load of the assigned logical CPU cores may not exceed the 70% - 80% range. **Note:** When archiving large amounts of data, a corresponding reserve is required (high IO load). This is when the load is between 70% and 80%.

The following table shows the **minimal VM configuration** based on the PCS 7 V10.0 SP1 Readme, chapter "4.3.1.1 Recommended PC hardware configuration".

The specified values for the minimum configuration must be increased depending on the system specification, e.g.:

- to improve performance
- when OS Client, Batch Client and Route Control Client are operated on one VM
- when clients are operated with dual monitor

	Hard disk	Partition size	Virt. cores	RAM [GB]
OS Client, Batch Client, Route Control Client	>=160 GB HDD/SSD	C:\ 100 to 128GB	2	>= 8
ES	>=200 GB HDD/SSD	C:\ 100 to 128GB	4	>= 16
OS Server OS Single Station PCS 7 Web Server OS Client and BATCH Client on a PC BATCH Server BATCH Single Station Route Control Server Route Control single station	>=200 GB HDD/SSD	C:\ 100 to 128GB	2	>= 16

© Siemens 2025

The virtual hard disks can be set up in Thick as well as Thin Provisioning format.

- In the case of Thick Provisioning, the entire hard disk capacity is made available from the start. This prevents more storage from being requested than actually exists (over-provisioning).
- For Thin Provisioning, only the storage actually needed is allocated when necessary. This enables more efficient use of storage space, but there is the risk that more storage will be requested than is physically present (over-provisioning). Monitoring of storage space would then be absolutely necessary. It is recommended to enable the alarms "Storage space use on hard disk" and "No free space in data storage".

You can find the accepted operating systems in the PCS 7 V10.0 SP1 Readme, chapter "4.4.1.1 Requirements". Only use 64-bit operating systems.

NOTE For determination of suitable hardware for Process Historian, the tool "PH-HWAdvisor" must be used.

4.2.2. Special features for VMware by Broadcom ESXi

Properties	Requirements
VMware Tools	The "VMware Tools" must be installed within the virtual machines. This results in improved performance and maintainability of the VMs.
Operating states	Suspending/resuming the VMs as well as VMware options, such as vMotion, HA and FT are not supported. The VMs must be treated as purely hardware-based OS stations.

NOTICE **Adapter type of the virtual network adapters**

The use of "vmxnet3" is mandatory as the adapter type

The adapter type "vmxnet3" can only be used after installing the VMware Tools in the VM.

NOTE The "resource allocation" of the VMs can be left on default settings.

Remove any unneeded hardware, e.g.:

- HD audio
- Floppy disk drive

© Siemens 2025

4.2.3. Create and commission the VMs for Microsoft Hyper-V

Possible combinations of VMs:

		1st virtual machine												
		OS Server [1]	OS Single Station [1]	OS Web Server	OS Client	BATCH Server [2] [3]	BATCH Single Station [2] [3]	SNMC	DC / DNS / DHCP	WSUS	ES	Central ES	ES/OS Single	OpenPCS 7
2nd virtual machine	OS Server [1]	-	-	X	X	X	X	X	X	-	X	-	-	X
	OS Single Station [1]	-	-	X	X	X	X	X	X	-	X-	-	-	X
	OS Web Server	X	X	X	X	X	X	X	X	-	X	X	X	X
	OS Client	X	X	X	X	X	X	X	X	X	X	X	X	X
	BATCH Server [2] [3]	X	X	X	X	-	X	X	X	X	X	X	X	X
	BATCH Single Server [2] [3]	X	X	X	X	X	-	X	X	X	X	X	X	X
	BATCH Client [3]	X	X	X	X	X	X	X	X	X	X	X	X	X
	SMMC	X	X	X	X	X	X	-	X	X	X	X	X	X
	DC / DNS / DHCP	X	X	X	X	X	X	X	-	X	X	X	X	X
	WSUS	-	-	-	X	X	X	X	X	-	X	X	X	X
	ES	X	X	X	X	X	X	X	X	X	X	X	X	X
	Central ES	-	-	X	X	X	X	X	X	X	X	-	X	X
	ES/OS Single	-	-	X	X	X	X	X	X	X	X	X	-	X
	OpenPCS 7	X	X	X	X	X	X	X	X	X	X	X	X	-
3.- 4 Virtual machines [3]	OS Web Server	X	X	X	X	X	X	X	X	-	X	X	X	X
	OS Client	X	X	X	X	X	X	X	X	X	X	X	X	X
	BATCH Client [3]	X	X	X	X	X	X	X	X	X	X	X	X	X
	OpenPCS 7	X	X	X	X	X	X	X	X	X	X	X	X	-
	DC / DNS / DHCP	X	X	X	X	X	X	X	X	X	X	X	X	X

[1] maximum of 6,500 process objects

[2] No CDV archiving - only PH archiving / Distributed system (OS server on own station) / maximum 50 Units

[3] Windows Server 2019: max. count VM's: 2
These station types are not released with Windows Server 2019.

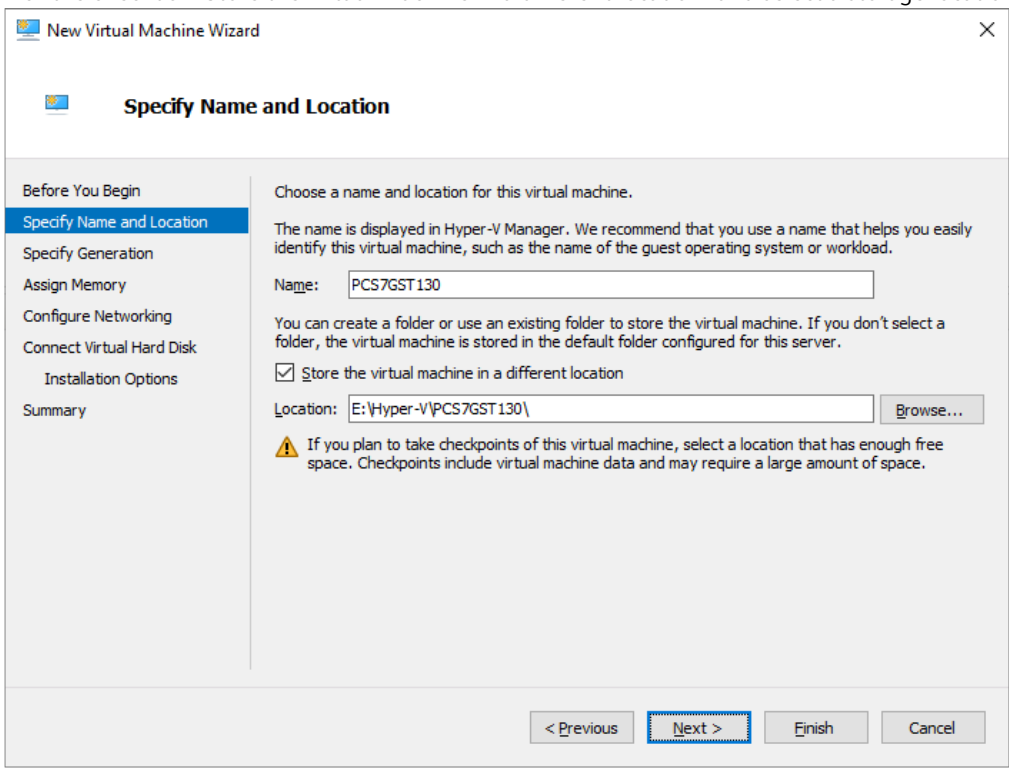
Windows Server 2022 - depending on Hardware:
547J: max. count VM's: 2
647E/847E: 6 Core CPU: max. count VM's: 2
647E/847E: 8 Core CPU: max. count VM's: 4

© Siemens 2025

NOTE All VMs, except those for which a suitable system image with PCS 7 is available, are deployed with the VHDX that was created from the operating system image "Windows (only)".

The following steps illustrate an example of how to create a VM:

1. In the Hyper-V Manager, open "New -> Virtual Machine..." from the context menu or with the actions of the virtualization host.
2. In the "Specify Name and Location" dialog, select a name for the VM that will be displayed in the Hyper-V Manager. This name does not need to be identical with the actual computer name.
   Tick the checkbox "Store the virtual machine in a different location" and select a storage location.

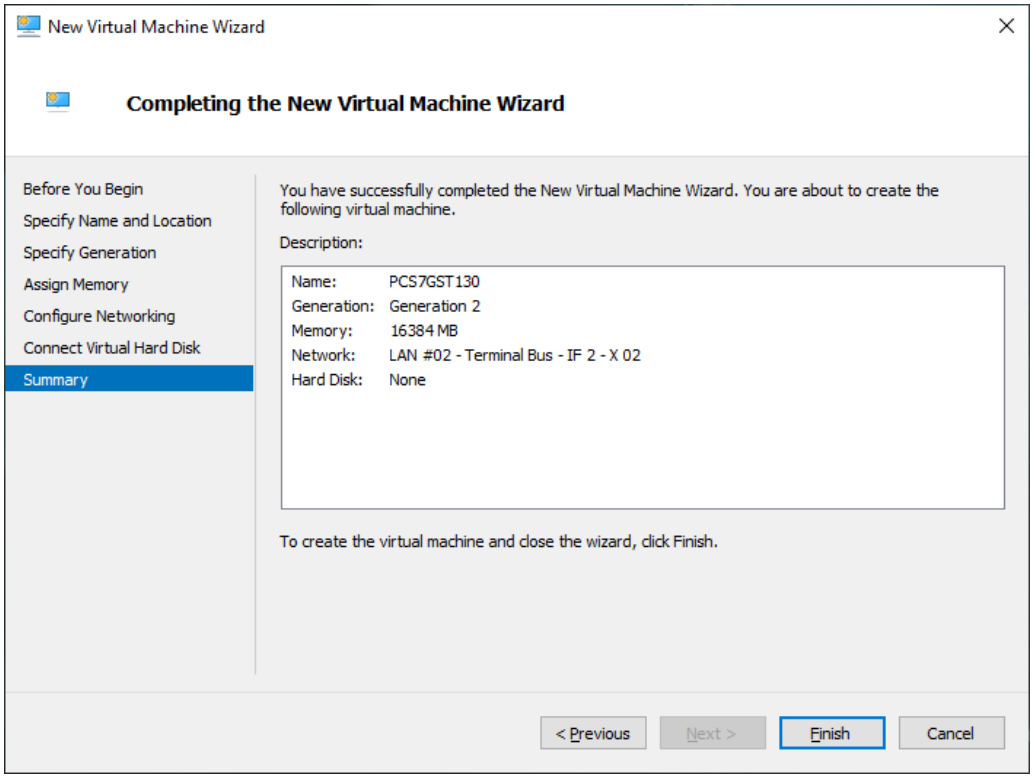


3. Make the following settings:

Name	Value	Note
Specify Generation	Generation 2	UEFI-based firmware
Assign Memory	Min. 8 GB or 16 GB	Depends on VM
Configure Networking	LAN #02 Terminal bus	Network adapter for the terminal bus
Connect Virtual Hard Disk	Attach a virtual hard disk later	The virtual hard disk will be added later.

NOTE Other network adapters required depending on the configuration must be added and installed one after the other in a later step.

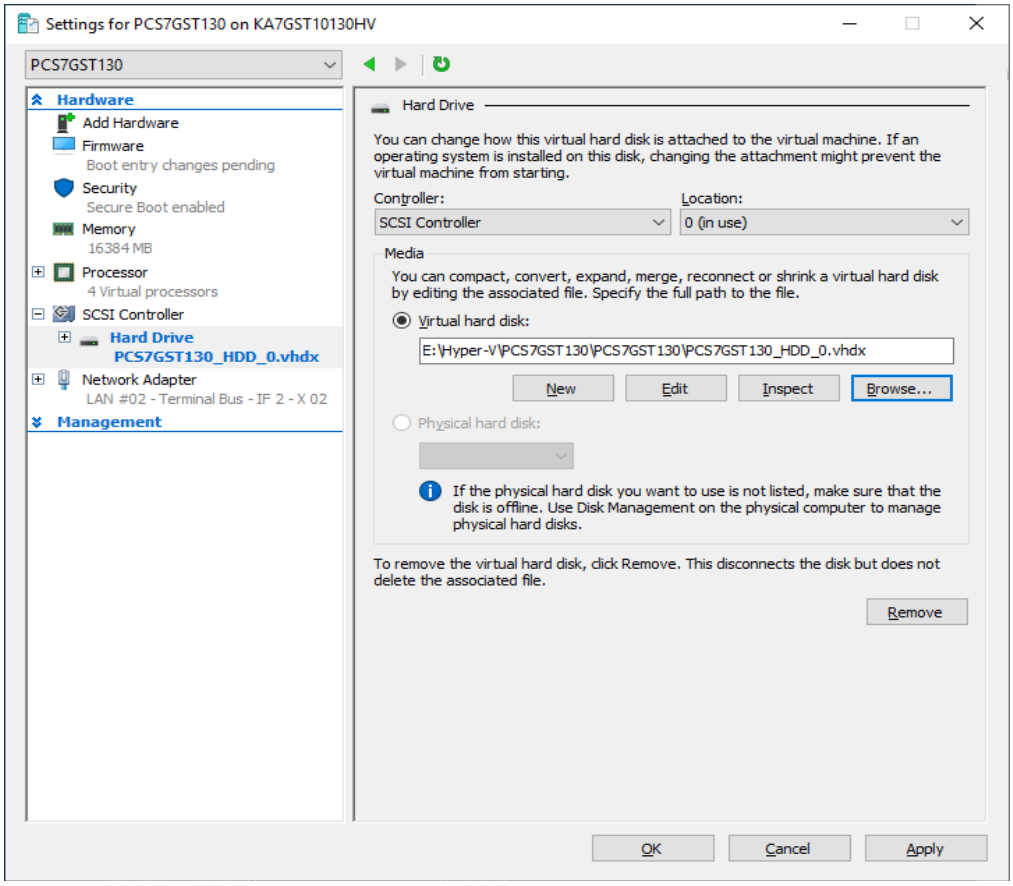
© Siemens 2025



4. Click "Finish".
   The VM has been created without virtual hard disks. These will be configured in the next steps.
5. Copy the virtual hard disk (VHDX file) created in chapter 4.1.4.3 to the folder of the VM.
6. In the Hyper-V Manager, select the VM and open the properties of the VM by right-clicking "Settings".
7. Check the settings that were already made.

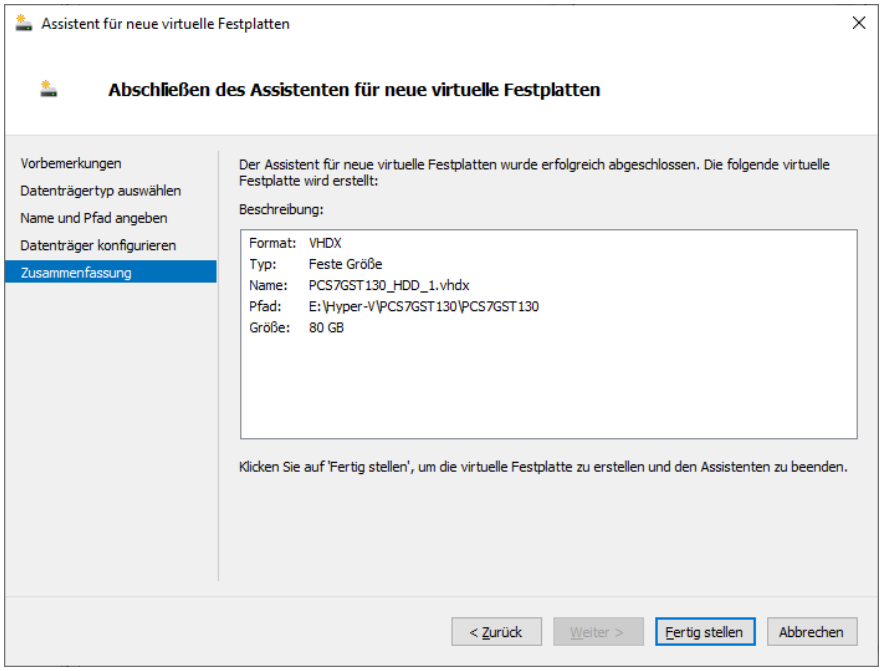
© Siemens 2025

8. Integrate the existing virtual hard disk (VHDX file).

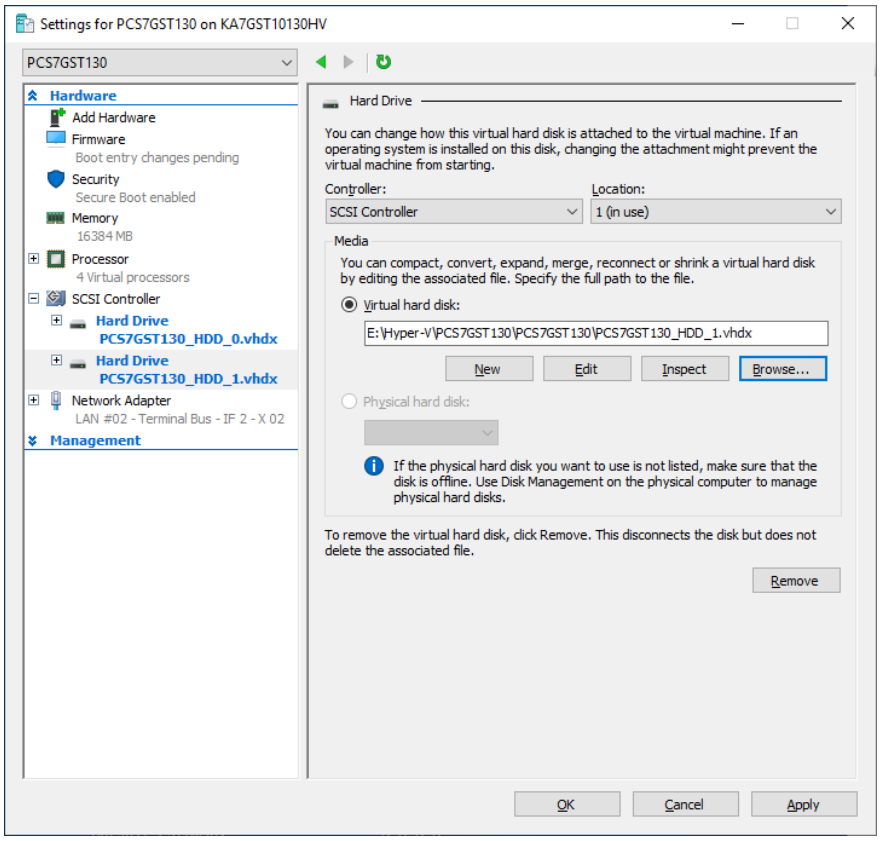


9. Create a second, new virtual hard disk in VHDX format and fixed size for data and integrate it.

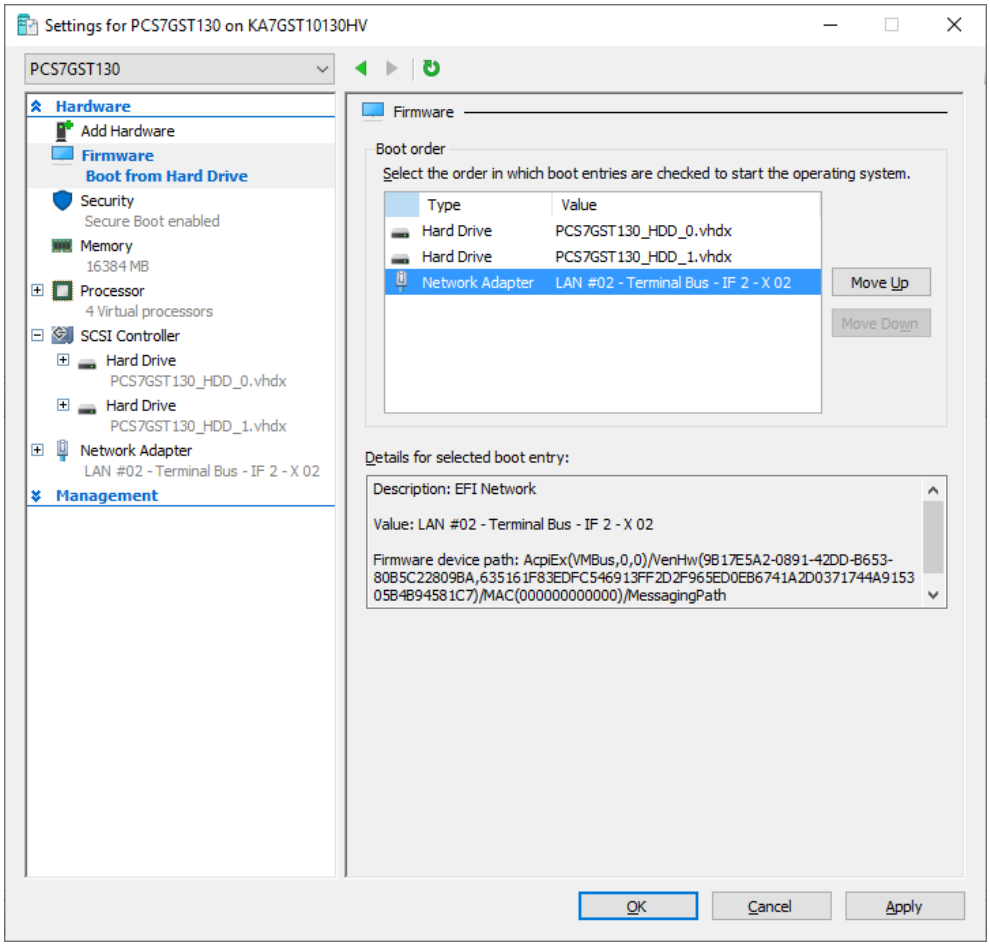
   Select the size of the second hard disk based on the available storage space and the expected future storage requirements.



© Siemens 2025



10. Modify the boot order so that the machine boots from the system hard disk.



© Siemens 2025

11. Select the services that Hyper-V should provide for the VM. Make the following management settings:

Name		Value	Description
Integration Services	Operating system shutdown	enabled	Shuts down the operating system
	Time synchronization	disabled	Time synchronization
	Data exchange	enabled	Data exchange
	Heartbeat	enabled	Clock
	Backup	enabled	Backup (volume shadow copy)
	Guest services	enabled	Guest services
Checkpoints	Enable checkpoints	disabled	No test points
Automatic Start Action	Always start this virtual machine automatically	selected	Always start automatically
	Startup delay	e.g. 30s / 90s	This setting should be adjusted such that the domain controller runs before the OS Server.
Automatic Stop Action	Shut down the guest operating system	selected	Shuts down the guest operating system

12. Click OK to close the dialog.
    The virtual hard disks have been added to the VM created earlier.
13. Start the VM to run through the restore process.
14. During the restore process, the following prompt will appear:
    "Do you want to use the SIMATIC Management Agent?"
    Click "Yes" to confirm this prompt for PCS 7 stations when using a SIMATIC Management Console.
15. After completing the restore process, perform the basic configuration, for instance the IP address, inclusion in a domain, etc. The second hard disk must be set to "online" in Computer Management.

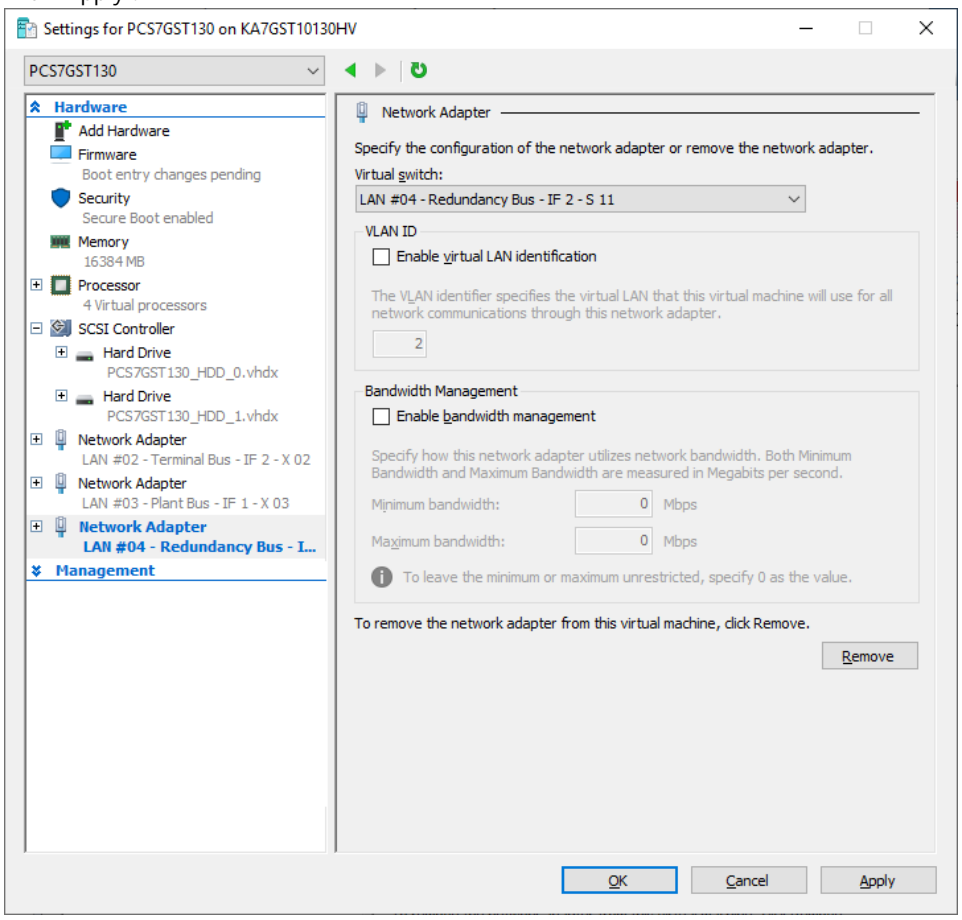
Result:

The basic configuration of the VM is now complete.

NOTE The following steps are only relevant for VMs that have a connection to the plant bus and/or redundancy bus, for example OS Servers. For further commissioning of other stations, refer to the corresponding documentation.

© Siemens 2025

16. If the VM is running, use the VM's properties to add the network adapter for the plant bus and apply the change with "Apply".
17. If the VM is running, use the VM's properties to add the network adapter for the redundancy bus and apply the change with "Apply".



18. Additional configuration steps inside the VM are performed in the same way as with a "normal" PCS 7 station, for example assigning IP addresses, removing certain protocols for plant bus and redundancy bus, configuration of the SIMATIC Shell, and so on.
19. If the OS Server image was used as the basis for the VM, uninstall the diagnostic monitor.

Result:

The expansion and basic configuration of the VM is now complete.

© Siemens 2025

4.2.4. Configuration of the network adapters

NOTICE

Interrupted process communication

- In the Windows "Network and Sharing Center", you shouldn't have any unused network adapters. Unused network adapters must be deactivated or removed from the virtual machine configuration.
- No network adapter may be assigned to the public network profile.

NOTE

The following Group Policy helps you ensure that no network adapter is assigned to the "Public network" network category.

Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Network Manager Policies > Non-identified Networks: Set the location type from "Not configured" to "Private". See SIMATIC PCS 7 PC-Configuration V10.0 SP1 , chapter 6.7.5 "How to set the communication module for connecting to the terminal bus".

NOTE

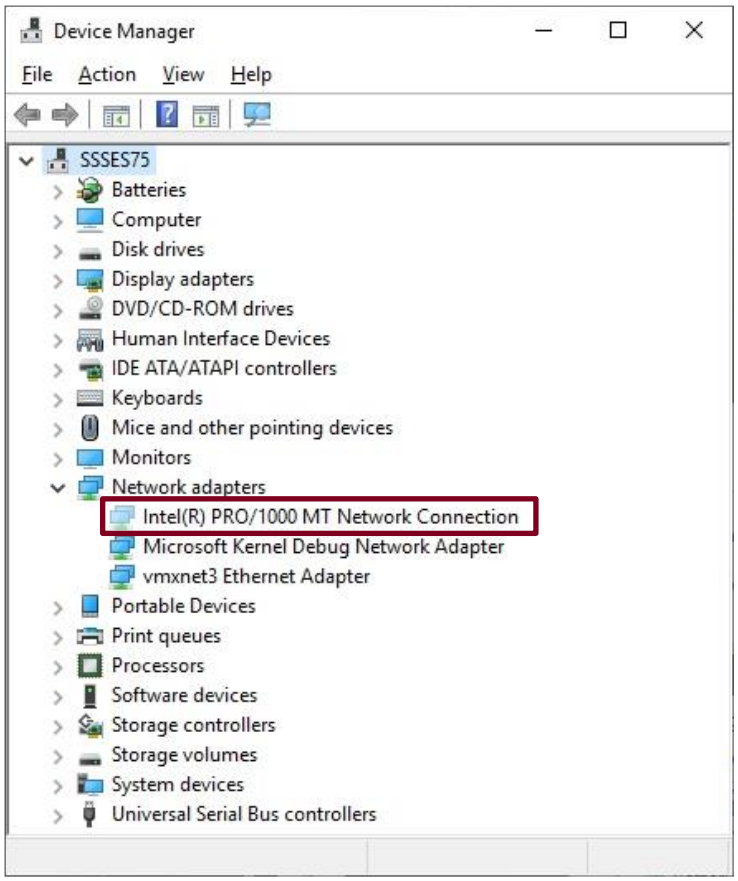
First uninstall all unused network adapters from the Windows Device Manager. Otherwise, residual data will remain in Windows in the VM's properties after the network adapters are deleted. These residual data must be made visible in the Device Manager before they can be removed. If these residual data are not removed, the name of the network adapter you removed cannot be used again.

© Siemens 2025

Procedure to uninstall "residual data":

To carry out the following steps, you must be logged in as an administrator. Before making changes to a registry key or subkey, you should export the key or subkey or generate a backup copy of it. You can save the backup copy wherever you want, for instance, in a folder on the hard disk. If you want to undo changes, you can import the backup copy.

1. Open the Device Manager and enable "Show hidden devices" in the View menu.
2. Uninstall the grayed-out network adapters via the context menu without deleting the driver software.



Perform the following steps if no grayed-out devices appear:

1. Open the Registry Editor. To do this, click the Windows "Start" button and type "regedit" in the search field, then press the Enter key. Enter the password or confirm the dialog if prompted to enter an administrator password or give a confirmation.
2. Set the following registry keys
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment]
   "devmgr_show_nonpresent_devices"="1"
   "devmgr_show_details"="1"

© Siemens 2025

Checking the configuration

Check whether the following requirements have been fulfilled:

- There are no unused network adapters.
- No network adapter is in the public network.
- ESXi: The network adapters of the VM have been assigned the type "vmxnet3".
- Unneeded network protocols have been removed.

NOTE You can find additional information on this topic in the chapter "Communications module drivers" of the SIMATIC PCS 7 - PC Configuration V10.0 SP1 manual.

Type	Protocol name	Default [1]	Terminal bus	Plant bus	Redundancy bus
Windows	Client for Microsoft Networks	enabled		disabled	
	File and printer sharing for Microsoft Networks	enabled		disabled	
	QoS Packet Scheduler	enabled			
	Internet Protocol Version 4 (TCP/IPv4)	enabled			
	Microsoft Network Adapter Multiplexor Protocol	disabled			
	Microsoft LLDP Protocol Driver	enabled			
	Internet Protocol Version 6 (TCP/IPv6)	enabled			
	Link-Layer Topology Discovery Responder	enabled			
	ISO protocol	enabled			
	Energy saving options	disabled			
	Link-Layer Topology Discovery Mapper I/O Driver	enabled			
SIMATIC	PROFINET IO protocol (DCP/LLDP)	enabled	disabled	enabled	disabled
	SIMATIC Industrial Ethernet (ISO)	enabled	disabled	enabled	disabled
	PROFINET IO RT Protocol V2.3	enabled	disabled	enabled	disabled

[1] Default: After installing Windows or SIMATIC NET

© Siemens 2025

4.2.5. Licensing

With regard to licensing, installation in a virtual machine does not differ from installation on real hardware (SIMATIC PCS 7 Industrial Workstation). The operating system and each SIMATIC software installation on a virtual machine, e.g. SIMATIC PCS 7, must be licensed.

Since the communication on the plant bus for SIMATIC PCS 7 takes place in a virtual environment over BCE, corresponding licenses must be used for SIMATIC NET (see chapter 4.5.5).

NOTE When operating the regional SIMATIC PCS 7 OS software ASIA, a USB hardlock is required for the license check. You can find additional information on this in chapter "7.2 Managed USB HUB" of the entry: WinCC-Virtualisierung.

4.3. Configuration examples for ESXi

4.3.1. Configuration of the VMs

ES, OS Server, Batch Server/RC Server

Hardware	ES	OS Server	Batch Server / RC Server
Installiertes Betriebssystem	Windows 10 Enterprise LTSC 2021	Windows Server 2022	
RAM [GB]	≥ 16		
Virt. cores	4		
Video memory	36 MB		
Hard disk 1: System [1] [GB]	100	100	
Hard disk 2: Daten [1] [GB]	100	100	
Hard disk 3: BatchData [2] [GB]	None		≥50
Network adapter 1 (vmxnet3)	Terminal bus		
Network adapter 2 (vmxnet3)	Plant bus		
Network adapter 3 (vmxnet3)	Not available	Not available	

1) The storage space for the hard disk must be adapted to the project requirements. The sum of the size corresponds to the minimum recommended size of the hard disk specified in the

2) SIMATIC PCS 7 Readme V10.0 SP1 (chapter 4.3.1.1).

3) The batch database must be on a separate storage media (if possible, a dedicated SSD hard disk/SSD RAID array).

© Siemens 2025

OS Client / BATCH Client / RC Client, PCS 7 Web Server / OpenPCS 7

Hardware	OS Client /Batch Client / RC Client	OpenPCS 7	Datamonitor Server / PCS 7 Web Server
Installed operating system	Windows 10 Enterprise LTSC 2019		Windows Server 2019
RAM [GB]	≥ 8 [2]	≥ 16	
Virt. cores	2		
Video memory	36 MB [3]		
Hard disk 1: System [1] [GB]	100		
Hard disk 2: Data [1] [GB]	60		
Network adapter 1 (vmxnet3)	Terminal bus		

1) The storage space for the data partition must be adapted to the project requirements. The sum of the size corresponds to the minimum recommended size of the hard disk specified in the SIMATIC PCS 7 Readme V10.0 SP1 (chapter 4.3.1.1).

2) If OS Client, Batch Client and RC Client are running on one VM, at least 16 GB RAM and 4 vCores should be configured.

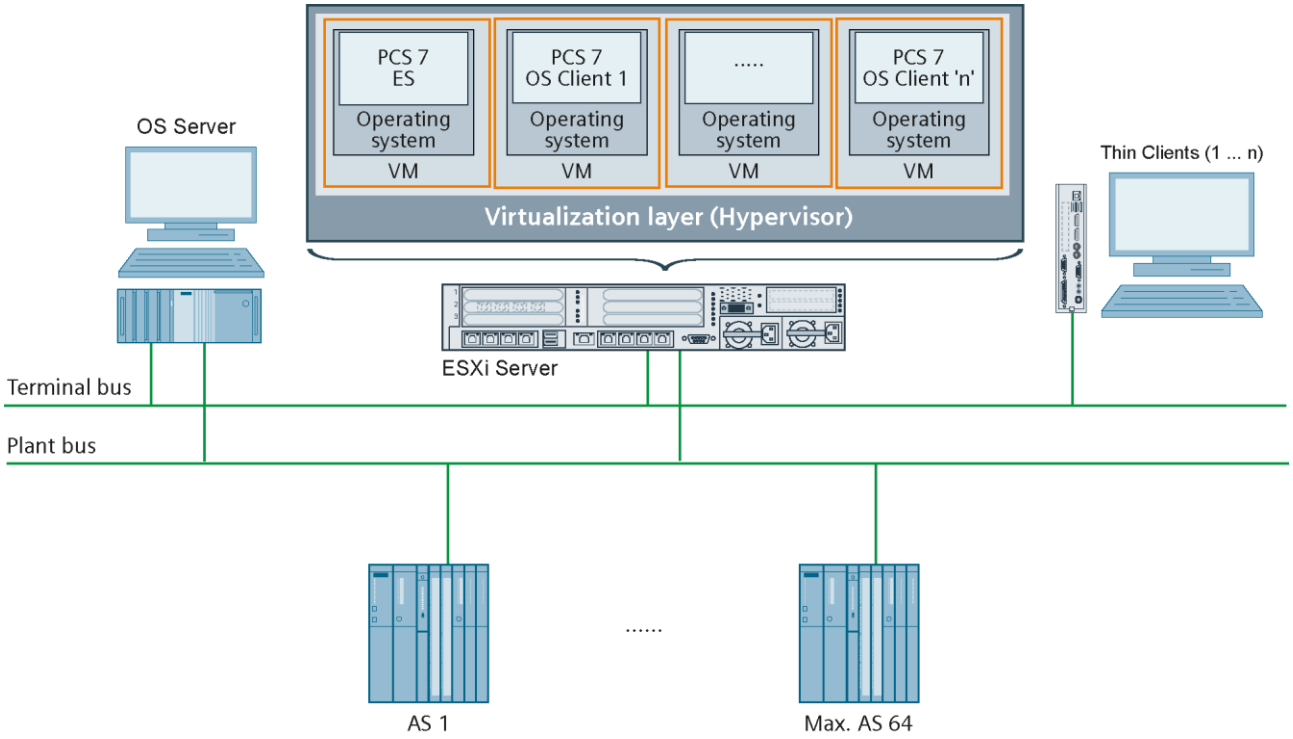
3) If you run Dual Monitoring with a virtual OS Client, please observe chapter 6.4.

© Siemens 2025

4.3.2. Configuration 1

- 1x virtual ES
- Virtual OS Clients (1...n)
- 1x hardware-based OS Server
- Thin Clients (1...n)
- Automation systems (AS 1...max. AS 64)

In this configuration, the communication to the AS occurs from a physical OS Server, i.e. via CP1623.

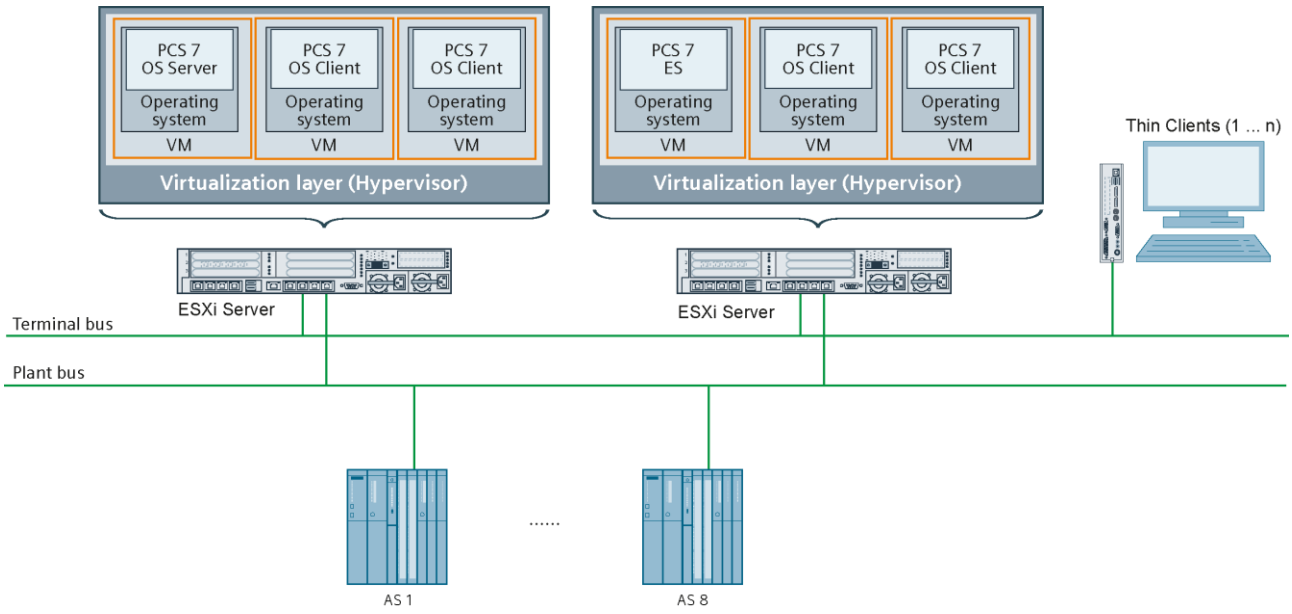


© Siemens 2025

4.3.3. Configuration 2

- 1x virtual ES
- 1x virtual OS server on ESXi Server 1
- 4x virtual OS Clients on ESXi Server 1 and 2
- Thin Clients (1...n)
- Automation systems (AS 1... AS 8)

The ES, OS Server and OS Clients were virtualized in this configuration. The communication to the AS passes over a standard network adapter, i.e. BCE. Since there is only one OS Server in this example, you do not need a redundancy bus.

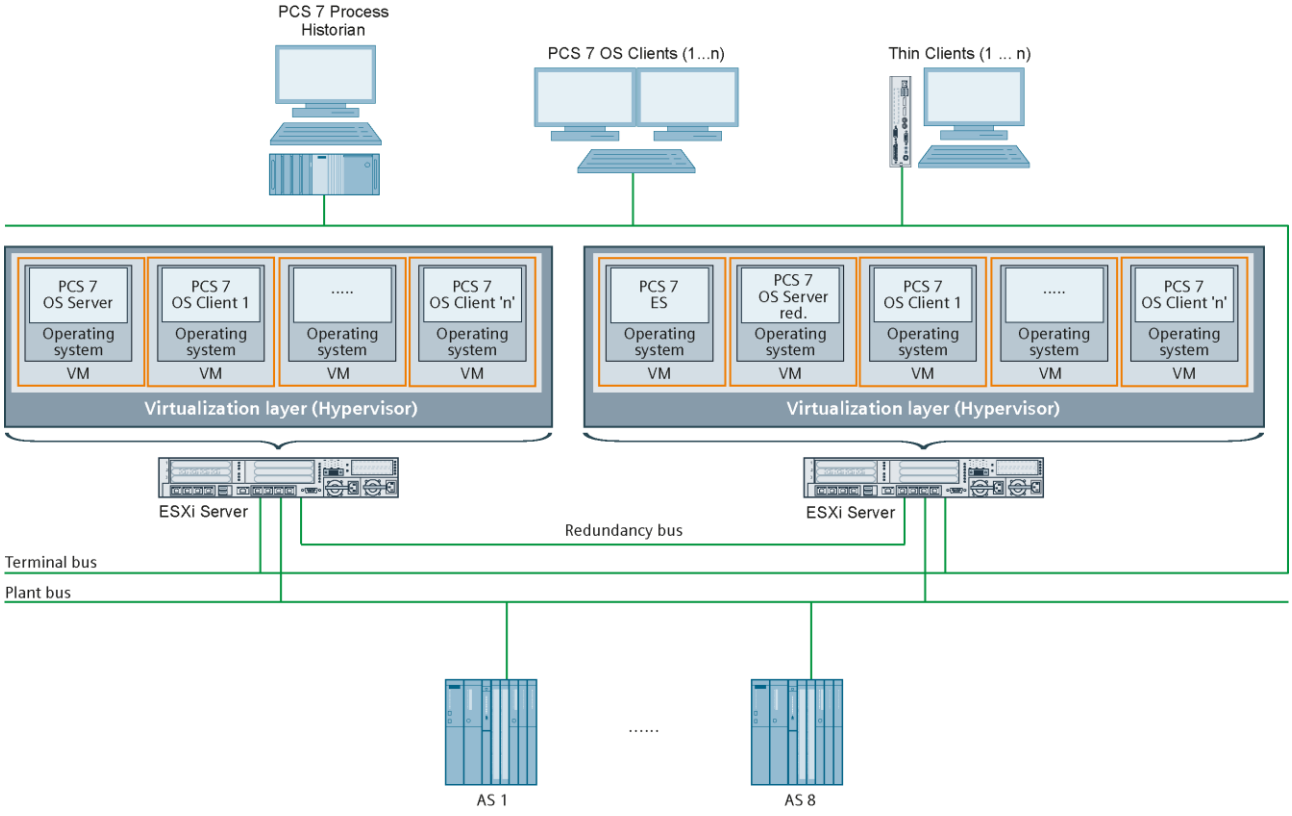


© Siemens 2025

4.3.4. Configuration 3

- 1x virtual ES
- 1x virtual redundant pair of OS Servers
- Virtual OS Clients (1...n) on ESXi Server 1 and 2
- Real Process Historian
- Real OS Client
- Thin Clients (1...n)
- Automation systems (AS 1... AS 8)

In contrast to configuration 2, a redundant pair of OS Servers is used in this example. A redundancy bus is therefore required.



© Siemens 2025

4.4. Remote access

Access to the VMs is made with a Thin Client or with a remote system via RDP, VNC, the "Remote Console" (VMRC) or "Web Console" or a VMware "vSphere Client (HTML5)".

General notes

The following points apply to all remote connections:

- All operator stations can be operated using just one open remote connection.
- In case of remote connection, the existing session must be taken over. This means that a user must be logged on to the operator station.
- Remote service and remote operation:
  For information regarding this topic, please refer to the SIMATIC PCS 7 Readme V10.0 SP1, chapter "4.4.14 Remote service and remote operation".
- An RDP connection may only be used for accessing OS Clients, BATCH Clients, Route Control Clients and clients without additional functions.
- Remote Desktop may only be used via "mstsc /console" or "mstsc /admin".
- When using an RDP connection, automatic logon must be configured in Windows inside of the VM, e.g. with "control userpasswords2" or "Autologon for Windows" (Windows Sysinternals). You should never write the login data to the registry, under any circumstance.
- In order to be able to access a VM with automatic logon in Windows via RDP, the following registry entry must not be present as of Windows Server 2012 R2 and Windows 10 (default setting):
  "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceAutoLogon"

RealVNC

It is not possible to transmit audio signals over a RealVNC connection.

The compatibility tool contains the approved version of RealVNC for PCS 7: http://www.siemens.com/kompatool

4.5. Communication

4.5.1. Name resolution

In a virtual environment, a management network is generally used for administering the virtual infrastructure. In this management network, it is recommended to use a DNS Server for the name resolution of the host.

NOTE If using a DNS/WINS Server, the required name resolution of the VMs for SIMATIC PCS 7 operation must take place via the terminal bus or by using the locally configured hosts and lmhosts files.

The name resolution must be assured via the IPv4 protocol.

4.5.2. VLANs

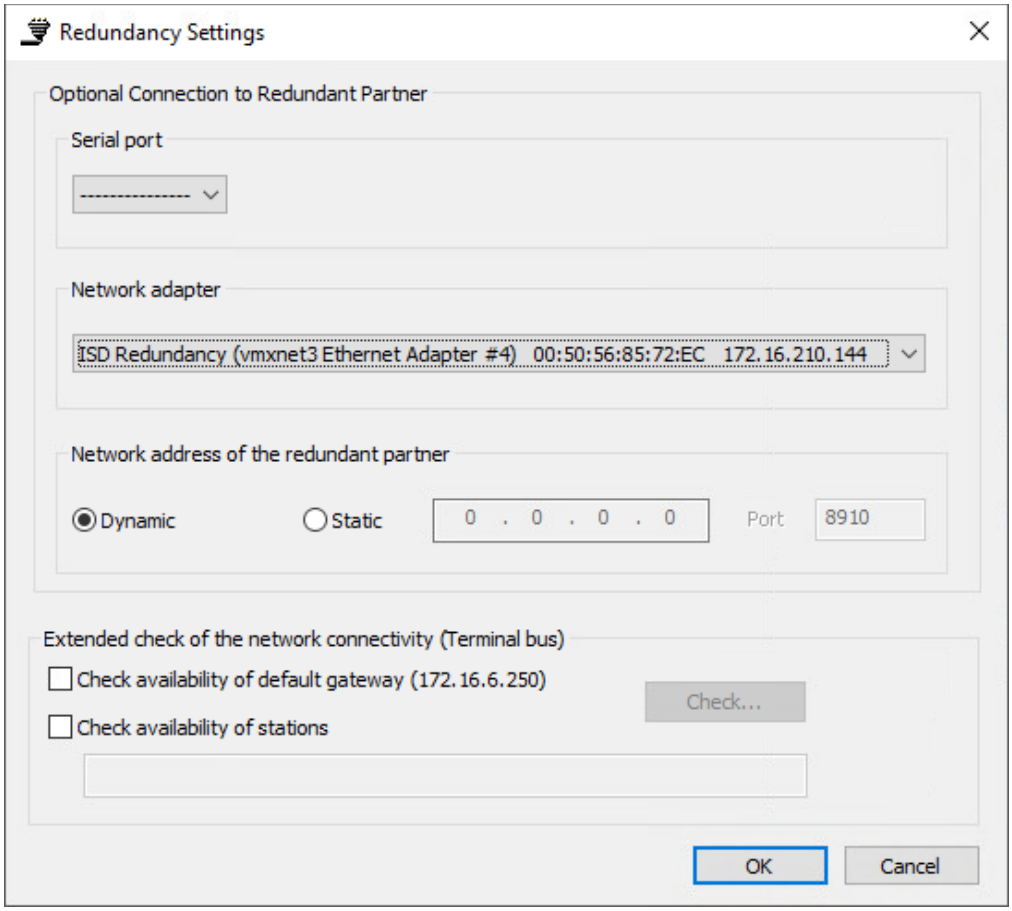
VLANs can be used in SIMATIC PCS 7. You can find additional information in the FAQ entry:
"How do you configure a Virtual Local Area Network (VLAN) in PCS 7?".

4.5.3. Redundancy connection between servers

Redundant OS Servers, Batch Servers or RC Servers for redundancy synchronization must be connected via Ethernet.

The figure below shows settings within the configuration of the SIMATIC Shell:

- Virtual network adapter selection for the redundancy bus in the redundancy settings
- Deactivation of the serial port



© Siemens 2025

4.5.4. Communication over multiple subnets (Terminal bus)

For more on this topic, see SIMATIC PCS 7 - PC Configuration V10.0 SP1, chapter 6.7.9 "How to access PC stations outside a subnet."

4.5.5. Communication with the AS

Principle

The plant bus communication with the automation system passes exclusively over the (virtual) standard network adapter (BCE connector).

NOTE The "passthrough mode" is not approved in SIMATIC PCS 7.

NOTE Communication to fault-tolerant automation systems
is approved for H CPUs from V6.0 onward.

NOTE Check the assemblies used to see if they are approved with PCS 7 V10.0:
SIMATIC Process Control System PCS 7 Released Modules (V10.0 SP1)

Then check the "CPU and CP compatibility", especially when communicating with high-availability automation systems: "Information about manuals on the topic of "CPU and CP Compatibility", Compatibility_List_S7400_IE_CPs_V17_d.pdf

Licenses for PCS 7 V10.0

Communication	License packages	Order number	Licenses
≤ 8 AS	SIMATIC PCS 7 BCE V10.0	6ES7650-1CD78-2YB5	BCE
	SIMATIC NET SOFTNET-IE S7 LEAN V18	6GK1704-1LW18-0AA0	SOFTNET-IE S7 Basic SOFTNET-IE S7 Lean
> 8 AS	SOFTNET-IE S7 V18	6GK1704-1CW18-0AA0	SOFTNET-IE S7 Basic SOFTNET-IE S7 Lean SOFTNET-IE S7 Power Pack
H stations	SOFTNET-IE S7 REDCONNECT V18	6GK1704-0HB18-0AA0	SOFTNET-IE S7 Basic SOFTNET-IE S7 Lean SOFTNET-IE S7 Power Pack SOFTNET-IE S7 Advanced Power Pack SOFTNET-IE S7 REDCONNECT SOFTNET-IE S7 REDCONNECT VM

- To upgrade "SOFTNET-IE REDCONNECT VM" V8.2 or higher, you can use the license "SIMATIC NET IE SOFTNET-S7 REDCONNECT VM UPGRADE" (order number: 6GK1704-0HB00-3AE0).
- An upgrade from "HARDNET-IE S7 REDCONNECT" to "SOFTNET-IE S7 REDCONNECT" is not possible.
- Only the license and not(!) the software, "SIMATIC NET SOFTNET-IE V18", can also be used for PCS 7 V8.2.

NOTE In SIMATIC NET, you always need only **one license package**, because the licenses for the subordinate license packages are also included with each function extension.

If communicating to 8 or fewer AS, the SIMATIC PCS 7 BCE V10.0 or SIMATIC NET SOFTNET-IE S7 LEAN V16 license package can be used.

Monitoring times/quantity structure

NOTICE

Interrupted process communication

For fault-tolerant S7 connections via TCP/IP, sufficient monitoring times must be configured.

With ESXi, the quantity structure (number of connections, number of alarms, number of data items) must not exceed 50% of the approved values.

For information on monitoring times and quantity structures, refer to the FAQ "What are the quantity frameworks and performance data of each of the SIMATIC NET products?"https://support.industry.siemens.com/cs/ww/en/view/15227599 under "Performance data and quantity frameworks for products of SIMATIC NET PC software V18".

Communication via subnets at the plant bus

If the OS communication to the AS on the plant bus takes place outside the network boundaries, the OS and ES must know the routes.

The following additional configuration steps are required:

1. In NetPro, enter a router as gateway on the AS for the CP443-1 or on the internal interface of the CPU.
2. On the OS Server and the ES, configure the routes to the AS for Windows, e.g. with the command "route add –p ...".

© Siemens 2025

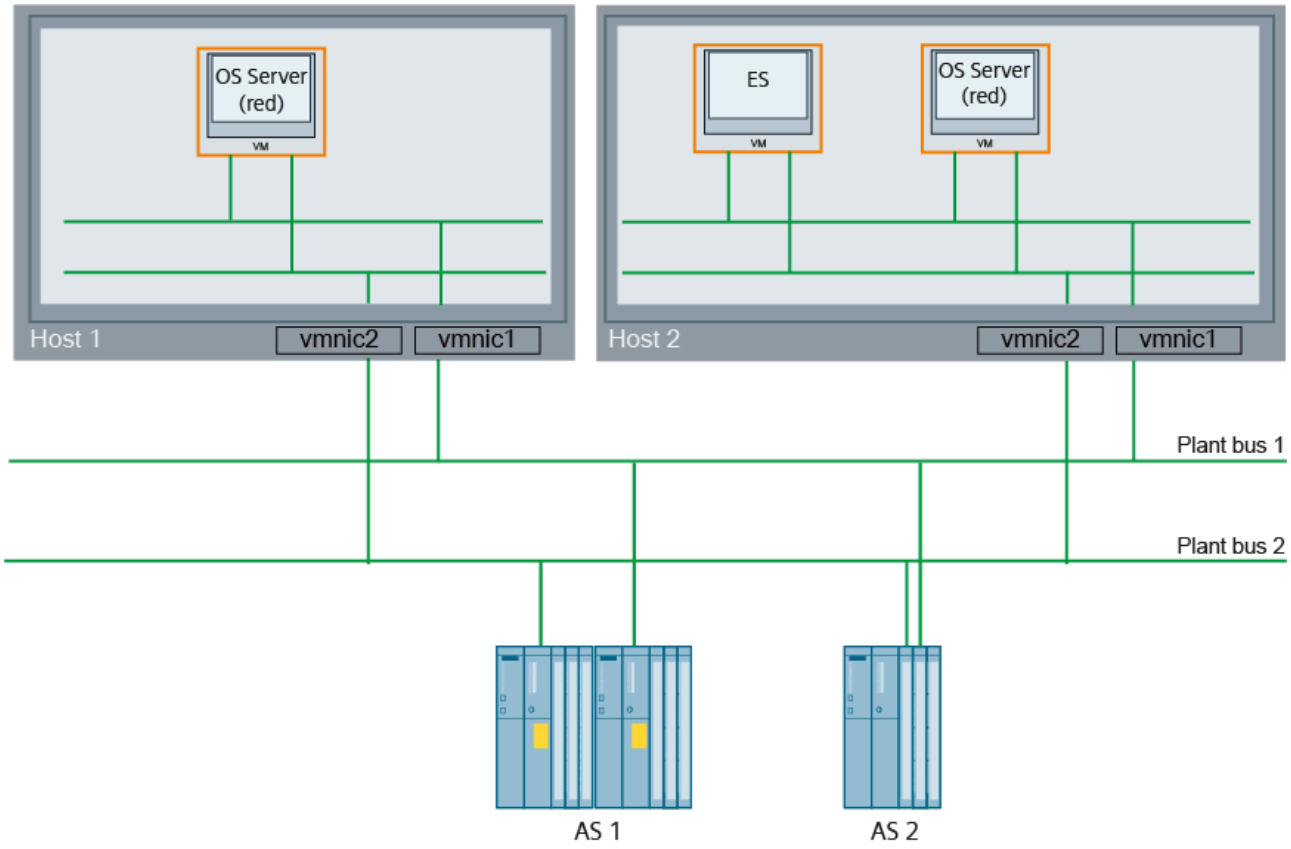
4.5.6. Redundant, fault-tolerant plant bus only with ESXi

NOTE Please also note the information in the manual SIMATIC Process Control System PCS 7 Fault-tolerant Process Control Systems (V10.0), chapter 5.3.4 "Solutions for the plant bus" in a real environment.

In this case, a redundant, high availability (fault-tolerant) plant bus is implemented from two physically separated networks. Each of these networks can be designed as a ring structure.

A redundant, fault-tolerant plant bus is possible with 2-way redundancy. The following points must be observed:

- The virtual OS Server is configured with two virtual network adapters for connection to the virtual plant bus 1 and virtual plant bus 2.
- The host has dedicated physical network adapters for connection to the real plant bus 1 and real plant bus 2.
- The ASs are configured with two CPs for connection to the real plant bus 1 and real plant bus 2.

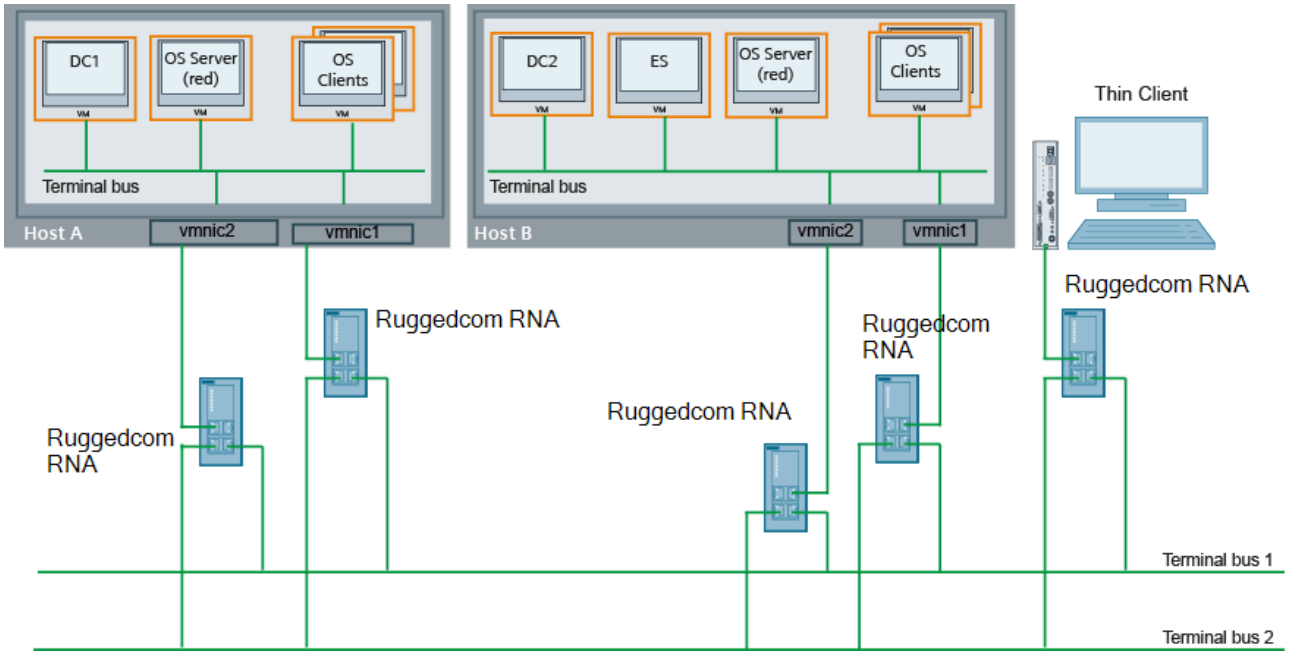


© Siemens 2025

4.5.7. Redundant terminal bus

4.5.7.1. Redundant terminal bus only for ESXi

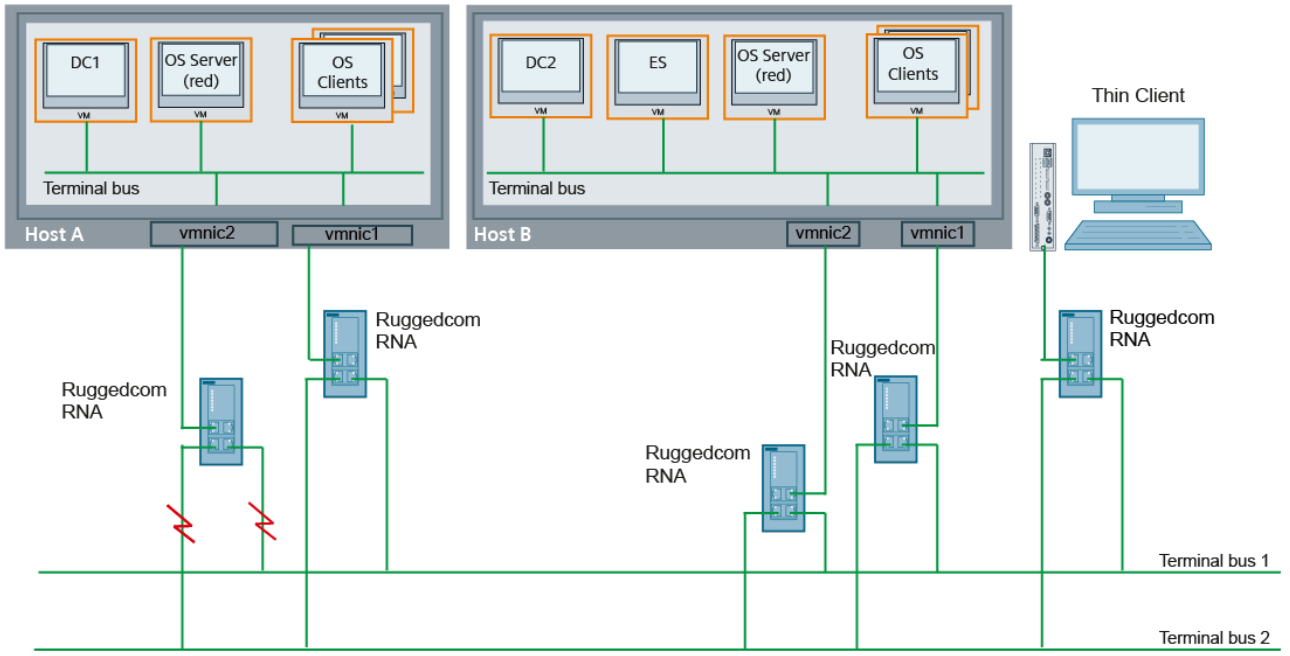
The following configuration is possible for running a redundant terminal bus:



NOTE

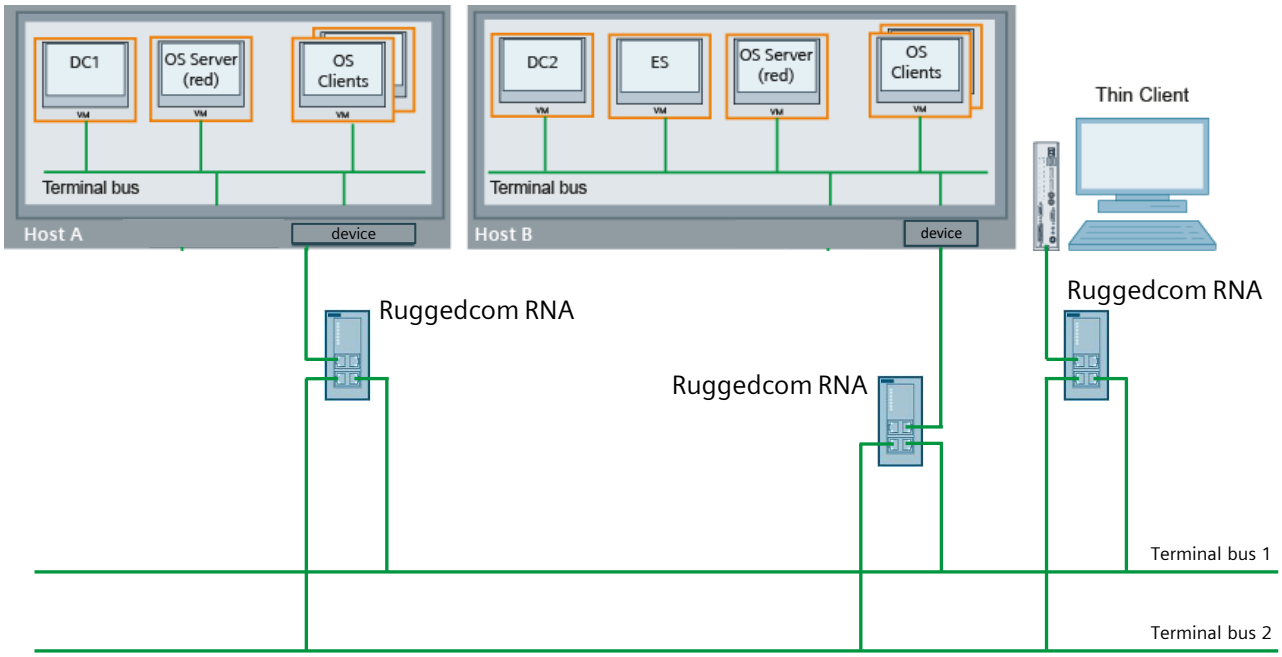
Assuming that the VMs' communication to Host A takes place through the ESXi network layer via vmnic2, these VMs will lose the connection to systems outside of Host A in the event of simultaneous/pending errors (see figure).

The ESXi network layer cannot recognize total loss of connection between RNA device (redbox) and the terminal buses, and therefore no changeover to the redundant RNA device via vmnic1 will occur there.



© Siemens 2025

4.5.7.2. Redundant terminal bus for Hyper-V



4.5.7.3. RNA devices

The following RNA devices, also known as redboxes, are recommended for use of the redundant terminal bus with ESXi:

- RSG909R 6GK6498-0RB00-1AN0
- RSG907R 6GK6490-7RB00-1AN0
- RST2228 with PRP module 6GK6297-8SB00-2AAO

For connecting the RSG909R and RSG907R devices to terminal bus 1 and terminal bus 2, the following SFP (Copper) is recommended in each case:

- 6GK6000-8CG01-0AA0

NOTE The VMs are configured for the terminal bus with exactly one virtual network adapter.

Use of the "SIMATIC NET SOFTNET-IE RNA" software in the VM is not approved.

5. User scenarios

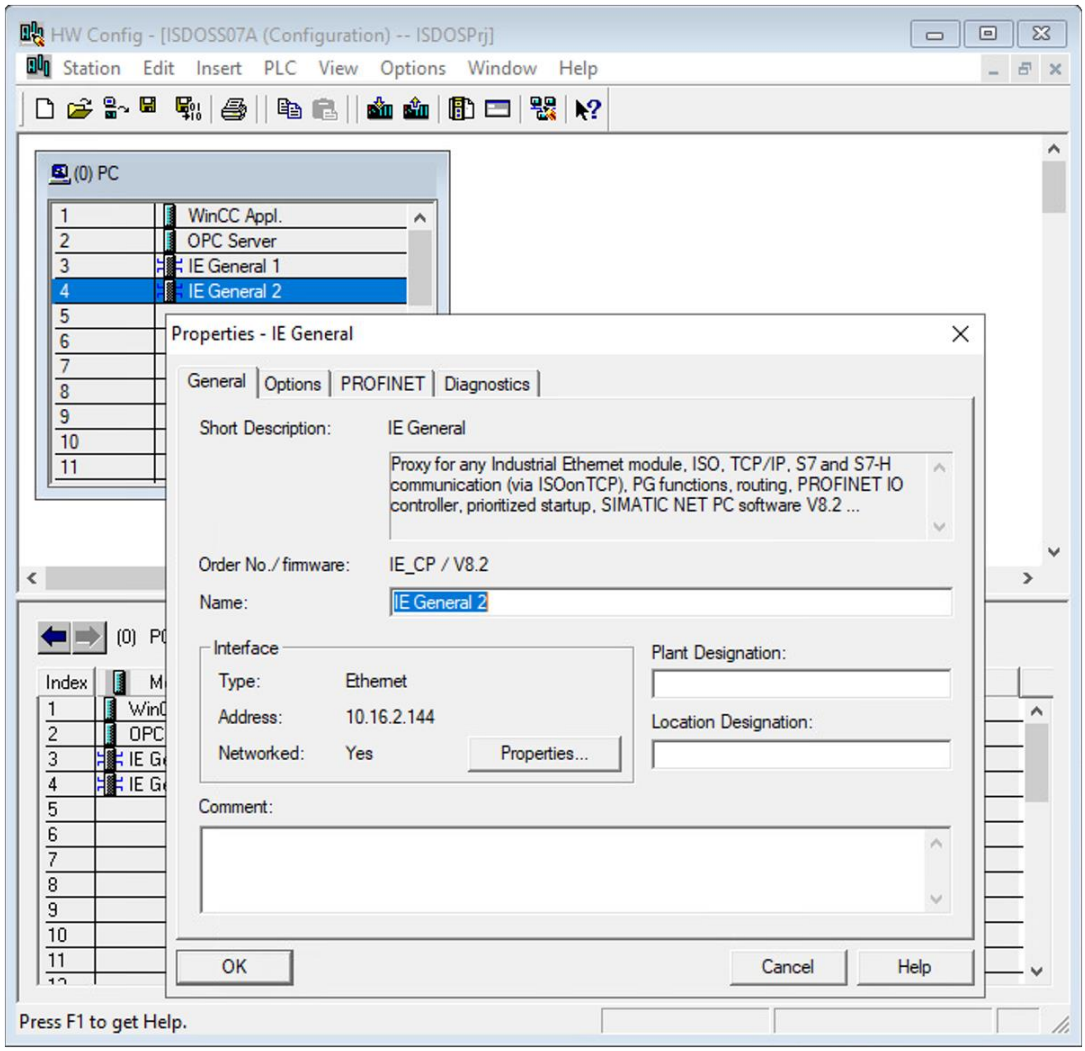
An important difference to real PCs is that the VMs (ES, OS Server, OS Client, etc.) are accessed via remote connection by means of a Thin Client or a remote system.

5.1. Engineering functions

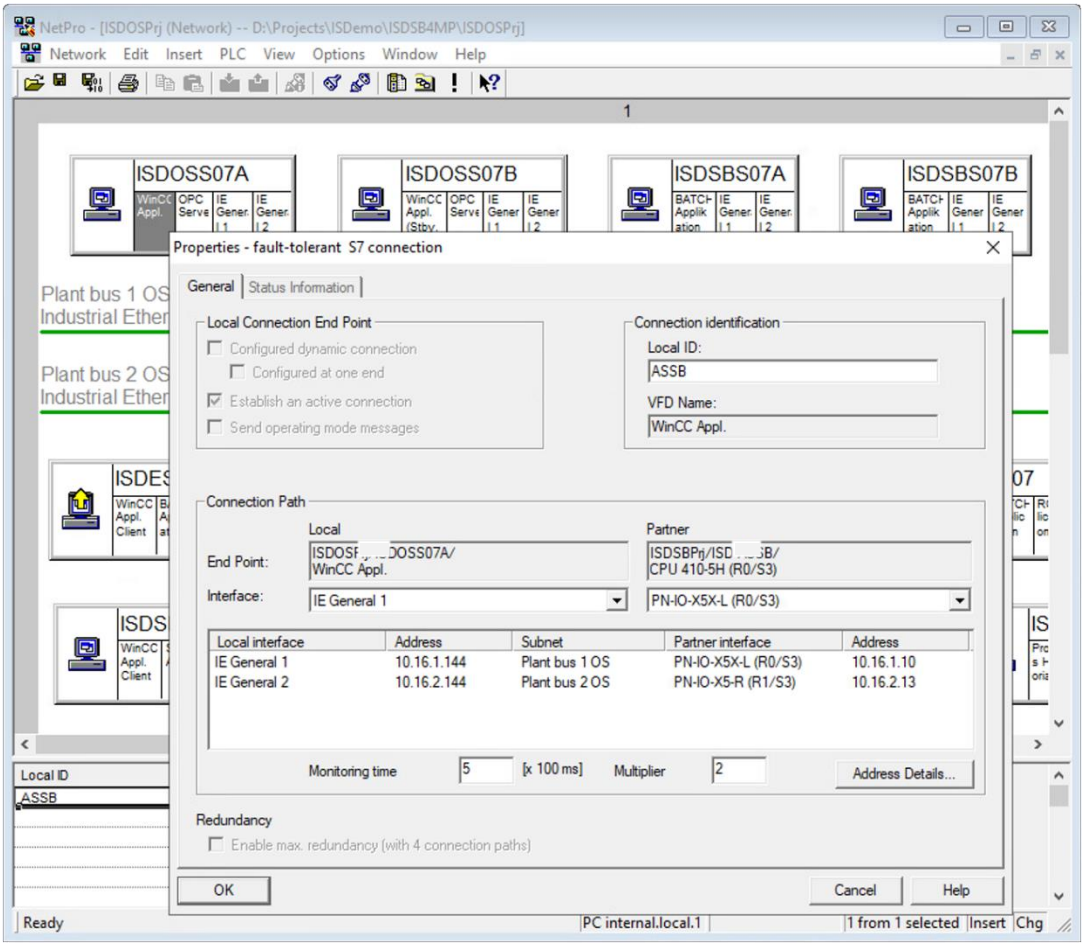
Configuration

The configuration procedure does not differ from that in the real environment. Even with real PCs, communication is still possible via BCE. In this instance, "IE General" must be used for the PC stations in HW Config.

The following figures show the hardware configuration (HW Config) of an OS Server with two configured "IE General" interfaces for connection to a redundant, fault-tolerant plant bus and the associated configured fault-tolerant connection of an "IE General" in NetPro.



© Siemens 2025



Downloading target systems

In a virtual ES, the target system is downloaded with the same functions as with the real one. In principle, there is no difference between a virtual or a real target system during a target system download.

© Siemens 2025

5.2. Process mode

In a virtual environment, the visualization takes place in the same way as with real PCS 7 stations, e.g. Single Station, OS Server, OS Client, etc. Real and virtual systems can coexist in mixed operation, with just an exception.

NOTE Mixed operation in a redundant server pair is not approved, i.e. either you have two real servers or two virtual servers.

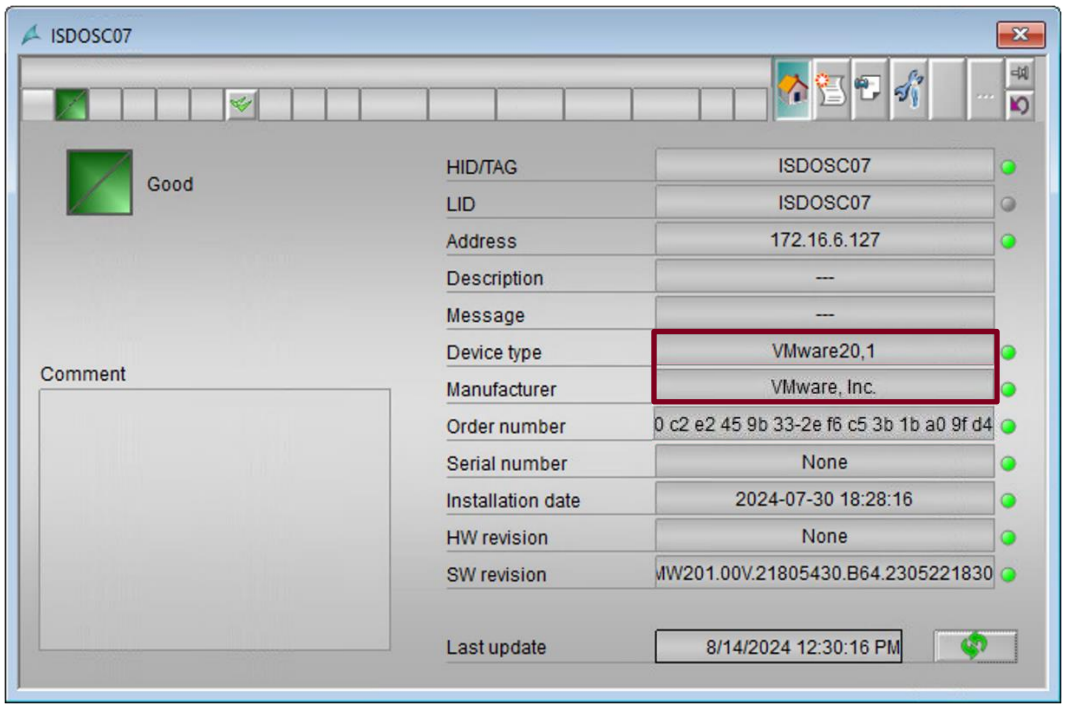
The real and/or virtual clients can visualize process data from both virtual and real servers.

5.3. Maintenance Server and Maintenance Client

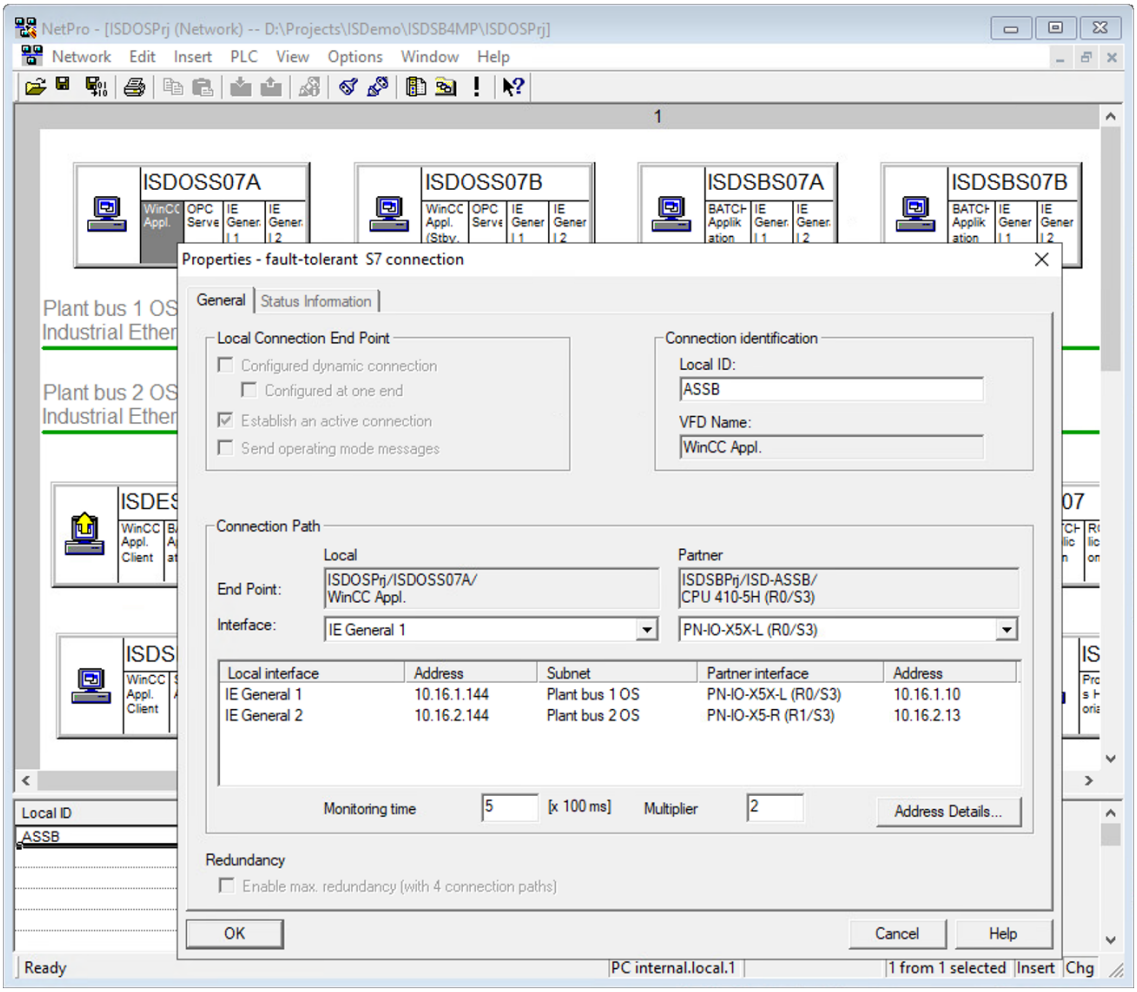
Principle

An OPC UA connection is created for the virtual machine if it is a WinCC station. This OPC UA connection is used for the client connection view.

For example, the following information is displayed in a VM:



© Siemens 2025



NOTE Via SIMATIC Virtualization as a Service (SIVaaS), it is possible to display the diagnostic data of an ESXi Host Server in the PCS 7 maintenance system (asset management) with SIMATIC PCS 7.

© Siemens 2025

Virtual ES as a Maintenance Client

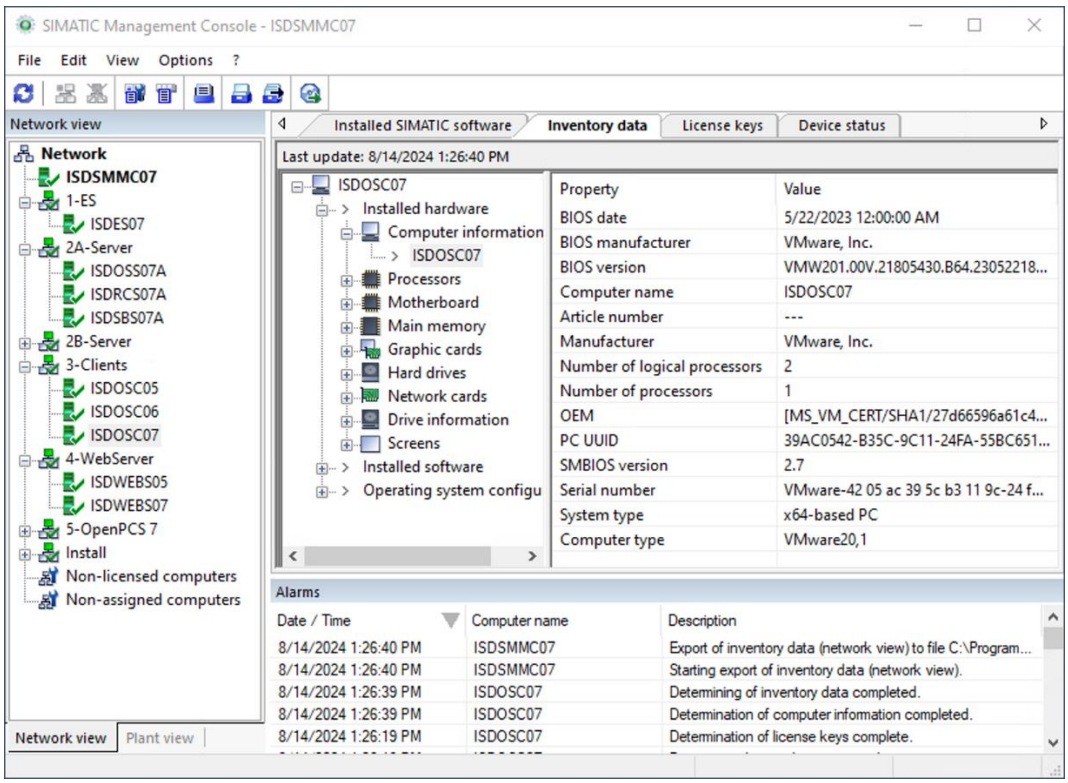
The SIMATIC PDM application is installed on the virtual ES. These enable the following functions:

- Access HW Config directly
- Access PDM via the "PDM Web Server" functionality
- Access SIMATIC Net products, such as SCALANCE X (invocation via the faceplate of the network device or directly in the browser), via HTTPS
- Display diagnostic data of an IPC via SIMATIC IPC OPRCLA

5.4. SIMATIC Management Console (SMMC)

The SMMC is installed as a separate VM. The SIMATIC Management Agent must be installed on all the stations you want to manage.

The following figure illustrates examples of the inventory data of a VM:



© Siemens 2025

6. Notes / constraints

6.1. SIMATIC BATCH

NOTICE

Limited plant availability

The batch database, and only this, must be stored on a dedicated hard disk. The (write) performance of the memory is imperative in this case. The memory size plays a secondary role. This is due to the high amount of 4 KB write activity on the batch database.

For this reason, it is recommended to use an SSD hard disk or an SSD RAID array for storing the batch database.

6.2. Special hardware

Signal modules and multi-monitor video cards are based on special hardware and therefore cannot be used in VMware vSphere.

NOTE

All modules used in the ESXi Server, whether by themselves or combined, must be listed in the VMware compatibility list (https://www.vmware.com/resources/compatibility/search.php) and approved for the corresponding version of VMware vSphere.

6.3. New VMs/templates/clones with VMware by Broadcom ESXi

Uniqueness

The following information must be observed, irrespective of how the VMs were created:

- All computers on the network must be unique. This applies equally for real and virtual components, even if combined, i.e. no identical computers may be in the network.
- Therefore, all computer names, network settings (MAC and IP addresses) and the so-called SID (this is generated automatically during the Windows installation) must be unique.

Creating new VMs

If a virtualization infrastructure (ESXi Server, vCenter Server and vSphere Client) is present, there are various ways of creating new VMs:

- Complete installation of VMs from scratch within a vSphere Client
- Creation of new VMs from templates within a vSphere Client connected to a vCenter Server
- Conversion of real machines into VMs using the VMware Converter (consolidation)
- Export/deploy prepared VMs in vSphere Client using OVF templates

© Siemens 2025

Requirements when creating new VMs

- The source VM or the template may only contain the operating system and never a SIMATIC PCS 7 installation.
- After creating the VM you have to generate a new SID. This can be done automatically or manually. In an adequately prepared Windows system, this is generated automatically the first time Windows runs (see the examples below about VMware options or the "sysprep" command).
- A new computer name must be assigned after creating the VM.

Therefore, the following applies when creating new VMs:

- If templates are located in a vSphere Client that is connected to a vCenter Server, the "Generate New Security ID (SID)" option must be selected.
- After cloning VMs to create new VMs, you have to run the command: sysprep /restart /generalize. This generates new SIDs and a new computer name must be assigned.
- If using OVF templates, these should have already been prepared with "sysprep /shutdown /generalize".

Using OVF templates

If OVF templates are present, they can be used, for instance, for the following tasks:

- Transferring VMs to another host
- Archiving exported VMs to external media
- Creating new VMs without a SIMATIC PCS 7 installation

VMware features

- You are not permitted to use the suspend/resume function in VMs.
- You are not permitted to use snapshots, especially during PCS 7 runtime operation.
- The FT function is not approved for use in virtual SIMATIC PCS 7 environments.
- The vMotion function may not be used during engineering and PCS 7 runtime operation (except for special scenarios in connection with SIVaaS).

NOTE VMware by Broadcom uses "vMotion" to describe the movement of virtual machines from one ESXi server to another during operation. The "vMotion" functionality is released for the operation of SOFTNET-IE S7 via the virtual network adapter "VMXNET 3". Communication interruptions occur during the movement of a virtual machine. Keep this in mind when configuring monitoring times of the communication protocols.

- The following special scenarios are supported by SIVaaS:
  - vMotion and High Availability (HA) for PCS 7 Clients during runtime operation
  - Distributed Resource Scheduler (DRS) with specific configuration

© Siemens 2025

6.4. Dual monitors

Dual-monitor operation is possible if the VM settings and WinCC project editor are properly configured and if the hardware is supported by the Thin Client.

6.5. Chip card reader

In PCS 7, a chip card reader in conjunction with SIMATIC Logon can be used to check the operating authorization at a single station or a client. In a virtual operating environment, the chip card reader is connected to a USB port of the thin client.

In this example, the "SIMATIC PCS7, USB Chip Card Reader, Chip Card Reader" (6ES7652-0XX02-1XC0) is used.

NOTE **Further information**

SIMATIC Logon V2.0, Chapter 9.4.3.3 Login via chip reader
https://support.industry.siemens.com/cs/ww/de/view/109973482

Prerequisite

- SIMATC Logon from V1.5.3
- Connection of the smart card reader to a USB port of the thin client
- Access to the virtualized OS client with SIMATIC Logon installed via RDP, see Cap. 4.4

NOTE If the user connects to a SIMATIC Logon computer via RDP, a card reader connected via RDP and local from the user's point of view can be selected as the login device. This setting is configured in the "Login Device" tab in the SIMATIC Logon configuration dialog. SIMATIC Logon always reads the map of the currently active user session.

Procedure

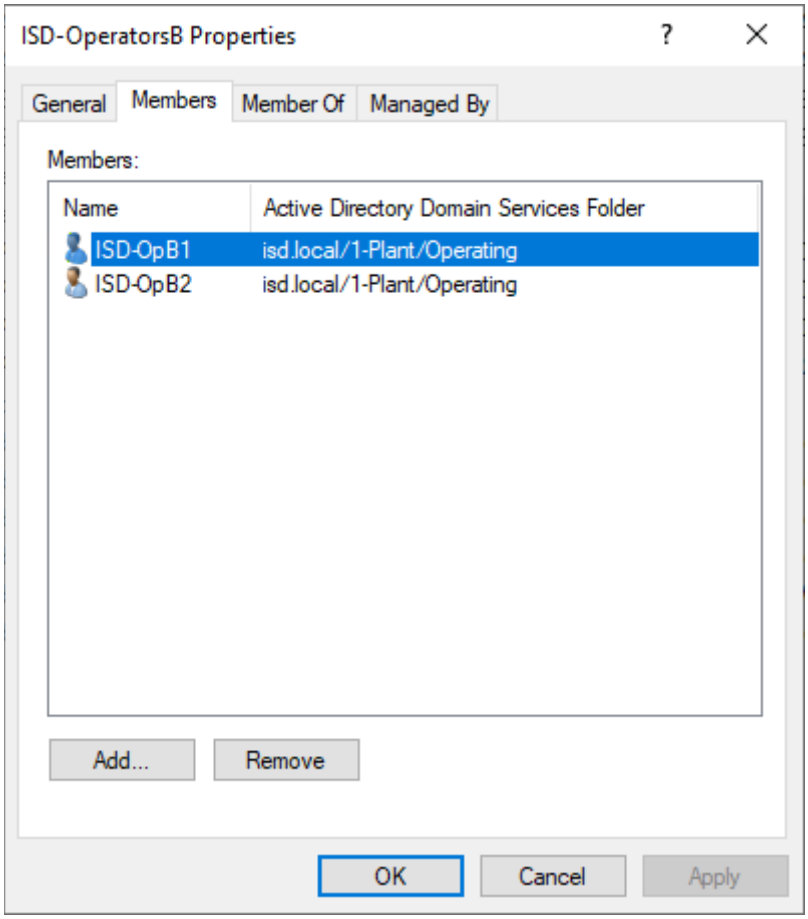
1. Configuration of users and groups for login
2. Configuration in the WinCC User Administrator of an OS Client
3. Connect the smart card reader to a USB port on the thin client
4. Configuration of SIMATIC Logon on the OS Client
5. Processing the chip card
6. Start runtime and login with the chip card

© Siemens 2025

6.5.1. Configuration of users and groups for login

This example uses the isd.local domain, the ISD-OperatorsB global domain group, and the ISD-OpB2 domain user to log on.

NOTE The configuration of a login computer for SIMATIC Logon is usually used in a workgroup.



© Siemens 2025

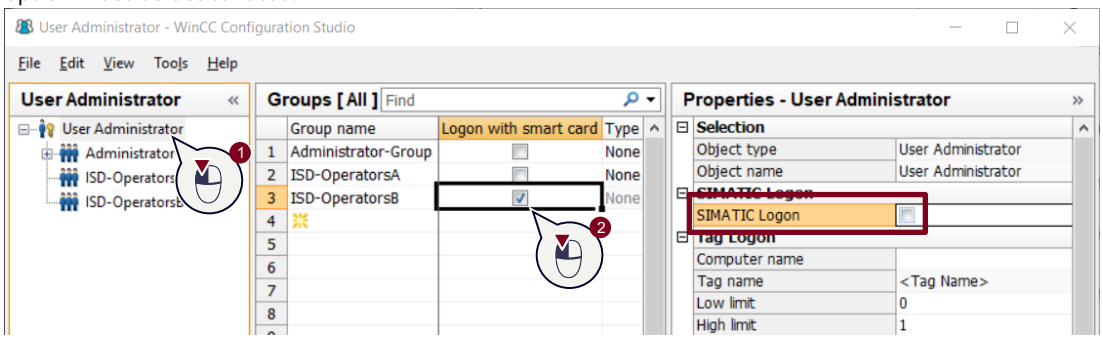
6.5.2. Configuration in the WinCC User Administrator of an OS Client

NOTE This step is usually configured on the ES in the User Administrator of the OS clients. The OS clients are then loaded onto the target station.

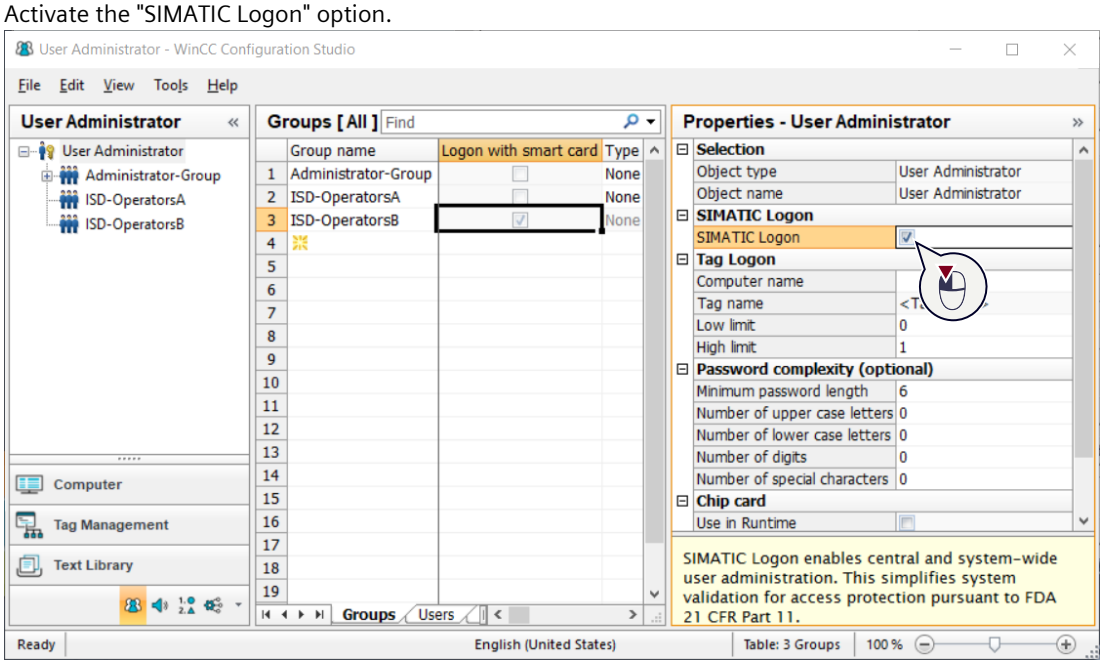
1. Project and configure the group "ISD OperatorsB" in the "User Administrator"

NOTE The group in the User Administrator must have the same name as the Windows group on the SIMATIC Logon login computer or a global domain group, such as the global domain group "ISD-OperatorsB" in this example.

2. Select "User Administrator" and activate the option "Logon with smart card" for "ISD-OperatorsB". The "SIMATIC Logon" option must be deactivated.

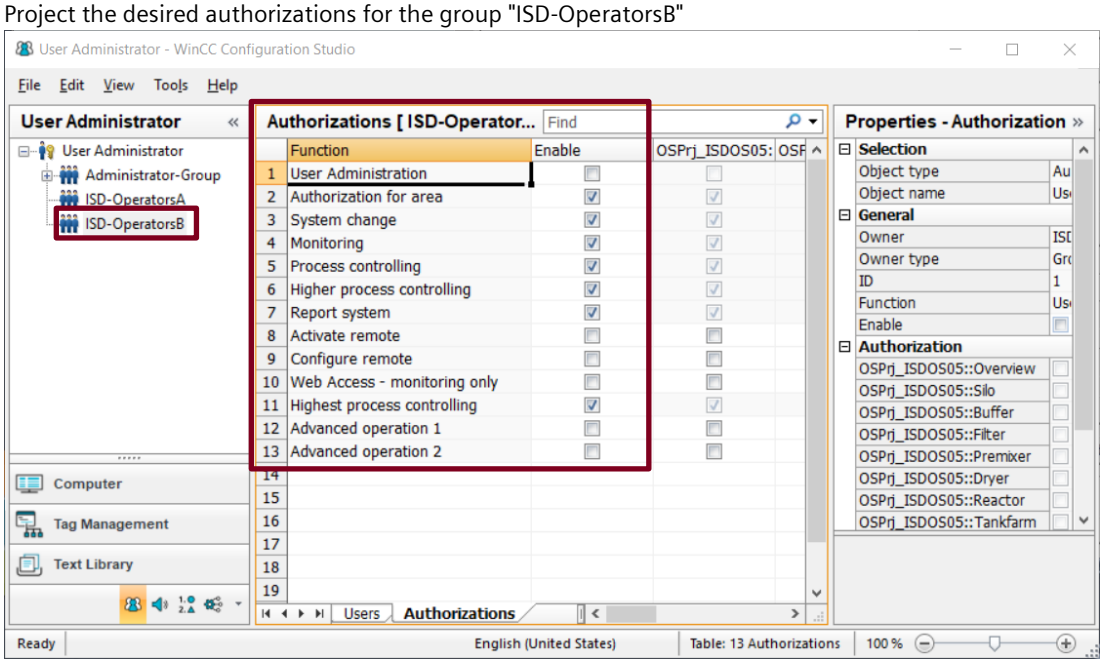


3. Activate the "SIMATIC Logon" option.



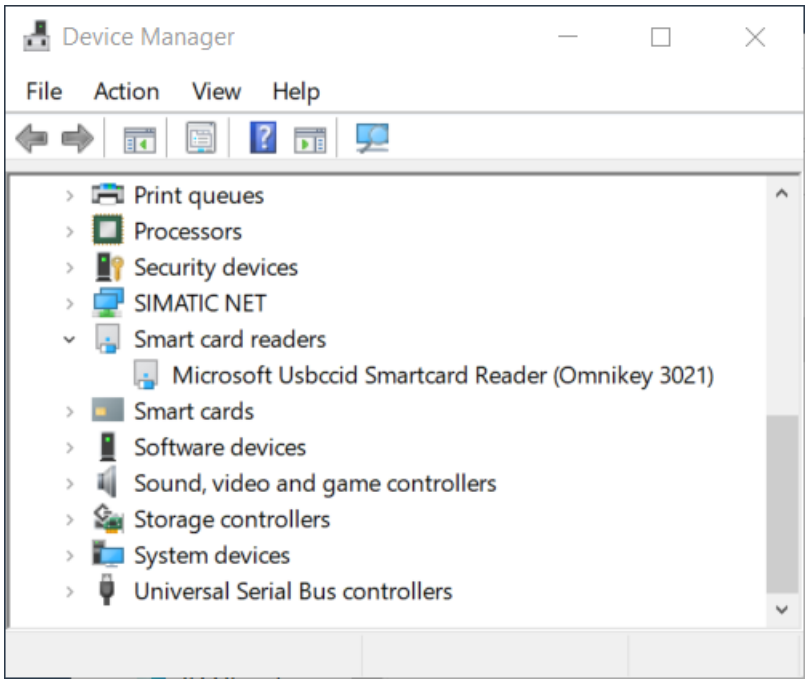
© Siemens 2025

4. Project the desired authorizations for the group "ISD-OperatorsB"



6.5.3. Connecting the smart card reader to a USB port on the thin client

After connecting the chip card reader to a USB port of the thin client, it must be visible in the device manager of the thin client. The driver should be included in the operating system.



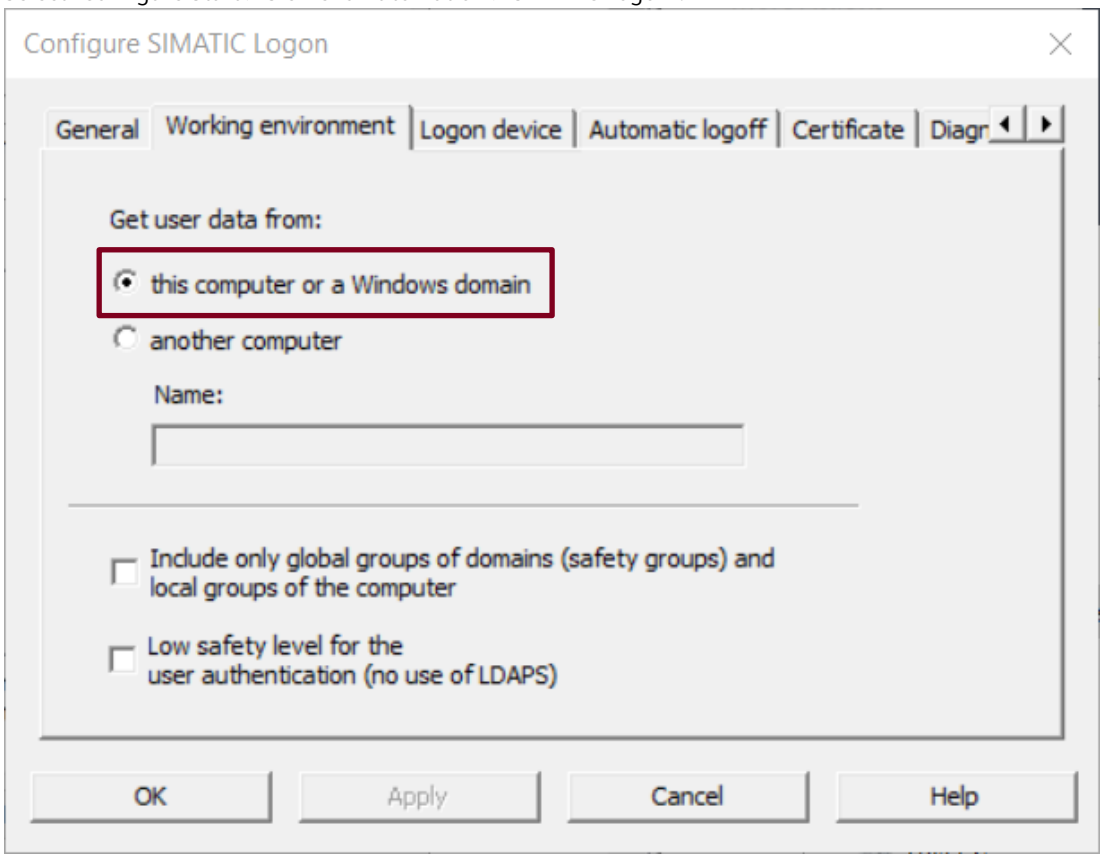
© Siemens 2025

6.5.4. Configuring SIMATIC Logon on the OS Client

SIMATIC Logon configured as in a real environment.

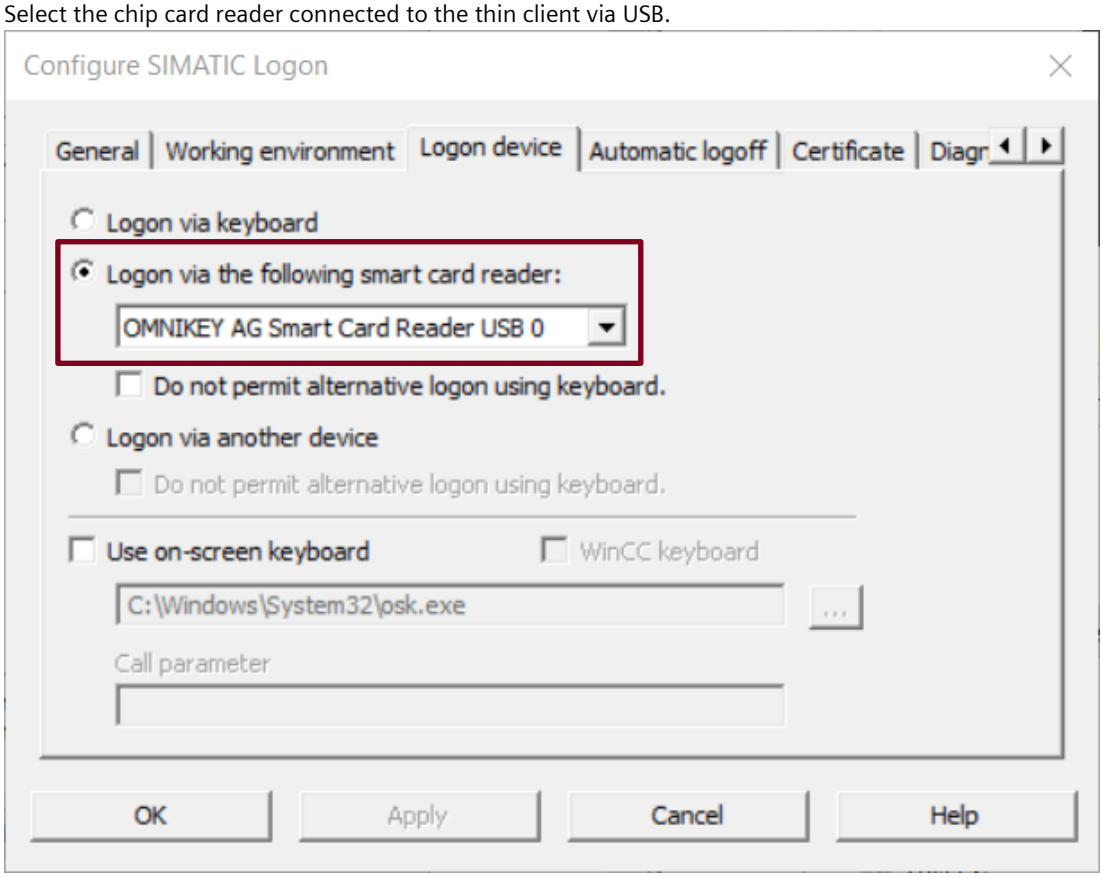
In this example, the domain isd.local and the domain user “ISD-OpB2” are used to log on.

1. Connect to OS Client
   Connect to the virtualized OS client via RDP, e.g. with the command mstsc /admin.
2. Selection of the working environment
   Select "Configure Start > Siemens Automation > SIMATIC Logon".



© Siemens 2025

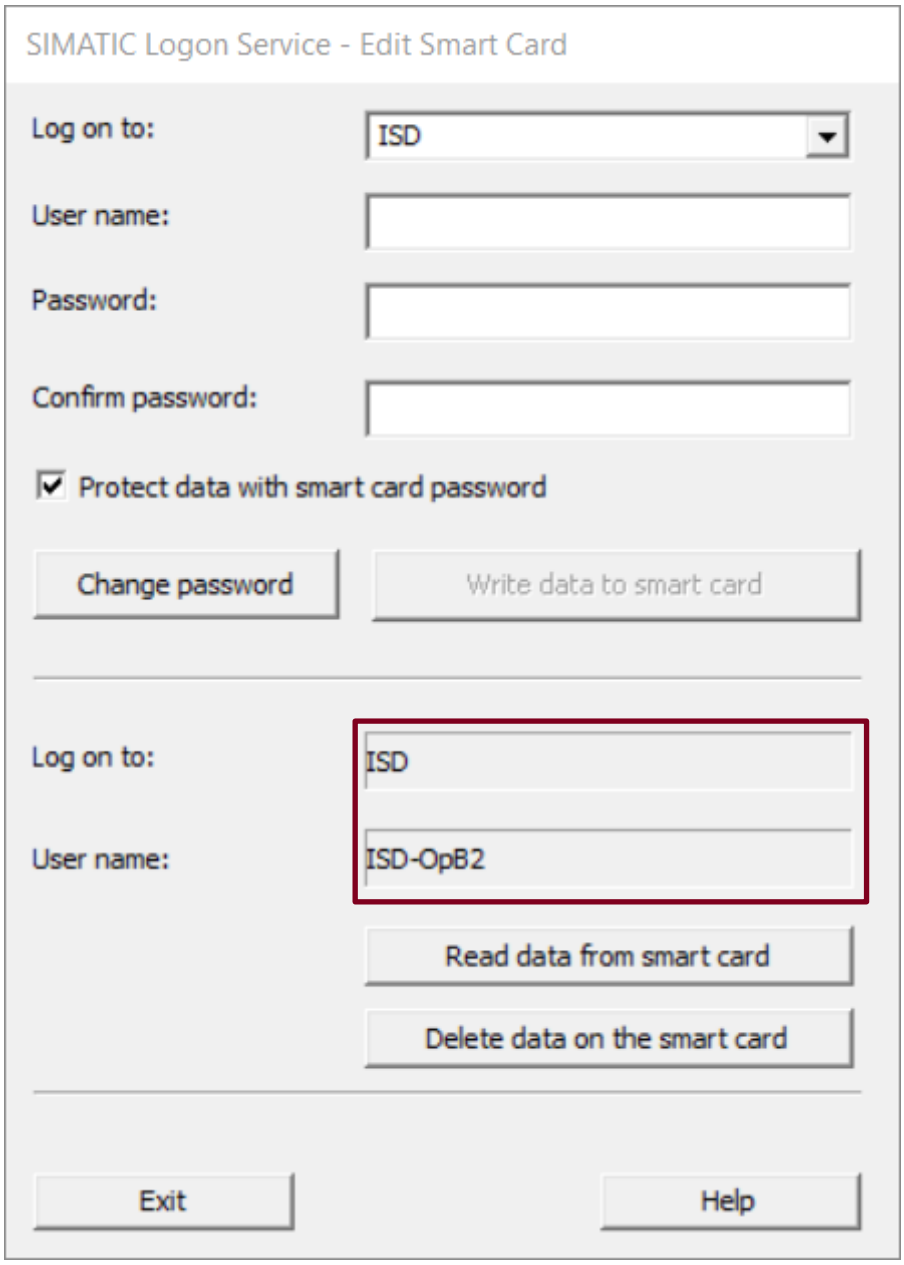
3. Selection of the input device
   Select the chip card reader connected to the thin client via USB.



© Siemens 2025

6.5.5. Editing the chip card

Select "Start > Siemens Automation > Edit Chip Card".



© Siemens 2025

6.5.6. Logging in to OS Runtime with Smart Card

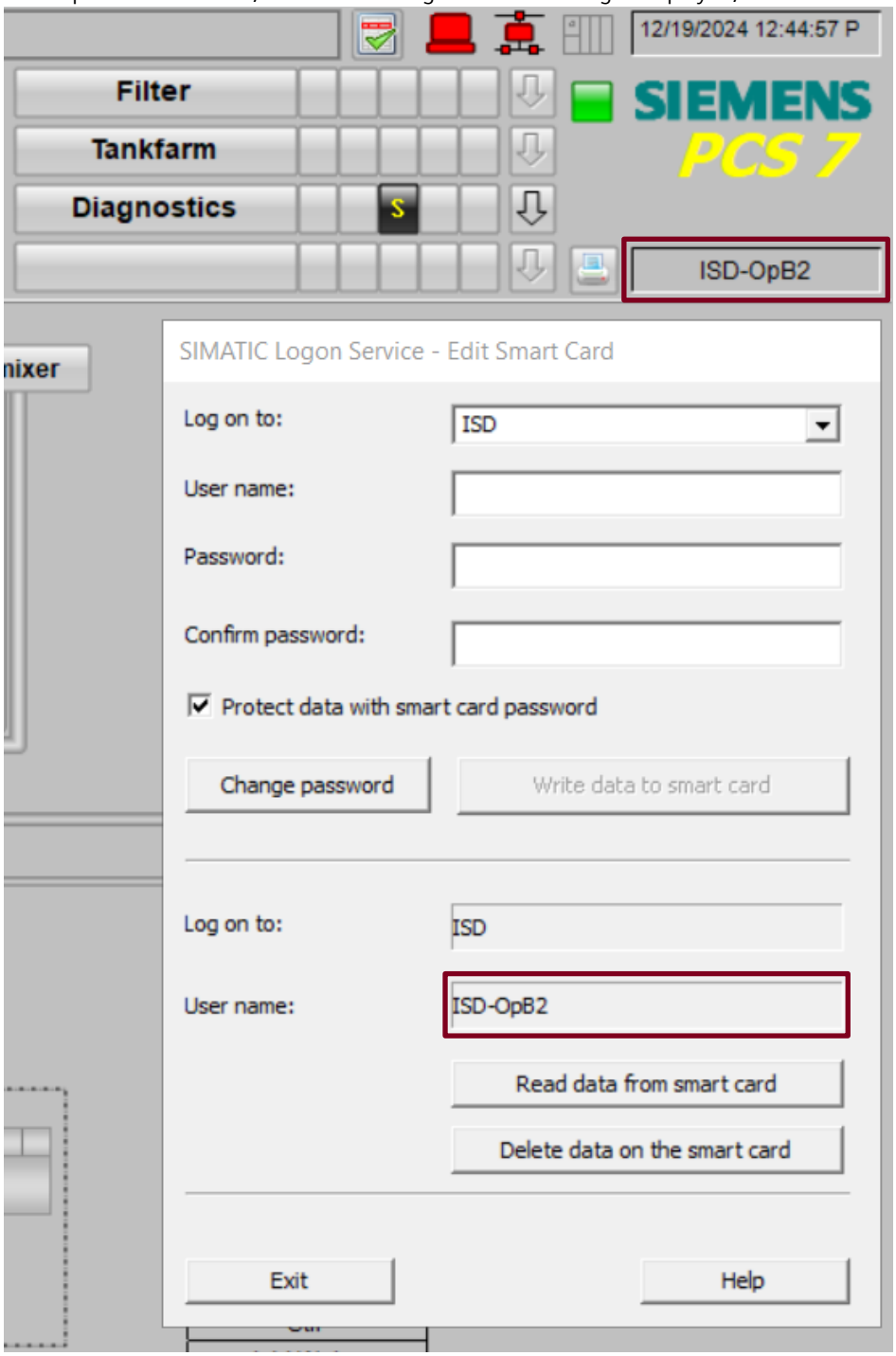
Prerequisite

- The smart card reader is connected to the thin client via USB and is displayed in the device manager.
- The users and groups for the login have been configured, for this example the group "ISD-OperatorsB" and the user "ISD-OpB2" in Active Directory.
- The user administrator on the OS client is configured, for this example the group "ISD-OperatorsB" for SIMATIC logon and chip card.
- The Logon device in SIMATC Logon has been configured.
- The chip card is written with the correct user and is inserted into the chip card reader.
- Runtime on the OS client is enabled

Procedure

Connect from the thin client to the virtualized OS client via RDP, e.g. with the command: mstsc /admin.

The following dialog shows the runtime image of the virtualized OS client with the user "ISD-OpB2", who is logged in via the chip card. In addition, the "SIMATIC Logon Service" dialog is displayed, which shows the user read from the chip card.



© Siemens 2025

6.6. S7 F/FH systems

S7 F/FH systems can be operated in a virtual environment.

You can find additional information in the FAQ entry
"What are the requirements for S7 F/FH systems in virtual environments and for remote access?".

6.7. Diagnostics with VMware by Broadcom ESXi

Diagnostics with VMware vSphere Client/vSphere Web Client

It is recommended to monitor the resources of the host and guest systems regularly using the vSphere Client/vSphere Web Client, such as:

- RAM utilization
- Operating state
- CPU load
- Hard disk use
- Network utilization

CPU use of the guest systems

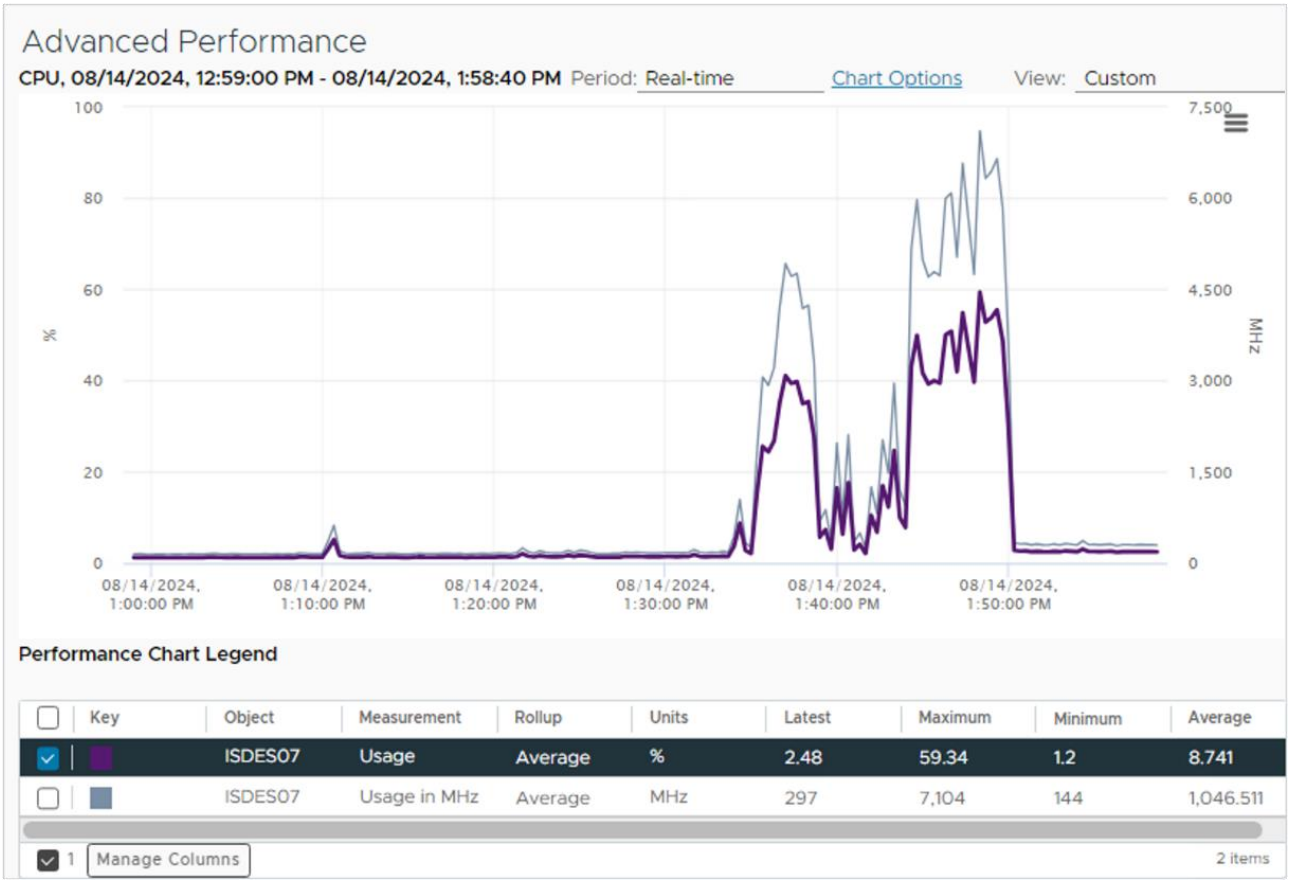
In a series of actions, the CPU load increases significantly, regardless of whether they are real systems or VMs.

- Web View Publisher
- Export configuration data
- Save as project with reorganization
- WinCC Project Migrator
- Compile the OS
- Advanced engineering: Import/export of data

© Siemens 2025

The following figure shows an ES with increased CPU load:

- During OS compiling (at approx. 1:35 PM)
- During the publishing of pictures (starting approx. 1:43 PM)

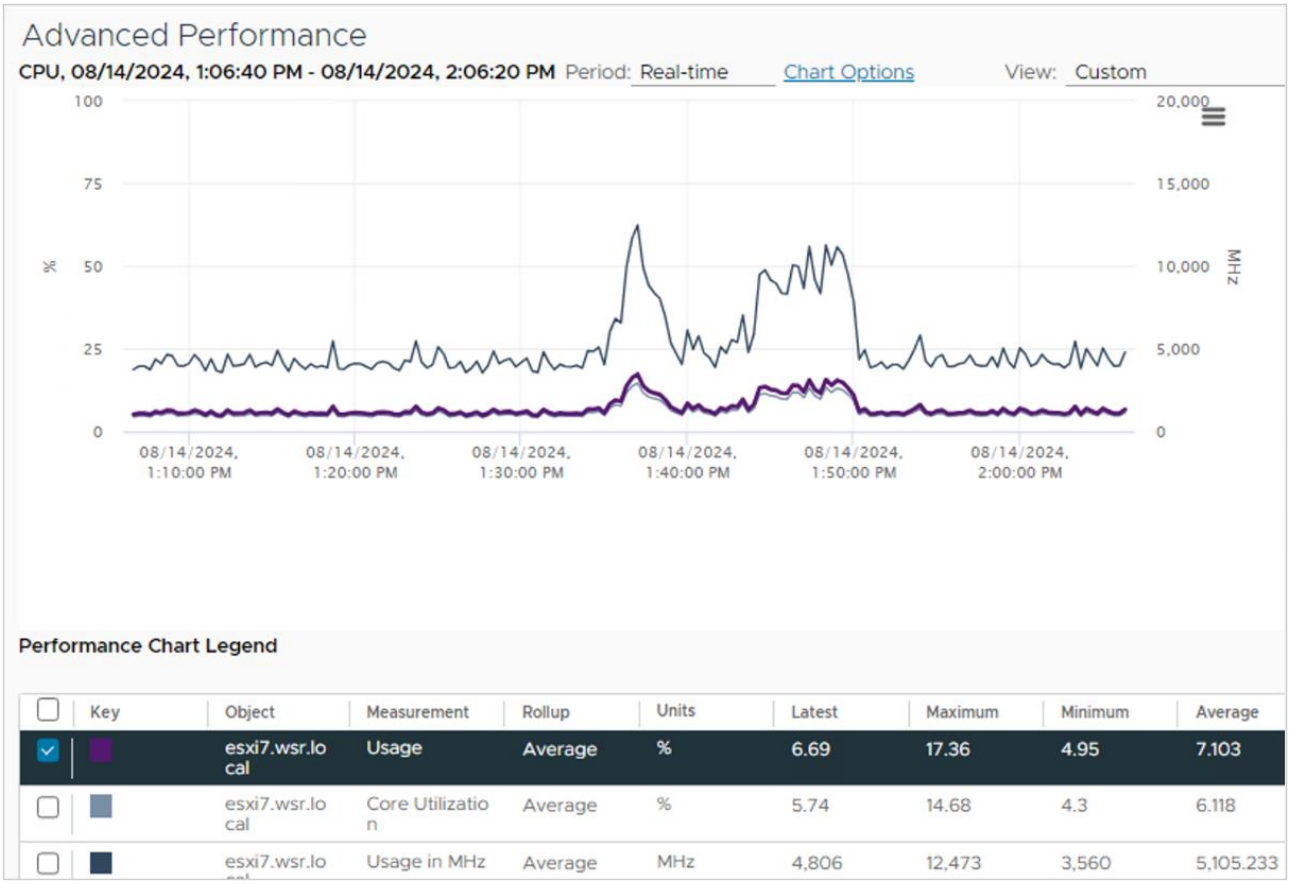


If the CPU load sticks to around 100% for an extended period, the host generates a warning followed by an error message. The message disappears automatically after completion. The task is completed without errors.

An warning appears in the default setting if a CPU load of 75% persists for longer than 5 min.
An alarm message is displayed in the default setting if a CPU load of 90% persists for longer than 5 min.

This also increases the load of the hypervisor.

This figure shows the increased CPU load of the corresponding hypervisor.

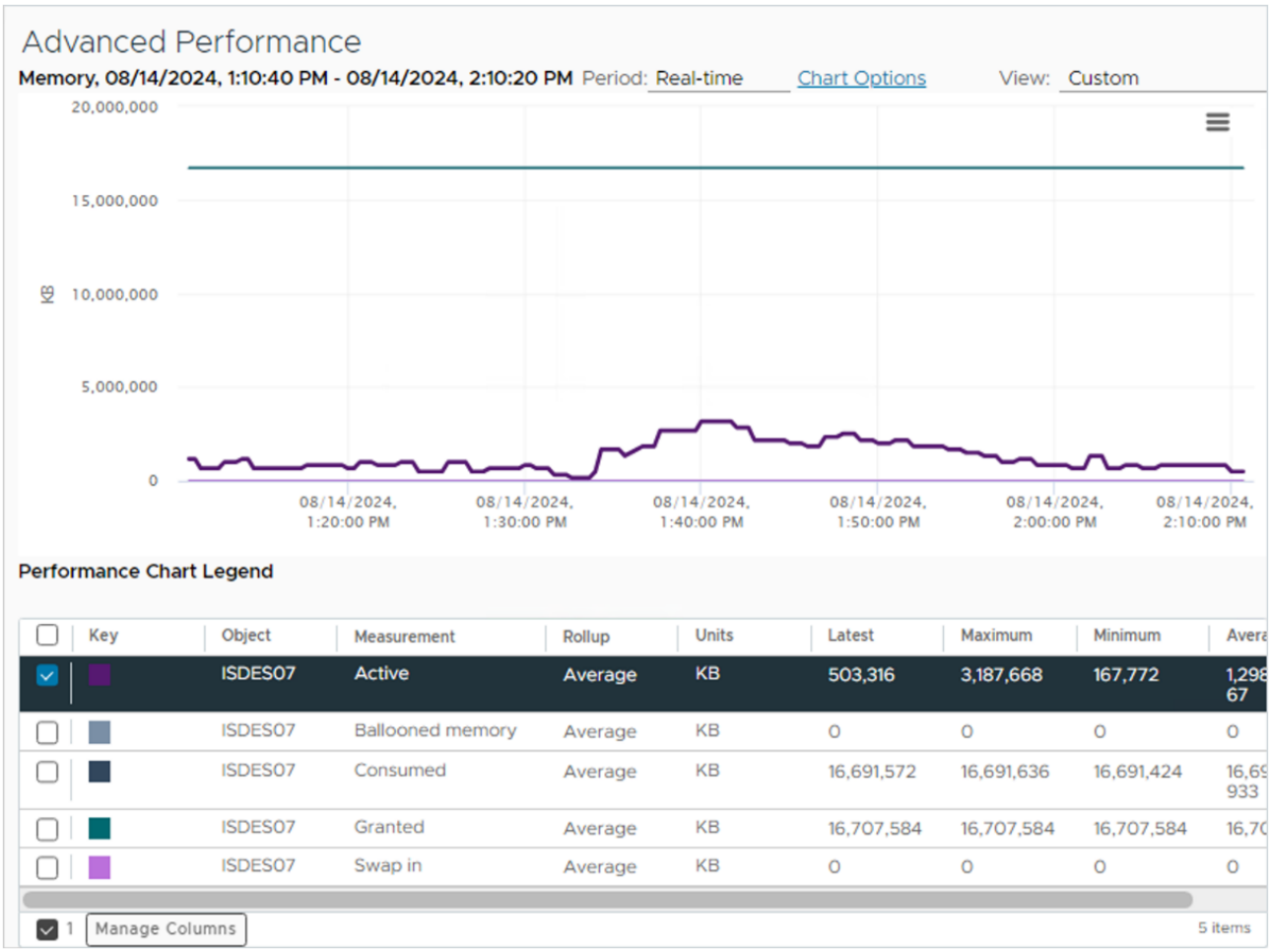


Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
■	esxi7.wsr.local	Usage	Average	%	6.69	17.36	4.95	7.103
■	esxi7.wsr.local	Core Utilization	Average	%	5.74	14.68	4.3	6.118
■	esxi7.wsr.lo	Usage in MHz	Average	MHz	4,806	12,473	3,560	5,105.233

© Siemens 2025

The figure shows the main memory used by the VM:

- The values for Balloon and "Swap out" must be 0. If this is not the case, either more RAM has to be allocated for the ESXi host, or VMs on this VMware by Broadcom ESXi Host have to be turned off. In this way, the host attempts to balance out resource bottlenecks.
- The values "Granted" and "Consumed" are identical because in this instance, the entire configured main memory (RAM) was reserved for the VM.



© Siemens 2025

7. Glossary

Guest

A guest is a virtualized computer running on a host (equivalent to VM).

Host

A host is the real hardware that the hypervisor, such as VMware by Broadcom ESXi or Microsoft Hyper-V, runs on. The host provides its resources to the virtual machines.

Hyper Threading

Hyper Threading is a technology for more efficiently processing commands on processors that support this technology. A real processor core will appear to the system as two processor cores.

Microsoft Hyper-V

Microsoft Hyper-V is a type 1 hypervisor.

Virtual hardware

Real resources are not directly available for virtual machines. Instead, they are virtualized to enable shared use.

Such shared hardware includes network adapters, CPU cores and hard disks. These can be used by all virtual machines either in part or concurrently.

Virtual processor core (vCore)

A virtual CPU core is a processor core that is allocated to a VM.

Virtual machine (VM)

See Guest

Virtual network

Virtual network is a network which is allocated to the virtual machine by the host. This enables multiple VMs to communicate on this network.

VMware by Broadcom

VMware was acquired by Broadcom. VMware by Broadcom is a company and manufacturer of virtualization software.

VMware by Broadcom ESXi

VMware by Broadcom ESXi is a type 1 hypervisor and is a central component of VMware vSphere.

VMware Remote Console (VMRC)

VMRC facilitates remote access to VMs with a console.

VMware vCenter Server

VMware vCenter Server is part of VMware vSphere and serves for central administration of the virtual infrastructure.

VMware vSphere

VMware vSphere is a range of products by VMware for virtualization based on a type 1 hypervisor.

VMware vSphere Client

VMware vSphere Client forms part of VMware vSphere and enables access to the vCenter Server or VMware ESXi Server. This makes it a tool for managing the virtual infrastructure; it also enables access to VMs.

VMware Workstation

This is a Type 2 hypervisor that is used to generate and manage virtual systems on an existing operating system.

© Siemens 2025

8. Appendix

8.1. Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

https://support.industry.siemens.com/

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers
– ranging from basic support to individual support contracts.

Please send queries to Technical Support via Web form:

https://support.industry.siemens.com/cs/my/src

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

https://support.industry.siemens.com/cs/sc

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for iOS and Android:

https://new.siemens.com/global/en/products/software/mobile-apps/industry-online-support.html

© Siemens 2025

8.2. Links and literature

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download pages for this entry: Manual: https://support.industry.siemens.com/cs/ww/en/view/109812895 Overview of entries on the topic of "PCS 7 Virtualization": https://support.industry.siemens.com/cs/ww/en/view/51975791
\3\	OS client, Batch client, Route Control client with SIMATIC PCS 7 V10.0 SP1 released for virtual operating environments: https://support.industry.siemens.com/cs/document/109987430
\4\	Compatibilitytool: http://www.siemens.com/kompatool
\5\	FAQ: Technical support for the design of a virtual SIMATIC PCS 7 / WinCC system: https://support.industry.siemens.com/cs/ww/en/view/109749129
\6\	AE: WinCC Virtualization: https://support.industry.siemens.com/cs/ww/en/view/49368181
\7\	Sales/delivery release of SIMATIC NET PC Software V18: https://support.industry.siemens.com/cs/ww/en/view/109815654
\8\	FAQ: Quantity frameworks and performance data of the SIMATIC NET products: https://support.industry.siemens.com/cs/ww/en/view/15227599
\9\	SIMATIC Virtualization as a Service: http://www.siemens.com/sivaas
\10\	AE: Service Bridge – Setup and Configuration: https://support.industry.siemens.com/cs/ww/en/view/109747975
\11\	SIMATIC PCS 7 Time Synchronization (V10.0): https://support.industry.siemens.com/cs/ww/en/view/109973498
\12\	SIMATIC PCS 7 Readme V10.0 SP1 (Online): https://support.industry.siemens.com/cs/document/109976468
\13\	AE: Determination of suitable hardware for the Process Historian with the "PH-HWAdvisor" tool: https://support.industry.siemens.com/cs/ww/en/view/109740115
\14\	SIMATIC PCS 7 PC - Configuration (V10.0): https://support.industry.siemens.com/cs/document/109986626
\15\	FAQ: How do you configure a Virtual Local Area Network (VLAN) in PCS 7? https://support.industry.siemens.com/cs/ww/en/view/66807297
\16\	SIMATIC PCS 7 High Availability Process Control Systems (V10.0): https://support.industry.siemens.com/cs/ww/en/view/109973497
\17\	VMware Compatibility Guide: https://www.vmware.com/resources/compatibility/search.php
\18\	FAQ: What are the requirements for S7 F/FH systems in virtual environments and for remote access?: https://support.industry.siemens.com/cs/ww/en/view/109475027

© Siemens 2025