Experion PKS with PMD Controller
Virtualization User's Guide

PMDOC-X303-en-900B
October 2017
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 Oy.

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 2017 - Honeywell Oy
Contents

1 About this document .................................................................................................................. 7

2 Getting started with PMD virtualization ................................................................................... 9
  2.1 Virtualization components ...................................................................................................... 10
     2.1.1 vSphere components ..................................................................................................... 10
     2.1.2 ESXi ............................................................................................................................. 10
     2.1.3 vCenter ....................................................................................................................... 10
     2.1.4 vSphere Client interfaces ............................................................................................ 10
     2.1.5 Storage ....................................................................................................................... 10
  2.2 Task overview for preparing an PMD virtualization environment ........................................ 12

3 Planning for PMD DCS architecture ..................................................................................... 13
  3.1 PMD DCS architecture options in a virtualized environment ............................................... 14
     3.1.1 Example DCS architecture in a virtualized environment with non-redundant management
          network ............................................................................................................................ 14
  3.2 Overview of distributing workload across ESXi hosts for PMD DCS architecture ............... 16

4 Planning the virtualization environment ............................................................................... 17
  4.1 Determining the number of ESXi hosts and hardware requirements ....................................... 18
  4.2 Identifying virtualization hardware and software requirements .......................................... 21
     4.2.1 Hardware requirements .............................................................................................. 21
     4.2.2 Software requirements .............................................................................................. 21
     4.2.3 VMware software and licenses .................................................................................. 22
     4.2.4 Other requirements ................................................................................................... 22
  4.3 Planning for the management ESXi host and management network ...................................... 23
     4.3.1 Supported management workloads ............................................................................. 24
  4.4 Planning for the production ESXi host and production network ........................................... 25
  4.5 Planning how to organize the vCenter Server ........................................................................ 26
  4.6 Planning for time synchronization ........................................................................................ 27
  4.7 Planning to maintain the VMware environment .................................................................... 28
  4.8 Planning to backup the virtual infrastructure and virtual machines ..................................... 33

5 Implementing networks for a PMD DCS architecture ............................................................ 35
  5.1 Implementing a non-redundant management network for a DCS architecture ..................... 36
  5.2 Implementing production network and other layers .............................................................. 38

6 Implementing a management ESXi host ................................................................................ 39
  6.1 Configure the ESXi host local disk array .............................................................................. 40
  6.2 Configure the ESXi host BIOS settings .............................................................................. 41
  6.3 Install and configure ESXi server .......................................................................................... 42
     6.3.1 Install ESXi Operating System ................................................................................... 42
     6.3.2 Configure ESXi Server .............................................................................................. 47
  6.4 Install and configure vSphere Client ..................................................................................... 50
     6.4.1 Install VMware vSphere Client .................................................................................. 50
     6.4.2 License the ESXi Server ............................................................................................ 54
  6.5 Network configuration for a management host in a DCS architecture .................................. 58
     6.5.1 Configure the virtual switch for the management network ........................................ 58
     6.5.2 Enable 1 Gbps network .............................................................................................. 59
     6.5.3 Configure the Virtual Switch port security settings .................................................... 60

Honeywell
CONTENTS

6.5.4 Connect physical network switches ................................................................. 61
6.6 Create management virtual switch ........................................................................................................ 62
6.7 Configure ESXi host time synchronization ..................................................................................... 64
6.8 Install and configure Domain Controller ....................................................................................... 65
6.9 Install and configure vCenter Server ................................................................................................. 66
6.9.1 Considerations for vCenter Server ................................................................................................. 66
6.9.2 Create a vCenter Server virtual machine ......................................................................................... 67
6.9.3 Setup and configure web client ................................................................................................... 86
6.9.4 Configure the vCenter Server ................................................................................................... 91
6.10 Install VMware vSphere Update Manager .................................................................................... 99
6.11 Install the VMware vSphere Update Manager plug-in ............................................................. 104
6.12 Configure VMware vSphere Update Manager ........................................................................... 107
6.13 Upgrade virtual hardware version ............................................................................................... 109
6.14 Install the Experion virtual machine utility .................................................................................. 111
6.15 Organizing VMware inventory objects ....................................................................................... 112
6.16 VM auto startup and shutdown settings ...................................................................................... 113

7 Implementing a production ESXi host ........................................................................................................... 115
7.1 Configure the ESXi host local disk array .......................................................................................... 116
7.2 Configure the ESXi host BIOS settings ............................................................................................ 117
7.3 Install and configure ESXi server ..................................................................................................... 118
7.3.1 Install ESXi Operating System .................................................................................................. 118
7.3.2 Configure ESXi Server ........................................................................................................... 123
7.4 Add the ESXi host to the vCenter Server .......................................................................................... 126
7.5 Network configuration for a production host in a DCS architecture ........................................ 129
7.5.1 Configure virtual switch for the production network ............................................................. 130
7.5.2 To enable 1 Gbps network ......................................................................................................... 134
7.6 Configure the Virtual Switch port security settings ...................................................................... 136
7.7 Connect to physical network switches ............................................................................................ 137
7.8 Configure ESXi host time synchronization .................................................................................... 138
7.9 Domain name resolution .................................................................................................................. 139

8 Installing of PMD nodes on a Virtual Machine .................................................................................... 141
8.1 Install PMD Server .......................................................................................................................... 142
8.2 Install PMD HMI ............................................................................................................................. 143
8.3 Install PMD RHS .............................................................................................................................. 144
8.4 Install PMD Design Module ............................................................................................................ 145

9 Installing and configuring thin clients ...................................................................................................... 147

10 Configuring the PMD nodes .................................................................................................................. 149

11 Configuring the EBR application ........................................................................................................ 151

12 Administering of the virtualization environment .................................................................................. 153
12.1 Monitor the virtualization environment .......................................................................................... 154
12.1.1 About resource usage .............................................................................................................. 154

13 Supplementary task ............................................................................................................................ 157
13.1 Export and import the virtual machine .......................................................................................... 158
13.1.1 Export the VM file .................................................................................................................... 158
13.1.2 Import the VM file .................................................................................................................... 159

14 Troubleshooting ................................................................................................................................. 163
14.1 TCP Checksum offload ................................................................................................................. 164
14.2 FTE fails on PMD nodes and causes system to hang ...................................................................... 167
14.3 Virtual machine time gets out of sync with NTP server .............................................................. 177
14.4 Virtual machine issues .................................................................................................................. 178
14.4.1 Virtual Machine black screen issue ................................................................. 178
14.4.2 Virtual Machine mouse or video performance issue ......................................... 178
1 About this document

The Experion PKS with PMD Controller Virtualization User’s Guide provides guidance to plan and implement a virtualized PMD environment.

Revision history

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>November 2016</td>
<td>Initial release of the document.</td>
</tr>
<tr>
<td>B</td>
<td>October 2017</td>
<td>Includes installation and configuration of VMware Update Manager.</td>
</tr>
</tbody>
</table>

Related documents

The following are the list of documents that are source of reference for content discussed in this publication.

- Experion PKS Virtualization Planning and Implementation Guide
- Experion PKS Wyse Z90DE7 Thin Client Planning Installation and Service Guide
- Experion PKS with PMD Controller Getting Started User’s Guide
- Experion PKS with PMD Controller Network Planning and Design Guide
- Experion PKS with PMD Controller Installation of PMD R900 using ESIS on: Virtual Server, Virtual DM, Virtual HMI, and Virtual RHS
- Experion PKS with PMD Controller Experion Backup and Restore R500.1 for PMD User’s Guide
- HPS Virtualization Specification document, p/n EP03-700-100

Support and Contacts

For any support, contact your local Honeywell Technical Assistance Center (TAC).

<table>
<thead>
<tr>
<th>Finland</th>
<th>Mail: Honeywell Oy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GTAC P3-DCS</td>
</tr>
<tr>
<td></td>
<td>Navitas 1, B-block, 4.kerros, Wredenkatu 2</td>
</tr>
<tr>
<td></td>
<td>FI-78250 Varkaus, Finland</td>
</tr>
<tr>
<td></td>
<td>Phone: +358 20 752 2000</td>
</tr>
<tr>
<td></td>
<td>Email: DL HPS_Q_GTAC_P3_DCS</td>
</tr>
</tbody>
</table>

| Elsewhere     | Call your nearest Honeywell office.                                  |

2 Getting started with PMD virtualization

Virtualization of an Experion PKS with PMD Controller (PMD) system involves allocating system and application nodes to virtual machines rather than physical machines. A key aspect of an PMD 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 PMD system include:

- The production workload is consolidated on ESXi server grade hosts and connected to a production network.
- The production ESXi hosts are 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 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 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.

You can virtualize the PMD Server, Human Machine Interface (HMI), Remote HMI Server (RHS), and Design Module (DM) nodes.

Related topics

“Virtualization components” on page 10
“Task overview for preparing an PMD virtualization environment” on page 12
2.1 Virtualization components

2.1.1 vSphere components

VMware vSphere is a suite of software components for virtualization. To run vSphere environment, you must have the components such as, ESX/ESXi, vCenter Server, Datastore, and so on.

2.1.2 ESXi

VMware ESXi is an enterprise level computer virtualization product and it used to host the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine. Through ESXi, you can run the virtual machines, install operating systems, run applications, and configure the virtual machines. The ESXi server provides management capabilities and other services that manage the virtual machines.

2.1.3 vCenter

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. The vCenter Server contains the required software components for the administration of virtual machines, ESXi hosts, and the virtualization environment.

2.1.4 vSphere Client interfaces

There are several ways to access vSphere components. vSphere interface options include, vSphere Client, vSphere Web Access, VMware Service Console, and vSphere Command-Line Interface. The vSphere Client interface is the tool most often used to interface with a virtualized PMD system.

vSphere Client

vSphere Client is a required component and the primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. In addition, it provides console access to virtual machines. vSphere Client is installed on a physical Windows computer with network access to the ESXi system. You cannot use the vSphere Client to edit the settings of virtual machines of hardware version 10 or higher.

vSphere Web Client

The vSphere Web Client is a server application that provides a browser-based alternative to the traditional vSphere Client. The editing setting of a virtual machine running hardware version 10 is supported only with the vSphere Web Client. After upgrading to hardware version 10, you must use vSphere Web Client to perform edit settings.

2.1.5 Storage

Datastore

Datastore represents a storage location for virtual machine files. A storage location can be a VMFS volume, a directory on Network Attached Storage, or a local file system path. Currently, only local file system path is supported.
A datastore is platform-independent and host-independent. Therefore, datastore do not change when the virtual machines they contain are moved between ESXi hosts.
### 2.2 Task overview for preparing an PMD virtualization environment

The following table captures a high level overview of the tasks that must be completed to setup the virtual environment.

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine architecture</td>
<td>Refer to “Planning for PMD DCS architecture” on page 13.</td>
</tr>
<tr>
<td>Planning for the virtualization environment</td>
<td>Refer to “Planning the virtualization environment” on page 17.</td>
</tr>
<tr>
<td>Build the networks:</td>
<td></td>
</tr>
<tr>
<td>• Management network</td>
<td>For management network: Refer to “Planning for the management ESXi host and management network” on page 23.</td>
</tr>
<tr>
<td>• Production network</td>
<td>For production network: Refer to “Planning for the production ESXi host and production network” on page 25.</td>
</tr>
<tr>
<td>Implementing a management ESXi host</td>
<td>Refer to “Implementing a management ESXi host” on page 39.</td>
</tr>
<tr>
<td>Implementing a production ESXi host</td>
<td>Refer to “Implementing a production ESXi host” on page 115.</td>
</tr>
<tr>
<td>Installing PMD nodes on a virtual machine</td>
<td>Refer to “Installing of PMD nodes on a Virtual Machine” on page 141.</td>
</tr>
<tr>
<td>Installing and configuring thin clients</td>
<td>Refer to “Installing and configuring thin clients” on page 147.</td>
</tr>
<tr>
<td>Configuring the PMD nodes</td>
<td>Refer to the <em>Experion PKS with PMD Controller Getting Started User’s Guide</em>.</td>
</tr>
<tr>
<td>Configuring Experion Backup and Restore (EBR)</td>
<td>Refer to “Configuring the EBR application” on page 151.</td>
</tr>
<tr>
<td>Administering the virtualization environment</td>
<td>Refer to “Administering of the virtualization environment” on page 153.</td>
</tr>
</tbody>
</table>
3 Planning for PMD DCS architecture

Related topics

“PMD DCS architecture options in a virtualized environment” on page 14
“Overview of distributing workload across ESXi hosts for PMD DCS architecture” on page 16
3.1 PMD DCS architecture options in a virtualized environment

A virtualized PMD architecture requires ESXi host at Level 2 and Level 2.5 and optional at 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. 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 management network deployment options at Level 2 with recommended usages.

<table>
<thead>
<tr>
<th>Non-redundant management network with single routed connection to L2.5 network layer</th>
<th>Production Network Security</th>
<th>Mgmt Network High Availability</th>
<th>Relative Cost</th>
<th>Usage</th>
</tr>
</thead>
</table>
| Good | No | Low | • Small-medium system deployment  
• Single PMD department  
• Local storage solution  
• New sites  
• Existing sites with single PMD Department  
• Single management network for automation levels (L2, L2.5, and L3) |

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

Use of a single dedicated switch/router is recommended for single PMD Department 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.

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 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
Figure 1: Example DCS architecture network topology with non-redundant management network
3.2 Overview of distributing workload across ESXi hosts for PMD 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 at Level 3 and above.

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.

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.

<table>
<thead>
<tr>
<th>Example process operational workloads</th>
<th>Example application workloads</th>
<th>Example management workloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>• PMD Server A</td>
<td>• PHD</td>
<td>• vCenter Server</td>
</tr>
<tr>
<td>• PMD Server B</td>
<td></td>
<td>• vSphere Client</td>
</tr>
<tr>
<td>• HMI</td>
<td></td>
<td>• Domain controller</td>
</tr>
<tr>
<td>• Design Module</td>
<td></td>
<td>• EBR Manager</td>
</tr>
<tr>
<td>• RHS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Attention

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

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

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

Related topics
“Determining the number of ESXi hosts and hardware requirements” on page 18
“Identifying virtualization hardware and software requirements” on page 21
“Planning for the management ESXi host and management network” on page 23
“Planning for the production ESXi host and production network” on page 25
“Planning how to organize the vCenter Server” on page 26
“Planning for time synchronization” on page 27
“Planning to maintain the VMware environment” on page 28
“Planning to backup the virtual infrastructure and virtual machines” on page 33
4.1 Determining the number of ESXi hosts and hardware requirements

Before identifying any hardware requirements, the PMD system must be defined. This requires a knowledge of all planned PMD virtual nodes and the topology that must 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 connects to the same network. To do this, identify workloads that operates on the same network level. For example, workload belonging (PMD Server, HMI, DM, and RHS) to the Level 2 network for PMD DCS architectures or the production network, should be grouped into the PMD department workload.

**PMD architecture example**

An example PMD architecture grouping at this point is:

- Level 2 (PMD Department workload)
- Level 2.5 (Management workload)
- Level 3 (Advanced Application workload) (Optional)

**Determining ESXi host groups**

The aim of creating a ESXi host group listing is to form the groups of virtual nodes that can consolidated into an ESXi host.

In a single ESXi host group, assigning all PMD redundant servers or HMI nodes and RHS on a single node is not a good practise, a failure in a ESXi host can cause complete failure of process, so it is recommend to evenly distribute across the host group. For information about distributing the workload in host group, refer to the following “PMD architecture example” on page 18.

**Attention**

- Redundant servers must not be placed in the same ESXi host group. The redundant server must have mandatorily have two ESXi host group.
- No more than one Windows domain controller can run in the same host group.

**PMD architecture example**

**PMD Department workload (Level 2)**

- **PMD Department ESXi host group A:**
  - PMD Server A
  - HMI Station 1
  - HMI Station 3
  - DM 2
  - RHS 2

- **PMD Department ESXi host group B:**
  - PMD Server B
  - HMI Station 2
  - HMI Station 4
  - DM 1
Management workload (Level 2.5)
- vCenter Server
- vSphere Client
- Windows domain controller

Application workload (Level 3) (optional)
- PHD

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.

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 x 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 PMD 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 16020 MHz (2670 x 6 = 16020).

---

**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.

**Storage requirements**
Honeywell supports local host storage and network attached storage (NAS).

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 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.
4.2 Identifying virtualization hardware and software requirements

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

4.2.1 Hardware requirements

This section lists the hardware requirements for the ESXi host server and vSphere client workstation.

**ESXi host**

For ESXi host hardware version, refer to the *HPS Virtualization Specification Document, p/n EP03-700-100*.

**Client workstation**

HPS recommended workstation class computer running on Windows 10 professional can be used for vSphere Client Node. Some of the workstation class computers recommended by HPS are:

- Dell Precision T5810 Workstation (for vSphere Client and vSphere Web Client)
- Dell Precision T3600XL Workstation (for vSphere Client and vSphere Web Client)
- Dell OptiPlex XE2

**Thin clients**

- Wyse Z90DE7 thin client workstation
- FTE redundant port protector

**Switches**

- For management network use Cisco 3560 / Cisco 3850 switch
- For production network use Experion R500 recommended switches, for example: Cisco2960/Cisco2960 Plus switches
- For backup use Cisco 3560/Cisco 2960 Plus switch

4.2.2 Software requirements

The software requirements are the following:

- ESXi operating system 6.0
- vCenter Server 6.0 U3 installer image
- Experion PKS System Initialization media 200.1
- Experion PKS R500.1 software and license
- Experion PKS with PMD Controller R900.1 software and license
- Windows Server 2016
  - 64-bit for PMD Server, RHS
- Windows Server 2008 R2 Standard Edition SP2
  - 32-bit for DM
- Windows 10
  - 64-bit for PMD HMI, Console
4.2.3 VMware software and licenses

Ensure that the following VMware software and licenses are available.

- 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.
- 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.

4.2.4 Other requirements

Windows domain controllers

The Windows domain controller is required on the management network. The Domain Name System (DNS) server needs to be implemented on all domain controllers. Configure DNS with forward and reverse lookup.
### 4.3 Planning for the management ESXi host and management network

**About management network**

The management network separates the management network traffic between the ESXi hosts and the management nodes from the PMD department network (Level 2) network or production traffic. Honeywell recommends that network traffic between ESXi hosts and the management host be directed to a separate network called the management network. The management network does not have any connection to the production network.

**Figure 3: Management network topology**

**About management workload**

Management workloads are virtual machines that normally run on a dedicated Management ESXi Host Server and only connect to the management network. Examples of management workloads are vCenter Server VM and EBR Manager VM. 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.

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 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. 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 leads to high CPU ready time and all management workloads slows 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 the disk storage capacity is adequate for the virtual machines planned to run and store on the management ESXi host. Never plan to use more than 70% of the total datastore space.
4.3.1 Supported management workloads

The supported management workloads are:

- **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 has members before vCenter Server is prepared.

- **VMware 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.

- **VMware 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 ESIS virtual hard disk and utility virtual hard disks, which are used for the installation of PMD 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 using Windows authentication. If you are using vSphere Client to connect to an ESXi host directly, the vSphere Client authenticates access using local ESXi host account. You cannot use the vSphere Client to edit the settings of virtual machines of hardware version 11 or higher.

- **VMware vSphere Web Client**: The vSphere Web Client is a server application that provides a browser-based alternative to the traditional vSphere Client. The editing setting of a virtual machine running hardware version 10 is supported only with the vSphere Web Client. After upgrading to hardware version 10, you must use vSphere Web Client to perform the edit settings.

- **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 deduplication store for this appliance and this NAS device is also connected to the management network.

- For more information about the requirements for the virtual machines that reside on the Management Host, refer to the *HPS Virtualization Specification document, p/n EP03-700-100*. 


4.4 Planning for the production ESXi host and production network

About production network
The PMD system VMs (PMD Server, HMI, DM, and RHS) run on the ESXi server host and connect to a separate network, called the Production Network (Level 2).

![Production network topology](image)

About production workload
A production ESXi host runs the production workload. The production workload consists of virtual machines that run on the production host and only connects to the production network. Examples of production workloads are PMD Server, HMI, DM, and RHS.
4.5 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.

**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.

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>datacenter</td>
<td><em>A datacenter</em> is the primary container of inventory objects, such as hosts and virtual machines. A vCenter Server can contain multiple datacenters.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For PMD virtualizations, a datacenter is used to contain all of the virtual machines.</td>
</tr>
<tr>
<td>folder</td>
<td><em>A folder</em> is a PMD 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.</td>
</tr>
<tr>
<td></td>
<td>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 PMD cluster or system. You can use folders to group hosts into any logical grouping that suits your organization.</td>
</tr>
<tr>
<td>ESXi host</td>
<td><em>A host</em> is a computer that is running ESXi virtualization software to run virtual machines. 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.</td>
</tr>
</tbody>
</table>
4.6 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.

![Attention]
Virtualization infrastructure mandatorily requires a physical hardware that act as NTP server, it can be an External time source, Domain server or switch.

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 PMD 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:

<table>
<thead>
<tr>
<th>Windows domain</th>
<th>Set up time synchronization by following the instructions in the Experion PKS Supplementary Installation Tasks Guide.</th>
</tr>
</thead>
</table>
| ![Attention]                 | The ESXi hosts must synchronize with the domain controller or the external time source that the domain controller synchronizes with.

<table>
<thead>
<tr>
<th>Workgroup without an external time source</th>
<th>Set up time synchronization by following the instructions in the Experion PKS with PMD Controller Getting Started User’s Guide. When using virtual machines as the authoritative time source, time drift can occur and this practice is not recommended.</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Attention]</td>
<td>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:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Workgroup with an external time source</th>
<th>Set up time synchronization by following the instructions in the Experion PKS with PMD Controller Getting Started User’s Guide.</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Attention]</td>
<td>The ESXi hosts must synchronize with the external time source.</td>
</tr>
</tbody>
</table>
4.7 Planning to maintain the VMWare environment

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

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.

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 and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization Administrator</td>
<td>• Manages the Datacenter and the provision of resources.</td>
</tr>
<tr>
<td></td>
<td>• Creates and configures the virtual machines.</td>
</tr>
<tr>
<td></td>
<td>• Creates and maintains the network configuration.</td>
</tr>
<tr>
<td></td>
<td>• Manages updates to the ESXi hosts and virtual machines.</td>
</tr>
<tr>
<td></td>
<td>• Defines security for the ESXi host.</td>
</tr>
<tr>
<td></td>
<td>• Manages other virtual appliances.</td>
</tr>
<tr>
<td>Experion Virtualization Administrator</td>
<td>• Manages Experion virtual machines.</td>
</tr>
<tr>
<td></td>
<td>• Manages patches to virtual machine guest operating system and Experion software.</td>
</tr>
<tr>
<td></td>
<td>• Creates and configures Experion virtual machines. Starts up and shuts down Experion virtual machines.</td>
</tr>
<tr>
<td>Experion Virtualization User</td>
<td>Starts up and shuts down Experion virtual machines.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Assign the following vCenter role</th>
<th>To the following user or global group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization Administrator</td>
<td>System administrator users.</td>
</tr>
<tr>
<td>Experion Virtualization Administrator</td>
<td>Honeywell Administrators or Product Administrators global group.</td>
</tr>
<tr>
<td>Experion Virtualization User</td>
<td>Local Engineers global group.</td>
</tr>
</tbody>
</table>

### ESXi host users

Each ESXi host has two default users:

- The *root* user has full administrator privileges.
- The *vpxuser* 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.

### 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.
Security hardening

In addition to guidelines in the Virtualization with Premium Platform guide, Honeywell recommends that you follow these guidelines from VMware when implementing your virtual infrastructure:

In vSphere 6.0 VMware has split security hardening into two areas:

- **Operational Guidance** – How you use the product in your environment
- **Programmatic Guidance** – What settings should be applied OR audited

These guidelines are documented in the:

- Operational Guidance - vSphere_Hardening_Guide_6_0_GA_Moved_to_Documentation.xls
- Programmatic Guidance - vSphere_6_0_Hardening_Guide_GA_15_Jun_2015.xls

These guides deal 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 regarding the structure of your virtual infrastructure, some of the guidelines in VMware Hardening may not Planning the virtualization environment 79 Honeywell 2017 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 Hardening Guide should be followed.

The programmatic guidance document provides details on how to apply and how to audit for the item, in addition VMware’s vRealize Operations (vROps) can also be used to check the status of your system with the programmatic guidance items.

**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
- Use of 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 regarding other host hardening guidelines:

- Use of SNMP - Ensure SNMP is disabled unless you have an appropriate SNMP infrastructure.

**vNetwork hardening**

Please note the following comments regarding network hardening:

- Discount all profile 1 items
- Isolate Management Network VLAN- Domain Controller, RDP and ports related to WSUS and anti-virus may also need to be allowed between management networks if they are common with the production network.

**vCenterServer hardening**

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

- Discount all Profile 1 items.

**VUM hardening**

For Update Manager, Honeywell recommends following all Profile 1 hardening guidelines.
SSO hardening
For SSO, Honeywell recommends following all Profile 1 hardening guidelines.

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 VMware vSphere Replication to replicate 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.

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

You must use Experion Backup and Restore (EBR) to perform backups of the virtual infrastructure and virtual machines. EBR is the primary backup tool that allows virtual machine backups to be moved out of the virtual infrastructure and onto separate storage.
5 Implementing networks for a PMD DCS architecture

Related topics
“Implementing a non-redundant management network for a DCS architecture” on page 36
“Implementing production network and other layers” on page 38
5.1 Implementing a non-redundant management network for a DCS architecture

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

**Prerequisites**

The procedures to establish the network levels are beyond the scope of this guide. The *Experion PKS with PMD Controller Network Planning and Design Guide* provides recommendations and guidelines to consider when establishing Level 1, Level 2, and Level 3. Honeywell Network Services can be consulted for the proper configuration of the router at Level 3. In addition, you can refer to the *Experion Network Best Practices Guide*.

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 following figure 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 following figure, 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 is unused at this time.
- Common definition of a VLAN in both Level 2.5 A and B routers for the management network.

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 sample configuration files for level 2.5 routers are available in the Honeywell Process Solution website.
5.2 Implementing production network and other layers

For implementing production network and other layers, refer to the *Experion PKS with PMD Controller Network Planning and Design Guide.*
6 Implementing a management ESXi host

You must prepare a management ESXi host for management workloads. Before you can create PMD 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.

The initial configuration of the virtual environment requires a vSphere Client to connect to the management host. A workstation connected to the management network can be used to perform this role.

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:

- Domain controller
- vCenter Server
- All others

Related topics

- “Configure the ESXi host local disk array” on page 40
- “Configure the ESXi host BIOS settings” on page 41
- “Install and configure ESXi server” on page 42
- “Install and configure vSphere Client” on page 50
- “Network configuration for a management host in a DCS architecture” on page 58
- “Create management virtual switch” on page 62
- “Configure ESXi host time synchronization” on page 64
- “Install and configure Domain Controller” on page 65
- “Install and configure vCenter Server” on page 66
- “Install VMware vSphere Update Manager” on page 99
- “Install the VMware vSphere Update Manager plug-in” on page 104
- “Configure VMware vSphere Update Manager” on page 107
- “Upgrade virtual hardware version” on page 109
- “Install the Experion virtual machine utility” on page 111
- “Organizing VMware inventory objects” on page 112
- “VM auto startup and shutdown settings” on page 113
6.1 Configure the ESXi host local disk array

This section must be followed only if Honeywell factory is setting up the ESXi host server for PMD virtualization services. Prior to installing the ESXi software, you must prepare the local disk array on the ESXi host.

Attention

This section is not intended for the customer if they are using their own ESXi host. This is a procedure to install and configure ESXi host for production, management, and application networks.

The Dell PowerEdge R730 XL should be pre-configured as RAID 10 with Hot Spare as shipped from Dell. If it is not configured as RAID 10 with Hot Spare then it must be configured manually.

To configure the computer to use RAID 10 with Hot Spare in R730 XL platform

1. To start the RAID Configuration Utility program, press <Ctrl+R> while booting up the computer.
2. Under Virtual Disk Management (VD Mgmt), select Controller 0 by using the UP/DOWN ARROW key.
3. Press F2 to view the options available.
4. Select Create New VD by using the UP/DOWN ARROW key.
5. Press Enter.
   The Create New VD screen appears.
6. Press Enter.
7. Press Tab key to select the RAID Level row.
8. Press Enter to view the list of RAID Level available.
9. Select RAID-10 from the list by using the UP/DOWN ARROW key, and then press Enter.
10. Press Tab key, to go to Physical Disks section.
11. Under Physical Disks, select drives 00:00, 00:01, 00:02, 00:03, 00:04, 00:05, 00:06, and 00:07 by using SPACE key.
12. Press Tab key, to go to VD Name field, under Basic Settings section.
13. Under Basic Settings, type VD Name in the VD Name field. For example: SYSTEM.
14. Press Tab key, to go to Advanced Settings section, and press SPACE key to select it.
15. Press Tab key, to move to Initialize row, and press SPACE key to select it.
16. Press Tab key, to move to OK, and press Enter.
   Initialization deletes all the data in the virtual disk and a message appears, and prompts you to confirm deletion the data.
17. Select OK and press Enter to continue.
18. Press <Ctrl+N> to go to PD Mgmt window.
19. Under Physical Disk Management, select disk 00:08 by using the UP/DOWN ARROW key.
20. Press F2 to view the options available.
21. Select Make Global HS from the list.
22. Press Enter.
   If a message appears, and prompts you to confirm that the global hot spare to give priority to the enclosure in which it resides. Then, select YES, and press Enter.
23. Press Esc to exit.
   A confirmation message appears to exit, select OK, and press Enter.
6.2 Configure the ESXi host BIOS settings

Press F2 while booting up the computer, go to the BIOS Setup menu and set the following BIOS settings 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
Only enable the settings which are available.

- Node Interleaving disabled.
- Unused hardware disabled.
- Hardware clock is set to UTC.
- Power Management set to Maximum Performance (that is, disable Power Management).
- CD-ROM device should be set first in the BOOT sequence.

Press Save and exist.
6.3 Install and configure ESXi server

Related topics
“Install ESXi Operating System” on page 42
“Configure ESXi Server” on page 47

6.3.1 Install ESXi Operating System

The Honeywell Virtualization platforms must be installed using the Dell customized ESXi media.
The VMware ESXi installation media from VMware website does not contain the appropriate network drivers
for the Broadcom NIC's that are part of this configuration.
A copy of the Dell customized ESXi media is available from the Honeywell Support Web site. For obtaining
this media, refer to the instructions in the section “Download the Dell customized ESXi installer image” on
page 42.

6.3.1.1 Download the Dell customized ESXi installer image

To download the Dell customized ESXi installer image from HoneywellProcess.com website
1. Click the link: https://www.honeywellprocess.com/library/support/software-downloads/Customer/VMware-
VMvisor-Installer-201501001-2403361.x86_64.pdf
2. Log on to the HoneywellProcess.com website.
The Software Download Datasheet opens.
3. Click the VMware-VMvisor-Installer-6.0.0.update03-5050593.x86_64-Dell_Customized-A00 link.
4. Click Save and select the appropriate folder to save the VMware-VMvisor-
Installer-6.0.0.update03-5050593.x86_64-Dell_Customized-A00 file.
5. Extract the zip file and burn the ESXi software installer ISO file to a DVD.

6.3.1.2 Install ESXi 6.0 using the interactive mode

To install the ESXi 6.0 software, you must use the ESXi 6.0 DVD created in the section “Download the Dell
customized ESXi installer image” on page 42.

To install the ESXi 6.0 software on the host server
1. Insert the ESXi 6.0 installable CD/DVD into the CD/DVD-ROM drive.
2. Restart the machine.
The Welcome to the VMware ESXi 6.0.0 Installation screen appears.
3 Press Enter to continue with the installation. The End User License Agreement (EULA) screen appears.

4 Read the VMware end-user license agreement, and press F11 to accept it. The Select a Disk to Install or Upgrade screen appears.

5 Select the disk drive on which you have to install ESXi 6.0, and press Enter to continue. If there are two hard disks, select the one on which the OS is installed.

   Attention
   - Press F1 for information about the selected disk. If the disk you selected contains data, the Confirm Disk Selection screen appears.

The Please select a keyboard layout screen appears.
6 Select **US Default**, and press **Enter** to continue.
The **Please enter a root password (recommended) screen** appears.

7 Enter the **Root password** and **Confirm password**, press **Enter** to continue.

   ![Password Input Screen](image)

   **Attention**
   - Ensure to note down the root password, so that it can be used for future reference.

   The **Confirm Install** screen appears.

8 Press **F11** to start the installation.
The installation begins and displays the progress.
The **Install Complete** screen appears after installation is complete.

9 Remove the ESXi installation **CD/DVD**, and press **Enter** to reboot the host.

10 Press F2 while booting up the computer, go to the BIOS Setup menu and set the following BIOS settings on the ESXi host:
   - Change first boot sequence from CD-ROM device setting to first boot device to be the drive on which you have installed the ESXi host.

11 Press **Save** and exist.

### 6.3.1.3 Upgrade from ESXi 5.1/5.5 to ESXi 6.0

**To upgrade from ESXi 5.1/5.5 to ESXi 6.0**

1 In vSphere client workstation, log on to vSphere client using the credentials of root user.
2 Shut down all PMD nodes and then shutdown all running virtual machines.

   Attention
   The upgrade from ESXi 5.1/5.5 to ESXi 6.0 may cause some production downtime.

3 Select the ESXi server, and right-click and select Enter Maintenance Mode.

4 Click Yes.
The maintenance mode task completed message appears.

5 In the Recents tasks section, the details appear.

6 In the ESXi server, open the console of ESXi 5.1/5.5.

7 Insert the ESXi 6.0 media in the ESXi Server.

8 Press F12.
The Authentication screen appears.

9 Type the login name and password, and press Enter.
A confirmation message appears.

10 Press F11 to restart the server.
A confirmation message appears.

   If you do not make any selection, it automatically boots from the installer.

11 Press Enter.
   Wait for few minutes. The Welcome to the VMware ESXi 6.0.0 Installation screen appears.

12 Press Enter to continue with the installation.
The End User License Agreement (EULA) screen appears.

13 Read the VMware end-user license agreement, and press F11 to accept it.
The Select a Disk to Install or Upgrade screen appears.
Select the disk drive on which you have to install ESXi 6.0, and press Enter to continue.
If there are two hard disks, select the one on which the OS is installed.

Attention
Press F1 for information about the selected disk. If the disk you selected contains ESXi OS, the Confirm Disk Selection screen appears.

15 Press Enter to continue.

16 Select Upgrade ESXi, preserve VMFS datastore.

17 Press Enter.
A confirmation message appears.
18 Press **F11** to upgrade. After the upgrade is completed, a confirmation message appears.

19 Remove the DVD from ESXi server, and press **Enter** to reboot.

20 After upgrading the ESXi server, the vSphere client has to be upgraded to version 6.0. Open the vSphere client machine and install version 6.0 by following the section “Install VMware vSphere Client” on page 50.

21 After ESXi server startup, open vSphere client and connect to ESXi server by providing root password.

22 Right-click the **ESXi Server**, and select **Exit Maintenance Mode**.

### 6.3.2 Configure ESXi Server

After you install the ESXi, you must configure the network settings and the ESXi password.

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.

#### 6.3.2.1 Configure IP Settings for ESXi

By default, the ESXi host server setup uses DHCP to get its IP address, subnet mask, and default gateway. You must use the following procedure to set the IP address of the ESXi Host server.

**To configure IP settings from the direct Console**

1. Press **F2** to customize the system.
2. Select **Configure Management Network**, and press **Enter**.
3 Select Network Adapters, and press Enter. The Network Adapter wizard appears.

4 Press SPACE BAR and press Enter to select the vmnic you want to connect to the management network.

   Attention
   * Recommended to use vmnic0.

5 Select IPv4 Configuration and press Enter.

6 Press Space bar to select Set static IPv4 address and network configuration option if the system uses Static IP addresses or select Use dynamic IPv4 address and network configuration option if the system uses dynamic IP address (DHCP).

7 Enter the IP address, subnet mask, and default gateway, and press Enter (only for Static IP configuration).

8 Press Esc.

9 Press Y to apply changes and restart the management network.

6.3.2.2 Configure the ESXi host DNS settings

To configure the ESXi host DNS settings
1 Press F2 to customize the system.
2 Select Configure Management Network, and press Enter.
3 Select DNS Configuration, and press Enter.
4 Press Space bar and press Enter to select the Use the following DNS server addresses and hostname.
5 Enter the primary server, an alternative server (optional), and the host name.
6 Press Esc.
7 Press Y to apply changes and restart the management network.
6.3.2.3 Change the ESXi host root password

You can use the direct console to set the password for the administrator account (root). During the ESXi software installation, the root (administrative user name for the ESXi host) password has been set. You change the password, if required.

Attention
To change the ESXi host root password is an optional procedure.

To change the root password

1. Press F2 to customize the system.
2. Select Configure Password, and press Enter.
   
   Attention
   If a password is already set up, type the password in the Old Password line, and press Enter (Optional).

3. In the New Password line, type a new password, and press Enter.
4. Retype the new password, and press Enter.
6.4 Install and configure vSphere Client

6.4.1 Install VMware vSphere Client

After the ESXi host is installed, the management network configured and the host password defined; you can manage the host using the vSphere Client. The vSphere Client is the management node for the ESXi host. The vSphere Client software must be installed on a computer serving as a management workstation with network access to the ESXi host. The vSphere Client can be installed on any workstation grade computer where Windows client operating system is running (For example, Windows 10 Professional).

In PMD Virtualization a non-RAID T5810/T3600XL machine with Windows 10 64-bit operating system is normally used for the vSphere Client.

Note
VMware vSphere Client / vSphere Web Client also supported in Windows 7 Professional.

To install VMware vSphere Client

1. In the vSphere Client machine, insert the vCenter 6.0 DVD and connect the DVD to vCenter Server.
2. Right-click autorun executable and Run as administrator.

Note
If User Account Control popup appears, then click OK.

The vmware vSphere window appears.

3. Select vSphere Client under VMware vCenter Desktop Client on left pane.
4. Click Install.
5 The files are extracted and **InstallShield Wizard** appears.
6 Select the language for the installation as **English (United States)** and click **OK**.
   The **Welcome to the installation wizard for VMware vSphere Client 6.0** dialog box appears.
7 Click Next. The End-User Patent Agreement page appears.

8 Select I agree to the terms in the license agreement and click Next. The Destination Folder dialog box appears.
9 If you want to change the installation path, click **Change** and type the desired path or continue with the default path.

10 Click **Next**.
   The **Ready to Install the Program** dialog box appears.

11 Click **Install**.
   After the installation is complete, the Installation Completed dialog box appears.
6.4.2 License the ESXi Server

The licensing must be performed for all ESXi host, that is, production and management ESXi hosts.

To license the ESXi Server
1. Launch the vSphere Client utility, VMware vSphere Client login window appears.
2. Provide the IP Address or Host name, User name, and Password to connect to the Host.
3. In the left pane, select the ESXi Host name or IP Address, and in right pane, select Configuration tab.

12 Click Finish.
4 Under **Software**, click **Licensed Features**. The **ESX Server License Type** window appears.

5 Click **Edit**. The **Assign License** dialog box appears.
6 Select Assign a new license key to this host and click Enter Key. The Add License Key dialog box appears.

7 Type the new license key, and click OK.

8 On the Assign License window, click OK.

9 Ensure the license details is displayed under the ESX Server License Type.
6.5 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.

![Diagram of network configuration](image)

Figure 6: Example configuration of a management ESXi host with local storage

Use single vSwitch to connect to management router Level 2.5 router.

6.5.1 Configure the virtual switch for the management network

To configure the virtual switch for the management network

1. Launch the the vSphere client utility.
   The VMware vSphere Client login window appears.

2. Provide the IP Address or Host name, User name (root), and Password to connect to the Host.

3. On the vSphere Client, under Home > Inventory > Inventory view, locate the ESXi host.

4. Click Configuration tab, and then under the Hardware, click Networking.
Ensure vSwitch0 is already configured as the management network and connected with physical adapter vmnic0. In addition, it must display the IP address which you set during installation and configuration of the ESXi server.

Attention
A default virtual switch is created when installing VMware ESXi. This is the initial virtual switch you can view when looking at the network configuration of an ESXi host. This switch is labeled vSwitch0. This switch hosts the primary management network port.

6.5.2 Enable 1 Gbps network

For management network switch, Cisco 3560 is recommended for use.

To enable 1 Gbps network
1. On the vSphere Client, under Home > Inventory > Inventory view locate the ESXi host.
2. Click Configuration tab, and then under the Hardware, click Networking.
3. Click Properties.
The vSwitch0 Properties dialog box appears.
4. Click Network Adapters (vmnic0).
5. Click Edit.
The vmnic0 dialog box appears.
6. In the **Configured Speed Duplex** list, select **1000 Mb, Full Duplex**.
7. Click **OK**.
8. Click **Close**.

### 6.5.3 Configure the Virtual Switch port security settings

To protect virtual machines from intrusion, ensure that the virtual switch port security settings must not be modified from the default values.

#### To configure the Virtual Switch port security settings

1. On the **vSphere Client**, under **Home > Inventory > Inventory** view locate the ESXi host.
2. Click **Configuration** tab, and then under the **Hardware**, click **Networking**.
3. Click **Properties**.
4. Click **Ports** tab.
5. Select the virtual switch and click **Edit**.
6. Click the **Security** tab.
7. Ensure that the policy exception are as follows:

<table>
<thead>
<tr>
<th>Policy exception name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promiscuous Mode</td>
<td>Accept</td>
</tr>
<tr>
<td>MAC Address Changes</td>
<td>Reject</td>
</tr>
<tr>
<td>Forged Transmits</td>
<td>Reject</td>
</tr>
</tbody>
</table>

---
6.5.4 Connect physical network switches

After the configuration is completed, connect the network cable from management ESXI host’s first physical Ethernet port (vmnic0) to management network level 2.5 switch.
6.6 Create management virtual switch

To create management virtual switch
1 Log on to the Vsphere Client using management ESXi IP.
2 In the left pane, click the ESXi Server, in the right pan, click Configuration tab.
3 Under Hardware > Networking.
4 Click Add Networking.
The Add Network Wizard dialog box appears.
The Connect Types page appears.
5 Under Connect Types.
6 Click Virtual Machine.
7 Click Next.
The Network Access page appears.
By default, Create a vSphere standard switch is selected.
8 Click Use vSwitch0 (Management Network Created during ESXi installation).

9 Click Next.
The Connect Settings page appears.
10 In the Network Label box, type VM Management Network.
11 Click Next.
The Ready to Complete page appears.
12 Verify if one VMKernel Port (Management Network) and one Virtual Machine Port Group is added to vmnic0.

13 Click Finish.
6.7 Configure 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.
6.8 Install and configure Domain Controller

To install and configure Domain Controller

1 Create a virtual machine to host Domain Controller: to create a virtual machine, refer to the section “Create a virtual machine to host vCenterServer” on page 71.

6.9 Install and configure vCenter Server

Related topics
“Considerations for vCenter Server” on page 66
“Create a vCenter Server virtual machine” on page 67
“Setup and configure web client” on page 86
“Configure the vCenter Server” on page 91

6.9.1 Considerations for vCenter Server

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

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management host workload</td>
<td>The vCenter Server runs as a virtual machine on the management host in the virtual infrastructure. It is important to consider the number of virtual machines that run on the management host so that adequate resources are available. All template creation and storage should be encapsulated by the management host so that production workloads are not affected by this type of operation.</td>
</tr>
</tbody>
</table>
| Windows domain controller        | A Windows domain must exist before you create the vCenter Server. Ensure that a physical domain controller exists so that vCenter can communicate with or install a new Windows domain controller on the management host. The Windows domain controller must:  
  • Perform the role as a DNS server  
  • Use reverse lookup zones for all subnets in the infrastructure  
  • 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.  
  Windows domain controller must be created and configured before installing vCenter server. For more information, refer to the *Experion PKS Windows Domain and Workgroup Implementation for Windows Server 2016*.                                                                                       |
| vCenter Server Databases         | vCenter Server and vSphere Update Manager installations require a database, decide which database to use.  
If virtual infrastructure system is up to 5 ESXi hosts and 50 virtual machines:  
  • vCenter Server version of Embedded database (PostgreSQL) database package is supplied with the vCenter Server installation.  
  • Microsoft SQL Server 2012 Express database package is supplied with the vSphere Update Manager installation.  
If the virtual infrastructure you are creating is exceeding 5 ESXi hosts and 50 virtual machines, you must purchase and install a full version of Microsoft SQL Server 2014 for use with vCenter Server and vSphere Update Manager. Refer *Experion R500 Installing and Configuring SQL Server 2014 and vCenter Server 6.0* document for SQL configuration. |
6.9.2 Create a vCenter Server virtual machine

Use this section to create a virtual machine to host vCenter Server. The vCenter Server is installed with and configured to use the Microsoft SQL Server 2014 Express database.

Attention
- If the virtual infrastructure you are creating is exceeding 5 ESXi hosts and 50 virtual machines, you must purchase and install a full version of Microsoft SQL Server for use with vCenter Server and vSphere Update Manager. Refer Experion R500 Installing and Configuring SQL Server 2014 and vCenter Server 6.0 document for SQL configuration.

6.9.2.1 Domain user and group creation and security

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

To create domain accounts
1. In the Domain Controller, go to Start > Windows Administrative Tools > Active Directory Users and computers.
   The Active Directory Users and Computers dialog box appears.
2. Right-click Users and select New > User.
   The New Object – User dialog box appears.
3. In the First name, Initials, Last name, Full name boxes, type the required details.
4. In the User logon name box, type as Vcenteradmin.
5. Click Next.
6. Type the password and clear the User must change the password at next logon check box.
7. Select Password never expires check box.
8. Click Next and verify the details.
9. Click Finish.

10. Using the Active Directory Users and Computers console on the domain controller, create a security group called vCenterAdmin and vCenterVUM and then add the new domain users to the group. To create a security group:
      The Active Directory Users and Computers dialog box appears.
   b. Right-click Users and select New > Group.
      The New Object – Group dialog box appears.
   c. In the Group name box, type as vCenter Admin.
   d. Select Group scope as Global and Group type as Security.
   e. Click OK.
   f. Repeat the above procedure and create one more user named vCenterVUM.

11. Add the vCenter Server virtual machine to both the forward and reverse lookup of your DNS server. To add the vCenter Server virtual machine to both the forward and reverse lookup of your DNS server, perform the following steps:
   a. Open the domain controller, go to Start > Windows Administrative Tools > DNS.
      The DNS Manager dialog box appears.
   b. Under the Domain server name > Forward Lookup Zones, select the Domain Name.
      Ensure that the Server in which the VCenter is installed is listed with proper IP address.
c Right-click **Reverse Lookup Zones**, select **New Zone**.
The **New Zone** Wizard appears.
d Click **Next**.
The **Zone Type** page appears.
e Select **Primary Zone**, and click **Next**.
The **Active Directory Zone Replication Scope** page appears.
f Select **To all the DNS servers in this domain**: `<domain name>`, click **Next**.
The **Reverse Lookup Zone Name** page appears.
g Select **IPV4 Reverse Lookup Zone**, and click **Next**.
The **Reverse Lookup Zone Name** page appears.

![New Zone Wizard](image)

h Click **Network ID** and type the first three digits of the network ID.
i Click **Next**.
The **Dynamic Update** page appears.
j Select **Do not allow dynamic updates** check box.
Click Next.

The Completing the New Zone Wizard page appears.

Click Finish.

In the DNS Manager, select the newly created Zone, right-click and select New Pointer (PTR). The New Resource Record dialog box appears.
n  In the **Host IP Address**, type the **IP address** of the vcenter server Virtual Machine.

o  Click **Browse** and select **Name of your Domain Server Machine Name**.

p  Click **OK**.

q  Select the **Forward Lookup Zones**.

r  Click **OK**.

s  Select the **Domain**.

t  Click **OK**.

u  Select the **VCenter server name** from the list, and click **OK**.

v  Click **OK**.

---

**Attention**

Verify that the **fully qualified domain name** of the virtual machine where you install vCenter Server is resolvable. Verify that the DNS reverse lookup returns a fully qualified domain name when queried with the IP address of the vCenter Server.

---

### 6.9.2.2 Download the vCenter Server 6.0 U3 installer image

**To download the vCenter Server 6.0 U3 installer image from HoneywellProcess.com website**

1  Click the link: https://www.honeywellprocess.com/library/support/softwaredownloads/ Experion/VMware-VIMSetup-all-6.0.0-5202527.pdf.

2  Log on to the HoneywellProcess.com website.

   The **Software Download Datasheet** appears.

3  Click the **VMware-VIMSetup-all-6.0.0-5202527** link.
4 Click Save and select the appropriate folder to save the VMware-VIMSetup-all-6.0.0-5202527 file.

5 Extract the zip file and burn the vCenter Server 6.0 U3 installer ISO file to a DVD.

6.9.2.3 Create a virtual machine to host vCenterServer

To create a virtual machine to host vCenterServer

1 From the vSphere Client machine 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 created the management ESXi host.

2 After you have connected to the management ESXi host, then create a virtual machine, follow steps 3–26 to create a virtual machine.

   Attention
   * For the vCenter Server (management node) virtual machine configuration details, refer to the HPS Virtualization Specification, p/n EP03-700-100

3 Launch the vSphere Client utility.
   The VMware vSphere Client login window appears.

4 Provide the IP Address or Host name, User name and Password to connect to the vSphere Server.

5 Select the ESXi host, where the PMD node must be installed.

6 In the left pane, right-click ESXi Host name or IP Address and select New Virtual Machine.
   The Create New Virtual Machine wizard appears.

7 In the Configuration page, select Custom, and click Next.
   The Name and Location page appears.
8 In the **Name** box, type the required virtual machine name, and click **Next**.

⚠️ **Attention**
- The VM name can be different from the windows computer name. Do not use the special characters in Virtual Machine name. For example, !, $, #, %.

The **Storage** page appears.

9 Select the **Datastore** where the virtual machine file is stored, and click **Next**.

The **Virtual Machine Version** page appears.

10 Select **Virtual Machine Version: 11**, and click **Next**.

The **Guest Operating System** page appears.

11 Under **Guest Operating System**, select **Windows** and under **Version** list, select **Microsoft Windows Server 2008 R2**.

12 Click **Next**.

The **CPUs** page appears.

13 In the **Number of cores per virtual socket** list, select the number of virtual CPUs for the respective virtual machine. For specification information, refer to the *HPS Virtualization Specification document, p/n EP03-700-100*.

⚠️ **Attention**
- For more information about host CPU requirements, number of virtual socket, and cores per virtual socket, refer to the *Experion PKS with PMD Controller Virtualization User's Guide*.

14 Click **Next**.

The **Memory** page appears.
In the **Memory Size** list, select memory size, and click **Next**. For specification information, refer to the *HPS Virtualization Specification document, p/n EP03-700-100*.

The **Network** page appears.

16 In the **How many NICs do you want to connect** list, select number of **NICs** as 1 and select the **Network type** as **VM Management Network** switch from the list.

17 Select adapter as **E1000** for all the **NIC** from the list.

18 Select the **Connect at Power On** check box, and click **Next**.

The **SCSI Controller** page appears.
Retain the default settings, and click **Next**. The **Select a Disk** page appears.
Select **Create a new virtual disk**, and click **Next**. The **Create a Disk** page appears.
21 Set the **Disk Size**. For Disk Size specification information for different nodes, refer to the *HPS Virtualization Specification* document, p/n EP03-700-100.

22 Under **Disk Provisioning**, select **Thin Provision**.

23 Under **Location**, select **Store with the virtual machine**, and click **Next**. The **Advanced Options** page appears.
24 Under **Virtual Device Node**, select **SCSI (0:0)** from the list, and click **Next**. The **Ready to Complete** page appears.

25 Read through the **Settings** summary, and if required, click **Back**, and **Edit** the details.

26 Click **Finish**.

27 Install the supported Windows Server 2008 R2 on the virtual machine.

---

**Attention**

- 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.

28 Install VMware Tools:

a In the **vSphere Web Client** home page, click **vCenter Inventory Lists > Virtual Machine**. The list of Virtual Machine appears.
b Right-click on the required virtual machine select Guest OS > Upgrade VMware Tools…

The Upgrade VMware Tools window appears

- **Interactive Upgrade**
  - The disk image with VMware Tools will be mounted onto the virtual CD/DVD drive. The guest OS of the virtual machine must be running. Then, go to the console to run the VMware Tools Upgrade wizard from the virtual CD/DVD.

- **Automatic Upgrade**
  - VMware Tools will be upgraded without interacting with the guest OS. If required, the guest OS will be automatically rebooted. You can adjust the behavior using Advanced Options.

Advanced Options: 

[Upgrade] [Cancel]

c Select **Automatic Upgrade** option.
6.9.2.4 Install 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.

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 is established.
- Create domain users: Domain accounts are used as service accounts to facilitate the installation vCenter Server. These accounts control authentication between the different applications and strengthen the security of the management infrastructure.
  - Use the Active Directory Users and Computers console on the domain controller to add 2 domain users: vCenterAdmin and vCenterVUM.
  - Set the password expiry for each account to a long period of time or never to expire, depending on your site security policy.

To install vCenter Server
1. Add the VM created for the vCenter Server to the domain.
2. Log on to the newly created VM for the vCenter Server as a local administrative user, which is part of the Administrators group.
3. To add two domain accounts to the local administrators group:
   a. Go to Start > Windows Administrative Tools > Server Manager. The Server Manager dialog box appears.
   b. In the left pane, go to Configuration > Local Users and Groups > Groups.
   c. In the right pane, right-click Administrators and click Properties. The Administrators Properties dialog box appears.
   d. Click Add. The Select Users, Computers, Service Accounts, or Groups dialog box appears.
   e. In the From this location box, ensure that location is your Domain Server.
   f. Click Advanced. The Select Users, Computers, Service Accounts, or Groups dialog box appears.
   g. Click Find Now.
   h. Select vCenterAdmin and vCenterVUM groups and click OK.
   i. Click OK.
   j. Click Apply.
   k. Click OK.
4. Log on to the newly created vCenter Server virtual machine as the Domain Server Name\vCenterAdmin user.
5 In the vSphere Client machine, insert the vCenter 6.0 DVD and connect the DVD to vCenter Server.

6 When the AutoPlay dialog is displayed, select **RUN autorun.exe** to start the installer.

7 Under **VMware vCenter Server**, select **vCenter Server for Windows** and click **Install**.

The **Welcome to the VMware vCenter Server 6.0.0 Installer** page appears.

**Attention**

- From the **Control Panel**, verify if the required prerequisites software listed under **Prerequisites** section are installed, else click the hyperlink and follow the on-screen instructions to install the software.

8 Click **Next**.

The **End-User License Agreement** page appears.

9 Select **I accept the terms of the license agreement** check box and click **Next**.

The **Select deployment type** page appears.

10 Select **vCenter Server and Embedded Platform Services Controller** and click **Next**.

The **System Network Name** page appears.

11 Type the **System Name**.

12 Click **Next**.

The **vCenter Single Sign-On Information** page appears.
13 In the **Password** and **Confirm Password** boxes, type the password.

14 Click **Next**.

---

**Attention**

Ensure to enter a complex password, if the password does not satisfy the complexity requirement a message appears, click **OK** and enter the a complex password in the **vCenter Single Sign-On Information** page according to the password guidelines.

---

The **vCenter Server Service Account** page appears.

15 Select **Use Windows Local System Account** and click **Next**.

The **Database Settings** dialog box appears.
16 Select **Use an embedded database (vPostgres)** and click **Next**.

The **Configure Ports** page appears.

17 Retain the default port details.

![Configure Ports](image)

18 Click **Next**.

The **Destination Directory** page appears.

19 Click **Next**.

The **Customer Experience Improvement Program** page appears.

20 Ensure that **Join the VMware customer Experience Improvement Program** check box is unchecked.

21 Click **Next**.

The **Ready to Install** page appears.
Verify the details and click Install. The Installation progress page appears.

Click Next.

The vCenter Server installation setup automatically completes the installation. The Setup Completed page appears.
25 Click **Finish**.

### 6.9.2.5 Install VMware vSphere Web Client plug-in

The editing setting of a virtual machine running hardware version 10 is supported only with the vSphere Web Client. After upgrading to hardware version 10, you must use vSphere Web Client to perform the edit settings.

You must install Google chrome and then you must install vSphere Web Client in the same computer where the vSphere Client is installed.

You must configure the vSphere Web Client using Google chrome.

**To install VMware vSphere Web Client plug-in**

1. To launch the **vSphere Web Client** from internet browser, type `https://vCenter IP address:9443/vsphere-client/`.

2. Press **Enter**.
   - If you get a security warning, click **Proceed anyway**.
Attention

In case you get a connection error, click **Advanced** and then click **Proceed**.

3 In the **vSphere Web Client** home page, click **Download the Client Integration Plug-in**.

The plug-in is downloaded
Close the browser, go to the folder where it is downloaded and double-click the `exe`. The VMware Client Integration Plug-in 6.0.0 wizard appears.

Click `Next`. The End-User License Agreement page appears.

Select I accept the terms in the License Agreement option.

Click `Next`. The Destination Folder page appears.

Click `Next`. The Ready to Install the Plug-in page appears.

Click Install. After installation is completed, the Installation Complete page appears.

Click Finish.

### 6.9.3 Setup and configure web client

To configure the vCenter Server

1. Launch vCenter Server virtual machine and log in as **Domain\vCenterAdmin** user.
2. Download Acrobat Flash Player 15 or later offline installation. Select the check box to accept the terms and conditions, then click Install.
3. Select the Never check for updates check box to disable updates, then click Done.
4 Open Server Manager for the vCenter Server.

5 In right pane, click Configure IE ESC under Security Information.
   The Internet Explorer Enhanced Security Configuration dialog box appears.
6 Select **Off** for both **Administrators** and **Users**.
7 Click **OK**.
8 Download and Install **IE11**.

9 Click **Start > VMware Web Client**.
10 Take note of the address on Internet Explorer’s address bar. It will look something like this: “https://vCenterMachine.vCenterDomain.local/vsphere-client/”. This is the address you should use in Internet Explorer on your Virtual Infrastructure Management Node. The first part of the address (up to the third forward slash) is what will be required later in the Trusted Sites configuration below. Once you know how to connect to your vCenter server, log into your Virtual Infrastructure Management Node using a standard user account. Alternatively, if you intend for the \administrator account on your vCenter VM to be able to launch the web client, you can use these same instructions on that node.

11 Login to the machine you’re planning to use to connect to vCenter. Note that you need only belong to the “Users” group on this machine.

12 Launch Internet Explorer. If prompt appears asking to setup the Internet Explorer defaults, choose recommended settings and close the dialog.
13 Click **Setting** icon and select **Internet Options**.
14 Click **Security** tab and then click **Trusted sites**.
15 Click **Sites** button.
16 Check that the correct address is already entered in the **Add this website to the zone** textbox. If not, enter the website address. For example, if your vCenter server was renamed **vCenterMachine** and joined to the domain **vCenterDomain.local**, then the website would look like: https://vCenterMachine.vCenterDomain.local.
17 Click the **Add** button.
18 Click **Close** to dismiss the dialog box.
19 Click **OK** in **Internet Options** dialog box.
20 Internet Explorer will show a page **There is a problem with this website’s security certificate**. On the page, click the hyperlink **Continue to this website (not recommended)**.

**Note**

In case error found while opening the web client page like Page could not be found, then please download the Microsoft security patch “MS14-065” in the system.

21 At the login screen, wait until the **Download Client Integration Plugin** appears.
22 Click on the hyperlink and follow prompts to install. You will need to get this from another machine if the client does not have internet access (Just copy the url and download the file from the internet. “https://vsphereclient.vmware.com/vsphereclient/VMware-ClientIntegrationPlugin-6.0.0.exe”).
23 After the client is installed, restart Internet Explorer.
Navigate to the address of your vCenter web client, noted above.

If you see a dialog asking if you want to run the program VMware Client Integration Plug-in, de-select the check box Always ask before opening this type of address and click on the Allow button.

Login using the administrator@vsphere.local account as the user name.

6.9.4 Configure the vCenter Server

Prior to adding ESXi hosts to the vCenter Server, you must configure it. To configure the database retention policy and logging options, the vSphere Web Client must be connected to a vCenter Server system.

To configure the vCenter Server

1. To launch the vSphere Web Client from internet browser, type https://vCenter IP address:9443/vsphere-client/.
2. Press Enter.
   If you get a security warning, click Proceed anyway.
3. In the vSphere Web Client home page, log on with user name and password used while installing vCenter server. (Refer to the Step 13, in the section “Install vCenter Server” on page 79).
4. Click Login.
   The vSphere Web Client window appears.
5. Click Home > Administration > Configuration.
6. In the main pane, select the Identity Sources tab.
7. Click the Add Identity Source (+) button to add the required domain.
8 The **Add identity source** window appears.
9 Select **Active Directory (Integrated Windows Authentication)** and ensure that **Use machine account** is selected under **Domain name**.
10 Click **OK**.
11 In main pane, click **Home > Host and Clusters**.
12 Click **Manage** tab.
13 Click **Permissions** sub tab
14 Click the **Add permission (+)** button to add the required permission. The **Add Permissions** dialog box appears.
15 Click **Add**.

The **Select Users/Groups** dialog box appears.
16 Select the local domain from Domain dropdown and select vCenterVUM and vCenterAdmin user accounts.

17 Click Add.

18 Click OK.

19 In the Add Permissions dialog box, from Assigned Role list, select Administrator.
20 Click **OK**.

21 Log off and then log on to the **vSphere Web Client** with administrative privileges. The **vSphere Web Client** home page appears.

22 Click **vCenter Inventory Lists > vCenter Servers**, double-click the **vCenter Server**.

23 In the right pane, click **Manage > Settings**, click **Edit**.
The Edit vCenter Server Settings dialog box appears.

24 Click Logging Settings.

Attention
- 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 Info (Normal logging) to reduce the size of the logs maintained on the vCenter Server.

25 From the Logging options, select required logging options. Option Description are as follows:
• **None (Disable logging):** Turn off logging
• **Error (Errors only):** Display only error log entries
• **Warning (Errors and warnings):** Display warning and error log entries
• **Info (Normal logging):** Displays information, error, and warning log entries
• **Verbose (Verbose):** Displays information, error, warning, and verbose log entries
• **Trivia (Extended verbose):** Displays information, error, warning, verbose, and trivia log entries

26 Click **OK**.

27 Click **Database**.
Attention

- The vCenter Server stores the task, event, and performance data in the vCenter database. Over time, this collection of data continues 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. 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 limits the retention of these events to 60 days.

28 In the Task retention box, type the value in days. Information about tasks performed on this vCenter Server system is discarded after the specified number of days.

29 In the Event retention box, type the value in days. Information about events for this vCenter Server system is discarded after the specified number of days.

30 Click OK.

Attention

- Changes to the logging settings take effect immediately. Do not restart vCenter Server system.
6.10 Install VMware vSphere Update Manager

To install VMware update manager, perform the below steps

1. Ensure that you are logged into the vCenter Server virtual machine as the Domain\vCenterAdmin user.
2. Open the VMware Install content, click on auto run
   The VMware vCenter Installer window appears.
3. Click Server option under VMware vSphere Update Manager.
4. Select Use Microsoft SQL Server 2012 Express as the embedded database check box and then click Install.
5. On the Language selection dialog, select the applicable language and then click OK.
   The Welcome to the InstallShield... window appears.
6 Click Next. The License Agreement window appears.

7 Select I accept the terms in the license agreement and click Next. The Support Information window appears.

8 Uncheck the Download updates… check box, then click Next.
The **vCenter Server Information** window appears.

![vCenter Server Information Window]

9 Accept the default IP Address and Http port settings. Add the **Domain\vCenterVUM** user and password details, then click **Next**.

The **VMware vSphere Update Manager Port Settings** window appears.

![VMware vSphere Update Manager Port Settings Window]

10 Accept the default values and click **Next**.
The Destination Folder window appears.

11 Click Change for the downloading patches location.

12 Use the same path but change the C: to a D: so that the patches are stored on the D drive.

Note
If prompted about Free space on the selected drive… then click OK.

13 The Ready to Install the Program window appears.

14 Click Install.

15 The installer completes the installation. After installation complete, the InstallShield Wizard Completed window appears.

16 Click Finish to complete the Installation and exit the Installer screen.

17 Click Start > Administrative Tools > Services.

The Services window appears.
18 From the Services window, select VMware vSphere Update Manager service, right-click and choose Properties.
   The Properties dialog box appears.

19 On Log On tab, select This account option.
20 Enter the Domain\vCenterVUM account for the service.
21 Click Apply and click OK.
22 The Services popup appears, click OK.
23 From the Services window, right-click on the Vmware vSphere Update Manager Service and select Restart.
6.11 Install the VMware vSphere Update Manager plug-in

To Install the VMware vSphere Update Manager plug-in

1. From the vSphere Client, click Plug-ins > Manage Plug-ins.. from the menu. The Plug-in Manager window appears.

2. In Available Plug-ins section at the bottom of the window, click Download and Install for the VMware vSphere Update Manager Extension plugin.

3. If prompted with the security warning, click Run.

4. Select the required Installation language then click OK.

5. The Welcome to the InstallShield Wizard….. window appears.
6 Click Next.
The License Agreement window appears.
7 Select I accept the terms in the license agreement and click Next.
The Ready to Install window appears.
8 Click Install.
9 If prompted by a User Account Control dialog, click Yes.
10 The installer completes the installation. After installation complete, the InstallShield Wizard Completed window appears.

11 Click Finish.
12 If prompted by a certificate security warning dialog, select the Install this certificate… check box and click Ignore.
13 Click Close to close the Plug-in Manager.
6.12 Configure VMware vSphere Update Manager

To Configure VMware vSphere Update Manager

1. Open vSphere Client and click Home.

2. Double-click Update Manager.

3. Select the Configuration tab.

4. On left pane, select Download Settings.
5 Clear all the check boxes under **Download Sources**.
6 Select **Download Schedule**, clear the **Enable scheduled download** option and click **Apply**.
7 Select **Notification Check Schedule**, clear the **Enable scheduled download** option and click **Apply**.
8 Select **Virtual Machine Settings**, select **Take a snapshot of virtual machines**… and select the **Keep for 18 hours** option and then click **Apply**.
9 Select **ESX Host/Cluster Settings**, clear the **Retry entering maintenance mode**… option, select the **Temporarily disable removable media devices**… option, and clear all other options on the page and click **Apply**.

>Note
For more details about vSphere Update Manger, refer to Experion PKS Virtualization Planning and Implementation Guide document
6.13 Upgrade virtual hardware version

The virtual machine created from vSphere client is with hardware version 8 and it must be upgraded to hardware version 10. First upgrade the domain controller hardware version to 10 and then upgrade the vCenter server hardware version to 10.

To upgrade virtual hardware version

1. Log on to the vSphere Web Client with administrative privileges.
   The vSphere Web Client window appears.
2. Click vCenter Inventory List > Virtual Machines.
   The list of Virtual Machine appears.
3. Select the required Virtual Machine, in the Summary section, click Edit Settings.

   ![VSphere Web Client](image)
   The Edit Settings dialog box appears.

4. Expand Upgrade.
5 Select the Schedule VM Compatibility Upgrade… check box.
6 Select the Only upgrade after normal guest OS shutdown check box.
7 In the Compatible with (*) list, select ESX 6.0 and later option.
8 Click OK.
9 Right-click Virtual Machine > Power > Restart Guest OS.
6.14 Install the Experion virtual machine utility

You must install the Experion virtual machine utility if the version of vCenter Server on your system is 6.0.

To install the Experion virtual machine utility

1. Connect to the ESXi host and open the console for vCenter Server.
2. On the vCenter Server machine, insert the latest Experion System Initialization R200.1 Updates media.
3. Navigate to \Packages\vCenter_utility\. Right-click Honeywell_vCenter_utility.exe file, and click Run as Administrator.
4. Click Install.
   After the installation completes, a confirmation dialog box appears.
5. Click OK to close the dialog box and launch the Experion Virtual Machine Maintenance Service Tool.
6. Enter the credentials for a user with the privileges to read/write/configure your virtual machines.
7. Click Start Service to optimize existing virtual machines to execute with Experion.

Attention

If you must 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 ExpVCControlPanel.exe file. The Experion Virtual Machine Maintenance Service Panel dialog box appears. If the service is already running, you must click Stop Service so that you can enter the new credentials.

This may occur if the server credentials change in response to IT Policies.
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.

**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.
6.16 VM auto startup and shutdown settings

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:

- Domain controller
- vCenter server
- Other management workload.

To enable VM auto start up

1. In the vSphere Web Client home page, click Home > Hosts and Clusters.
2. Select the required host, click Host.
3. Click Manage tab > Settings tab > VM Startup Shutdown option.
4. Click Edit.

The Edit VM Startup and Shutdown dialog box appears
5 Select the **Automatically start and stop the virtual machines with the system** check box.
6 In the **Startup Delay** box, type time as 120 seconds.
7 Click **Continue immediately if the VMware Tools starts** check box for the operating system to boot immediately after **VMware Tools** starts.
8 In the **Shutdown Delay** box, type time as 120 second to delay shutdown for each virtual machine by a certain amount of time.

<table>
<thead>
<tr>
<th>Attention</th>
</tr>
</thead>
<tbody>
<tr>
<td>This shutdown delay applies only if the virtual machine has not already shut down before the delay period elapses. If the virtual machine shuts down before that delay time is reached, the next virtual machine starts shutting down.</td>
</tr>
</tbody>
</table>

9 In the **Shutdown Action**, select shutdown action as **Shutdown Guest**.
10 Use **Move Up** and **Move Down** to specify the order in which the virtual machines start when the system starts.

Add the virtual machines to the Automatic Startup group in the following order:

- Windows domain controller
- vCenter Server
- EBR application
- Other management nodes

11 Click **OK**.
7 Implementing a production ESXi host

Implementation of a production ESXi host for production workloads.

Related topics
“Configure the ESXi host local disk array” on page 116
“Configure the ESXi host BIOS settings” on page 117
“Install and configure ESXi server” on page 118
“Add the ESXi host to the vCenter Server” on page 126
“Network configuration for a production host in a DCS architecture” on page 129
“Configure the Virtual Switch port security settings” on page 136
“Connect to physical network switches” on page 137
“Configure ESXi host time synchronization” on page 138
“Domain name resolution” on page 139
7.1 Configure the ESXi host local disk array

This section must be followed only if Honeywell factory is setting up the ESXi host server for PMD virtualization services. Prior to installing the ESXi software, you must prepare the local disk array on the ESXi host.

⚠️ **Attention**

This section is not intended for the customer if they are using their own ESXi host. This is a procedure to install and configure ESXi host for production, management, and application networks.

The Dell PowerEdge R730 XL should be pre-configured as RAID 10 with Hot Spare as shipped from Dell. If it is not configured as RAID 10 with Hot Spare then it must be configured manually.

**To configure the computer to use RAID 10 with Hot Spare in R730 XL platform**

1. To start the RAID Configuration Utility program, press `<Ctrl+R>` while booting up the computer.
2. Under *Virtual Disk Management (VD Mgmt)*, select *Controller 0* by using the UP/DOWN ARROW key.
3. Press F2 to view the options available.
4. Select *Create New VD* by using the UP/DOWN ARROW key.
5. Press Enter.
   - The *Create New VD* screen appears.
6. Press Enter.
7. Press Tab key to select the RAID Level row.
8. Press Enter to view the list of RAID Level available.
9. Select *RAID-10* from the list by using the UP/DOWN ARROW key, and then press Enter.
10. Press Tab key, to go to *Physical Disks* section.
11. Under *Physical Disks*, select drives 00:00, 00:01, 00:02, 00:03, 00:04, 00:05, 00:06, and 00:07 by using SPACE key.
12. Press Tab key, to go to *VD Name* field, under *Basic Settings* section.
13. Under *Basic Settings*, type *VD Name* in the *VD Name* field. For example: SYSTEM.
14. Press Tab key, to go to *Advanced Settings* section, and press SPACE key to select it.
15. Press Tab key, to move to *Initialize* row, and press SPACE key to select it.
16. Press Tab key, to move to *OK*, and press Enter.
   - Initialization deletes all the data in the virtual disk and a message appears, and prompts you to confirm deletion the data.
17. Select *OK* and press Enter to continue.
18. Press <Ctrl+N> to go to *PD Mgmt* window.
19. Under *Physical Disk Management*, select disk 00:08 by using the UP/DOWN ARROW key.
20. Press F2 to view the options available.
21. Select *Make Global HS* from the list.
22. Press Enter.
   - If a message appears, and prompts you to confirm that the global hot spare to give priority to the enclosure in which it resides. Then, select YES, and press Enter.
23. Press Esc to exit.
   - A confirmation message appears to exit, select OK, and press Enter.
7.2 Configure the ESXi host BIOS settings

Press F2 while booting up the computer, go to the BIOS Setup menu and set the following BIOS settings 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
Only enable the settings which are available.

- Node Interleaving disabled.
- Unused hardware disabled.
- Hardware clock is set to UTC.
- Power Management set to Maximum Performance (that is, disable Power Management).
- CD-ROM device should be set first in the BOOT sequence.

Press Save and exist.
7.3 Install and configure ESXi server

Related topics
“Install ESXi Operating System” on page 42
“Configure ESXi Server” on page 47

7.3.1 Install ESXi Operating System

The Honeywell Virtualization platforms must be installed using the Dell customized ESXi media.

The VMware ESXi installation media from VMware website does not contain the appropriate network drivers for the Broadcom NIC's that are part of this configuration.

A copy of the Dell customized ESXi media is available from the Honeywell Support Web site. For obtaining this media, refer to the instructions in the section “Download the Dell customized ESXi installer image” on page 42.

7.3.1.1 Download the Dell customized ESXi installer image

To download the Dell customized ESXi installer image from HoneywellProcess.com website

1. Click the link: https://www.honeywellprocess.com/library/support/software-downloads/Customer/VMware-VMvisor-Installer-201501001-2403361.x86_64.pdf
2. Log on to the HoneywellProcess.com website.
   The Software Download Datasheet opens.
3. Click the VMware-VMvisor-Installer-6.0.0.update03-5050593.x86_64- Dell_Customized-A00 link.
4. Click Save and select the appropriate folder to save the VMware-VMvisor-Installer-6.0.0.update03-5050593.x86_64- Dell_Customized-A00 file.
5. Extract the zip file and burn the ESXi software installer ISO file to a DVD.

7.3.1.2 Install ESXi 6.0 using the interactive mode

To install the ESXi 6.0 software, you must use the ESXi 6.0 DVD created in the section “Download the Dell customized ESXi installer image” on page 42.

To install the ESXi 6.0 software on the host server

1. Insert the ESXi 6.0 installable CD/DVD into the CD/DVD-ROM drive.
2. Restart the machine.
   The Welcome to the VMware ESXi 6.0.0 Installation screen appears.
3 Press **Enter** to continue with the installation.

The **End User License Agreement (EULA)** screen appears.

4 Read the VMware end-user license agreement, and press **F11** to accept it.

The **Select a Disk to Install or Upgrade** screen appears.

5 Select the disk drive on which you have to install **ESXi 6.0**, and press **Enter** to continue.

If there are two hard disks, select the one on which the OS is installed.

---

**Attention**

- Press **F1** for information about the selected disk. If the disk you selected contains data, the **Confirm Disk Selection** screen appears.

The **Please select a keyboard layout** screen appears.
6 Select **US Default**, and press **Enter** to continue.  
The **Please enter a root password (recommended) screen** appears.

7 Enter the **Root password** and **Confirm password**, press **Enter** to continue.

   **Attention**
   - Ensure to note down the root password, so that it can be used for future reference.

   The **Confirm Install** screen appears.

8 Press **F11** to start the installation.
   The installation begins and displays the progress.
   The **Install Complete** screen appears after installation is complete.

9 Remove the ESXi installation **CD/DVD**, and press **Enter** to reboot the host.

10 Press F2 while booting up the computer, go to the BIOS Setup menu and set the following BIOS settings on the ESXi host:
   - Change first boot sequence from CD-ROM device setting to first boot device to be the drive on which you have installed the ESXi host.

11 Press **Save** and exist.

### 7.3.1.3 Upgrade from ESXi 5.1/5.5 to ESXi 6.0

**To upgrade from ESXi 5.1/5.5 to ESXi 6.0**

1 In vSphere client workstation, log on to vSphere client using the credentials of root user.
2 Shut down all PMD nodes and then shutdown all running virtual machines.

Attention

The upgrade from ESXi 5.1/5.5 to ESXi 6.0 may cause some production downtime.

3 Select the ESXi server, and right-click and select Enter Maintenance Mode.

4 Click Yes.

The maintenance mode task completed message appears.

5 In the Recents tasks section, the details appear.

6 In the ESXi server, open the console of ESXi 5.1/5.5.

7 Insert the ESXi 6.0 media in the ESXi Server.

8 Press F12.

The Authentication screen appears.

9 Type the login name and password, and press Enter.

A confirmation message appears.

10 Press F11 to restart the server.

A confirmation message appears.

If you do not make any selection, it automatically boots from the installer.

11 Press Enter.

Wait for few minutes. The Welcome to the VMware ESXi 6.0.0 Installation screen appears.

12 Press Enter to continue with the installation.

The End User License Agreement (EULA) screen appears.

13 Read the VMware end-user license agreement, and press F11 to accept it.

The Select a Disk to Install or Upgrade screen appears.
Select the disk drive on which you have to install ESXi 6.0, and press Enter to continue.
If there are two hard disks, select the one on which the OS is installed.

Attention
Press F1 for information about the selected disk. If the disk you selected contains ESXi OS, the Confirm Disk Selection screen appears.

Press Enter to continue.

Select Upgrade ESXi, preserve VMFS datastore.

Press Enter.
A confirmation message appears.
18 Press F11 to upgrade. After the upgrade is completed, a confirmation message appears.

19 Remove the DVD from ESXi server, and press Enter to reboot.

20 After upgrading the ESXi server, the vSphere client has to be upgraded to version 6.0. Open the vSphere client machine and install version 6.0 by following the section “Install VMware vSphere Client” on page 50.

21 After ESXi server startup, open vSphere client and connect to ESXi server by providing root password.

22 Right-click the ESXi Server, and select Exit Maintenance Mode.

### 7.3.2 Configure ESXi Server

After you install the ESXi, you must configure the network settings and the ESXi password. 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.

#### 7.3.2.1 Configure IP Settings for ESXi

By default, the ESXi host server setup uses DHCP to get its IP address, subnet mask, and default gateway. You must use the following procedure to set the IP address of the ESXi Host server.

**To configure IP settings from the direct Console**

1. Press F2 to customize the system.
2. Select Configure Management Network, and press Enter.
3 Select **Network Adapters**, and press **Enter**.
The **Network Adapter** wizard appears.

4 Press **SPACE BAR** and press **Enter** to select the **vmnic** you want to connect to the management network.

   ![Image of Network Adapter wizard]

   **Attention**
   - Recommended to use vmnic0.

5 Select **IPv4 Configuration** and press **Enter**.

6 Press **Space bar** to select **Set static IPv4 address and network configuration** option if the system uses Static IP addresses or select **Use dynamic IPv4 address and network configuration** option if the system uses dynamic IP address (DHCP).

7 Enter the IP address, subnet mask, and default gateway, and press **Enter** (only for Static IP configuration).

8 Press **Esc**.

9 Press **Y** to apply changes and restart the management network.

### 7.3.2.2 Change the ESXi host root password

You can use the direct console to set the password for the administrator account (root). During the ESXi software installation, the root (administrative user name for the ESXi host) password has been set. You change the password, if required.

**Attention**
- To change the ESXi host root password is an optional procedure.

**To change the root password**

1. Press **F2** to customize the system.
2. Select **Configure Password**, and press **Enter**.
Attention

- If a password is already set up, type the password in the Old Password line, and press Enter (Optional).

3 In the New Password line, type a new password, and press Enter.
4 Retype the new password, and press Enter.
7.4 Add the ESXi host 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 new ESXi hosts to the vCenter Server**
1. To launch the **vSphere Web Client** from internet browser, type `https://vCenter IP address:9443/vsphere-client/`.
2. Press **Enter**.
   If you get a security warning, click **Proceed anyway**.
3. In the **vSphere Web Client** home page, type the network credentials for the vCenter server.
4. Click **Login**.
   The **vSphere Web Client** window appears.
5. Click **vCenter > Hosts**, in the right pane, under **Objects**, click **Add a Host** icon.
   The **Add Host** dialog box appears.
6. In the **Host name or IP address** box, type the **Host name or IP address**.
7. Under **Location**, select the location.
8. Click **Next**.
9. Under **Connection Settings**, in the **User Name** and **Password** box, provide the administration login credential of the host.
   A **Security Alert** dialog box appears.
10. Click **Yes**.
11 Verify the details, and click Next. The Assign License page appears.

12 If the ESXi host is already licensed, select the existing license, click Next.

13 Else assign a new license key to this host, click Next. The Lockdown Mode page appears.

14 Clear Enable Lockdown Mode check box, and click Next. The VM Location page appears.

15 Select the newly created data center.

16 Click Next.
17 Verify the details and click **Finish**.
   It takes few minutes to add the host to the vcenter.
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 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.

The host shown in the image is configured to use the on-board 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 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 network port from each of the external 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.

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 above.

<table>
<thead>
<tr>
<th>Virtual switch</th>
<th>VMkernel port</th>
<th>Virtual machine port group</th>
<th>Uplink</th>
<th>Speed and duplex value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSwitch0</td>
<td>Management network name</td>
<td>None</td>
<td>vmnic0 (connected to management physical switch A) vmnic1 (connected to management physical switch B)</td>
<td>1000/Full</td>
</tr>
<tr>
<td>vSwitch1</td>
<td>None</td>
<td>FTE Yellow 1</td>
<td>vmnic2 (connected to FTE yellow physical switch)</td>
<td>100/Full</td>
</tr>
<tr>
<td>vSwitch2</td>
<td>None</td>
<td>FTE Green 1</td>
<td>vmnic3 (connected to FTE green physical switch)</td>
<td>100/Full</td>
</tr>
</tbody>
</table>
7.5.1 Configure virtual switch for the production network

To configure the virtual switch for the production network

1 Log on to the vSphere Web Client with administrative privileges.
   The vSphere Web Client home page appears.
2 Click Home > Hosts and Clusters, click Hosts.
3 Select the Host, right-click the Host and select Add Networking.

The Add Networking dialog box appears.
4 Under Select connection type, select Virtual Machine Post Group for a Standard Switch option.
Click Next.
The Select target device page appears.

Under Select target device, select New standard switch.

Click Next.
The Create a Standard Switch page appears.

In the Create a Standard Switch, click Add adapters icon.
The **Add Physical Adapters to the Switch** dialog box appears.

In the **Network Adapters** list, select the required adapter, and click **OK**.
10 The newly created adapter is added under **Active adapters** list, click **Next**. A confirmation message appears.

**Physical Network Adapters Warning**

There are no active physical network adapters for the switch.

Click OK to continue or Cancel to review your changes.

11 Click **OK**.

The **Connection Settings** page appears.

12 In the **Network Label** box, type the **Network label** name as **FTE Yellow**.
13 Click Next.
The Ready to Complete page appears.
14 Click Finish.

Attention
- Repeat the steps 5 to 14 to configure the FTE green switch.

7.5.2 To enable 1 Gbps network

To enable 1 Gbps network
1 Log on to the vSphere Web Client with administrative privileges.
The vSphere Web Client window appears.
2 Click Home > Hosts and Clusters, click Hosts.
3 Click Manage > Networking > Physical adapters.
4 Click Edit adapters settings.
The `vmnic – Edit Settings` dialog box appears.

5 In the `Configured Speed, Duplex` list, select **1000 Mb, Full Duplex**.

6 Click Close.
7.6 Configure the Virtual Switch port security settings

To protect virtual machines from intrusion, ensure that the virtual switch port security settings must not be modified from the default values.

To configure the Virtual Switch port security settings

1. Log on to the vSphere Web Client with administrative privileges. The vSphere Web Client home page appears.
2. Click Home > Hosts and Clusters.
3. Click Host.
4. Click Manage > Networking.
5. Select the required switch, and click Edit Settings.

Ensure that the policy exception are as follows:

<table>
<thead>
<tr>
<th>Policy exception name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promiscuous Mode</td>
<td>Reject</td>
</tr>
<tr>
<td>MAC Address Changes</td>
<td>Reject</td>
</tr>
<tr>
<td>Forged Transmits</td>
<td>Reject</td>
</tr>
</tbody>
</table>
7.7 Connect to physical network switches

After the configuration is completed, connect the network cable from vmnic2 and vmnic3 to yellow and green production network switches (level 2), respectively.
7.8 Configure 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. Log on to the **vSphere Web Client** with administrative privileges.
   The **vSphere Web Client** home page appears.
2. Click **vCenter Inventory Lists**.
3. Locate and select the ESXi host that requires time configuration.
4. Click **Configuration** tab.
5. Click the **Time Configuration** option.
6. At the top right of the page, click **Properties**.
   The **Time Configuration** dialog box appears.
7. Click **Options**.
   The **NTP Daemon (ntpd) Options** dialog box appears.
8. Click **NTP Settings** and then click **Add**.
   The **Add NTP Server** dialog box appears.
9. Type the IP address or host name of the NTP time server and then click **OK**.
10. 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.
11. 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.
7.9 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.
8 Installing of PMD nodes on a Virtual Machine

Related topics

“Install PMD Server” on page 142
“Install PMD HMI” on page 143
“Install PMD RHS” on page 144
“Install PMD Design Module” on page 145
8.1 Install PMD Server

The following table provides list of tasks to install virtual PMD Server.
Refer to the relevant sections in the *Experion PKS with PMD Controller Installation of PMD R900.1 on Virtual Server using ESIS* document.

<table>
<thead>
<tr>
<th>Task no</th>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate configuration files</td>
<td>Refer to the section <em>Generate configuration files.</em></td>
</tr>
<tr>
<td>2</td>
<td>Create and set up virtual machine</td>
<td>Refer to the section <em>Create and set up virtual machine.</em></td>
</tr>
<tr>
<td>3</td>
<td>Install operating system and Experion PKS</td>
<td>Refer to the section <em>Install operating system and Experion PKS.</em></td>
</tr>
<tr>
<td>4</td>
<td>VMware tool installation</td>
<td>Refer to the section <em>VMware tool installation.</em></td>
</tr>
<tr>
<td>5</td>
<td>Windows settings</td>
<td>Refer to the section <em>Windows settings.</em></td>
</tr>
<tr>
<td>6</td>
<td>Install PMD software</td>
<td>Refer to the section <em>Install PMD software.</em></td>
</tr>
<tr>
<td>7</td>
<td>Post-installation tasks</td>
<td>Refer to the section <em>Post-installation tasks.</em></td>
</tr>
<tr>
<td>8</td>
<td>Install Hot Fixes</td>
<td>Refer to the section <em>Install Hot Fixes.</em></td>
</tr>
<tr>
<td>9</td>
<td>Verify the system</td>
<td>Refer to the section <em>Verify the PMD Server system.</em></td>
</tr>
</tbody>
</table>
8.2 Install PMD HMI

The following table provides list of tasks to install virtual PMD HMI.
Refer to the relevant sections in the *Experion PKS with PMD Controller Installation of PMD R900.1 on Virtual HMI using ESIS* document.

<table>
<thead>
<tr>
<th>Task no</th>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Generate configuration files</td>
<td>Refer to the section <em>Generate configuration files.</em></td>
</tr>
<tr>
<td>2.</td>
<td>Create and set up virtual machine</td>
<td>Refer to the section <em>Create and set up virtual machine.</em></td>
</tr>
<tr>
<td>3.</td>
<td>Install operating system and Experion PKS</td>
<td>Refer to the section <em>Install operating system and Experion PKS.</em></td>
</tr>
<tr>
<td>4.</td>
<td>VMware tool installation</td>
<td>Refer to the section <em>VMware tool installation.</em></td>
</tr>
<tr>
<td>5.</td>
<td>Windows settings</td>
<td>Refer to the section <em>Windows settings.</em></td>
</tr>
<tr>
<td>6.</td>
<td>Install PMD software</td>
<td>Refer to the section <em>Install PMD software.</em></td>
</tr>
<tr>
<td>7.</td>
<td>Post-installation tasks</td>
<td>Refer to the section <em>Post-installation tasks.</em></td>
</tr>
<tr>
<td>8.</td>
<td>Install Hot Fixes</td>
<td>Refer to the section <em>Install Hot Fixes.</em></td>
</tr>
<tr>
<td>10.</td>
<td>Verify the system</td>
<td>Refer to the section <em>Verify the PMD HMI system.</em></td>
</tr>
</tbody>
</table>
8.3 Install PMD RHS

The following table provides list of tasks to install virtual PMD RHS.
Refer to the relevant sections in the *Experion PKS with PMD Controller Installation of PMD R900.1 on Virtual RHS using ESIS* document.

<table>
<thead>
<tr>
<th>Task no</th>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate configuration files</td>
<td>Refer to the section <em>Generate configuration files</em>.</td>
</tr>
<tr>
<td>2</td>
<td>Create and set up virtual machine</td>
<td>Refer to the section <em>Create and set up virtual machine</em>.</td>
</tr>
<tr>
<td>3</td>
<td>Install operating system and Experion PKS</td>
<td>Refer to the section <em>Install operating system and Experion PKS</em>.</td>
</tr>
<tr>
<td>4</td>
<td>VMware tool installation</td>
<td>Refer to the section <em>VMware tool installation</em>.</td>
</tr>
<tr>
<td>5</td>
<td>Windows settings</td>
<td>Refer to the section <em>Windows settings</em>.</td>
</tr>
<tr>
<td>6</td>
<td>Install PMD software</td>
<td>Refer to the section <em>Install PMD software</em>.</td>
</tr>
<tr>
<td>7</td>
<td>Post-installation tasks</td>
<td>Refer to the section <em>Post-installation tasks</em>.</td>
</tr>
<tr>
<td>8</td>
<td>Setting Remote Desktop Services</td>
<td>Refer to the section <em>Setting Remote Desktop Services</em>.</td>
</tr>
<tr>
<td>9</td>
<td>Install Hot Fixes</td>
<td>Refer to the section <em>Install Hot Fixes</em>.</td>
</tr>
<tr>
<td>10</td>
<td>Verify the system</td>
<td>Refer to the section <em>Verify the PMD RHS system</em>.</td>
</tr>
</tbody>
</table>
# 8.4 Install PMD Design Module

The following table provides list of tasks to install virtual PMD Design Module.

Refer to the relevant sections in the *Experion PKS with PMD Controller Installation of PMD R900.1 on Virtual Design Module using ESIS* document.

<table>
<thead>
<tr>
<th>Task no</th>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate configuration files</td>
<td>Refer to the section <em>Generate configuration files</em>.</td>
</tr>
<tr>
<td>2</td>
<td>Create and set up virtual machine</td>
<td>Refer to the section <em>Create and set up virtual machine</em>.</td>
</tr>
<tr>
<td>3</td>
<td>Install operating system</td>
<td>Refer to the section <em>Install operating system</em>.</td>
</tr>
<tr>
<td>4</td>
<td>VMware tool installation</td>
<td>Refer to the section <em>VMware tool installation</em>.</td>
</tr>
<tr>
<td>5</td>
<td>Run the install updates batch file</td>
<td>Refer to the section <em>Run the install updates batch file</em>.</td>
</tr>
<tr>
<td>6</td>
<td>Windows settings</td>
<td>Refer to the section <em>Windows settings</em>.</td>
</tr>
<tr>
<td>7</td>
<td>Create MNGR user</td>
<td>Refer to the section <em>Create MNGR user</em>.</td>
</tr>
<tr>
<td>8</td>
<td>Disable Administrator user</td>
<td>Refer to the section <em>Disable Administrator user</em>.</td>
</tr>
<tr>
<td>9</td>
<td>Install PMD software</td>
<td>Refer to the section <em>Install PMD software</em>.</td>
</tr>
<tr>
<td>10</td>
<td>Post-installation tasks</td>
<td>Refer to the section <em>Post-installation tasks</em>.</td>
</tr>
<tr>
<td>11</td>
<td>Install Hot Fixes</td>
<td>Refer to the section <em>Install Hot Fixes</em>.</td>
</tr>
<tr>
<td>12</td>
<td>Verify the system</td>
<td>Refer to the section <em>Verify the PMD Design Module system</em>.</td>
</tr>
</tbody>
</table>
9 Installing and configuring thin clients

To install and configure thin clients, refer to the sections Installing the Dell Wyse Z90DE7 Thin Client hardware and Configuring the Dell Wyse Z90DE7 Thin Client in the Wyse Z90DE7 Thin Client Planning Installation and Service Guide HWDOC-X280-en document.
10 Configuring the PMD nodes

For configuring the PMD nodes, refer to the *Experion PKS with PMD Controller Getting Started User’s Guide.*
11 Configuring the EBR application

You must use EBR to perform backups of the virtual infrastructure and virtual machines. EBR 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. 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.

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

To configure the EBR application. Refer to the Experion Backup and Restore R500.1 for PMD User’s Guide PMDOC-X111-en-900.
12 Administering of the virtualization environment

Related topics
“Monitor the virtualization environment” on page 154
12.1 Monitor 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 of callups or inconsistent refresh rates on displays. Using the Station Display Performance table in the Experion Station Specification document, 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 display inconsistency.

12.1.1 About resource usage

Virtual infrastructure resource usage is monitored using the performance charts in the vSphere Client. These performance charts help administrators view the resource usage and performance indicators in the virtual environment.

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.

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual machine CPU usage</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual machine CPU contention</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Disk I/O performance**

Disk I/O performance should be considered whenever monitoring virtual machines or the virtual infrastructure. Monitoring disk I/O usage helps to 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 Read latency and Write latency selected. Ensure that the virtual machine disk I/O latency runs below 25ms. Occasional spikes above 25ms are acceptable.  
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 Average write requests per second and Average read requests per second 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 HPS Virtualization Specification.  

**Memory performance**  
Memory usage in the 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 and view its advanced performance chart. Select the real-time memory chart with Balloon and Swap Used selected. Ensure that the ESXi host always has zero balloon and zero swap used usage as displayed in the charts.  
ESXi host memory usage | When monitoring ESXi hosts memory for usage select the ESXi host and view its advanced performance chart. Select the real-time memory chart with Active, Consumed and Granted 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 and view its advanced performance chart. Select the real-time memory chart with Active, Balloon, Consumed and Granted 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 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 Transmit packets dropped, Receive packets dropped, Data receive rate and Data transmit rate selected in the counters selection. Ensure that all transmit packets dropped and receive packets dropped show zero. View the Data receive rate and the Data transmit rate trends 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 and view its advanced performance chart. Select the real-time network chart with the virtual machine name selected in the objects selection and Data receive rate and Data transmit rate 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.

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Datastore performance</strong></td>
<td>When the total datastore performance or datastore usage statistics are required select the ESXi host 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 click the manage paths button) and select the <strong>Read latency</strong>, <strong>Write latency</strong> and <strong>Average commands issued per second</strong> in the counters selection. Ensure that <strong>Read latency</strong> and <strong>Write latency</strong> do not run higher than 25 ms. Occasional spikes above 25 ms are acceptable. Using the <strong>Average commands issued per second</strong> helps you to establish the IOPs on the whole datastore.</td>
</tr>
<tr>
<td><strong>Disk array performance</strong></td>
<td>When the total disk array performance or disk array usage statistics are required select the ESXi host 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 &gt; Storage Adapters device command) and select the <strong>Read latency</strong>, <strong>Write latency</strong> and <strong>Average commands issued per second</strong> in the counters selection. Ensure that <strong>Read latency</strong> and <strong>Write latency</strong> do not run higher than 25 ms. Occasional spikes above 25 ms are acceptable. Using the <strong>Average commands issued per second</strong> helps you to establish the IOPs on the disk array.</td>
</tr>
<tr>
<td><strong>Storage used</strong></td>
<td>When the total used space on each ESXi host datastore is required to use the ESXi host Configuration &gt; Storage command to see the total capacity and free space on each datastore. The storage views tab gives 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 displays a persistent alarm if this threshold is crossed.</td>
</tr>
</tbody>
</table>
13 Supplementary task

Related topics

“Export and import the virtual machine” on page 158
13.1 Export and import the virtual machine

Export and Import option in vSphere Web Client enables you to take manual backup of a VM in a single file format over network or in the local or external hard disk.

Export and Import option can be used for creating multiple VMs out of one single VM. The user can Export a single VM and deploy multiple times by changing the VM name using the PC Rename utility.

13.1.1 Export the VM file

To export the VM

1  In the vSphere Web Client home page, click vCenter Inventory Lists > Virtual Machine, click Virtual Machine.
   The list of Virtual Machine appears.
2  Right-click Virtual Machine, click Template > Export OVF Template.

![Export OVF Template dialog box](image)

The Export OVF Template dialog box appears.
3 In the **Name** box, type the **Name**. For example, type VM123.

4 In the **Directory**, the default location where the exported virtual machine template is saved appears. Click **Choose** to change the directory location, browse for the location where the exported virtual machine template is located.

5 In the **Format** list, select the required format. Select Physical Media (OVA) to package the OVF template into a **Single file (OVA)**.

6 In the **Annotation** box, type a description for the virtual machine if required.

7 Ensure that the **Enable advanced options** check box is unselected.

   **Note**
   The Enable advanced options have limited portability. Select Enable advanced options check box only when absolutely required.

8 Click **OK**.

### 13.1.2 Import the VM file

To import the VM

1 In the **vSphere Web Client** home page, click **Home > Hosts and Clusters**.

2 Right-click the **Host** and select **Deploy OVF Template**.
The **Deploy OVF Template** dialog box appears.

3 Under **Select Source**, click the **Local file** option. To change the location, click **Browse** and select the required location.

4 Click **Next**.
The Review details page appears.
5 Verify the details, and click Next.
The Select name and folder page appears.
6 In the Name box, type the name.
7 Under Select a folder or datacenter, select the location where the OVF template is stored.
8 Click Next.
The Select Storage page appears.
9 In the Select virtual disk format list, select disk format option.
   • Thick Provisioned Lazy Zeroed: Creates a virtual disk in a default thick format.
   • Thick Provision Eager Zeroed: A type of thick virtual disk that supports clustering features such as Fault tolerance.
   • Thin Provision: Use this format to save storage space.
10 Select the data store location to store the deployed OVF template, and click Next.
11 For each network specified in the OVF template, right-click Destination Network column to select a network to set up the network mapping.
12 On the IP Allocation menu, configure how IP addresses are allocated for the virtual appliance.
   This option does not appear if the deployed OVF template does not contain information about the IP scheme it supports.
13 Type the network protocol information.
   This option only appears if the OVF you deploy contains network properties.
14 Click Next.
15 Customize the deployment properties.
16 Click Next.
17 Select a binding service provider.
18 Click Next and click Finish.
14 Troubleshooting

Related topics
“TCP Checksum offload” on page 164
“FTE fails on PMD nodes and causes system to hang” on page 167
“Virtual machine time gets out of sync with NTP server” on page 177
“Virtual machine issues” on page 178
14.1 TCP Checksum offload

If you are using old network interface card you might get a network communication issue, these issues are due to TCP Checksum offload (TCO), so it is recommended to disable the TCO.

To disable TCO, you must perform the following:

- Enable SSH in the ESXi host: refer to “Enable SSH in the ESXi host” on page 164
- Log on to ESXi host through SSH and run the commands to disable the TCO: refer to “Log on to ESXi host through SSH and run the commands to disable the TCO” on page 165

Attention

Ensure to shutdown all the running machines, before you disable TCO.

Enable SSH in the ESXi host

2. Press Enter.
   If you get a security warning, click Proceed anyway.
3. In the vSphere Web Client home page, type the network credentials for the vCenter server.
4. Click Login.
   The vSphere Web Client window appears.
5. Click vCenter > Hosts, click Hosts.
6. Click Manage > Settings > Security profile.
7. Click Services > Edit.
   The Edit Security Profile dialog box appears.
8. In the **Startup Policy** list, select **Start and stop manually** option.

9. Click **Start**.
   
   A dialog box appears.

10. Click **OK**.

---

**Log on to ESXi host through SSH and run the commands to disable the TCO**

1. Connect the remote system/laptop in the same network of ESXi from where you are going to troubleshoot the ESXi.

2. To the remote system/laptop, download the Putty from http://www.putty.org/.

3. Double-click the **Putty.exe**.

4. In the **Host Name (or IP address section)** box, type the IP address of the ESXi server.

5. Click **SSH** option and click **Open**.

6. In the **Command Prompt** window, type the user name of the ESXi Host (root) and press **Enter**.

7. Type the **Password** for root.
Type the command `ethtool -k vmnic0 2>&1 | egrep 'tx|rx'` to display the current state of TCO on an adapter and press Enter.

For `vmnicx`, `x` is the physical NIC number of production network. For example, `ethtool -k vmnic0 2>&1 | egrep 'tx|rx'`.

The output similar to following appears.

- rx-checksumming: on
- tx-checksumming: on

To disable TCO in an ESXi host, use the commands:

- `ethtool -K vmnic0 rx off`
- `ethtool -K vmnic0 tx off`

⚠️ **Attention**

If there is any data transfer is going on you may not be able to disable the both rx and tx.

If you use Broadcom adapter, you may not be able to turn off the tx-checksum and an error message may appear as `cannot set device tx csum settings: function not implemented`. 
14.2 FTE fails on PMD nodes and causes system to hang

**Error Indication:** FTE fails on PMD nodes and causes the system to hang.

**Description:** Network connection icon will be in the network identifying mode for a long time and IP config from the command prompt displays empty. The management console application such as, task manager and server manager gets hanged. Shut down of the machine does not happen.

**Recovery:** Forcefully shutdown the machine from vCenter server, and select **Power off the virtual machine** option.

**Workaround:**

1. Log on to the vSphere Web Client with administrative privileges.
   The vSphere Web Client home page appears.

2. Click vCenter > Virtual Machine, double-click Virtual Machine.
   The list of Virtual Machine appears.

3. Select the required virtual machine, click Edit Settings.
   The Edit Settings dialog box appears.

4. Select Network adapter 1, click Remove.

5. Select Network adapter 2, click Remove.

6. Click OK.
   The network adapters are removed.
7 Right-click the virtual machine and click **Power on**.
8 Log on to the virtual machine which is part of the product administrator and administrator.
9 Wait until the system icon turns to x mark.

10 In the **Control Panel**, select **Network and Sharing Centre**.
    The **Network and Sharing Centre** window is displayed.
11 From the left pane, select **Change adapter settings**.
    The **Network Connections** window is displayed.
12 Select **Honeywell FTE Adapter**, and right-click **Honeywell FTE Adapter** and select **Properties**.
    The **Honeywell FTE Adapter Properties** dialog box appears.
13 Select Honeywell FTE Mux-IM Protocol Driver check box, and click Uninstall. A confirmation message appears.

14 Click Yes and wait for some time, once the uninstallation is completed, close the window.

15 Now the Network Connections window is empty, close the Network Connections window.

16 Right-click Command Prompt and click Run as Administrator.

17 In the Command Prompt, type `set devmgr_show_nonpresent_devices=1`.

18 Press Enter.

19 Type `start devmgmt.msc`.

The Device Manager window appears.
20 Click View > Show hidden devices.

21 Navigate to Network Adaptors.

22 Select the Intel (R) PRO/1000MT Network Connection network adaptor, right-click and select Uninstall. A confirmation dialog box appears.

23 Click OK.

24 Repeat the steps 22–23 for the other Intel (R) PRO/1000MT Network Connection #2 network adaptor.

25 Close the Device Manager window.

26 In the vSphere Web Client, click vCenter > Virtual Machine, double-click Virtual Machine. The list of Virtual Machine appears.

27 Select the required virtual machine, click Edit Settings. The Edit Settings dialog box appears.

28 In the New device list, select Network and click Add.

29 In the Adapter Type list, select the adapter type as E1000.

30 Select Connect At Power On check box.

31 Click OK.

32 Repeat the steps 28-30 to add second network adaptor.

33 Select the network adaptors and verify the MAC address.
34 For the network card which is having the least MAC address, select the **Network Label** as **FTE Yellow** and for other network card, select the **Network Label** to **FTE Green**.

35 Click **OK**.

36 Log on to the virtual machine.

37 Right-click **Command Prompt** and click **Run as Administrator**.

38 In the **Command Prompt**, type `ip config \ all`.

39 Note down the network adaptor having the least MAC address.

40 In the Control Panel, select **Network and Sharing Centre**. The **Network and Sharing Centre** window is displayed.

41 From the left pane, select **Change adapter settings**. The **Network Connections** window is displayed.

42 Right-click and rename as **FTE Yellow** and rename other network as **FTE Green**.

43 Right-click **FTE Yellow**. The **Intel (R) PRO/1000 MT Network Connection Properties** dialog box appears.

44 Click **Advanced**.

45 Select **Large Send Offload (IPV4)** as **Disabled**.

46 Select **Link Speed and Duplex** as **100 mbs Full Duplex**.
47  Click **OK**.

48  Repeat the steps 43-48 for FTE Green.

49  Click **Advanced > Advanced Settings**.

50  Ensure that FTE Yellow and FTE Green appears.
51 Click OK.

52 Select FTE Yellow, and right-click FTE Yellow and select Properties.
   The FTE Yellow Properties dialog box appears.

53 Select Internet Protocol Version (TCP/IPv4) check box.

54 Click Properties.
   The Internet Protocol Version (TCP/IPv4) Properties dialog box appears.

55 Click Use the following IP address option.

56 In the IP address, Subnet mask, and Default gateway boxes, type the IP details.

57 Click OK.

58 Select FTE Yellow, and right-click FTE Yellow and select Properties.
   The FTE Yellow Properties dialog box appears.

59 Click Install.
The Select the Feature Type dialog box appears.

60 Click Protocol.

61 Click Add.

The Select Network Protocol dialog box appears.

62 Select HONEYWELL and select the driver, which has the latest date.
Click **OK**.

The **Honeywell FTE Adaptor # 1** is created.

Right-click **Honeywell FTE Adaptor # 1** and rename to **Honeywell FTE Adaptor**.

elect **Honeywell FTE Adaptor**, right-click **Honeywell FTE Adaptor** and select **Properties**.

The **Honeywell FTE Adaptor Properties** dialog box appears.

Select **Internet Protocol Version (TCP/IPv4)** check box.

Click **Properties**.

The **Internet Protocol Version (TCP/IPv4) Properties** dialog box appears.

Verify if the new IP details are appearing in **Honeywell FTE Adaptor**.

Click **OK**.

Select **FTE Yellow**, right-click **FTE Yellow** and select **Properties**.

The **FTE Yellow Properties** dialog box appears.

Select **Honeywell FTE Mux-IM Protocol Driver** check box, and click **Properties**.

The **FTE MUX-IM Protocol Driver Properties** dialog box appears.

Click the **Configure** tab.
In the **Device Index Value**, update the **Device Index Value**.

**Attention**
- The Device Index Value is the last octet of the IP address set in the Honeywell FTE MUX Adaptor. For example, if IP address is 10.1.19.210, then 210 is Device Index Value

Click **OK**.

Log out and log on to HPSInstall user.

Wait until the machine has completed all the process starts and network connections, and then verify Network Settings using **ipconfig/all** command from a command window. If FTE Mux Driver is working correctly, **Honeywell FTE MUX-IM Virtual Miniport Driver** is displayed in the **ipconfig** command.
14.3 Virtual machine time gets out of sync with NTP server

**Error Indication**: VM time gets out of sync with NTP server.

**Description**: VM machine synchronizes time from ESXi host automatically during restart. If the ESXi host time is different than NTP server then VM machine gets a wrong time. This can happen if ESXi host is not configured to get the time from NTP server.

**Recovery**: Configure the ESXi host to get the time from NTP server and ensure all the ESXi host and VM machines are getting time from the same NTP source.

**Workaround**: For NTP configuration, refer to the *NTP configuration* sections in the *Experion PKS with PMD Controller Virtualization User’s Guide* document.
14.4 Virtual machine issues

You may encounter one or more of the following issues with the VM:

- A black screen on the virtual machine may appear when using Windows Server 2008 R2 as a guest operating system on ESXi 5.1.
- Slow mouse performance on Windows Server 2008 R2 virtual machine.
- Windows Server 2008 R2 virtual machine console appears to be frozen.

14.4.1 Virtual Machine black screen issue

If you are using ESXi 5.1, a new WDDM driver is installed with the updated VMware Tools and is compatible with Windows Server 2008 R2. The WDDM driver only works with hardware version 7 and above. But sometimes, a black screen on the virtual machine may appear.

To solve the black screen issue
1. Right-click Virtual Machine.
2. Select Edit Settings.
3. Change the video settings to 32 MB.
4. Ensure that VMware Tools is installed on the virtual machine.

14.4.2 Virtual Machine mouse or video performance issue

If the mouse or video performance is poor, replace the Display Adapter default-installed driver within the virtual machine with the driver contained in the wddm_video folder. The wddm_video folder is found on the virtual machine (for Windows Server 2008 R2 operating systems) in \Program Files\Common Files\VMware\Drivers. In addition, you have an option of copying it from a good working virtual machine.

To solve the mouse or video performance issue
1. Ensure that you are logged on as a user with administrator privileges.
2. Navigate to \Program Files\Common Files\VMware\Drivers, and copy the driver to a location on the virtual machine (for example, C:\). 
3. Within the virtual machine, right-click Computer > Manage > Diagnostics > Device Manager, then expand the Display Adapters.
4. Right-click the driver that is currently installed and chooses Update Driver Software. Browse to the folder where you have copied the new driver, select it, then follow the wizard.
5. Once the wizard completes, reboot the virtual machine.