

Manual • 10/2016

PCS 7 Virtualization – Project Engineering and Configuration

SIMATIC PCS 7 V8.2



<https://support.industry.siemens.com/cs/ww/en/view/109739973>

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.

Security information

Siemens provides products and solutions with industrial security 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 security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit <http://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <http://www.siemens.com/industrialsecurity>.

Table of contents

Legal information	2
1 Preface	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 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
3.3 SIMATIC PCS 7, SIMATIC WinCC and SIMATIC NET	16
3.4 SIMATIC Virtualization as a Service	17
4 Configuration	18
4.1 Configuration of the host system.....	18
4.1.1 Hardware	18
4.1.2 Network	19
4.1.3 Time synchronization	21
4.1.4 DNS and routing	24
4.2 Configuration of the guest system.....	25
4.2.1 General information	25
4.2.2 Configuration of the network adapters	27
4.2.3 Licensing	31
4.3 Configuration examples.....	32
4.3.1 Configuration of the VMs.....	32
4.3.2 Configuration 1	34
4.3.3 Configuration 2	35
4.3.4 Configuration 3	36
4.4 Remote access.....	37
5 User scenarios	38
5.1 Engineering functions.....	38
5.2 Process mode	40
5.3 Maintenance server and Maintenance client.....	40
5.4 SIMATIC Management Console (SMMC)	41

6	Notes / constraints	42
6.1	SIMATIC Batch.....	42
6.2	Special hardware.....	42
6.3	Communication	42
6.3.1	VLANs	42
6.3.2	Redundant plant or terminal bus	43
6.3.3	Redundancy connection between servers	43
6.3.4	Name resolution	43
6.3.5	Communication over multiple subnets	44
6.3.6	Communication with the AS	45
6.4	New VMs/templates/clones	47
6.5	Dual-monitor	49
6.6	Chipcard reader.....	49
6.7	S7 F/FH systems.....	49
6.8	Diagnostics	49
7	Glossary	53
8	Service and Support.....	55
9	Appendix	56
9.1	Related literature	56
9.2	History	56

1 Preface

Aim of the document

This document gives you an overview of the PCS 7 virtualization feature. It shows the typical configurations and addresses the specific features of PCS 7 in a virtual environment.

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.

Validity

This document applies to PCS 7 V8.2.

Please observe the information and notes in the article [Release of SIMATIC PCS 7 V8.2 system components for virtual operating environments](#).

2 Automation task

2.1 Overview

The virtualization of servers has already achieved a high status in information technology. Even users of automation technology (e.g. SIMATIC PCS 7) have recognized the benefits of virtualization and apply it increasingly.

This application example includes the following information:

- Virtualization of typical PCS 7 system configurations
- Which infrastructure is required for the virtualization of PCS 7 systems?
- What should I consider when running 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 Player, VMware Workstation, Windows Virtual PC ... VMware vSphere
Production plants	VMware vSphere

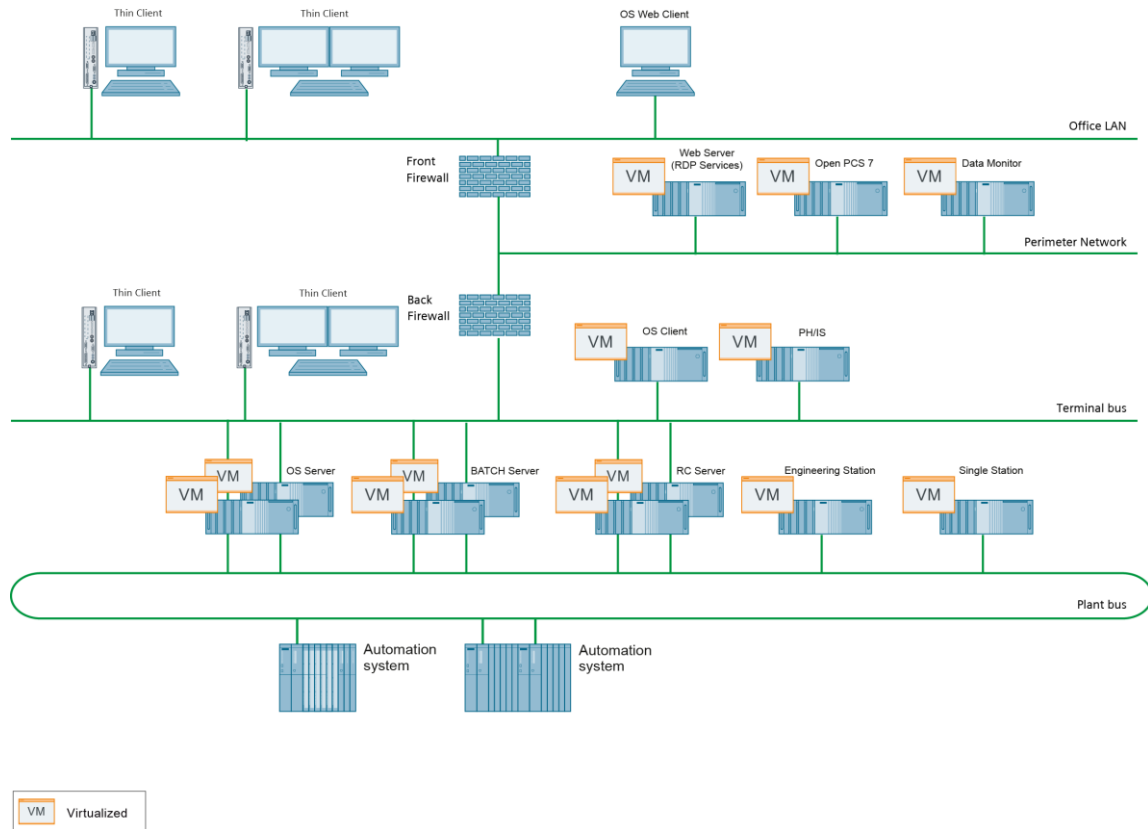
CAUTION Approval of the virtualization software

SIMATIC PCS 7 has been exclusively approved for VMware vSphere. The approved version of VMware vSphere for PCS 7 is included in the respective Release FAQ for PCS 7 in a virtual environment and in the [Compatibility tool](#).

3 Automation solution

3.1 PCS 7 system architecture in a virtual environment

The PCS 7 systems marked with "VM" in the following figure can be virtualized.



3.2 What is virtualization?

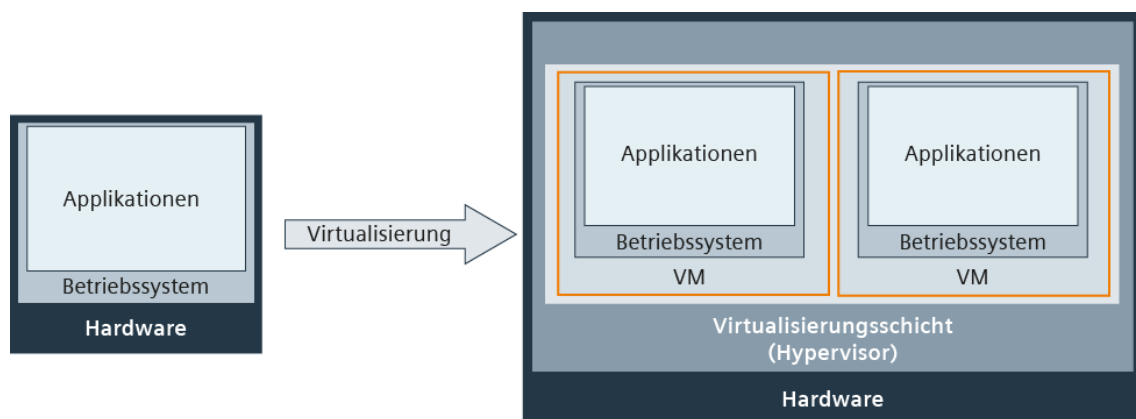
3.2.1 Definition

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 enables the realization of multiple virtual machines (VM) with their own virtual hardware components, which are isolated from each other on one real physical PC. They behave like real computers and can run their own applications independently.

Diagram about Virtualization

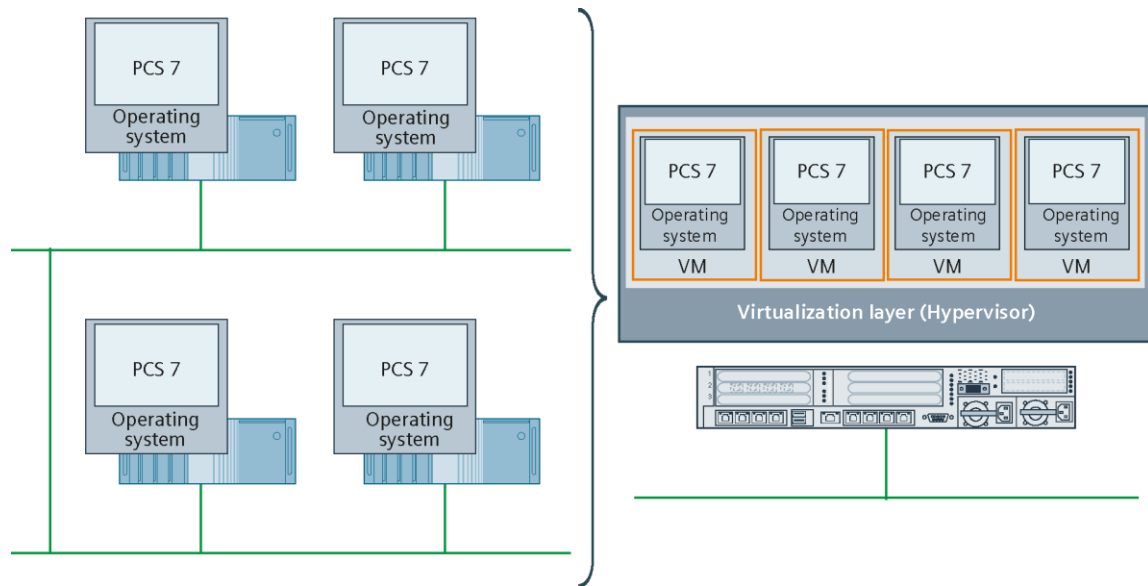


Tasks of the hypervisor

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:

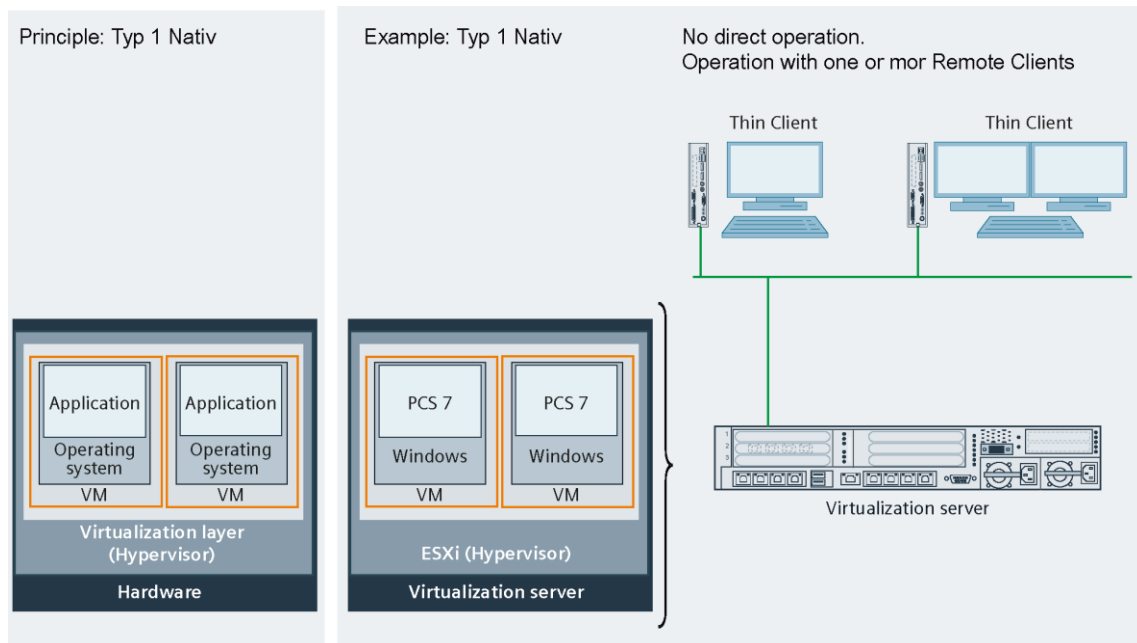
- Server-based virtualization (Type 1: Native)
- Client-based virtualization (Type 2: Hosted)

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

Example

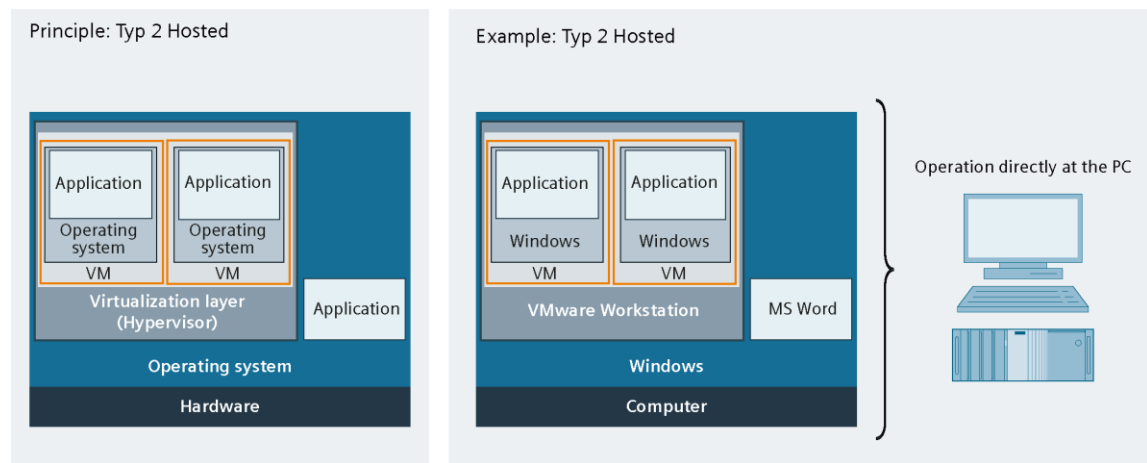


3.2.3 Client-based virtualization (Type 2: Hosted)

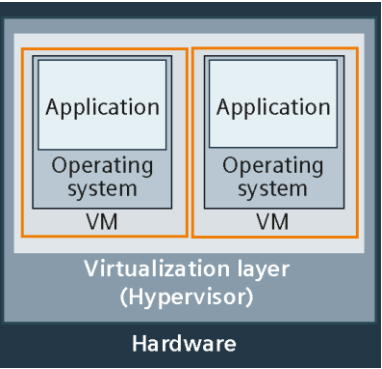
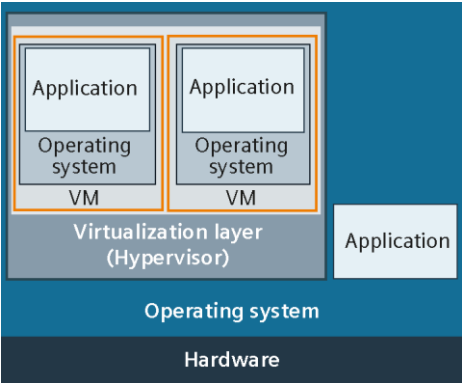
This virtualization type is characterized by the following features:

- 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



3.2.4 Summary of server-based and client-based virtualization

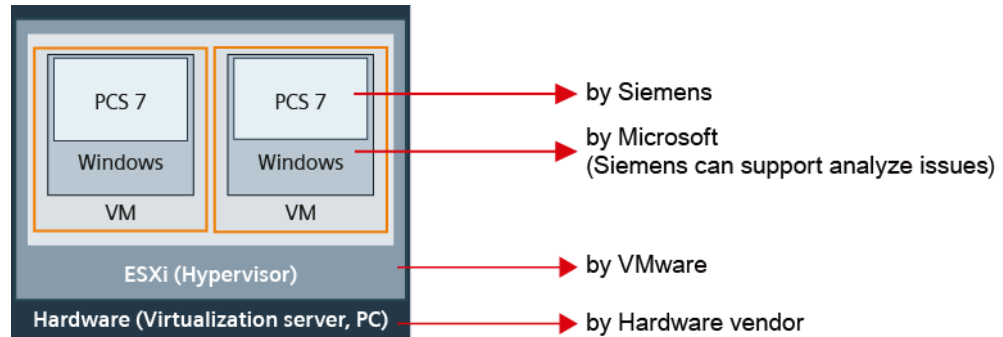
Server-based virtualization (Type 1 Native)	Client-based virtualization (Type 2 Hosted)
	
The hypervisor runs directly on the hardware of the host and is more efficient. It requires fewer resources, but must provide all the drivers.	The hypervisor is based on a full-fledged operating system (e.g. Windows) and uses the device drivers of the operating system.
No direct operation: The VMs are operated via remote client.	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

3.2.5 Advantages and disadvantages of virtualization

	Benefits	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
Safety	Increased security • Increased security via remote access and centralized rights administration • Reduced attack possibilities with thin clients; central protection on the ESXi server for the virtual machines	• Possible increase in security-related expenses (additional layers, data security)
Availability	Increase of availability • Virtual machines running on ESXi servers 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 ESXi server • Possibility of adding virtual machines by starting another VMware session	-
System complexity	-	• Significant increase of system complexity • Higher administration costs

Support

If a problem occurs when operating a virtual machine, the needed 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 ch. 3.4) you not only get preinstalled and preconfigured ESXi servers incl. PCS 7 installations in the form of VMs, but also the services for these complete systems from a single source.

3.3 SIMATIC PCS 7, SIMATIC WinCC and SIMATIC NET

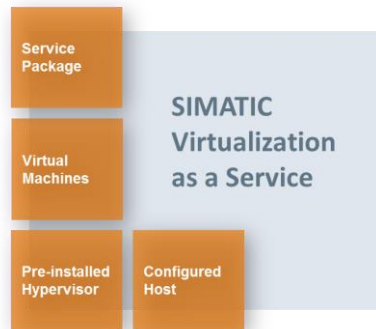
Apart from this document, you can find further information and notes on how to operate PCS7 in a virtual environment in the article [Release of SIMATIC PCS 7 V8.2 system components for virtual operating environments](#).

SIMATIC WinCC and SIMATIC NET are two essential components of SIMATIC PCS 7. There are therefore plenty of similarities, but also differences. For further information, please refer to:

- [FAQ: WinCC Virtualization](#)
- [Sales/delivery release of SIMATIC NET DVD V13 SP2](#)
- [Quantity frameworks and performance data of the SIMATIC NET products](#)

3.4 SIMATIC Virtualization as a Service

SIMATIC Virtualization as a Service is a preconfigured, ready-to-use virtualization system for the implementation of efficient automation solutions for SIMATIC systems.



A hypervisor server 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 pre-configured 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:

- [SIMATIC Virtualization as a Service](#)

4 Configuration

4.1 Configuration of the host system

CAUTION	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 Hardware

The following proven recommendations are based on practical experience:

- The configured main memory (RAM) for all concurrent VMs must not exceed 90% of the available physical RAM.
- The 1:2 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 assignment:

Hardware	Quantity	Use
Intel® Xeon® Processor E5-2660 (20M cache, 2.20 GHz, 8.00 GT/s Intel® QPI)	8 cores	1 core per host
		1x OS server: 2 virtual cores 5x OS clients: 10 virtual cores

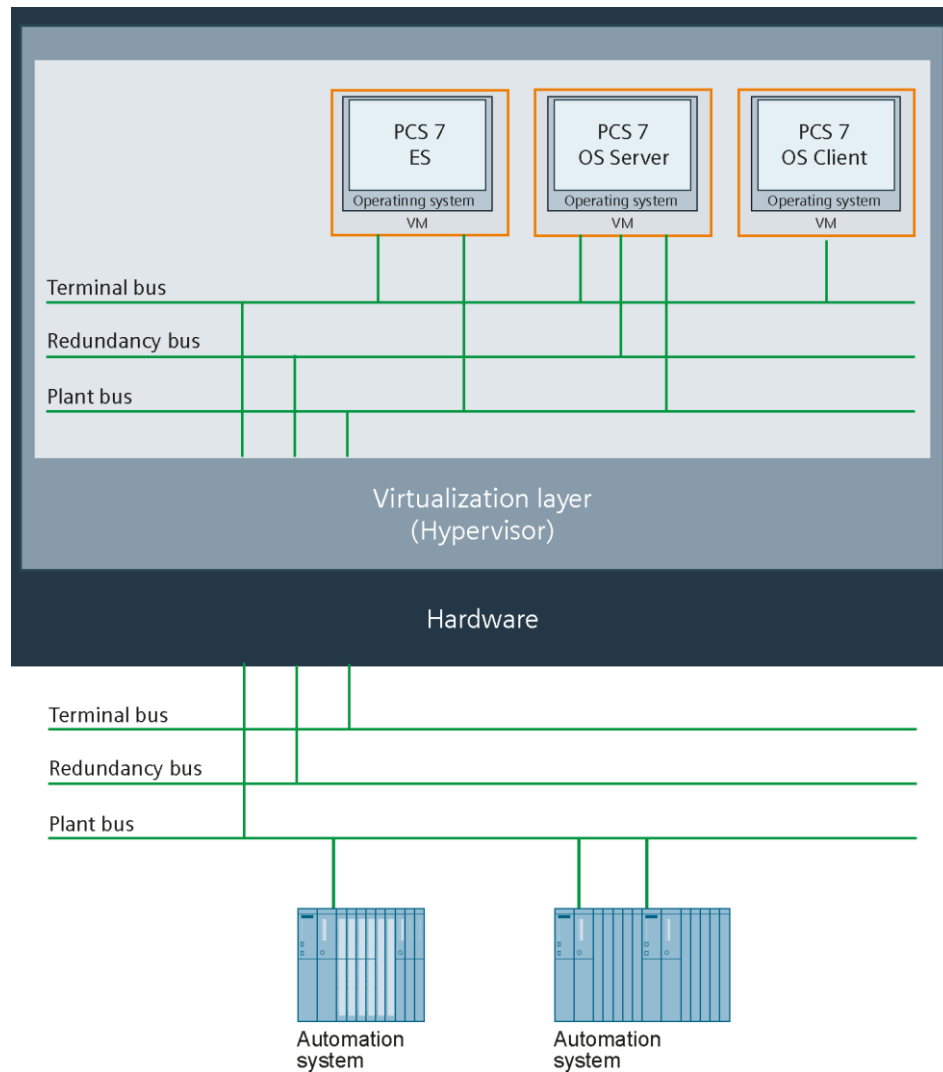
- For performance reasons, the size of the data stores may not exceed 2TB per RAID system.
- The best read-write performance can be achieved by implementing a RAID 10 system.
- PCS 7 performs better when preference is given to a CPU with fewer cores and higher clock frequency compared to a CPU with more cores and lower clock frequency.

4.1.2 Network

Principle

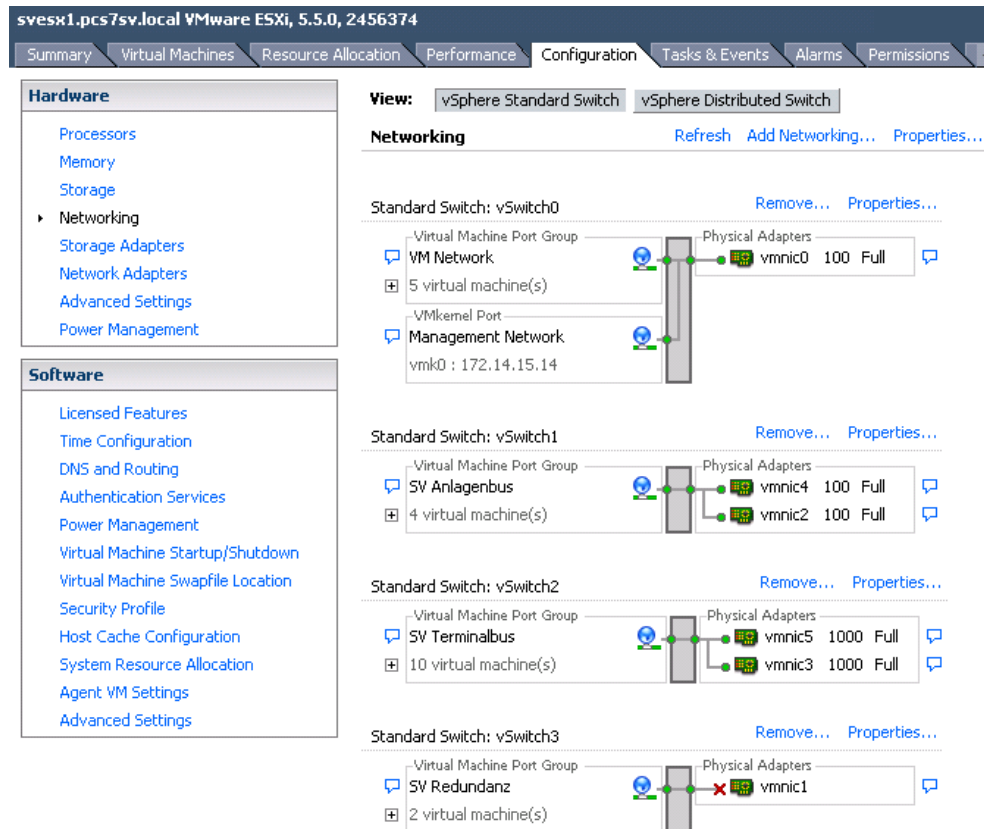
The following figure illustrates the communication principle of a virtualization system:

- 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 ESXi server.



The following figure shows:

- The management network, and the terminal, system and redundancy bus are fed outwards in a redundant manner via dedicated physical network adapters (vmnic0 ... vmnic4, partly redundant (optional)).
- No Ethernet cable is connected to the network adapter of the redundancy bus.
- The virtual standard switch (vSS) is used.
- No VLANs are used.



Note For the terminal, system and redundancy bus, it is recommended to use a dedicated network adapter on the host.

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

CAUTION **Virtual switch on the plant bus**
Only the "virtual standard switch" (vSS) may be used on the plant bus. You can also use the "virtual distributed switch" (vDS) on the other networks.

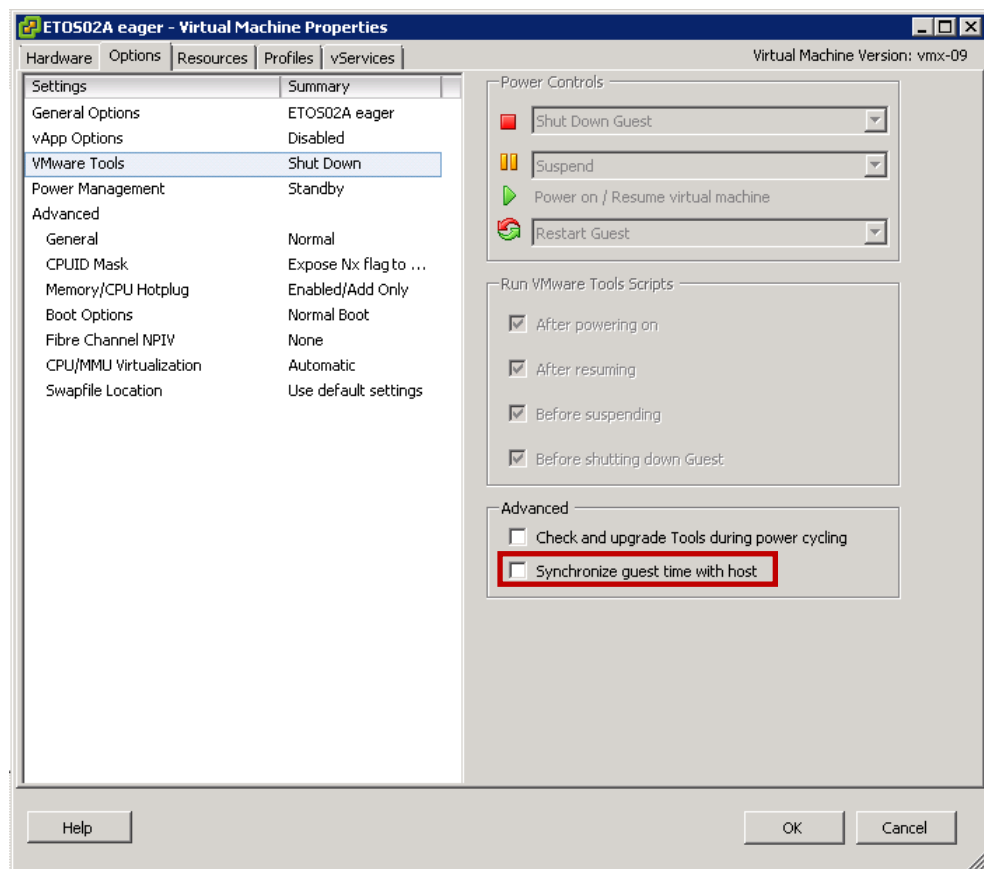
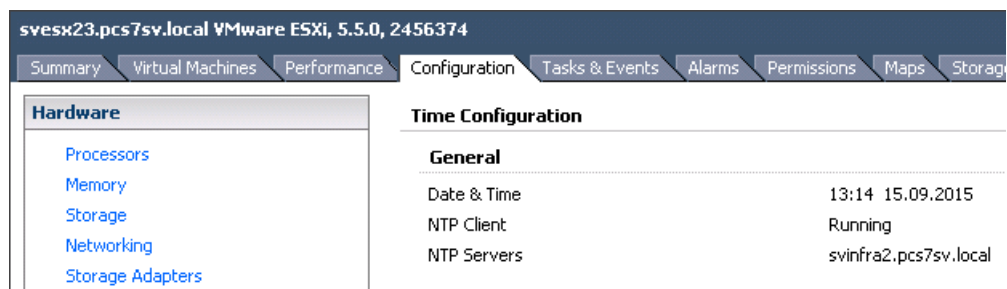
4.1.3 Time synchronization

CAUTION
Time synchronization

Besides the guest systems, even the ESXi server must be synchronized in a virtual environment. The ESXi server/s must have the same time source as the guest systems. This is because when starting a VM, the time of the host is set in the VM by default.

For the central time synchronization it is recommended to use a SICLOCK or another dedicated NTP server.

The following figure illustrates the configured time synchronization of an ESXi server. 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. The time synchronization of the VM with the ESXi server must be therefore deactivated.

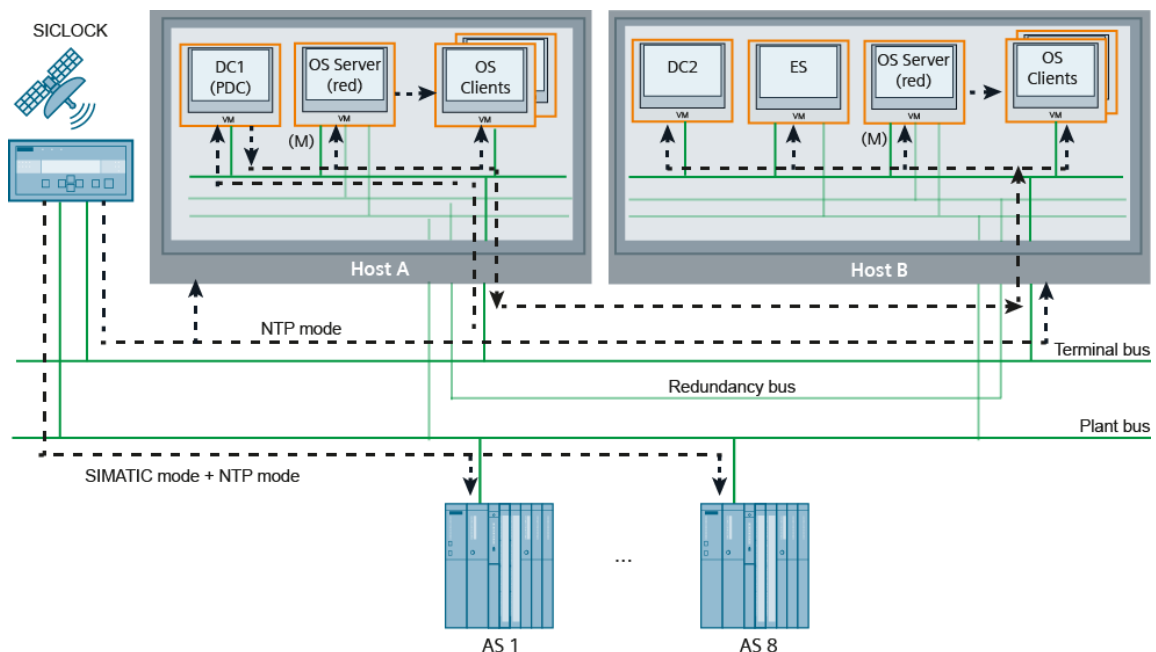
The following two scenarios are examples of the time synchronization of a virtual PCS 7 environment. For further information on the time synchronization of a PCS 7 system and its possibilities, please refer to the manual "[SIMATIC PCS 7 Process Control System Time synchronization](#)".

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 server) are synchronized directly from the central clock of the system 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, for instance, via SICLOCK TC 400. 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 one domain. This example based on chapter 3.8.2 "Network environment in one domain" in the manual "[SIMATIC PCS 7 Process Control System Time synchronization](#)".

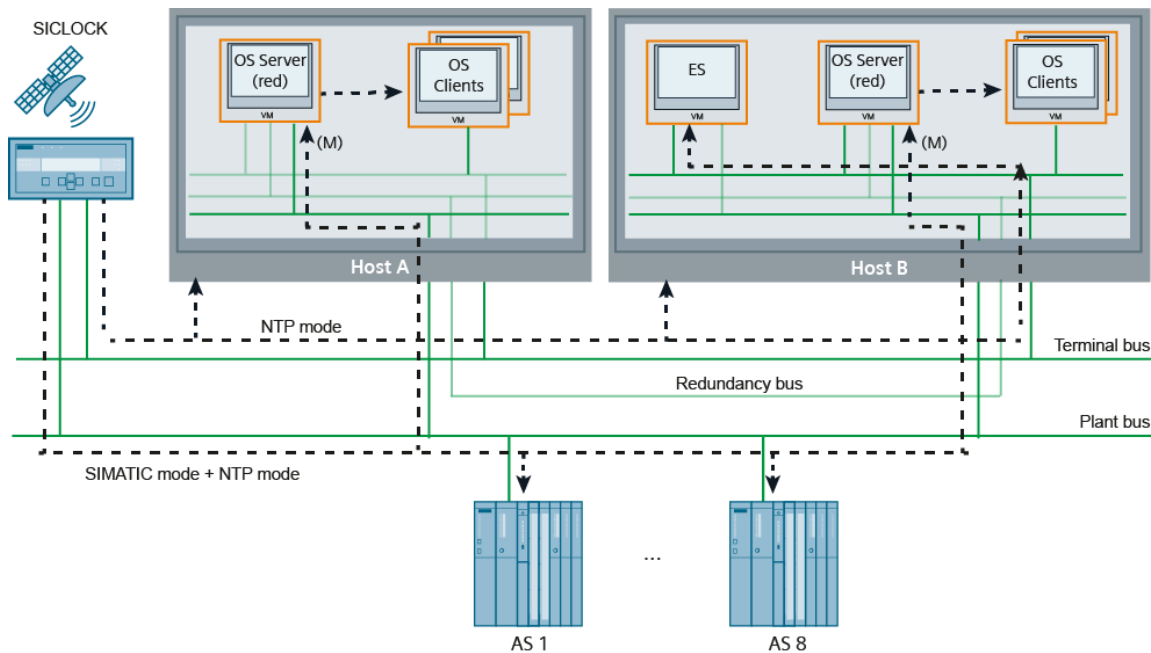


Time synchronization in a workgroup

Time synchronization in a workgroup proceeds as follows:

- Time synchronization on the terminal bus
The ES and the hosts (ESXi server) are synchronized by the central plant clock via the NTP process.
The OS clients receive the clock time from an OS server. OS clients only receive the clock time from such OS servers, from which they also have downloaded the server data.
- Time synchronization on the plant bus
The systems on the plant bus are synchronized, for instance, via SICLOCK TC 400. The synchronization processes depend on the type of CPU or CP of the automation system and the network configuration.

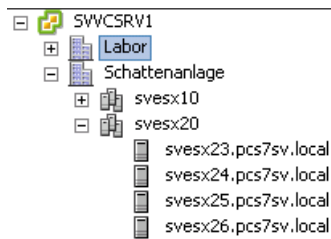
The following figure illustrates an example of a virtual configuration for a network environment in a workgroup. This example based on chapter 3.8.3 "Network environment in one workgroup" in the manual ["SIMATIC PCS 7 Process Control System Time synchronization"](#).



4.1.4 DNS and routing

Note

If you operate your ESXi servers in a cluster, the ESXi servers must be registered in the cluster with their DNS name. To do this, the system must be able to connect to a DNS server in the network.



The following figure shows the DNS and routing configuration of an ESXi server.

svesx23.pcs7sv.local VMware ESXi, 5.5.0, 2456374

Summary | Virtual Machines | Performance | **Configuration** | Tasks & Events | Alarms | Permissions | Maps

Hardware

- Processors
- Memory
- Storage
- Networking
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

Software

- Licensed Features
- Time Configuration
- DNS and Routing

DNS and Routing

Host Identification

Name	svesx23
Domain	pcs7sv.local

DNS Servers

Method	Static
Preferred DNS Server	172.14.24. [redacted]
Alternate DNS Server	10.116.82. [redacted]

Search Domains

pcs7sv.local

Default Gateways

VMkernel	10.116.82. [redacted]
VMkernel IPv6	

4.2 Configuration of the guest system

4.2.1 General information

Properties	Requirements
VM version	From PCS 7 V8, use version 8 or "vmx 09"
Hard disk memory management	Use the type: "Thick Provision Eager Zeroed"
Virtual network groups	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 3 virtual network adapters.
Disconnection of networks	It is recommended to virtually/physically disconnect the terminal, system and redundancy bus and to refrain from using any VLANs. The IP addresses of the terminal, system 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 lies between 70% and 80%.
VMware tools	The VMware tools must be installed within the virtual machines. This results in improved performance and maintainability of the VMs.
Operating modes	Suspending/Resuming the VMs as well as VMware options, such as vMotion are not supported. The VMs must be treated as if they were real OS stations.

CAUTION

Adapter type of the virtual network adapter

The adapter type of the virtual network adapter for the plant bus must be "E1000".

The map type of the virtual network adapter for the terminal or redundancy bus may be either "E1000" or "vmxnet3" (recommended). 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 to its default settings.

Remove any unneeded hardware, e.g.:

- HD audio
- Floppy disk drive
- Network adapters

The following table shows you the minimal VM configuration by means of [PCS 7 V8.2 Readme](#), chapter "3.3.1.1 Recommended PC hardware configuration".

	Hard disk (thick)	Virt. cores	RAM [GB]
OS client, Batch client, Route Control client	C:\ 100GB	2	4
ES	C:\ 100GB	4	6
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	C:\ 100GB	2	6

You can find the accepted operating systems in the [PCS 7 V8.2 Readme](#), chapter "3.4.1.1 Approved operating systems". It is recommended to only use 64 bit operating systems.

The configuration of the Process Historian / Information Server is based on the project requirements and on the manual "[Process Historian 2014: Administration](#)".

Note

For the configuration of the Process Historian/Information Server you need to specifically consult the [Technical support](#).

4.2.2 Configuration of the network adapters

CAUTION**Interrupted process communication**

- In 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.
- The order of network adapters changes in Windows after adding/removing them. After performing changes to the network configuration, ensure that the order of network adapters matches that in the PCS 7 documentation.

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 standard type from "Not configured" to "Private".

Note

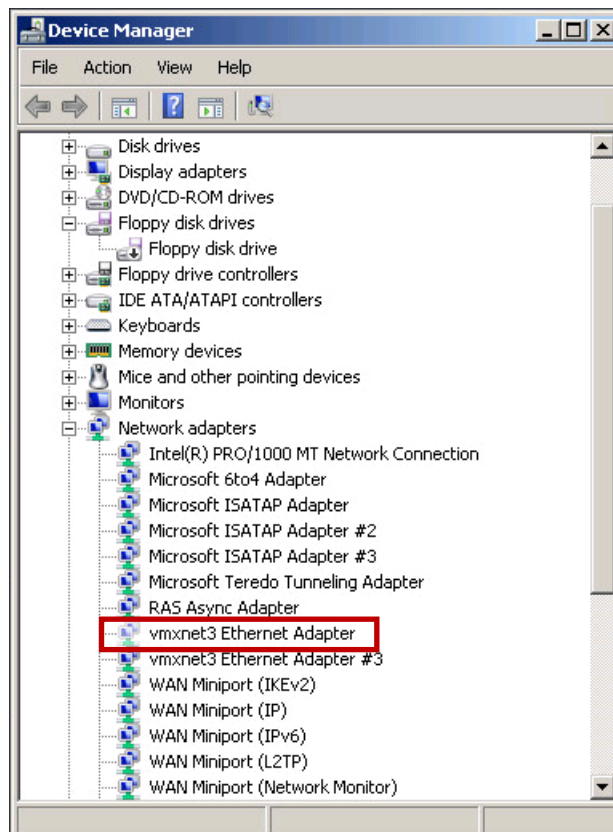
First uninstall all unused network adapters from the Windows device manager. Otherwise "residual files" will remain in the VM properties in Windows after deleting the network adapters. These "residual files" must be made visible in the device manager before they can be uninstalled. If these "residual files" are not removed, the name of the network adapter you removed cannot be used again.

Tip: BGInfo (not included with Windows) can be used to show you on the desktop if "residual files" are present.

Procedure to uninstall "residual files":

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 or on removable media. If you want to undo changes, you can import the backup copy.

1. Open the registration editor by clicking the "Start" button in Windows, type "regedit" in the search box and press the ENTER key. If your administrator password or confirmation is required, enter your password or confirm the dialog that appears.
2. Set the following registry keys
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment]
"devmgr_show_nonpresent_devices"="1"
"devmgr_show_details"="1"
3. Open the device manager and activate the option "View > Show hidden devices".
4. Uninstall the grayed out network adapters from the shortcut menu without deleting the driver software.



Checking the configuration

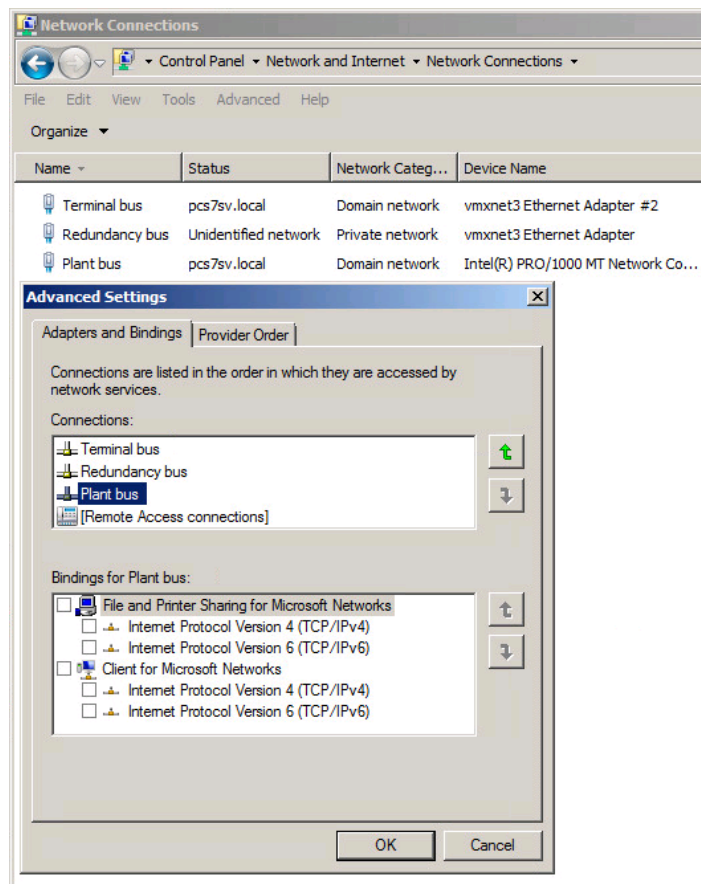
Check whether the following requirements have been fulfilled:

- There are no unused network adapters.
- The network adapters are in the correct order.
- No network adapter is in the public network.
- The network adapter E1000 is assigned to the plant bus. In Windows, this network adapter type is displayed as "Intel® PRO/1000 MT..."
- Unneeded network protocols have been removed.

This is done from the "Network and Sharing Center".

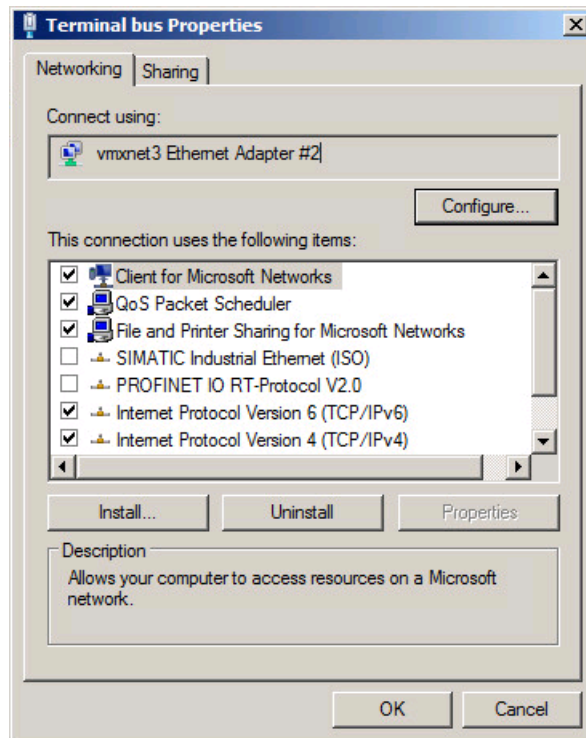
The figure below shows the following:

- There are no unused network adapters.
- The network adapters are in the correct order:
 1. Terminal bus
 2. Redundancy bus
 3. Plant bus
- The network adapters are in the "Domain network" or in the "Private network".
- The network adapter E1000 is assigned to the plant bus. In Windows, this network adapter type is displayed as "Intel® PRO/1000 MT..."
- Unneeded protocols have been deactivated for the plant bus. The same setting must be made for the redundancy bus.



Note

The "Internet Protocol Version 6 (TCP/IPv6)" may not be deactivated for the terminal bus.



4.2.3 Licensing

With regard to licensing, the installation on a virtual machine does not differ from the 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 of PCS 7 in a virtual environment occurs via BCE, you have to use the appropriate licenses for SIMATIC NET (see ch. 6.3.6).

When operating the regional SIMATIC PCS 7 OS software ASIA, a USB Hardlock is required for license verification. Further related information is available in the following FAQ article:

[How do you integrate a USB hardlock in a virtual environment in PCS 7 ASIA?](#)

4.3 Configuration examples

4.3.1 Configuration of the VMs

ES, OS server, Batch server/RC server

Hardware	ES	OS server	Batch server / RC server
Guest OS	Windows 7 SP1 Enterprise 64Bit	Windows Server 2008 R2 SP1 Standard	
VM version	vmx-09		
RAM [GB]	≥ 6		
Virt. cores	≥ 2		
Video memory	36 MB		
Hard disk 1: System [GB] (SCSI, thick)	100	100	
Hard disk 2: Data ¹⁾ [GB] (SCSI, thick)	50	20	
Hard disk 3: Batch data ²⁾ [GB] (SCSI, thick)	None		10
Network adapter 1 (VMXNET 3)	Terminal bus		
Network adapter 2 (E1000)	Plant bus		
Network adapter 3 (VMXNET 3)	Not available	Redundancy bus	

- ¹⁾ The memory for the data partition must be adapted to the project requirements.
- ²⁾ The batch database must lie on separate memory (if possible a dedicated SSD hard disk/SSD RAID array).

OS client / Batch client / RC client, PCS 7 Web server

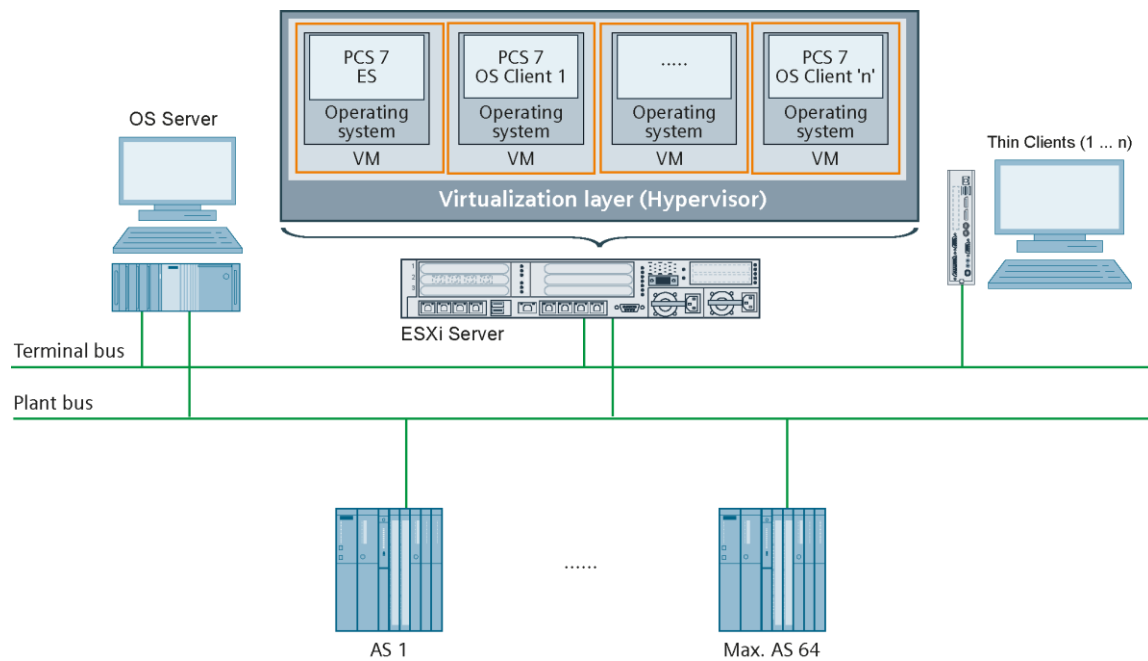
Hardware	OS client / Batch client / RC client	OpenPCS 7	Datamonitor server / PCS 7 Web server
Guest OS	Windows 7 SP1 Enterprise 64Bit		Windows Server 2008 R2 SP1 Standard
VM version	vmx-09		
RAM [GB]	4 ²⁾	6	
Virt. cores	2		
Video memory	36 MB ³⁾	36 MB ³⁾	
Hard disk 1: System [GB] (SCSI, thick)	100	100	
Hard disk 2: Data ¹⁾ [GB] (SCSI, thick)	10	20	
Network adapter 1 (VMXNET 3)	Terminal bus		

- ¹⁾ The memory for the data partition must be adapted to the project requirements.
- ²⁾ If the OS client, Batch client and RC client run on the same VM, you should allocate at least 6GB of RAM.
- ³⁾ If you operate within a virtual OS client Multi monitoring, note the following FAQ: <https://support.industry.siemens.com/cs/ww/en/view/109483016>

4.3.2 Configuration 1

- 1x virtual ES
- Virtual OS clients (1...n)
- 1x real OS server
- Thin clients (1...n)
- Automation systems (AS 1...max AS 64)

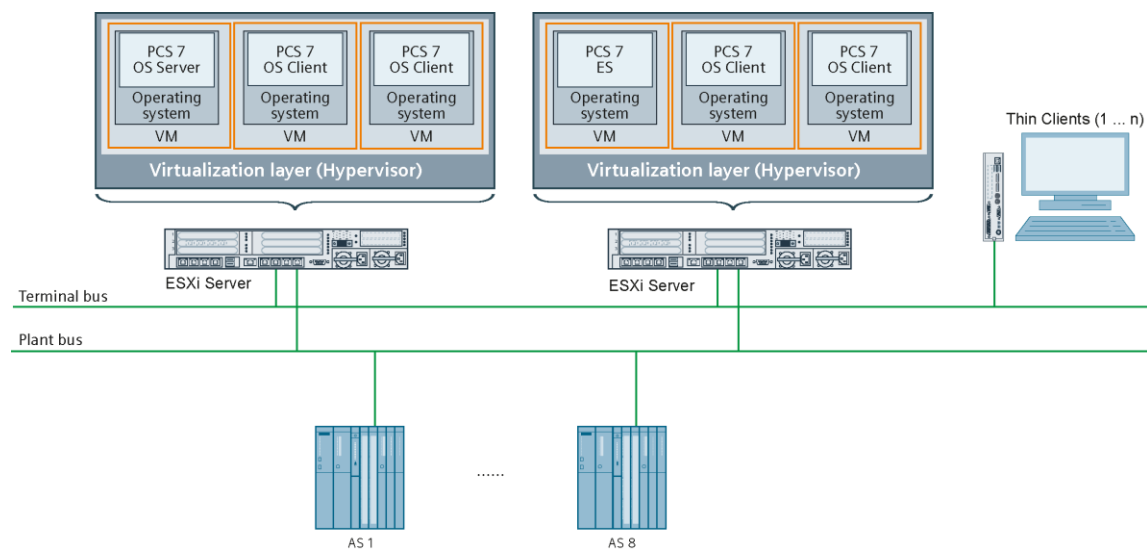
In this configuration, the communication to the AS occurs from a physical OS server, i.e., via CP1623/28.



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)

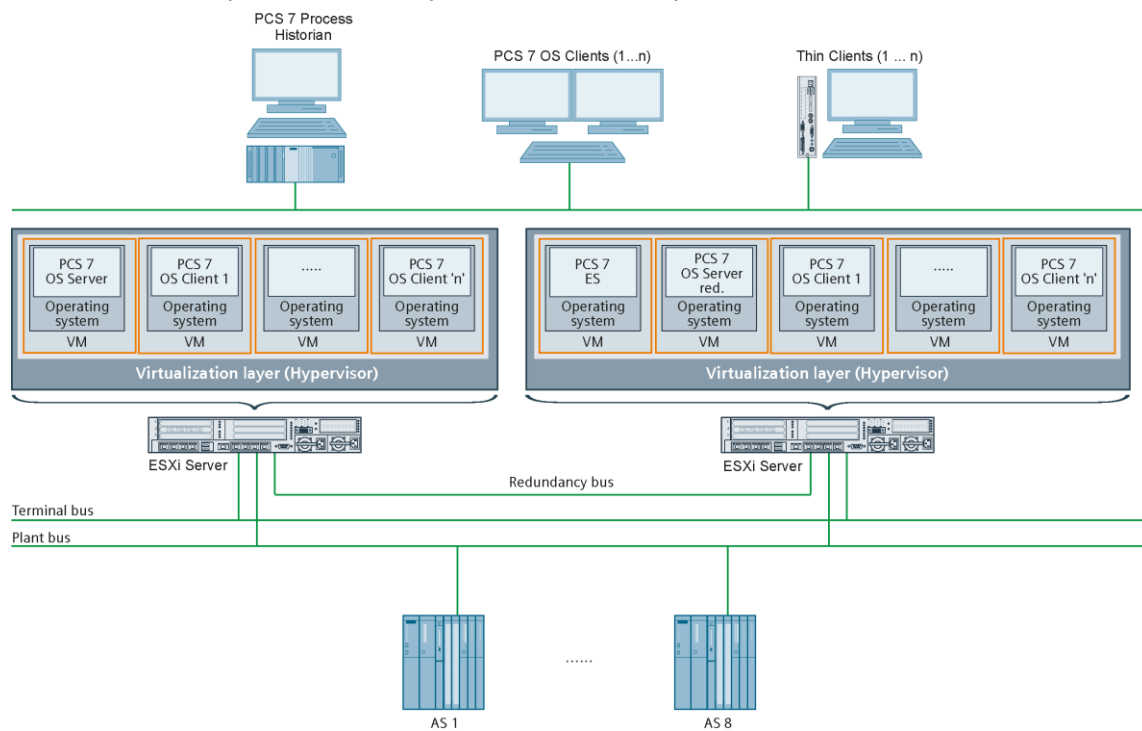
The ES, OS server and OS clients were virtualized in this configuration. The communication to the AS passes over a standard network adapter, i.e., BCE. Since there is only one OS server in this example, you do not need a redundancy bus.



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.



4.4 Remote access

The VMs are accessed with a thin client or a remote system by means of RDP, RealVNC, vSphere client or vSphere web client.

General

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 [PCS 7 V8.2 Readme](#), chapter "3.4.17 Remote service and remote control".
- Remote Desktop may only be used via "mstsc /console" or "mstsc /admin".
- An RDP connection may only be used for accessing OS clients, BATCH clients, Route Control clients and clients without additional functions.
- When using an RDP connection in a VM, you have to configure the automatic Windows login in it, for instance with "control userpasswords2" or "Autologon for Windows" (Windows Sysinternals). You should never write the login data in the registry, under any circumstance.
- Deactivating the TCP auto tuning level: The TCP auto tuning settings can be deactivated with the following command:

```
netsh interface tcp set global autotuninglevel=disabled
```

You can find additional information in the FAQ article: [Which settings should you make when an OVF export fails using the "VMware vSphere Client" application?](#)

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.de/kompatool>

vSphere client

It can take relatively long (35 sec) to open the console ("Open Console") of a VM in the vSphere client. This could happen if the certificates could not be verified due to a lack of Internet connection. To prevent this, configure the following Group Policies:

Set "Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Automatic Root Certificates Update" to "enabled".

5 User scenarios

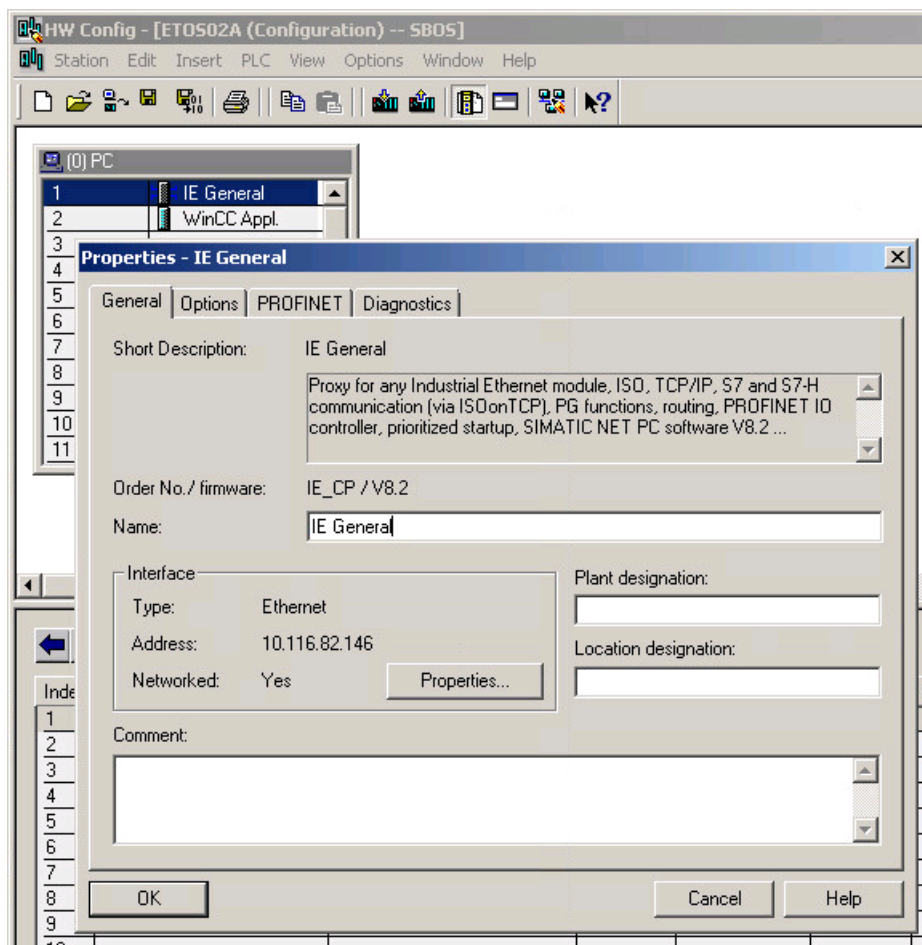
An important difference to real PCs is that the VMs (ES, OS server, OS client, etc.) are accessed via remote connection by means of a thin client or a remote system.

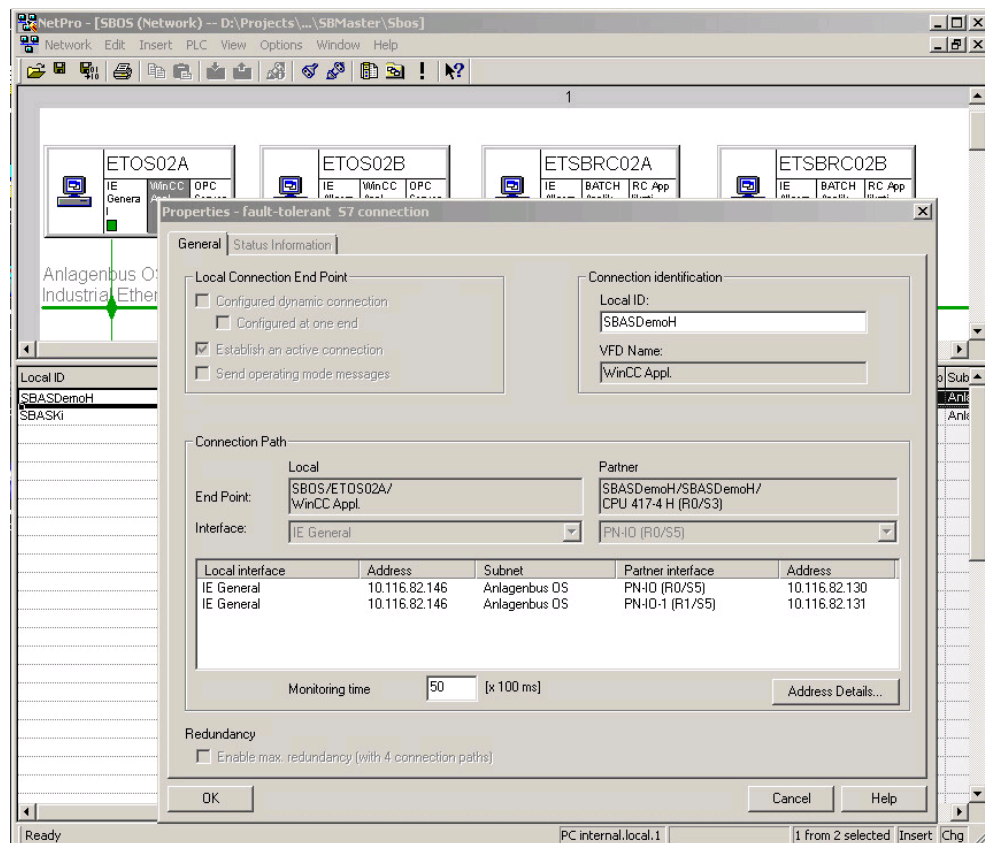
5.1 Engineering functions

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 HW Config with a configured "IE General" in an OS server and its configured high-availability connection in NetPro.





Download 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.

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

Virtual machines are regarded as third-party systems and are therefore not explicitly configured in the OPC server of the Maintenance server.

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

The screenshot shows the ETOS02B maintenance client window. On the left, there is a status indicator 'Good' with a green square icon and a 'Comment' text area. On the right, a table displays various device attributes:

HID/TAG	ETOS02B	●
LID	ETOS02B	●
Address	10.116.82.12	●
Description	---	
Message	---	
Device type	VMware Virtual Platform	●
Manufacturer	VMware, Inc.	●
Order number	4 11 a2 cc eb ae-63 9d 83 fa c2 d7 2d 60	●
Serial number	None	●
Installation date	2015-06-29 13:46:43	●
HW revision	None	●
SW revision	6.00	●
Last update	2015-09-10 15:02:25	●

Note PCS 7 doesn't currently offer the possibility of showing the diagnostics data of an ESXi host server in the Maintenance system (Asset Management)

Virtual ES as a Maintenance client

The applications SNMP, SIMATIC PDM and SIMATIC IPC DiagMonitor are installed on the virtual ES.

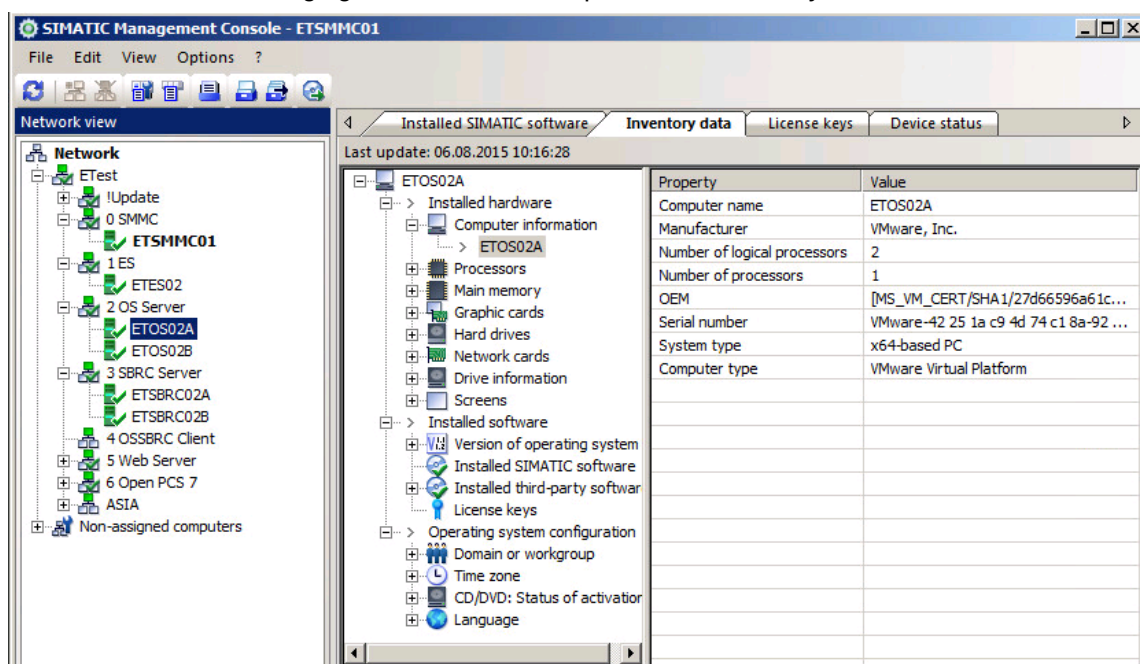
These enable the following functions:

- 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 HTTP
- Display diagnostics data of an IPC via the "Diagnose Web Server" functionality (access via the faceplate of the IPC)
- Display IPC diagnostics data by means of the "Management Explorer" (SIMATIC IPC DiagMonitor)

5.4 SIMATIC Management Console (SMMC)

The SMMC was installed as a separate VM. The SIMATIC Management Agent must be installed on all the stations you want to manage. This can be installed as part of the system setup or separately. The users that are permitted access via SMMC must be also entered in the "SIMATIC Management Users" group.

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



6 Notes / constraints

6.1 SIMATIC Batch

CAUTION	Limited plant availability The batch database, and only this, must be stored on dedicated memory. 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

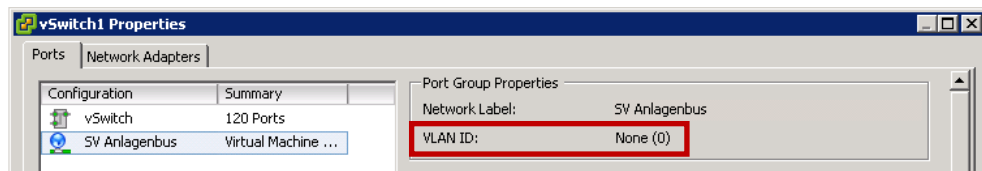
All modules used in the ESXi server, whether by themselves or combined, must be listed in the VMware compatibility list (<http://www.vmware.com/go/hcl>) and approved for the corresponding version of VMware vSphere.

6.3 Communication

6.3.1 VLANs

VLANs can be used in PCS 7. You can find additional information in the FAQ article "[How do you configure a Virtual Local Area Network \(VLAN\) in PCS 7?](#)"

CAUTION	Fault in process communication It is only allowed to use VLANs on the plant bus in a virtual environment if you follow the instruction in chapter 4 of the manual "SIMATIC NET PC software SIMATIC NET PC Software V13" and keep the described setting "VLAN ID: None (0)".
----------------	--



6.3.2 Redundant plant or terminal bus

CAUTION Interrupted process communication

No redundant plant bus may be used when communication is transmitted over BCE (standard network adapter).

It is not permitted to use a redundant plant or terminal bus in a virtual environment.

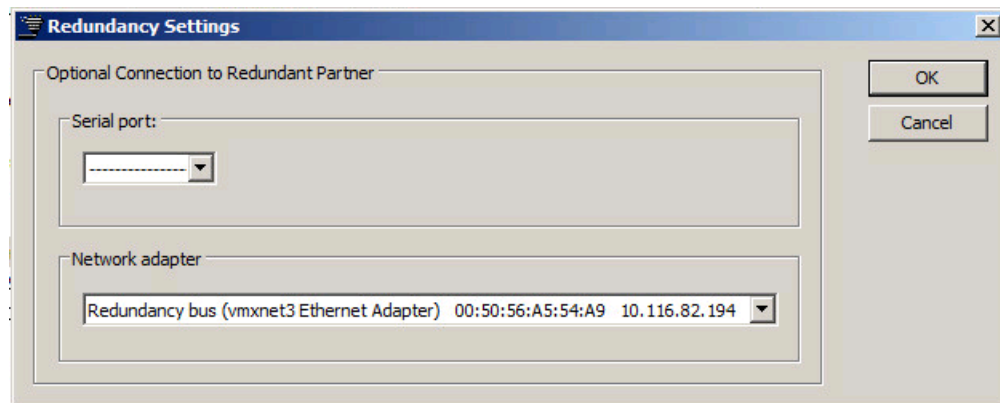
Irrespective of the recommendation in chapter "4.1.2 Network", it must be connected to the virtual terminal and virtual plant bus with two physical network adapters on the real terminal and real plant bus.

6.3.3 Redundancy connection between servers

Redundant OS servers, Batch servers or RC servers for redundancy synchronization must be connected via Ethernet. A serial connection (RS 232) was not included.

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 serial ports



6.3.4 Name resolution

In a virtual environment, even 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 ESXi server.

Note

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

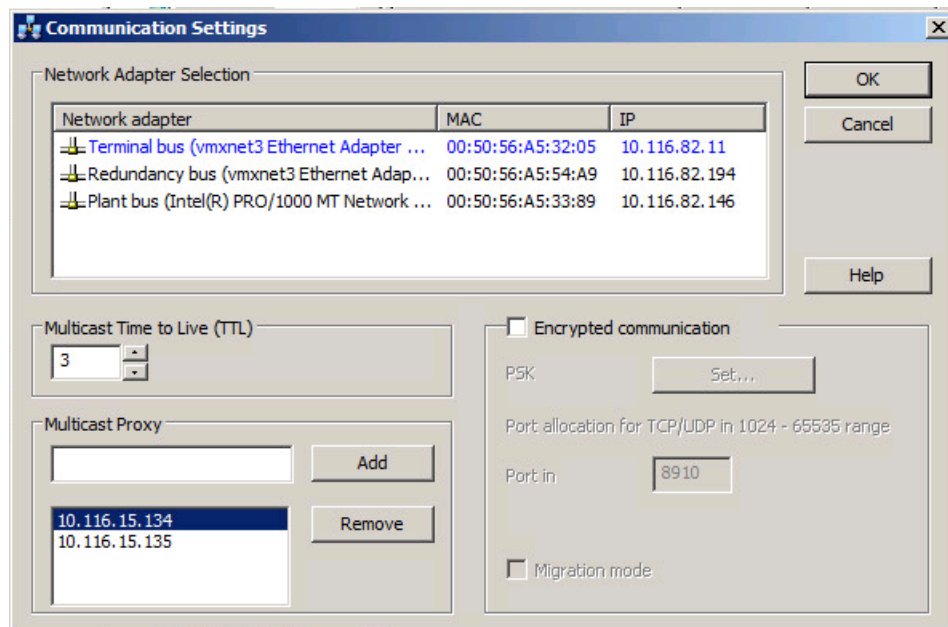
The name resolution must take place over the IPv4 protocol.

6.3.5 Communication over multiple subnets

If the communication on the terminal bus takes place outside the network boundaries, the SIMATIC shell must be configured accordingly. This is independent of the virtualization.

The following figure shows:

- The selected virtual network adapter for the terminal bus
- The selected multicast service life
- The selected Multicast proxy PC in another subnet. These should be OS servers present in the other subnet. The configuration must be done in a similar manner on these OS servers.
- The IP addresses of terminal, plant and redundancy bus are in the various subnets, e.g.:
 - Terminal bus: 10.116.82.0/25
 - Plant bus: 10.116.82.128/26
 - Redundancy bus: 10.116.82.192/26



6.3.6 Communication with the AS

Principle

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

Note

It is not recommended to operate the CP1623/28 in the ESXi server using the so called "passthrough process".

Licenses for PCS 7 PCS 7 V8.2

Communication	License packages	Order number	Licenses
≤ 8 AS	SIMATIC PCS 7, SOFTWARE, BCE V8.2	6ES7650-1CD28-2YB5	
	SIMATIC NET SOFTNET-IE S7 LEAN V13	6GK1704-1LW13-0AA0	SOFTNET-IE S7 Basic SOFTNET-IE S7 Lean
> 8 AS	SIMATIC NET SOFTNET-IE S7 V13	6GK1704-1CW13-0AA0	SOFTNET-IE S7 Basic SOFTNET-IE S7 Lean SOFTNET-IE S7 Power Pack
H stations	SOFTNET-IE S7 REDCONNECT V13 VM	6GK1704-0HB13-0AA0	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 "SIMATIC NET SOFTNET-IE REDCONNECT VM" V8.2 or higher to V13, you can use the license "SIMATIC NET IE SOFTNET-S7 REDCONNECT VM UPGRADE" (Order number: 6GK1704-0HB00-3AE0).
- Only the license and not(!) the software, "SIMATIC NET SOFTNET-IE V13" can also be used for PCS 7 V8.2.

Note

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

Monitoring times

CAUTION Interrupted process communication

Sufficient monitoring times must be configured for high-availability S7 connections over TCP/IP. The default monitoring time of 500ms (of CP1623) is not enough! The times to be configured depend on the number of connections, but no less than 5s.

You can find information about monitoring times in the FAQ ["What are the quantity frameworks and performance data of each of the SIMATIC NET products?"](#) under "Performance data and quantity frameworks for products of SIMATIC NET PC software V13", chapter 7 "IE S7 REDCONNECT quantity framework".

The figure below shows a selected monitoring time of 5 s. Please note that if the factor is 100 ms, the default setting is 500 ms.

Properties - fault-tolerant S7 connection

General | Status Information

Local Connection End Point

- ☐ Configured dynamic connection
- ☐ Configured at one end
- ☒ Establish an active connection
- ☐ Send operating mode messages

Connection identification

Local ID: SBASDemoH

VFD Name: WinCC Appl.

Connection Path

Local			Partner	
End Point:	Interface:		End Point:	Interface:
SBOS/ETOS02A/ WinCC Appl.	IE General		SBASDemoH/SBASDemoH/ CPU 417-4 H (R0/S3)	PN-IO (R0/S5)

Local interface	Address	Subnet	Partner interface	Address
IE General	10.116.82.146	Anlagenbus OS	PN-IO (R0/S5)	10.116.82.130
IE General	10.116.82.146	Anlagenbus OS	PN-IO-1 (R1/S5)	10.116.82.131

Monitoring time: 50 [x 100 ms]

Address Details...

Redundancy

- ☐ Enable max. redundancy (with 4 connection paths)

OK Cancel Help

Communication via subnets

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 configuring steps are required:

1. In NetPro, enter a router on the OS as a gateway for the "IE General".
2. In NetPro, enter a router as gateway on the AS for the CP443-1 or on the internal interface of the CPU.
3. On the OS server in Windows, enter the router configured in NetPro on the OS for the "IE General" as a standard gateway for the plant bus.
4. On the OS server and the ES for Windows, enter the routes to the AS, e.g. with "route add -p ..."

6.4 New VMs/templates/clones

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
- Creating 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

Requirements when adding new VMs

- The source VM or the template may only contain the operating system and never a 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 PCS 7 installation

VMware features

- You are not permitted to suspend/resume VMs.
- You are not permitted to use snapshots, especially during PCS 7 runtime operation.
- You are not permitted to use vMotion, especially during the engineering phase and the PCS 7 runtime operation.
- HA, DRS and FT were not taken into consideration in this application example. They are also not approved for use in the virtual PCS 7 environment.

6.5 Dual-monitor

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.

Further related information is available in the following FAQ articles:

- [How do you extend the display of a virtual machine to other monitors?](#)
- [How do you operate Multi Monitoring with a virtual OS Client?](#)

6.6 Chipcard reader

It is possible to connect a chipcard reader to a thin client via USB. This thin client is then connected to an OS client via RDP.

You can find additional information in the FAQ article: "[How do you utilize a Chip Card Reader in a virtual operating environment?](#)".

6.7 S7 F/FH systems

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

You can find additional information in the FAQ article "[What are the requirements for S7 F/FH systems in virtual environments and for remote access?](#)".

6.8 Diagnostics

Diagnostics with VMware vSphere client

It is recommended to monitor the resources of the hosts and guest systems regularly with the vSphere client, for instance:

- Utilization of the work memory
- Operating mode
- CPU load
- Hard disk
- Network utilization

CPU use of the guest system

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

The following figure shows an ES with increased CPU load:

- During OS compiling (at approx. 14:22)
- During the publishing of pictures (from approx. 14:30)

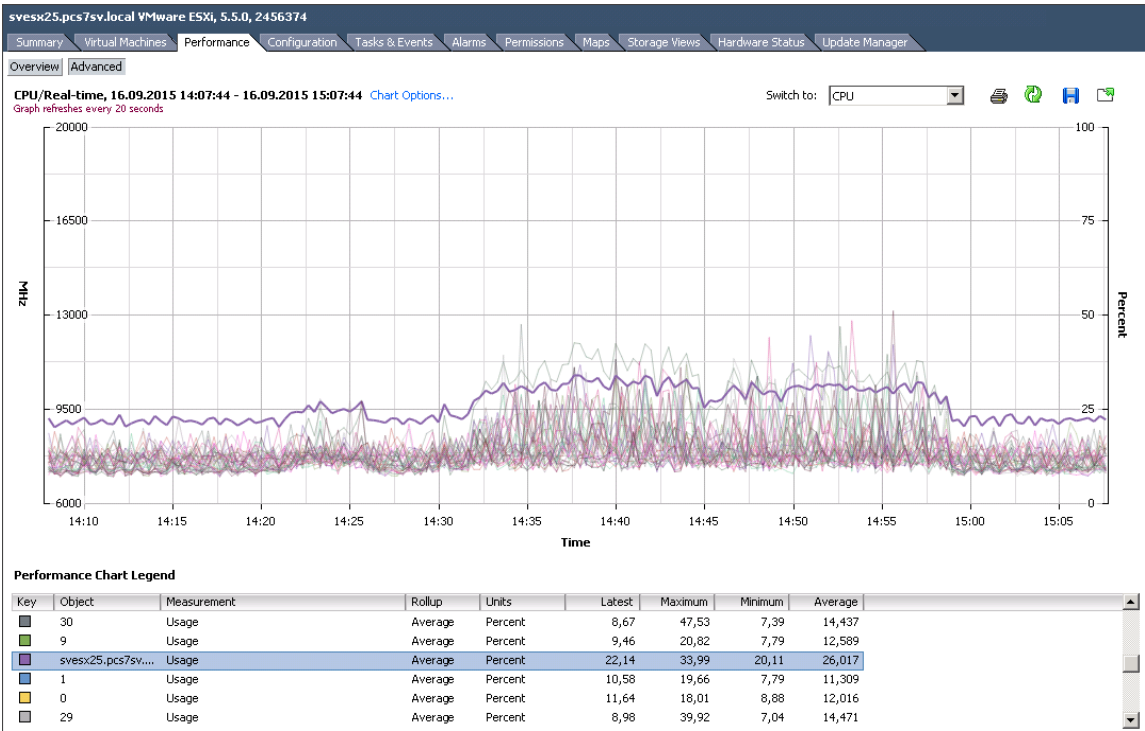


If the CPU load sticks to around 100% for an extended period, the host generates a warning followed an error message. The message disappears automatically after completion. The task is completed without errors.

An error is displayed in the default setting if a CPU load of 75 % persists for longer than 5 min.

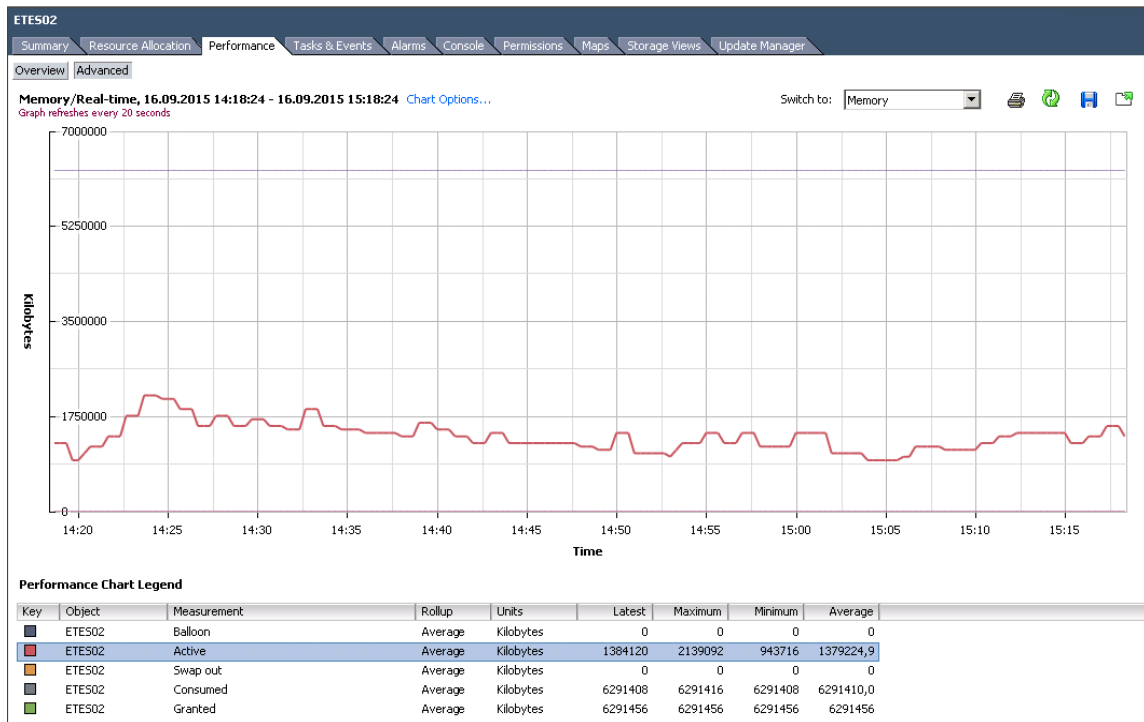
An alarm message is displayed in the default setting if a CPU load of 90 % persists for longer than 5 min.

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



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, you either need to add more RAM to the ESXi server or switch off VMs on this server. The host then attempts to compensate resource constraints.
- The values "Granted" and "Consumed" are identical because in this instance, the entire configured RAM of the VM was reserved.



7 Glossary

Guest

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

Host

A host is the real hardware on which the ESX or ESXi server runs. The host also provides its resources to the virtual machines.

The computers running within the host are called guests or VMs.

Hyper threading

Hyper threading is a technology that improves the processing of commands by the CPU. The CPU core appears externally as two process cores.

Virtual CPU cores

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

Virtual hardware

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

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

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

VMware is a company and manufacturer of virtualization software.

VMware ESX and ESXi

The VMware ESX server or VMware ESXi server are a core component of VMware vSphere. They correspond to a hypervisor Type 1.

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 Hypervisor type 1.

VMware vSphere client

VMware vSphere Client forms part of VMware vSphere and enables access to the vCenter server or ESX server. This makes it the tool for virtual infrastructure administration.

VMware workstation

This is a hypervisor type 2 and serves for the generation and administration of virtual systems on an operating system that already exists.

8 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 at:

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

Industry Online Support App

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

Phone: <https://support.industry.siemens.com/cs/ww/en/sc/2067>

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. You send queries to Technical Support via Web form: www.siemens.com/industry/supportrequest.

Range of services

Our range of services includes, inter alia, the following:

- Product trainings
- 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:

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

Contact partners

If you want to request on-site service or need spare parts, please get in touch with your local Siemens representative, who will put you in contact with the responsible service center. You can find your contact partner in the contact database:

www.siemens.com/yourcontact

9 Appendix

9.1 Related literature

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of this entry - Manual https://support.industry.siemens.com/cs/ww/de/view/109739973
\2\	Downloadseiten des Beitrages: - Handbuch: https://support.industry.siemens.com/cs/ww/en/view/109739973 - Overview to the topic „PCS 7 Virtualization“: https://support.industry.siemens.com/cs/ww/en/view/51975791
\3\	Release of SIMATIC PCS 7 V8.2 system components for virtual operating environments https://support.industry.siemens.com/cs/ww/en/view/109737952
\4\	SIMATIC PCS 7 OS Software Client V7.1 + SP2 and higher released for use in virtual operating environments https://support.industry.siemens.com/cs/ww/en/view/51401737

9.2 History

Version	Date	Modifications
V1.0	10/2016	First version