

Experion PKS  
Virtualization Planning and Implementation Guide

EPDOC-X147-en-431A  
February 2015

**Release 431**

Document	Release	Issue	Date
EPDOC-X147-en-431A	431	0	February 2015

## Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2015 - Honeywell International Sàrl

# Contents

<b>About this guide .....</b>	<b>7</b>
<b>Getting started with Experion virtualization .....</b>	<b>11</b>
Task overview for preparing an Experion virtualization environment .....	13
<b>Planning for a DCS architecture .....</b>	<b>17</b>
Example DCS architecture virtualization scenario .....	18
DCS architecture options in a virtualized environment .....	19
Example DCS architecture in a virtualized environment with non-redundant management network .....	22
Example DCS architecture in a virtualized environment with redundant management network .....	24
Example DCS architecture in a virtualized environment with separate management network .....	26
Overview of distributing workload across ESXi hosts for a DCS architecture .....	29
<b>Planning for a SCADA architecture .....</b>	<b>31</b>
Example SCADA architecture virtualization scenario .....	32
Example SCADA architecture in a virtualized environment .....	33
Overview of distributing workload across ESXi hosts for a SCADA architecture .....	34
<b>Planning for off-process usage .....</b>	<b>35</b>
<b>Planning the virtualization environment .....</b>	<b>37</b>
Determining the number of ESXi hosts and hardware requirements .....	38
Host CPU requirements .....	40
Host memory requirements .....	41
Storage requirements .....	42
Network requirements for a DCS architecture .....	44
Network requirements for a SCADA architecture .....	50
Identifying virtualization hardware and software requirements .....	53
Software requirements .....	53
Thin client requirements .....	54
Other requirements .....	54
Planning for the management ESXi host and management network .....	56
Planning the management network in a DCS architecture .....	58
Planning the management network in a SCADA architecture .....	59
Planning how to organize the vCenter Server .....	61
VMware inventory objects .....	61
Datacenter organization guidelines .....	61
Planning for time synchronization .....	63
Planning to maintain the VMware environment .....	65
About vSphere Update Manager .....	65
Considerations for VMware maintenance when using local storage .....	66
Considerations about upgrades, patches, and updates .....	66
Planning security for the VMware environment .....	67
User accounts, roles, and permissions .....	67
About host lockdown mode .....	68
About VMware security hardening .....	68
Planning to backup the virtual infrastructure and virtual machines .....	70
Planning for disaster recovery .....	71
Planning to replicate the virtual machines .....	72

<b>Implementing networks for a DCS architecture .....</b>	<b>75</b>
Implementing a non-redundant management network for a DCS architecture .....	76
Implementing a redundant management network for a DCS architecture .....	81
Implementing a separate management network for a DCS architecture .....	86
<b>Implementing networks for a SCADA architecture .....</b>	<b>93</b>
Preparing a gateway router for a SCADA architecture .....	94
Preparing the production network for a SCADA architecture .....	95
Configuring the virtual production network for a SCADA architecture .....	96
Implementing the management network for a SCADA architecture .....	97
<b>Implementing shared storage networks .....</b>	<b>99</b>
About shared storage .....	100
Redundancy for physical SANs .....	101
Distributing datastores and volumes across storage networks .....	102
Preparing the storage network .....	104
Configuring the storage area network .....	105
Configuring redundancy across multiple physical SANs .....	106
Setting up vDR for volume 1 .....	106
Setting up asynchronous replication for volume 2 .....	106
<b>Preparing a management ESXi host .....</b>	<b>107</b>
Configuring the ESXi host local disk array .....	109
Configuring the ESXi host BIOS settings .....	110
Installing the ESXi software on a host .....	111
Configuring the ESXi host network settings .....	112
Network configuration for a management host in a DCS architecture .....	113
Network configuration for a management host in a SCADA architecture .....	113
Configuring NIC teaming .....	114
Configuring the virtual switch port security settings .....	115
Configuring ESXi host time synchronization .....	116
Adding and renaming datastores .....	117
Preparing a vCenter Server .....	118
Creating a vCenter Server virtual machine with bundled SQL .....	119
Configuring the vCenter Server .....	124
Installing the Experion virtual machine utility .....	125
Organizing VMware inventory objects .....	125
Adding the ESXi host to the vCenter Server .....	126
Configuring the virtual machine load order on the management ESXi host .....	127
Configuring security in a vCenter Server .....	128
Creating vCenter roles and assigning privileges .....	128
Assigning vCenter roles to Experion users or global groups .....	128
Configuring host lockdown mode .....	129
<b>Preparing a production ESXi host .....</b>	<b>131</b>
Configuring the ESXi host local disk array .....	132
Configuring the ESXi host BIOS settings .....	133
Installing the ESXi software on a host .....	134
Configuring the ESXi host network settings .....	135
Network configuration for a production host in a DCS architecture .....	136
Network configuration for a production host in a SCADA architecture .....	139
Configuring NIC teaming .....	142
Configuring the virtual switch port security settings .....	143
Configuring ESXi host time synchronization .....	144
Adding the ESXi host to the vCenter Server .....	145
Domain name resolution .....	146

Creating and managing virtual machines .....	147
<b>Administering the virtualization environment .....</b>	<b>149</b>
Replicating a virtual machine .....	150
Virtual machine replication pre-requisites .....	152
Preparing the virtual machine for replication .....	154
Preparing the vCenter Server for virtual machine replication .....	156
Restoring and recovering a replicated virtual machine .....	161
Patching or upgrading the VMware environment .....	163
Downloading the patches or upgrades .....	164
Importing the patches or upgrades into Update Manager .....	165
About baseline and compliance views .....	166
Remediating patches and upgrades .....	166
Remediating target objects using Update Manager .....	168
Remediating target objects manually .....	169
Upgrading Virtual Hardware and VMware tools versions .....	172
Upgrading virtual infrastructure software .....	173
Maintaining hardware devices in a virtualization environment .....	176
Maintaining the level 2.5 router .....	176
Monitoring the virtualization environment .....	178
About resource usage .....	178
About system status .....	180
<b>Notices .....</b>	<b>183</b>
Documentation feedback .....	184
How to report a security vulnerability .....	185
Support .....	186
Training classes .....	187



# About this guide

This guide provides high-level guidance on how to implement a virtualized Experion environment.

## Revision history

Revision	Date	Description
A	February 2015	Initial release of document.

## Intended audience

This guide is for people who are responsible for planning, installing, and configuring VMware and Experion components in a virtualized Experion environment. Use this guide as your starting point for virtual platforms other than the BladeCenter S.

To plan and implement a deployment with the BladeCenter S, use the *Virtualization with BladeCenter S Guide*.

## Prerequisite skills

It is assumed that you have familiarity with the Microsoft Windows operating systems that are supported for the relevant Experion release. You should also have some experience with Experion node installations.

If you are unfamiliar with virtualization technologies, Honeywell recommends that you read the Honeywell whitepaper, *Virtualization Reduces the Cost of Supporting Open Industrial Control Systems*. This whitepaper is available from the Honeywell Process Solutions website (<http://www.honeywellprocess.com/>):

1. Login to the Honeywell Process Solutions website <http://www.honeywellprocess.com/>.
2. In the **Resources** column at the bottom of the page, click **Whitepapers**.
3. In the **Enter search terms** box, type **virtualization**.
4. Click **Search**.

The **Whitepaper Search Results** appear.

5. Click the **Virtualization Reduces the Cost of Supporting Open Industrial Control Systems** link.

## How to use this guide

This guide provides high-level guidance on:

- How to plan for a VMware-based virtualization environment.
- How to install and configure VMware virtualization software.
- How to create Experion virtual machines in the virtualization environment.
- How to perform system administration of the virtualization environment.
- How to monitor the virtualization environment.

**Required Honeywell documentation**

Document	Description
<i>HPS Virtualization Specification</i>	This specification identifies the supported Experion and VMware components for Experion virtualization.
<i>Experion Fault Tolerant Ethernet Specification</i>	This specification identifies the supported FTE switch hardware.
<i>Software Installation User's Guide</i>	This guide describes how to install Experion software. You will need to reference this guide to install Experion software on virtual machines.
<i>Supplementary Installation Tasks Guide</i>	This guide describes how to change computer name and setting up time synchronization.
<i>Getting Started with Experion Software Guide</i>	For Experion R31x only: This guide describes how to configure the Windows operating system.
<i>Experion Network Best Practices</i>	Document ID: WP-07-02-ENG
<i>Backup and Restore Guide</i>	This guide describes how to install the Experion Backup and Restore software, which is used to clone a physical computer to a virtual machine.
<i>Virtualization with BladeCenter S Guide</i>	This guide describes how to deploy virtualization with Experion on the BladeCenter S platform which offers a packaged solution including shared storage at Level 2. Although this Experion Virtualization Planning and Implementation Guide includes shared storage, it is limited to external SANs connected to multiple ESXi hosts with local storage. This shared storage solution can be used with DCS architectures for Level 3 or with SCADA architectures.
<i>Installation and Configuration of SQL Server and vCenter Server white paper</i>	This document gives guidance on the installation, configuration, and maintenance of SQL Server to be used with vCenter Server and VMware Update Manager.

You can download Honeywell documentation from the <http://www.honeywellprocess.com/support> website.

**Required VMware vSphere documentation****Attention**

You should use document versions that match the version of the products or software that you use. VMware documentation references within this guide are for the vSphere 5.1 documentation set. Use the table below to find the reference in the previous vSphere release.

vSphere 5.1	vSphere 5.0	vSphere 4.1
<i>vSphere Installation and Setup</i>	<i>vSphere Installation and Setup</i>	<i>ESXi Installable and vCenter Server Setup Guide</i>
<i>vSphere Networking</i>	<i>vSphere Networking</i>	<i>ESXi Configuration Guide</i>
<i>vSphere Security</i>	<i>vSphere Security</i>	<i>vSphere Datacenter Administration Guide</i>
<i>Hardening Guide – vSphere 5.1 – GA release public.xlsx</i>	<i>vSphere Security Hardening Guide (version 1.1)</i>	<i>vSphere Security Hardening Guide (version 1.0)</i>
<i>vSphere Security</i>	<i>Defined Privileges</i>	<i>vSphere Datacenter Administration Guide</i>
<i>vCenter Server and Host Management</i>	<i>vCenter Server and Host Management</i>	<i>vSphere Datacenter Administration Guide</i>
<i>vSphere Monitoring and Performance</i>	<i>vSphere Monitoring and Performance</i>	<i>vSphere Datacenter Administration Guide</i>
<i>vSphere Troubleshooting</i>	<i>vSphere Troubleshooting</i>	<i>vSphere Datacenter Administration Guide</i>
<i>Guest Operating System Installation Guide</i>	<i>Guest Operating System Installation Guide</i>	<i>Guest Operating System Installation Guide</i>



vSphere 5.1	vSphere 5.0	vSphere 4.1
<i>Installing and Configuring VMware Tools</i>	<i>Installing and Configuring VMware Tools</i>	<i>vSphere Virtual Machine Administration Guide</i>
<i>vSphere Virtual Machine Administration</i>	<i>vSphere Virtual Machine Administration</i>	<i>vSphere Virtual Machine Administration Guide</i>
<i>vSphere Resource Management</i>	<i>vSphere Resource Management</i>	<i>vSphere Resource Management Guide</i>
	<i>VMware Data Recovery Administration Guide</i>	<i>VMware Data Recovery Administration Guide</i>
<i>Installing and Administering VMware vSphere Update Manager</i>	<i>Installing and Administering VMware vSphere Update Manager</i>	<i>vCenter Update Manager Administration Guide</i>
<i>Reconfiguring VMware vSphere Update Manager</i>	<i>Reconfiguring VMware vSphere Update Manager</i>	<i>vCenter Update Manager Administration Guide</i>
<i>vSphere Storage</i>	<i>vSphere Storage</i>	<i>iSCSI SAN Configuration Guide</i>
<i>vSphere Upgrade</i>	<i>vSphere Upgrade</i>	<i>Upgrade Guide</i>

You can download VMware documentation from <http://www.vmware.com/support/pubs/> on the VMware website.

### Other required documentation



#### Attention

- You should use document versions that match the version of the products or software that you use.

- *Administrators Guide, Wyse ThinOS*
- *Reference Guide, Wyse ThinOS INI Files*
- *Iomega Store User Manual*



# Getting started with Experion virtualization

This guide assumes that you are experienced with Experion installations and virtualization technology and terminology.

Virtualization of an Experion system involves allocating Experion system and application nodes to virtual machines rather than physical machines. A key aspect of an Experion system that is deployed with virtualization is the addition of the virtual infrastructure. The virtual infrastructure is comprised of the hardware and software components required to host and manage the system. Some important characteristics of a virtualized Experion system that include:

- The Experion production workload is consolidated on ESXi server grade hosts and connected to a production network.
- The production ESXi hosts are also connected to a separate management network to isolate the traffic generated from management of the ESXi hosts and virtual machines from that of the production network.
- The production ESXi hosts are optionally connected to a separate storage network.
- The virtual infrastructure management workload is consolidated on a separate ESXi host that can be shared between production and application levels of the system.
- Workload distribution strategies for optimum performance and minimal scope of loss.
- Use of thin clients to provide user interaction with virtual desktops. No Experion application software is installed on the thin client.
- Workload backup and recovery strategies to minimize downtime in the event of a host or virtual machine failure.
- Hardware and software update strategies to maximize efficiency and minimize downtime and/or scope of loss.

## If you are familiar with virtualization and VMware

Learn about	Description
What Experion nodes can be virtualized	See the <i>HPS Virtualization Specification</i> .
Supported Experion topologies	For more information about the supported DCS architecture networks, see “Planning for a DCS architecture” on page 17.  For more information about the supported SCADA architecture networks, see “Planning for a SCADA architecture” on page 31.  If you plan to use shared storage, see “Implementing shared storage networks” on page 99.
Hardware and software requirements to support Experion virtual machines	See “Planning the virtualization environment” on page 37.
Creating Experion virtual machines	See the <i>Software Installation User’s Guide</i> .

**If you are new to virtualization**


Learn about	Description
Virtualization and industrial control systems	See the Honeywell white paper <i>Virtualization Reduces the Cost of Supporting Open Industrial Control Systems</i> .
Virtualization terms	See <i>VMware vSphere Basics Guide</i> from VMware, Inc.
Practical skills implementing virtualization	See <i>VMware vSphere Basics Guide</i> from VMware, Inc.
Virtual network concepts	See <i>VMware vSphere Basics Guide</i> from VMware, Inc.
Implementing a virtualized Experion environment	Once you have a practical understanding of virtualization, continue with the content presented in this guide.

**Related topics**

“Task overview for preparing an Experion virtualization environment” on page 13

## Task overview for preparing an Experion virtualization environment

The following table captures a high level overview of the tasks that need to be completed to prepare the virtual environment. For more information about each task, see the relevant chapter within this guide.

Task	Description
Determine architecture	<p>Depending on the characteristics of your target system, you can follow one of two architecture paths:</p> <ul style="list-style-type: none"> <li>Follow the DCS architecture path if your target system has: <ul style="list-style-type: none"> <li>A plant network with at least 3 network layers or levels</li> <li>An FTE network at level 1 and 2</li> <li>Multiple clusters and multiple FTE communities</li> <li>A requirement of a high level of security and reliability where the emphasis is on isolating critical areas of function such as local peer-peer control, peer to external peer.</li> </ul> <p>For more information, see “Planning for a DCS architecture” on page 17</p> </li> <li>Follow the SCADA architecture path if your target system has: <ul style="list-style-type: none"> <li>A plant network that is inherently flat (Level 1 and Level 2 only with no FTE)</li> <li>A small number of Experion clusters</li> </ul> </li> </ul> <hr/> <p> <b>Tip</b> For small Experion systems with FTE (a single FTE community), consider the SCADA architecture path to establish the management network.</p> <hr/> <p>For more information, see “Planning for a SCADA architecture” on page 31.</p>
Plan for virtualization	For assistance creating your virtual infrastructure, see “Planning the virtualization environment” on page 37
Build the physical networks	<p>Build the:</p> <ul style="list-style-type: none"> <li>Management network See “Implementing networks for a DCS architecture” on page 75 or “Implementing networks for a SCADA architecture” on page 93.</li> <li>Production network See the <i>Fault Tolerant Ethernet Overview and Implementation Guide</i> for creating the Level 1 and Level 2 networks, or “Preparing the production network for a SCADA architecture” on page 95.</li> <li>Storage network, if applicable See “Implementing shared storage networks” on page 99.</li> </ul>
Install the gateway router (for SCADA architecture)	<ul style="list-style-type: none"> <li>Configure to route domain controller information between the management and production networks.</li> <li>Configure to route information to the IT environment/WAN.</li> <li>Connect the management network.</li> <li>Connect the production network.</li> <li>If applicable, connect the storage network.</li> </ul> <p>See “Preparing a gateway router for a SCADA architecture” on page 94.</p>

Task	Description
Install the management ESXi host	<ul style="list-style-type: none"> <li>• Install the ESXi host hardware.</li> <li>• Configure the RAID configuration.</li> <li>• Configure the BIOS.</li> <li>• Connect the ESXi host to all the required networks.</li> <li>• Install the ESXi software</li> <li>• Configure the default virtual connection for the management network.</li> </ul> <p>See “Preparing a management ESXi host” on page 107.</p>
Install the management client	<p>Install the vSphere Client on a separate physical computer.</p> <p>See “Preparing a management ESXi host” on page 107.</p>
Configure the management ESXi host	<p>Configure the ESXi host network settings.</p> <p>See “Preparing a management ESXi host” on page 107.</p>
Install and configure the storage device(s) (for Level 3 DCS architectures and SCADA architecture)	<p>Use the physical management client to connect to the storage device through the management network, if the device permits. Otherwise, connect through the storage network.</p> <ul style="list-style-type: none"> <li>• Configure storage for the SAN using the storage device software or web interface (that is, set iSCSI TCP/IP settings, set iSCSI security, create iSCSI groups and volumes).</li> <li>• Configure storage for the ESXi host using vSphere Client (that is, iSCSI Initiator, iSCSI security, and create datastores).</li> </ul> <p>See “Implementing shared storage networks” on page 99.</p>
Create the management workloads	<ul style="list-style-type: none"> <li>• Prepare for vCenter Server.</li> <li>• Create the vCenter Server virtual machine using local storage, ensuring the virtual machine is added to the domain prior to installing the vCenter software.</li> <li>• Install the vCenter Server software.</li> <li>• Install the Update Manager on the vCenter Server virtual machine.</li> <li>• Add the management ESXi host to the vCenter Server.</li> <li>• Configure vCenter Server security.</li> </ul> <p>See “Preparing a vCenter Server” on page 118.</p> <p>Prepare for virtual machine replication (optional).</p> <p>See “Planning to replicate the virtual machines” on page 72.</p>
Install the production ESXi hosts	<ul style="list-style-type: none"> <li>• Install the ESXi host hardware.</li> <li>• Configure the RAID configuration.</li> <li>• Configure the BIOS.</li> <li>• Connect the ESXi host to all the required networks.</li> <li>• Install the ESXi software</li> <li>• Configure the default virtual connection for the management network.</li> <li>• Add the ESXi host to the vCenter Server.</li> </ul> <p>See “Preparing a production ESXi host” on page 131.</p> <p>If using shared storage, ensure that the ESXi host can connect to the shared storage.</p> <p>See “Implementing shared storage networks” on page 99.</p>
Create a virtual management client	<ul style="list-style-type: none"> <li>• This virtual machine can be used in preference to the physical management client and contains the same software as the physical management client.</li> <li>• The physical management client should continue to be maintained.</li> </ul>
Secure the system	<ul style="list-style-type: none"> <li>• Ensure the appropriate security groups and policy is in place on the vCenter Server.</li> <li>• Lockdown the ESXi hosts.</li> </ul>

Task	Description
Install and configure the production nodes	Create and install the Experion virtual machines and other production workloads. See the <i>Software Installation User's Guide</i> .
Install and configure thin clients	Prepare, install, and configure thin clients. See the <i>Wyse Z90DE7 Thin Client Planning Installation and Service Guide</i> .
Install and configure NAS devices	Install and configure NAS devices. See the <i>Backup and Restore Guide</i> .
Configure Experion Backup and Restore (EBR)	Configure the EBR application. See the <i>Backup and Restore Guide</i> .
Configure the virtual machine replication	Configure virtual machine replication (optional). See “Planning to replicate the virtual machines” on page 72.





# Planning for a DCS architecture

## Related topics

“Example DCS architecture virtualization scenario” on page 18

*Prior to implementing Experion virtualization for a DCS architecture, understand the supported topologies.*

“DCS architecture options in a virtualized environment” on page 19

“Example DCS architecture in a virtualized environment with non-redundant management network” on page 22

“Example DCS architecture in a virtualized environment with redundant management network” on page 24

“Example DCS architecture in a virtualized environment with separate management network” on page 26

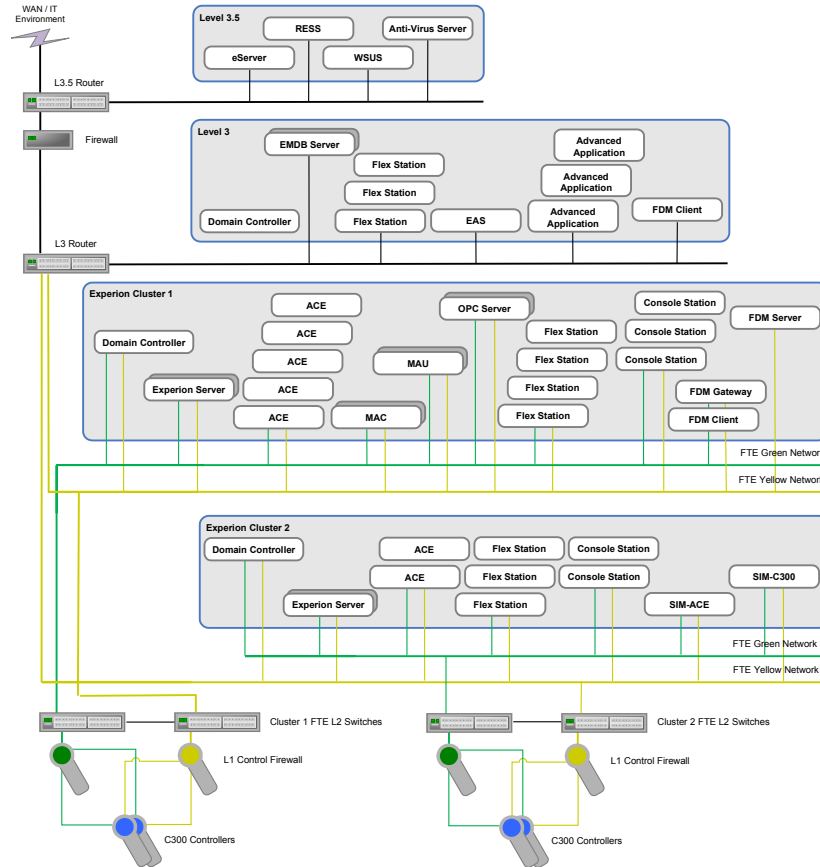
“Overview of distributing workload across ESXi hosts for a DCS architecture” on page 29

*An ESXi host’s workload consists of the set of nodes that reside as guests on that host. When planning for the distribution of the nodes, you need to consider the type of workloads to be deployed.*

## Example DCS architecture virtualization scenario

Prior to implementing Experion virtualization for a DCS architecture, understand the supported topologies.

Discussion within this guide about supported DCS architecture topologies is based on the virtualization of the following example scenario.



**Figure 1: DCS architecture virtualization scenario**

In this example scenario, there are two Experion clusters to be virtualized at Level 2:

- **Experion cluster 1**  
This Experion cluster includes redundant Experion servers, multiple ACEs, multiple Flex stations, multiple Console Stations, redundant OPC Server, redundant MAC and MAU servers, and an FDM.
- **Experion cluster 2**  
This Experion cluster includes redundant Experion servers, multiple ACEs, multiple Flex stations, multiple Console Stations, a SIM-ACE, and a SIM-C300.

Each Experion cluster hosts a Windows domain controller.

## DCS architecture options in a virtualized environment

A virtualized DCS architecture requires ESXi hosts at Level 2 and Level 3 to support the production workloads as well as at least one ESXi host to support the management workload. While the network connectivity of the virtualized production workloads is the same as in a physical system (for example, FTE at Level 2 with network isolation from Level 3), there is an additional network introduced for the management infrastructure. This management network connects all ESXi hosts in order to provide management access to all elements of the virtualized infrastructure.

Note that this Level 2.5 network layer is introduced to both physical and virtual systems to expand high security communications beyond the FTE community. The bare metal system requires this for cross community peer to peer and PCDI communications. DCS architecture with virtualization is leveraging this same network approach to provide a secure method of distributing the management between FTE communities without open access of these networks to Level 3.

The table below identifies three management network deployment options for local storage deployments at Level 2 with recommended usages.

	Production Network Security	Mgmt Network High Availability	Supports intercluster Comms Best Practice	Relative Cost	Usage	Go To
Non-redundant management network with single routed connection to L2.5 network layer	Good	No	No	Low	<ul style="list-style-type: none"> <li>• small-medium system deployment</li> <li>• single Experion cluster</li> <li>• multiple Experion clusters with no requirement for intercluster comms</li> <li>• local storage solution</li> <li>• new sites</li> <li>• existing sites with low number of Experion clusters</li> <li>• single mgmt network for PCN levels (L2, L2.5, L3, and L3.5)</li> </ul>	“Example DCS architecture in a virtualized environment with non-redundant management network” on page 22
Redundant management network with dual-routed connection to L2.5 network layer	Good	Yes	Yes	Medium	New sites with: <ul style="list-style-type: none"> <li>• multiple Experion clusters requiring intercluster comms</li> <li>• shared storage at L3</li> </ul>	“Example DCS architecture in a virtualized environment with redundant management network” on page 24

	Production Network Security	Mgmt Network High Availability	Supports intercluster Comms Best Practice	Relative Cost	Usage	Go To
Non-redundant management network with single switch connection to redundant L2.5 network layer	Better	No	No	High	<ul style="list-style-type: none"> <li>Existing sites where                             <ul style="list-style-type: none"> <li>there are a large number of FTE communities and / or</li> <li>L2.5 port usage is limited and/or</li> <li>use of VLANs is not possible</li> </ul> </li> <li>single Experion cluster</li> <li>multiple Experion clusters requiring intercluster communications</li> <li>local storage solution</li> <li>separation of management LANs between security levels to support ACLs or firewalls</li> </ul>	“Example DCS architecture in a virtualized environment with separate management network” on page 26

	Production Network Security	Mgmt Network High Availability	Supports intercluster Comms Best Practice	Relative Cost	Usage	Go To
Management network with switch connection to redundant L3 network layer	Better	No	No	High	<ul style="list-style-type: none"> <li>Existing sites where                             <ul style="list-style-type: none"> <li>there are a large number of FTE communities and / or</li> <li>L3 port usage is limited and/or</li> <li>use of VLANs is not possible</li> </ul> </li> <li>single or multiple Experion clusters</li> <li>local storage solution</li> <li>separation of management LANs between security levels to support ACLs or firewalls</li> </ul>	“Example DCS architecture in a virtualized environment with separate management network” on page 26

---

## Example DCS architecture in a virtualized environment with non-redundant management network

Use of a single dedicated switch/router is recommended for single or low cluster DCS deployments with virtualization. This example illustrates the option to share the management infrastructure at L2 with Level 3 and Level 3.5. If site security best practices restrict access at Level 3 and above, then a separate management infrastructure would need to reside at any level requiring isolation.

Consider the following connectivity and configuration strategies listed below to deploy L2.5 with a switch/router for DCS virtualization:

- Each FTE community is connected to L2.5 as routed port
- Non-redundant management network is implemented as vLAN in L2.5 router
  - Recommendation is to plan/design for dual L2.5 routers but physically connect with single L2.5
  - Consider the option to implement dual connection from host to the single router. This option is shown in the figure below with a dashed line
- ACLs are defined at L2.5 to limit access to management network
- Management infrastructure is common between L2, L3, and L3.5
  - Separate management subnet defined at L3 and routed through L3 routers to enable secure access for shared management infrastructure
  - Separate management subnet defined at L3.5 and routed through L3 routers to enable secure access for shared management infrastructure
- ACLs defined at L3 and L3.5 to limit access to management network and to enable peer to peer DC synchronization

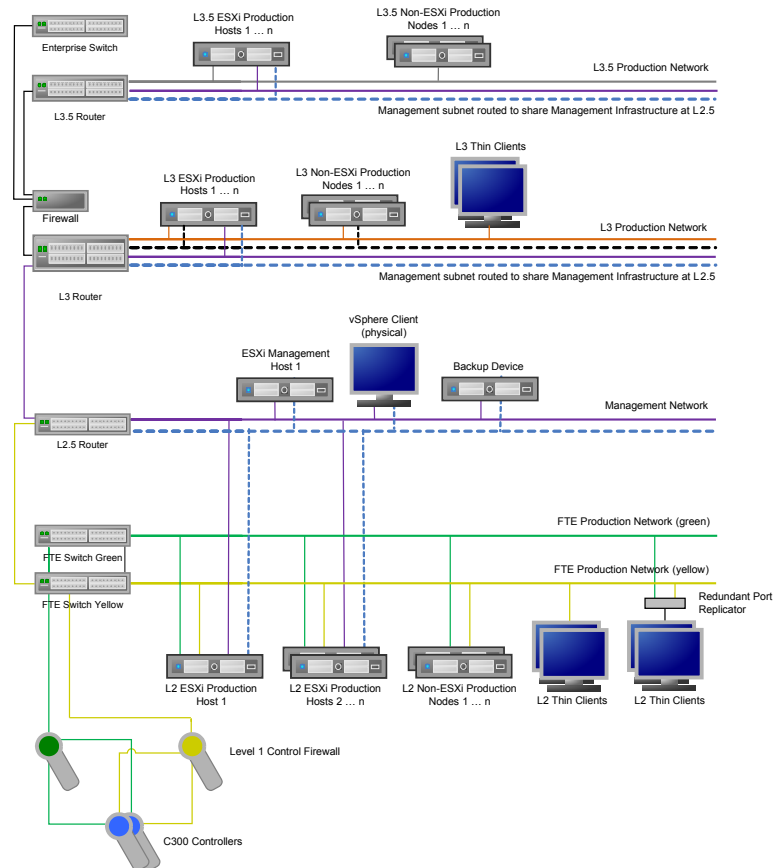


Figure 2: Example DCS architecture network topology with non-redundant management network

---

## Example DCS architecture in a virtualized environment with redundant management network

Use of redundant dedicated switch/routers is the recommendation for multi-cluster DCS deployments with virtualization. This example illustrates the option to share the management infrastructure at L2 with Level 3. If site security best practices restrict access at Level 3 and above, then a separate management infrastructure would need to reside at any level requiring isolation.

This example illustrates a separate management infrastructure at Level 3.5. If site security best practices do not restrict access at Level 3, then consider the option to share the management infrastructure at Level 3 and Level 3.5. For an example illustration of this option, see the diagram in “Example DCS architecture in a virtualized environment with non-redundant management network”.

Consider the following connectivity and configuration strategies listed below to deploy L2.5 with redundant switch/routers for DCS virtualization:

- Each FTE community is connected to L2.5 as routed port
- Management network is implemented as vLAN in L2.5 Routers
  - Crossover is established between A and B routers
  - Router redundancy is defined (such as HSRP)
- ACLs are defined at L2.5 to limit access to management network
- Management infrastructure is common between L2 and L3
  - Separate management subnet defined at L3 and routed through L3 routers to enable secure access for shared management infrastructure
  - ACLs defined at L3 to limit access to management network and to enable peer to peer DC synchronization
- Separate management network with infrastructure at L3.5



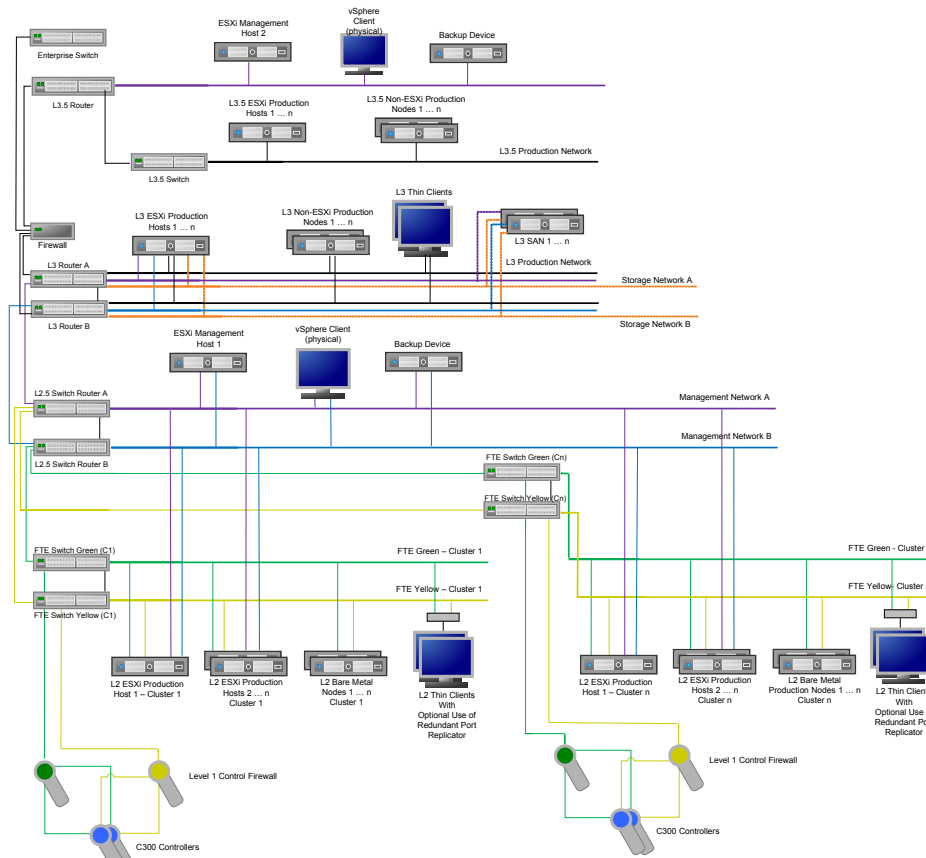


Figure 3: Example DCS architecture network topology with redundant management network

### Option for shared storage at level 3

There is also an additional network at Level 3 for the optional use of shared storage. In a Level 3 shared storage solution, the SAN(s) would host the Level 3 production workload. Storage traffic must be separated from production traffic. The figure above shows one option to separate the storage traffic from the Level 3 production traffic by routing the traffic through the Level 3 routers. The use of this option would require an additional vLAN to be defined in the Level 3 routers.

An alternative approach to separate the storage traffic is to connect the redundant SANs to a redundant pair of storage network switches. This would be similar to the shared storage topology shown for use with SCADA architecture. The use of separate network switches should be strongly considered if the Level 3 workload is disk I/O intensive.

For either approach, the solution requires aggregated ports between the redundant pair of switch-routers. For more information about planning and deploying shared storage, see the related topics.

The figure above shows the Level 2 production ESXi hosts and the Level 2 thin clients independent of Experion clusters. For more information about the deployment considerations for multiple Experion clusters at Level 2, see the related topics.

### Related topics

“Storage requirements” on page 42

“Implementing shared storage networks” on page 99

*If you have chosen shared storage for your virtual infrastructure, implement this shared storage network.*

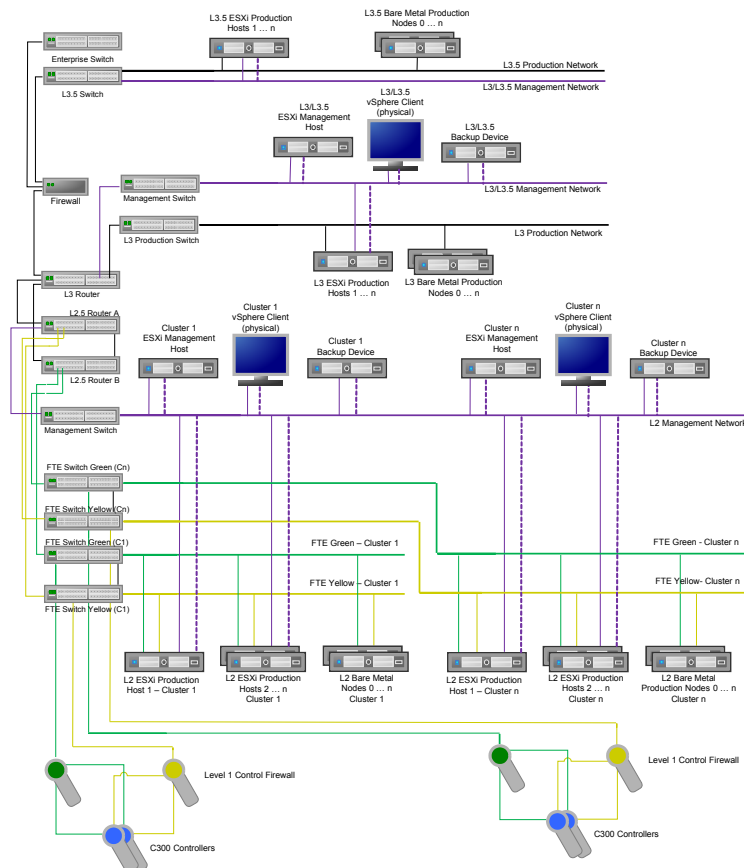
## Example DCS architecture in a virtualized environment with separate management network

This example uses either the same redundant L2.5 backbone that was previously introduced, or an existing redundant L3 backbone (i.e. no L2.5). The option with L2.5 provides both high security and high availability for communication between FTE communities. The option without L2.5 is for those sites that do not require the communication between FTE communities. In either option, the management network is implemented as a separate network with its own management switch that is connected to L2.5 or L3 via a routed port. This approach is more suited for brown field sites where existing network infrastructure limits the number of available ports that can be used for the virtual infrastructure.

This can be implemented with a single management network. An additional option would be to implement this with redundant management switches. The management infrastructure at L2 or L3 is not shared. The management infrastructure that resides at Level 3 can be optionally shared with L3.5.

Consider the following connectivity and configuration strategies listed below to deploy L2.5 or L3 with redundant switch/routers for DCS virtualization:

- Redundant L2.5 and/or L3 with:
  - Crossover is established between A and B routers
  - Router redundancy is defined (such as HSRP)
- Each FTE community is connected to L2.5 as routed port
- Management Network at L2 is isolated from L2 production
  - Management infrastructure (management host, physical vSphere client and backup device) with management switch established on separate subnet
  - Consider the following recommendations for the management switch:
    - The same switch device as recommended for the management network in the SCADA architecture
    - Any of the current set of recommended FTE switches that has enough gigabit ports for management infrastructure connections
  - Management network is connected to L2.5 as routed port
  - Consider the option to implement dual connection from L2 hosts to the single router. This option is shown in the figure below with a dashed line.
  - ACLs defined at L3 to limit access to management network and to enable peer to peer DC synchronization
- ACLs are defined at L2.5 to limit access to management network
- Separate Management network and infrastructure resides at L3 and is shared with L3.5
  - Separate management subnet defined at L3.5 and routed through L3 routers to enable secure access for shared management infrastructure
  - Consider the option to implement dual connection from L3 or L3.5 hosts to the single router. This option is shown in the figure below with a dashed line



**Figure 4: Example DCS architecture network topology with separate management network connected to L2.5**

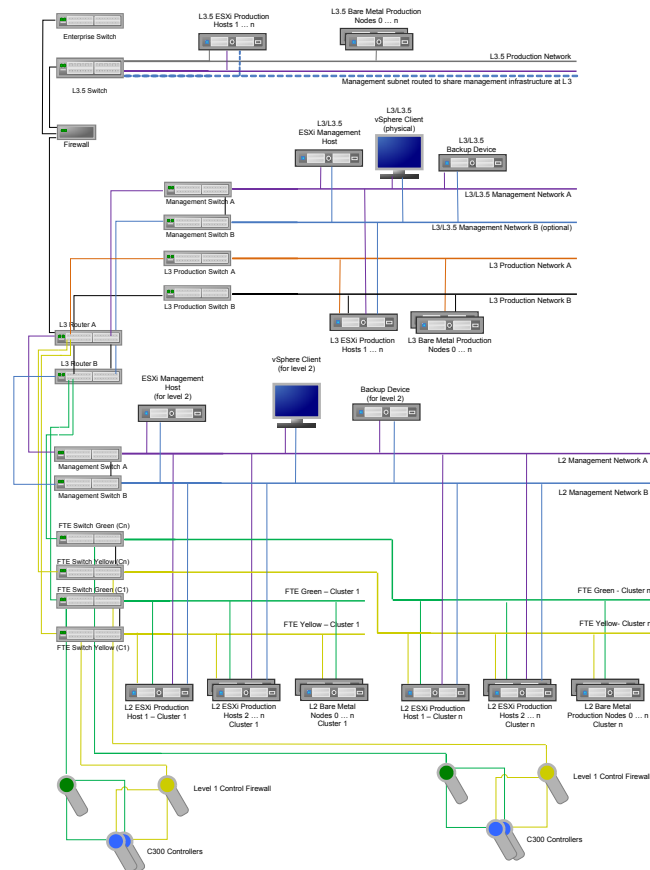


Figure 5: Example DCS architecture network topology with separate management network connected to L3

## L2 management infrastructure deployment options for multi-cluster systems

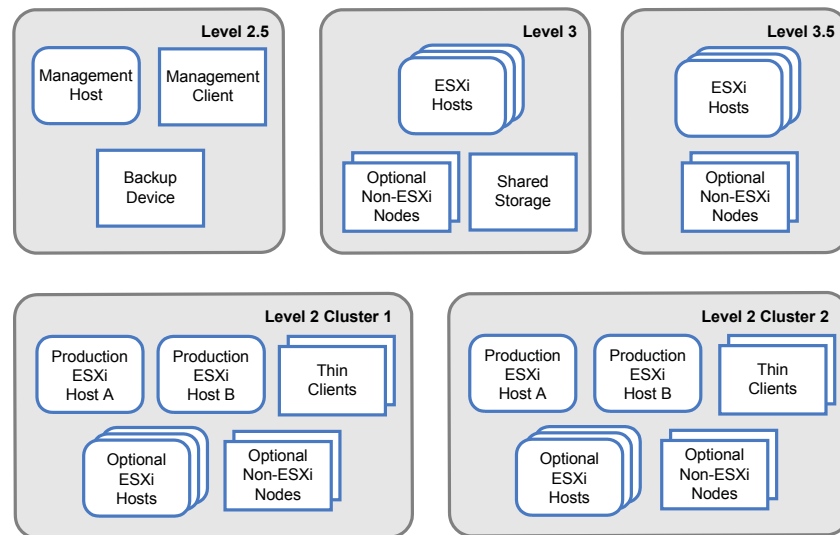
The figure above illustrates a management infrastructure deployment strategy for multiple Experion clusters. In this example, the deployment uses a silo or island approach where each Experion cluster has its own virtual infrastructure management (i.e. management host, physical vSphere client and backup device). If a silo approach is not required, then deployment of a single management infrastructure that is shared by all the clusters at L2 is recommended.

## Overview of distributing workload across ESXi hosts for a DCS architecture

An ESXi host's workload consists of the set of nodes that reside as guests on that host. When planning for the distribution of the nodes, you need to consider the type of workloads to be deployed.

Process operational workloads refer to the set of nodes that execute at Level 2. Application operational workloads refer to the set of nodes that execute above Level 2.

Distributing nodes across the ESXi hosts is based on the high level deployment model. In a virtualized environment, Level 2.5 is introduced into this model. It contains the workload used to manage the ESXi hosts and other components that form part of the virtual infrastructure.



**Figure 6: Multiple plant level deployment model with a management network at Level 2.5**

The process of distributing nodes begins with the identification and separation of workloads. Begin by separating the workload by plant level. Separate the Level 2 workload by Experion cluster.

Example process operational workloads	Example application workloads	Example management workloads
<ul style="list-style-type: none"> <li>Experion server A - Cluster 1</li> <li>Experion server B - Cluster 1</li> <li>Flex Stations - Cluster 1</li> <li>Console Stations - Cluster 1</li> <li>ACEs - Cluster 1</li> <li>MAC server X - Cluster 1</li> <li>MAC server Y - Cluster 1</li> <li>MAU server X - Cluster 1</li> <li>MAU server Y - Cluster 1</li> <li>OPC server A - Cluster 1</li> <li>OPC server B - Cluster 1</li> <li>Domain controller - Cluster 1</li> <li>FDM gateway- Cluster 1</li> <li>FDM client- Cluster 1</li> <li>FDM server- Cluster 1</li> </ul>	<ul style="list-style-type: none"> <li>eServer</li> <li>EMDB server A</li> <li>EMDB server B</li> <li>Experion Application Server (EAS)</li> <li>Flex Stations</li> <li>Domain controller</li> <li>Honeywell Advanced Applications</li> </ul>	<ul style="list-style-type: none"> <li>vCenter Server</li> <li>vSphere Client</li> <li>vDR appliance</li> <li>Domain controller</li> </ul>

Example process operational workloads	Example application workloads	Example management workloads
<ul style="list-style-type: none"> <li>• Experion server A - Cluster 2</li> <li>• Experion server B - Cluster 2</li> <li>• Flex Stations - Cluster 2</li> <li>• Console Stations - Cluster 2</li> <li>• ACEs - Cluster 2</li> <li>• SIM-ACE - Cluster 2</li> <li>• SIM-C300 - Cluster 2</li> <li>• Domain controller - Cluster 2</li> </ul>		



#### Attention

In a virtualization environment, a domain controller is required for the management network, which is introduced as part of the virtualization environment.

When using Virtual Machine replication, the task of planning the workload deployment requires that the original virtual machine and the cloned replica virtual machine must both be considered in the workload deployment. For more information, see the related topics.

For most virtualization environments, it is expected that the management workloads can be hosted on a single ESXi host.

Distribution of workload is a significant contributing factor to the number of required ESXi hosts as well as the capacity and expected performance of each ESXi host. For more information on how to allocate operational workload to ESXi hosts, see the related topics. For more information about the host considerations for the management workload, see the related topics.

#### Related topics

“Planning for the management ESXi host and management network” on page 56

*One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.*

“Determining the number of ESXi hosts and hardware requirements” on page 38

# Planning for a SCADA architecture

## Related topics

“Example SCADA architecture virtualization scenario” on page 32

*Prior to implementing Experion virtualization for a SCADA architecture, understand the supported topologies.*

“Example SCADA architecture in a virtualized environment” on page 33

“Overview of distributing workload across ESXi hosts for a SCADA architecture” on page 34

## Example SCADA architecture virtualization scenario

Prior to implementing Experion virtualization for a SCADA architecture, understand the supported topologies. Discussion within this guide about supported SCADA architecture topologies is based on the virtualization of the following example scenario.

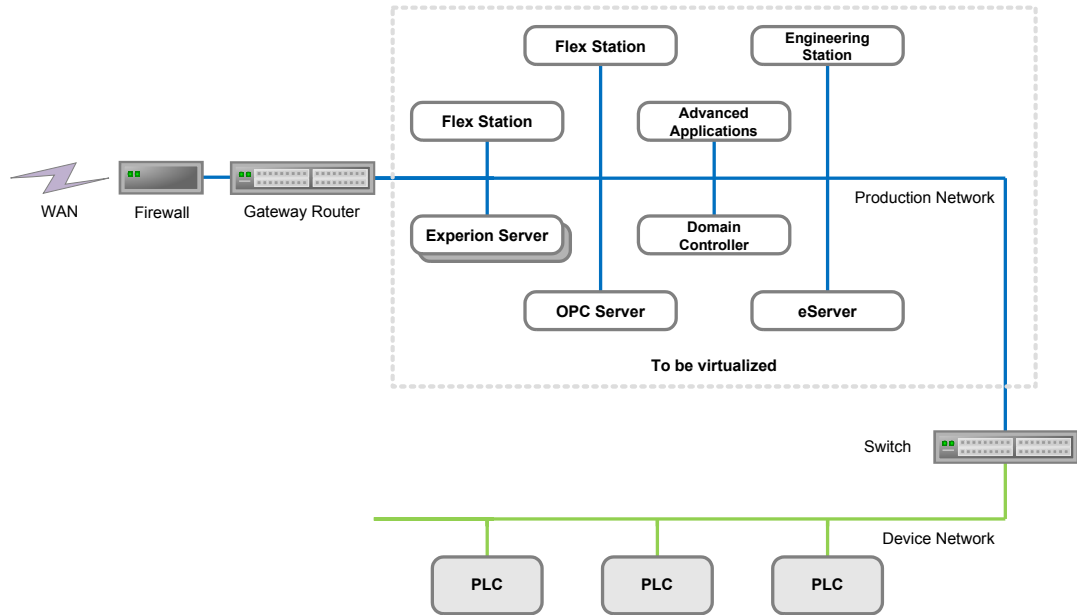


Figure 7: SCADA architecture virtualization scenario



### Attention

- For the virtualization of OPC servers, it is assumed that these servers use an Ethernet network connection to the programmable logic controller (PLC).
- Advanced Applications include AAM, Business FLEX, Profit Suite, and Procedure Analyst. While this scenario includes Advanced Applications, this guide does not provide any instructions for the installation or deployment of these applications in a virtualization environment.



# Example SCADA architecture in a virtualized environment

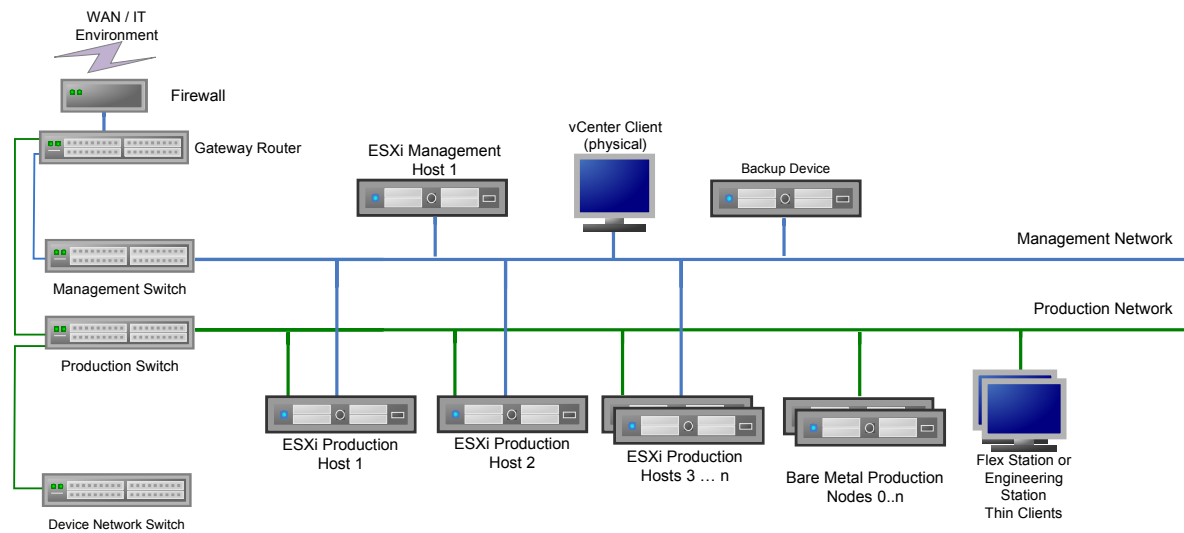


Figure 8: Example SCADA architecture network topology using local storage on the ESXi hosts

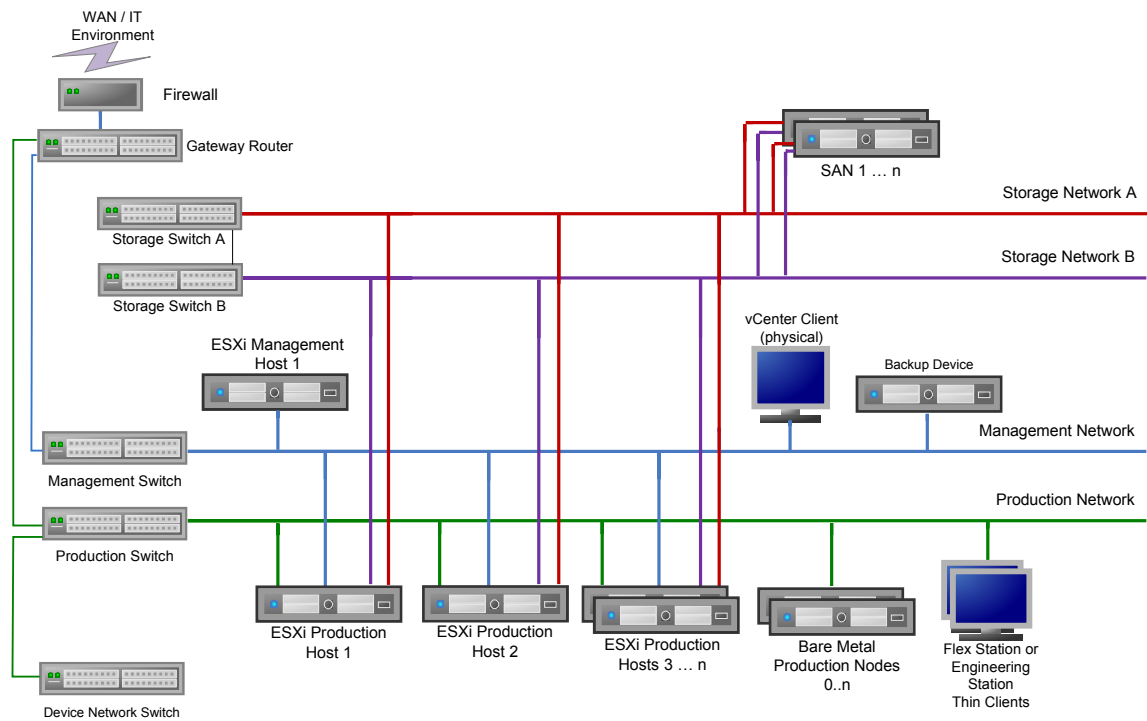


Figure 9: Example SCADA architecture network topology using shared storage

## Overview of distributing workload across ESXi hosts for a SCADA architecture

An ESXi host's workload consists of the set of nodes that reside as guests on that host. When planning for a the distribution of the nodes, you need to consider the types of workloads to be deployed.

The process of distributing nodes begins with the identification and separation of workloads.

Example process operational workloads	Example application workloads	Example management workloads
<ul style="list-style-type: none"> <li>• Experion server A</li> <li>• Experion server B</li> <li>• OPC server</li> <li>• Flex Station</li> <li>• Engineering Station</li> <li>• Secondary domain controllers</li> </ul>	<ul style="list-style-type: none"> <li>• eServer</li> <li>• Honeywell Advanced Applications</li> </ul>	<ul style="list-style-type: none"> <li>• vCenter Server</li> <li>• vCenter Client</li> <li>• VMware Data Recovery (vDR) appliance</li> <li>• Primary domain controller</li> </ul>



### Attention

In the example scenario, there is only one domain controller. In a virtualization environment, more than one domain controller is required (a domain controller is required for the management network, which is introduced as part of the virtualization environment, and another domain controller is required for the process operational network). The primary domain controller, which is connected to the management network, is considered part of the management workload, while secondary domain controllers are considered part of the process operational workloads.

For most virtualization environments, it is expected that the management workloads can be hosted on a single ESXi host.

Distribution of workload is a significant contributing factor to the number of required ESXi hosts as well as the capacity and expected performance of each ESXi host. For more information on how to allocate operational workload to ESXi hosts, see the related topics. For more information about the host considerations for the management workload, see the related topics.

### Related topics

“Determining the number of ESXi hosts and hardware requirements” on page 38

“Planning for the management ESXi host and management network” on page 56

*One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.*

# Planning for off-process usage

If you are implementing an Experion virtual system for off-process usage, you should follow the relevant planning and implementation topics for DCS and SCADA-based architectures. An off-process system is not intended for on-process control and is typically isolated from an on-process systems.

Depending on the intended usage, an off-process system, when compared to an on-process system, may have the following:

- A flatter network topology.  
Consider the network security, functionality, and performance offerings of an on-process system before discounting network configurations.
- Higher consolidation ratios.  
Consider the scope of loss and the acceptable performance of ESXi hosts for off-process usage.



# Planning the virtualization environment

The following topics describe the planning considerations for an Experion virtualization environment.

## Related topics

“Determining the number of ESXi hosts and hardware requirements” on page 38

“Identifying virtualization hardware and software requirements” on page 53

*You need to consider other software and hardware requirements prior to implementing a virtualization environment.*

“Planning for the management ESXi host and management network” on page 56

*One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.*

“Planning how to organize the vCenter Server” on page 61

*Hosts and their virtual machines should be organized within vCenter Server based on logical groupings.*

“Planning for time synchronization” on page 63

*Time synchronization requires an NTP server to distribute time throughout the virtual infrastructure.*

“Planning to maintain the VMware environment” on page 65

*You need to consider how to maintain and update the VMware components within a virtualization environment.*

“Planning security for the VMware environment” on page 67

*You need to consider how to implement security within the VMware virtualization environment.*

“Planning to backup the virtual infrastructure and virtual machines” on page 70

*Plan for the use of Experion Backup and Restore (EBR) to perform backups of the virtual infrastructure and virtual machines.*

---

## Determining the number of ESXi hosts and hardware requirements

Before identifying any hardware requirements, the Experion system must be defined. This requires a knowledge of all planned Experion virtual nodes and the topology that will be used in the system.

Use the following steps to estimate your virtualization hardware requirements.

### Planning workload grouping

The aim of workload grouping is to form groups of virtual machines that will connect to the same network. To do this, identify workloads that will operate on the same network level. Workloads belonging to the Level 2 network (for DCS architectures) or the production network (SCADA architecture), should also be grouped into Experion clusters.

The groupings that are achieved by this differentiation are now ready for further workload distribution assessment.

---

#### DCS architecture example

An example DCS architecture grouping at this point may be:

- Level 2 Experion cluster 1
- Level 2 Experion cluster 2
- Level 3 group
- Level 3.5 group
- Management workload (Level 2.5)

---

#### SCADA architecture example

An example SCADA architecture grouping at this point may be:

- Process operational workload
- Application operational workload
- Management workload

---

### Determining host groups

The aim of creating a host group listing is to form the first tentative groups of virtual nodes that can be consolidated into an ESXi host. Host performance and capacity is not considered at this point.

To create host groups, assess the availability requirements for each virtual node in a given workload group and place in a host group. At this point in time, it is also recommended to consider scope of loss when assigning multiple workloads to a given host group. For example, assigning all flex stations, console stations, or ACE nodes to a given host group should be avoided. Distribute them evenly across applicable host groups.



#### Attention

- Redundant applications should not be placed in the same host group.
  - No more than one Windows domain controller can run in the same host group.
  - Replicated virtual machines should be included in deployment and host resource requirement calculations
-

---

**DCS architecture example**

Level 2 Experion cluster 1 host group A:

- Experion server A
- Flex Station 1
- Flex Station 3
- ACE 1
- ACE 3
- ACE 5

Level 2 Experion cluster 1 host group B:

- Experion server B
- Flex Station 2
- Flex Station 4
- ACE 2
- ACE 4

This example is not complete, as it does not list all nodes for Experion cluster 1, nor does it show all groupings, such as Experion cluster 2, Level 3 group, Level 3.5 groups, and management workload.

---

**SCADA architecture example**

Process operational workload group A

- Experion server A
- OPC server
- Flex Station

Process operational workload group B

- Experion server B
- Engineering Station
- Windows domain controller

Application operational workload

- eServer
- Honeywell Advanced Applications

Management workload

- vCenter Server
  - vSphere Client
  - VMware Data Recovery (vDR)
  - Windows domain controller
- 

**Identifying host group resource requirements**

The aim of this step is to calculate the resources for each host group.

To perform this calculation, use the virtual machine workload data contained in the *HPS Virtualization Specification* and derive the total resource requirements for each host group.

To sustain a high level of robustness and availability for each console station that will reside on a given host, two additional vCPUs should be reserved. These reserved vCPUs will not be allocated to any virtual machine.

### Defining the host hardware specifications

The aim of this step is to define and calculate the resources that will be provided by a given hardware platform. Platform capabilities should be assessed by CPU, hard disk capacity and performance, memory, and network bandwidth. Each of these parameters need to be considered for workload assignment and must be known at this point.

### Assessing the targeted host hardware against the host groups

The aim of this step is to establish if the assessed hardware is capable of providing the resources required by each host group.

To do this, compare the host group resource requirements with the hardware platform capabilities.

If the platform is not able to provide the calculated resources, the following should be considered:

- Adjust the configuration of the platform to provide the required resources.
- Adjust host group size by redistributing workloads to additional host groups.

For additional information on resource requirements, see the related topics.

When host groups are assessed and resource requirements are met, each host group can now form the planned ESXi host consolidated workload.

### Related topics

“Overview of distributing workload across ESXi hosts for a DCS architecture” on page 29

*An ESXi host's workload consists of the set of nodes that reside as guests on that host. When planning for the distribution of the nodes, you need to consider the type of workloads to be deployed.*

“Planning for the management ESXi host and management network” on page 56

*One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.*

“Overview of distributing workload across ESXi hosts for a SCADA architecture” on page 34

“Host CPU requirements” on page 40

*You need to consider host CPU requirements.*

“Host memory requirements” on page 41

*For estimating and planning purposes, the total allocated virtual memory must be equal to, or less than, the total physical memory available on the ESXi host.*

“Network requirements for a DCS architecture” on page 44

“Network requirements for a SCADA architecture” on page 50

*There are specific network-related requirements for a SCADA architecture.*

“Planning to backup the virtual infrastructure and virtual machines” on page 70

*Plan for the use of Experion Backup and Restore (EBR) to perform backups of the virtual infrastructure and virtual machines.*

## Host CPU requirements

You need to consider host CPU requirements.

### Virtual CPU allocation

When considering virtual machine consolidation, the assignment of virtual CPU is an important factor as it will directly affect the performance of the virtual machines. Every ESXi host has a specified number of logical processors that can be calculated based on the number of physical cores in the hardware platform processors and



the use of hyper threading, if enabled. When hyper threading is enabled, the number of logical processors is twice the number of physical cores.

The total number of assigned virtual CPUs on an ESXi host should not exceed the number of logical processors on that ESXi host.

---

#### Example of how to calculate the number of logical processors on an ESXi host

An ESXi host has an Intel Xeon E5620 CPU installed. The CPU has 4 cores and hyper threading is enabled. The total number of logical processors is  $2 \times 4 = 8$ .

---

#### CPU MHz considerations

The clock speed of the hardware platform CPU is important. This is in addition to the virtual CPU requirements and should be considered to ensure that the hardware can satisfy CPU time for the virtual machines. The performance matrix table in the *HPS Virtualization Specification* includes a CPU MHz value for each Experion node. The sum of the CPU MHz for all virtual machines in each host group should not exceed 80% of the available hardware MHz. This ensures that hypervisor overhead is included in planning.

#### ! Attention

- If you use or are planning future usage of a storage area network (SAN) with the iSCSI protocol, each ESXi host requires an additional 10% CPU overhead on top of the total virtual machine CPU MHz. This consideration is important as it may limit the ability to consolidate as many virtual machines in each ESXi host.
- 

#### Example of how to calculate the available hardware MHz

An ESXi host has one Intel Xeon X5650 CPU installed. The CPU has 6 cores at 2.67 GHz per core. The total available hardware MHz is 16020MHz ( $2670 \times 6 = 16020$ ).

---

#### Related topics

“Determining the number of ESXi hosts and hardware requirements” on page 38

## Host memory requirements

For estimating and planning purposes, the total allocated virtual memory must be equal to, or less than, the total physical memory available on the ESXi host.

#### Memory overcommitment

Unused memory (the difference between allocated memory and active memory) can be shared with other virtual machines. In addition, VMware uses other techniques to optimize memory usage.

These memory management techniques, collectively known as *memory overcommitment*, enable you to run virtual machines where the total allocated memory is greater than the physical memory available on the ESXi host.

On-process usage	Off-process usage
Reduced performance may be unacceptable and the level of memory overcommitment may need to be reduced to improve performance of the virtual machines. The total allocated memory must be equal to, or less than, the total physical memory available on the ESXi host.	<p>It may be acceptable for slightly reduced performance for the benefit of improved host utilization and increased cost savings. Extreme use of memory overcommitment can result in poor system performance. Honeywell recommends that you limit the total active memory to no greater than 100% above the physical memory available on the ESXi host. An ESXi host level alarm will trigger if the host has reached a configured level of usage of physical memory. The default usage level is 90%. If host memory usage alarms are generated and/or your performance is poor, then you should consider reducing the amount of memory overcommitment. The amount of allocated memory for each Experion virtual machine should not be adjusted. Instead, you need to reallocate the virtual machines across ESXi hosts to achieve the best performance/cost/host utilization characteristics.</p> <hr/> <p><b>! Attention</b></p> <p>For both on-process and off-process usage, you should monitor the active memory for each virtual machine and factor into your calculation adequate memory to handle peak memory usage across the virtual machines.</p>

#### Related topics

“Determining the number of ESXi hosts and hardware requirements” on page 38

## Storage requirements

Honeywell supports local host storage, shared storage, and network attached storage (NAS). This guide describes a shared storage solution with multiple ESXi hosts with local storage connected to an external storage device such as a SAN. This solution is limited to Level 3 only in DCS architectures or SCADA architectures. Use the *Experion Virtualization with BladeCenter S Guide* for a shared storage solution for Level 2.

ESXi uses virtual disk files as the disk drives for virtual machines. Each virtual machine stores these files (with the .vmdk file extension) in a directory in a datastore. You need to identify:

- The location of the datastores. There are two types of storage that can be used for virtual machines:
  - Local storage
  - Shared storage
- The performance requirements of the disk array. Consider the planned virtual machine workload for each host with local storage and the total virtual machine workload for shared storage. Use the performance matrix table in the *HPS Virtualization Specification* to calculate the total average IOPs and total maximum IOPs for each workload and ensure the disk arrays can meet that demand. Inadequate disk performance affects the performance of all virtual machines on that host or shared storage.
- The size of the datastore, taking into consideration the number of virtual machines, the guest operating systems, the application software, and additional space for data and growth.

The total disk space of the disk/volume must be greater than the allocated disk size requirements for each Experion virtual machine, plus additional space for swap files and partition, and a diagnostic partition.

If you also want to store snapshots, ISO images, virtual machine templates, or floppy disk images, you will need additional disk space.

**Attention**

- The maximum size of a virtual disk is restricted by the block size when the datastore is created. When creating datastores, keep in mind the size of your virtual disks.

For more information about block sizes and datastores, see the Block size limitations of a VMFS datastore (KB1003565) knowledge base article on the VMware web site.

You also need to consider the storage requirements for virtual machine backups. Honeywell recommends that a NAS be used as the backup repository for VMWare Data Recovery.

**Local storage**

Virtual machines images are stored directly on the disks within the ESXi host that is hosting the virtual machine.

During the installation of ESXi, empty disk space on the partition where ESXi is installed is automatically partitioned and formatted, and converted into a datastore. Disk space on empty partitions are also formatted and converted into datastores. Hardware vendor partitions, such as Dell Utility partitions are retained and not formatted.

You should plan a naming convention for the datastores created on local storage. When using vCenter Server, you will be presented with a list of datastores, which are easier to manage if they are uniquely and consistently named.

**Shared storage**

Virtual machine images are stored on shared storage devices that one or more ESXi hosts can access.

Shared storage is a key requirement to enable advanced virtualization features such as vMotion and Site Recovery Manager (SRM) for business continuity and disaster recovery. If none of these features are required now, or in the future, local storage will meet your needs.

You should plan a naming convention for the volumes and datastores created on shared storage. The volume name and the datastore name may differ. When using vCenter Server, you will be presented with a list of datastores, which are easier to manage if they are uniquely and consistently named.

**Backup storage**

VMWare Data Recovery (vDR) requires the use of a backup repository, which can be configured as a virtual disk on local or shared storage, or as a NAS device. Honeywell recommends use of a NAS device for the storage of vDR backups.

The VMware vDR documentation recommends that a share size be a maximum of 500GB on a NAS device.

You can use multiple NAS devices to allow for the rotation in off-site storage of the backup data.

**About virtual machine disk formats**

The following virtual machines disk formats are supported:

- Thick Provisioned Format (the default virtual disk format)

The size of the .vmdk file in the datastore is always the allocated disk size of the virtual machine. If the virtual machine's allocated disk size is 300 GB it will always be 300 GB, even if the used disk space of the virtual machine is less than 300 GB.

**Attention**

- Thick provisioned format is the only supported format for on-process systems. However, thick provisioned format can also be used for off-process systems. You may want the off-process system to be the same as the on-process system.

- Thin Provisioned Format

The size of the .vmdk file in the datastore is the disk space used by the virtual machine. If the virtual machine's allocated disk size is 300 GB but the used disk space of the virtual machine is 100 GB, the .vmdk file will be 100 GB in size.

**Attention**

Thin provisioned format is only supported for off-process systems.

**CAUTION**

With thin provisioned disks, the used disk space can grow to be greater than the allocated disk size. This could result in an 'oversubscription' situation where the used disk space attempts to be larger than the actual capacity of the datastore. To avoid an oversubscription of the datastore, you should set up an alarm notification to indicate when the used disk space reaches a specified threshold.

**Related topics**

“Example DCS architecture in a virtualized environment with redundant management network” on page 24

“Implementing shared storage networks” on page 99

*If you have chosen shared storage for your virtual infrastructure, implement this shared storage network.*

## Network requirements for a DCS architecture

There are network-related requirements that should be considered to optimize the alignment between the virtual network (vNetwork) and the physical network of a DCS architecture. Prior to determining the network requirements, understand the relationship between the virtual and physical networks. For more information about the concepts of virtual networking, see the following sections in the *vSphere Networking* guide:

- Introduction to Networking
- Basic Networking with vNetwork Standard Switches

**Common network configuration decisions**

When implementing a production network for a DCS architecture you need to consider the following:

Consideration	Description
Network speeds	Network speeds affect the number of physical network connections from the ESXi host to the production network. Only 10/100Mbps networks are supported for FTE dual production network. The network speed that the physical production switch supports is the maximum bandwidth that the production vSwitch can support between virtual machines running on separate ESXi hosts to the FTE physical switches. This limitation needs to be used in any calculation for determining the number of virtual machines that can connect to each vSwitch. More network adapters may be required to satisfy the total virtual network throughput.
Network security	You should eliminate all unwanted network traffic in the production network. A pair of Level 2.5 routers can connect the FTE production networks, management network, and application network (Level 3).

**ESXi hosts**

Experion DCS architecture includes ESXi hosts for management, L2 production and L3 production. (An ESXi production host contains process operational or application operational workloads.) The network requirements vary depending on the usage of the ESXi host. Each ESXi host must meet the following general hardware requirements:

- Supported server-grade hardware. Varying levels of capacity are recommended based on the intended use of each ESXi host. For example, an operational ESXi host on the production network may require more capacity than the management ESXi host on the management network. For more information about the server-grade hardware requirements and recommended capacities, see the *HPS Virtualization Specification* from the Honeywell Process Solutions website.

**Attention**

- Use the same vendor, family, and generation of CPUs throughout your virtualization environment. This will ensure the portability of virtual machines when using vMotion.

The table below identifies general ESXi host hardware considerations that impact the networking options.

ESXi Host Usage Description	Physical Specification of Network Capacity	Example Usage
Management Host	Includes an on-board dual port Network Interface Card	Management host
Single VM Host	<ul style="list-style-type: none"> <li>Includes an on-board dual port Network Interface Card</li> <li>Includes one dual port external Network Interface Card</li> </ul>	L2 production host with single workload consolidation ratios. For an example, see the Console Station Host description in the <i>HPS Virtualization Specification</i> available from the Honeywell Process Solutions web site.
Lower Point Counts	<ul style="list-style-type: none"> <li>Includes an on-board dual port Network Interface Card</li> <li>Includes two single port external Network Interface Cards</li> <li>Option to replace single port Network Interface Cards with two dual port external Network Interface Cards</li> </ul>	<ul style="list-style-type: none"> <li>L2 production host with multiple workloads and lower point count. For examples, see the Small, Medium or Large Cluster Host descriptions in the <i>HPS Virtualization Specification</i> available from the Honeywell Process Solutions web site</li> <li>L3 production host with local storage and low workload consolidation ratios.</li> </ul>
Higher Point Counts	<ul style="list-style-type: none"> <li>Includes an on-board dual port Network Interface Card</li> <li>Includes two dual port external Network Interface cards</li> <li>Supports the ability to replace the dual port Network adapter cards with two quad port Network Interface Cards</li> </ul>	<ul style="list-style-type: none"> <li>L2 production host with multiple workloads and higher point count. For examples, see the Performance Cluster Host descriptions in the <i>HPS Virtualization Specification</i> available from the Honeywell Process Solutions web site</li> <li>L3 production hosts with local storage and higher workload consolidation ratios</li> <li>L3 production host with shared storage</li> </ul>

- In the VMware environment, the physical network adapters on the ESXi host are named vmnic n, where n is unique number identifying a single port on the network interface card. For production ESXi hosts, the following network interface ports are required. Since, it is possible to deploy with single or multi-port network interface cards, the table below uses the VMware notation where one vmnic equals a single port on a network adapter card.

**Attention**

- Onboard NICs can be used for connections to the management and storage networks.
- External Network Interface cards can be used for production networks including FTE. Intel NICs can optionally be used for connection to FTE networks. For more information, see the *Fault Tolerant Ethernet (FTE) Specification* available from the Honeywell Process Solutions web site

Implementation type	Storage type	Minimum network interface card (NIC) requirements (including any on-board NICs)	Additional considerations
Level 2, on-process	Local	Each ESXi host must have four vmnics: <ul style="list-style-type: none"> <li>Two vmnics for connecting to each FTE network, that is, the yellow and green.</li> <li>Two vmnics for the management network. These are teamed.</li> </ul>	If supported by ESXi host, add two more vmnics for FTE mapped across separate Network Adapter Cards. The additional FTE vmnics are used to minimize scope of loss or increase network performance. See the figure "High Capacity ESXi Production Host with single FTE connection".

Implementation type	Storage type	Minimum network interface card (NIC) requirements (including any on-board NICs)	Additional considerations
Level 3, on-process	Local	Each ESXi host must have three vmnics: <ul style="list-style-type: none"> <li>One vmnic for connecting to the Level 3 production network.</li> <li>Two vmnics for the management network. These vmnics are teamed.</li> </ul>	If supported by the ESXi host, add one more vmnic for L3 production network. The additional vmnics are used to minimize scope of loss or increase network performance.
Level 3, on-process (option)	Shared	Each ESXi host must have five vmnics: <ul style="list-style-type: none"> <li>One vmnic for connecting to the Level 3 production network.</li> <li>Two vmnics for the management network. These vmnics are teamed.</li> <li>Two vmnics for the storage network.</li> </ul>	It is recommended to deploy with high capacity ESXi host. Consider use of a quad port adapter card to connect to the production and storage networks.

This guide provides a number of examples that illustrate the detailed ESXi host configuration from a network perspective. The figures "Network Connection for Management Host" and "High Capacity ESXi Production Host with single FTE connection" introduce the ESXi host notation that is used throughout the guide. See the ESXi host notation to ensure that:

- Network ports are identified from bottom right to upper right starting with vmnic0. Ports that are grouped together indicate use of a multi port Network Interface Card.
- Each ESXi host deployed with local storage, regardless of usage, uses the on-board dual port Network Interface Card to connect to the management network. This recommendation applies to both single and dual management network implementations. As a result, vmnic0 and vmnic1 are always assigned to the management network.
- Each ESXi host, regardless of usage, is configured to use VMware NIC teaming when configuring the uplink configuration from the management vSwitch (vSwitch0) to vmnic0 and vmnic1. For more information, see the "NIC Teaming" section that follows

The figure "Network Connection for Management Host" shows an example of the required connectivity between the vNetwork and the physical network at the level of an ESXi host used for management. Note the following regarding the connection from virtual machine to vSwitch0 to physical ports vmnic0 and vmnic1:

- The on-board dual port Network Interface Card is recommended for connection to the management network. This recommendation applies when implementing a dual or single management network.
- The management network requires configuration of a single vSwitch. vSwitch0 is created as a result of ESXi hypervisor installation.
- VMkernel connection to vSwitch0 is notated by ESXi management connection to vSwitch0. This enables network connectivity between the hypervisor and network.
- Management workload (for example, vCenterServer) is connected to vSwitch0 from single virtual NIC (vNIC0). This is a virtual machine port group.

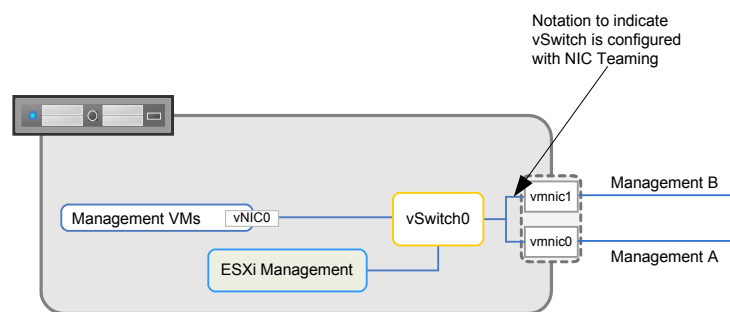


Figure 10: Network Connection for Management Host

The figure "High Capacity ESXi Production Host with single FTE connection" shows an example of the required connectivity between the vNetwork and the physical network at the level of an ESXi host used for L2

production. The network connection to the management network is identical to that shown in the figure above, with the exception that a production host does not include management workload. Note the following regarding the FTE connection from virtual machine to vSwitch1 and vSwitch2 to physical ports vmnic2 and vmnic4:

- A dual port Network Interface Card enables a single connection to the yellow side of the physical FTE network. An additional dual port Network Interface Card enables a single connection to the green side of the physical FTE network.
  - Note the recommendation of two dual port Network Interface cards for single FTE connection. Separation of FTE between two physical cards minimizes the scope of loss. In this case, the spare vmnics (vmnic3 and vmnic5) are reserved for future use. An example of future usage might be that unacceptable network performance of the Experion workload may warrant consideration to split the FTE workload between two FTE connections (see below).
  - Low capacity ESXi Production hosts (not shown) use either one dual port Network Interface Card or two single port Network Interface cards.
- Single FTE connection requires configuration of two vSwitches – one for yellow and one for green.
  - Dual FTE connection option (not shown): Configure an additional yellow vSwitch (vSwitch3) to connect to vmnic3. Configure an additional green vSwitch (vSwitch4) to connect to vmnic5. Consider this option if the host is planned to deploy FTE workload that warrants separation
- Each virtual machine with FTE is configured with two virtual NICs – one for yellow and one for green. In the single FTE connection example, Yellow virtual NIC is connected to vSwitch1. Green virtual NIC is connected to vSwitch2..
  - Dual FTE connection option (not shown): virtual machines with FTE are either connected to vSwitch1 and vSwitch2 OR to vSwitch3 and vSwitch4

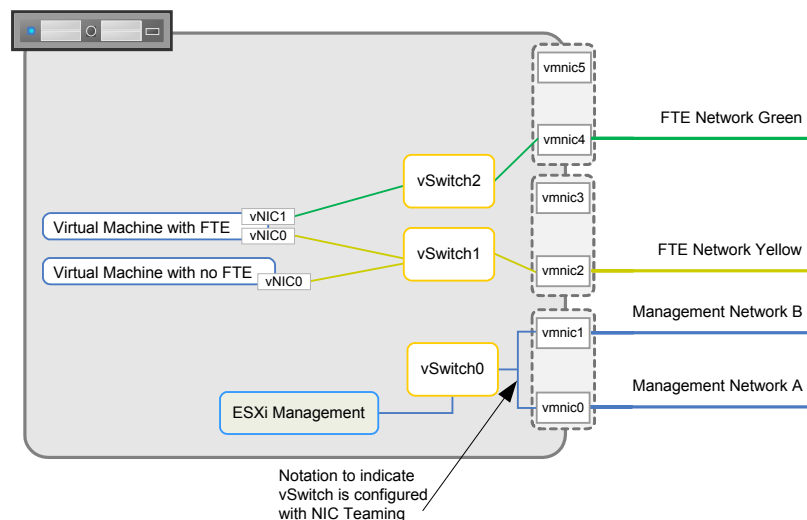


Figure 11: High Capacity ESXi Production Host with single FTE connection

### NIC teaming

VMware NIC teaming is the grouping together of several physical NICs in order to minimize the loss of network connectivity due to a PCI card failure in an ESXi host. VMware NIC teaming also provides a load balancing feature which when used in this context provides for a balance of the number of connections from the virtual network to the physical network. This is unlike typical load balancing in a physical network where traffic flow is balanced through all available adapters. to form a single logical NIC.

For on-process systems, VMware NIC teaming is recommended for the connection to the management network. Each vmnic used in the NIC team for the management network is configured as active in order to take advantage of the VMware load balancing feature. This applies to traffic from the ESXi host to the physical switches only. There are no required configuration settings on the physical switches.

NIC teaming can also be used at Level 3 for network fault tolerance and improved performance for connection to the storage network.

Below is a summary of the VMware NIC teaming expectations for each network type.

Network	Purpose of NIC teaming
Management	For fail over and VMware load balancing.
Storage	For fail over and performance.

VMware NIC teaming is a network policy property of each vSwitch. For example, enabling VMware NIC teaming for the management network connection requires configuration of vSwitch0.

### Switches and routers

The following table identifies the switch and router requirements, based on each network type.

Network type	Switch requirements
FTE network	Two switches, one for the green network and another for the yellow network. For more information about the FTE switch hardware requirements, see the <i>Product Specification for Experion Fault Tolerant Ethernet (FTE)</i> from the Honeywell Process Solutions web site ( <a href="http://www.honeywellprocess.com">http://www.honeywellprocess.com</a> ).



Network type	Switch requirements
Management network	<ol style="list-style-type: none"> <li>1. If implementing a non-redundant management network.                      Use one enterprise-class gigabit switch-router for the management network. For systems that implement multiple plant network levels, it is recommended that the management network be implemented in between the supervisory control level (Level 2) and the application control level (Level 3). When implemented in this fashion, the management network becomes Level 2.5 which is connected to Level 2 and Level 3. Establishing the management (Level 2.5) network also requires the following:                     <ul style="list-style-type: none"> <li>• Allocate four IP addresses in unused subnet for adding redundant IP routing between Level 2.5 and Level 3</li> <li>• Allocate an unused subnet with enough IP addresses to accommodate management network connections (for example, ESXi hosts, NAS, management client).</li> <li>• Hostname and IP for Level 2.5 router</li> </ul> </li> <li>2. If implementing a redundant management network.                      Use two enterprise-class gigabit switch-routers for the management network. A cross-over cable is required between the two switch-routers. For systems that implement multiple plant network levels, it is recommended that the management network be implemented in between the supervisory control level (Level 2) and the application control level (Level 3). When implemented in this fashion, the management network becomes Level 2.5 with Level 2.5 Router A and Level 2.5 Router B which are connected to Level 2 and Level 3. Establishing the management (Level 2.5) network also requires the following:                     <ul style="list-style-type: none"> <li>• Allocate four IP addresses in unused subnet for adding redundant IP routing between Level 2.5 and Level 3</li> <li>• Allocate unused subnet with enough IP addresses to accommodate management network connections (for example, ESXi hosts, NAS, management client).</li> <li>• Hostname and IP for Level 2.5 router A</li> <li>• Hostname and IP for Level 2.5 router B</li> </ul> </li> <li>3. If implementing a separate management network.                      Use one enterprise-class or small business class gigabit switch for the management network. For systems that implement multiple plant network levels, it is recommended that the management switch network be implemented at Level 2. When implemented in this fashion, the management network connects to Level 2.5. Establishing the management (Level 2) network also requires the following:                     <ul style="list-style-type: none"> <li>• Allocate four IP addresses in unused subnet for adding redundant IP routing between Level 2.5 and Level 3</li> <li>• Allocate an unused subnet with enough IP addresses to accommodate management network connections (for example, ESXi hosts, NAS, management client)</li> <li>• Hostname and IP for Level 2.5 router A</li> <li>• Hostname and IP for Level 2.5 router B</li> <li>• Single gigabit port in Level 2.5 router A for connection from management switch</li> </ul> </li> </ol> <p>For more information about the recommended switch-router specifications, see the <i>HPS Virtualization Specification</i> from the Honeywell Process Solutions web site.</p>
Storage network	If you are using shared storage, two storage network switches, which must be gigabit switches.

### ESXi host IP addresses

The following table identifies the IP address requirements for each ESXi host, based on each network type.

Network type	IP address requirements
Management network	One (1) static IP address for each ESXi Host that is connected to the management network.
Storage network	If using shared storage, four (4) static IP addresses for each ESXi host that is connected to the storage network. See the related documents for implementation details.

**Related topics**

“Determining the number of ESXi hosts and hardware requirements” on page 38

“Network configuration for a production host in a DCS architecture” on page 136

*After you complete the initial network configuration, you need to configure the virtual network for the production host.*

**Network requirements for a SCADA architecture**

There are specific network-related requirements for a SCADA architecture.

**Common network configuration decisions**

When implementing a production network for a SCADA architecture, you need to consider the following.

Consideration	Description
Network availability.	<p>At least 2 physical network adapters should be used in each ESXi host for the production network.</p> <p>For single Ethernet production networks, the network adapters are teamed together for network availability. Each teamed NIC connects a vSwitch to the physical network and switch.</p> <hr/> <p><b>! Attention</b></p> <ul style="list-style-type: none"> <li>Ensure that any physical network adapters used in a NIC team do not belong to the same embedded or PCI-e network card.</li> </ul> <hr/> <p>For dual Ethernet production networks, single physical network adapters connect separate vSwitches to the physical network and switch. As there are two paths of communication between the virtual machines and the SCADA controllers, a single network adapter failure should not result in a loss of view.</p> <p>For more information about dual networks, see the “Network redundancy with dual networks” topic in the <i>Server and Client Configuration Guide</i>.</p>
Network speeds.	<p>Network speeds affect the number of physical network connections from the ESXi host to the production network.</p> <p>Both 10/100Mbps and 1Gbps networks are supported for non-FTE production networks. The network speed that the physical production switch supports is the maximum bandwidth that the production vSwitch can support between virtual machines running on separate ESXi hosts to the SCADA controllers. This limitation needs to be used in any calculation for determining the number of virtual machines that can connect to each vSwitch.</p> <p>More network adapters may be required to satisfy the total virtual network throughput.</p> <hr/> <p><b>! Attention</b></p> <ul style="list-style-type: none"> <li>The recommended settings used for NIC teaming do not increase the network bandwidth for single virtual machines beyond the single physical uplink speed to the physical switch. The actual network adapter used is based on the virtual port that the virtual machine traffic entered the vSwitch.</li> </ul>
Network security.	<p>You should eliminate all unwanted network traffic in the production network. A gateway router can connect the production networks, management network, and IT environment/WAN networks.</p>

**ESXi hosts**

Each ESXi host must meet the following hardware requirements:

- Supported server-grade hardware. For more information about the server-grade hardware requirements, see the *HPS Virtualization Specification* from the Honeywell Process Solutions web site.


**Attention**

Use the same vendor, family, and generation of CPUs throughout your virtualization environment. This will ensure the portability of virtual machines when using vMotion.

- For operational ESXi hosts (that is, for ESXi hosts that contain process operational or application operational workloads), the following network interface cards (NICs) are required.

Implementation type	Storage type	Minimum network interface card (NIC) requirements (including any on-board NICs)
On-process	Local	Each ESXi host must have four network interface cards (NICs): <ul style="list-style-type: none"> <li>– two NICs for the production network</li> <li>– two NICs for the management network</li> </ul>
On-process	Shared	Each ESXi host must have six network interface cards (NICs): <ul style="list-style-type: none"> <li>– two NICs for the production network</li> <li>– two NICs for the management network</li> <li>– two NICs for the storage network</li> </ul> <div> <b>Attention</b>                      Honeywell recommends the use of NIC teaming, which is where two or more physical adapters are used to share the traffic load or provide passive failover in the event of a physical adapter hardware failure.                 </div>
Off-process	Local	Each ESXi host must have two network interface cards (NICs): <ul style="list-style-type: none"> <li>– one NIC for connecting to the production network</li> <li>– one NIC for connecting to the management network</li> </ul>
Off-process	Shared	Each ESXi host must have four network interface cards (NICs): <ul style="list-style-type: none"> <li>– one NIC for the production network</li> <li>– one NIC for the management network</li> <li>– two NICs for the storage network</li> </ul>


**Attention**

The network interface card (NIC) requirements described above represent the minimum requirements. You can use more NICs for each network.

### NIC teaming

For on-process systems, NIC teaming is recommended. NIC teaming is the grouping together of several physical NICs to form a single logical NIC. NIC teaming can be used for network fault tolerance and performance reasons. Here is a summary of the NIC teaming expectations for each network type.

Network	Purpose of NIC teaming
Management	For fail over, not performance.
Production	For fail over, not performance.
Storage	For fail over and performance.

### Gateway router

You need a gateway router to enable a connection between the production network and the IT environment. The gateway router provides access control connections between the production network, management network, IT environment, and optionally, the storage network. If you are creating a virtualization environment from an existing system, the gateway router may already exist.

### Switches

The following table identifies the switch requirements, based on each network type.

Network type	Switch requirements
Non-FTE network	A switch for the production network.
Management network	A switch for the management network, which must be a gigabit switch.
Storage network	If you are using shared storage, two (2) storage network switches, which must be gigabit switches.

### ESXi host IP addresses

The following table identifies the IP address requirements for each ESXi host, based on each network type.

Network type	IP address requirements
Management network	One (1) static IP address for the management network.
Storage network	If using shared storage, four (4) static IP addresses, one for each VMkernel. For each additional VMkernel, you need an additional storage network static IP address.

### Management workloads

The following requirements need to be met for the management workloads:

Implementation type	Management workload requirements
On-process usage	The management workloads of vCenter Server, vSphere Update Manager, VMware Data Recovery, and the Windows domain controller must be virtual machines. Other management workloads, can be either virtual or physical. However, there must be at least one instance of vSphere Client running on a physical computer.
Off-process usage	Can be either a physical server or one or more virtual machines.

### Related topics

“Determining the number of ESXi hosts and hardware requirements” on page 38

# Identifying virtualization hardware and software requirements

You need to consider other software and hardware requirements prior to implementing a virtualization environment.

## Related topics

“Software requirements” on page 53

*Software requirements are important and should be defined while planning a system.*

“Thin client requirements” on page 54

*For virtualized Experion client nodes, access to the user interface of the virtual machine is through a thin client. A thin client is a device that fulfills the traditional computational role of a typical workstation computer while the actual workload resides on a remote server, not on the thin client itself.*

“Other requirements” on page 54

*There are additional requirements for Experion virtualization.*

## Software requirements

Software requirements are important and should be defined while planning a system.

### VMware software and licenses

Ensure that the following VMware software and licenses are considered:

- For every ESXi host, a license based on the number of CPU sockets is required. The latest ESXi hypervisor software image is required.
- A vCenter Server license is required and a supported 64-bit operating system and license.
- If Site Recovery Manager is required, ensure that the Backup Control Center licensing of ESXi hosts and vCenter Server are included, plus add the Site Recovery Manager license to both sites.



#### Attention

vSphere Essentials Plus 4.1 and vSphere Standard 4.1 licensing restricts ESXi Host processors to 6 cores per socket. This limitation requires hardware with greater than 6 cores per socket to have the core count reduced to 6 cores per socket using the hardware BIOS. Failure to do this will result in licensing errors when connecting these ESXi Hosts to a vCenter Server. This limitation is removed from vSphere 5.0.

### Operating system software and licenses

Ensure that the operating systems being used in your virtual environment are correctly licensed. You can leverage either your own enterprise operating system agreements or Honeywell can supply these operating systems for you. Additionally, please ensure that there are no special licensing considerations for the applications that are running in the virtualized environment.

### Other software and licenses

Experion software and licensing should be considered for all required nodes in the system. Add licensing as required, based on the Experion system size and additional application and engineering functionality.

SQL server software and licensing (for vCenter Server and vSphere Update Manager) may be required if the virtual infrastructure has greater than 5 ESXi hosts or 50 virtual machines, as a standard version of SQL Server must be used. Add this license for each vCenter Server virtual node, if required.

## Thin client requirements

For virtualized Experion client nodes, access to the user interface of the virtual machine is through a thin client. A thin client is a device that fulfills the traditional computational role of a typical workstation computer while the actual workload resides on a remote server, not on the thin client itself.

Thin clients are physically connected to the same network as the virtual machines that they connect to. Typically, a thin client provides a single LAN connection only. If you need a dual Ethernet connection to a thin client, a secondary network media splitter or Redundant Port Protector can be placed in series between the thin client and the network switches that the thin client connects to. While thin clients can be connected to an FTE network, they are currently not FTE aware.

Typically, one thin client is required for each Flex Station or Console Station virtual machine. Depending on your site requirements and usage, thin clients may also be shared for Server, Engineering Station, and other Experion virtual machines.

For more information about the supported thin clients, see the *HPS Virtualization Specification*.

Refer to the *Wyse z90DE7 Thin Client Planning Installation and Service Guide* for information about deploying thin clients.



### Attention

Consideration	Description Column 2 heading	Options
High availability of thin client	<p>Thin clients are not FTE enabled devices. Deploying thin clients with a redundant port protector provides a higher level of availability. A redundant port protector will provide protection against:</p> <ul style="list-style-type: none"> <li>Cable failure between the thin client and its directly connected switch.</li> <li>Port or switch failure for the directly connected port and associated switch.</li> </ul> <p><b>Attention</b></p> <p>If the target virtual machine exists on a different set of FTE switches then the thin client, any failure of the upper level switches joining the two networks will not be re routed.</p>	<ul style="list-style-type: none"> <li>Consider use of thin clients with redundant port protectors when connected to the same FTE switch pair as the ESXi host with the client workload.</li> <li>Consider use of physical stations when the FTE community is implemented as a hierarchy of FTE switches and thin clients are not on the same set of FTE switches as the ESXi hosts.</li> <li>Consider a hybrid deployment of Station workload, such that at least one physical Station is FTE enabled and can take over for a thin client that has lost communication.</li> </ul>

## Other requirements

There are additional requirements for Experion virtualization.

### Windows domain controllers

For on-process usage, an additional Windows domain controller is required on the management network. This new domain controller is a peer to any existing domain controllers on the production network at Level 2 and Level 3. Make the domain controller on the management network a PDC emulator master if no other PDC emulator master exists. The PDC emulator master domain controller must be configured to synchronize to an external NTP time source.

For off-process usage, a minimum of one Windows domain controller is required.

Regardless of the usage, the Domain Name System (DNS) server needs to be implemented on all domain controllers. Configure DNS with forward and reverse lookup.

**Choosing what nodes to virtualize**

You may choose not to virtualize all node types. For more information, including known exceptions, see the *HPS Virtualization Specification*.

**Windows operating system updates**

You should use existing techniques for applying Windows operating system updates to virtual machines. The Experion best practices for installing Honeywell-qualified Microsoft updates are identified in chapter 6, “Microsoft Security Updates and Service Packs” of the *Network and Security Planning Guide*.

## Planning for the management ESXi host and management network

One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.

### Management network

Honeywell recommends that network traffic between ESXi hosts and the management host be directed to a separate network called the management network.



#### Attention

- Separating the management network traffic isolates access to the ESXi hosts, which is in alignment with Honeywell security recommendations.

One or more of the following items also reside on the management network:

- vSphere Client hosted on a physical computer.
- Network Attached Storage (NAS) device(s) will also be placed on the management network for use by Experion Backup and Restore (EBR) for storage of virtual machine backups of both management and production workloads. For more information, see the related topics.

### Management ESXi host

A management ESXi host runs the management workload. Management workload consists of virtual machines that run on the management host and only connect to the management network. Examples of management workload are vCenter Server and EBR. EBR runs as a virtual machine as it is supplied as an appliance. An example of a management workload that can run as either a physical machine or a virtual machine is a domain controller.

Management nodes are virtual machines on the management ESXi host. The management ESXi host runs management workloads and has a connection to the management network only. There is no connection to the production network. When planning the management host consider the number of and type of management nodes to be included as this will determine the sizing and performance requirements of the hardware. Consider the role that the management ESXi host will play in creation of templates and virtual machines as this will require more storage capacity to be planned for this node.

Basic rules used when selecting the management ESXi host hardware are:

- Ensure that the CPU in the hardware provides as many logical processors as the number of total planned virtual CPU in the host. This consideration includes any template or Experion node virtual machines that may be created on the management hosts. A simple approach for this rule may be selecting a Quad core physical CPU (with hyper-threading) that supports 8 logical processors. The vCenter requires 2 vCPU, domain controller requires 2 vCPU, EBR requires 2 vCPU and this leaves 2 vCPU for staging Experion virtual machine installations. It is important not to underestimate this requirement in the management ESXi host as CPU contention caused by running too many vCPU compared to logical processors will lead to high CPU ready time and all management workloads will slow down.
- Ensure that the allocated memory is supported by physical RAM in the hardware. This rule requires that all allocated memory run on physical RAM so that ballooning and swapping never occurs in the ESXi Host.
- Ensure that management workloads run on a separate group of disks compared to any template or Experion installation virtual machine. This rule separates the critical management virtual machines disk usage from any virtual machines used for staging an operating system installation or Experion installation. This separation ensures that high disk requests and throughput demanded by the installations do not affect the management workload performance. A simple approach to follow for this is to build a RAID group for management workload and a separate RAID group for staging virtual machine installations.
- Ensure that the disk storage capacity is adequate for the virtual machines planned to run and also stored on the management ESXi host. Never plan to use more than 70% of the total datastore space.



## Supported management workloads

The supported management workloads are:

- Domain controller
- VMware vCenter Server, including VMware Update Manager
- VMware vSphere Client (optional)
- Experion Backup and Restore (EBR)
- VMware Site Recovery Manager

### Domain controller

Including the domain controller in the management host serves the purpose of providing domain controller redundancy for the system (as other domain controllers are required) and reducing the cost of providing hardware for this required node. If domain infrastructure already exists and the management network has the required access, the domain controller may not be required on the management host. Ensure that the domain intended for vCenter Server is a member exists before vCenter Server is prepared.

### vCenter Server

vCenter Server is a windows application that is installed on a virtual machine running a supported 64-bit Windows operating system. This virtual machine is the central point to the management of the virtual infrastructure and allows the creation, configuration, management and control of the virtual infrastructure. Using vCenter Server, you can manage the ESXi hosts and their virtual machines from a single user interface. vCenter Server consists of a server component and an agent running on each ESXi host. The server component, vCenter Server, runs on a management node and contains a database to store the configuration and performance data. The vCenter Server database must reside on the vCenter Server node. Each ESXi host includes a vCenter Agent that provides the required communication between each ESXi host and the vCenter Server.

### vSphere Client

A vSphere Client virtual machine is in addition to the physical vSphere Client requirement. This virtual machine should contain a 32-bit Windows operating system and can be used for the creation of an ESXi virtual hard disk and Utility virtual hard disks, which are used for the installation of Experion virtual machines.

vSphere Client virtual machine is an optional requirement that can be used for the primary connected virtual machine when using vSphere Client to manage and configure the virtual environment. It may be required when there is a desire to restrict interactive access to the vCenter Server for security purposes.

When connecting to the vCenter Server, the vSphere Client authenticates access to the vCenter Server by way of Windows authentication. If you are using vSphere Client to connect to an ESXi host directly, the vSphere Client authenticates access by way of a local ESXi host account.



#### Tip

The content and procedures in this guide are based on the usage of the vSphere Client.

### Experion Backup and Restore (EBR)

The EBR node is deployed into the management host and connects to the management network to perform backup and recovery tasks. A NAS device is used as the de-duplication store for this appliance and this NAS device is also connected to the management network. For more information about the planning and configuration of EBR, see the related topics.

For more information about the requirements for the virtual machines that reside on the Management Host, see the *HPS Virtualization Specification*.

### Using the management host to stage the installation of production workloads

The management host can be used to provide a part of the virtual infrastructure where Experion virtual machines and operating system templates can be created and stored. This ESXi host is ideal as an installation platform, as it segregates the installation process away from potential disk I/O effects on the process workloads

and stops potential interference on the process networks. To accommodate for this type of workload, consideration needs to be made where you select the management host hardware. Define the installation scenarios and template creation scenarios that your system requires, and provide enough resources on the management host to successfully accomplish this. As there is limited storage on a management host, you cannot stage or store the virtual machines of an entire Experion system. You should move staged Experion virtual machines to the required production ESXi host or a NAS device.

Do not stage Experion virtual machine installations on live production ESXi hosts.

To successfully stage Experion virtual machine installations on the management host:

- One or more virtual switches configured with the same name and setting as the production ESXi hosts. These virtual switches are configured with no up-links.
- Separate disk groups for management workload and installation workload to protect the management workloads from disk contention. Use a separate build/installation volume. Do not use the management volume as a storage repository.
- DVD media converted to ISO format for operating systems and Experion installation. These ISO files are uploaded to the build/installation volume on the management host.
- Resource pools for the installation virtual machines configured with CPU limits to protect the management workloads.

### Related topics

“Overview of distributing workload across ESXi hosts for a DCS architecture” on page 29

*An ESXi host's workload consists of the set of nodes that reside as guests on that host. When planning for the distribution of the nodes, you need to consider the type of workloads to be deployed.*

“Determining the number of ESXi hosts and hardware requirements” on page 38

“Overview of distributing workload across ESXi hosts for a SCADA architecture” on page 34

“Creating a vCenter Server virtual machine with bundled SQL” on page 119

“Planning to backup the virtual infrastructure and virtual machines” on page 70

*Plan for the use of Experion Backup and Restore (EBR) to perform backups of the virtual infrastructure and virtual machines.*

“Preparing a vCenter Server” on page 118

*On the management ESXi host, you need to create a virtual machine to host the vCenter Server (and vCenter Update Manager). The vCenter Server contains the required software components for the administration of virtual machines, ESXi hosts, and the virtualization environment. You need to install a vCenter Server to manage the virtual environment.*

## Planning the management network in a DCS architecture

The management network spans the entire system in order to provide management access to all elements of the virtualization infrastructure.

In this context, virtual infrastructure refers to the basic elements needed to enable consolidation of workload (virtual machines) one or more hardware platforms together with the means to manage those virtual machines and the hosting hardware. Specifically, the virtual infrastructure includes:

- ESXi hosts
- Hypervisor installed on each ESXi host
- Virtual machines
- Virtual infrastructure management tools
- Management User Interfaces
- Backup Devices

At the core of the virtual infrastructure is the virtual infrastructure management tools, which are used to:

- configure the virtualized system
- create virtual servers and desktops
- provision of virtual machines to hosts
- start virtual machines and monitoring their health
- monitor the health of hosts
- backup and restore virtual machines to/from backup devices
- facilitate the update of each element of the virtual infrastructure

The management network is used to perform these tasks. Adding the management network to a system to serve the needs of the FTE networks at the production level as well as the that of the application level requires special considerations.

### **Planning the management network for usage with multiple plant levels**

A multi-plant level Experion system is typically deployed with a Level 2 subnet with a minimum of two FTE switches for each FTE community, Level 3 subnet and Level 3 router, and a firewall and additional routers that restricts connection to and from Level 3.5 and the enterprise level. The management network is inserted between the FTE production network (Level 2) and the application network (Level 3). The management network is a dual one gigabyte network that is connected to the production and application levels of the system with a redundant set of multi-layer switches with routing capabilities. The ESXi hosts, vSphere Clients and backup devices are connect directly to the management network. Each ESXi host, regardless of the plant level location is also directly connected to the management network. This connection for ESXi hosts is in addition to the required production network connections (that is, FTE at Level 2). Physical nodes that are used for production at Level 2, Level 3 or Level 3.5 have no connection to the management network, and are therefore, are not managed by, nor visible to the virtual infrastructure management tools.

### **Dual management network**

Dual management networks are supported for DCS architecture networks.

This requires the following:

- a separate pair of network interface ports on each ESXi host
- a separate pair of multi-layer switches with routing capabilities with crossover cable
- cabling

In a multiple plant level system, the dual management network can be implemented between the supervisory level (Level 2) and the application level (Level 3). This deployment is referred to as Level 2.5.

### **Related topics**

“Network configuration for a management host in a DCS architecture” on page 113

*After you complete the initial network configuration, you need to configure the virtual network for the management host.*

## **Planning the management network in a SCADA architecture**

A single management network is supported for SCADA architecture networks.

This requires a separate pair of network interface ports on each ESXi host and a separate management network switch and cabling. Both the production and management networks are routed to a gateway router that enables secured access to business network (WAN).

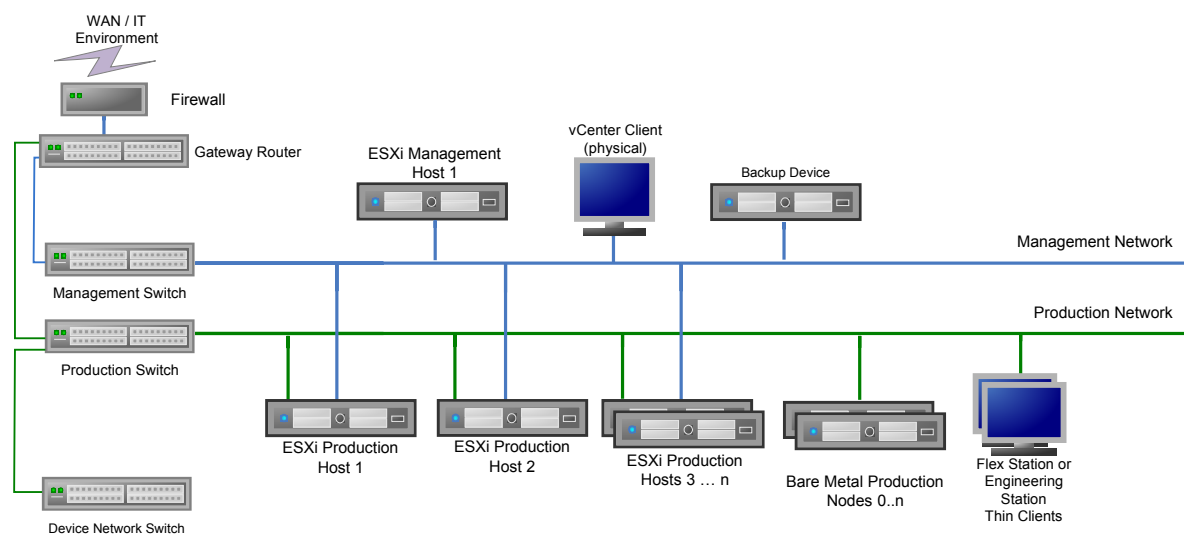


Figure 12: Example SCADA architecture topology with a single management network

## Planning how to organize the vCenter Server

Hosts and their virtual machines should be organized within vCenter Server based on logical groupings.

These logical grouping will be different for each site depending on the scale of the virtualization environment and topology.

### Related topics

“Organizing VMware inventory objects” on page 125

*You should identify how to organize inventory objects in vCenter Server.*

## VMware inventory objects

VMware inventory objects are used to help manage and organize hosts and virtual machines within the VMware virtualization environment. VMware inventory objects include datacenters, folders, hosts, and virtual machines. You can organize these inventory objects into a hierarchy to help monitor and manage the VMware virtualization environment.

VMware inventory objects include datacenters, folders, hosts, and virtual machines. You can organize these inventory objects into a hierarchy to help monitor and manage the VMware virtualization environment.

Object	Description
datacenter	<p>A <i>datacenter</i> is the primary container of inventory objects, such as hosts and virtual machines. A vCenter Server can contain multiple datacenters.</p> <p>For large virtualization implementations, datacenters can be used to represent organizational units within the enterprise. In addition to providing a container, the datacenter also serves as a boundary when using advanced features including vMotion.</p> <p>For Experion virtualizations, a datacenter is used to contain all of the Experion virtual machines.</p>
folder	<p>A <i>folder</i> is a container to further refine the grouping of inventory objects, for example, to group objects based on a physical location. Folders can also be used to assign security permissions. Inventory objects placed within a folder have the same permissions as the folder.</p> <p>For large virtualization implementations, folders can be used to group datacenters, and then within datacenters, folders can be used to group related ESXi hosts for an Experion cluster or system. You can use folders to group hosts into any logical grouping that suits your organization.</p>
ESXi host	<p>A <i>host</i> is a computer that is running ESXi virtualization software to run virtual machines.</p> <p>Hosts provide the CPU and memory resources that the virtual machines use and give virtual machines access to storage and network resources. Multiple virtual machines can run a host at the same time.</p>

There are other inventory objects, such as clusters and resource pools. For more information about these inventory objects, see the “vSphere Managed Inventory Objects” section of *vSphere Server and Host Management*.

## Datacenter organization guidelines

The recommended steps for creating an organization hierarchy within vCenter Server (within the **Home > Inventory > Hosts and Cluster** view) is:

1. Create a datacenter.
2. Create and organize folders within the datacenter.
3. Add the ESXi hosts to the folders.

After you add an ESXi host, you configure the ESXi host network settings, and then you can create virtual machines on the ESXi host.

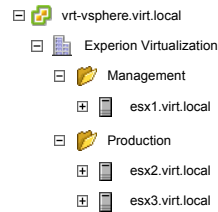
### Organizing the datacenter

Folders should be used to group like components within the systems, for example, hosts, virtual machines, templates, and so on. When naming a folder, give it a name that clearly identifies this logical grouping. As your virtualization environment grows over time, specific hardware can be more easily found in its folder as opposed to having to search through all generic names to find a given virtual machine or host. You can create folders within other folders to further refine these groupings.

**Attention**

- ESXi hosts should be allocated to either on-process usage or off-process usage.

### Example datacenter organization



In this example, at the top of the tree is the vCenter Server (management node) name. This node name cannot be changed.

At the next level of the tree is a datacenter, which is 'Experion Virtualization'.

This datacenter is further organized into 'Management' and 'Production' folders, containing the ESXi hosts that contain the management workloads and production workloads, respectively.

# Planning for time synchronization

Time synchronization requires an NTP server to distribute time throughout the virtual infrastructure.



An NTP server could reside outside of the virtual infrastructure, or it could be a virtual machine. All virtual machines synchronize time from this NTP server.


## Time synchronization considerations

Identify the NTP server that will be the main timekeeper for the virtual environment. The NTP server could be a physical piece of hardware, such as a computer or switch, or it could be the primary Experion server. You may already have an established NTP source for serving time to the control hardware.

Ensure that the identified NTP server can be accessed by the virtual machines.

Using the table below, determine the time synchronization scenario based on whether you are using a Windows workgroup or domain:

Windows domain	<p>Set up time synchronization by following the instructions in the “Setting up time synchronization in a Windows domain checklist” topic in the “Setting up time synchronization” chapter of the <i>Supplementary Installation Tasks Guide</i>.</p> <p>Consider if your Domain controllers are virtual machines or physical machines as this will change the requirement for an external time source. When all domain controllers are virtual machines an external time source is required as the local clock on the virtual machine will drift. The following VMware white paper gives more detail <i>Virtualizing a Windows Active Directory Domain Infrastructure</i>.</p> <p>When you have a domain controller running as a physical machine the local clock of this machine can provide a time reference that can be used for the domain. This domain controller will need to be set as the PDC emulator. In this scenario a Windows server uses the local clock as the time reference, the value of Root Dispersion for NTP reply sent back to the ESXi Host will have a value too high for the ESXi host to use. Changing the following Registry setting in the Windows server from its default value of 10 to a new value of 0 will adjust the root dispersion value to a value that will allow the ESXi hosts to successfully synchronize time:</p> <pre>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\LocalClockDispersion</pre> <div>  <b>Attention</b> <ul style="list-style-type: none"> <li>The ESXi hosts must synchronize with the domain controller or the external time source that the domain controller synchronizes with.</li> </ul> </div>
Workgroup without an external time source	<p>Set up time synchronization by following the instructions in the “Setting up time synchronization in a workgroup without an external time source checklist” topic in the “Setting up time synchronization” chapter of the <i>Supplementary Installation Tasks Guide</i>.</p> <p>When using virtual machines as the authoritative time source, time drift can occur and this practice is not recommended.</p> <div>  <b>Attention</b> <ul style="list-style-type: none"> <li>The ESXi hosts must synchronize with the authoritative root server. In this scenario a Windows server uses the local clock as the time reference, the value of Root Dispersion for NTP reply sent back to the ESXi Host will have a value too high for the ESXi host to use. Changing the following Registry setting in the Windows server from its default value of 10 to a new value of 0 will adjust the root dispersion to a value that will allow the ESXi hosts to successfully synchronize time:</li> </ul> </div> <pre>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\LocalClockDispersion</pre>

Workgroup with an external time source	<p>Set up time synchronization by following the instructions in the “Setting up time synchronization in a workgroup with an external time source checklist” topic in the “Setting up time synchronization” chapter of the <i>Supplementary Installation Tasks Guide</i>.</p> <hr/> <p> <b>Attention</b> The ESXi hosts must synchronize with the external time source.</p>
--	---



## Planning to maintain the VMware environment

You need to consider how to maintain and update the VMware components within a virtualization environment.

### Related topics

“About vSphere Update Manager” on page 65

*With vSphere Update Manager, you can automate patch management and eliminate manual tracking and patching of ESXi hosts.*

“Considerations for VMware maintenance when using local storage” on page 66

*To remediate or apply a patch or upgrade requires the ESXi host to be placed into maintenance mode.*

“Considerations about upgrades, patches, and updates” on page 66

*Understand the differences between upgrades, patches, and updates.*

### About vSphere Update Manager

With vSphere Update Manager, you can automate patch management and eliminate manual tracking and patching of ESXi hosts.

Honeywell recommends that you use vSphere Update Manager to administer and automate the application of patches and updates to ESXi hosts.

You can use vSphere Update Manager to:

- Apply patches to ESXi hosts.
- Upgrade ESXi hosts to new releases.
- Upgrade VMware Tools within virtual machines.
- Upgrade virtual machine hardware versions.
- Upgrade virtual appliances.

For applying patches to Windows guest operating systems, Honeywell recommends that you use the existing techniques for applying Windows operating system updates to virtual machines. The Experion best practices for installing Honeywell-qualified Microsoft updates are described in “Microsoft Security Updates and Services Packs” of the *Network and Security Planning Guide*.

VMware Tools and virtual machine hardware version upgrades require the virtual machine to be restarted. Therefore, you should coordinate the remediation of these upgrades to occur with the installation of Honeywell and qualified Microsoft updates.

Honeywell recommends that the vSphere Update Manager be installed on the vCenter Server virtual machine.

vSphere Update Manager requires a database. The same database should be across the virtualization environment. That is, you should use the same database that is used for vCenter Server, and the database location should be on the vCenter Server virtual machine. For Essentials Plus deployments, you can use the Microsoft SQL Server 2008 R2 Express database included with vCenter Server. For larger virtualization deployments, use a Microsoft SQL Server database. Database planning and installation is required.

For more information about planning a Update Manager deployment, see *Installing and Administering VMware vSphere Update Manager*.

### Related topics

“Creating a vCenter Server virtual machine with bundled SQL” on page 119

## Considerations for VMware maintenance when using local storage

To remediate or apply a patch or upgrade requires the ESXi host to be placed into maintenance mode.

Maintenance mode requires all virtual machines on the ESXi host to be moved to another ESXi host using vMotion, or for the virtual machines on the ESXi host to be shutdown. vMotion is not supported when the virtual machines are stored on the local storage of an ESXi host. Therefore, to remediate or apply a patch or upgrade to an ESXi host with local storage requires all virtual machines on the ESXi host to be shutdown.

If on-process patching or upgrading of an ESXi host is required, the issue of all virtual machines on the ESXi host to be shutdown at the same time must be considered when assigning Experion virtual machines to an ESXi host. To perform an on-process patch or upgrade of an ESXi host, virtual machines, or virtual appliances (VAs) requires a predefined process or plan. The process or plan must clearly specify the shutdown and restart order of virtual machines, VAs, and ESXi hosts that support the running of the process.

Honeywell recommends that ESXi host patches and upgrades be done during planned outages if virtual machines are stored on the local storage of an ESXi host.

Update Manager cannot be used to patch or upgrade an ESXi host if it hosts a local storage vCenter Server. All virtual machines on the ESXi host must be shutdown before it can be patched or upgraded. Shutting down vCenter Server will shutdown the Update Manager.

The ESXi host of a local storage virtual vCenter Server must be patched or upgraded manually.

## Considerations about upgrades, patches, and updates

Understand the differences between upgrades, patches, and updates.

### What are upgrades?

An upgrade is a VMware version or point release change. For example, an upgrade is required to go from version 5.0 to 5.1.

An upgrade affects multiple components of the VMware infrastructure, including:

- vSphere Client
- vCenter Server
- Update Manager
- ESXi hosts
- VMWare Tools
- virtual machine hardware versions

To maintain communication between these components during the upgrade process, the upgrade must be completed in a specific order. It is important to use VMware upgrade documentation to perform the upgrade. In addition, it is also important to keep in mind the local storage special considerations during the upgrade process.

### What are patches?

A patch contains one or more cumulative bulletins and patches a specific VMware version. For example, a patch name is ESXi410-201104001.

The patch details include information on the action required on the ESXi host and hosted virtual machines. For example, if the ESXi host needs to be restarted, if the hosted virtual machines need to be shutdown.

Patches typically affect a single component so they can be applied without the concern of losing communications with other components.

### What are updates?

An update is a bulletin within a patch that contains a rollup of patches for a release. For example, 4.1 Update 1 includes all of the version 4.1 patches up to the date when 4.1 Update 1 was released.

# Planning security for the VMware environment

You need to consider how to implement security within the VMware virtualization environment.

## User accounts, roles, and permissions

VMware user accounts are not created within vCenter. Instead, vCenter authorizes users based on accounts defined within the Windows operating system, either on a Windows domain controller or local Windows users on the vCenter Server. Within vCenter, you define roles and configure appropriate permissions for these roles. You then assign Windows users or groups to these roles.

### vCenter Server users

Honeywell recommends that user accounts be maintained within Active Directory on a Windows domain. It is also recommended that you use the Honeywell High Security Policy, and assign users to the High Security Policy global groups. You can then assign global groups to vCenter roles. For more information about the Honeywell High Security Policy, see the “Honeywell High Security Policy” topic in the “Securing access to the Windows operating system” chapter of the *Network and Security Planning Guide*.

When planning for virtualization, you need to identify the roles required to meet your security needs, and the permissions required for each role.

Honeywell recommends that you create the following roles in vCenter:

Role	Responsibilities
Virtualization Administrator	<ul style="list-style-type: none"> <li>Manages the Datacenter and the provision of resources.</li> <li>Creates and configures the virtual machines.</li> <li>Creates and maintains the network configuration.</li> <li>Manages updates to the ESXi hosts and virtual machines.</li> <li>Defines security for the ESXi host.</li> <li>Manages other virtual appliances.</li> </ul>
Experion Virtualization Administrator	<ul style="list-style-type: none"> <li>Manages Experion virtual machines.</li> <li>Manages patches to virtual machine guest operating system and Experion software.</li> <li>Creates and configures Experion virtual machines.</li> <li>Starts up and shuts down Experion virtual machines.</li> </ul>
Experion Virtualization User	Starts up and shuts down Experion virtual machines.

For more information about roles and permissions, including the hierarchical inheritance of permissions and details about each permission, see the following VMware references:

- "Authentication and User Management" in *vSphere Security*
- *Defined Privileges*

### Roles and Experion security groups

Honeywell recommends that the following users or global groups be assigned the following roles:

Assign the following vCenter role	To the following user or global group
Virtualization Administrator	System administrator users.
Experion Virtualization Administrator	<i>Honeywell Administrators</i> or <i>Product Administrators</i> global group.
Experion Virtualization User	<i>Local Engineers</i> global group.

**ESXi host users**

Each ESXi host has two default users:

- The *root* user has full administrator privileges.
- The *vpuser* is a user created only when the ESXi host is being managed by a vCenter Server, and is the account used by vCenter Server to manage activities on that ESXi host.

**Related topics**

“Assigning vCenter roles to Experion users or global groups” on page 128

*After you have defined vCenter roles, assign the role to the required Experion users or global groups to associate these access permissions to the datacenter and its contents.*

“Creating vCenter roles and assigning privileges” on page 128

*vCenter roles are a collection of defined privileges that control individual user or group access to particular vSphere objects.*

**About host lockdown mode**

Host lockdown mode prevents remote users from logging into an ESXi host using the root user and password.

Host lockdown mode must be enabled to restrict direct access to the ESXi host. That is, remote access to the ESXi host through the vSphere Client, the remote command-line interface (CLI), and access through the Virtual Infrastructure (VI) API are not allowed for the root user.

**Attention**

- The root user is still authorized to log in to the direct console user interface when host lockdown mode is enabled.

Host lockdown mode does not affect how other users access virtual machines through the vSphere Client or Remote Desktop Connection (RDC).

Before you enable host lockdown mode, add the ESXi host to the vCenter Server inventory. If you try to enable host lockdown mode before adding the ESXi host to a vCenter Server, the enabling of host lockdown mode will fail. When you add an ESXi host to vCenter Server, you can choose to enable the host lockdown mode at that time. In emergency situations where direct access to the ESXi host is required, you can disable host lockdown mode by logging in to the ESXi host console directly and disabling host lockdown mode.

**Related topics**

“Configuring host lockdown mode” on page 129

*Host lockdown mode ensures that the ESXi host is managed only through vCenter Server.*

**About VMware security hardening**

In addition to guidelines in this document, when implementing your virtual infrastructure, Honeywell recommends that you follow the guidelines provided by VMware.

These guidelines are documented in the *vSphere 5.5 Update 1 Security Hardening Guide (HardeningGuide-vSphere5-5-Update-1-GA.xlsx)*. This guide deals with three general operating environments:

- All Environments - Profile 3
- Sensitive Environments - Profile 2
- Highest Security Environments - Profile 1

For Experion virtualized deployments you should consider off-process systems as being in the "Profile 3" operational environment and on-process systems should be considered as being in the "Profile 2" operational environment. Due to other recommendations in this document in regards to the structure of your virtual infrastructure, some of the guidelines in the *VMware Hardening Guide* may not be applicable or suitable for Experion systems. Details for these are specified below. In addition, only the “ESXi”, “vNetwork”,

“vCenterServer”, “VUM”, and “SSO” sections of the *vSphere 5.5 Update 1 Security Hardening Guide* should be followed.

VMware also provides a Compliance Checker for vSphere Client to help check the status of your system against these hardening guidelines.

### ESXi hardening

All ESXi hardening guidelines should be considered. However, based on a typical Experion virtualized system, the following guidelines could be discounted when hardening the virtual infrastructure:

- Discount all profile 1 items
- esxi-no-self-signed-certs - This affects communication on the management network, which already has limited access as it is largely not shared with other networks. If, however you have a suitable certificate infrastructure at your site, you may implement this guideline.
- enable-remote-syslog - Unless an existing syslog infrastructure exists, to which the management network could connect, there is little value in adding this if the Experion infrastructure has a low ESXi host count.

Please also note the following comments regarding other host hardening guidelines:

- config-snmp - Ensure SNMP is disabled unless you have an appropriate SNMP infrastructure.
- verify-config-files - This information is only available on the management network.

### vNetwork hardening

Please note the following comments regarding network hardening:

- Discount all profile 1 items.
- isolate-mgmt-network-vlan - Domain Controller, RDP and ports related to WSUS and anti-virus also need to be allowed between management network.
- All DVS subcomponent items- Honeywell does not support distributed vSwitches.

### vCenterServer hardening

The following guidelines could be discounted when hardening your vCenterServer infrastructure:

- Discount all Profile 1 items.
- install-with-service-account - Honeywell allows the use of the SYSTEM account for running the vCenter Server services. This only applies to deploying vCenter Server with bundled SQL.
- no-self-signed-certs, restrict-certificate-access - Unless an existing certification infrastructure exists, Honeywell allows self-signed certificates to be used due to the isolation of the management network.
- disable-datastore-browser - This has a large impact on diagnosing any problems that may occur in your virtual infrastructure so for Experion systems this guideline should not be followed.
- no-vum-self-signed-certs - Unless an existing certification infrastructure exists, Honeywell allows self-signed certificates to be used due to the isolation of the management network.

### VUM hardening

For Update Manager, Honeywell recommends following all Profile 1 hardening guidelines with the possible exception of:

- no-vum-self-signed-certs - Unless an existing certification infrastructure exists, Honeywell allows self-signed certificates to be used due to the isolation of the management network.

### SSO hardening

Please note the following comments regarding network hardening:

- no-SSO-self-signed-certs - Unless an existing certification infrastructure exists, Honeywell allows self-signed certificates to be used due to the isolation of the management network.

## Planning to backup the virtual infrastructure and virtual machines

Plan for the use of Experion Backup and Restore (EBR) to perform backups of the virtual infrastructure and virtual machines.

Virtual machine and virtual infrastructure backup uses two different mechanisms:

- EBR: This is the primary backup tool that allows virtual machine backups to be moved out of the virtual infrastructure and onto separate storage. This data can also be moved to different physical locations for Disaster recovery if required.
- Virtual Machine Replication: uses PowerShell scripting to clone virtual machines to different ESXi hosts. This method is useful for virtual machines that run applications that are inherently non-redundant. This backup method is to be used in addition to EBR as a backup method.

The following table outlines scenarios where EBR, Virtual machine replication, or no action should be used when virtual machines and ESXi hosts are powered off.

Scenario	EBR	Replication	No Backup Action	Comment
Hardware failure, repaired within 1 hour and all data lost	X			Use EBR and restore directly to repaired Host
Hardware failure, repaired within 1 hour and no data lost			X	
Hardware failure, replace host within 1 hour,	X			Use EBR and restore directly to new host.
Hardware failure, repair longer than 1 hour and no data lost.		X		
Hardware failure, repair longer than 1 hour and all data lost.	X	X		Run replication VMs immediately and transition back to original VMs after using EBR to restore to the repaired ESXi host.
Hardware failure, replacement host takes longer than 1 hour	X	X		Run replication VMs immediately and transition back to original VMs after using EBR to restore to new ESXi host.
Hypervisor Update			X	
Virtual Machine complete failure in Guest Operating system.	X			Use EBR to restore single virtual machine directly to Host.
Virtual Machine loss of files.	X			Use EBR to restore a file from a backed up virtual machine.

### Planning for EBR

EBR should run on the management ESXi host, so as not to put additional load on the production ESXi hosts. EBR consumes two vCPU, 2 GB of memory, and disk performance on the ESXi host where it is running.

Honeywell recommends the use of network attached storage (NAS) for the EBR backup data. Sizing guidelines are described in the *VMware Data Recovery Administration Guide*.



#### Attention

- The backup storage device must be installed and operational before installing EBR.

If you are using shared storage, ensure the destination location for backups are on different disk arrays to the virtual machines being backed up. This will ensure that an array failure will not lose the original virtual machines and the backups.

**Attention**

- For virtual machines that were created using vSphere 4.0 and later upgraded: If you plan to back up Windows Server 2008 virtual machines initially created in vSphere 4.0 and later upgraded, you need to enable the disk UUID attribute in VMware Tools. For more information, see the *VMware Data Recovery Administration Guide*.

**Backup storage device considerations**

Honeywell recommends use of a file share on a NAS.

The following list summarizes the planning considerations for each backup storage type:

- Network file share on a NAS

Smaller backup location sizes are allowed. The NAS must be accessible from the management network. Examples are the Iomega PX4–300 series network storage devices, with the windows file share (CIFS) service enabled, connected to the management network. You may need to consider an additional NIC on the management ESXi host to handle the additional network traffic.

- Local storage on the ESXi

A second hard drive needs to be added to the EBR appliance (ensure that you use SCSI controller 1). The location of this second hard drive is a local datastore. The block size of this datastore may need to be increased to allow for a larger hard drive size. For more information about block sizes and datastores, see the Block size limitations of a VMFS datastore (KB1003565) knowledge base article on the VMware web site.

An example of local storage is using the local datastore of the management host for the storage of backups of Experion virtual machines running on other ESXi hosts.

- iSCSI target

A second hard drive needs to be added to the EBR (ensure that you use SCSI controller 1). The location of this second hard drive is the desired datastore. The block size of this datastore may need to be increased to allow for a larger hard drive size.

An example of an iSCSI target is using a second iSCSI SAN on the storage network that has a LUN configured for use by management host as a datastore. This datastore will only be used by EBR as the backup store.

**Related topics**

“Planning for the management ESXi host and management network” on page 56

*One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.*

“Replicating a virtual machine” on page 150

“Determining the number of ESXi hosts and hardware requirements” on page 38

**Planning for disaster recovery**

Disasters do happen, so it is important that critical management workloads containing your virtualization infrastructure, along with your production workloads, are backed up.

**Backing up your virtualization infrastructure**

The following nodes need to be considered in any backup plan:

- vCenter Server

Including the Microsoft SQL Server database used to store the information about your virtualization infrastructure. The Microsoft SQL VSS Writer needs to be installed on this node. This virtual machine will be vital in restoring the rest of your virtual infrastructure in the event that it is lost.

- Domain controller

At least one domain controller should be backed up. In the event that all domain controllers are lost this one can be restored and other domain controllers can be built from scratch and synchronized with this one.

If at least one domain controller survives the disaster, domain controller should not be restored, instead a new domain controller should be created.

- Anti-virus software, WSUS, and so on

Any other management workload that contains important state information.

For any of these machines that use Microsoft SQL Server, ensure that the Microsoft SQL VSS Writer is installed.

Also ensure that VMware Tools is installed on all management workloads.

The use of VMWare Tools and VSS Writer helps to ensure that the operating system is correctly disabled prior to doing a vDR backup.

### **Off-site backup**

The frequency that the backups are taken off-site is determined by the importance of the data and systems. Any mission-critical systems or data (those that must be recovered within minutes or hours of a system failure) must be backed up and taken off-site daily, as a minimum. The location you choose is important. The backups must not only be safe and secure, but quickly and easily accessible in the event of a disaster.

Honeywell recommends that you transfer your backup data onto a removable media on a regularly-scheduled basis. You can store the media off-site in a secure temperature-controlled environment for long-term storage. In addition, you can define the backup retention period for the media.

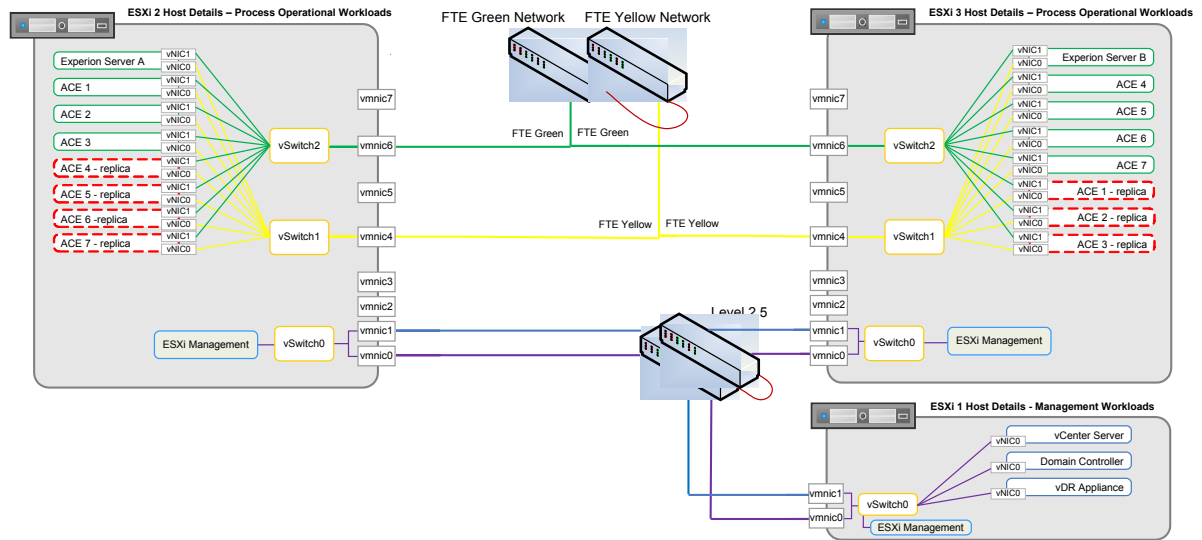
For details of how to create and restore backups on the NAS, see the related topics.

## **Planning to replicate the virtual machines**

Virtual machine replication is the process where a workload that is not inherently redundant is automatically replicated onto a peer ESXi host. This solution uses scheduled PowerShell scripts to periodically check for specific changes to virtual workload and initiate the cloning process when required. In the event of a failure of an ESXi Host any replicated workload can be powered on and used until the failure is rectified.

Virtual machine replication is primarily used for ACE virtual machines in an Experion system. However, methodologies could be applied to other non-redundant virtual machines if required. The ACE virtual machines can be made available very quickly in the event of a hardware failure when an ESXi host is unavailable for an extended period of time.





**Figure 13: Example ACE workload replicated onto a different production ESXi host**

The virtual system illustrated above is an example of a system where ACE workload is replicated onto a different production ESXi Host and maintained in a powered off state. The virtual machines with the suffix "-replica" in the name are the cloned virtual machines from the other ESXi Host. In this example "ACE 1" is running on ESXi Host 2 and the replica of ACE 1 called "ACE 1 - replica" is not running but exists in the inventory on ESXi Host 3. In the event of a hardware failure on ESXi Host 2 the replica virtual machine "ACE 1 - replica" can be quickly powered on and this will allow the control strategy run by "ACE 1" to now be run by "ACE 1 - replica". When the hardware failure is rectified and the original virtual machine "ACE 1" is again available, the replica virtual machine "ACE 1 - replica" can be powered off then "ACE 1" can be powered on and the control strategy restarted on "ACE 1".

### ESXi Host resource requirements

Successful implementation of replication requires all ESXi Hosts that are intended to run any replicated workload to have enough hardware resources. This is important so that resource contention does not occur. Each replicated virtual machine needs to be considered as a normal workload on the ESXi Host when determining the workload deployment.

Refer to “Determining the number of ESXi hosts and hardware requirements” to ensure that the hardware is provisioned correctly.

Refer to “Replicating a virtual machine” for implementation details.



# Implementing networks for a DCS architecture

## Related topics

“Implementing a non-redundant management network for a DCS architecture” on page 76

*Prior to implementing the management hosts and virtual infrastructure tools, the management network must be established and configured.*

“Implementing a redundant management network for a DCS architecture” on page 81

*Prior to implementing the management hosts and virtual infrastructure tools, the management network must be established and configured.*

“Implementing a separate management network for a DCS architecture” on page 86

*Prior to implementing the management hosts and virtual infrastructure tools, the management network must be established and configured.*

## Implementing a non-redundant management network for a DCS architecture

Prior to implementing the management hosts and virtual infrastructure tools, the management network must be established and configured.

Shown below is the typical network topology for a multiple plant level system with the management network at Level 2.5.

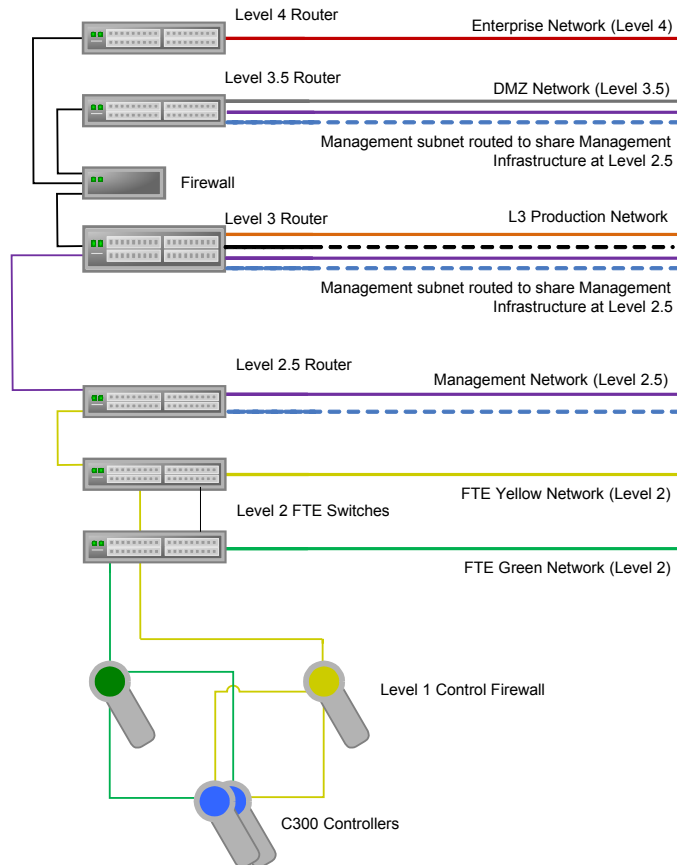


Figure 14: Example network topology with the non-redundant management network at Level 2.5

### Prerequisites

The procedures to establish the network levels other than Level 2.5 are beyond the scope of this guide. The *Experion Network Best Practices Guide* provides recommendations and guidelines to consider when establishing Level 1, Level 2, Level 3, Level 3.5 and Level 4. Honeywell Network Services can be consulted for the proper configuration of the router at Level 3.

The Fault Tolerant Ethernet Overview and Implementation Guide can also be used to establish Level 1 and Level 2 networks.

The procedure to connect Level 2.5 to Level 3 requires the establishment of Level 3 network including the configuration of the Level 3 router(s).

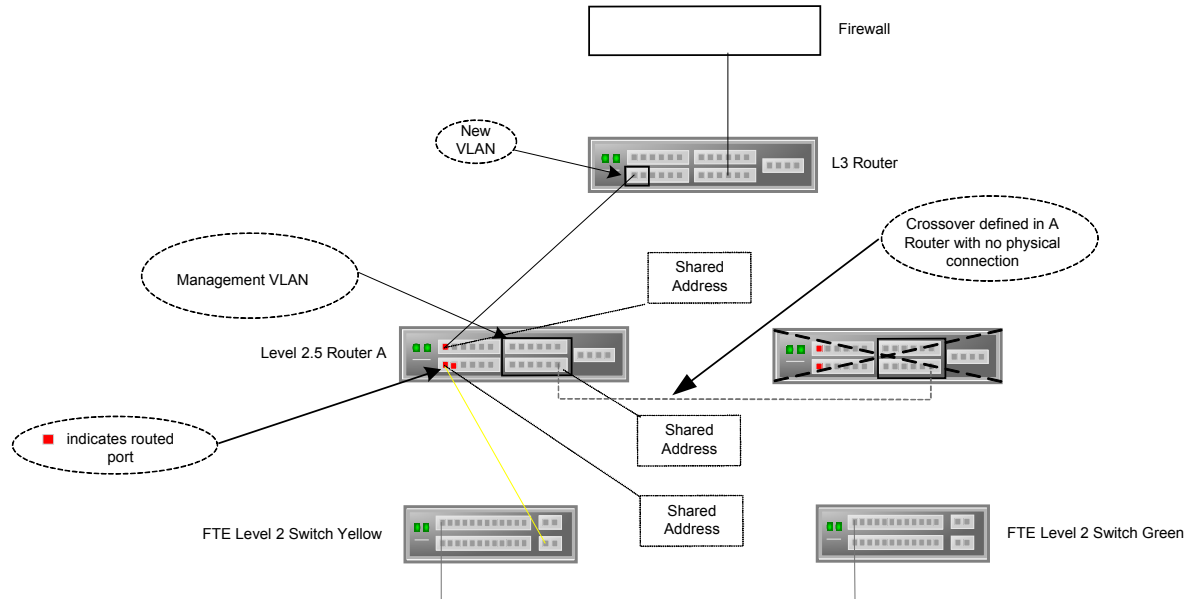
The procedure to connect Level 2 to Level 2.5 requires the establishment of Level 2 (FTE) including the configuration of FTE switches for each FTE community.

The figure below illustrates the connection of Level 2.5 to Level 3 with the use of a single Level 3 router connected to a single Level 2.5 router. This option requires that the Level 2.5 router support routing redundancy. The configuration of the single L2.5 router is implemented with dual redundancy. This approach enables usage

of the Honeywell provided L2.5 configuration templates. No update is required if dual redundancy is physically implemented at some later time.

From the figure below, note the following:

- Use of a single Level 2.5 router that supports routing redundancy. For example, Cisco Systems' Hot Standby Router Protocol (HSRP).
- Allocation of two Level 3 router ports in the same VLAN. This VLAN is dedicated to the connection to the A and B Level 2.5 routers. One port will be unused at this time.
- Common definition of a VLAN in both Level 2.5 A and B routers for the management network.



**Figure 15: Connection of non-redundant Level 2.5 to Level 3 using a single Level 3 router**


An alternative approach is to use redundant Level 3 routers with a VLAN common between the two Level 3 routers. This would be similar to that which is illustrated above for the Level 2.5 Routers or the FTE Level 2 switches and would therefore include the use of a crossover between the primary and secondary Level 3 routers.


The table below can be used as a guide to performing the Level 3 and Level 2.5 router configuration tasks to establish the management network as shown in the figure above. This procedure assumes usage of the recommended Cisco switch-routers that support HSRP.

**To implement the management network for a DCS architecture (configure the Level 2.5 router and connect it to the Level 3 router)**

Stage	Task	Description
Define subnets required by adding management network and Level 2.5 HSRP subnet.	1. Allocate four IP addresses in an unused subnet for use redundant IP routing between Level 2.5 and Level 3. This assumes a single Level 3 router where Level 2.5 connections are grouped together on Level 3 router with a VLAN.	IP addresses required to run with the HSRP in Level 2.5 1. Level 3 VLAN IP address 2. Unique IP address for Level 2.5 A router connection in Level 3 VLAN 3. Unique IP address for Level 2.5 B router connection in Level 3 VLAN 4. Subnet mask for Level 3 VLAN 5. Shared address for items 2 and 3 above.

Stage	Task	Description																									
	2. Allocate unused subnet with enough IP address to accommodate all management network connection requirements.	<ul style="list-style-type: none"><li>IP addresses for the management VLAN<ol style="list-style-type: none"><li>Unique IP address for Level 2.5 A router connection.</li><li>Unique IP address for Level 2.5 B router connection (for future use).</li><li>Subnet mask for items 1 and 2 above.</li><li>Shared address for items 1 and 2 above.</li></ol></li><li>IP addresses for all other management connected devices (ESXi hosts, management client, NAS, and vDR).</li></ul>																									
Prepare to update the Level 3 router configuration.	3. Allocate 1 physical interface (port) on the router. Note that you may be re-allocating an existing interface that is currently used for Level 2 connection to Level 3. Reserve 1 physical interface (port) on the router for future use.	<table><tr><th>Interface (Port) Usage</th><th>Quantity</th><th>Gigabit</th><th>Routed Port</th><th>Switch Port</th></tr><tr><td>Level 2.5 A</td><td>1</td><td>O</td><td></td><td>Y</td></tr><tr><td>Level 2.5 B</td><td>1</td><td>O</td><td></td><td>Y</td></tr></table> <p>O = Optional Y = Yes</p>	Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port	Level 2.5 A	1	O		Y	Level 2.5 B	1	O		Y										
Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port																							
Level 2.5 A	1	O		Y																							
Level 2.5 B	1	O		Y																							
	4. Define the ID of the new VLAN on the Level 3 router.	New VLAN ID																									
	5. Be familiar with how to update the current configuration of the Level 3 router																										
Prepare to configure the Level 2.5 router.	6. Download the Level 2.5 router A template and the Level 2.5 router B template from the Honeywell Process Solutions web site ( <a href="http://www.honeywellprocess.com">http://www.honeywellprocess.com</a> ) .	<p>The templates define a configuration for a 24 port switch router from the Cisco family of switch routers.</p> <p>Honeywell recommends usage of the port allocation scheme as defined in the templates.</p> <p>The default definition in the configuration files is for usage with non-stackable switch-routers. Modifications are required for usage with stackable switch-routers.</p>																									
	7. Validate that the IOS in the Level 2.5 router meets the site requirements for minimum IOS version.	Consult with site policies regarding the minimum IOS version that should be installed in the Level 2.5 switch-router.																									
	8. Define host name for each router.																										
	9. Allocate physical interfaces (ports) for each Level 2.5 router.  Note that FTE community connections are defined as the top level of yellow side for the Level 2.5. (The top side of green side would be allocated on the 2nd router if implemented in the future	<table><tr><th>Interface (Port) Usage</th><th>Quantity</th><th>Gigabit</th><th>Routed Port</th><th>Switch Port</th></tr><tr><td></td><td>1</td><td>Y</td><td>Y</td><td></td></tr><tr><td>FTE Communities</td><td>1 per community</td><td>O</td><td>Y</td><td></td></tr><tr><td>Virtual Infrastructure Management Connections</td><td>1 per connection</td><td>Y</td><td></td><td>Y</td></tr><tr><td>Crossover Cable</td><td>1</td><td>Y</td><td></td><td>Y</td></tr></table> <p>O = Optional Y = Yes</p>	Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port		1	Y	Y		FTE Communities	1 per community	O	Y		Virtual Infrastructure Management Connections	1 per connection	Y		Y	Crossover Cable	1	Y		Y
Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port																							
	1	Y	Y																								
FTE Communities	1 per community	O	Y																								
Virtual Infrastructure Management Connections	1 per connection	Y		Y																							
Crossover Cable	1	Y		Y																							

Stage	Task	Description
	10. For each FTE community, know the FTE IP addresses that are used for HSRP between Level 2.5 and Level 2.	IP addresses for each FTE community: <ol style="list-style-type: none"> <li>1. Unique IP address for yellow connection in FTE community subnet.</li> <li>2. Unique IP address for green connection in FTE community subnet.</li> <li>3. Subnet mask for FTE Community.</li> <li>4. Unique shared virtual address (default gateway) for FTE Community.</li> </ol>
	11. Define management network VLAN.	Define VLAN ID (this is pre-defined in Level 2.5 template files as 401).
	12. Review ACLs.	Update to be site compliant.
	13. Be familiar with how to set up and access the Level 2.5 routers for configuration.	 <b>Tip</b> Loading the Level 2.5 configuration files is similar to the steps documented in section 9.7, “Configuring Cisco Switches” of the <i>Fault Tolerant Ethernet Overview and Implementation Guide</i> .
Complete physical connections.	14. Complete the physical connections according to the interface (port) allocations established in the router preparation tasks for both Level 3 and Level 2.5.	Use the information defined in tasks 3 and 9.
Update the Level 3 router configuration.	15. Add VLAN for Level 2.5 connections.	Use the information defined in tasks 1.1 and 4.
	16. Update the IP route settings.	Add the IP address of the VLAN defined in task 1.5.
	17. Add interface for uplink from Level 2.5 A router.	Use the information defined in tasks 3 and 4: <ul style="list-style-type: none"> <li>• Assign the interface to the VLAN defined in task 15.</li> <li>• Do not assign an IP address.</li> <li>• Disable any discover protocol.</li> </ul>
	18. Add interface for uplink from Level 2.5 B router (for future use).	Use the information defined in tasks 3 and 4: <ul style="list-style-type: none"> <li>• Assign the interface to the VLAN defined in task 15.</li> <li>• Do not assign an IP address.</li> <li>• Disable any discover protocol.</li> </ul>
Configure Level 2.5 router.	19. Create configuration file	Preferred method is to use the Honeywell provided Level 2.5 templates (see task 6). These instructions assume usage of the preferred method to create Level 2.5 configuration file.
	20. Add VLAN for Management Network	Pre-defined in the A template (that is, VLAN 401) as its own spanning tree instance.  No additional updates if the pre-definition is suitable for usage.
	21. Add the interface for the Level 3 router connection.	Use the information defined in tasks 1.2, 1.4, 1.5 and 9.  Pre-defined in the template with HSRP activated.
	22. Add a interface for each Yellow FTE community connection.	Use the information defined in tasks 9 and 10.1, 10.3, and 10.4.

Stage	Task	Description
	23. Add the interface range for the Virtual Infrastructure connections.	Use the information defined in tasks 9 and 11.
	24. Add the interface for the crossover cable.	Use the information defined in tasks 9 and 11.
	25. Add the VLAN interface for the management network.	Use the information defined in tasks 2.1, 2.3, 2.4 and 11 (for A router).  This is pre-defined in the template to activate HSRP on the default gateway IP address of the management network.
	26. Update the IP route settings.	Add default route for the IP address of the Level 3 VLAN.  Use the information from task 1.1.
	27. Copy the updated configuration file to the Level 2.5 router.	 <b>Tip</b> Loading the Level 2.5 configuration files is similar to the steps documented in section 9.7, “Configuring Cisco Switches” of the <i>Fault Tolerant Ethernet Overview and Implementation Guide</i> .
Confirm that the Level 2.5 router is operational	28. Validate the following: 1. No blocked ports. 2. Correct states for Primary. 3. Protocol and interface are “active”	Use: 1. Sho span. 2. Sho standby (Primary is in active state). 3. Sho interface (Interface is Up, Protocol is Up).



# Implementing a redundant management network for a DCS architecture

Prior to implementing the management hosts and virtual infrastructure tools, the management network must be established and configured.

Shown below is the typical network topology for a multiple plant level system with the management network at Level 2.5.

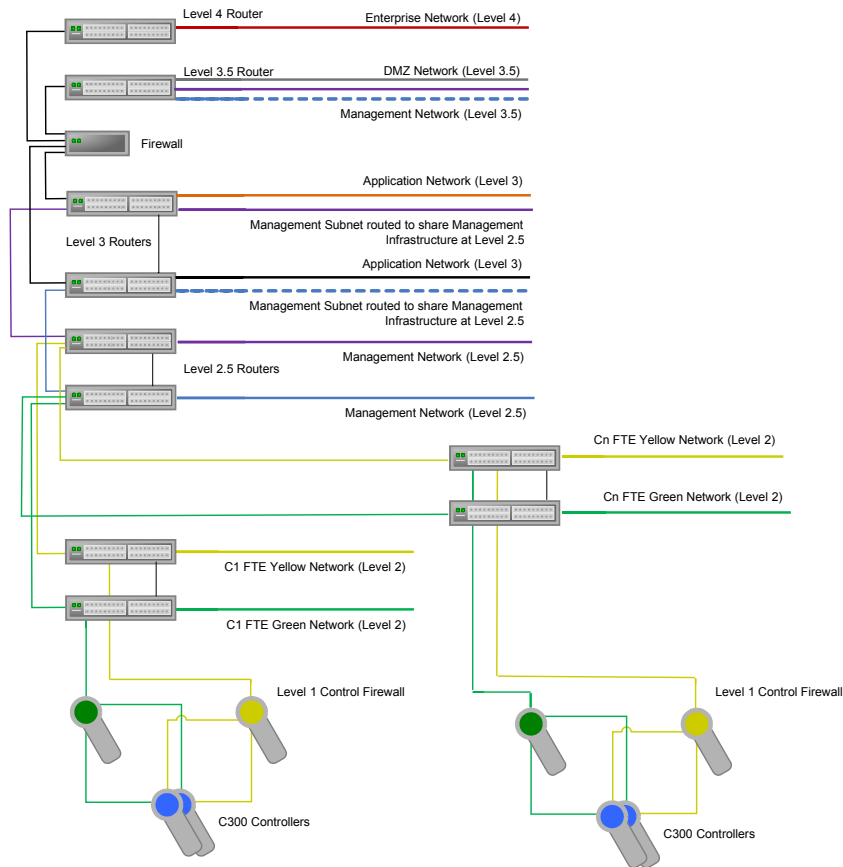


Figure 16: Example network topology with the redundant management network at Level 2.5

## Prerequisites

The procedures to establish the network levels other than Level 2.5 are beyond the scope of this guide. The *Experion Network Best Practices Guide* provides recommendations and guidelines to consider when establishing Level 1, Level 2, Level 3, Level 3.5 and Level 4. Honeywell Network Services can be consulted for the proper configuration of the router at Level 3.

The Fault Tolerant Ethernet Overview and Implementation Guide can also be used to establish Level 1 and Level 2 networks.

The procedure to connect Level 2.5 to Level 3 requires the establishment of Level 3 network including the configuration of the Level 3 router(s).

The procedure to connect Level 2 to Level 2.5 requires the establishment of Level 2 (FTE) including the configuration of FTE switches for each FTE community.

The figure below illustrates the connection of Level 2.5 to Level 3 with the use of a single Level 3 router connected to a pair of Level 2.5 routers. This option requires that the Level 2.5 routers support routing redundancy.

From the figure below, note the following:

- Use of redundant Level 2.5 routers that support routing redundancy. For example, Cisco Systems’ Hot Standby Router Protocol (HSRP).
- Allocation of two Level 3 router ports in the same VLAN. This VLAN is dedicated to the connection to the A and B Level 2.5 routers.
- Common definition of a VLAN in both Level 2.5 A and B routers for the management network.

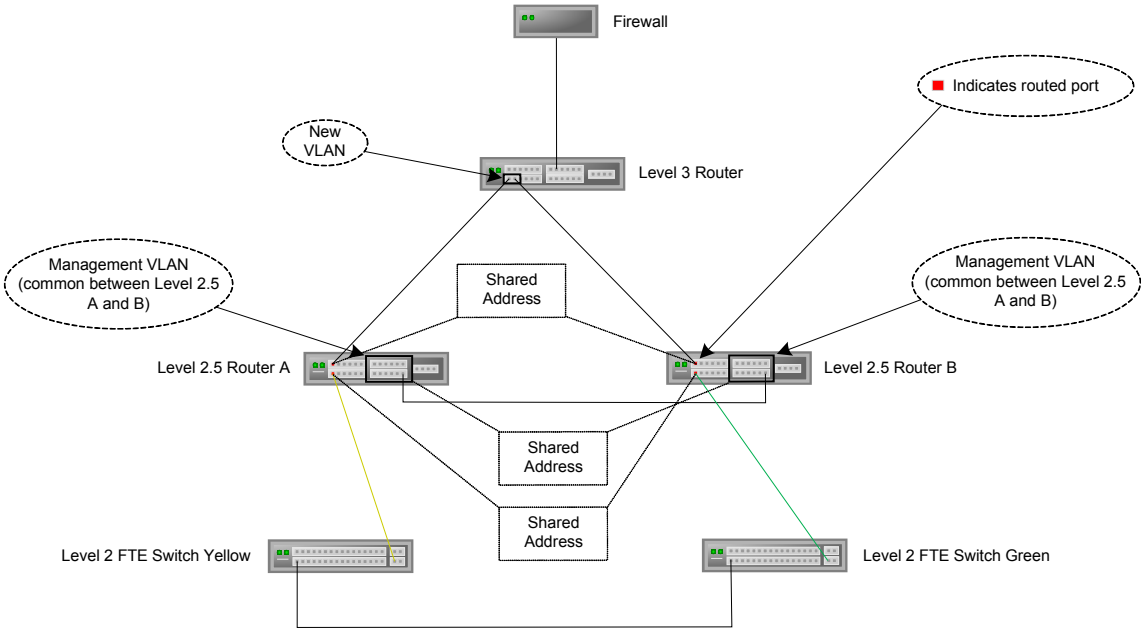


Figure 17: Connection of redundant Level 2.5 to Level 3 using a single Level 3 router


An alternative approach is to use redundant Level 3 routers with a VLAN common between the two Level 3 routers. This would be similar to that which is illustrated above for the Level 2.5 Routers or the FTE Level 2 switches and would therefore include the use of a crossover between the primary and secondary Level 3 routers.


The table below can be used as a guide to performing the Level 3 and Level 2.5 router configuration tasks to establish the management network as shown in the figure above. This procedure assumes usage of the recommended Cisco switch-routers that support HSRP.

To implement the management network for a DCS architecture (configure the Level 2.5 router and connect it to the Level 3 router)

Stage	Task	Description
Define subnets required by adding management network and Level 2.5 HSRP subnet.	1. Allocate four IP addresses in an unused subnet for use redundant IP routing between Level 2.5 and Level 3. This assumes a single Level 3 router where Level 2.5 connections are grouped together on Level 3 router with a VLAN.	IP addresses required to run with the HSRP in Level 2.5 1. Level 3 VLAN IP address 2. Unique IP address for Level 2.5 A router connection in Level 3 VLAN 3. Unique IP address for Level 2.5 B router connection in Level 3 VLAN 4. Subnet mask for Level 3 VLAN 5. Shared address for items 2 and 3 above.

Stage	Task	Description																									
	2. Allocate unused subnet with enough IP address to accommodate all management network connection requirements.	<ul style="list-style-type: none"><li>IP addresses for the management VLAN<ol style="list-style-type: none"><li>Unique IP address for Level 2.5 A router connection.</li><li>Unique IP address for Level 2.5 B router connection.</li><li>Subnet mask for items 1 and 2 above.</li><li>Shared address for items 1 and 2 above.</li></ol></li><li>IP addresses for all other management connected devices (ESXi hosts, management client, NAS, and vDR).</li></ul>																									
Prepare to update the Level 3 router configuration.	3. Allocate 2 physical interfaces (ports) on the router Note that you may be re-allocating an existing interface that is currently used for Level 2 connection to Level 3.	<table><tr><th>Interface (Port) Usage</th><th>Quantity</th><th>Gigabit</th><th>Routed Port</th><th>Switch Port</th></tr><tr><td>Level 2.5 A</td><td>1</td><td>O</td><td></td><td>Y</td></tr><tr><td>Level 2.5 B</td><td>1</td><td>O</td><td></td><td>Y</td></tr></table> <p>O = Optional Y =Yes</p>	Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port	Level 2.5 A	1	O		Y	Level 2.5 B	1	O		Y										
Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port																							
Level 2.5 A	1	O		Y																							
Level 2.5 B	1	O		Y																							
	4. Define the ID of the new VLAN on the Level 3 router.	New VLAN ID																									
	5. Be familiar with how to update the current configuration of the Level 3 router																										
Prepare to configure the Level 2.5 A and B routers.	6. Download the Level 2.5 router A template and the Level 2.5 router B template from the Honeywell Process Solutions web site.	<p>The templates define a configuration for a 24 port switch router from the Cisco family of switch routers.</p> <p>Honeywell recommends usage of the port allocation scheme as defined in the templates.</p> <p>The default definition in the configuration files is for usage with non-stackable switch-routers. Modifications are required for usage with stackable switch-routers.</p>																									
	7. Validate that the IOS in the Level 2.5 A router is the same version as the IOS in the Level 2.5 B router.	<p>Ensure that each switch router is installed with the same IOS version to avoid communication problems.</p> <p>Consult with site policies regarding the minimum IOS version that should be installed in each Level 2.5 switch-router.</p>																									
	8. Define host name for each router.																										
	9. Allocate physical interfaces (ports) for each Level 2.5 router.  Note that FTE community connections are defined as the top level of yellow side for the Level 2.5 A and top side of green side for Level 2.5 B.	<table><tr><th>Interface (Port) Usage</th><th>Quantity</th><th>Gigabit</th><th>Routed Port</th><th>Switch Port</th></tr><tr><td>Level 3</td><td>1</td><td>O</td><td>Y</td><td></td></tr><tr><td>FTE Communities</td><td>1 per community</td><td>O</td><td>Y</td><td></td></tr><tr><td>Virtual Infrastructure Management Connections</td><td>1 per connection</td><td>Y</td><td></td><td>Y</td></tr><tr><td>Crossover Cable</td><td>1</td><td>Y</td><td></td><td>Y</td></tr></table> <p>O = Optional Y =Yes</p>	Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port	Level 3	1	O	Y		FTE Communities	1 per community	O	Y		Virtual Infrastructure Management Connections	1 per connection	Y		Y	Crossover Cable	1	Y		Y
Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port																							
Level 3	1	O	Y																								
FTE Communities	1 per community	O	Y																								
Virtual Infrastructure Management Connections	1 per connection	Y		Y																							
Crossover Cable	1	Y		Y																							

Stage	Task	Description
	10. For each FTE community, know the FTE IP addresses that are used for HSRP between Level 2.5 and Level 2.	IP addresses for each FTE community: <ol style="list-style-type: none"> <li>1. Unique IP address for yellow connection in FTE community subnet.</li> <li>2. Unique IP address for green connection in FTE community subnet.</li> <li>3. Subnet mask for FTE Community.</li> <li>4. Unique shared virtual address (default gateway) for FTE Community.</li> </ol>
	11. Define management network VLAN.	Define VLAN ID (this is pre-defined in Level 2.5 template files as 401).
	12. Review ACLs.	Update to be site compliant.
	13. Be familiar with how to set up and access the Level 2.5 routers for configuration.	 <b>Tip</b> Loading the Level 2.5 configuration files is similar to the steps documented in section 9.7, “Configuring Cisco Switches” of the <i>Fault Tolerant Ethernet Overview and Implementation Guide</i> .
Complete physical connections.	14. Complete the physical connections according to the interface (port) allocations established in the router preparation tasks for both Level 3 and Level 2.5.	Use the information defined in tasks 3 and 9.
Update the Level 3 router configuration.	15. Add VLAN for Level 2.5 connections.	Use the information defined in tasks 1.1 and 4.
	16. Update the IP route settings.	Add the IP address of the VLAN defined in task 1.5.
	17. Add interface for uplink from Level 2.5 A router.	Use the information defined in tasks 3 and 4: <ul style="list-style-type: none"> <li>• Assign the interface to the VLAN defined in task 15.</li> <li>• Do not assign an IP address.</li> <li>• Disable any discover protocol.</li> </ul>
	18. Add interface for uplink from Level 2.5 B router.	Use the information defined in tasks 3 and 4: <ul style="list-style-type: none"> <li>• Assign the interface to the VLAN defined in task 15.</li> <li>• Do not assign an IP address.</li> <li>• Disable any discover protocol.</li> </ul>
Configure Level 2.5 A router.	19. Create configuration file	Preferred method is to use the Honeywell provided Level 2.5 templates (see task 6). These instructions assume usage of the preferred method to create Level 2.5 configuration file.
	20. Add VLAN for Management Network	Pre-defined in the A template (that is, VLAN 401) as its own spanning tree instance.  No additional updates if the pre-definition is suitable for usage.
	21. Add the interface for the Level 3 router connection.	Use the information defined in tasks 1.2, 1.4, 1.5 and 9.  Pre-defined in the template with HSRP activated.
	22. Add a interface for each Yellow FTE community connection.	Use the information defined in tasks 9 and 10.1, 10.3, and 10.4.

Stage	Task	Description
	23. Add the interface range for the Virtual Infrastructure connections.	Use the information defined in tasks 9 and 11.
	24. Add the interface for the crossover cable.	Use the information defined in tasks 9 and 11.
	25. Add the VLAN interface for the management network.	Use the information defined in tasks 2.1, 2.3, 2.4 and 11 (for A router).  This is pre-defined in the template to activate HSRP on the default gateway IP address of the management network.
	26. Update the IP route settings.	Add default route for the IP address of the Level 3 VLAN.  Use the information from task 1.1.
	27. Copy the updated configuration file to the Level 2.5 A router.	 <b>Tip</b> Loading the Level 2.5 configuration files is similar to the steps documented in section 9.7, “Configuring Cisco Switches” of the <i>Fault Tolerant Ethernet Overview and Implementation Guide</i> .
Configure Level 2.5 B router.	28. Repeat tasks 19 through to 26 for the Level 2.5 B router.	Predefined in the B template. Adjust the Level 2.5 A tasks as follows: <ul style="list-style-type: none"> <li>• Task 21: Use the information defined in tasks 1.3, 1.4, 1.5 and 9.</li> <li>• Task 22: Use the information defined in tasks 9 and 10.2, 10.3, and 10.4.</li> <li>• Task 25: Use the information defined in tasks 2.2, 2.3, 2.4, and 11 (for B router).</li> </ul>
	29. Copy the updated configuration file to the B device	
Confirm that Level 2.5 Routers are operational	30. Validate the following: <ol style="list-style-type: none"> <li>1. No blocked ports.</li> <li>2. Correct states for Primary/Secondary.</li> <li>3. Protocol and interface are “active”</li> </ol>	Use: <ol style="list-style-type: none"> <li>1. Sho span.</li> <li>2. Sho standby (Primary is in active state, Secondary is in standby state).</li> <li>3. Sho interface (Interface is Up, Protocol is Up).</li> </ol>

## Implementing a separate management network for a DCS architecture

Prior to implementing the management hosts and virtual infrastructure tools, the management network must be established and configured.

Shown below is the typical network topology for a multiple plant level system with single management network at Level 2 that is connected to Level 2.5 or Level 3. The primary difference between this implementation and that of the previous section is that the management network connection is limited to a single routed port on Level 2.5 or Level 3 network layer. This implementation approach can be used with a new or pre-existing Level 2.5 or Level 3 network layer.

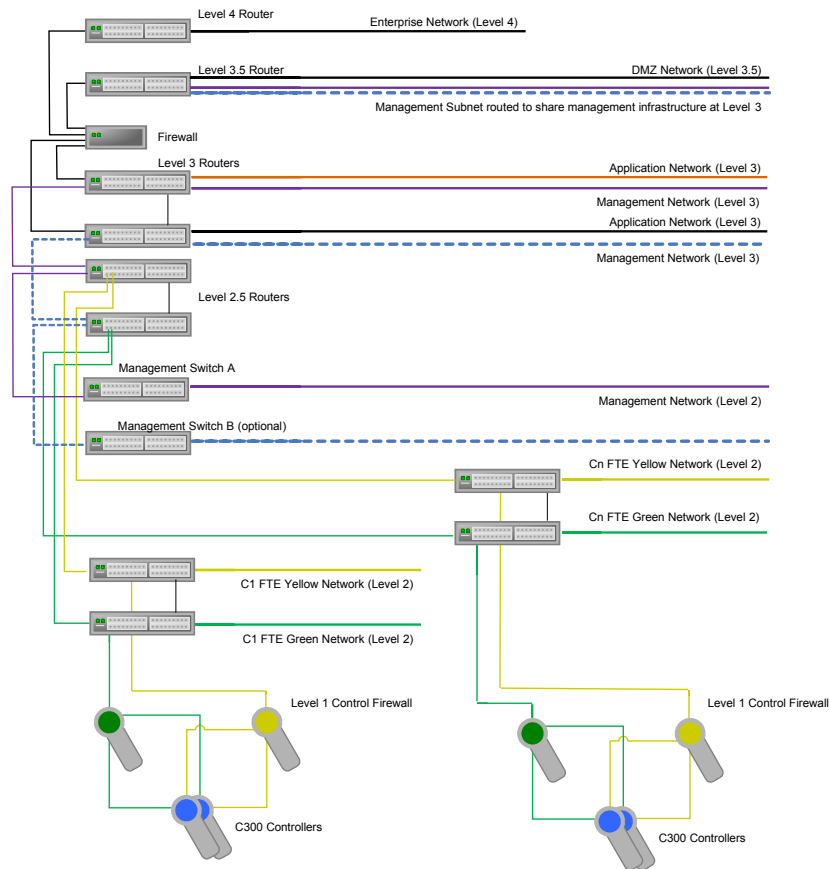
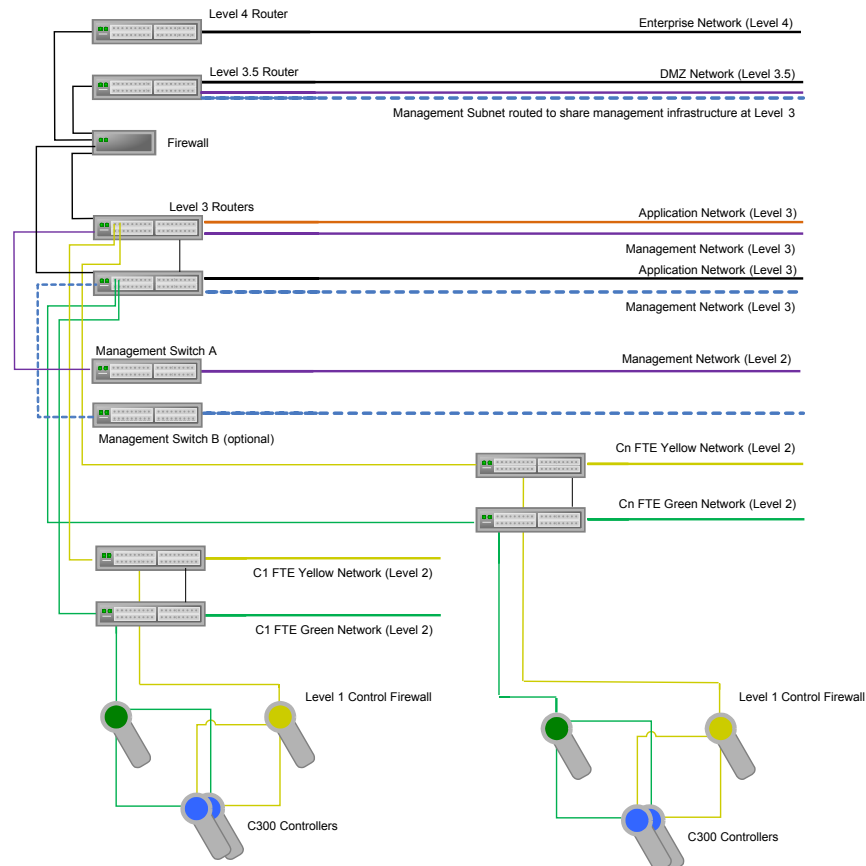


Figure 18: Example network topology with management network at Level 2 connected to Level 2.5



**Figure 19: Example network topology with management network at Level 2 connected to Level 3**

The procedures to establish the network levels other than Level 2.5 are beyond the scope of this guide. The Experion Network Best Practices Guide provides recommendations and guidelines to consider when establishing Level 1, Level 2, Level 3, Level 3.5 and Level 4. Honeywell Network Services can be consulted for the proper configuration of the router at Level 3.

The Fault Tolerant Ethernet Overview and Implementation Guide can also be used to establish Level 1 and Level 2 networks.

The procedure to connect Level 2.5 to Level 3 requires the establishment of Level 3 network including the configuration of the Level 3 router(s).

The procedure to connect Level 2 to Level 2.5 or Level 3 requires the establishment of Level 2 (FTE) including the configuration of FTE switches for each FTE community.

The figure below illustrates the connection of a single management network to redundant Level 2.5 routers. Also illustrated is the connection from Level 2.5 to Level 3 with the use of a single Level 3 router connected to redundant Level 2.5 routers. This option requires that the Level 2.5 router support routing redundancy. The Honeywell provided L2.5 configuration templates can be used to configure L2.5 routers. However, the templates assume implementation of the management network as a separate vLAN. See the table below to determine the template items that can be ignored when implementing a separate management network.

From the figure below, note the following:

- Use of redundant Level 2.5 or Level 3 routers that support routing redundancy. For example, Cisco Systems' Hot Standby Router Protocol (HSRP).
- Allocation of two Level 3 router ports in the same VLAN. This VLAN is dedicated to the connection to the A and B Level 2.5 routers (if deploying with L2.5 only).

- Allocation of a single router port in Level 2.5 Router A or Level 3 Router A for the connection of the management switch.
- Option: Allocation of a single router port in Level 2.5 Router B or Level 3 Router B for the connection of the management switch.

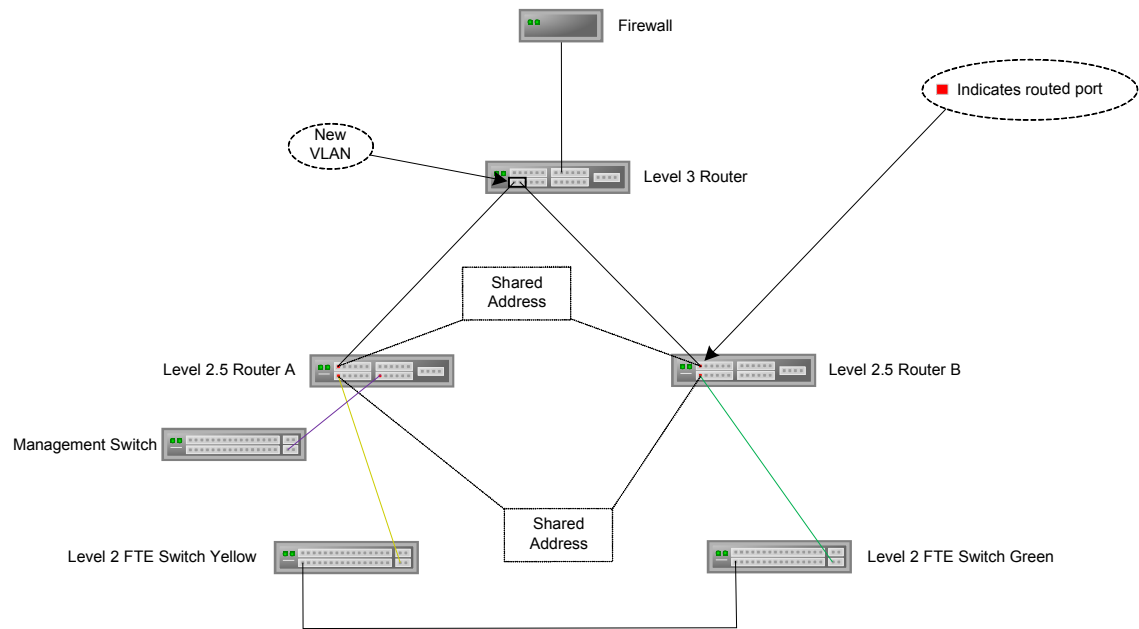


Figure 20: Connection of single management network to redundant Level 2.5

An alternative approach is to use redundant Level 3 routers with a VLAN common between the two Level 3 routers. This would be similar to that which is illustrated above for the Level 2.5 Routers or the FTE Level 2 switches and would therefore include the use of a crossover between the primary and secondary Level 3 routers.


The table below can be used as a guide to performing the Level 3 and Level 2.5 router configuration tasks as well as the management switch configuration tasks to establish the management network as shown in the figure above. This procedure assumes usage of the recommended Cisco switch-routers for use at Level 2.5 and the Level 2 management switch.


To implement a separate management network for a DCS architecture

Stage	Task	Description
Define subnets required by adding management network and Level 2.5 HSRP subnet.	1. Allocate four IP addresses in an unused subnet for use redundant IP routing between Level 2.5 and Level 3. This assumes a single Level 3 router where Level 2.5 connections are grouped together on Level 3 router with a VLAN.	IP addresses required to run with the HSRP in Level 2.5 1. Level 3 VLAN IP address 2. Unique IP address for Level 2.5 A router connection in Level 3 VLAN 3. Unique IP address for Level 2.5 B router connection in Level 3 VLAN 4. Subnet mask for Level 3 VLAN 5. Shared address for items 2 and 3 above.
	2. Allocate unused subnet with enough IP address to accommodate all management network connection requirements.	1. Subnet mask for Level 2 management network. 2. IP addresses for all other management connected devices (ESXi hosts, management client and NAS).



Stage	Task	Description																				
Prepare to update the Level 3 router configuration.	3. Allocate 2 physical interfaces (ports) on the router Note that you may be re-allocating an existing interface that is currently used for Level 2 connection to Level 3.	<table><tr><th>Interface (Port) Usage</th><th>Quantity</th><th>Gigabit</th><th>Routed Port</th><th>Switch Port</th></tr><tr><td>Level 2.5 A</td><td>1</td><td>O</td><td></td><td>Y</td></tr><tr><td>Level 2.5 B</td><td>1</td><td>O</td><td></td><td>Y</td></tr></table> <p>O = Optional Y = Yes</p>	Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port	Level 2.5 A	1	O		Y	Level 2.5 B	1	O		Y					
Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port																		
Level 2.5 A	1	O		Y																		
Level 2.5 B	1	O		Y																		
	4. Define the ID of the new VLAN on the Level 3 router.	New VLAN ID																				
	5. Be familiar with how to update the current configuration of the Level 3 router																					
Prepare to configure the Level 2.5 A and B routers.	6. Download the Level 2.5 router A template and the Level 2.5 router B template from the Honeywell Process Solutions web site.	<p>The templates define a configuration for a 24 port switch router from the Cisco family of switch routers.</p> <p>Honeywell recommends usage of the port allocation scheme as defined in the templates.</p> <p>The default definition in the configuration files is for usage with non-stackable switch-routers. Modifications are required for usage with stackable switch-routers. The default definition in the configuration files implements the redundant management network as a vLAN. Modifications are required to remove this vLAN and are identified in the remaining tasks.</p>																				
	7. Validate that the IOS in the Level 2.5 A router is the same version as the IOS in the Level 2.5 B router.	<p>Ensure that each switch router is installed with the same IOS version to avoid communication problems.</p> <p>Consult with site policies regarding the minimum IOS version that should be installed in each Level 2.5 switch-router.</p>																				
	8. Define host name for each router.																					
	9. Allocate physical interfaces (ports) for each Level 2.5 router.  Note that FTE community connections are defined as the top level of yellow side for the Level 2.5 A and top side of green side for Level 2.5 B. Allocate an additional physical interface (port) in Level 2.5 A for the management switch connection.	<table><tr><th>Interface (Port) Usage</th><th>Quantity</th><th>Gigabit</th><th>Routed Port</th><th>Switch Port</th></tr><tr><td></td><td>1</td><td>O</td><td>Y</td><td></td></tr><tr><td>FTE Communities</td><td>1 per community</td><td>O</td><td>Y</td><td></td></tr><tr><td>Management Switch</td><td>1</td><td>Y</td><td>Y</td><td></td></tr></table> <p>O = Optional Y = Yes</p>	Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port		1	O	Y		FTE Communities	1 per community	O	Y		Management Switch	1	Y	Y	
Interface (Port) Usage	Quantity	Gigabit	Routed Port	Switch Port																		
	1	O	Y																			
FTE Communities	1 per community	O	Y																			
Management Switch	1	Y	Y																			

Stage	Task	Description
	10. For each FTE community, know the FTE IP addresses that are used for HSRP between Level 2.5 and Level 2.	IP addresses for each FTE community: <ol style="list-style-type: none"> <li>1. Unique IP address for yellow connection in FTE community subnet.</li> <li>2. Unique IP address for green connection in FTE community subnet.</li> <li>3. Subnet mask for FTE Community.</li> <li>4. Unique shared virtual address (default gateway) for FTE Community.</li> </ol>
	11. Review ACLs.	Update to be site compliant.
	12. Be familiar with how to set up and access the Level 2.5 routers for configuration.	 <b>Tip</b> Loading the Level 2.5 configuration files is similar to the steps documented in section 9.7, “Configuring Cisco Switches” of the <i>Fault Tolerant Ethernet Overview and Implementation Guide</i> .
Complete physical connections.	13. Complete the physical connections according to the interface (port) allocations established in the router preparation tasks for both Level 3 and Level 2.5.	Use the information defined in tasks 3 and 9.
Update the Level 3 router configuration.	14. Add VLAN for Level 2.5 connections.	Use the information defined in tasks 1.1 and 4.
	15. Update the IP route settings.	Add the IP address of the VLAN defined in task 1.5.
	16. Add interface for uplink from Level 2.5 A router.	Use the information defined in tasks 3 and 4: <ul style="list-style-type: none"> <li>• Assign the interface to the VLAN defined in task 14.</li> <li>• Do not assign an IP address.</li> <li>• Disable any discover protocol.</li> </ul>
	17. Add interface for uplink from Level 2.5 B router.	Use the information defined in tasks 3 and 4: <ul style="list-style-type: none"> <li>• Assign the interface to the VLAN defined in task 14.</li> <li>• Do not assign an IP address.</li> <li>• Disable any discover protocol.</li> </ul>
Configure Level 2.5 A router.	18. Create configuration file	Preferred method is to use the Honeywell provided Level 2.5 templates (see task 6). These instructions assume usage of the preferred method to create Level 2.5 configuration file.
	19. Remove VLAN for Management Network	Remove the following lines from the configuration file in order to eliminate the pre-defined vLAN for management in the A template (that is, VLAN 401):  <pre> vlan 401 name VL-Management ! ! Configure L2.5 as spanning tree root for management network ! spanning-tree mst configuration revision 1 instance 4 vlan 401 spanning-tree mst 4 priority 4096           </pre>
	20. Add the interface for the Level 3 router connection.	Use the information defined in tasks 1.2, 1.4, 1.5 and 9.  Pre-defined in the template with HSRP activated.

Stage	Task	Description
	21. Add a interface for each Yellow FTE community connection.	Use the information defined in tasks 9 and 10.1, 10.3, and 10.4.
	22. Replace the interface range for the Virtual Infrastructure with the interface for the management switch connection.	<p>Use the information defined in tasks 9. Remove the following lines from the configuration file in order to eliminate the Virtual Infrastructure interfaces defined on vLAN:</p> <pre>interface range GigabitEthernet 0/13 - 23 description virtual management network switchport access vlan 401 switchport mode access spanning-tree portfast</pre> <p>Replace the removed lines with the following:</p> <pre>interface GigabitEthernet 0/13 description Management Network for virtual Infrastructure at L2 no switchport ip address &lt;ManagementNetwork Subnet Mask&gt; no ip redirects no ip unreachableables no ip proxy-arp no ip mroute-cache</pre> <p>Use the information in task 2.1 for Management Network Subnet Mask</p>
	23. Remove the interface for the crossover cable.	<p>Remove the following lines from the configuration file in order to eliminate the use of the crossover cable:</p> <pre>interface GigabitEthernet0/24 description virtual managment network crossover cable switchport access vlan 401 switchport mode access</pre>
	24. Add the VLAN interface for the management network.	<p>Remove the following lines from the configuration file in order to eliminate the pre-defined vLAN for management in the A template (that is, VLAN 401):</p> <pre>interface vlan401 description managment vlan ip address MgmtAddrA subnetmask no ip redirects no ip unreachableables no ip proxy-arp no ip mroute-cache ip access-group 130 in standby 241 ip SharedVirtMgmtAddr standby 241 timers 2 6 standby 241 priority 105 standby 241 preempt delay minimum 90</pre>
	25. Update the IP route settings.	<p>Add default route for the IP address of the Level 3 VLAN.</p> <p>Use the information from task 1.1.</p>
	26. Copy the updated configuration file to the Level 2.5 A router.	<p> <b>Tip</b> Loading the Level 2.5 configuration files is similar to the steps documented in section 9.7, “Configuring Cisco Switches” of the <i>Fault Tolerant Ethernet Overview and Implementation Guide</i>.</p>

Stage	Task	Description
Configure Level 2.5 B router.	27. Repeat tasks 18 through to 26 for the Level 2.5 B router.	<p>Predefined in the B template. Adjust the Level 2.5 A tasks as follows:</p> <ul style="list-style-type: none"> <li>Task 20: Use the information defined in tasks 1.3, 1.4, 1.5 and 9.</li> <li>Task 21: Use the information defined in tasks 9 and 10.2, 10.3, and 10.4.</li> <li>Task 22: Perform only the part of task to remove lines. Since there is no management switch connection on Level 2.5 B router, skip the part of task to add lines.</li> </ul>
	28. Copy the updated configuration file to the B device	
Confirm that Level 2.5 Routers are operational	29. Validate the following: <ul style="list-style-type: none"> <li>No blocked ports.</li> <li>Correct states for Primary/Secondary.</li> <li>Protocol and interface are “active”</li> </ul>	Use: <ol style="list-style-type: none"> <li>Sho span.</li> <li>Sho standby (Primary is in active state, Secondary is in standby state).</li> <li>Sho interface (Interface is Up, Protocol is Up).</li> </ol>
Configure Management switch	30. Complete the physical connections to the port allocations established in task 2.	
	31. Configure the switch with recommended settings.	<ol style="list-style-type: none"> <li>Configure the global wide settings on the switch, including:               <ul style="list-style-type: none"> <li>Enable rapid spanning tree (RSTP) On Cisco switches, this is MST or PVRSTP+.</li> <li>On Cisco switches, configure VLAN trunking protocol (VTP) mode transparent, which disables the auto VLAN configuration. Other switch manufacturers may have a similar configuration setting.</li> <li>No ip gratuitous-arps.</li> <li>No ip domain-lookup.</li> </ul> </li> <li>Best practice recommendation is that you enable "spanning-tree portfast" on all non-uplink ports (ports that aren't connected to other switches) and enable "switchport mode access" on all ports.</li> <li>The interfaces on the management network that connect to the ESXi host need to match the speed and duplex settings of the ESXi host physical network interface cards (NICs).</li> <li>Best practice recommendation is that unused ports are shutdown and placed in an unused VLAN.</li> </ol>

# Implementing networks for a SCADA architecture

## Related topics

“Preparing a gateway router for a SCADA architecture” on page 94

*Prepare a gateway router to enable communication between the production and management networks, and to control the flow of network traffic between the production network and the business network (WAN).*

“Preparing the production network for a SCADA architecture” on page 95

*Prepare the production network, including installing the production network switch and network cabling, and configuring the production network switch (if not already installed and configured).*

“Configuring the virtual production network for a SCADA architecture” on page 96

*Configure the virtual production network on the ESXi host and configure the virtual switch to communicate with the physical production NICs.*

“Implementing the management network for a SCADA architecture” on page 97

---

## Preparing a gateway router for a SCADA architecture

Prepare a gateway router to enable communication between the production and management networks, and to control the flow of network traffic between the production network and the business network (WAN).

The purpose of the gateway router is to:

- Enable communication between the production and management networks. This communication should be well documented and limited so that it protects the integrity and security of the overall network.
- For virtualization environments that are part of a backup control center (BCC) solution, the gateway router enables communication between the storage and management networks for data that must cross through a wide area network (WAN).

You can use a multi-layer switch with routing capabilities as the gateway router.

### Prerequisites

- Best practice is to place a firewall between the WAN and the gateway router.
- Network access control lists (ACLs) are configured on the gateway router. For more information about configuring network access control lists (ACLs), see the *Experion Virtualization: Network Router Configuration Best Practices* whitepaper.
- *Experion Virtualization: Network Router Configuration Best Practices* whitepaper, which is available from the Honeywell Process Solutions web site (<http://www.honeywellprocess.com>).

### To prepare a gateway router

1. Define and configure the subnets and VLANs.
2. Connect the gateway router to the WAN through a firewall. This connection is recommended to be a single point of connectivity.
3. Disable the proxy address resolution protocol (ARP) on the gateway router.
4. The gateway router must be connected to the production, management, and storage switch interfaces that are configured as uplink ports.
5. Enable filtering as described in the *Experion Virtualization: Network Router Configuration Best Practices* whitepaper.

---

## Preparing the production network for a SCADA architecture

Prepare the production network, including installing the production network switch and network cabling, and configuring the production network switch (if not already installed and configured).

### Prerequisites

- You have followed the manufacturer's instructions and setup the production network switch on the required subnet.

### To prepare the production network

1. Configure global wide settings on the switch, including:
  - a. Enable rapid spanning tree (RSTP). On Cisco switches, this is MST or PVRSTP+.
  - b. On Cisco switches, enable VLAN trunking protocol (VTP) mode transparent, which disables the auto VLAN configuration.  
  
Other switch manufacturers may have a similar configuration setting.
  - c. No ip gratuitous-arps.
  - d. No ip domain-lookup.
2. Configure the switch to meet any additional requirements of the selected SCADA devices.
3. Honeywell best network practices recommends that you enable “spanning-tree portfast” on all non-uplink ports (ports that aren’t connected to other switches) and enable “switchport mode access” on all ports.
4. The interfaces on the production network that connect to the ESXi host need to match the speed and duplex settings of the ESXi host physical network interface cards (NICs).

---

## Configuring the virtual production network for a SCADA architecture

Configure the virtual production network on the ESXi host and configure the virtual switch to communicate with the physical production NICs.

### To configure the virtual production network

- 1 On the vSphere Client (within the **Hosts > Inventory > Hosts and Clusters** view), locate the ESXi host. Click on the **Configuration** tab and then under the **Hardware** group, click the **Networking** link.
- 2 On the top-right of the screen, click the **Add Networking** link.  
The **Add Network Wizard** appears.
- 3 Select **Virtual Machine** and then click **Next**.  
The **Network Access** page of the wizard appears.
- 4 Select **Create a virtual switch** and then select the production network vmnics.
- 5 Click **Next**.  
The **Connection Settings** page of the wizard appears.
- 6 Set the following connection settings:

Setting	Value
Connection Type	Select <b>Virtual Machine</b> .
Network Label	Type the name for the vSwitch. For example, Production Network.
VLAN ID (Optional)	Leave empty.

- 7 Click **Next**.
- 8 Click **Finish**.

### Next steps

- Configure security and policy exceptions on the vSwitch.



---

## Implementing the management network for a SCADA architecture

Prior to implementing the management ESXi hosts and virtual infrastructure tools, the management network must be established and configured. For SCADA architectures, consider the following settings when implementing the management network.

### To implement the switch for the management network in a SCADA architecture

1. Configure the global wide settings on the switch, including:
  - a. Enable rapid spanning tree (RSTP). On Cisco switches, this is MST or PVRSTP+.
  - b. On Cisco switches, configure VLAN trunking protocol (VTP) mode transparent, which disables the auto VLAN configuration.  
  
Other switch manufacturers may have a similar configuration setting.
  - c. No ip gratuitous-arps.
  - d. No ip domain-lookup.
2. Honeywell recommends that you enable “spanning-tree portfast” on all non-uplink ports (ports that aren’t connected to other switches) and enable “switchport mode access” on all ports.
3. Place all interfaces in the management VLAN.
4. The interfaces on the management network that connect to the ESXi host need to match the speed and duplex settings of the ESXi host physical network interface cards (NICs).
5. Honeywell recommends that unused ports are shutdown and placed in an unused VLAN.



# Implementing shared storage networks

If you have chosen shared storage for your virtual infrastructure, implement this shared storage network.

## Related topics

“About shared storage” on page 100

“Redundancy for physical SANs” on page 101

*The use of redundant physical SANs can increase the availability of the virtual environment.*

“Distributing datastores and volumes across storage networks” on page 102

*Splitting the available storage space on a SAN into multiple volumes helps to distribute virtual machines across SAN volumes and supports availability, should a SAN volume go offline.*

“Preparing the storage network” on page 104

*Prepare the storage network, including installing the storage network switch and network cabling, and configuring the storage network switch.*

“Configuring the storage area network” on page 105

*If you are using shared storage, configure the virtual storage network on the ESXi host and configure the virtual switch to communicate with the physical storage NICs.*

“Configuring redundancy across multiple physical SANs” on page 106

“Example DCS architecture in a virtualized environment with redundant management network” on page 24

“Storage requirements” on page 42

---

## About shared storage

Use of physical SANs is supported at Level 3 for DCS and SCADA architectures. Deploying shared storage in either architecture requires a dedicated storage network.

Use of shared storage at Level 2 is offered with the BladeCenter S platform (see the *Experion Virtualization with BladeCenter S Guide* for planning and implementation details).

### **Physical Storage Area Network (pSAN)**

A pSAN is a physical storage device that is separate to any ESXi host. This device typically contains a large number (greater than 10) of high speed disk drives (10K or 15K rpm). It is connected to one or more ESXi hosts through a dedicated storage network, such as Fibre Channel or iSCSI.

Currently, iSCSI is the only supported storage network, over multiple one gigabit Ethernet connections.

---

## Redundancy for physical SANs

The use of redundant physical SANs can increase the availability of the virtual environment.

If all the virtual machines are stored on a single physical SAN device there is the possibility that the physical SAN may fail and you will be unable to access the virtual machines stored within it. By using multiple physical SANs, you can develop a redundancy strategy that will allow access to the virtual machines, should there be a single physical SAN failure.

For redundant virtual machines, you should follow the same philosophy as allocating virtual machines to ESXi hosts. That is, the virtual machine images for redundant nodes should be stored on separate physical SANs. If the physical SAN storing the virtual machine for the primary node fails, there should be a fail-over to the backup node, whose virtual machine is stored on a different physical SAN. In addition, vDR can be used to backup the virtual machines to another SAN. These backups can be restored to the failed SAN after it has been brought back online, or they can be restored to another SAN if the original SAN is not available for an extended period.

For non-redundant nodes, you will need to restore the virtual machine from a backup. The SANs asynchronous replication should be used to replicate the entire volume holding the datastore and virtual machines to another SAN. If there is a failure of the SAN, the replica volume can be promoted and discovered on the ESXi hosts. The virtual machines contained on this replica volume can be added to the inventory of ESXi hosts and be brought back online. The asynchronous replication would operate at a frequency dependant on the SAN devices.

The best practice using redundant/multiple SANs is to spread the virtual machine load, and to also spread vDR and/or synchronous backup load evenly across all SANs. Using this best practice will help to ensure that if a SAN fails (or is taken offline), the available SANs remain evenly loaded, although with a potentially higher load than when all SANs were available.

## Distributing datastores and volumes across storage networks

Splitting the available storage space on a SAN into multiple volumes helps to distribute virtual machines across SAN volumes and supports availability, should a SAN volume go offline.

When configuring shared storage, the storage available within the device needs to be allocated into units known as volumes. You will create datastores for the virtualization environment in these volumes. The maximum size of a datastore is 2 terabytes (TB). Typically, datastores have a one to one relationship with volumes, which means that volumes should not be sized greater than 2 TB. Even if the total storage available in the SAN device is less than 2 TB you should consider subdividing the available storage into multiple volumes.

For a single SAN, Honeywell recommends the following volumes be created:

- Volume 1 - for A Server. Size this volume larger than the expected server disk size.
- Volume 2 - for B server. Size this volume larger than the expected server disk size.
- Volume 3 - for all other nodes. Size this volume larger than the disk size of all the virtual machines expected on this volume.
- Volume 4 - for virtual machine creation. Size this volume larger than the disk size of all the virtual machines you expect to create simultaneously.

For multiple physical SANs, Honeywell recommends the following volumes be created:

- Volume 1 - for nodes that always run on this SAN device, such as Experion servers, domain controllers, redundant OPC servers, and other redundant nodes.
- Volume 2 - for nodes that can be run on any SAN device, such as Flex Stations, and non-redundant nodes.
- Volume 3 - for vDR backups of virtual machines on volume 1 from another SAN.
- Volume 4 - for an asynchronous replica of volume 2 from another SAN.
- Volume 5 - for virtual machine creation. Size this volume larger than the disk size of all the virtual machines you expect to create simultaneously.

### ! Attention

- Depending on the size of the volume, number of virtual machines, and the number of SAN devices you may choose to further subdivide volume 1 and volume 2. For each subdivided volume 1 and volume 2 there needs to be a matching subdivided 'volume 3' and 'volume 4' on another SAN device.

### Example 2 SAN design

For a two (2) SAN design, the replication pattern may look like the following diagram.

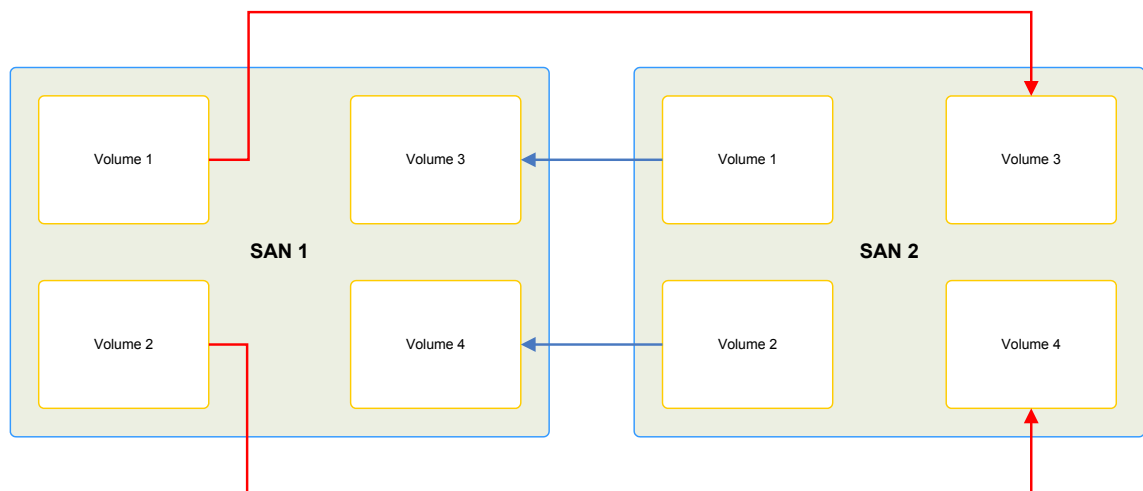


Figure 21: Example 2 SAN design

**Attention**

- Volume 5 is not shown as it is not backed up or replicated to another SAN.

---

---

## Preparing the storage network

Prepare the storage network, including installing the storage network switch and network cabling, and configuring the storage network switch.

### Prerequisites

- You have followed the manufacturer's instructions and setup the storage network switch on the required subnet. You have also followed the best practices supplied by the manufacturer for connecting and configuring the SAN with VMware.
- *vSphere Installation and Setup*

### To prepare the storage network

1. Configure storm control on the storage network switches.
2. On the storage network switches, enable the following for each interface that is an end point interface (for example, iSCSI):
  - a. Port fast.
  - b. BPDU guard.
  - c. Switch port access.



#### Attention

In this document, an endpoint interface refers to the termination of the connection. Therefore, an endpoint is not an uplink to another switch or network.

3. Enable jumbo packets on the both the storage network switches and the network interface cards (NICs).
4. Use the default rapid spanning tree protocol (RSTP). On Cisco switches, this is PVRSTP+ or MST.
5. Set the speed and duplex settings wherever possible (avoid auto negotiate).
6. Open the ports identified in *vSphere Installation and Setup*.



---

## Configuring the storage area network

If you are using shared storage, configure the virtual storage network on the ESXi host and configure the virtual switch to communicate with the physical storage NICs.

**Attention**

- Only software iSCSI initiators are supported. iSCSI HBAs are not supported.

**Prerequisites**

- Storage network NICs are installed on the ESXi host.
- At least 2 static IP addresses for the storage network have been allocated per ESXi host.
- Storage network NICs, switches, and network cabling are connected and configured.
- ESXi host added to the vCenter Server.
- Refer to SAN Vendor guidance for iSCSI connectivity with vSphere. An example is: *Dell Equallogics - Configuring iSCSI Connectivity with VMware vSphere 5 and Dell EqualLogic PS Series Storage TR1075*.

---

## Configuring redundancy across multiple physical SANs

### Related topics

“Setting up vDR for volume 1” on page 106

*Set up vDR backup jobs for virtual machines contained on volume 1.*

“Setting up asynchronous replication for volume 2” on page 106

*Set up asynchronous replication for virtual machines contained on volume 2.*

### Setting up vDR for volume 1

Set up vDR backup jobs for virtual machines contained on volume 1.

#### Prerequisites

- The physical SAN devices have been installed and configured.
- Volume 1 and volume 3 have been created on the physical SAN devices.
- Datastores have been created on volume 1 and volume 3.
- Virtual machines have been created in volume 1.
- vDR has been installed and configured.

#### To set up vDR for volume 1

- For each virtual machine contained in volume 1, create a vDR backup job where the backup destination is volume 3 on another physical SAN.

### Setting up asynchronous replication for volume 2

Set up asynchronous replication for virtual machines contained on volume 2.

#### Prerequisites

- The physical SAN devices have been installed and configured.
- Volume 2 and volume 4 have been created on the physical SAN devices.
- The physical SAN device manufacturer’s configuration instructions.

#### To set up asynchronous replication for volume 2

- Configure asynchronous replication of the contents of volume 2 to volume 4 on another physical SAN. Follow the physical SAN device manufacturer’s configuration instructions, and ensure the follow options are enabled:
  - Bandwidth throttling.
  - Replication schedule.

# Preparing a management ESXi host

Prepare a management ESXi host for management workloads.

Before you can create Experion virtual machines, you need to prepare the VMware virtualization environment, including configuring physical and virtual networks, preparing the ESXi hosts, configuring the vCenter Server, and adding and organizing the ESXi hosts to the vCenter Server.

If you have an existing VMware virtualization environment, you may only need to complete some of these tasks. For example, you may already have configured the vCenter Server. Ensure that the planning sections of this guide are read and understood before continuing the implementation.

## Management ESXi host preparation considerations

Consideration	Description
vSphere Client	<p>The initial configuration of the virtual environment requires a vSphere Client to connect to the management host. A workstation or laptop connected to the management network can be used to perform this role. The requirements outlined in the “vCenter Server and the vSphere Client Hardware Requirements” section of <i>vSphere Installation and Setup</i> from VMware outline the minimum requirements for this hardware.</p> <p>This vSphere Client should be retained after the configuration of ESXi hosts. It is required for recovery purposes.</p> <p>To install the vSphere Client, see the “After you install and set up ESXi” section in <i>vSphere Installation and Setup</i>.</p>
Hardware is installed	Verify that the required hardware, such as drives, memory, and NICs, have been installed.

- Honeywell recommends that you enable startup and shutdown behavior of virtual machines. If you do not specify this behavior, you will need to manually start each virtual machine on an ESXi host after the ESXi host is restarted.
- The recommended startup order is:
  1. Domain controller
  2. vCenter Server
  3. All others



### Attention

If any components in the management workload access an external database server (for example, vCenter Server or Update Manager), the database server must be started and running before starting the management workload.

## Related topics

“Configuring the ESXi host local disk array” on page 109

*Prior to installing the ESXi hypervisor software, you must prepare the local disk array on the ESXi host.*

“Configuring the ESXi host BIOS settings” on page 110

“Installing the ESXi software on a host” on page 111

*Use the guidance in this section to perform a clean install of the ESXi software on the host. If you are upgrading or migrating an existing ESXi installation, see “Upgrading virtual infrastructure software”.*

“Configuring the ESXi host network settings” on page 112

*After you install the ESXi software on a host, you need to configure the network settings and the ESXi password.*

“Configuring ESXi host time synchronization” on page 116

“Adding and renaming datastores” on page 117

“Preparing a vCenter Server” on page 118

*On the management ESXi host, you need to create a virtual machine to host the vCenter Server (and vCenter Update Manager). The vCenter Server contains the required software components for the administration of virtual machines, ESXi hosts, and the virtualization environment. You need to install a vCenter Server to manage the virtual environment.*

“Configuring the virtual machine load order on the management ESXi host” on page 127

*Management ESXi hosts require configuration to ensure that the management virtual machines are automatically started and started in a specific order.*

“Configuring security in a vCenter Server” on page 128

*Create vCenter roles and assign them to Experion users or global groups, and configure host lockdown mode.*

## Configuring the ESXi host local disk array

Prior to installing the ESXi hypervisor software, you must prepare the local disk array on the ESXi host.

The RAID configuration of a performance production host should be RAID 10 with a hot spare. The RAID configuration of a lower capacity production host can be RAID 1.

The following table provides guidance on RAID configuration based on the usage of the ESXi host:

ESXi host type	RAID configuration
Production ESXi host in a SCADA architecture.	RAID 10 with a hot spare. <sup>1</sup>
Production ESXi host in a DCS architecture.	RAID 10 with a hot spare.
Production ESXi host in a DCS architecture with low capacity.	RAID 1. <sup>2</sup>
Management ESXi host.	RAID 1. <sup>3</sup> Create multiple groups: <ul style="list-style-type: none"> <li>• One group for management workloads (which will form the <i>management datastore</i>).</li> <li>• One group for staging Experion virtual machine installations (which will form the <i>staging datastore</i>).<sup>4</sup></li> </ul>

Prior to ESXi installation, confirm that the preferred boot device is selected. Refer to the appropriate Dell document for the RAID controller on the server hardware for instructions to assign a preferred boot device.

<sup>1</sup> RAID 5 with hot spare optional to achieve greater capacity

<sup>2</sup> If the hardware is capable then “Production host in a DCS architecture” configuration is permitted

<sup>3</sup> If the hardware is capable then “Production host in a DCS architecture” configuration is permitted

<sup>4</sup> Higher performance host / RAID configuration to be considered

## Configuring the ESXi host BIOS settings

Virtualization technology abstracts the Experion application from the ESXi host hardware so that when virtualized, Experion interactions with the BIOS are minimized.

Use the following steps to deploy an ESXi host with a BIOS that is optimized for virtualization. For detailed instructions on how to view and update the BIOS settings, see the host computer manufacturer's documentation.

1. Use the latest version of the BIOS that is available for your virtualization host.
2. Confirm that the following BIOS settings have been set on the ESXi host:
  - Sockets and cores enabled.
  - 64-bit mode enabled.
  - (VT) Intel Virtualization Technology enabled (for CPU and for memory).
  - Turbo Mode enabled.
  - Execute Protection feature is enabled (for Intel, eXecute Disable (XD) enabled).
  - Hyper Threading enabled.



### Attention

You may have to enable this through vSphere Client.

- Node Interleaving disabled.
- Unused hardware disabled (including iDRAC).
- Hardware clock is set to UTC.
- Power Management set to Maximum Performance (that is, disable Power Management).

For additional information related to recommended BIOS settings on an ESXi host, refer to the VMware document, *Performance Best Practices for VMware vSphere® x*, where “x” is the vSphere release of the ESXi hypervisor, for example, 4.1, or 5.0 or 5.1.

For additional information relating to ESXi host platform specifications pertaining to validated BIOS revisions, refer to the *HPS Virtualization Specification*.

# Installing the ESXi software on a host

Use the guidance in this section to perform a clean install of the ESXi software on the host. If you are upgrading or migrating an existing ESXi installation, see “Upgrading virtual infrastructure software”.



## Attention

Before you begin the clean install of ESXi, review any differences that have been introduced with the new vSphere release. Check for related topics in the "Introduction to vSphere Installation and Setup" section of *vSphere Installation and Setup*.



## CAUTION

The root password for each ESXi host should be set during installation. Each ESXi host should not be connected to a trusted network until you have configured a root password on the ESXi host.

## Prerequisites

- On the host computer, you have set up:
  - the disk array
  - the BIOS settings
- Review "Introduction to vSphere Installation and Setup" in *vSphere Installation and Setup*. The following guidance is for the Interactive ESXi Installation option.



## Tip

Experion virtualization media and documentation is available for download from the Honeywell Online Support web site <http://www.honeywellprocess.com/>.

- If you plan to create an Experion virtual machine on this ESXi host that requires a USB security device (dongle), see *vSphere Virtual Machine Administration* for guidance.

## To install an ESXi host

1. Install the ESXi host using the instructions in "Installing ESXi Interactively" in the *vSphere Installation and Setup guide*.
2. If you plan to create an Experion virtual machine on this ESXi host that requires a USB security device (dongle), add the USB security device to this ESXi host by following the instructions in the “USB Configuration from an ESXi Host to a Virtual Machine” topic in *vSphere Virtual Machine Administration*.

In the VMware environment, the physical network adapters on the ESXi host are named vmnic *n*, where *n* is unique number identifying the network adapter. During the installation of the ESXi software, network adapters are assigned a vmnic number (starting with 0) in the order in which the adapters are detected. Physical network adapters are referenced with the vmnic *n* names when configuring a vSwitch or viewing the vSwitch configuration.

Honeywell recommends that the network adapter cards (single or multiple port) be assigned the same slots in each ESXi host.

The set of virtual network adapters configured for a virtual machine are referenced as vNIC *n* where *n* is a unique number identifying the virtual network adapter. This naming convention is for documentation purposes only.

# Configuring the ESXi host network settings

After you install the ESXi software on a host, you need to configure the network settings and the ESXi password.



## CAUTION

Since the root password for ESXi is blank after the initial installation, the ESXi host should only be connected to a trusted network until you have configured a new root password on the ESXi host.

After you have configured the IP address of the ESXi host from the direct console, you can connect to the ESXi host from the vSphere Client. However, to complete the network connectivity configuration of the ESXi host, access from the direct console is required.

## Prerequisites

- You have installed vSphere Client on a physical node that is connected to the management network.
- You have the network details for the ESXi host, such as:
  - The IP address, subnet mask, and default gateway of the network interface cards (NICs) for the management network.
  - Primary and alternative (secondary) DNS server IP addresses.
  - DNS search suffixes.
- Familiarity with, or access to the “Setting Up ESXi” section in *vSphere Installation and Setup*.

## To configure the ESXi root password and host IP address

1. Connect to the ESXi host from the Direct Console to configure the root password. Use the instructions in the section "Set the Password for the Administrator Account".
2. Connect to the ESXi host from the Direct Console or from the vSphere client to configure the ESXi host IP address. Use the instructions in the "Configuring IP Settings for ESXi" section of *vSphere Installation and Setup*.
3. Associate the IP address with the default pNIC0 used for management network.

## To configure the ESXi host DNS settings

1. Connect to the ESXi host from Direct Console.
2. Follow the instructions in the "Configure DNS Settings from the Direct Console" section of **vSphere Installation and Setup**.
3. From the direct console, select **Test Management Network** to confirm that you have network connectivity.

## Related topics

“Network configuration for a management host in a DCS architecture” on page 113

*After you complete the initial network configuration, you need to configure the virtual network for the management host.*

“Network configuration for a management host in a SCADA architecture” on page 113

*After you complete the initial network configuration, you need to configure the virtual network for the management host.*

“Configuring NIC teaming” on page 114

*Configure the NIC teaming settings. A NIC team can share the traffic load between the physical and virtual networks among some or all of the NIC team members, or provide passive failover in the event of a hardware failure or a network outage.*



“Configuring the virtual switch port security settings” on page 115

*To protect virtual machines from intrusion, the virtual switch port security settings should be modified from the default values.*

## Network configuration for a management host in a DCS architecture

After you complete the initial network configuration, you need to configure the virtual network for the management host.

### Network configuration for management hosts with local storage

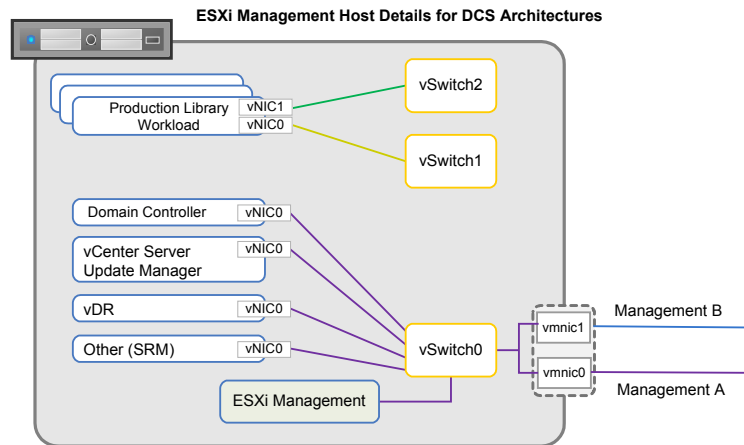


Figure 22: Example configuration of a management ESXi host with local storage

Use a single vSwitch with one management port. Use two NICs that are separately connected to Management A (Level 2.5 A router) and Management B (Level 2.5 B router).

If you plan to use the management ESXi host to stage the installation of Experion virtual machines, you need to configure the FTE virtual switches; one for FTE Yellow, and another for FTE Green. Do not add uplinks to the physical FTE network. For more information, see the related topics.

### Related topics

“Planning the management network in a DCS architecture” on page 58

*The management network spans the entire system in order to provide management access to all elements of the virtualization infrastructure.*

## Network configuration for a management host in a SCADA architecture

After you complete the initial network configuration, you need to configure the virtual network for the management host.

### Network configuration for management hosts with local storage

The minimum three ESXi host network configuration for a SCADA architecture using only local ESXi storage. Flex Station and Engineering Station thin clients connect to the production network, while any physical vCenter Client nodes connect to the management network. The backup storage device is for the backup of virtual machines on the ESXi hosts.

An ESXi host using local storage and containing only management workloads, connects to the management network only.

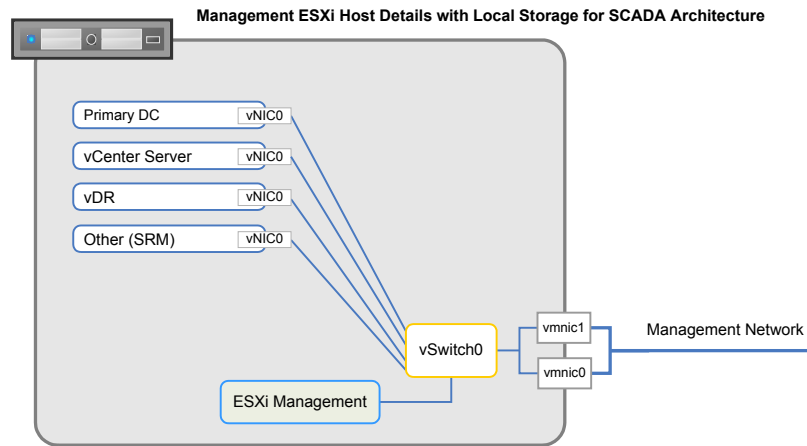


Figure 23: Example configuration of a management ESXi host with local storage

### Network configuration for management hosts with shared storage (using a storage network)

The minimum three ESXi host network configuration for a SCADA architecture using shared storage. Flex Station and Engineering Station thin clients connect to the production network, while any physical vCenter Client nodes connect to the management network. The backup storage device is for the backup of virtual machines on the ESXi hosts. The storage network connects the ESXi hosts to the storage area network (SAN).

An ESXi host using shared storage and containing only management workloads, connects to both the management network and the shared storage network.

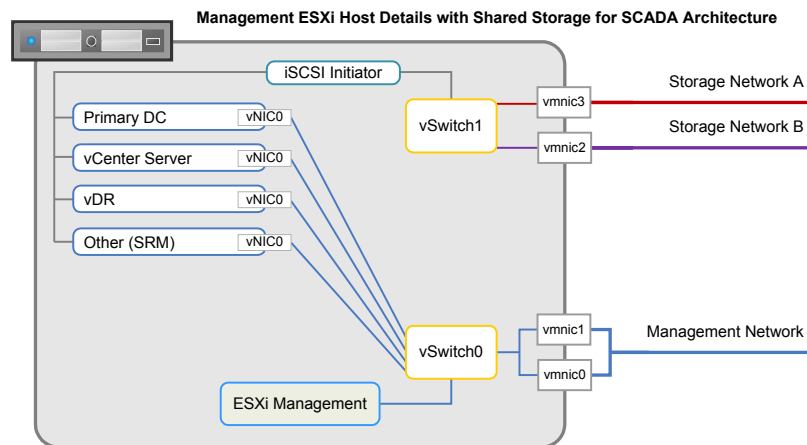


Figure 24: Example configuration of a management ESXi host with shared storage

## Configuring NIC teaming

Configure the NIC teaming settings. A NIC team can share the traffic load between the physical and virtual networks among some or all of the NIC team members, or provide passive failover in the event of a hardware failure or a network outage.

### To configure NIC teaming

- 1 On the vSphere Client (within the **Home > Inventory > Inventory** view), locate the ESXi host. Click on the **Configuration** tab, and then under the **Hardware** group, click the **Networking** link.
- 2 Locate the vSwitch0 virtual switch, and then click the associated **Properties** link.  
The **vSwitch Properties** dialog box appears.

- 3 To construct a NIC team (connecting redundant network adapters to the management network switch), do the following:
  - a Click on the **Network Adapters** tab and then click **Add**.  
The **Add Adapter Wizard** dialog box appears.
  - b In the **Unclaimed Adapters** group, select the vmnic adapters (NICs) that need to be connected to the vSwitch, and then click **Next**.

**Attention**

- If there are already adapters connected to the vSwitch, the selected adapters must belong to the same Layer 2 broadcast domain as the existing adapter.

- c Move the selected vmnic adapter into the **Active Adapters** group using the **Move Up** and **Move Down** buttons.
  - d Click **Next**.
  - e Review the information and then click **Finish**.
- 4 To set the NIC teaming policy exceptions, do the following:
  - a Click on the **Ports** tab, select the **vSwitch** configuration, and then click **Edit**.
  - b Click the **NIC Teaming** tab.
  - c Set the following policy exceptions:

Policy exception name	Value
Load Balancing	Route based on the originating virtual port ID
Network Failover Detection	Link status only
Notify Switches	Yes
Failback	No

- d Click **OK**.
- 5 Click **Close** to close the **vSwitch Properties** dialog box.

## Configuring the virtual switch port security settings

To protect virtual machines from intrusion, the virtual switch port security settings should be modified from the default values.

### Prerequisites

- *vSphere Networking*.

### To configure the virtual switch port security settings

- Configure the security policy on a virtual switch by following the instructions in the “Edit Security Policy for a vSphere Standard Switch” topic in *vSphere Networking*. Use the following table to identify the policy exception:

Policy exception name	Value
Promiscuous Mode	Reject
MAC Address Changes	Reject
Forged Transmits	Reject

---

## Configuring ESXi host time synchronization

ESXi hosts require time synchronization that is accurate when compared to the time used within the whole infrastructure. Ensure that you have determined the time source for all ESXi hosts and configured the time configuration.

### To configure ESXi host time synchronization

- 1 In the vSphere Client (within Home > Inventory >), choose the **Inventory** view.
- 2 Locate and select the ESXi host that requires time configuration.
- 3 Click the **Configuration** tab.
- 4 Click the **Time Configuration** option.
- 5 At the top right of the page, click **Properties**.  
The **Time Configuration** dialog box appears.
- 6 Click **Options**.  
The **NTP Daemon (ntpd) Options** dialog box appears.
- 7 Click **NTP Settings** and then click **Add**.  
The **Add NTP Server** dialog box appears.
- 8 Type the IP address or host name of the NTP time server and then click **OK**.
- 9 Select the **Restart NTP service to apply changes** check box and then click **OK**.  
This adds the NTP server and restarts the NTPD daemon.  
You should see an event in the vSphere Client recent tasks status bar stating **Update service activation policy**. The **Time Configuration** dialog box appears.
- 10 Click **OK**.  
You should see an event in the vSphere Client recent tasks status bar stating **Update date or time**.

### Results

Within 15 minutes, the ESXi host time should synchronize with the NTP time server.

## Adding and renaming datastores

During the installation of an ESXi host, one datastore is formatted as *vmfs* and named as a default “datastore” or “datastore(1)” format. This datastore name needs to be changed to help identify the ESXi Host that the datastore belongs to, and to help identify where a virtual machine storage is located in the future.

To assist with identification of storage resources within the virtual infrastructure, Honeywell recommends the use of a datastore naming convention. An example convention is:

Name:Datastore*x*

Where:

- *Name* is the ESXi host
- *x* is the number that is used to identify the datastore

### To rename an existing datastore

- 1 In the vSphere Client (within Home > Inventory >), choose the **Inventory** view.
- 2 Locate and select the ESXi host that needs its datastore to be renamed.
- 3 Click the **Configuration** tab.
- 4 Click the **Storage** option in the Hardware pane.  
The existing datastore(s) are listed.
- 5 Right-click on the name of the datastore that needs to be renamed and select **Rename**.

### To add a new datastore to an ESXi host

- 1 In the vSphere Client (within Home > Inventory >), choose the **Inventory** view.
- 2 Locate and select the ESXi host to which you want to add a datastore.
- 3 Click the **Configuration** tab.
- 4 Click the **Storage** option in the Hardware pane, then click **Add storage**.  
The **Add Storage** dialog is displayed.
- 5 Click **Disk/LUN** and then click **Next**.
- 6 Confirm the review of the disk layout and then click **Next**.
- 7 Select the required maximum file size for virtual machines on the datastore. In most cases the default of 256GB will be enough.
- 8 Click **Next**.
- 9 Review the system properties and formatting and then click **Finish**.  
The datastore will be formatted into a *vmfs* datastore ready for virtual workload to use.

## Preparing a vCenter Server

On the management ESXi host, you need to create a virtual machine to host the vCenter Server (and vCenter Update Manager). The vCenter Server contains the required software components for the administration of virtual machines, ESXi hosts, and the virtualization environment. You need to install a vCenter Server to manage the virtual environment.

### vCenter Server preparation considerations

Consideration	Description
Management host workload	The vCenter Server will run as a virtual machine on the management host in the virtual infrastructure. It is important to consider the number of virtual machines that will also run on the management host so that adequate resources are available. All template creation and storage should also be encapsulated by the management host so that production workloads are not affected by this type of operation. For more information, see the related topic.
Windows domain controller	<p>A Windows domain must exist before you create the vCenter Server. Ensure that a physical domain controller exists that vCenter can communicate with or install a new Windows domain controller on the management host. The Windows domain controller must:</p> <ul style="list-style-type: none"> <li>• Perform the role as a DNS server</li> <li>• Use reverse lookup zones for all subnets in the infrastructure</li> <li>• Use DNS HOST A and PTR records to the Forward and Reverse lookup Zones for each of the ESXi hosts, using their management network IP address. For more information about setting up a Windows domain controllers, see the <i>Window Domain and Workgroups Implementation Guide</i> available from the Honeywell Process Solutions Support web site.</li> </ul>
vCenter Server Databases	<p>vCenter Server and vSphere Update Manager installations require a database and you need to decide which database to use. A bundled version of Microsoft SQL Server 2008 R2 Express database package is supplied with the vCenter Server installation. This version of SQL is only supported for systems with up to 5 ESXi hosts and 50 virtual machines. If the virtual infrastructure you are creating is likely to exceed this size, you must purchase and install a full version of Microsoft SQL Server for use with both vCenter Server and vSphere Update Manager.</p> <p>When you choose to use one of the qualified databases (not the bundled Microsoft SQL Server 2008 R2 Express database), you will need to create vCenter Server and vSphere Update Manager databases and configure an appropriate connection to these databases prior to installing vCenter Server and vSphere Update Manager. You also need to install Microsoft SQL Server on the vCenter Server virtual machine. For more information refer to the <i>Installation and configuration of SQL server and vCenter server</i> white paper, available from the Honeywell Process Solutions web site.</p> <p>It is important that the Microsoft SQL Server database being used for vCenter Server and vCenter Update Manager follow a database maintenance process. Monitoring the growth of database log files and compacting those log files, and regular backups are important.</p>
Virtual Machine Replication	When virtual machine replication is used the vCenter Server requires extra applications to be installed. Installing these applications during the initial installation and configuration phase of the vCenter server will prevent possible restarts later when this type of interruption may not be acceptable. Refer to “Replicating a virtual machine” for an overview of this functionality and requirements in the vCenter Server.

### Introduction to vCenter Server installation

ESXi 5.x uses the same installer for clean installations and upgrades or migrations. If the installer encounters an existing ESXi 4.1 or ESXi 5.0 installation, it provides the option to upgrade or do a clean install. For deployments with bundled SQL, vCenter Server 5.1 provides a *vCenter Server Simple Install* option that installs the following in the same virtual machine:

- vCenter Single Sign-On

- Inventory Service
- vCenter Server

vSphere Update Manager will be installed into the same virtual machine after the vCenter Server Simple Install is complete.

Listed below are the components that make up the management infrastructure.

Component	Description
VMware vCenter Server	Windows service to manage ESXi hosts
vCenter Single Sign On	vSphere 5.1 introduces <i>vCenter Single Sign On</i> as part of the vCenter Server management infrastructure. This additional component affects vCenter Server installation, upgrading, and operation. Authentication by vCenter Single Sign On allows the vSphere software components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory. Experion Virtualization includes guidance to install and configure vCenter Single Sign On, but its usage is not required unless you choose to use the vSphere Web Client.
vCenter Inventory Service	<i>Inventory Service</i> stores vCenter Server application and inventory data, enabling you to search and access inventory objects across linked vCenter Servers. Prior to ESXi 5.0, this component was automatically installed on the same host as vCenterServer. Since Inventory Service can reside on remote hosts, its installation is a separate step. For the installation of vCenter Server with embedded SQL, the inventory service will continue to be installed on the same host as vCenter Server.
vSphere Web Client	The <i>vSphere Web Client</i> is a server application that provides a browser-based alternative to the traditional vSphere Client. Experion Virtualization continues to provide guidance through usage of the vSphere Client. Use of the vSphere Web Client is optional.

#### Related topics

“Planning for the management ESXi host and management network” on page 56

*One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.*

“Replicating a virtual machine” on page 150

## Creating a vCenter Server virtual machine with bundled SQL

Use this section to create a virtual machine to host vCenter Server with bundled SQL and vSphere Update Manager. Both vCenter Server and Update Manager are installed with and configured to use Microsoft SQL Server 2008 R2 Express database. This means that the virtual infrastructure you are creating meets the criteria identified in the above table (see vCenterServer Databases row)

**Attention**

- If your virtual infrastructure is greater than 5 hosts with 50 virtual machines, you must purchase and install a full version of Microsoft SQL Server for use with both vCenter Server and vSphere Update Manager. Microsoft SQL Server should be installed on the vCenter Server virtual machine. To perform the installation with separate SQL, use the *Installing and configuring SQL server and vCenter server* white paper rather than the instructions in this section. This document is available from the Honeywell Process Solutions web site. When you have finished the procedure contained in the white paper, proceed to the “Preparing the vCenter utility” and “Organizing VMware Inventory objects” sections in this guide.

**Prerequisites**

Before creating the vCenter Server virtual machine, ensure that you have:

- Installed and configured the management network.
- Created the management ESXi host and connect it to the management network.
- A supported 64-bit Windows operating system license.

Honeywell recommends that you use a 64-bit version of the Windows operating system that is currently used for your Experion system or organization for operating system consistency.

- A Windows domain controller established.
- Reviewed and confirmed that the vCenter Server prerequisites are met, as defined in the “Before You Install vCenter Server” section of *vSphere Installation and Setup*. This would include:
  - Prerequisites for Understanding and Preparing for the Installation Process
  - System Prerequisites
  - Network Prerequisites

**Domain user and group Creation and Security**

Domain accounts are used as service accounts to facilitate the Installation of SQL Server, vCenter Server and VMware Update Manager. These accounts control authentication between the different applications and also strengthen the security of the management infrastructure.

To create domain accounts:

1. Use the **Active Directory Users and Computers console** on the domain controller to add 2 domain users:
  - vCenterAdmin
  - vCenterVUM
2. Set the password expiry for each account to a long period of time or never to expire, depending on your site security policy.

**To create a virtual machine to host vCenterServer and vSphere Update Manger with bundled SQL**

1. From the vSphere Client connected to the management network, connect to the management ESXi host, using the IP address of the management ESXi host and the user name and password that you defined when you prepared the management ESXi host.
2. After you have connected to the management ESXi host, create a virtual machine. For the vCenter Server (management node) virtual machine configuration details, see the *HPS Virtualization Specification*.
3. Install a supported 64-bit Windows operating system on the virtual machine.

If Microsoft Internet Information Services (IIS) is installed as part of the Windows operating system installation, you should uninstall it to avoid conflicts with the web server installed as part of vCenter Server.

4. Login to the vCenter Virtual machine as a local administrative user and use the Computer Management Console to add the two domain accounts to the Local Administrators group.
5. Using the **Active Directory Users and Computers console** on the domain controller, create a security group called **vcenterAdmins**, and add the new domain users to the group.
6. Install VMware Tools. For more information, see the related topics.



7. Add the vCenter Server virtual machine to both the forward and reverse lookup of your DNS server.
  - a. Verify that the fully qualified domain name of the virtual machine where you will install vCenter Server is resolvable
  - b. Verify that the DNS reverse lookup returns a fully qualified domain name when queried with the IP address of the vCenter Server
8. If you are performing a clean install of vCenterServer, then proceed to **step 7**. Otherwise, perform the following steps:
  - a. Make a backup of your existing vCenterServer database and SSL certificates.
  - b. Make a backup of your existing UpdateManager database.
  - c. Stop the vCenter Server service which is named *VMware VirtualCenter Server*.
9. Log-on to the newly created vCenter Server virtual machine as the **Domain\vCenterAdmin** user.
10. Using the vSphere Client, mount the vCenter Server iso as a DVD to the vCenter Server virtual machine. When the AutoPlay dialog is displayed, select **RUN autorun.exe** to start the installer.
11. Under **VMware Product**, verify that the **VMware vCenter Simple Install** is selected by default. Click **Install** and click **OK**.

The **vCenter Single Sign On Installation wizard** is displayed.

12. On the **vCenter Single Sign On** page, click **Next**.
13. On the **Welcome** page, click **Next**.
14. On the **End-User Patent Agreement** page, click **Next**.
15. On the **License Agreement** page, select **I agree to the terms in the license agreement** and click **Next**.
16. On the **vCenter Single Sign On Information** page, enter the password. Confirm the password and click **Next**. Record this password for later usage.
17. On the **vCenter Single Sign On Database** page, accept the default selection to install Microsoft SQL Server 2008 R2 Express in the virtual machine. Click **Next**.
18. On the **Set Database User Information** page, enter the passwords for the default database SQL users, DBA user, RSA\_DBA and RSA\_USER. Record these passwords, then click **Next**.
19. On the **Local System Information** page, enter the fully qualified domain name for the virtual machine. For example, **myvcvirtualmachine.mydomain.local**, then click **Next**.
20. On the **Security Support Provider Interface Service Information** page, clear the **Use the Network service account** check box. Enter **vCenterAdmin** as the User name, then enter the password and domain for vCenterAdmin account. Click **Next**.
21. On the **Destination Folder** page, accept the default destination folder and click **Next**.
22. On the **vCenter Single Sign On Port Settings** page, accept the default port number. Click **Next**.
23. On the **Ready to Install** page, click **Install** to perform the installation of both the vCenter Single Sign On and the VMware vCenter Server Inventory Service on the vCenter virtual machine. This takes at least 5 minutes to complete.
24. When the installation of vCenter Single Sign On and the VMware vCenter Server Inventory Service is complete, the installation wizard continues with the vCenter Server install process.
25. On the **License Key** page, enter your vCenterServer license key and click **Next**.
26. On the **Database Options** page, click **Next** since you are using the default vCenter Server database (Microsoft SQL Server 2008 R2 Express)
 

If you receive a warning that this vCenter Server system is being used by the VMware vSphere Update Manager, click **OK**. You will upgrade Update Manager in a later step.
27. On the **Database Upgrade Warning** page (only appears if the installer detects an existing database), click **Upgrade existing vCenter Server database**. Select the box that verifies that you have made a backup of the existing vCenter Server database and SSL certificates. Click **Next**.
28. On the **vCenter Agent Upgrade** page (only appears if the installer detects an existing vCenter Server), confirm that **Automatic** is selected and click **Next**.

29. On the **vCenter Server Service** page, select **Use SYSTEM Account**. Verify that your vCenter Server host name appears in the **Fully Qualified Domain Name** field. Click **Next**.
30. On the **Configure Ports** page, accept the default port values and confirm that the **Increase the number of ephemeral ports** check box is cleared. Click **Next**.
31. On the **vCenter Server JVM Memory** page, accept **Small** (the default) and click **Next**.
32. On the **Ready to Install the Program** page, click **Install**. The installation process typically takes up to 15 minutes to complete.
33. Click **Finish** when the install is complete.
34. Click **OK** when prompted to confirm that the vCenter package containing vCenter Single Sign-On, VMware vCenter Inventory Service, and VMware vCenter Server has installed successfully. Verify that the vCenter Server service started automatically as a result of the successful installation.

#### Installing VMware vCenter Update Manager

1. From the **VMware vCenter Installer** window, select **VMware vSphere Update Manager**. Click **Install** to begin the Update Manager installation process.
2. On the **Installation Language** page, select the desired installation language and click **OK**.
3. On the **Update Manager Warning** page (only appears if installer detects an existing version of Update Manager), click **OK** to the warning stating that an earlier version of Update Manager is already installed on this system.
4. On the **Welcome** page, click **Next**.
5. On the **End-User Patent Agreement** page, click **Next**.
6. On the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. On the **Support Information** page, clear the **Download updates from default sources immediately after installation** check box, then click **Next**.
8. On the **vCenter Server Information** page:
  - a. In the **IP Address/Name** field, verify that the host name or IP address of your vCenter Server system is displayed.
  - b. Accept the default port in the **HTTP Port** field.
  - c. In the **Username** field, type **vcenterVUM**
  - d. In the **Password** field, type the vCenterVUM password that you created previously.
  - e. Click **Next**.
9. On the **Database Options** page, select the **Install a Microsoft SQL Server 2008 R2 Express instance** option, then click **Next**.
10. On the **Database Information** page (only appears if installer detects an existing version of Update Manager):
  - a. Click **Yes, I want to upgrade my Update Manager database**.
  - b. Select the **I have taken a backup of the existing Update Manager database** check box.
  - c. Click **Next**.
11. On the **VMware vSphere Update Manager Port Settings** page, confirm the host name for the Update Manager system. Accept the default ports and click **Next**.
12. On the **Ready to Install the Program** page:
  - a. Click **Install**. The install process typically takes less than 5 minutes to complete.
  - b. Click **Finish** when the install is complete.

#### Installing VMware vSphere Client

1. From the **VMware vCenter Installer** window, select **VMware vSphere Client**. Click **Install** to begin the installation.
2. On the **User Account Control** dialog, click **Yes**.

3. On the **Installation Language** page, select the desired installation language and click **OK**.
4. On the **Welcome** page, click **Next**.
5. On the **End-User Patent Agreement** page, click **Next**.
6. On the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. On the **Destination Folder** page, accept the default destination provided, then click **Next**.
8. On the **Ready to Install the Program** page, click **Install**.

The installation typically takes about 5 minutes to complete. Click **Finish** when prompted.

### Installing VMware vSphere Web Client

1. From the **VMware vCenter Installer** window, select **VMware vSphere Web Client**. Click **Install** to begin the installation.
2. On the **User Account Control** dialog, click **Yes**.
3. On the **Installation Language** page, select the desired installation language and click **OK**.
4. On the **Welcome** page, click **Next**.
5. On the **End-User Patent Agreement** page, click **Next**.
6. On the **License Agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. On the **Destination Folder** page, accept the default destination provided, then click **Next**.
8. On the **VMware vSphere Web Client Port Settings** page, accept the default port settings and click **Next**.
9. On the **vCenter Single Sign On Information** page, enter the administrator password that you created previously when setting the Database user information for single sign on, then click **Next**.
10. On the **Ready to Install the Program** page, click **Install**.

The installation typically takes about 5 minutes to complete. Click **Finish** when prompted.

### Setting up Single Sign On

1. Download and install Adobe flash player on the vCenter Server from <http://www.adobe.com/products/flashplayer/distribution3.html>. (Flash is required when using the vSphere web client).  
Note: From the Adobe download page, scroll down and click the option containing the text **Download EXE installer**. Clicking the **Download Adobe Flash Player** option will fail as it requires internet connectivity.
2. From the Start menu, locate and click on the **vSphere Web Client application**.
3. When the error page is displayed, click **Continue to this website**.
4. Type **admin@system-domain** in the **User name** field, and the password recorded when single sign-on was installed in the **Password** field. Click **Login**.
5. From the navigation pane, click **Administration**.
6. From the navigation pane, click **SSO Users and Groups**, then click the **Groups** tab.
7. Select the **\_Administrators\_** row in the table.
8. Click the **Add group members** icon underneath the table.
9. On the **Add Principals** dialog, select the Windows domain from the **Identity source** list.
10. Type **vcenterAdmins** in the **Search** field and click **Search**.

The vCenterAdmins group is displayed.

11. Select the **vCenterAdmins** group and click **Add**.

The Selected principals field updates to list the vCenterAdmins domain group.

12. Click **OK**.

The Groups tab refreshes and lists the vCenterAdmins group in the Group Members section.

13. From the navigation pane, click **Configuration**.
14. Select the domain **ldap** item in the table, and then click the **Add Default Domain** icon from the tool bar on the tab.

15. A warning about having multiple domains appears. Click **OK** to dismiss the message.
16. The local domain is listed in the **Default Domains** section. Click the **Save** icon to save your changes.
17. Close the vSphere Web Client.

### Related topics

“Planning for the management ESXi host and management network” on page 56

*One or more management ESXi hosts contain the software components for the administration and management of virtual infrastructure. The management network separates the management network traffic between the ESXi hosts and the management nodes from the process control network (PCN) or production traffic.*

“About vSphere Update Manager” on page 65

*With vSphere Update Manager, you can automate patch management and eliminate manual tracking and patching of ESXi hosts.*

## Configuring the vCenter Server

Prior to adding ESXi hosts to the vCenter Server, you need to configure it.

### To configure a vCenter Server

1. Configure the vCenter Server by following the instructions in the “Configuring vCenter Server” topic in the “Configuring Hosts and vCenter Server” section of *vCenter Server and Host Management*. Use the following table to identify appropriate values to enter for each setting.

Setting	Description
Logging Options	ESXi hosts publish many events, which can fill the vCenter Server logs. Most of these events are not necessary for ESXi host maintenance. Therefore, it is recommended to set the Logging Options to <b>Info (Normal logging)</b> to reduce the size of the logs maintained on the vCenter Server.
Database Retention Policy	<p>The vCenter Server stores the task, event, and performance data in the vCenter database. Over time, this collection of data will continue to grow, unless this database has been constrained by a preset limit, which is known as the Database Retention Policy. The default setting for this policy is to save all data values without limitation.</p> <p>To control the size of this database, it is recommended that these events be held for a specific period and then purged. The recommended setting is 60 days. This will limit the retention of these events to 60 days, at which time they will be purged from the database. Ensure that the <b>Tasks Retained for</b> and <b>Events retained for</b> options are selected.</p>

### To configure vSphere Update Manager

1. The default installed configuration of the vSphere Update Manager server will access the internet to download patches and extensions to the Update Manager patch repository. Honeywell recommends disabling internet downloads and using the “Import Patches Manually” method described in the “Configuring the Update Manager Download Sources” section of *Installing and Administering VMware vSphere Update Manager*. This method supports the Honeywell methodology of only installing Honeywell SUIT evaluated VMware patches or updates.
2. Configure the vSphere Update manager by following the instructions in the “Configuring Update Manager” section of *Installing and Administering VMware vSphere Update Manager*. The following table includes the Honeywell recommended settings for each of the topics which include disabling the default settings to access the internet.

Setting	Recommended values
Network Connectivity settings	Accept default values unless a conflict exists

Setting	Recommended values
Download Settings	<ol style="list-style-type: none"> <li>1. Disable Patch Download Sources</li> <li>2. Select <b>Direct connection to Internet</b></li> <li>3. Clear <b>(ALL) Enabled Patch Sources</b></li> <li>4. Proxy Settings <ul style="list-style-type: none"> <li>• Clear <b>Use Proxy</b></li> </ul> </li> </ol>
Download Schedule	<ol style="list-style-type: none"> <li>1. Disable Patch Download</li> </ol>
Notification Check Schedule	<ol style="list-style-type: none"> <li>1. Disable Notification Check</li> </ol>
Virtual Machine Settings	<ol style="list-style-type: none"> <li>1. Select <b>Take a snapshot of virtual machine</b></li> <li>2. Set <b>Keep for to 18 hrs</b></li> </ol>
ESX Host/Cluster Settings	<ol style="list-style-type: none"> <li>1. Clear <b>Retry entering maintenance mode in case of failure</b></li> <li>2. Select <b>Temporarily disable any removable media devices</b></li> <li>3. Clear <b>Distributed Power Management</b></li> <li>4. Clear <b>High Availability Admission Control</b></li> <li>5. Clear <b>Fault Tolerance (FT)</b></li> <li>6. Clear <b>Enable parallel remediation for hosts in cluster</b></li> <li>7. Clear <b>Migrate powered off and suspended virtual machines to other hosts in cluster</b></li> <li>8. Clear <b>Allow installation of additional software on PXE booted ESXi 5.x hosts</b></li> </ol>
vApp Settings	Accept default values.

## Installing the Experion virtual machine utility

You need to install this utility if the version of vCenter Server on your system is 5.1 or later.

1. On the vCenter Server machine, open the Experion System Initialization Updates media.
2. Navigate to `\Packages\vCenter_utility\`. Right-click on the **Honeywell\_vCenter\_utility.exe** file and click **Run as Administrator**.
3. Click **Install**.
4. When the installation completes, click **OK** to close the dialog box and launch the **Experion Virtual Machine Service Panel**.
5. Enter the credentials for a user with the privileges to read/write/configure your virtual machines.
6. Click **Start Service** to optimize existing virtual machines to execute with Experion.



### Tip

If you need to change the credentials for the Experion Virtual Machine Service Panel, navigate to `"c:\program files (x86)\Honeywell\ExpVCSERVICE\"` on the vCenter Server machine and run the `ExpVCSERVICEControlPanel.exe` file. The Experion Virtual Machine Maintenance Service Panel dialog box appears. If the service is already running, you will need to click **Stop Service** so that you can enter the new credentials. This may occur if the server credentials change in response to IT Policies.

## Organizing VMware inventory objects

You should identify how to organize inventory objects in vCenter Server.

A logical grouping of inventory objects will help you more easily locate ESXi hosts and virtual machines within vCenter Server.

You should identify this grouping and then create the required inventory objects in vCenter Server, such as datacenters and folders, before adding the ESXi host to vCenter Server.

The *"Planning how to organize the vCenter Server"* section of this guide provides more detail and planning considerations on the layout of the inventory. This planning section should be read and fully understood before commencing the organization of inventory objects.

### Naming the virtual machine

- Within the inventory objects virtual machines are created. These virtual machines need to be clearly identified. The naming convention used for virtual machines may include the guest OS name and optionally any other information of use.
- An example Virtual Machine naming convention is `hostname-xxxx`, where:
  - *Hostname* is the name of the guest operating system
  - *XXXX* is optional information of significance respective to applications and system implementation.
- An example Virtual Machine name using this convention is: `esxivcenter-cluster1`



#### Attention

Virtual Machine names may be used by other applications and scripts. Avoid extensive names and special characters.

---

### Related topics

“Planning how to organize the vCenter Server” on page 61

*Hosts and their virtual machines should be organized within vCenter Server based on logical groupings.*

## Adding the ESXi host to the vCenter Server

Add new ESXi hosts to the vCenter Server.

### Prerequisites

- *vCenter Server and Host Management.*
- The Windows hosts file on vCenter Server must be updated to include the ESXi host name resolution (host name or IP address).

### To add an ESXi host to vCenter Server

1. Add the ESXi host to the vCenter Server by following the instructions in the “Add Hosts” topic in the “Organizing Your Inventory” section of *vCenter Server and Host Management*.

## Configuring the virtual machine load order on the management ESXi host

Management ESXi hosts require configuration to ensure that the management virtual machines are automatically started and started in a specific order.

As part of this configuration, you can also specify a delay for virtual machines to start up or shut down. A startup delay is recommended to minimize overburdening the resources of an ESXi host by limiting the number of simultaneous virtual machine start ups or shut downs.

Honeywell recommends that you enable the startup and shutdown behavior of all virtual machines. If you do not specify this behavior, you will need to manually start each virtual machine on an ESXi host after the ESXi host is restarted.

The recommended startup order for workloads is:

1. Domain controller
2. vCenter server



### Attention

If any components in the vCenter Server access an external database server (for example, vCenter Server or Update Manager), the database server must be started and running before starting the management workload.

3. Other management workload.

### To configure the virtual machine load order

- Configure the virtual machine load order by following the instructions in the “Edit Virtual Machine Startup and Shutdown Settings” topic in *vSphere Virtual Machine Administration*.

Set the following configuration settings.

Configuration Item	Setting
<b>Allow virtual machines to start and stop automatically</b> check box.	Selected
<b>Default Startup Delay</b> text box	120 seconds
<b>Continue immediately if the VMware tools start</b> check box.	Selected
<b>Startup Order</b> list	For process operational workloads: add the virtual machines to the <b>Automatic Startup</b> group in the following order: <ol style="list-style-type: none"> <li>1. Windows domain controller</li> <li>2. vCenter Server —includes Update Manager</li> <li>3. EBR application</li> <li>4. VMware Site recovery manager (optional)</li> <li>5. Other management nodes</li> </ol>

## Configuring security in a vCenter Server

Create vCenter roles and assign them to Experion users or global groups, and configure host lockdown mode.

### Related topics

“Creating vCenter roles and assigning privileges” on page 128

*vCenter roles are a collection of defined privileges that control individual user or group access to particular vSphere objects.*

“Assigning vCenter roles to Experion users or global groups” on page 128

*After you have defined vCenter roles, assign the role to the required Experion users or global groups to associate these access permissions to the datacenter and its contents.*

“Configuring host lockdown mode” on page 129

*Host lockdown mode ensures that the ESXi host is managed only through vCenter Server.*

## Creating vCenter roles and assigning privileges

vCenter roles are a collection of defined privileges that control individual user or group access to particular vSphere objects.

### Prerequisites

- You are logged into vSphere Client with administrator privileges.

### To create vCenter roles and assign privileges

- 1 On the vSphere Client, choose the **Home > Administration > Roles** view.
- 2 Click **Add Role**.  
The **Add New Role** dialog box appears.
- 3 In the **Name** box, type the role name.
- 4 In the **Privileges** list, select or clear the appropriate privilege check boxes for this role.
- 5 Click **OK** to create the role.

### Related topics

“User accounts, roles, and permissions” on page 67

*VMware user accounts are not created within vCenter. Instead, vCenter authorizes users based on accounts defined within the Windows operating system, either on a Windows domain controller or local Windows users on the vCenter Server. Within vCenter, you define roles and configure appropriate permissions for these roles. You then assign Windows users or groups to these roles.*

## Assigning vCenter roles to Experion users or global groups

After you have defined vCenter roles, assign the role to the required Experion users or global groups to associate these access permissions to the datacenter and its contents.

### To assign vCenter roles to Experion users or global groups

- 1 On the vSphere Client, choose the **Home > Inventory > Host and Clusters** view.
- 2 Locate and right-click on the datacenter and choose **Assign Permission**.  
The **Assign Permissions** dialog box appears.
- 3 In the **Assigned Role** list, select the role to be assigned.



- 4 Click **Add**.  
The **Select Users and Groups** dialog box appears.
- 5 Select the appropriate Windows domain and then select the user or global group to be assigned the role.
- 6 Click **OK**.
- 7 Select the **Propagate to Child Objects** check box to propagate the user/role to all hosts and virtual machines within the datacenter.
- 8 Click **OK**.

#### Related topics

“User accounts, roles, and permissions” on page 67

*VMware user accounts are not created within vCenter. Instead, vCenter authorizes users based on accounts defined within the Windows operating system, either on a Windows domain controller or local Windows users on the vCenter Server. Within vCenter, you define roles and configure appropriate permissions for these roles. You then assign Windows users or groups to these roles.*

## Configuring host lockdown mode

Host lockdown mode ensures that the ESXi host is managed only through vCenter Server.

#### To configure host lockdown mode using vSphere Client

- 1 On the vSphere Client, choose the **Home > Inventory > Hosts and Clusters** view.
- 2 Locate and click on the host computer.
- 3 Click the **Configuration** tab.
- 4 Under the **Software** group, click the **Security Profile** link.
- 5 Click **Edit**.  
The **Configure Host Lockdown mode** dialog box appears.
- 6 Select the **Enable Host Lockdown mode** check box.  
A confirmation message appears.
- 7 Click **OK**.

#### To configure host lockdown mode using the ESXi host console

- 1 On the ESXi host console, select **Configure Lockdown Mode** and press **Enter**.
- 2 Press the spacebar to select **Enable Lockdown Mode** and press **Enter**.
- 3 Press **Enter**.

#### Related topics

“About host lockdown mode” on page 68

*Host lockdown mode prevents remote users from logging into an ESXi host using the root user and password.*



# Preparing a production ESXi host

Prepare a production ESXi host for production workloads.

## Related topics

“Configuring the ESXi host local disk array” on page 132

*Prior to installing the ESXi hypervisor software, you must prepare the local disk array on the ESXi host.*

“Configuring the ESXi host BIOS settings” on page 133

“Installing the ESXi software on a host” on page 134

*Use the guidance in this section to perform a clean install of the ESXi software on the host. If you are upgrading or migrating an existing ESXi installation, see “Upgrading virtual infrastructure software”.*

“Configuring the ESXi host network settings” on page 135

*After you install the ESXi software on a host, you need to configure the network settings and the ESXi password.*

“Configuring ESXi host time synchronization” on page 144

“Adding the ESXi host to the vCenter Server” on page 145

*Add new ESXi hosts to the vCenter Server.*

“Domain name resolution” on page 146

*ESXi hosts need to be manually added to the domain name server (DNS).*

“Creating and managing virtual machines” on page 147

## Configuring the ESXi host local disk array

Prior to installing the ESXi hypervisor software, you must prepare the local disk array on the ESXi host.

The RAID configuration of a performance production host should be RAID 10 with a hot spare. The RAID configuration of a lower capacity production host can be RAID 1.

The following table provides guidance on RAID configuration based on the usage of the ESXi host:

ESXi host type	RAID configuration
Production ESXi host in a SCADA architecture.	RAID 10 with a hot spare. <sup>5</sup>
Production ESXi host in a DCS architecture.	RAID 10 with a hot spare.
Production ESXi host in a DCS architecture with low capacity.	RAID 1. <sup>6</sup>
Management ESXi host.	RAID 1. <sup>7</sup> Create multiple groups: <ul style="list-style-type: none"> <li>• One group for management workloads (which will form the <i>management datastore</i>).</li> <li>• One group for staging Experion virtual machine installations (which will form the <i>staging datastore</i>).<sup>8</sup></li> </ul>

Prior to ESXi installation, confirm that the preferred boot device is selected. Refer to the appropriate Dell document for the RAID controller on the server hardware for instructions to assign a preferred boot device.

<sup>5</sup> RAID 5 with hot spare optional to achieve greater capacity

<sup>6</sup> If the hardware is capable then “Production host in a DCS architecture” configuration is permitted

<sup>7</sup> If the hardware is capable then “Production host in a DCS architecture” configuration is permitted

<sup>8</sup> Higher performance host / RAID configuration to be considered

## Configuring the ESXi host BIOS settings

Virtualization technology abstracts the Experion application from the ESXi host hardware so that when virtualized, Experion interactions with the BIOS are minimized.

Use the following steps to deploy an ESXi host with a BIOS that is optimized for virtualization. For detailed instructions on how to view and update the BIOS settings, see the host computer manufacturer's documentation.

1. Use the latest version of the BIOS that is available for your virtualization host.
2. Confirm that the following BIOS settings have been set on the ESXi host:
  - Sockets and cores enabled.
  - 64-bit mode enabled.
  - (VT) Intel Virtualization Technology enabled (for CPU and for memory).
  - Turbo Mode enabled.
  - Execute Protection feature is enabled (for Intel, eXecute Disable (XD) enabled).
  - Hyper Threading enabled.



### Attention

You may have to enable this through vSphere Client.

- Node Interleaving disabled.
- Unused hardware disabled (including iDRAC).
- Hardware clock is set to UTC.
- Power Management set to Maximum Performance (that is, disable Power Management).

For additional information related to recommended BIOS settings on an ESXi host, refer to the VMware document, *Performance Best Practices for VMware vSphere® x*, where “x” is the vSphere release of the ESXi hypervisor, for example, 4.1, or 5.0 or 5.1.

For additional information relating to ESXi host platform specifications pertaining to validated BIOS revisions, refer to the *HPS Virtualization Specification*.

## Installing the ESXi software on a host

Use the guidance in this section to perform a clean install of the ESXi software on the host. If you are upgrading or migrating an existing ESXi installation, see “Upgrading virtual infrastructure software”.



### Attention

Before you begin the clean install of ESXi, review any differences that have been introduced with the new vSphere release. Check for related topics in the "Introduction to vSphere Installation and Setup" section of *vSphere Installation and Setup*.



### CAUTION

The root password for each ESXi host should be set during installation. Each ESXi host should not be connected to a trusted network until you have configured a root password on the ESXi host.

### Prerequisites

- On the host computer, you have set up:
  - the disk array
  - the BIOS settings
- Review "Introduction to vSphere Installation and Setup" in *vSphere Installation and Setup*. The following guidance is for the Interactive ESXi Installation option.



### Tip

Experion virtualization media and documentation is available for download from the Honeywell Online Support web site <http://www.honeywellprocess.com/>.

- If you plan to create an Experion virtual machine on this ESXi host that requires a USB security device (dongle), see *vSphere Virtual Machine Administration* for guidance.

### To install an ESXi host

1. Install the ESXi host using the instructions in "Installing ESXi Interactively" in the *vSphere Installation and Setup guide*.
2. If you plan to create an Experion virtual machine on this ESXi host that requires a USB security device (dongle), add the USB security device to this ESXi host by following the instructions in the “USB Configuration from an ESXi Host to a Virtual Machine” topic in *vSphere Virtual Machine Administration*.

In the VMware environment, the physical network adapters on the ESXi host are named vmnic *n*, where *n* is unique number identifying the network adapter. During the installation of the ESXi software, network adapters are assigned a vmnic number (starting with 0) in the order in which the adapters are detected. Physical network adapters are referenced with the vmnic *n* names when configuring a vSwitch or viewing the vSwitch configuration.

Honeywell recommends that the network adapter cards (single or multiple port) be assigned the same slots in each ESXi host.

The set of virtual network adapters configured for a virtual machine are referenced as vNIC *n* where *n* is a unique number identifying the virtual network adapter. This naming convention is for documentation purposes only.

# Configuring the ESXi host network settings

After you install the ESXi software on a host, you need to configure the network settings and the ESXi password.



## CAUTION

Since the root password for ESXi is blank after the initial installation, the ESXi host should only be connected to a trusted network until you have configured a new root password on the ESXi host.

After you have configured the IP address of the ESXi host from the direct console, you can connect to the ESXi host from the vSphere Client. However, to complete the network connectivity configuration of the ESXi host, access from the direct console is required.

## Prerequisites

- You have installed vSphere Client on a physical node that is connected to the management network.
- You have the network details for the ESXi host, such as:
  - The IP address, subnet mask, and default gateway of the network interface cards (NICs) for the management network.
  - Primary and alternative (secondary) DNS server IP addresses.
  - DNS search suffixes.
- Familiarity with, or access to the “Setting Up ESXi” section in *vSphere Installation and Setup*.

## To configure the ESXi root password and host IP address

1. Connect to the ESXi host from the Direct Console to configure the root password. Use the instructions in the section “Set the Password for the Administrator Account”.
2. Connect to the ESXi host from the Direct Console or from the vSphere client to configure the ESXi host IP address. Use the instructions in the “Configuring IP Settings for ESXi” section of *vSphere Installation and Setup*.
3. Associate the IP address with the default pNIC0 used for management network.

## To configure the ESXi host DNS settings

1. Connect to the ESXi host from Direct Console.
2. Follow the instructions in the “Configure DNS Settings from the Direct Console” section of **vSphere Installation and Setup**.
3. From the direct console, select **Test Management Network** to confirm that you have network connectivity.

## Related topics

“Network configuration for a production host in a DCS architecture” on page 136

*After you complete the initial network configuration, you need to configure the virtual network for the production host.*

“Network configuration for a production host in a SCADA architecture” on page 139

*After you complete the initial network configuration, you need to configure the virtual network for the production host.*

“Configuring NIC teaming” on page 142

*Configure the NIC teaming settings. A NIC team can share the traffic load between the physical and virtual networks among some or all of the NIC team members, or provide passive failover in the event of a hardware failure or a network outage.*

“Configuring the virtual switch port security settings” on page 143

*To protect virtual machines from intrusion, the virtual switch port security settings should be modified from the default values.*

## Network configuration for a production host in a DCS architecture

After you complete the initial network configuration, you need to configure the virtual network for the production host.

A virtualized DCS architecture requires ESXi hosts at Level 2 and Level 3 to support the production workloads as well as an ESXi host to support the management workload.

While the network connectivity of the virtualized production workloads is the same as in a physical system (for example, FTE at Level 2 with network isolation from Level 3), there is an additional network introduced for the management infrastructure. This management network may span all ESXi hosts in order to provide management access to all elements of the virtualized infrastructure.

### High capacity hosts

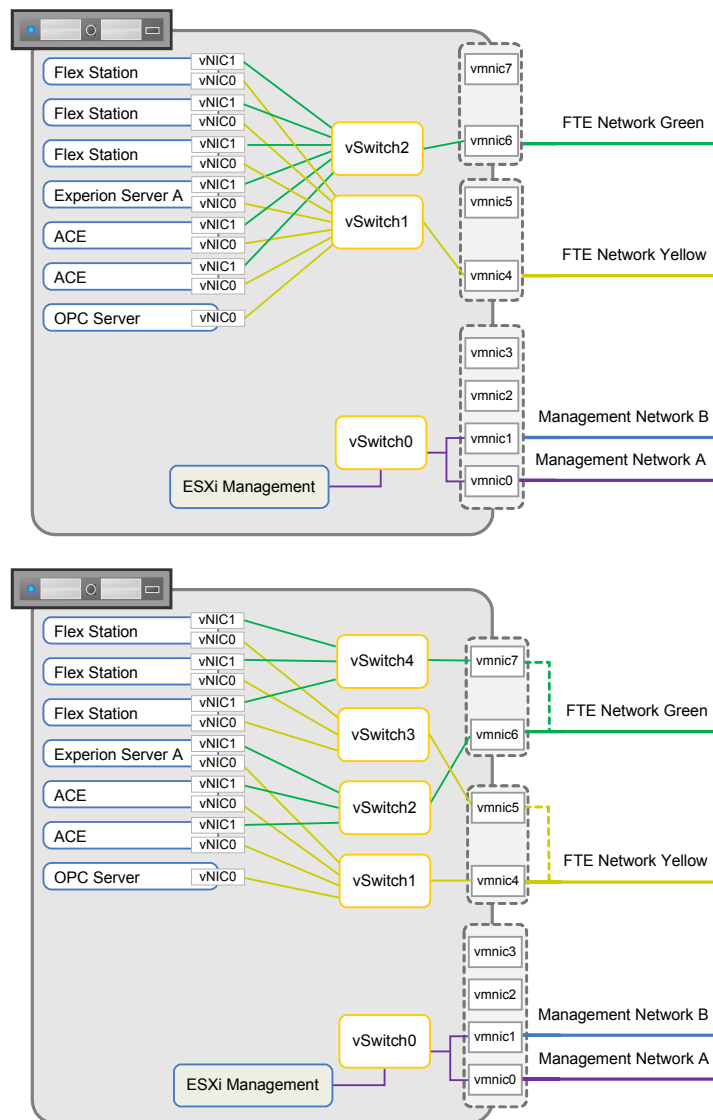


Figure 25: Example configurations of high capacity production ESXi host with local storage



You need a NIC allocation scheme for each production ESXi host. For more information, see the related topics.

The high capacity host shown in the first image is configured to use the on-board multi port NIC to connect the ESXi management component to the physical management network. The virtual switch, vSwitch0, which is created by default as a result of installing ESXi, is used for this connection. A single port from each external multi port Network Adapter Card is used to connect Level 2 production workload to FTE. In the first example figure, vmnic4 and vmnic6 are the respective yellow and green FTE connections. Using a single port from each of the external multi port Network Adapter cards as shown above minimizes the scope of loss in the event one of the external Network Adapter Cards should fail. Two additional virtual switches, vSwitch1 and vSwitch2, must be created and configured to enable connectivity from the production workload to the physical FTE network.

The high capacity host shown in the second image is an example of a production host with dual FTE connectivity. In this example, the connectivity to the management network is identical to that shown in the first figure. However, the FTE workload is split between 2 separate connections from the ESXi host to the physical FTE network. This configuration fully utilizes the ports available on the two external multi port Network Adapter Cards. Note that one of the external multi port Network Adapter cards is used for the yellow connection (see vmnic4 and vmnic5 in the second example) while the second external multi port Network Adapter card is used for the green connection (see vmnic6 and vmnic7 in the first example). Four virtual switches, vSwitch1, vSwitch2, vSwitch3, and vSwitch4, must be created and configured to enable connectivity from the production workload to the physical FTE network.



#### Attention

- Follow the instructions in the "Setting Up Networking with vSphere Standard Switches" section of *vSphere Networking*, and the tables below to create and configure vSwitches. Note that vSwitch0 will already exist as a result of ESXi installation and host configuration. Refer to the "Port Group Configuration for Virtual Machines" section of *vSphere Networking* to create or edit a standard vSwitch with a virtual machine port group. To configure the remaining properties, such as speed and duplex, refer to "vSphere Standard Switch Properties" in *vSphere Networking*.

Use the following table to configure the virtual switches in each Level 2 production ESXi host that is deployed with single FTE connectivity as shown in the first figure.

Virtual switch	VMkernel port	Virtual machine port group	Uplink	Speed and duplex value
vSwitch0	Management network name	None	vmnic0 (connected to management physical switch A) vmnic1 (connected to management physical switch B)	1000/Full
vSwitch1	None	FTE Yellow 1	vmnic2 (connected to FTE yellow physical switch)	100/Full
vSwitch2	None	FTE Green 1	vmnic3 (connected to FTE green physical switch)	100/Full

Use the following table to configure the virtual switches in each Level 2 production ESXi host that is deployed with dual FTE connectivity as shown in the second figure above.

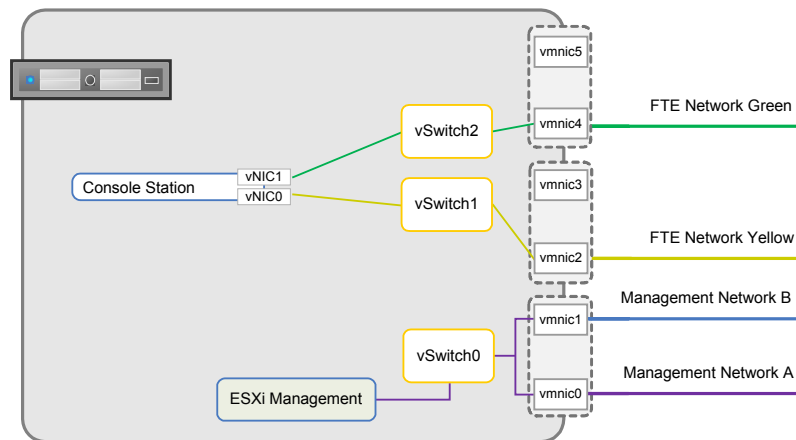
Virtual switch	VMkernel port	Virtual machine port group	Uplink	Speed and duplex value
vSwitch0	Management network name	None	vmnic0 (connected to management physical switch A) vmnic1 (connected to management physical switch B)	1000/Full
vSwitch1	None	FTE Yellow 1	vmnic2 (connected to FTE yellow physical switch)	100/Full
vSwitch2	None	FTE Green 1	vmnic4 (connected to FTE green physical switch)	100/Full

Virtual switch	VMkernel port	Virtual machine port group	Uplink	Speed and duplex value
vSwitch3	None	FTE Yellow 2 Both FTE Yellow 1 and FTE Yellow 2 should be on the same dual NIC.	vmnic3 (connected to FTE yellow physical switch)	100/Full
vSwitch4	None	FTE Green 2 Both FTE Green 1 and FTE Green 2 should be on the same dual NIC.	vmnic5 (connected to FTE green physical switch)	100/Full

**Attention**

- The virtual machine port group is created by default for the management network as a result of the ESXi installation. Honeywell recommends that this port group be removed from the production ESXi host.

**Low capacity hosts**



**Figure 26: Example configuration of an production ESXi host with local storage containing low capacity workloads**

The production host illustrated in the above example uses a NIC allocation scheme for a single virtual machine host. For more information, see the related topics.

**Attention**

- Follow the instructions in the "Setting Up Networking with vSphere Standard Switches" section of *vSphere Networking* and the tables below to create and configure vSwitches. Note that vSwitch0 will already exist as a result of ESXi installation and host configuration. Refer to the "Port Group Configuration for Virtual Machines" section of *vSphere Networking* to create or edit a standard vSwitch with a virtual machine port group. To configure the remaining properties, such as speed and duplex, refer to "vSphere Standard Switch Properties" in *vSphere Networking*.

Use the following table to configure the virtual switches in each Level 2 production ESXi host.

Virtual switch	VMkernel port	Virtual machine port group	Uplink	Speed and duplex value
vSwitch0	Management network name	None	vmnic0 (connected to management physical switch A) vmnic1 (connected to management physical switch B)	1000/Full
vSwitch1	None	FTE Yellow 1	vmnic2 (connected to FTE yellow physical switch)	100/Full

Virtual switch	VMkernel port	Virtual machine port group	Uplink	Speed and duplex value
vSwitch2	None	FTE Green 1	vmnic4 (connected to FTE green physical switch)	100/Full



#### Attention

The virtual machine port group is created by default for the management network as a result of ESXi installation. It is recommended that this port group be removed from the production ESXi host.

#### Related topics

“Network requirements for a DCS architecture” on page 44

## Network configuration for a production host in a SCADA architecture

After you complete the initial network configuration, you need to configure the virtual network for the production host.

### Network configuration for production hosts with local storage

The minimum three ESXi host network configuration for a SCADA architecture using only local ESXi storage. Flex Station and Engineering Station thin clients connect to the production network, while any physical vCenter Client nodes connect to the management network. The backup storage device is for the backup of virtual machines on the ESXi hosts.

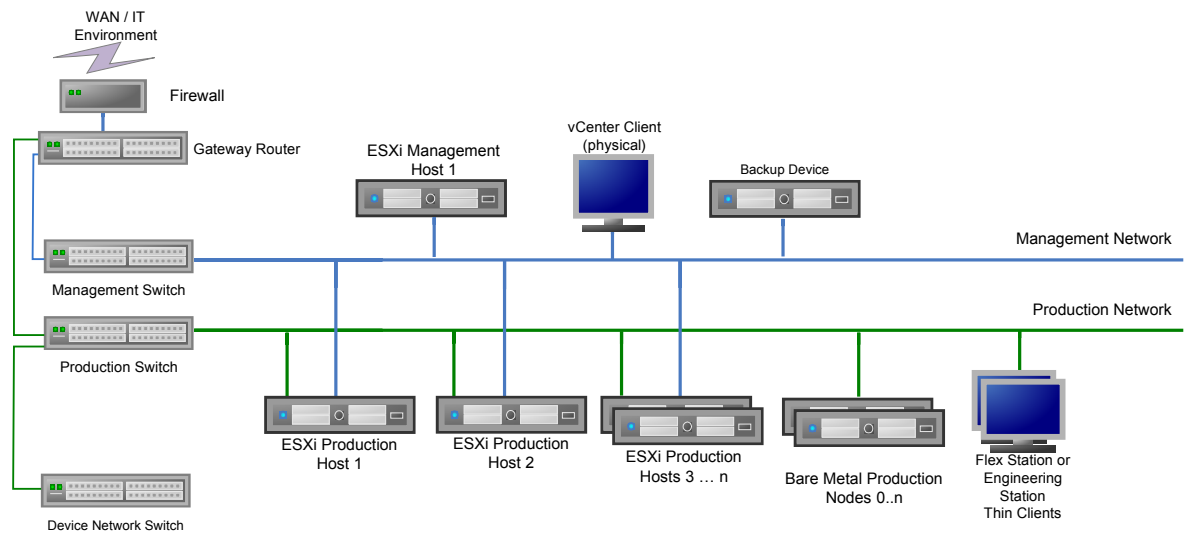


Figure 27: Example topology of a SCADA architecture using local storage on the ESXi hosts

In “Figure 28: Example configuration of an ESXi host with local storage containing production workloads” vmnic2 and vmnic3 have been teamed, and connect a single production vSwitch (vSwitch1) to the physical production network and switch.

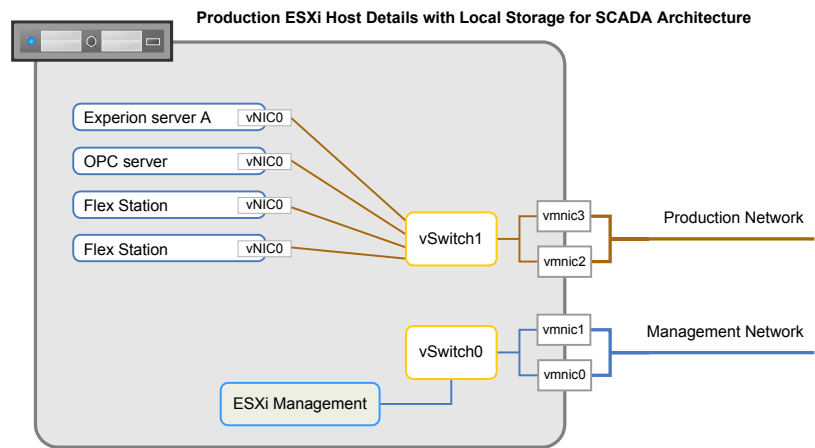


Figure 28: Example configuration of an ESXi host with local storage containing production workloads

In “Figure 29: Example configuration of an ESXi host with local storage containing production workloads and using dual production networks” vmnic2 and vmnic3 connect to separate vSwitches (vSwitch1 and vSwitch2 respectively), which connect to the dual Ethernet production network.

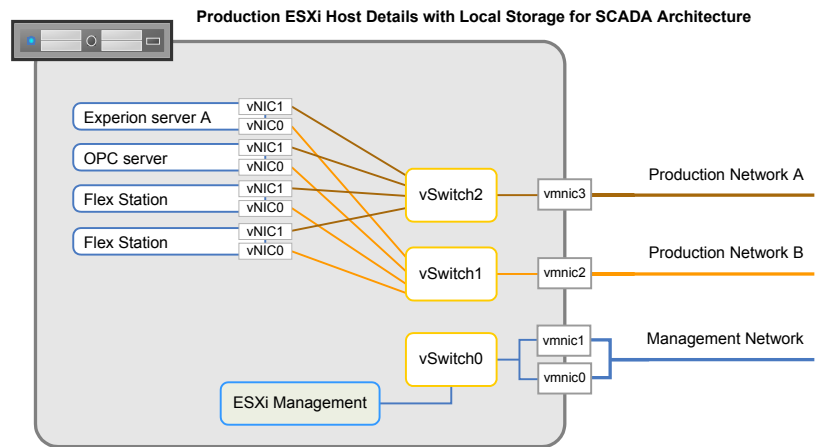
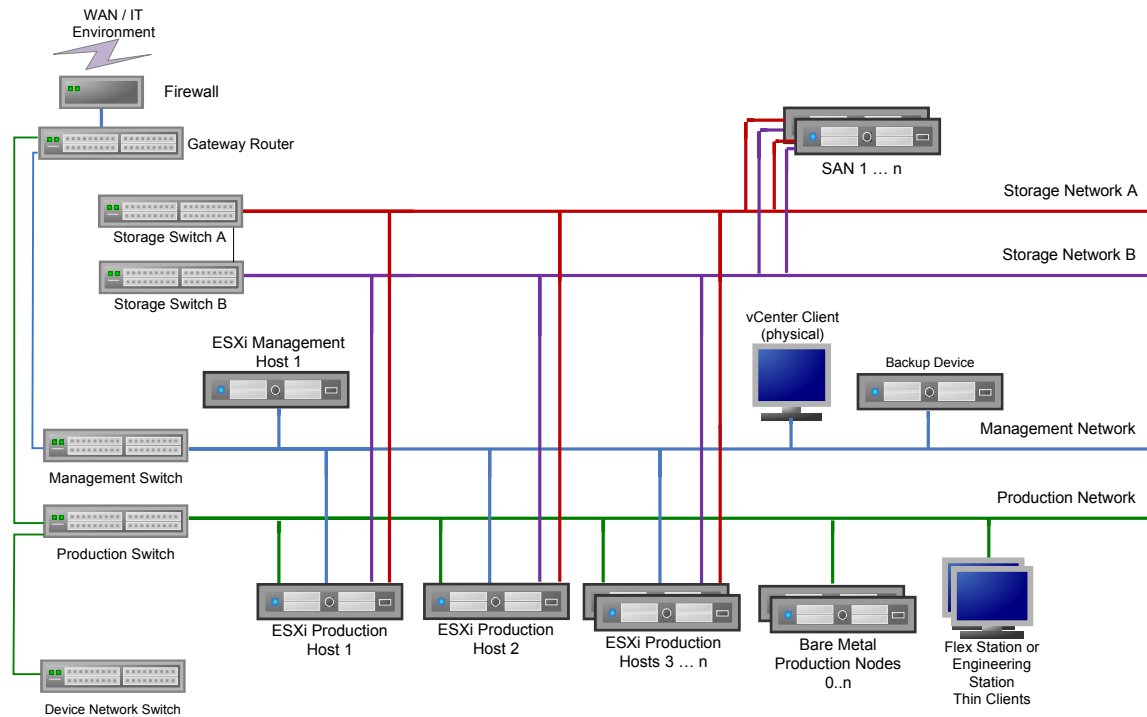


Figure 29: Example configuration of an ESXi host with local storage containing production workloads and using dual production networks

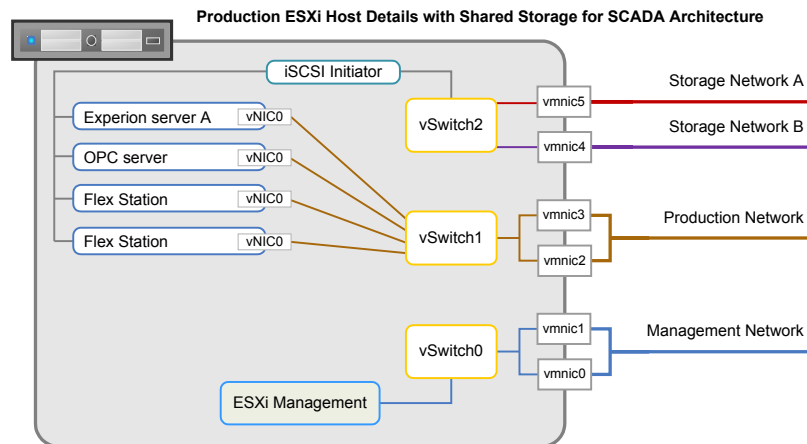
**Network configuration for production hosts with shared storage (using a storage network)**

The minimum three ESXi host network configuration for a SCADA architecture using shared storage. Flex Station and Engineering Station thin clients connect to the production network, while any physical vCenter Client nodes connect to the management network. The backup storage device is for the backup of virtual machines on the ESXi hosts. The storage network connects the ESXi hosts to the storage area network (SAN).



**Figure 30: Example topology of a SCADA architecture using shared storage**

In “Figure 31: Example configuration of an ESXi host using shared storage containing process operational workloads” vmnic2 and vmnic3 have been teamed, and connect a single production vSwitch (vSwitch1) to the physical production network and switch. Virtual machines connect through the iSCSI Initiator to a vSwitch (vSwitch2) to connect to the storage network.



**Figure 31: Example configuration of an ESXi host using shared storage containing process operational workloads**

In “Figure 32: Example configuration of an ESXi host with local storage containing process operational workloads and using dual production networks” vmnic2 and vmnic3 connect to separate vSwitches (vSwitch1 and vSwitch2 respectively), which connect to the dual Ethernet production network. Virtual machines connect through the iSCSI Initiator to a vSwitch (vSwitch2) to connect to the storage network.

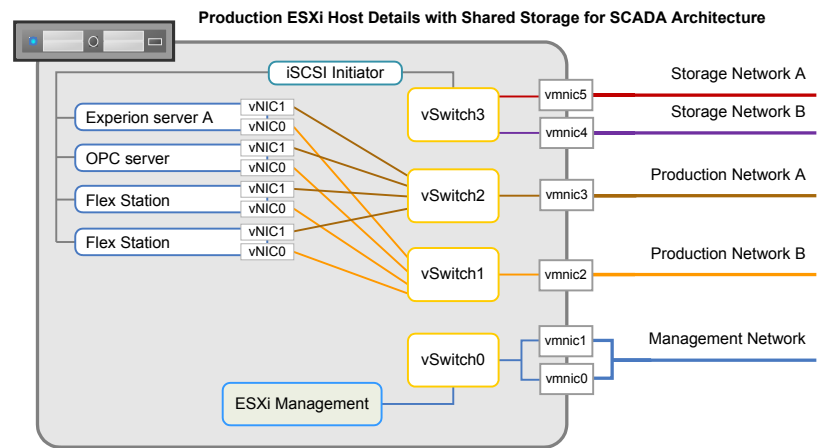



Figure 32: Example configuration of an ESXi host with local storage containing process operational workloads and using dual production networks

Configuring NIC teaming

Configure the NIC teaming settings. A NIC team can share the traffic load between the physical and virtual networks among some or all of the NIC team members, or provide passive failover in the event of a hardware failure or a network outage.

To configure NIC teaming

- 1 On the vSphere Client (within the **Home > Inventory > Inventory** view), locate the ESXi host. Click on the **Configuration** tab, and then under the **Hardware** group, click the **Networking** link.
- 2 Locate the vSwitch0 virtual switch, and then click the associated **Properties** link. The **vSwitch Properties** dialog box appears.
- 3 To construct a NIC team (connecting redundant network adapters to the management network switch), do the following:
  - a Click on the **Network Adapters** tab and then click **Add**. The **Add Adapter Wizard** dialog box appears.
  - b In the **Unclaimed Adapters** group, select the vmnic adapters (NICs) that need to be connected to the vSwitch, and then click **Next**.
-  **Attention**  
If there are already adapters connected to the vSwitch, the selected adapters must belong to the same Layer 2 broadcast domain as the existing adapter.
- c Move the selected vmnic adapter into the **Active Adapters** group using the **Move Up** and **Move Down** buttons.
  - d Click **Next**.
  - e Review the information and then click **Finish**.
- 4 To set the NIC teaming policy exceptions, do the following:
  - a Click on the **Ports** tab, select the **vSwitch** configuration, and then click **Edit**.
  - b Click the **NIC Teaming** tab.
  - c Set the following policy exceptions:

Policy exception name	Value
Load Balancing	Route based on the originating virtual port ID

Policy exception name	Value
Network Failover Detection	Link status only
Notify Switches	Yes
Failback	No

- d Click **OK**.
- 5 Click **Close** to close the **vSwitch Properties** dialog box.

## Configuring the virtual switch port security settings

To protect virtual machines from intrusion, the virtual switch port security settings should be modified from the default values.

### Prerequisites

- *vSphere Networking*.

### To configure the virtual switch port security settings

- Configure the security policy on a virtual switch by following the instructions in the “Edit Security Policy for a vSphere Standard Switch” topic in *vSphere Networking*. Use the following table to identify the policy exception:

Policy exception name	Value
Promiscuous Mode	Reject
MAC Address Changes	Reject
Forged Transmits	Reject

---

## Configuring ESXi host time synchronization

ESXi hosts require time synchronization that is accurate when compared to the time used within the whole infrastructure. Ensure that you have determined the time source for all ESXi hosts and configured the time configuration.

### To configure ESXi host time synchronization

- 1 In the vSphere Client (within Home > Inventory >), choose the **Inventory** view.
- 2 Locate and select the ESXi host that requires time configuration.
- 3 Click the **Configuration** tab.
- 4 Click the **Time Configuration** option.
- 5 At the top right of the page, click **Properties**.  
The **Time Configuration** dialog box appears.
- 6 Click **Options**.  
The **NTP Daemon (ntpd) Options** dialog box appears.
- 7 Click **NTP Settings** and then click **Add**.  
The **Add NTP Server** dialog box appears.
- 8 Type the IP address or host name of the NTP time server and then click **OK**.
- 9 Select the **Restart NTP service to apply changes** check box and then click **OK**.  
This adds the NTP server and restarts the NTPD daemon.  
You should see an event in the vSphere Client recent tasks status bar stating **Update service activation policy**. The **Time Configuration** dialog box appears.
- 10 Click **OK**.  
You should see an event in the vSphere Client recent tasks status bar stating **Update date or time**.

### Results

Within 15 minutes, the ESXi host time should synchronize with the NTP time server.



---

## Adding the ESXi host to the vCenter Server

Add new ESXi hosts to the vCenter Server.

### Prerequisites

- *vCenter Server and Host Management*.
- The Windows hosts file on vCenter Server must be updated to include the ESXi host name resolution (host name or IP address).

### To add an ESXi host to vCenter Server

1. Add the ESXi host to the vCenter Server by following the instructions in the “Add Hosts” topic in the “Organizing Your Inventory” section of *vCenter Server and Host Management*.

---

## Domain name resolution

ESXi hosts need to be manually added to the domain name server (DNS).

The domain name server (DNS) must contain the name of the ESXi host. You must manually add these names to the DNS server, by adding a 'Host A' record to the appropriate Forward Lookup zone.

**Attention**

- The names of virtual machines do *not* need to be manually added to the DNS server.
- 

To verify name resolution:

- Verify that vCenter Server can resolve the host name of each ESXi host in the inventory.
- Verify that each ESXi host in the vCenter Server inventory can resolve the name of the management node where vCenter Server is installed.

---

## Creating and managing virtual machines

You have successfully built your virtual infrastructure, and you are now ready to create and deploy virtual machines to your virtual environment.

For guidance creating, deploying, and managing virtual machines, see the *Software Installation User's Guide*.



# Administering the virtualization environment

## Related topics

“Replicating a virtual machine” on page 150

“Preparing the virtual machine for replication” on page 154

“Preparing the vCenter Server for virtual machine replication” on page 156

*The PowerShell script that is run on the vCenter server controls the core functions of virtual machine replication. This script requires a number of actions to be performed before it can be run.*

“Restoring and recovering a replicated virtual machine” on page 161

“Patching or upgrading the VMware environment” on page 163

“Maintaining hardware devices in a virtualization environment” on page 176

“Monitoring the virtualization environment” on page 178

# Replicating a virtual machine

The implementation of virtual machine replication requires the use of a number of components in the virtual infrastructure. These include:

- Powershell scripts
- vCenter Server and ESXi Hosts
- Custom attributes
- VMware tools

## Powershell scripts

Powershell scripts are used in both the guest OS of the virtual machine that is being replicated and within vCenter Server. These scripts are run from the windows task scheduler daily and control the replication process. The following scripts are available for download from the Honeywell Process Solutions web site and should be used to implement the approach discussed here:

### 1. UpdateStatus.ps1 Powershell script

All virtual machines that need to be replicated require the UpdateStatus.ps1 Powershell script. This script runs once a day and uses the vmtoolsd.exe application (installed with VMware tools) to push four status values to the vCenter server. These status values are:

- Last reboot time
- Last Honeywell update
- Last Microsoft update
- Current date and time

### 2. VMreplicate.ps1 Powershell script

The vCenter Server uses one Powershell script to action the process of replicating virtual machines. This Script uses a CSV file to determine which virtual machines should be replicated and then uses the latest virtual machine status (supplied by the UpdateStatus.ps1 script) to determine when a new clone is required. This script requires Powershell version 2 and PowerCLI supplied by VMware to function.

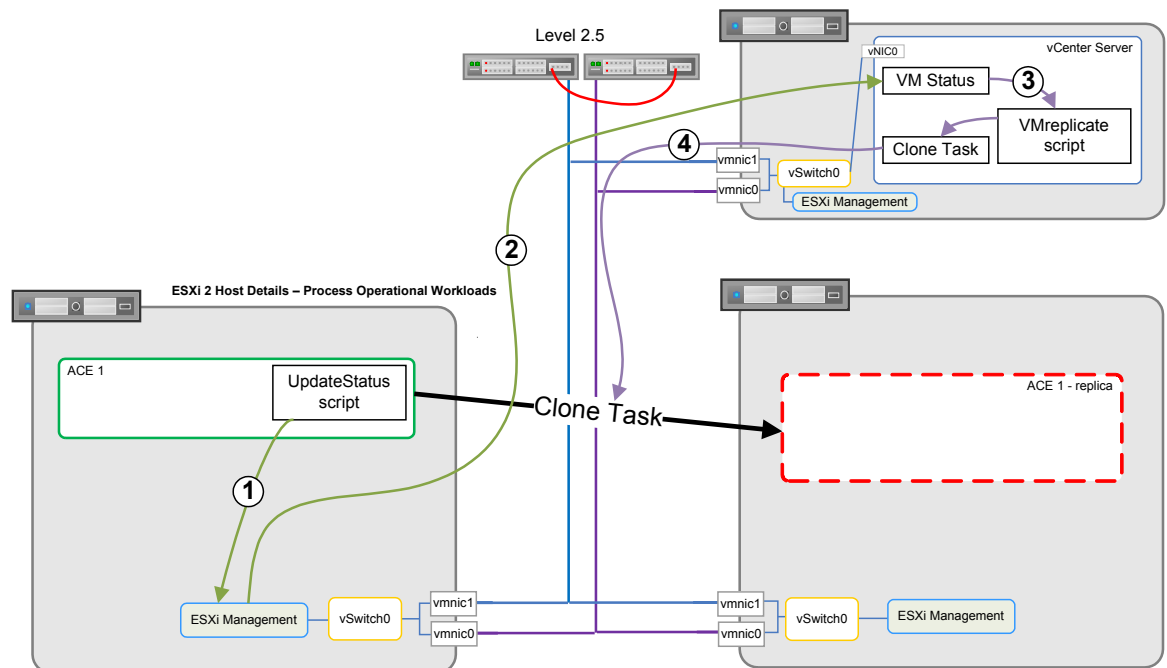


Figure 33: Components and process flow involved in VM replication

The system illustrated above shows the components that are used and the process flow involved when running virtual machine replication. The system illustrated includes 3 ESXi hosts, vCenter Server and the original virtual machine that is configured for replication.

The following list outlines the actions indicated by the numbers on the system illustrated above. Actions 1 and 2 are controlled by the Powershell script that runs on the virtual machine that is being replicated. Actions 3 and 4 are controlled by the Powershell script that runs on the vCenter Server.

1. The Powershell script is run on the virtual machine. This is initiated by the Windows Task Scheduler once a day. It checks the latest values for the last reboot date, last Microsoft update date, latest Honeywell update date and the current date/time. This information is passed into VMware tools.
2. The *vmtoolsd* application pushes the current four status values into the vCenter Server configuration information for that virtual machine. The update process is done using the virtual infrastructure and management network and no direct connection between the virtual machine and vCenter server is required. The VM status is kept in vCenter server for later use.
3. The Powershell script is run on the vCenter server. It is initiated by the Windows Task Scheduler once a day. It retrieves the latest status for the virtual machine. The last recorded status for last reboot date, last Microsoft update date and latest Honeywell update date is retrieved from the vCenter custom annotations. The script then compares the latest values pushed from the virtual machine with the last values.
4. If a difference between the last and latest values is seen, a clone task is started. The clone task is initiated by the vCenter Server and the ESXi Hosts facilitate this task. The custom annotations that are checked next time the script is run are updated with the latest values.

### vCenter Server and ESXi Hosts

The vCenter Server and ESXi Hosts perform the cloning process. The vCenter Server controls the security authentication from the script and is used to retrieve the last and latest virtual machine status dates. The ESXi Hosts facilitate the clone of the virtual machine as initiated by vCenter Server.

### Custom attributes

vSphere custom attributes for virtual machine objects are used to store the last status dates for the replicated virtual machines and indicate the status of the replication process. The following custom attributes are created and used:

- Last Failed Replica: used to record the date and time of a configuration error or clone error. A custom alarm is defined to trigger an alert on the virtual machine whenever this value changes.
- Last Successful Replica: Used to record the date and time of the last successful replication.
- LastHWUpdate: Used to record the date of the latest Honeywell update in the virtual machine. The **vmreplicate.ps1** script compares this value with the new value from the virtual machine to decide if a clone is required.
- LastMsUpdate: Used to record the date of the latest Microsoft update in the virtual machine. The **vmreplicate.ps1** script compares this value with the new value from the virtual machine to decide if a clone is required.
- LastReboot: Used to record the date of the last reboot of the virtual machine. The **vmreplicate.ps1** script compares this value with the new value from the virtual machine to decide if a clone is required.
- Replica Information: Records the status after the latest run of the **vmreplicate.ps1** script. Error messages can be seen here too.

### VMware tools

The VMware tools are used in the virtual machine to push the status information from the virtual machine to the vCenter Server. This is done through the management network and does not require any direct connection from the virtual machine and the vCenter Server.

**Related topics**

“Virtual machine replication pre-requisites” on page 152

*A number of prerequisite configurations and conditions must be met in order to successfully implement virtual machine replication. Ensure all prerequisites are completed.*

“Planning to backup the virtual infrastructure and virtual machines” on page 70

*Plan for the use of Experion Backup and Restore (EBR) to perform backups of the virtual infrastructure and virtual machines.*

“Preparing a vCenter Server” on page 118

*On the management ESXi host, you need to create a virtual machine to host the vCenter Server (and vCenter Update Manager). The vCenter Server contains the required software components for the administration of virtual machines, ESXi hosts, and the virtualization environment. You need to install a vCenter Server to manage the virtual environment.*

**Virtual machine replication pre-requisites**

A number of prerequisite configurations and conditions must be met in order to successfully implement virtual machine replication. Ensure all prerequisites are completed.

**ESXi Host resource requirements**

When considering which ESXi host to replicate a virtual machine (VM) to, you also need to consider the resourcing requirements of this VM. When provisioning that host, also consider the resource requirements of all VMs that the host will contain replicated copies of. This includes the CPU, RAM, disk capacity, disk throughput and network throughput the VMs require.

In addition, do not load the replicated VM into the same resource pool nor the same datastore folder as the master VM.

**Virtual Machine software prerequisites**

The following software needs to be installed on each Virtual Machine that will be replicated

- PowerShell v1 or later – a suitable version will need to be installed on Windows Server 2008, Windows Server 2008 R2 and Windows 7. For earlier versions of Windows this can be downloaded directly from Microsoft.
- VMware Tools – A version compatible with your ESXi hosts.

**vCenter Server software prerequisites**

The following software needs to be installed on the vCenter server that will be coordinating the replicating operations:

- PowerShell v2 – Ensure that PowerShell v2.0 or newer is installed on the vCenter Server. It is installed by default on Server 2008 R2 and installation is required on other operating systems. The installation package is available at the following link: <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20430> To check the installed version, open a PowerShell command prompt and type Get-Host, the PowerShell version will be shown.

**Attention**

- Installation of this package will require a restart

- VMware PowerCLI v5.0.1 – is available from VMware at the following link: <http://www.vmware.com/support/developer/PowerCLI/index.html> Ensure that you choose version 5.0.1 before downloading.

**Replica VM Clone failed alarm**

To ensure that an alarm is raised in vCenter when a clone fails for a replicated VM:



1. Open vSphere Client and connect to your vCenter, then switch to Hosts and Clusters view.
2. Select the top level Datacenter.
3. Select the Alarms tab and click **Definitions**.
4. Right-click in the blank area to the right of the existing definitions and select **New Alarm...**
5. In the Alarm Settings window:
  - a. Click the **General** tab.
  - b. Enter an Alarm Name similar to “Replica Clone Process Failed”. This is the name that will be displayed when the alarm is triggered.
  - c. In the **Monitor** box, ensure Virtual Machines is selected.
  - d. Below the **Monitor** box, ensure **Monitor for specific events occurring on this object** is selected.
  - e. Click the **Triggers** tab.
  - f. Click **Add**.
  - g. In the new row displayed edit the value in the **Event** column to be: **vim.event.CustomFieldValueChangedEvent**. (note this value is case sensitive).
  - h. Click on **Advanced...** in the **Conditions** column.
  - i. In the **Trigger Conditions** window click **Add**.
  - j. In the new row change the **Argument** column value to **name**.
  - k. Change the **Operator** column value to **equal to**.
  - l. Change the **Value** column value to **Last Failed Replica**.
  - m. Click **OK**.
  - n. On the **Alarm Settings dialog** click **OK**.
6. Verify that the new alarm appears in the list.

This alarm will trigger whenever the value of the custom attribute Last Failed Replica is changed.

## Preparing the virtual machine for replication

The virtual machine that is to be replicated requires a once-off configuration to enable a PowerShell script to periodically pass information to the virtual infrastructure. This information includes:

- Last reboot date
- Last Microsoft update date
- Last Honeywell update date
- Last successful completion of the script

### Creating and saving the PowerShell script

- 1 Download the PowerShell script from the Honeywell Process Solutions website.  
The PowerShell script is required to run on the virtual machine to push the most recent status information to the virtual infrastructure. The PowerShell script file is called `updateStatus.ps1` and is supplied with a `.txt` extension.
- 2 Change the extension for the PowerShell script from `.txt` to `.ps1` so that the script will run in PowerShell.
- 3 Save the PowerShell script in the `C:\Program Files\Honeywell\Experion PKS\PS` (or `C:\Program Files (x86)\Honeywell\ExperionPKS\PS` on 64 bit virtual machines) folder on each virtual machine that needs to be replicated.  
You might need to create this folder manually.
- 4 Ensure the following folder exists `C:\ProgramData\Honeywell\Experion PKS\PS` as this is the destination of the PowerShell script log file.

### Create the windows user to run the script

- 1 In the virtual machine guest operating system click **Start**, then click **Administrative Tools**, and **Computer Management**.
- 2 Expand **Local Users and Groups** and click **Users**.
- 3 Create a new User called **ReplicationUser** and ensure that the **Password never expires** option is selected. It is important to apply a very strong password to this user as it will not expire.
- 4 Select the properties for the new user and ensure that the user is a member of the **Backup Operators**, **Local View Only Users** and **Users** groups for the local machine.  
The *Local View Only Users* group will only exist on an Experion node. If replication is being configured for a non-Experion node, this user will require full control of the `C:\ProgramData\Honeywell\Experion PKS\PS` folder so that the log file can be created and appended.
- 5 Click **Start** then click **Administrative Tools** and **Local Security Policy**.
- 6 Expand **Local Policies** and click **User Rights Assignment**.
- 7 Ensure that the new user *ReplicationUser* is added to the **Deny log on locally** and the **Deny access to this computer from the network** policies.

### Enabling the PowerShell script

- 1 Open an instance of PowerShell as an Administrator (with elevated privileges) and then type **set-executionPolicy RemoteSigned**  
A confirmation prompt may be displayed.
- 2 Type **Y** and then click **Enter** to confirm this action.

### Scheduling the PowerShell script

- 1 From the Control Panel, click **Administrative Tools** and then **Computer Management**.
- 2 From the Computer Management application in the left hand pane click **Computer Management (Local)**, then **System Tools**, then **Task Scheduler**, then **Task Scheduler Library**.

- 3 In the right-hand pane under **Actions** click **Create Basic Task...**  
The **Create Basic Task** wizard is displayed.
- 4 Enter a name similar to Replicate VM Trigger and click **Next**.
- 5 Select **Daily** and then click **Next**.
- 6 Enter the required time that this task will run each day and then click **Next**.
- 7 Select **Start a Program** and then click **Next**.
- 8 Click **Browse...** and locate the PowerShell executable. Typically this would be `C:\windows\system32\windowspowershell\v1.0\powershell.exe`.
- 9 Click **Open**.
- 10 In the **Add arguments** entry, add in the path to the UpdateStatus.ps1 script.  
The & is required at the beginning of the argument. for example, & 'C:\Program Files\Honeywell\Experion PKS\PS\UpdateStatus.ps1'.  
A summary of the new schedule task is displayed.
- 11 Check the details and then click **Finish**.
- 12 Ensure the new schedule is shown in the library.
- 13 Right-click on the new schedule item and click **Properties**.
- 14 On the Properties dialog:
  - a Change the Security option to **Run whether user is logged on or not**.
  - b Click **OK**.
- 15 When prompted, enter the ReplicationUser and password to run the script.  
The script will run daily at the specified time.

#### Testing the PowerShell script

- 1 From the Control Panel, click **Administrative Tools**, and then **Computer Management**.
- 2 From the Computer Management application in the left hand pane click **Computer Management (Local)**, then **System Tools**, then **Task Scheduler**, then **Task Scheduler Library**.
- 3 Select the task that schedules the PowerShell script to run.
- 4 In the right-hand pane under **Actions** click **Run**.
- 5 Check the `updateStatus.log` file located in folder location `C:\ProgramData\Honeywell\Experion PKS\PS` for any logs entries starting with ERROR.  
Errors may be seen in the PowerShell script log file if the virtual machine has not been installing Windows updates. It is important to apply Windows updates to the virtual machine to ensure that the script will run successfully.

#### Configuring the virtual network adapter settings

- 1 Open vSphere client and connect to vCenter.
- 2 Navigate to the **Hosts and clusters** view of the infrastructure.
- 3 Select the virtual machine that is to be replicated to edit its settings.
- 4 Select the network adaptors and clear the **Connect at power on check box** (do this step for both the yellow FTE and green FTE adapters).
- 5 Click **OK** to save the changes.  
The change to this setting will ensure that no duplicate IP address or duplicate FTE device id will be seen on the process control network.  
Every virtual machine that has this change applied will require manual intervention whenever the ESXi Host is restarted and the automatic startup procedure is run. This is because the virtual machine will start but the virtual network will not be connected until the **Connected** check box is checked in the virtual machine settings for each network adapter.

## Preparing the vCenter Server for virtual machine replication

The PowerShell script that is run on the vCenter server controls the core functions of virtual machine replication. This script requires a number of actions to be performed before it can be run.

Each ESXi Host that is used as a destination host requires a resource pool to be created. This resource pool will be referenced in the PowerShell CSV file and is the pool where the replica virtual machines are created when the PowerShell script runs. Reservations and limits are not required for this resource pool as the virtual machines will only be powered-on in emergency situations.



### Attention

It is important that the name of the resource pool on each ESXi host is unique. Identically named resource pools on the same host will cause the PowerShell script to fail. An example name for this resource pool is "ReplicaVMs" and best practice is to use the same or similar name resource pool in each ESXi host.

Each vSphere Datacenter (as viewed in the VMs and Templates view in the vSphere Client) requires a folder. You need to create this folder in the same datacenter as the virtual machines that are going to be replicated. It will display as a blue folder. It is the destination folder for all replicated virtual machines when the VMs and Templates view is used to navigate the virtual infrastructure. An example name for this folder is "Replicas".

### To create and prepare the windows user account to run the PowerShell script

- 1 In the vCenter Server guest operating system click **Start** and then click **Administrative Tools** then **Computer Management**.
- 2 Expand **Local Users and Groups** and click **Users**.
- 3 Create a new User called **ReplicationUser** and check the **Password never expires** check box.  
It is important to apply a very strong password to this user as it will not expire.
- 4 Select the properties for the new user and ensure that the user is a member of the Backup Operators and Users groups for the local machine.  
The folder that is required to hold the PowerShell script credentials file and log file needs to be created and have permissions adjusted. The adjustment of the folder permissions is required so that the PowerShell script will be able to write to the files in the folder.

### To create the folder for the PowerShell script and adjust the permissions

- 1 Use Windows Explorer to create the following folder *C:\ProgramData\Honeywell\Experion PKS\PS*.
- 2 Navigate to the *C:\ProgramData\Honeywell\Experion PKS* folder and right click on the *PS* folder and click **Properties**.
- 3 Select the **Security** tab and then click **Edit**.
- 4 Click **Add** and add the *ReplicationUser* created earlier to the folder.
- 5 Click **OK**.
- 6 Select the *ReplicationUser* from the list of users and groups and ensure that the user has full control of the folder. If required check the **Full Control** check box.
- 7 Click **OK**.

### To create the role for replication

- 1 Open the vSphere client and navigate to the **Home** menu.
- 2 Click the **Roles** icon and then click **Add Role**.
- 3 Enter the name **Replication** and then select the following privileges:
  - a Datastore.Allocate Space
  - b Global.Manage custom attributes
  - c Global.Set custom attribute

- d Network.Assign Network
  - e Permissions.Modify permission
  - f Resource.Assign virtual machine to resource pool
  - g Virtual machine.Configuration.Add existing disk
  - h Virtual machine.Configuration.Add new disk
  - i Virtual machine.Configuration.Raw device
  - j Virtual machine.Configuration.Rename
  - k Virtual machine.Inventory.Create from existing
  - l Virtual machine.Inventory.Create new
  - m Virtual machine.Inventory.Remove
  - n Virtual machine.Provisioning.Clone virtual machine
  - o Virtual machine.Provisioning.Customize
  - p Virtual machine.Provisioning.Deploy template
- 4 Click **OK**.

#### To add a user role to the vSphere datacenter

- 1 Open the vSphere client and navigate to the **Hosts and Cluster** view.
- 2 Select the top level datacenter and then the **Permissions** tab.
- 3 Right-click in the white area and select **Add Permission**.  
The **Assign Permissions** dialog is displayed.
- 4 Click **Add**  
The **Select Users and Groups** dialog is displayed.
- 5 Click the Add button and will appear.
- 6 Select the user account that will be used for virtual machine replication script connection to vCenter
- 7 Click **Add** and then **OK** to close the dialog.
- 8 Select the Replication role created earlier from the drop down box under **Assign Role**.
- 9 Ensure that **Propagate to child objects** is checked and click **OK**.  
A new user with role replication will be created.

#### To create the PowerCLI credentials file

- 1 Open a PowerCLI command prompt as the ReplicationUser. This is done by holding down the shift key and right-clicking on **Start**, then selecting **Run as a different user**.
- 2 When prompted, enter the ReplicationUser and password and this will open the PowerCLI window as this user.
- 3 Use the following command to create the credential store XML file:.  

```
New-VICredentialStoreItem -Host <vCenter server name/IP> -User ReplicationUser -Password <Password> -File <Location where you want to save the file along with file name>
```

Example usage: `New-VICredentialStoreItem -Host 10.2.80.112 -User ReplicationUser -Password aLongSecurePassword123! -File "C:\ProgramData\Honeywell\Experion PKS\PS\creds.crd"`



#### Attention

The credentials file can only contain one user. If multiple users are added to the file the PowerShell script will not work correctly. To ensure that the credentials file only has one user, use the `Get-VICredentialStoreItem -File "C:\ProgramData\Honeywell\Experion PKS\PS\creds.crd"` command from the PowerCLI prompt and ensure only one user appears in the output.

- 4 You can now refer to the credentials file in the main PowerShell script.

**To create the VM replica CSV file**

- 1 Create a CSV file in Notepad or Microsoft Excel to be used by the PowerShell script running in the vCenter Server. This file will contain all the site specific virtual machine and infrastructure information so that the script knows what is required. An example CSV file is available from the Honeywell Process Solutions web site.
- 2 Format the CSV file as a table and include a header or first line to define the fields in the table. The header or first line must contain: **SourceHost**, **SourceVMName**, **DestHost**, **DestDataStore**, **DestResourcePool**, **DestFolder**.
- 3 In the rows after the header, define the information for each virtual machine, as shown in the following table:

Configuration Item	Description
<b>SourceHost</b>	The ESXi host running the virtual machine that needs to be replicated. This is the ESXi Host name exactly as seen in vSphere Client.
<b>SourceVMName</b>	The virtual machine that needs to be replicated. This is the virtual machine name exactly as seen in vSphere Client.
<b>DestHost</b>	The ESXi host that will receive the replica virtual machine clone. This is the ESXi Host name exactly as seen in vSphere Client.
<b>DestDataStore</b>	The Datastore on the ESXi host that will receive the replica virtual machine clone. This is the Destination Datastore Name exactly as seen in vSphere Client.
<b>DestResourcePool</b>	The Resource Pool on the ESXi host that will receive the replica virtual machine clone. This is a resource pool on the destination ESXi host and must be unique on the ESXi host.
<b>DestFolder</b>	The Folder in the Datacenter that will receive the replica virtual machine clone.. This is a folder created in the VMs and Templates view in vSphere Client and spans the entire Datacenter

- 4 Save the CSV file to the `C:\ProgramData\Honeywell\Experion PKS\PS` folder on the vCenter server.

**Creating and saving the PowerShell script**

- 1 Download the PowerShell script from the Honeywell Process Solutions web site.  
The PowerShell script is required to run on the virtual machine to push the most recent status information to the virtual infrastructure. The PowerShell script file is called `vmreplicate.ps1` and is supplied with a `.txt` extension.
- 2 Change the extension for the PowerShell script from `.txt` to **.ps1** so that the script will run in PowerShell.
- 3 Save the PowerShell script in the `C:\Program Files\Honeywell\Experion PKS\PS` on the vCenter Server.  
You might need to create this folder manually.
- 4 Use a text editor to customize the script for your environment by editing the following variables at the beginning of the script:
  - a Edit the name and folder path of the credentials file that you are using, for example, `$fileCreds = "C:\ProgramData\Honeywell\Experion PKS\PS\creds.crd"`
  - b Edit the name and folder path of the CSV file that holds all the virtual machine information for your system, for example, `$fileCSV = "C:\ProgramData\Honeywell\Experion PKS\PS\vmreplicas.csv"`
  - c Edit the value of `$nAutoReplicatedays`. This value sets the period for an automatic update of the replica virtual machine in number of days. A value of zero will disable this function.
- 5 Save the script.

**Enabling the PowerShell script**

- 1 Open an instance of PowerShell as an Administrator (with elevated privileges) and then type **Set-ExecutionPolicy RemoteSigned**  
A confirmation prompt may be displayed.

- 2 Type **Y** and then click **Enter** to confirm this action.

### Scheduling the PowerShell script

- 1 From the Control Panel, click **Administrative Tools** and then **Computer Management**.
- 2 From the Computer Management application in the left hand pane click **Computer Management (Local)**, then **System Tools**, then **Task Scheduler**, then **Task Scheduler Library**.
- 3 In the right-hand pane under **Actions** click **Create Basic Task...**  
The **Create Basic Task** wizard is displayed.
- 4 Enter a name similar to Replicate VM Trigger and click **Next**.
- 5 Select **Daily** and then click **Next**.
- 6 Enter the required time that this task will run each day and then click **Next**.
- 7 Select **Start a Program** and then click **Next**.
- 8 Click **Browse...** and locate the PowerShell executable. Typically this would be *C:\windows\system32\windowsPowerShell\v1.0\powershell.exe*.
- 9 Click **Open**.
- 10 In the **Add arguments** entry, add in the path to the UpdateStatus.ps1 script.  
The & is required at the beginning of the argument. for example, & 'C:\Program Files\Honeywell\Experion PKS\PS\VMReplicate.ps1'.  
A summary of the new schedule task is displayed.
- 11 Check the details and then click **Finish**.
- 12 Ensure the new schedule is shown in the library.
- 13 Right-click on the new schedule item and click **Properties**.
- 14 On the Properties dialog:
  - a Change the Security option to **Run whether user is logged on or not**.
  - b Click **OK**.
- 15 When prompted, enter the ReplicationUser and password to run the script.  
The script will run daily at the specified time.

### Testing the PowerShell script

- 1 From the Control Panel, click **Administrative Tools**, and then **Computer Management**.
- 2 From the Computer Management application in the left hand pane click **Computer Management (Local)**, then **System Tools**, then **Task Scheduler**, then **Task Scheduler Library**.
- 3 Select the task that schedules the PowerShell script to run.
- 4 In the right-hand pane under **Actions** click **Run**.
- 5 Check the *VMReplicate.log* file located in folder location *C:\ProgramData\Honeywell\Experion PKS\PS* for any logs entries starting with ERROR.  
Errors may be seen in the PowerShell script log file if the virtual machine has not been installing Windows updates. It is important to apply Windows updates to the virtual machine to ensure that the script will run successfully.

### Disabling vDR backup on replica virtual machines

- 1 Open the VMware Data Recovery plugin in vSphere and navigate to the **Backup** tab..
- 2 Edit each Backup job shown and view the **Virtual Machines** option for each backup job.
- 3 Ensure that the **Resource pool** on each ESXi host that was created as the destination for the replica virtual machines is not checked in each backup job.

**Adding additional security for the ReplicationUser**

- 1 Click **Start**, then **Administrative Tools**, and then **Security Policy**.
- 2 Expand **Local Policies** then click **User Rights Assignment**.
- 3 Ensure that the local windows user **replicationUser** is added to the **Deny log on locally** and **Deny access to this computer from the network** policies.

This change will need to be reversed if a new credentials file needs to be created as this change will not allow the PowerCLI prompt to be opened as the *ReplicationUser*.



## Restoring and recovering a replicated virtual machine

In the event of an ESXi Host failure the clone of any replicated virtual machine can be powered on and run in place of the original. This will allow for the functionality of the original virtual machine to be replaced by the clone while hardware repairs or replacement is undertaken. The following failure scenarios outline where replicated virtual machines can be used:

- Unrecoverable failure of ESXi Host Hardware where no replacement is available within 1 hour
- Failure of ESXi Host hardware where recovery will take greater than 1 hour.

It is important to determine the length of time that the ESXi host will be in a failed state. If the downtime is estimated to be more than 1 hour and a replacement ESXi host is not immediately available, the replicated virtual machine(s) need to be used to replace the original.

### Starting replicated machines

- 1 Run the vSphere Client and connect to vCenter.
- 2 Find the replicated virtual machine and click **Power-on**.
- 3 After the virtual machine has started, open the direct console using vSphere Client or a remote desktop connection and login to the guest operating system. Re-join the virtual machine to the process control domain to re-establish a trust relationship and restart the virtual machine.
- 4 If your replicated virtual machine is an ACE, login to the Experion engineering station for your system and use control builder to load the latest checkpoint. Start your control strategy if required.

The system is now running in a “replicated” state, where the ESXi Host that the original virtual machines had previously run has failed and the replicated virtual machines are now running on a different ESXi host. In an Experion system this model would typically be used for ACE virtual machines. It is important to ensure that the ESXi hosts that run the cloned ACE are provisioned with enough resources to run the “replicated” workloads.

All Experion workloads that are inherently redundant that were running on the failed ESXi host will also be running in a degraded state, as only one half of the redundant pair will be running.



#### Attention

To ensure that any additional hardware failures do not affect the process control system, only run the system in the “replicated” state for as short a time as possible.

### Reconnecting a repaired ESXi host

- 1 Repair the failed ESXi Host.
- 2 Power-on the ESXi Host.
- 3 Open vSphere client and connect to vCenter.
- 4 Allow all virtual machines to automatically start on the repaired ESXi host.
- 5 Ensure that all virtual machine with a current running replica have started successfully and that the virtual network to each is disconnected.
- 6 Ensure that all virtual machines that do not have a running “replicated” clone are operating normally. This includes synchronizing Experion servers. For each replicated virtual machine:
  - a Perform a checkpoint on any ACE virtual workload that is currently running on a replica virtual machine and ensure that the checkpoint is completed.
  - b Power off the running replica virtual machine.
  - c Use the virtual machine settings to connect the virtual network of the original virtual machine.
  - d Re-join the process control domain from the original virtual machine to re-establish a trust relationship and then restart.
  - e If the virtual machine is an ACE, load the latest checkpoint from an Experion engineering station and control builder.

**Attention**

Multiple checkpoint restore requests from the same engineering station occur one at a time and may take longer than expected. Requesting one checkpoint restore from multiple engineering stations may speed up the restore process.

The Experion System should now be running normally as before the ESXi Host failure.

**Reconnecting a replaced ESXi host**

- 1 When the failed ESXi host is replaced or the repair is completed but disk data is lost, you will need to:
  - a Perform a clean installation of the ESXi hypervisor on the ESXi host
  - b Restore the original virtual machine workload from the latest vDR backup.
- 2 Replace ESXi host hardware.
- 3 Install ESXi software and configure ESXi. Refer to the “Preparing a production ESXi host” section in the *Experion Virtualization Planning and Implementation Guide*.
- 4 Reconnect the ESXi host in vCenter. This will require acknowledgement of a new certificate for the ESXi host.
- 5 Restore all virtual machines to the replaced ESXi host using the latest vDR backup.
- 6 Start all virtual machines that do not have a running “replicated” clone and ensure that each operates normally. This includes establishing domain trusts and synchronizing Experion servers.

The Experion System should now be running normally as before the ESXi Host failure.
- 7 For each replicated virtual machine:
  - a Perform a checkpoint on any ACE virtual workload that will be affected and ensure that the checkpoint is completed.
  - b Power off the running clone virtual machine.
  - c Power on the restored original virtual machine.
  - d Use the virtual machine settings to connect the virtual network of the virtual machine.
  - e Re-join the process control domain from the original virtual machine to re-establish a trust relationship and then restart.
  - f If the virtual machine is an ACE, load the latest checkpoint from an Experion engineering station and control builder.

**Attention**

Multiple checkpoint restore requests from the same engineering station occur one at a time and may take longer than expected. Requesting one checkpoint restore from multiple engineering stations may speed up the restore process.

The Experion System should now be running normally as before the ESXi Host failure.

## Patching or upgrading the VMware environment

The virtual environment is made up of the following components vSphere Client, vCenter Server, vCenter Update Manager, ESXi host, virtual machine hardware, VMware Tools, and VMware Data Recovery (vDR).

Patching or upgrading can affect one or all of these components. It is important to update each component in the proper order to maintain communication and to ensure that data is not lost. Detailed instructions for performing a upgrade is provided in *VMware upgrade*. Patches typically apply to individual components. However, ESXi host patches can affect a virtual machines's virtual hardware and/or VMware Tools. The "Remediating vSphere objects" section in *Installing and Administering VMware vSphere Update Manager* recommends upgrading VMware Tools before upgrading virtual hardware.

Honeywell recommends using vSphere Update Manager to administer and automate the application of patches and upgrades to the VMware environment, when possible.

Update Manager Client has two views available through vSphere client. The *Administration view* and the *Compliance view*. For more information about how to access these view, see the "Update Manager Client Overview" section in *Installing and Administering VMware vSphere Update Manager*.

The *Update Manager Client Administration view* provides the interface for configuring the Update Manager, viewing Update Manager events, creating/modifying baselines and baseline groups, for importing patches/updates into the patch repository, and for importing upgrades into the upgrade release repository. Using baselines and baseline groups, you can organize patches from the patch repository into a Honeywell approved set for deployment/remediation.

The *Update Manager Compliance view* provides the interface for associating baselines (the desired set of patches) and baseline groups with target objects, such as hosts, virtual machines, virtual appliances, or containers. A container has one or more hosts, virtual machines/appliances. The Compliance view provides the interface for scanning the target objects to determine if they contain the patches defined in the attached baseline or baseline group.

Target objects containing the patches are considered to be in compliance with the baseline or baseline group. The compliance status is also reported in the compliance view. A status of *in compliance* is green, while a status of *non-compliance* is red. If the object is not in compliance with the attached baseline or baseline group the Compliance view also provides the interface for deploying/remediating the patches to the target object. If the target is an ESXi host, the compliance view provides an additional optional interface for staging (copying) the patch to the target host in preparation for remediation. The compliance view provides the interface for initiating the deployment/remediation of the patch to the target object. Details on these topics can be found in *Installing and Administering VMware vSphere Update Manager*.



### Attention

If vCenter Server or Update Manager reside on the local storage of an ESXi host, Update Manager cannot be used to deploy/remediate patches to that ESXi host. An ESXi must be put into maintenance mode to remediate patches. Maintenance mode requires all local storage virtual machines to be shutdown. A manual procedure is used to deploy/remediate patches or upgrades to this ESXi host.

### Prerequisites

- *Installing and Administering VMware vSphere Update Manager*, to understand the patching process.
- *vSphere Command-Line Interface Installation and Scripting Guide*, for installing the Command-Line Interface (CLI).
- *vSphere Upgrade*
- A computer that has access to the Internet for downloading updates and patches.
- Update Manager is installed on the vCenter Server and the Update Manager plug-in installed on the vSphere Client node.
- The Command-Line Interface (CLI) is installed on vSphere client node.
- You must have the *Remediate to Apply Patches*, *Extensions*, and *Upgrades* privileges associated with your login to remediate vSphere objects.

- You know the vSphere product edition and version that is installed.
- You have a predefined procedure defining the specific order for shutting down and restarting virtual machines, virtual appliances, and ESXi hosts to support a running process.

#### To patch or upgrade the VMware environment

1. Use the Update Manager air-gap deployment model but do not use the Update Manager Download Service to retrieve updates from VMware. Honeywell evaluates VMware updates and posts a list of qualified and approved updates on the Honeywell Process Solutions web site.
2. Download the approved updates directly from VMware download site. See the “Update Manager Deployment Models” section in *Installing and Administering VMware vSphere Update Manager* for guidance on how to set up the air-gap deployment model.
3. Install the Update Manager and its database on the same virtual machine as the vCenter Server. See the “Best Practices and Recommendations for Update Manager Environment” topic in *Installing and Administering VMware vSphere Update Manager*.
4. Use vCenter Update Manager to:
  - a. Import patches or upgrades.
  - b. Manage baselines and baseline groups to contain the desired patches.
  - c. Associate baselines and baseline groups to target objects.
  - d. Scan objects for compliance with the baseline.
  - e. Apply patches to ESXi hosts.
  - f. Upgrade ESXi host to new releases.
  - g. Upgrade VMware Tools within virtual machines.
  - h. Upgrade virtual machine hardware versions.
  - i. Upgrade virtual appliances.
  - j. Scan objects to verify target objects are in compliance with the attached baselines.
5. Use a manual procedure to apply patches to ESXi hosts that contain Update Manager and vCenter Server on local storage.
6. Use Honeywell documented procedures to:
  - a. Apply Experion patches to virtual machines.
  - b. Apply Microsoft patches or security updates to virtual machines.

#### Related topics

- “Downloading the patches or upgrades” on page 164
- “Importing the patches or upgrades into Update Manager” on page 165
- “About baseline and compliance views” on page 166
- “Remediating patches and upgrades” on page 166
- “Remediating target objects using Update Manager” on page 168
- “Remediating target objects manually” on page 169
- “Upgrading Virtual Hardware and VMware tools versions” on page 172
- “Upgrading virtual infrastructure software” on page 173

## Downloading the patches or upgrades

You need to identify and evaluate the VMware patches to be downloaded from the Honeywell Process Solutions website.

VMware upgrades supported by Honeywell can be found in the *HPS Virtualization Specification*.

**Prerequisites**

- You need to complete this task on a computer with access to the Internet.
- You need a Honeywell Online Support account.

**To identify the required patches from Online Support**

- 1 Logon to the Honeywell Online Support web site <http://www.honeywellprocess.com/>.
- 2 Click the **Support** tab.
- 3 Type **vmware update** in the **Search** field, and press ENTER.  
The Honeywell-qualified VMware updates are listed.
- 4 Review the updates and decide which ones are appropriate for your environment.

**To download patches from VMware**

- 1 The VMware patch release ID on the **VMware update summary** page is a link to the consolidated patch .zip file.
- 2 Click the link and follow the instructions to download the consolidated patch package.
- 3 Copy or move the consolidated patch .zip file to a location or media that can be accessed by the vSphere Client.

**To download upgrades from VMware**

- 1 Connect to VMware web site <http://vmware.com/download/>.
- 2 In the **Product Index**, click **VMware vSphere *n*** (where *n* is the vSphere release number, such as 4 or 5).
- 3 Based on your license, find the required VMware ESXi version.
- 4 Click **Download** to download the upgrade.

**Importing the patches or upgrades into Update Manager**

Once you have downloaded the required patches or upgrades from the VMware web site, you need to load these patches or upgrades into Update Manager.

**Prerequisites**

- *Installing and Administering VMware vSphere Update Manager*
- The patch must be in the zip file format.
- You import patches and upgrades from the Update Manager Client *Admin* view.

**Patches or updates**

1. To import patches or updates, see *Installing and Administering VMware vSphere Update Manager*.

**Attention**

- Patches can also be imported using the Import Patches link in the Patch Repository tab.

**Host upgrades**

1. To import ESXi host upgrades, see *Installing and Administering VMware vSphere Update Manager*.

**Attention**

- It is important to ensure that a host upgrade is only performed within the context of a full system upgrade. If an ESXi host is upgraded to a version or release newer than the vCenter Server, the ESXi host will not connect to vCenter Server.

## About baseline and compliance views

Update Manager Client has two views available through vSphere client. The *Administration view* and the *Compliance view*. For more information on how to access these views, see *Installing and Administering VMware vSphere Update Manager*.

### Administration view

The Update Manager Client *Administration view* provides an interface for creating editing or deleting baselines and baseline groups. Using baselines and baseline groups you can organize patches from the patch repository into the Honeywell approved set for deployment/remediation. Update Manager also comes with built-in (default) baselines which automatically include updates downloaded from VMware. However, the default baselines cannot be edited. To exclude one or more of the downloaded patches requires you to create a new baseline. For information about the default baselines and how to create and manage baselines and baseline groups see *Installing and Administering VMware vSphere Update Manager*.

To review the patches assigned to a baseline:

1. From the Admin view in the Update Manager Client, click the **Baselines and Groups** tab.
2. Click **Hosts or VMs/VAs**.
3. Select the number in the content column in the list of baselines.

A list of assigned patches appears.

Baselines and baseline groups are used to define a set of patches, updates, or upgrades. Baseline groups allow patch and upgrade baselines to be remediated together.

### Compliance view

The Update Manager Client *Compliance view* allows a user to specify the hosts, virtual machines, and virtual appliances that will be evaluated against a baseline or baseline group for compliance. The compliance view provides a status of the compliance scan/evaluation. A *non-compliance* status identifies the objects needing to be updated/remediated with the attached baseline. The compliance view also provides the interface for a user to initiate the remediation process for the object.

The Update Manager Client Compliance view provides an interface for:

- Attaching baselines or baseline groups to target objects or target containers. For more information, see *Installing and Administering VMware vSphere Update Manager*.
- Scanning to determine if target objects are in compliance (contains all the patches) defined in the attached baselines or baseline group. For more information, see *Installing and Administering VMware vSphere Update Manager*.
- Staging copies of the patch to the target objects in preparation for remediation. Doing this can reduce the time an ESXi host needs to be in maintenance mode. For more information, see *Installing and Administering VMware vSphere Update Manager*.
- Remediating baselines or baseline groups to target objects. For more information, see *Installing and Administering VMware vSphere Update Manager*.



#### Attention

Honeywell recommends initiating remediation on individual objects rather than initiating remediation on object container. This is so the order of shutting down and restarting virtual machines and ESXi hosts is done in a predetermined order.

## Remediating patches and upgrades

Honeywell recommends using Update Manager for determining patch and upgrade compliance and for remediation of all hosts, virtual machines and virtual appliances when possible.

A manual procedure is required to remediate an ESXi host with patches and upgrades if that ESXi host has vCenter Server or Update Manager hosted on its local storage. This procedure requires the Command-Line Interface (CLI) to be installed on the client node.

Additional consideration is required when remediating an ESXi host that has virtual machines or virtual appliances running on its local storage. The hosted virtual machines and virtual appliances must be shutdown before the ESXi host can be put into maintenance mode. The virtual machines should be shutdown in a pre-determined order to minimize the effect on the running process. You should checkpoint ACE nodes prior to shutting down.



#### Attention

- Honeywell also recommends user have a pre-defined shutdown and restart order for ESXi hosts, virtual machines, and virtual appliances to minimize the effect on the running process.

The Update Manager Client Compliance view provides access to the interface required for performing the procedures in this topic. For more information on how to access this view, see the “Update Manager Client Overview” section in *Installing and Administering VMware vSphere Update Manager*.

### Prerequisites

- User defined procedure defining the order for shutting down and restarting ESXi host and any virtual machines or virtual appliances hosted on their local storage.
- *Installing and Administering VMware vSphere Update Manager* to understand the patching process.
- *vSphere Command-Line Interface Installation and Scripting Guide* for installing the Command-Line Interface (CLI).
- vSphere Command-Line Interface (CLI) installed on the client node performing manual patching and upgrade of ESXi host.
- Baselines and baseline groups are created or identified that contain the desired patch or upgrade to be remediated.
- Baselines and baseline groups are attached to the target object.
- Remediating patches and upgrades together requires that the patch and upgrade baselines be added to a baseline group.

### Preparing for remediation

- 1 Attach baseline groups to ESXi host, virtual machines, and virtual appliances.  
Baselines or baseline groups can be attached to individual target objects or to their container. For more information, see the “Attach Baselines and Baseline Groups to Objects” topic in *Installing and Administering VMware vSphere Update Manager*.
- 2 Scan for compliance.  
Manually initiate a scan on individual target objects or all target objects within a container. For more information, see the “Scanning vSphere Object and Viewing Scan Results” in *Installing and Administering VMware vSphere Update Manager*.
- 3 Stage patches to an ESXi host.  
Staging is only available for ESXi hosts and is optional. Staging copies patches defined in the attached baseline to the target ESXi host while it is still operational reducing the amount of time required in maintenance mode. If the ESXi host requires manual remediation, staging has no value. For more information, see the “Stage Patches and Extensions to ESX/ESXi Hosts” topic in *Installing and Administering VMware vSphere Update Manager*.
- 4 Repeat the previous steps on all ESXi hosts prior to remediation.

## Remediating target objects using Update Manager

### Prerequisites

- You have completed the preparation for remediation.

### Remediate target objects using Update Manager

- Choose the update type and follow the required procedures:

Type	Action
<b>For Host patches only</b>	Complete the steps in the “Remediate Hosts Against Patch or Extension Baseline” topic in <i>Installing and Administering VMware vSphere Update Manager</i> .
<b>For Host upgrades only</b>	Complete the steps in the “Remediate Hosts Against an Upgrade Baseline” topic in <i>Installing and Administering VMware vSphere Update Manager</i> .
<b>For Host patches and upgrades</b>	Complete the steps in the “Remediate Hosts Against Baseline Groups” topic in <i>Installing and Administering VMware vSphere Update Manager</i> .
<b>For Virtual Machines and Appliances</b>	Complete the steps in the “Remediating Virtual Machines and Virtual Appliances” topic in <i>Installing and Administering VMware vSphere Update Manager</i> .
<b>View Update Manager Events</b>	Complete the steps in the “View Update Manager Events” topic in <i>Installing and Administering VMware vSphere Update Manager</i> .
<b>All types</b>	Complete a scan to verify that the remediation was successful and that the target object is now in compliance with the attached baseline.



#### Attention

When using Update Manager for remediation, Honeywell recommends:

- Using user-initiated and immediate remediation so a predetermined order can be followed for shutting down and restarting ESXi hosts, virtual machines and virtual appliances.
- Remediating one target object at a time to the attached baselines or baseline group.

Use the following input in the **Host Remediation** wizard:

Entry	Recommended value
Unique Name	Patch ID DDMMYYYY, Update ID DDMMYYYY, Upgrade ID DDMMYYYY, or Patch ID- Upgrade ID DDMMYYYY
Description	Describe the purpose of the patch, update, or upgrade
Schedule	Immediately
Failure Response	Fail Task
Cluster options	Disable if option provided

Use the following input in the **Virtual Machine Remediation** wizard:

Entry	Recommended value
Name	Upgrade ID DDMMYYYY
Description	Describe the purpose of the upgrade
Schedule	Immediately
Snapshot	Select
When to delete	Don't delete snapshot
Snapshot Name	Update ID DDMMYYYY
Snapshot Description	Describe the purpose of the upgrade



Entry	Recommended value
Snapshot memory of the VM	No

## Remediating target objects manually

### Prerequisites

- You have completed the preparation for remediation.

### To disable host lockdown mode

- On the vSphere Client, choose the **Home > Inventory > Hosts and Clusters** view.
- Locate and click on the ESXi host computer.
- Click the **Configuration** tab.
- Under the software group, click **Security Profile**.
- Click **Edit**.  
The **Configure Host Lockdown Mode** dialog box appears.
- Clear the **Enable Host Lockdown mode** check box.  
A confirmation message dialog box appears.
- Click **OK**.

### To put the ESXi host into maintenance mode

- Using vSphere Client from a client node with CLI installed, connect to the ESXi host directly.
- Shutdown all virtual machines and put the ESXi host in maintenance mode.

### To prepare using the VMware CLI

- Copy the patch or upgrade .zip package to the client node.  
Make sure there are no spaces in the path to the patch or upgrade .zip file on the client node.
- Open a Windows Command Prompt window with administrator privileges.
- Open the folder where the vCLI is installed.  
For example:

```
cd c:\Program Files\vmware\vmware vsphere CLI\bin
```

### To verify the host identity and confirm that it is in maintenance mode

- Note: the following commands require the double dash (--)
- Type the following command:

```
vicfg-hostops.pl --server <ip_address> --operation info
```

where:

- <ip\_address>* is the IP address of the ESXi host.



#### Attention

The **vicfg-hostops.pl** command requires the double dash (--) for each of the options.

- Type the username.
- Type the password.

Here is an example of the output. Note the status of Maintenance Mode.

```
Host Name : ESX5-R710.virtlab.local
Manufacturer : Dell Inc.
Model : PowerEdge R710
Processor Type : Intel(R) Xeon(R) CPU E5530 @ 2.40GHz
CPU Cores : 8 CPUs x 2393 GHz
Memory Capacity : 49141.6640625 MB
VMotion Enabled : no
In Maintenance Mode : Yes
Last Boot Time : 2011-06-24T17:22:02.593417Z
```

#### To verify what is currently installed

- 1 Type the following command:

```
esxcli--server=<ip_address> software vib list
```

where:

- *<ip\_address>* is the IP address of the ESXi host.

- 2 Type the username.
- 3 Type the password.  
A list of installed bundles is displayed.

#### To upload the update bundle to the ESXi host

- 1 Using vSphere client select the ESXi Host that requires updates. Browse a datastore on the ESXi Host.
- 2 Create a new folder in the root of the datastore called "**updates**".
- 3 Navigate into the new **updates** folder and upload the vmware update bundle (.zip file).  
The location of the update bundle is now **/vmfs/volumes/<ESXi datastore name>/updates/<update bundle name>**

where:

- *<ESXi datastore name>* is the name of the datastore where the update bundle was uploaded
- *<update bundle name>* is the name of the update bundle (.zip file)

#### To verify the contents of a .zip package

- 1 Type the following command:

```
esxcli--server=<ip_address> software sources vib list -d <package_path>
```

where:

- *<ip\_address>* is the IP address of the ESXi host.
- *<package\_path>* is the path and file name of the .zip package. For example, */vmfs/volumes/ESX\_Datastore?updates/ESXi500-201303001.zip*.

- 2 Type the username.
- 3 Type the password.  
A list of included bundles is displayed. The status of each update will be **Installed**, **Update**, or **New**.

#### To install the required updates

- 1 Type the following command:

```
esxcli --server=<ip_address> software vib update -d <package_path>
```

where:

- *<ip\_address>* is the IP address of the ESXi host.

- *<package\_path>* is the path and file name of the .zip package. For example, */vmfs/volumes/ESXi\_Datastore/updates/ESXi500-201303001.zip*.

2 Type the username.

3 Type the password. All applicable bundles that are included on the ESXi Host will be updated. No new bundles will be added.

Here is an example of the output, which will list all updated VIBs.

Installation result:

Message: the update completed successfully, but the system needs to be rebooted for the changes to be effective

VIBs Installed: ...

#### To restart the ESXi host

1 Type the following command:

```
vicfg-hostops.pl --server <ip_address> --operation reboot
```

where:

- *<ip\_address>* is the IP address of the ESXi host.

2 Type the username.

3 Type the password.

The ESXi host restarts. Several errors may be reported after running this command. However, the ESXi host does reboot.

#### To verify that the specified bulletins were installed

1 Type the following command:

```
esxcli --server=<ip_address> software vib list
```

where:

- *<ip\_address>* is the IP address of the ESXi host.

2 Type the username.

3 Type the password.

A list of installed bundles will be displayed ensure that the install date of the updates that were updated reflects the current date.

#### To restore the management workload back to service

1 From the vSphere Client on the client node, connect directly to the ESXi host.

2 Take the ESXi host out of maintenance mode.

3 Power on the domain controller virtual machine and allow it time to start up.

4 Power on the vCenter Server virtual machine and allow it time to start up.

5 Start the remaining virtual machines and/or virtual appliances.

#### To verify that the ESXi host is in compliance

1 From the vSphere Client on the client node, connect to the vCenter Server.

2 Go to the **Hosts and Clusters** view.

3 Click the Update Manager tab.

4 Scan the ESXi host for compliance.

The ESXi host should now be in compliance.

**To enable host lockdown mode**

- 1 On the vSphere Client, choose the **Home > Inventory > Hosts and Clusters** view.
- 2 Locate and click on the ESXi host computer.
- 3 Click the **Configuration** tab.
- 4 Under the software group, click **Security Profile**.
- 5 Click **Edit**.  
The **Configure Host Lockdown Mode** dialog box appears.
- 6 Select the **Enable Host Lockdown mode** check box.  
A confirmation message dialog box appears.
- 7 Click **OK**.

**Next steps**

- If applying a patch then patching of the host is complete.
- If upgrading then go to the next phase/step of the upgrade process.

**Upgrading Virtual Hardware and VMware tools versions**

Use the following steps to upgrade virtual machines to use the latest virtual hardware version and/or VMware Tools with Update Manager. Note that the upgrade requires one or more re-boots of the virtual machine in order to complete the upgrade.

Use this procedure if

- You are upgrading virtual machines that were created on a vSphere release that is older than the current release. This is optional. The current vSphere release will support virtual machines deployed with older Virtual Hardware or VMware tools versions. Refer to VMware compatibility guides to determine which Virtual Hardware or VMware tools versions are supported with each vSphere release.
- You created new virtual machines on vSphere 5.1 with the vSphere client. In this case, the new virtual machine wizard limits you to using Virtual Hardware version 8 (VH 8). To deploy the virtual machine with Virtual Hardware version 9 (VH 9), follow these instructions.

**Attention**

- If you are deploying virtual machines on a single host with different virtual hardware versions you may experience unpredictable performance behavior.

**To upgrade Virtual Hardware or VMware Tools versions on virtual machines**

- 1 From the vSphere client that is connected to vCenter Server, select **Inventory**, and then **VMs and Templates Inventory**.
- 2 Power on any virtual machines that are not running by right-clicking on the machine name and clicking **Power**.
- 3 From the navigation pane of the **VMs and Templates Inventory** view, right-click on your datacenter and click **New Folder**. Name the new folder **R430 Upgrades**.
- 4 Drag and drop the virtual machines that are to be upgraded into the new **R430 Upgrades** folder.
- 5 Create baselines for your virtual machines:
  - a From the navigation pane of the **VMs and Templates Inventory** page, select the **R430 Upgrades** folder, and click the **Update Manager** tab.
  - b Click **Attach**. The **Attach Baseline or Group** dialog box appears.
  - c Select the **VMware Tools Upgrade to Match Host** (Predefined) and **VM Hardware Upgrade to Match Host** (Predefined) check boxes.
  - d Click **Attach**.

- e Check that baselines now exist for all your virtual machines.
- 6 Scan your virtual machines against the baselines:
  - a Click **Scan**. The **Confirm Scan** dialog box appears.
  - b Select the **VM Hardware upgrades** and **VMware Tools upgrades** check boxes.
  - c Clear the **Virtual appliance upgrades** check box, then click **Scan**.
  - d When the scan finishes, check that your virtual machines are either **0% compliant** or **n% compliant**.
- 7 Upgrade the VMware Tools version in your virtual machines (if only upgrading Virtual Hardware, proceed to step 6):
  - a From the **VMs and Templates Inventory** page, select the **R430 Upgrades** folder, and click the **Update Manager** tab.
  - b Click **Remediate**. The **Remediate wizard** appears.
  - c On the **Remediation Selection** page, select the **VMware Tools Upgrade to Match Host** (Predefined) baseline.
  - d Check that all the virtual machines are selected and click **Next**.
  - e On the **Schedule** page, accept the defaults and click **Next**.
  - f On the **Rollback Options** page, clear the **Take a snapshot of the virtual machines before remediation to enable rollback option** check box, then click **Next**.
  - g On the **Ready to Complete** page, review the upgrade information and click **Finish**.
- 8 Upgrade VM Hardware to match the host in your virtual machines:
  - a From the navigation pane of the **VMs and Templates Inventory** page, select the **R430 Upgrades** folder, and click the **Update Manager** tab.
  - b Click **Remediate**. The **Remediate wizard** appears.
  - c On the **Remediation Selection** page, select **VM Hardware Upgrade to Match Host** (Predefined).
  - d Check that all the virtual machines are selected and click **Next**.
  - e On the **Schedule** page, accept the defaults and click **Next**.
  - f On the **Rollback Options** page, clear the **Take a snapshot of the virtual machines before remediation to enable rollback** check box, then click **Next**.
  - g On the **Ready to Complete** page, review the upgrade information and click **Finish**.
- 9 When remediation finishes, check that all of the virtual machines are compliant with the attached baselines.
- 10 Select each virtual machine and click the **Summary** tab. Check that the Virtual Hardware version is **9**, and that VMware Tools has a value of **Current**.

## Upgrading virtual infrastructure software

The upgrade of virtual infrastructure software is a task that should be planned very carefully. The process involves multiple stages and each stage needs to be performed in a particular order. When an upgrade is required use the vSphere Upgrade Guide from VMware, Inc. for the target release version of vSphere.

When upgrading to the next major release of vSphere always upgrade the infrastructure software in the following order:

1. vCenter Server
2. vSphere Update Manager
3. vSphere Client
4. Production ESXi hosts
5. VMware Tools
6. Management ESXi host
7. vDR Appliance

---

**Attention**

- It is important to ensure that the upgrade is planned as vCenter Server and ESXi host downtime is expected during the upgrade.
- 

**vCenter Server**

1. Review the vCenter Server prerequisites.
2. Review the vCenter Server database prerequisites, including a full database backup.
3. Review the database scenario used.
4. Backup the existing vCenter Server.
5. Run the vCenter Pre-upgrade Check tool.
6. Upgrade the vCenter Server.
7. Review the vCenter Server post upgrade tasks.
8. Review the upgrading datastore and network permissions.
9. Upgrade vSphere Client.

For more information about these tasks, see the *vSphere Upgrade Guide*.

**Update Manager**

1. Upgrade the vSphere Update Manager to the new vSphere version.
  - a. Review the Update Manager database privileges and DSN requirements.
  - b. Perform a full backup of the Update Manager database.
  - c. Upgrade Update Manager.
  - d. Upgrade the Update Manager plug-in.

For more information, see *Installing and Administering VMware vSphere Update Manager*.

**Production ESXi hosts**

1. Upgrade the production ESXi hosts using vSphere Update Manager.

---

**Attention**

- Do not upgrade the ESXi hosts until first upgrading the vCenter Server and Update Manager. The process of upgrading an ESXi host requires the ESXi host to be restarted. Therefore, prior planning is required for this task.
- 

To upgrade the production ESXi hosts:

- a. Download a host upgrade bundle.
- b. Creating a host upgrade baseline.
- c. Scan and remediate the ESXi host.

For more information, see *Installing and Administering VMware vSphere Update Manager*.

**VMware Tools**

1. Upgrade the VMware Tools on each virtual machine.

This process will require a restart of each virtual machine so this should be planned and timed to occur with the Windows updates.

For more information, see *Installing and Administering VMware vSphere Update Manager*.

**Management ESXi host**

1. Upgrade the management ESXi host using the manual remediation process.

**Attention**

Do not upgrade the ESXi hosts until first upgrading the vCenter Server and Update Manager. The process of upgrading an ESXi host requires the ESXi host to be restarted. Therefore, prior planning is required for this task.

This task may require the vCenter Server and Update Manager to be shutdown also, so the normal method of using Update Manager to update the management host is not possible.

To upgrade the management ESXi host:

- a. Download a host upgrade bundle
- b. Manually remediate the management host
- c. Restart the management host
- d. Ensure that vCenter Server is running

**vDR Appliance**

1. Upgrade the vDR appliance.

This step is optional and all documentation regarding the upgrade process and the features/fixes in the new version must be read and understood before proceeding. The upgrade process will be documented in the target vDR appliance Release Notes and it should be followed to complete the upgrade. The following steps help provide an overview of what it required.

- a. Allow all operations in the current vDR appliance to complete.
- b. Ensure that there are no damaged restore points on the de-duplication store.
- c. Unmount the destination disk(s).
- d. Shutdown the vDR appliance.
- e. Rename the current appliance.
- f. Download the latest VMware Data Recovery media.
- g. Deploy the new appliance.
- h. Power on the new appliance.
- i. Configure the appliance settings, including the IP address and Maximum backup tasks.
- j. Attach to the network share from the old appliance destination disk and select to restore configuration.
- k. Ensure that an integrity check on the destination disk is successful.

# Maintaining hardware devices in a virtualization environment

## Related topics

“Maintaining the level 2.5 router” on page 176

## Maintaining the level 2.5 router

This topic provides guidance for replacing or updating the virtual infrastructure level 2.5 router. Internetwork Operating System (IOS) is used in Cisco Systems routers and network switches.

### Prerequisites

- *Fault Tolerant Ethernet Overview and Implementation Guide.*
- Knowledge of the router configuration information, such as HostName, Enable secret, Passwords, IP addresses, and subnet masks.
- For replacing a failed router:
  - Image of the IOS matching the IOS version of the failed router.
  - Level 2.5 router configuration file for the failed router.
- For replacing/upgrading existing routers:
  - Image of the most current IOS version.
  - Level 2.5 router configuration files created from the latest Honeywell provided templates.
- A physical computer to connect directly to the COM port of the router with a RS-232 cable.
- Hyper Terminal is installed on the physical computer.



#### Attention

Hyper Terminal is not available on Windows 7 and Windows Server 2008 by default.

### To replace the Level 2.5 router

1. For instructions on how to replace or update a level 2.5 router, see the “Replacing Switches” topic in the *Fault Tolerant Ethernet Overview and Implementation Guide*.

There are some differences in maintaining a Level 2.5 router compared to maintaining an FTE switch. However, the rules and methodology apply.

Note the following differences:

- The Level 2.5 router is a switch with router capabilities. Whenever you see the term switch, substitute it with Level 2.5 router.
- Honeywell does not qualify the IOS versions for the Level 2.5 router.
- The IOS version applied depends on the reason for the update.
  - Replacing a failed Router the IOS version should match the failed router.
  - Upgrading existing Router the newest IOS version available should be used.



#### Attention

Older versions of a Router IOS are sometimes not available from the manufacturer. It is good practice to download and archive a copy of your current Router IOS version now for future recovery purposes.

- Honeywell Network Service does not provide copies or procedures for replacing the IOS of a Level 2.5 router.
- This information should be retrieved from the router manufacturer.



For example, IOS download and installation information for Cisco Routers can be found in the Cisco Release Notes document for each specific switch. The following link provides access to the release document for the Cisco 3560x [http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x\\_3560x/software/release/12.2\\_58\\_se/release/notes/OL24338.html](http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_58_se/release/notes/OL24338.html)

- Honeywell has not evaluated *stacking* of the Level 2.5 router. Therefore, stacking information should be ignored.
- The Host Name given to Level 2.5 routers should help in identifying their Hot Standby Router Protocol (HSRP) Primary and Secondary roles.

For example, a host name of level 2.5\_Yellow and level 2.5\_Green or level 2.5\_Primary and level 2.5\_Secondary is recommended.

- Honeywell provides two template config files for the Level 2.5 router and they are called *level 2.5Yconfig\_std.txt* and *level 2.5Gconfig\_std.txt*. The install package for these files can be downloaded from the Honeywell Process Solutions web site and is located with the other FTE Switch configuration files.
- SNMP configuration is not required for the Level 2.5 router.

## Monitoring the virtualization environment

The vSphere virtual environment provides built-in tools that provide the ability to monitor the resource usage of the virtual infrastructure and signal alarms as to the status of the virtual infrastructure when thresholds are crossed. It is important to understand these tools so that the health of the virtual environment is maintained.

The virtual environment may require monitoring when operators using Experion experience slow display call-up or inconsistent refresh rates on displays. Using the Station Display Performance table in the Experion Station Specification document as a guide, which can be found on the Honeywell Process Solutions web site, monitor Station display update rate and display call up times. Compare the specification limitations and call up times to the virtual Station performance and ensure that performance is within the specification limits.

Engineering tools usage can also give an indication that the virtual environment may require monitoring. When the Experion engineering tools are used, any inconsistency in the time to perform actions indicate that the resource usage of the virtual infrastructure may not be optimal.

To rectify performance issues seen when comparing update rate and call-up times with the specification and when engineering tools show inconsistency, see the following resource usage and system status topics.

### About resource usage

Virtual infrastructure resource usage is monitored using the performance charts in the vSphere Client. These charts help administrators view the resource usage and performance indicators in the virtual environment. Guidance on the usage of both the overview performance charts and the advanced performance charts are provided in the “Monitoring Inventory Objects with Performance Charts” section.

The five performance areas that define the health of the virtual environment are:

- CPU
- disk I/O
- memory
- network
- storage

#### CPU performance

CPU usage of virtual machines and the virtual infrastructure is a very important consideration in the overall performance on the system. Monitoring the CPU usage is the best way to ensure that performance degradation is not occurring. Usage of the advanced CPU performance charts helps to give the best understanding of the current and past system CPU usage.

Consideration	Description
Virtual machine CPU usage	When monitoring CPU usage on a virtual machine, select the virtual machine and view its advanced performance charts. Select the real-time CPU chart with Usage and Usage in MHz selected. The chart shows the last hour of CPU usage in relation to percentage and MHz used. Ensure that the CPU usage is not constantly above 90%. Occasional spikes up to 100% are acceptable. For more information, see the "Solutions for Consistently High CPU Usage" section in <i>vSphere Monitoring and Performance</i> .
Virtual machine CPU contention	When monitoring CPU contention on a virtual machine, select the virtual machine and view its advanced charts. Select the real-time CPU chart with Ready selected. The chart shows the last hour of CPU ready time. Ensure that the ready time does not run constantly above 2000ms, and that spikes do not exceed 4000ms. For more information, see the "Solutions for Consistently High CPU Usage" section in <i>vSphere Monitoring and Performance</i> .

#### Disk I/O performance

Disk I/O performance should be considered whenever monitoring virtual machines or the virtual infrastructure. Monitoring disk I/O usage will help give the best indication of the health of the systems disk arrays.

Consideration	Description
Virtual machine disk latency	When monitoring virtual machine disk latency, select the virtual machine and view its advanced performance chart. Select the real-time Datastore chart with <b>Read latency</b> and <b>Write latency</b> selected. Ensure that the virtual machine disk I/O latency runs below 25ms. Occasional spikes above 25ms are acceptable. For more information, see the "Solutions for Disk Performance Problems" section in <i>vSphere Monitoring and Performance</i> .
Virtual machine disk usage	When monitoring Virtual machine disk I/O usage, select the virtual machine and then view its advanced performance chart. Select the real-time datastore chart with <b>Average write requests per second</b> and <b>Average read requests per second</b> selected. There is no performance threshold for this chart type. As a general rule the sum of average read and writes should be below the maximum IOPs and average IOPs as documented in the <i>HPS Virtualization Specification</i> .

### Memory performance

Memory usage in the Experion virtual environment should not have performance issues if the amount of allocated memory is not greater than the physical memory in the host. Monitoring the usage of this memory can be done using the advanced performance charts.

Consideration	Description
ESXi host memory contention	When monitoring ESXi hosts memory for contention select the ESXi host in question and view its advanced performance chart. Select the real-time Memory chart with <b>Balloon</b> and <b>Swap Used</b> selected. Ensure that the ESXi host always has zero balloon and zero swap used usage as shown in the charts.
ESXi host memory usage	When monitoring ESXi hosts memory for usage select the ESXi host in question and view its advanced performance chart. Select the real-time Memory chart with <b>Active</b> , <b>Consumed</b> and <b>Granted</b> selected. Ensure that the ESXi host active memory is always less than 90%.
Virtual machine memory usage	When monitoring virtual machine memory select the virtual machine in question and view its advanced performance chart. Select the real-time memory chart with <b>Active</b> , <b>Balloon</b> , <b>Consumed</b> and <b>Granted</b> selected. Ensure that the balloon is always zero. Granted and consumed memory are normally the same.

### Network performance

Monitoring the virtual network usage is important as bandwidth usage on virtual machines and physical network uplinks are potential causes of performance degradation. Ensuring that the potential network bottle necks always have available overhead is important. Network usage can be monitored using the advanced performance charts.

Consideration	Description
ESXi host network usage	When monitoring ESXi hosts network usage select the ESXi host in question and view its advanced performance chart. Select the real-time Network chart with all physical vmnics used by the production network selected in the objects selection and <b>Transmit packets dropped</b> , <b>Receive packets dropped</b> , <b>Data receive rate</b> and <b>Data transmit rate</b> selected in the counters selection. Ensure that all <b>Transmit packets dropped</b> and <b>receive packets dropped</b> show zero. View the <b>Data receive rate</b> and the <b>Data transmit rate trends</b> and ensure that the average network usage is less than half of the total available bandwidth for the network connection.
Virtual machine network usage	When monitoring Virtual machine network usage select the virtual machine in question and view its advanced performance chart. Select the real-time Network chart with the virtual machine name selected in the objects selection and <b>Data receive rate</b> and <b>Data transmit rate</b> selected in the counters selection. Ensure that the virtual machine does not use excessive bandwidth compared to the available network bandwidth supplied by the physical switch connection to the ESXi host.

## Storage

Monitoring of storage performance is the same as disk I/O performance for virtual machines. Use disk I/O to gauge the performance of the storage for virtual machines. The use of the advanced performance charts for storage adaptor and storage path available when an ESXi host is selected give a view to the performance of the disk I/O from a different perspective inside the host. These different views into the storage performance allow the performance to be viewed from different path and adapter levels to help track down issues.

Consideration	Description
Datastore performance	When the total datastore performance or datastore usage statistics are required select the ESXi host in question and view its performance chart. Select the Storage Path Real time trend then the required runtime name in the objects selection (this can be determined by viewing the ESXi host summary and viewing the properties on the datastore and clicking on the manage paths button) and select the <b>Read latency</b> , <b>Write latency</b> and <b>Average commands issued per second</b> in the counters selection. Ensure that <b>Read latency</b> and <b>Write latency</b> do not run higher than 25ms. Occasional spikes above 25ms are acceptable. Using the <b>Average commands issued per second</b> helps you to establish the IOPs on the whole datastore.
Disk array performance	When the total disk array performance or disk array usage statistics are required select the ESXi host in question and view its performance chart. Select the Storage Adapter real time trend then the required adapter in the objects selection (this can be determined by using the Configuration > Storage Adapters device command) and select the <b>Read latency</b> , <b>Write latency</b> and <b>Average commands issued per second</b> in the counters selection. Ensure that <b>Read latency</b> and <b>Write latency</b> do not run higher than 25ms. Occasional spikes above 25ms are acceptable. Using the <b>Average commands issued per second</b> helps you to establish the IOPs on the disk array.
Storage used	When the total used space on each ESXi host datastore is required use the ESXi host Configuration > Storage command to see the total capacity and free space on each datastore. The Storage Views tab also give a good indication of the used space and any space used by snapshots. Always ensure that the total used capacity on each datastore is below 75% as the default vSphere warning for datastore usage is 75% and the datastore will display a persistent alarm if this threshold is crossed.

## About system status

The status of the virtual infrastructure is known through the usage of vSphere alarms. These alarms notify that specific events have occurred and that the virtual infrastructure may be in a state that requires attention. For more about these alarms, see the “Monitoring events, alarms and automated actions” section of *vSphere Monitoring and Performance*.

### Standard Alarms

vCenter is installed with a number of default alarms that warn you of resource usage status. The list of alarms shown below should be used as a warning that Experion virtual machine performance is likely to be affected:

- Virtual machine CPU usage - Shows a warning at 75% and an alert at 90% - warns that the virtual machine is approaching its CPU limit. No action should be taken unless CPU is constantly reaching 100%
- Virtual machine memory usage - Shows a warning at 85% and an alert at 95% - warns that the virtual machine is actively using its allocated memory and the guest operating system could potential start to use swap files instead of memory. When virtual machine memory is above 95% for extended periods of time virtual machine memory should be increased.
- Host CPU usage - Shows warning at 75% and an alert at 90% - warns of ESXi host CPU constraints that may be detrimental to performance of the Experion virtual machines. Virtual machines should be moved off the ESXi host if host CPU usage exceeds 90% for extended periods of time.
- Host memory usage - Shows warning at 90% and an alert at 95% - warns of ESXi host memory constraints that could lead to ballooning and memory swapping of Experion virtual machines. ESXi host memory should be increased or virtual machines should be moved off the ESXi host if host memory exceeds 90% for extended periods of time.

## Custom Alarms

The following alarm can be configured to warn that virtual machine performance is likely to be affected:

- Virtual machine CPU ready time - Set Alarm Type to monitor Virtual machines - Set trigger type to virtual machine CPU ready time (ms) - Set warning is above 1800 for 5 minutes and set alert is above 2000 for 5 minutes. This will warn of CPU contention on a virtual machine. When Console Stations are used in a large system where the number of Console Stations is approaching 20 this value should be reduced to set warning is above 800 for 5 minutes and set alert is above 1000 for 5 minutes.
- Virtual machine total disk latency - Defaults to show warning at 50ms and alert at 75ms - warns of virtual machine disk contention. Can indicate that another virtual machine is using abnormally high disk IOPs or that the disk array is running in a degraded state. As soon as an Experion virtual machine indicates in alarm action should be taken to fix the disk array performance or move virtual machines off the datastore to reduce the load. If IOPs limits are set on the Virtual Machine, consider raising the limit.



### Attention

- For better warning of disk performance issues the warning trigger can be adjusted to 25ms.
- 

## Host health

The status of the ESXi host hardware can also be monitored through vSphere. The hardware Status Tab is presented in the vSphere Client when the vCenter Hardware Status plug-in is installed and enabled. This plug-in allows the hardware status to be monitored. For more information, see the “Monitoring Host Health Status” section of *vSphere Monitoring and Performance*.



# Notices

## **Trademarks**

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

## **Other trademarks**

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

## **Third-party licenses**

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third\_party\_licenses on the media containing the product, or at <http://www.honeywell.com/ps/thirdpartylicenses>.

---

## Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

<http://www.honeywellprocess.com/support>

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

[hpsdocs@honeywell.com](mailto:hpsdocs@honeywell.com)

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.



---

## How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

<https://honeywell.com/pages/vulnerabilityreporting.aspx>

Submit the requested information to Honeywell using one of the following methods:

- Send an email to [security@honeywell.com](mailto:security@honeywell.com).
- or
- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

---

## Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, <https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx>.

---

## Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see <http://www.automationcollege.com>.

