

Experion PKS  
Virtualization with BladeCenter S

EPDOC-X241-en-B  
October 2014

Document	Issue	Date
EPDOC-X241-en-B		October 2014

## Disclaimer

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

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

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

Copyright 2014 - Honeywell International Sàrl

# Contents

<b>How to use this guide .....</b>	<b>5</b>
<b>Planning your Virtualization environment .....</b>	<b>7</b>
Introducing the BladeCenter S .....	8
Understanding the BladeCenter S chassis hardware .....	8
Planning the network architecture .....	14
Network requirements for management .....	16
Network requirements for DCS architecture .....	19
Network requirements for SCADA architecture .....	20
Planning your workload distribution .....	22
Understanding vSphere High Availability (HA) .....	22
Understanding vMotion and migration .....	23
Understanding shared storage .....	23
Availability considerations .....	24
Workload distribution tasks .....	25
Management workload distribution .....	28
Planning your datacenter layout .....	29
<b>Setting up hardware .....</b>	<b>31</b>
Verify shipment contents .....	32
Honeywell's provisioning of the BladeCenter S for Experion .....	33
Removing components from the chassis .....	35
Install the BladeCenter S chassis in a rack .....	36
Connecting the BladeCenter S to networks and power .....	41
<b>Configuring hardware to work with Experion virtualization .....</b>	<b>43</b>
Establishing remote web console connection to the BladeCenter S .....	44
Configuring the site specific management properties .....	46
Adjusting the production network properties .....	47
Backing up the AMM configuration .....	48
Setting the RSSM password .....	49
Verifying the hypervisor boot .....	50
Configuring an ESXi host .....	52
Configuring the ESXi host time synchronization .....	52
Updating vSwitch1 and/or vSwitch2 configuration .....	52
Preparing the vCenter server .....	54
Organizing your VMware inventory objects .....	55
Creating and updating high availability clusters .....	56
Creating an HA cluster .....	56
Adding a new host to an HA cluster .....	56
Migrating a VM to an HA cluster .....	57
Configuring the HA cluster VM options .....	57
Adding alarms to an HA cluster .....	57
Creating and managing virtual machines .....	59
<b>Administering the BladeCenter S system .....</b>	<b>61</b>
Monitoring the BladeCenter S .....	62
Moving a USB security device .....	63

Shutting down the chassis ..... 64

Starting up the chassis ..... 66

Removing and replacing modules ..... 67

**Glossary ..... 69**

**Notices ..... 73**

Documentation feedback ..... 74

How to report a security vulnerability ..... 75

Support ..... 76

Training classes ..... 77

# How to use this guide

This topic outlines the purpose of this guide, and its relationship with the *Experion Virtualization Planning and Implementation Guide*.

This guide gets you started with the BladeCenter S, which has been customized for easy install and configuration. *Virtualization with BladeCenter S* is also known as Honeywell's Premium Platform for Experion Virtualization Solutions. You will use this guide to plan your environment with the customized hardware. You will also use this guide to install and configure the hardware according to your plan. The guide is organized to show you:

- How to plan for a VMware-based virtualization environment with BladeCenter S, including workload distribution with shared storage.
- How to install the BladeCenter S and complete the configuration by providing site specific information.
- How to monitor the status of the BladeCenter S

This guide is your starting point to implementing Experion Virtualization with BladeCenter S, and is a companion to the *Experion Virtualization Planning and Implementation Guide*. There are instances where the Planning and Implementation guide is referenced rather than duplicating information in this BladeCenter S Guide. Both guides should therefore be available when planning and implementing your virtualization environment with the BladeCenter S.



# Planning your Virtualization environment

## Related topics

“Introducing the BladeCenter S” on page 8

*This topic lists the features of a virtualized system using BladeCenter S.*

“Planning the network architecture” on page 14

“Planning your workload distribution” on page 22

“Planning your datacenter layout” on page 29

*This topic provides guidelines for creating an organization hierarchy within vCenter Server.*

## Introducing the BladeCenter S

This topic lists the features of a virtualized system using BladeCenter S.

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

- The Experion production workload is consolidated on ESXi server grade hosts and connected to a production network. Each of the six Blade servers within the BladeCenter S is ESXi server grade hosts. The terms, ESXi hosts and Blade servers, therefore have the same meaning in this guide.
- The Blade servers 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 Blade servers are connected to the shared storage on a separate bus that is entirely embedded within the BladeCenter S chassis.
- The virtual infrastructure management workload can co-exist with the production workload on one or more ESXi hosts. This virtual infrastructure can be shared between production and application levels of the system.
- Use of vSphere High Availability (HA) and vMotion combined with workload distribution strategies offer optimum performance and minimal scope of loss.
- Thin clients provide user interaction with virtual desktops. No Experion application software is installed on the thin client.
- Workload backup and recovery strategies minimize downtime in the event of a virtual machine failure.
- Hardware and software update strategies maximize efficiency and minimize downtime and/or scope of loss.

Prior to implementing Experion virtualization with the BladeCenter S, it is recommended that you understand the key hardware features and how Honeywell has provisioned the hardware for optimal usage. This guide uses the terms:

- *BladeCenter S* to refer to the chassis as a whole entity with all its embedded components
- *Blade* or *Blade server* to refer to one of the six independent servers that run ESXi. A *Blade* or *Blade server* is an ESXi host.
- *Provision* or *provisioning* to refer to the tasks that Honeywell completed prior to shipping your BladeCenter S chassis
- *Configure* to refer to the set of tasks that must be completed on-site

## Understanding the BladeCenter S chassis hardware

This topic provides a graphic representation of the BladeCenter S chassis, and lists all hardware features included.

### Hardware features – front view

The figure below shows the key chassis hardware features that are visible from the front view of a BladeCenter S.



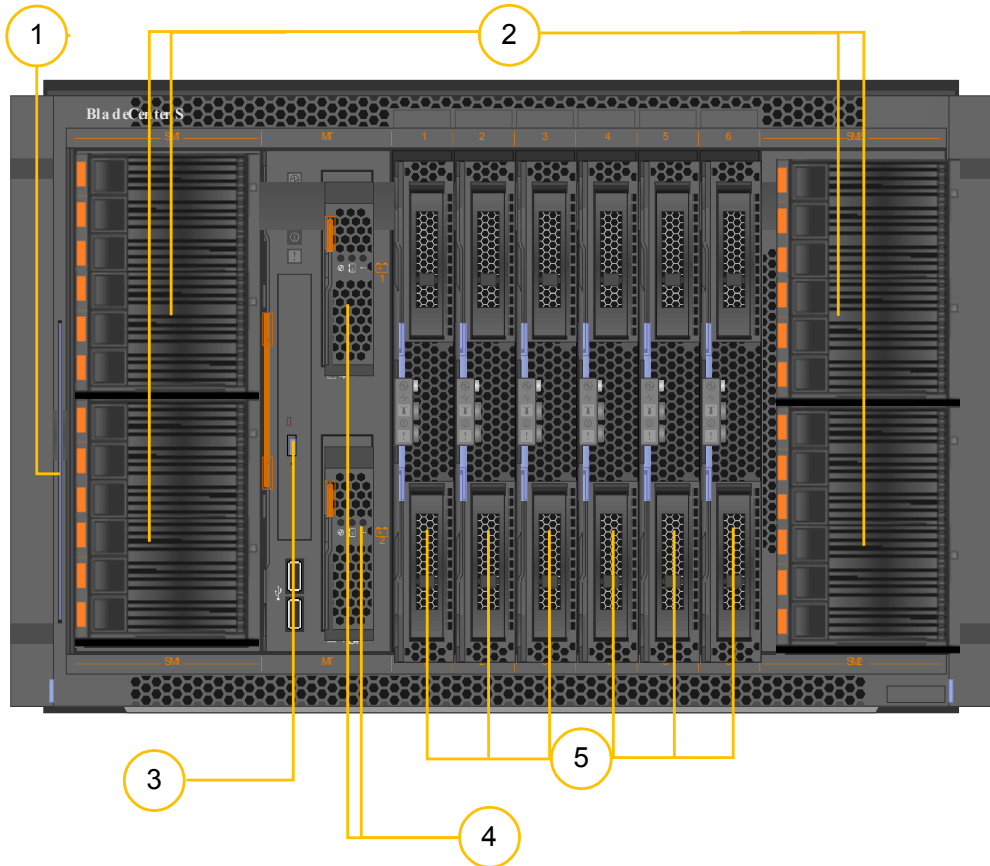



Figure 1: BladeCenter S features – front view

Callout	Description
1	<p>Service label and Microsoft Licensing cards slot</p> <p>This slot contains two blue service cards and one Microsoft license Certificate of Authenticity (COA) card. The blue service cards provide details of how to interpret the LED panels on either the front or back of the chassis. The COA card identifies an Embedded Windows® Server® Datacenter 2012 COA for each Blade server that is purchased with the BladeCenter S chassis. This COA card serves as your proof of purchase of the Microsoft licensing for the Blade chassis. Therefore, it is important to keep this card with the chassis. Note that the COA card is labeled with the serial number of the Blade chassis.</p>
2	<p>SAS disks</p> <p>Twenty four 2.5-inch SAS hard disk drives are split between two storage modules. The BladeCenter S with Experion uses the RAID storage solution. The hard drives and the redundant SAS RAID Controllers are the key components of the integrated shared storage subsystem. See the Raid Controller information in <i>Understanding the chassis hardware features - Back View</i> for high level storage architecture.</p>
3	<p>Media tray</p> <p>In addition to the two battery backup units, the media tray contains a single SATA multi-burner DVD drive and two USB 2.0 ports. The DVD drive and USB ports are shared by the Blade servers. Use the media-tray select button on the control panel of each Blade server to access the DVD drive or USB ports. The media tray also contains a system LED panel providing visible status information including over-temperature, power faults, and so on.</p> <div> <b>Tip</b> The USB ports in the media tray can be used to support security devices during Blade maintenance or failure.</div>

Callout	Description
4	<p>Battery backup units for SAS RAID controller</p> <p>Two battery backup units provide backup for the cache of the redundant SAS RAID controllers (see figure of Back View). The upper battery backup unit supports the top SAS RAID controller; the lower battery backup unit supports the bottom SAS RAID controller.</p>
5	<p>Blade Servers</p> <p>Each BladeCenter S chassis comes installed with the number of Blade servers ordered. Refer to the <i>HPS Virtualization Specification</i> for the Blade server types and associated specifics. This document is available from the Honeywell Process Solutions web site (<a href="http://www.honeywellprocess.com/">http://www.honeywellprocess.com/</a>)</p> <p>Blade servers are from the same BladeCenter server class with key characteristics that include high density and high performance.</p> <p>Each Blade has either 1 CPU or 2 CPUs. Those Blade servers with 2 CPUs have more memory. The single and dual CPU Blades are referred to as Performance A and Performance B, respectively. Neither the Performance A nor the Performance B Blades have local disk drives, however, each Blade comes pre-installed with an SAS expansion card that is required to access the integrated shared storage. Each Blade is provisioned to automatically boot from a volume that is pre-installed with ESXi.</p> <p>Use vSphere High Availability (HA) to recover from a Blade server failure within minutes. To enable use of vSphere HA, two Blade servers on the same chassis are paired together to form a vSphere HA cluster. The two Blades must be of the same specification (such as two Performance A or two Performance B Blades). See <i>Planning your workload distribution</i> for more details related to using vSphere HA with Experion.</p>

#### Hardware features – rear view

The figure below shows the key chassis hardware features that are visible from the rear view of a BladeCenter S.

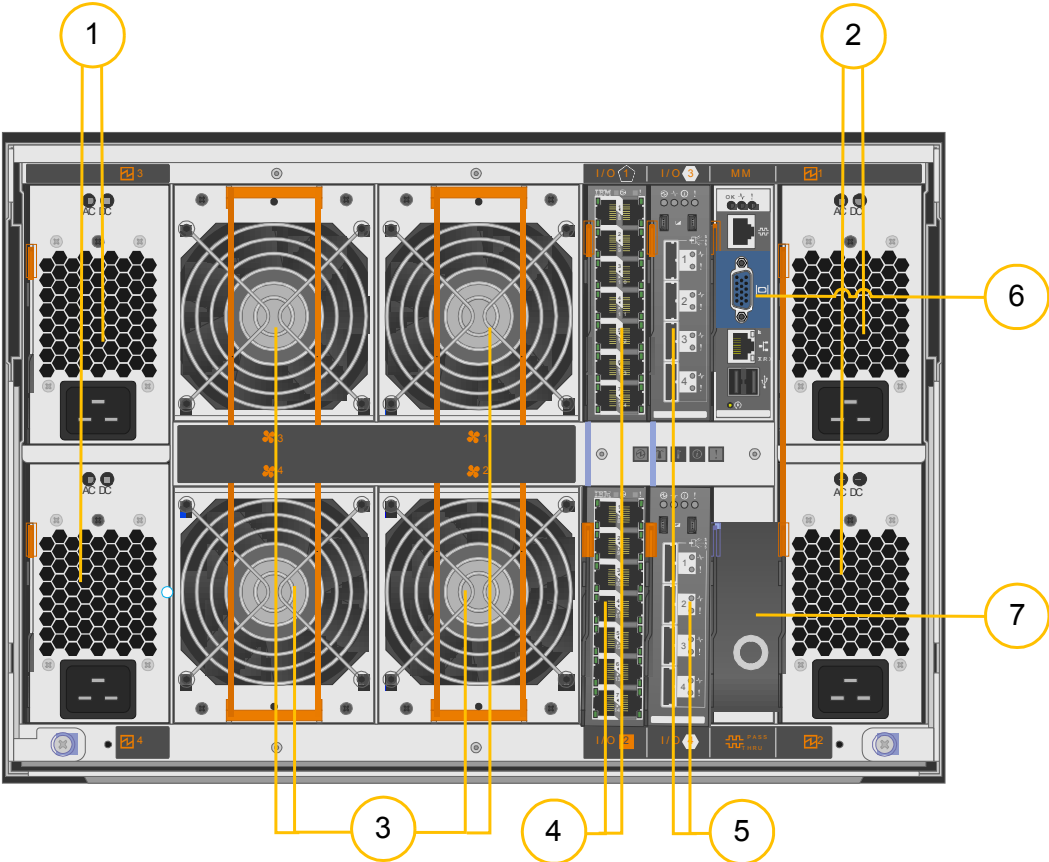


Figure 2: BladeCenter S features – rear view

Callout	Description
1 and 2	<p>Power supplies 1, 2, 3 and 4</p> <p>The four hot-swappable power supplies are able to auto-sense that the external power source is either 110 V ac or 220 V ac. In addition to supplying power to the chassis, each power supply has an internal fan that keeps the storage sub-system cool. Power supplies 1 and 2 provide cooling to storage module 1, while power supplies 3 and 4 provide cooling to storage module 2. The fan within the power supply will continue to operate if the external power is lost; that is, if the plug is disconnected.</p> <p>The BladeCenter S for Experion is provisioned to prevent an over-commitment of power usage that could adversely impact the system operation. This level of power management requires dual external power sources, preferably at 220 V ac. The recommended connection of power sources to power supplies is to connect power source 1 to power supplies 1 and 2, and power source 2 to power supplies 3 and 4. This minimizes cable crossings along the back of the chassis.</p> <p>The Blade chassis is provisioned to tolerate the loss of a single power supply without impacting the system operation.</p> <p>Each component within the Blade chassis contributes to the power usage. Each Blade chassis without Blade servers uses approximately 740 Watts. As expected, the Blade servers account for the majority of the power consumption.</p> <p>The Advanced Management Module (AMM) calculates the maximum power limit of the chassis based on two factors, one of which is VAC. The AMM will not allow one or more Blade servers to power on if the maximum power limit has been exceeded. The factors used by the AMM to calculate the maximum power limit of a chassis are:</p> <ul style="list-style-type: none"> <li>Each power supply is capable of supplying 950W if power source is 110 VAC, or 1450W if the power source is 220 VAC. The VAC for each power source must be the same.</li> <li>Power Management policy. Honeywell provisioning uses an n-2 policy with throttling, where <i>n</i> is the maximum number of power supplies. (In our case this is 4). This enforces a maximum power limit of 2250W for 110V, and 3422W for 220V.</li> </ul> <p>The AMM allocates a maximum power requirement of approximately 380w for each Performance B Blade server (MZ-PCVBP2). The AMM allocates a maximum power requirement of approximately 205W for each Performance A Blade server. Therefore, for a Blade chassis filled with 6 Performance B Blade servers running with 220V, the AMM allocates a maximum power requirement of 3020W, which is well below the enforce power limit of 3422W. For a Blade chassis filled with 6 Performance B Blade servers running with 110V however, the 3020W maximum power requirement exceeds the power limit of 2250W.</p> <p>If the maximum power limit enforced by the provisioned power management policy does not allow you to fill a chassis to desired capacity, consult with Honeywell Support to consider an alternative policy. Honeywell strongly discourages use of the “Basic Power Management” policy. Use the following instructions to adjust the policy to one that is suitable for your needs:</p> <ol style="list-style-type: none"> <li>From the menu pane of the AMM console, click <b>Monitors</b>.</li> <li>Select <b>Power Management</b> from the <b>Monitors</b> list.</li> <li>In the <b>Blade Center Power Domain Summary</b> section, select the link that indicates the current Power Management Policy. The provisioned value is <b>AC Power Source Redundancy with Blade Throttling Allowed</b>.</li> <li>Change the option to one of the following:                         <ul style="list-style-type: none"> <li><b>Power Module redundancy with Blade Throttling Allowed</b></li> <li><b>Power Module Redundancy</b></li> <li><b>AC Power Source Redundancy</b></li> </ul> </li> <li>Click <b>Save</b>.</li> </ol>
3	<p>Chassis cooling devices</p> <p>Each of the four hot-swappable fan modules contains two fans. These devices provide the cooling to the Blade servers and the IO modules. If one of the two fans fails within an individual fan module, the surviving fan will increase speed. If an entire fan module fails, then the fans in the surviving fan modules will increase speed.</p>

Callout	Description
4	<p>Intelligent Copper Pass-through Module (redundant)</p> <p>Redundant pass-through modules enable direct connection from the network ports of each Blade server to the external network infrastructure. The ports on both modules are provisioned for usage with separate management and production subnets. No further configuration is required for Blade servers that host L2 workload with FTE deployed with 1GB switches – simply connect the modules to the external network infrastructure using the guidelines in <i>Planning the network architecture</i>.</p> <p>Additional configuration is required for Blade servers hosting production workload running at different network settings than that set for FTE deployed with 1GB switches. For more information, refer to <i>Planning the network architecture</i> and <i>Configuring an ESXi Host</i>.</p>
5	<p>RAID controller (redundant)</p> <p>Redundant SAS RAID controllers enable the shared storage capabilities of the BladeCenter S. The storage is provisioned with:</p> <ul style="list-style-type: none"> <li>• RAID 10 with mirrors that span each storage module</li> <li>• Four hot spares (two in each mirror, or storage module)</li> <li>• Volumes created and mapped to LUNs, including the Blade boot volumes See <i>Honeywell's provisioning of the BladeCenter S for Experion</i> for detailed disk capabilities, including volumes created.</li> </ul>
6	<p>Advanced Management Module (AMM)</p> <p>The AMM is a hot-swappable module that manages the BladeCenter S components. It communicates with each Blade server to enable power-on requests, supports error and event reporting, and media tray usage requests. The AMM is provisioned with an IP address on the management subnet. To access the AMM console, you use a physical client. When setting up the BladeCenter S, you will be instructed to provide a minimal amount of site specific information to the AMM. The remainder of the AMM is already provisioned for usage.</p> <p>See <i>Monitoring the BladeCenter S</i> for information on how to monitor your BladeCenter S with AMM.</p> <p>An AMM failure would not impact the operation of running Blades. However, the AMM must be present and operational to start a Blade that is in the power off state. Therefore, it is essential that you restore operation to the AMM as soon as possible. If the AMM needs to be replaced, it must be provisioned to work with the target chassis.</p>
7	Empty

## Planning the network architecture

The BladeCenter S with Experion can be used with both DCS and SCADA architectures. Any of the documented topologies in the *Experion Virtualization Planning and Implementation Guide* are valid for use with the BladeCenter S. The supported topologies primarily address options for adding a management network for the virtual infrastructure to a typical Experion network infrastructure. The recommended topology that maximizes the features available with a BladeCenter S deployment is one with redundant management network. Unless otherwise noted, this guide assumes usage of a redundant management network.

The DCS and SCADA examples outlined in this section show that:

- One or more Blade chassis can be combined with existing bare metal and/or local storage virtualization platforms;
- For DCS, a single chassis can host workload from management, L2, L3 or L3.5 (Individual Blades have workload distribution constraints that are addressed later)
- For SCADA, a single chassis can host workload from management or SCADA (Individual Blades have workload distribution constraints that are addressed later)
- Blades are connected to external networks through the Intelligent Copper Pass-thru Module (ICPM). Both the management and production network connections are provisioned to run at 1GB. Note that connections to external networks (L2, L2.5, SCADA and so on) are at an individual Blade basis. This is represented in the diagrams with thicker lines from the chassis.
  - For example, in a fully populated chassis, there will be six pairs of management connections. For each chassis, there are an additional five connections: two for the SAS RAID controllers, two for the SAS switches, and one for the AMM connection.
  - Each Blade with a production workload is limited to one of the following:
    - One pair of yellow/green connections to FTE switches; or
    - One pair of connections to SCADA switches; or
    - One pair of connections to L3 routers; or
    - One pair of connections to L3.5 routers

Workload distribution is a key planning activity when deploying BladeCenter S with Experion. Refer to *Planning your workload distribution* for workload distribution considerations. In summary, as long as multi-level workload can be separated by a physical network, it can co-exist on a single Blade. For example, management and production workload can co-exist on the same Blade. In the DCS and SCADA examples that follow, note that there is no separate management host.

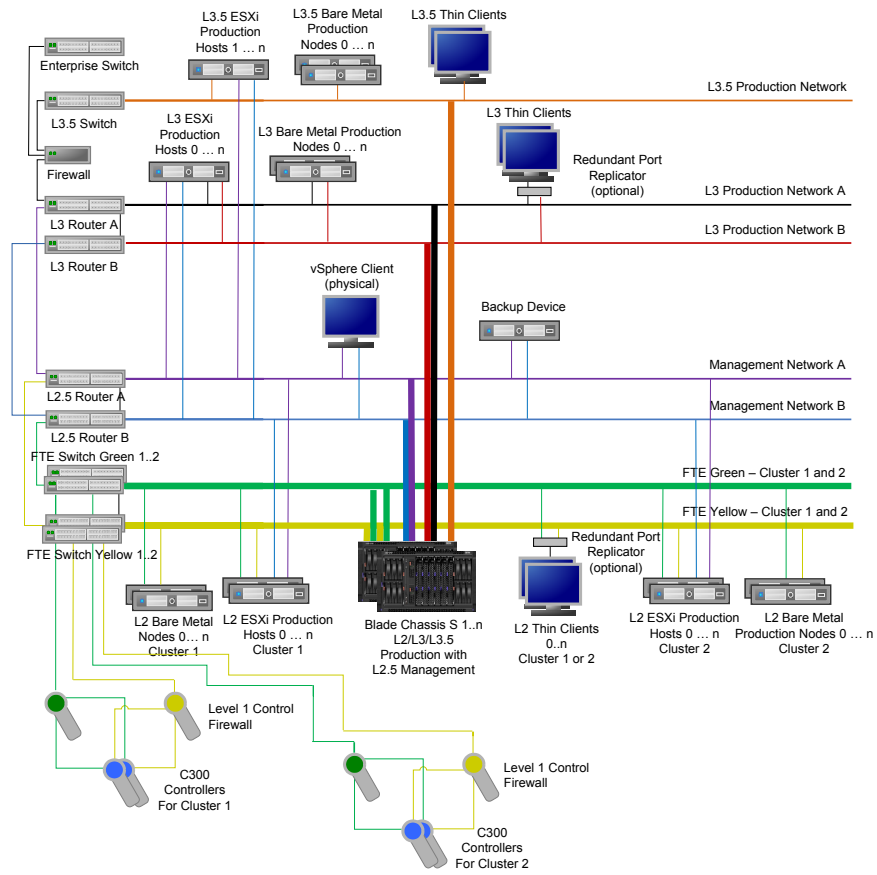


Figure 3: DCS architecture example with BladeCenter S

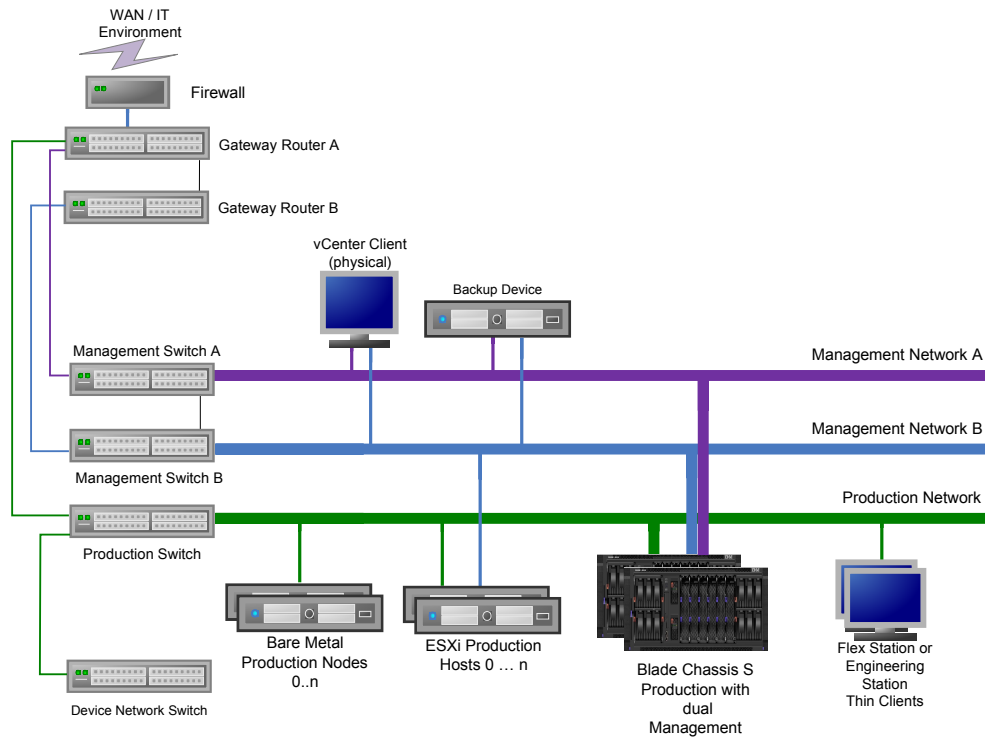


Figure 4: SCADA architecture example with BladeCenter S

### Related topics

“Network requirements for management” on page 16

*This topic describes how to connect the embedded elements of the BladeCenter S chassis to the management network, including the allocation of IP addresses and MAC address ranges.*

“Network requirements for DCS architecture” on page 19

*This topic explains how to connect Blade servers with DCS production workload from the internal side of the BladeCenter S to the DCS network infrastructure that is external to the chassis.*

“Network requirements for SCADA architecture” on page 20

*This topic outlines how to connect Blade servers with SCADA production workload from the internal side of the BladeCenter S to the SCADA production network infrastructure that is external to the chassis.*

## Network requirements for management

This topic describes how to connect the embedded elements of the BladeCenter S chassis to the management network, including the allocation of IP addresses and MAC address ranges.

The management network provides secured access to all elements of the virtual infrastructure. Each chassis embeds key elements of the virtual infrastructure, including the Blade servers, SAS RAID Controllers, Advanced Management Module (AMM) and Intelligent Copper Pass-thru Modules (ICPM). Each of these embedded elements requires a connection to the management network.

In addition to the elements within each chassis, the virtual infrastructure may also consist of vSphere clients, backup devices, or ESXi hosts with local storage. Use one or more instances of vCenter Server to manage one or more virtual infrastructures.

The management network is designed to deliver availability at the level required for each installation. The following example illustrates the management network connectivity for Blade 1 from the internal side of the



BladeCenter S to the network infrastructure that is external to the chassis. Blade 1 contains management workload as well as L2 workload.

- Each Blade server has four network adapters that are identified from bottom right to top right starting with vmnic0. The adapters are grouped together to indicate use of a multi port Network Interface Adapter. Each Blade is provisioned to connect vmnic0 and vmnic2 to the management network. This is a teamed connection where each adapter serves a unique primary role; one for management traffic and one for vMotion traffic. Additionally, each adapter serves as a standby adapter for the other. This teamed connection separates vMotion traffic so that there is no interference with the management traffic.
- On each ICPM, the ports are numbered from 1-7 starting from left side, top to bottom; numbered from 8-14 starting from right side top to bottom. The link speed and duplex is provisioned to auto detect for ports 1-14 on each ICPM. Ports 7 and 14 on ICPM in bay 2 are disabled. As shown in the diagram, for each Blade, connect vmnic 0 to ports 1-6 on ICPM in bay 2; connect vmnic 2 to ports 1-6 on ICPM in bay 1.
- Use ports 7 and 14 on ICPM in bay 1 to connect the redundant SAS RAID Controllers. These connections provide a communication path for status of the SAS RAID Controllers.
- The Advance Management Module (AMM) requires a single connection to the management network as illustrated in the diagram below.

Use the diagram below to connect each Blade server to the management network by matching the *vmnic n* from the Blade server with the port on either ICPM 1 or ICPM 2 that is labeled with Blade slot and *vmnic n*. The management connectivity is as shown below regardless of the type of production workload (i.e. FTE or SCADA or L3).

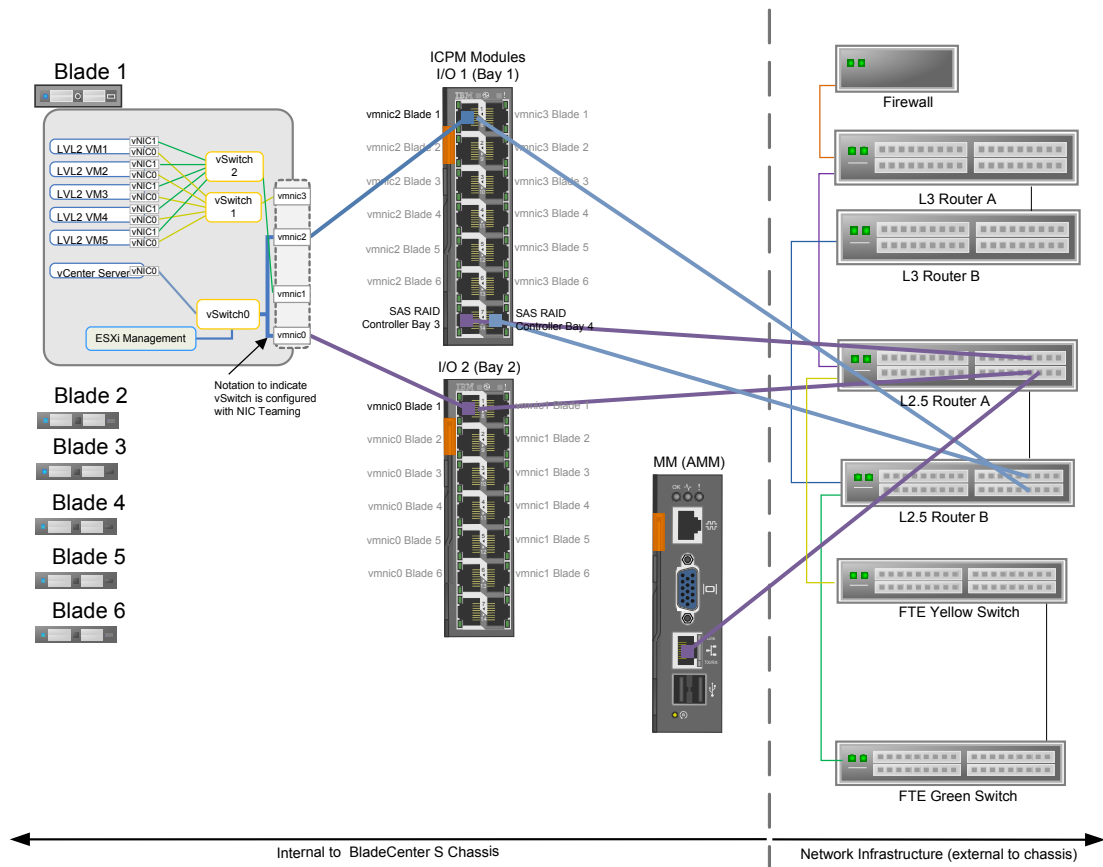


Figure 5: Connecting the BladeCenter S to the management network

#### Allocation of Management network IP addresses

Each BladeCenter S chassis is provisioned to connect to IP addresses on the management network that is defined as subnet 10.100.0.0, with subnet mask of 255.255.254.0 and gateway address of 10.100.0.1. IP

addresses have been reserved to allow multiple BladeCenter S chassis to connect to the same management network without duplication. Each BladeCenter S uses a range of twenty IP addresses.

Each BladeCenter S chassis uses the AMM to identify a unique DNS name and IP address. Identified below is the provisioned name and IP address for the AMM in the first deployed chassis. If another BladeCenter S chassis is deployed, its AMM is provisioned with the DNS name of **BCS02** and management IP address of **10.100.0.40**. Additional BladeCenter S chassis deployments use the next sequential DNS name and range of twenty IP addresses.

DNS Name	1st Management IP Address	2nd Management IP Address
BCSC01	10.100.0.20	None

Each Blade server within a single BladeCenter S chassis:

- has a unique DNS name that ties it to the chassis.
- is assigned two IP addresses to be used with redundant management network infrastructure, starting with the next sequential IP address after that assigned for the AMM.
- is uniquely provisioned to support redundant management connectivity with separation of vMotion traffic.
- Use the table below for an example of the DNS names and IP addresses assigned to the first deployed BladeCenter S chassis. DNS names associated with Blade server slots 1 through 6 for the second chassis deployed are *BCSC02-BS01*, *BCSC02-BS02*, *BCSC02-BS03*, *BCSC02-BS04*, *BCSC02-BS05*, and *BCSC02-BS06*. Any additional chassis deployed would be named with the next sequential numbering scheme.

BladeCenter Slot Number	DNS Name	1st Management IP address	2nd Management IP address
1	BCSC01-BS01	10.100.0.21	10.100.0.31
2	BCSC01-BS02	10.100.0.22	10.100.0.32
3	BCSC01-BS03	10.100.0.23	10.100.0.33
4	BCSC01-BS04	10.100.0.24	10.100.0.34
5	BCSC01-BS05	10.100.0.25	10.100.0.35
6	BCSC01-BS06	10.100.0.26	10.100.0.36

The shared storage subsystem of each BladeCenter S chassis requires four additional IP addresses for the management communication between the RAID controllers and internal SAS switches. The SAS Switch IP addresses for each I/O bay (3 and 4) are set at 8 or 9 plus the IP address of the AMM for the chassis.

The RAID Controller IP Addresses for each I/O bay (3 and 4) are set at 18 or 19 plus the IP address of the AMM for the chassis.

Use the table below for an example of the storage IP addresses assigned for the first chassis deployed.

IO Bay	SAS Switch IP Address	RAID Controller IP Address
3	10.100.0.28	10.100.0.38
4	10.100.0.29	10.100.0.39

### MAC address ranges

Each BladeCenter S chassis utilizes a range of MAC addresses to provision the Blade servers for hot replacement.

Use the table below to determine whether the provisioned MAC addresses conflict with existing MAC addresses. The first row in the table is the range assigned to the first BladeCenter S chassis deployed. Additional BladeCenter S chassis deployments are provisioned with the MAC address range as defined in the remaining rows.

Contact Honeywell support if you discover a duplicate MAC address already in use on the existing system.

DNS Name (AMM)	Management IP Address	Start MAC Address	End MAC Address
BCSC01	10.100.0.20	00:1A:64:76:00:00	00:1A:64:76:00:57
BCSC02	10.100.0.40	00:1A:64:76:00:60	00:1A:64:76:00:B7
BCSC03	10.100.0.60	00:1A:64:76:00:C0	00:1A:64:76:01:17
BCSC04	10.100.0.80	00:1A:64:76:01:20	00:1A:64:76:01:77
BCSC05	10.100.0.100	00:1A:64:76:01:80	00:1A:64:76:01:D7
BCSC06	10.100.0.120	00:1A:64:76:01:E0	00:1A:64:76:02:37
BCSC07	10.100.0.140	00:1A:64:76:02:40	00:1A:64:76:02:97
BCSC08	10.100.0.160	00:1A:64:76:02:A0	00:1A:64:76:02:F7
BCSC09	10.100.0.180	00:1A:64:76:03:00	00:1A:64:76:03:57
BCSC10	10.100.0.200	00:1A:64:76:03:60	00:1A:64:76:03:B7

## Network requirements for DCS architecture

This topic explains how to connect Blade servers with DCS production workload from the internal side of the BladeCenter S to the DCS network infrastructure that is external to the chassis.

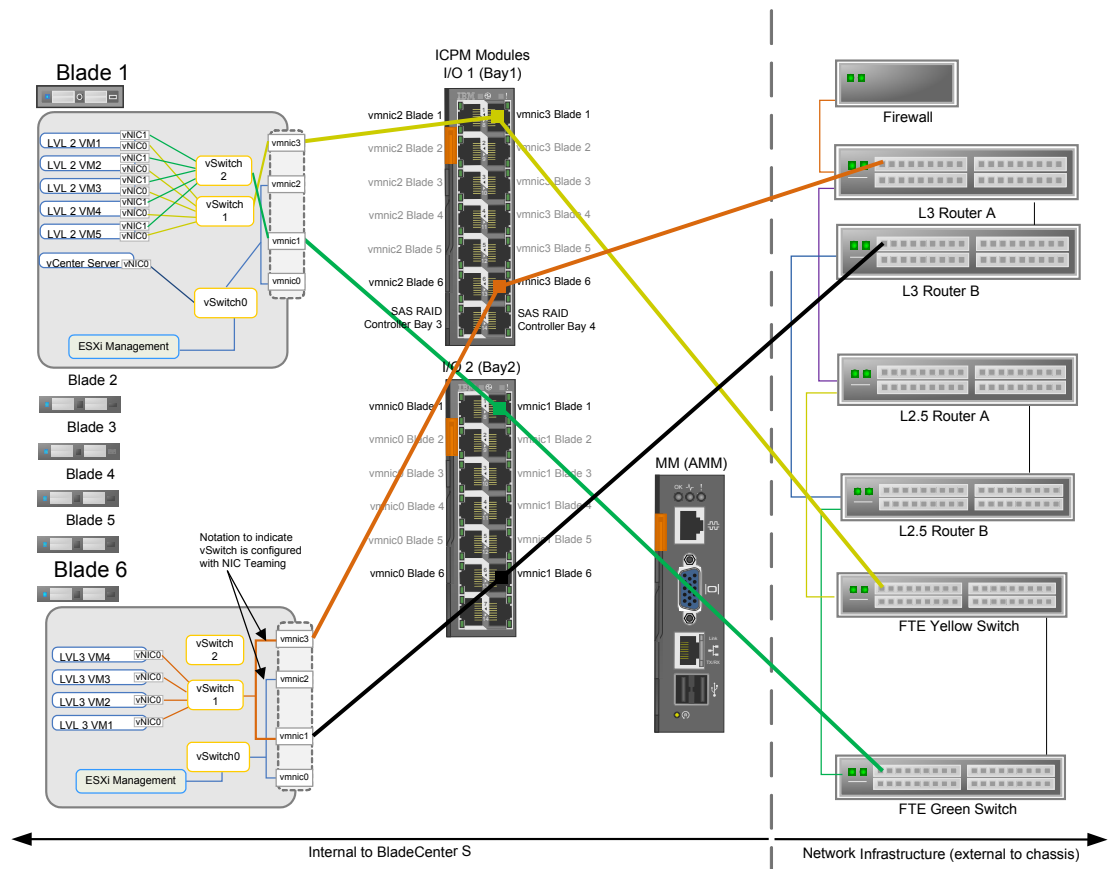


Figure 6: Connecting the BladeCenter S with DCS production workload to the network

In this example, Blade 1 contains management workload and L2 workload. Blade 6 contains Level 3 workload. Where the previous section focused on management network connectivity (including management workload), this section focuses on connectivity of DCS production workload.

- The production network is connected from the Blade server through vmnic1 and vmnic3. As mentioned previously, vmnic0 and vmnic2 are used for management traffic. Therefore, the production workload that resides on each Blade must connect to a single routed port on the external switch. For L2 production workload this is typically an FTE community. You can combine L2 production workload from multiple Experion clusters if those Experion clusters are defined within the same FTE community. Otherwise, the workload for each Experion cluster must reside on separate Blades.
- Similarly, since the L3 workload shown in Blade 6 in the diagram requires redundant routed ports on L3 routers A and B, the workload must reside on its own Blade. However, management workload could reside on Blade 6 if desired.

#### ! Attention

- The ICPM ports for production workload and the hypervisor in each Blade server are provisioned for usage with FTE deployed with 1GB switches. This means that the network properties are set to AUTO. If your production workload runs with different network properties, such as 100 mbps speed and FULL duplex, see
  - *Establishing remote web console connection to the BladeCenter S* to adjust the port speed on ICPM in I/O 1 and/or I/O 2
  - *Configuring an ESXi Host* to adjust the network properties of vSwitch 1 and/or vSwitch 2

Referring to the port numbering scheme described in the previous section, connect vmnic3 to ports 8-13 on ICPM 1; connect vmnic1 to ports 8-13 on ICPM 2, as shown in the image below.

## Network requirements for SCADA architecture

This topic outlines how to connect Blade servers with SCADA production workload from the internal side of the BladeCenter S to the SCADA production network infrastructure that is external to the chassis.

In this example, the SCADA production network is non-redundant. If implementing the SCADA architecture with a redundant production network, then the connectivity is similar to that shown in *Network requirements for DCS architecture*.

Blade 1 contains management workload and SCADA workload.

- The SCADA production network is connected from the Blade server through vmnic3. As mentioned previously, vmnic0 and vmnic2 are used for management traffic. Therefore, the production workload that resides on each Blade must connect to a single routed port on the external switch.

Referring to the port numbering scheme described in *Network requirements for management*, connect vmnic3 to ports 8-13 on the ICPM in Bay 1, as shown in the image below.

#### ! Attention

- The ICPM ports for production workload and the hypervisor in each Blade server are provisioned for usage with FTE deployed with 1GB switches. This means that the network properties are set to AUTO. If your production workload runs with different network properties such as, 100 mbps speed and FULL duplex, see:
  - *Establishing remote web console connection to the BladeCenter S* to adjust the port speed on ICPM in I/O 1 and/or I/O 2
  - *Configuring an ESXi Host* to adjust the network properties of vSwitch 1 and/or vSwitch 2
- The management network connectivity for each Blade server is identical to that shown in *Network requirements for management* with one exception: the redundant management network is implemented with a pair of switches rather than L2.5 routers.

Referring to the port numbering scheme described in *Network requirements for management*, connect vmnic2 to ports 1-6 on the ICPM in Bay 1; connect vmnic0 to ports 1-6 on the ICPM in Bay 2, as shown in the image below.

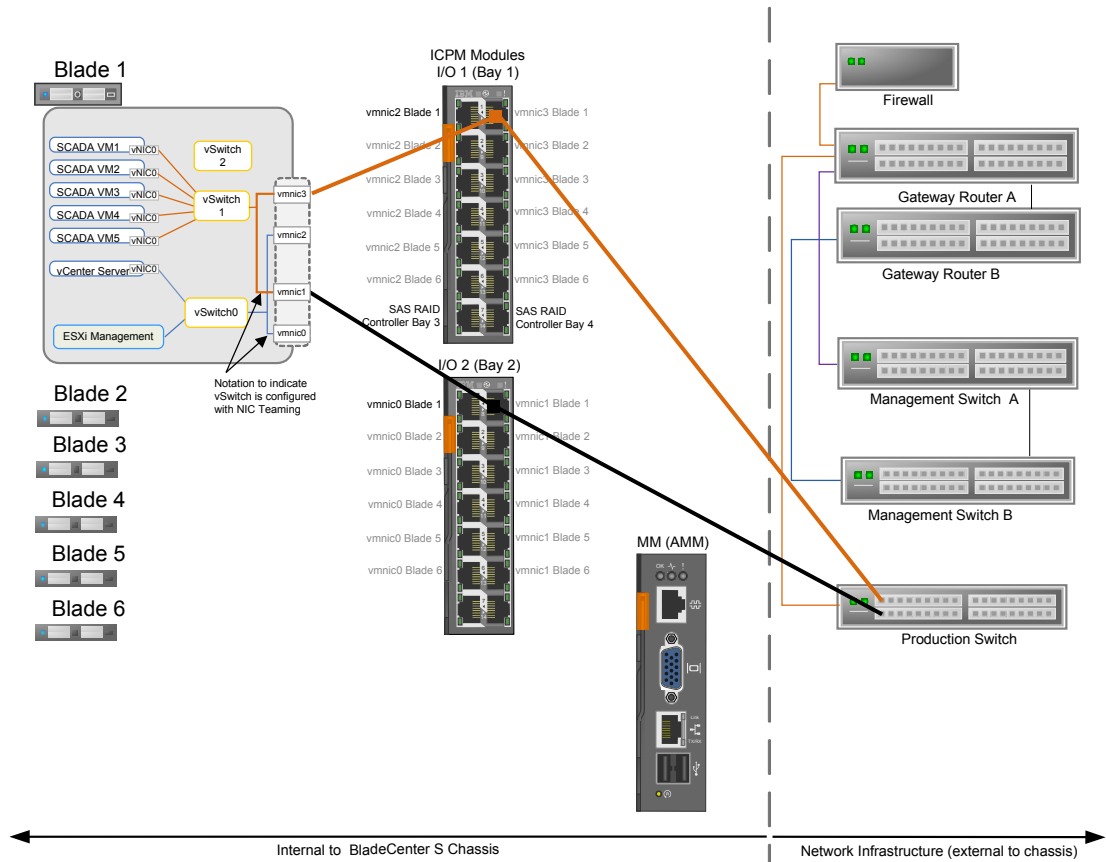


Figure 7: Connecting the BladeCenter S with SCADA production workload to the network

## Planning your workload distribution

Distribution of workload when using Experion Virtualization with BladeCenter S requires special consideration of availability requirements and resource usage. As the BladeCenter S incorporates shared storage for workloads in the same chassis, the advanced features, vSphere High Availability (HA) and vMotion can be used to easily manage the system during planned and unplanned outages. The workload distribution models described in this guide are based on usage of both vSphere HA and vMotion.

### The media tray

As the media tray is a shared resource, it is important to ensure that there is a clear mapping between USB ports and Experion servers when planning the virtual machine allocation to the Blade Server.



#### Tip

The media tray can only be mapped to a single Blade Server at a time. It is very important, however, that the media drive is not mounted to a specific VM on the Blade.

### Related topics

“Understanding vSphere High Availability (HA)” on page 22

*This topic describes how vSphere High Availability enables Blade servers to work together to provide high availability for your virtual environment.*

“Understanding vMotion and migration” on page 23

*This topic explains the benefits of using vMotion or migration to move a virtual machine from one ESXi host to another without any loss of network connectivity.*

“Understanding shared storage” on page 23

“Availability considerations” on page 24

*This topic provides availability options for three deployment scenarios, covering both single—chassis and multi-chassis situations.*

“Workload distribution tasks” on page 25

*This topic lists the tasks that will help you determine your workload distribution when using Experion Virtualization with BladeCenter S.*

“Management workload distribution” on page 28

*This topic defines management workload, and explains how they can be accommodated on Blade servers.*

## Understanding vSphere High Availability (HA)

This topic describes how vSphere High Availability enables Blade servers to work together to provide high availability for your virtual environment.

vSphere HA enables a collection of ESXi hosts (Blade servers) to work together as a group to provide higher availability for the virtual infrastructure. It pools virtual machines and ESXi hosts together into a cluster which is collectively monitored for failures. In the event of a Blade server failure, virtual machines are restarted on an alternate Blade server. This process allows for virtual machines and the applications running on them to be restarted within minutes without any manual intervention.

vSphere HA uses both network and datastore heartbeats to determine if hosts within the HA cluster are alive. vCenterServer is only required to configure the HA clusters. It is not required to control the availability of the cluster.

The Experion implementation of HA clusters uses two ESXi host in each HA cluster. Using a single pair of Blade servers per HA cluster results in:

1. Deterministic failover locations

2. Simple HA cluster configuration
3. Simple consolidation models.

Each Blade server in the HA cluster must be of the same Blade server type, that is, both Performance A or both Performance B.

## Understanding vMotion and migration

This topic explains the benefits of using vMotion or migration to move a virtual machine from one ESXi host to another without any loss of network connectivity.

The BladeCenter S platform allows vMotion to be used for process control systems. vMotion is a powerful feature of vSphere. It is a feature that allows a running virtual machine to be moved from one ESXi host to another ESXi host without having to power off the virtual machine.

This vMotion between two ESXi hosts occurs with no downtime and with no loss of network connectivity to the virtual machine.

Under normal running conditions, Experion virtual machines should stay on the Blade that has been provisioned for its resource needs. The advantage of vMotion is that critical Experion virtual machines can use vMotion to be moved to a different Blade within the *same* chassis and continue to run when a planned Blade upgrade or patch is applied. The destination Blade must have enough spare CPU and memory to support the added load of the virtual machine being migrated. The same virtual machine should be moved back to the original Blade after it is available again.

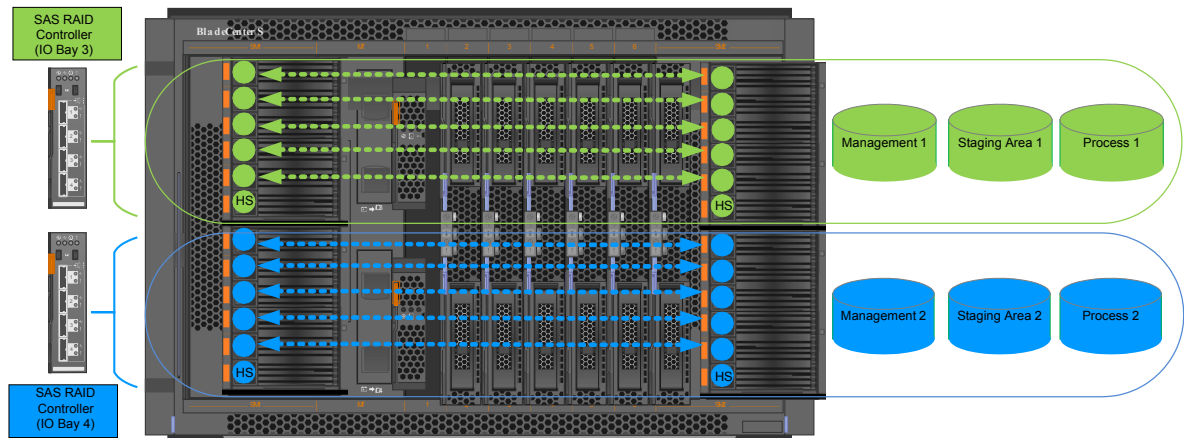
Migration of virtual machines can also be used to move workload between Blades or even between BladeCenter S chassis. Migration requires the virtual machine to be powered-off and allows both the host and the datastore to be changed at the same time. When planning a migration always ensure that the resource requirements of the virtual machine can be met by the target Blade and datastore.

## Understanding shared storage

The figure below illustrates how each SAS RAID controller is assigned to a set of disk drives. RAID 10 with two local hot spares (indicated by the letters **HS** in the following diagram) is applied to each set of disk drives. Each non-spare drive is mirrored to its counterpart drive in the opposite Drive Storage Module (DSM). A total of six volumes are available for workload distribution in the shared storage:

- **Management 1** and **Management 2** host management workload, such as vCenterServer, EBR (for virtual machine backup and restore), Update Manager, and a Domain Controller.
- **Staging Area 1** and **Staging Area 2** host workload installation and provisioning prior to deployment to its normal volume of operation. Instances of the Windows Server operating system are located in this volume.
- **Process 1** and **Process 2** host production workload. For example, these volumes would typically host the Level 2 workload.

Refer to the following figure for the allocation of shared volumes to each RAID controller.



**Figure 8: Workload distribution in the shared storage**

To achieve optimal storage performance, Honeywell recommends that you separate the workload between each set of volumes controlled by each RAID Controller. This separation should be such that the total IOPs assigned to each RAID Controller does not exceed half the maximum storage IOPs. Refer to the Honeywell Virtualization Specification for the maximum storage IOPs.

In addition to balancing the IOPs between the two RAID controllers, there may be other factors to consider when separating the workload. For example, separating workload between process levels is one consideration for Process 1 and Process 2. Another consideration for Process 1 and Process 2 would be to separate workload from the same process level between the two volumes. With careful workload separation (such as separate redundant Experion Servers), a corruption in one of the volumes would not impact the system operation. Similar considerations could be made for distributing management workload between Management 1 and Management 2.

In addition to workload installation and provisioning, Staging Area 1 and Staging Area 2 play a key role in On Process Migration (OPM) of Experion. Use of these volumes during a migration isolates the current production operation from the transition to the new release, helping to reduce the impact on production including the time spent in dual primary mode.

Refer to *Honeywell's Provisioning of the BladeCenter S for Experion* for the actual volume names as viewed through vSphere. Each volume is defined in vSphere as a separate datastore. Volume sizes are also listed in *Honeywell's Provisioning of the BladeCenter S for Experion*.

Note that the total available shared storage space for the set of disks controlled by SAS RAID Controller 1 is less than that of SAS RAID Controller 2. This is due to the overhead required to store a private volume for each Blade server, even if the Blade server is not present in the chassis. This private volume contains the hypervisor as well as vSphere logging.

## Availability considerations

This topic provides availability options for three deployment scenarios, covering both single—chassis and multi-chassis situations.

vSphere HA provides availability within a single BladeCenter S chassis. The degree of availability increases with a multi-chassis deployment.

In a multi-chassis deployment, servers with inherently redundant workload (Experion Servers) can reside in different HA Clusters and on different chassis. Distribution of other workloads must be balanced between multiple chassis. This distribution between chassis allows for complete failure of a chassis to occur and for the process control system to continue running. This approach may be required when the production network includes multiple FTE communities (or routed networks).

A similar strategy can be used within a single-chassis deployment for the Blade servers with inherently redundant workload. One option is to place the inherently redundant workload in different HA Clusters.



Distribution of other workloads must be balanced between HA Clusters. This option will protect against failures of one Blade per HA Cluster.

A second option is to split the inherently redundant workload between the Blade servers in the same HA Cluster. In this case, the inherently redundant workload is not configured to failover when a Blade server failure occurs. Distribution of other workloads must be balanced between the Blades within the HA Cluster. This option protects against failures of one Blade per HA Cluster, but relies on application redundancy during a failure.

## Workload distribution tasks

This topic lists the tasks that will help you determine your workload distribution when using Experion Virtualization with BladeCenter S.

### Pre-requisites

- It is expected that the system topology is already known. This should include the number and performance profile of all virtual machines, the network requirements and system availability requirement.
- You need to understand how to use the Performance Matrix defined in the *HPS Virtualization Specification*. The performance matrix contains the amount of resources required by each VM.
- You need to understand how to use the information listed in the *Honeywell Premium Platform for Virtualization in HPS Virtualization Specification*. Specifically, you will need to know the value of Storage IOPs for a Premium Platform Blade Chassis.
- You need to understand how the Premium Platform shared storage is provisioned. See “Understanding shared storage” in this document for more information.


The tasks identified below do not account for the use of USB security devices with Experion servers.






#### Tip

Replicated virtual machines can be used for workload distribution if desired.

If your environment uses USB security devices, you can only use one security device (dongle) per Blade server.

Task	With vSphere HA	Without vSphere HA
Plan workload grouping	<p>Form groups of virtual machines that will connect to the same routed network. To do this, identify workloads that will operate on the same network level.</p> <hr/> <p> <b>Tip</b> Each FTE community is a routed network. The groupings achieved by this differentiation are ready for further workload distribution assessment.</p>	<p>Form groups of virtual machines that will connect to the same network. To do this, identify workloads that will operate on the same network level. Workloads belonging to the Level 2 network (for DCS architectures) or the production network (SCADA architectures), should also be grouped into Experion clusters.</p>

Task	With vSphere HA	Without vSphere HA
Determine groups	<p>Form the first tentative groups of virtual machines that can be consolidated into one HA Cluster.</p> <p>It is best to consider the ESXi host failure scenario when creating this grouping and consider whether the consolidated workload can run in the same ESXi host at the same time. This will be the case when a failure occurs.</p> <p>This grouping should align with the multi or single chassis deployment strategy.</p>	<p>Form the first tentative groups of virtual nodes that can be consolidated into an ESXi host. Host performance and capacity is not considered at this point.</p> <p>To create host groups, assess the availability requirements for each virtual node in a given workload group and place in a host group. You should also consider scope of loss when assigning multiple workloads to a given host group. For example, assigning all flex stations or ACE nodes to a given host group should be avoided. Distribute them evenly across applicable host groups.</p> <hr/> <div>  <b>Tip</b> <ul style="list-style-type: none"> <li>• Redundant applications should not be placed in the same host group.</li> <li>• No more than one Windows domain controller can run in the same host group.</li> <li>• Replicated virtual machines should be included in deployment and host resource requirement calculations</li> </ul> <p>To learn more about replicated virtual machines, see “Planning to replicate the virtual machines” in the <i>Experion Virtualization Planning and Implementation Guide</i>.</p> </div> <hr/>
Identify virtual machine resource requirements	<p>Use the virtual machine workload data defined in the <i>HPS Virtualization Specification</i> to calculate the resources for each HA cluster group. These calculations will define the CPU, Memory, Disk and network requirements for the planned consolidation within the HA Cluster.</p> <p>Identify the virtual machine storage performance requirements for each of the two disk arrays in the chassis. This is required as each disk array spans all Blades in the chassis.</p> <p>Honeywell Services can assist with performance guidance.</p>	<p>Use the virtual machine workload data defined in the <i>HPS Virtualization Specification</i> to calculate the resources for each host group.</p> <p>Identify the virtual machine storage performance requirements for each of the two disk arrays in the chassis. This is required as each disk array spans all Blades in the chassis. Honeywell Services can assist with performance assessment.</p>
Define the host hardware specifications	<p>Choose between Performance A or Performance B Blade servers. Referring to the <i>HPS Virtualization Specification</i>, platform capabilities should be assessed by CPU, storage IOPs, memory, and network bandwidth. Each of these parameters need to be considered for workload assignment and must be known at this point. It is important to consider that during a Blade server failure all virtual workloads will be restarted on the surviving Blade server in the HA Cluster. Therefore, the resources available to the entire HA cluster be approximately that of a single Blade server (see the next task).</p>	<p>Choose between Performance A or Performance B Blade servers. Referring to the <i>HPS Virtualization Specification</i>, platform capabilities should be assessed by CPU, storage IOPs, memory, and network bandwidth. Each of these parameters need to be considered for workload assignment and must be known at this point. It is important to consider that during a Blade server failure all virtual workloads will be restarted on the surviving Blade server in the HA Cluster. Therefore, the resources available to the entire HA cluster be approximately that of a single Blade server (see the next task).</p>

Task	With vSphere HA	Without vSphere HA
Assess the targeted host hardware against the HA cluster or host group resources	<p>Determine if the hardware is capable of providing the resources required by each HA Cluster group. Each HA Cluster will use 2 Blades (ESXi Hosts) during normal operations but when a failure occurs only a single Blade will be in use. Since all virtual machines will run on the surviving Blade, the assessment of resources is performed against a single Blade. Use the following consolidation guidelines to implement the desired level of availability:</p> <ul style="list-style-type: none"> <li><i>High:</i> ensure that the assigned resources do not exceed the supplied resources for a single Blade or 50% of the total HA clusters resources.</li> <li><i>Medium:</i> ensure that the assigned resources do not exceed 60% of the total HA Cluster resources.</li> <li><i>Low:</i> ensure that the assigned resources do not exceed 70% of the total HA Cluster resources.</li> </ul> <p>Compare the IOPs requirement of the combined chassis workload with the storage IOPs for the chassis. . Storage IOPs is an estimate that is based on an even distribution of workload between the two SAS RAID controllers. See “Understanding Shared Storage” for more information.</p> <p>Over allocation of up to 15% above rated IOPs may be possible if willing to accept slightly slower disk performance.</p> <div>  <b>Tip</b>                      Disk intensive operations might take longer.                 </div> <p>Virtual workloads on each chassis share the capacity of the provisioned shared storage of each BladeCenter S chassis. Allocate up to the estimation capacity (which is 70% of total) for the total workload in each chassis.</p> <p>The limitation of two production network adapters per Blade server requires that network bandwidth is not over allocated.</p>	<p>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:</p> <ul style="list-style-type: none"> <li>Adjust the platform to provide the required resources.</li> <li>Adjust host group size by redistributing workloads to additional host groups.</li> </ul> <p>Compare the IOPs requirement of the combined chassis workload with the storage IOPs for the chassis. . Storage IOPs is an estimate that is based on an even distribution of workload between the two SAS RAID controllers. See “Understanding Shared Storage” for more information.</p> <p>Over allocation of up to 15% above rated IOPs may be possible if willing to accept slightly slower disk performance.</p> <div>  <b>Tip</b>                      Disk intensive operations might take longer.                 </div> <p>Virtual workloads on each chassis share the capacity of the provisioned shared storage. Allocate up to the estimation capacity (which is 70% of total) for the total workload in each chassis.</p> <p>The limitation of two production network adapters per Blade server requires that network bandwidth is not over allocated.</p>
Balance workload	<p>Determine the normal operating location of each VM in the HA Cluster. This requires that the workload be as balanced as possible. To do this, define the VMs that will run on each Blade server within each cluster and balance their collective resource requirements. This will allow implementation of the cluster to be performed as to this plan.</p>	N/A

Task	With vSphere HA	Without vSphere HA
vMotion, migration and upgrade considerations	N/A	<p>To ensure that upgrades and maintenance can be performed using vMotion, adequate spare resources need to be reserved to allow virtual machines to be migrated to different Blades.</p> <p>To do this, group the Blades that connect to the same process network and ensure that the Blade with the highest workload resource requirement has its virtual machines split between the spare resources on the other Blades.</p> <p>Update the host groups to accommodate any changes that are required to meet the resource requirements after a vMotion or migration.</p> <p>The Project may require a vMotion Plan to show normal running locations of virtual machines and upgrade/vMotion locations for virtual machines.</p>

## Management workload distribution

This topic defines *management workload*, and explains how they can be accommodated on Blade servers.

Management workload refers to the virtual machines that are connected to the management network as shown in the diagrams in *Planning the network architecture*.

Since all Blade servers in a BladeCenter S chassis are provisioned with this network connection, there is no requirement to dedicate a Blade server for this workload. They can co-exist with production workloads on the same Blade server. Therefore, the resources of the management workloads must be accounted for when determining workload distribution. Management workload network bandwidth will not use the production network adapters so does not need to be included.

Ideally, management workloads should be kept together on the same Blade. This allows for easy identification of its location. Higher availability can be applied to management workloads by including workloads in a vSphere HA Cluster. As a result, the management workloads automatically restart in the event of Blade server failure.

---

## Planning your datacenter layout

This topic provides guidelines for creating an organization hierarchy within vCenter Server.

When creating HA Clusters in vSphere Client, the hierarchical layout requires that clusters be grouped together to keep the Blade servers in similar folders so as to reflect the physical site. The example below shows the datacenter, folders, and clusters grouped using the recommended approach.

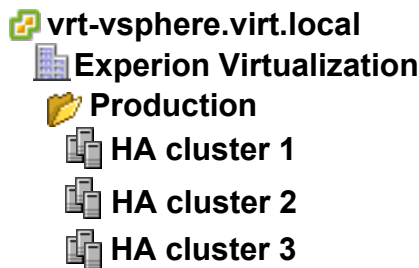
The recommended steps for creating an organization hierarchy within vCenter Server (within the *Home > Inventory > Hosts and Cluster* view) is:

1. Create a datacenter.
2. Create and organize folders within the datacenter.
3. Add the clusters to the folders. After you add a cluster, you can add your ESXi hosts, and then you can create virtual machines in the cluster.

Use folders to group items within the systems, for example, *Clusters* and *Standalone hosts*. When naming a folder, give it a name that clearly identifies this logical grouping. As your virtualization environment grows, specific hardware will be easier to find in its folder rather than having to search through generic names to find a given virtual machine or host. You can create folders within other folders to further refine these groupings

---

Example data center organization



In this example, at the top of the tree is the vCenter Server name. This node name cannot be changed. At the next level of the tree is a datacenter, which is *Experion Virtualization*. This datacenter contains a *Production* folder, which lists the HA clusters that contain the ESXi hosts and virtual machines.

---



# Setting up hardware

## Related topics

“Verify shipment contents” on page 32

*This topic lists the items included in the packaging with your BladeCenter S hardware.*

“Honeywell's provisioning of the BladeCenter S for Experion” on page 33

*This topic lists the provisioning performed by Honeywell on each BladeCenter S to ensure optimal usage with Experion, and to make it easier for you to connect to the system.*

“Removing components from the chassis” on page 35

“Install the BladeCenter S chassis in a rack” on page 36

*This topic provides detailed guidelines on how to install the BladeCenter S chassis, from checking the installation parts to connecting networks.*

“Connecting the BladeCenter S to networks and power” on page 41

*This topic describes how to connect the BladeCenter S to networks and power sources, and how to use the LED panel to monitor the power up process.*

## Verify shipment contents

This topic lists the items included in the packaging with your BladeCenter S hardware.

Use the front and back view figures in *Introducing the BladeCenter S* to verify that your BladeCenter S has the correct hardware components.

Besides the hardware, each box also contains:

- A printed copy of this guide
- Datacenter COAs on card with Service information cards
- Certificate of Conformance (COC)
- BladeCenter S Chassis Service information cards
- Blade fillers for each Blade server that occupies a slot. Empty slots contain a Blade filler which should not be removed.
- Recovery Media Thumb Drive containing the BladeCenter S media required to recover the system. A portion of the recovery content is unique to each chassis, and the media is labeled with the chassis serial number. Store this in a secure location.
- Rails for installing the BladeCenter S chassis in a rack
- Four power cords for installation in a rack or to local power
- Rack mounting template
- Miscellaneous IBM BladeCenter S and HS23 hardware documentation

Contact Honeywell Support if you need assistance recovering the system. You will need to provide one or more files from the BladeCenter S Recovery media.

The Recovery media contents are structured in this way:

- Configuration Files
  - Virtualization hardware and software configuration files, including Hypervisor images.
- Documents
  - An electronic version of this guide (PDF format)
  - An electronic version of the *IFM Installation and Users Guide* (PDF format)
  - Microsoft license activation spreadsheet (see below for more instructions)
- Firmware
  - Any customized firmware files for chassis components
  - Any customized firmware files for Blade servers
  - Bootable media *iso* file for updating firmware on a Blade server
- IFM
  - Installation media for IBM Fabric Manager
- ServerOS
  - ISO images of the OS installation media for the virtual machines

### Other tasks to complete

1. Check that the recovery media is readable prior to setting up the BladeCenter S. If this media is not readable, contact Honeywell Support for a replacement.
2. It is strongly recommended that you backup the recovery media as a precautionary step in case the media is lost, corrupted, or destroyed.
3. Copy the Microsoft license activation spreadsheet to a reliable location, one which allows you to edit the file. Use the spreadsheet to track virtual machine usage against the block of Microsoft server OS product keys. There is a virtual machine/OS server column pairing for each OS server supported. Product key usage is limited to one virtual machine per license key.



## Honeywell's provisioning of the BladeCenter S for Experion

This topic lists the provisioning performed by Honeywell on each BladeCenter S to ensure optimal usage with Experion, and to make it easier for you to connect to the system.

Review the following summary of the provisioning highlights before continuing with the chassis installation.

Provisioning Item	Description
BIOS and Firmware	The BIOS settings of each Blade server are provisioned for use with Experion Virtualization. No further BIOS settings are required. All chassis components including those within each Blade server have a firmware version that has been qualified with Honeywell. It is unlikely, but possible, that the chassis will require a firmware update during installation, but the set up instructions include a step to check for such updates. If you do require a firmware update, you will need to contact Honeywell Support for assistance prior to updating your BladeCenter S.
MAC Addresses	The hot Blade replacement feature requires a set of MAC addresses per chassis. Each chassis is labeled on both the front and back with the range of MAC addresses. Verify that the MAC addresses listed on the label are unique in your network. If duplicate MAC addresses are encountered, contact Honeywell Support for assistance.
Management Network	<p>The BladeCenter S chassis as provisioned expects to connect to the management network that is defined on the subnet 10.100.0.0 with subnet mask of 255.255.254.0 and gateway address of 10.100.1. See “Allocation of management IP addresses” in the <i>Network requirements for management</i> section for details of IP allocation. If use of this subnet is not possible, or if duplicate IP addresses are encountered, contact Honeywell Support for assistance.</p> <p>In addition to IP addresses, each BladeCenter S chassis is identified with a unique DNS name. This name is associated with the IP address for the Advanced Management Module (AMM). Each Blade server within the chassis has a unique name that ties it to the chassis. See the table in “Allocation of management IP addresses” in the <i>Network requirements for management</i> section for more information.</p>
External IO ports	Production, management and RAID Controller ports in the Intelligent Copper Pass-thru module (ICPM) are all provisioned for use with 1 Gb network speed. If one or more of the Blade servers are connected to uplink switches that do not auto detect, then follow the procedure in “Adjusting the production network properties”.
Shared Storage Datastores	<p>Listed below is the set of datastores provisioned within the shared storage subsystem and exposed through the ESXi hypervisor. The first six datastores listed below are shared between the Blade servers, and will be named <b>&lt;Name of datastore&gt;:BCSCxx:Datastore</b>, where <b>&lt;Name of datastore&gt;</b> is as defined in items 1–6 below, and <b>xx</b> maps to the chassis number.</p> <p>The final set of datastores described below (#7) map to usage by the individual Blade servers. Although these datastores reside within the shared storage subsystem, they are not shared by the Blade servers.</p> <ol style="list-style-type: none"> <li>1. Management1 (350 GB).</li> <li>2. Management2 (350 GB).</li> <li>3. Staging1 (500 GB).</li> <li>4. Staging2 (500 GB).</li> <li>5. Process1 (~1820 GB).</li> <li>6. Process2 (~1940 GB).</li> <li>7. In addition to the datastores identified above, there is a datastore created per Blade server. This datastore exists even if there is no Blade to occupy the slot. Each of these datastores is named <b>Logging:BCSCxxBy:Datastore</b>, where <b>xx</b> maps to the chassis number and <b>y</b> maps to the Blade number. These datastores host the ESXi hypervisor and hypervisor logs.</li> </ol>

Provisioning Item	Description
ESXi Installation	<p>Each Blade server is provisioned to boot its own copy of ESXi, which has been customized specifically for usage with the BladeCenter S. Honeywell installs ESXi with an evaluation license from VMware. A valid license key must be provided at the time the Blade server (ESXi host) is added to vCenterServer. The hypervisor is provisioned with:</p> <ul style="list-style-type: none"> <li>• Default system administrator account, <b>root</b>. You are required to change the password for this account</li> <li>• IP address, subnet mask, and default gateway of the network interface cards (NICs) for the management network</li> <li>• vSwitch0 defined for management network with vMotion usage. It uses vmnic0 and vmnic2 network adapters. Network speed, security, and teaming policy are defined. No additional configuration is required.</li> <li>• vSwitch1 default definition for usage with L2 production workload. It is the yellow connection. This connection uses vmnic3. Network speed of 1000 mbps will show from the vSphere Client. Security is defined. No additional configuration is required unless the production workload requires different network properties (speed). In that case, see <i>Establishing remote web console connection to the BladeCenter S</i> to adjust the port speed on ICPM in I/O 1 and/or I/O 2. See <i>Configuring and ESXi Host</i> to adjust the network properties of vSwitch 1 and/or vSwitch 2</li> <li>• vSwitch2 default definition for usage with L2 production workload. It is the green connection. This connection uses vmnic1. Network speed of 1000 mbps will show from the vSphere Client. Security is defined. No additional configuration is required unless the production workload requires different network properties ( speed). In that case, see <i>Establishing remote web console connection to the BladeCenter S</i> to adjust the port speed on ICPM in I/O 1 and/or I/O 2. See <i>Configuring and ESXi Host</i> to adjust the network properties of vSwitch 1 and/or vSwitch 2.</li> <li>• Datastores as defined in <i>Shared Storage Datastores</i>.</li> </ul>
BladeCenter S Management	<p>The AMM is provisioned to optimize usage with Experion Virtualization, including:</p> <ul style="list-style-type: none"> <li>• A power management policy that assumes power is supplied from 2 separate power sources (PDUs). If you are not using dual power sources to supply power to your chassis, contact Honeywell Support for assistance with power management policy alternatives.</li> <li>• AMM user accounts: <ul style="list-style-type: none"> <li>– The default Supervisor account (USERID) has full access rights. The password for this account is PASSWORD (note the zero in PASSWORD). You will be prompted to change this password on initial log on. During the set up of the BladeCenter S, you can use this account to supply site specific information (domain name, DNS, and so on). Use extreme caution when accessing the AMM with this account - make modifications only as instructed by this guide, or by Honeywell Support.</li> <li>– The Operator account (OPERATOR) is limited to read-only access rights. The password for this account is PASSWORD (note the zero in PASSWORD). You will be prompted to change this password on initial logon. It is strongly recommended that you log-off the Supervisor account when you have completed any required Honeywell configuration changes and then logon to the AMM using the Operator account. This will help prevent any accidental configuration changes that may override the Honeywell provisioning.</li> </ul> </li> </ul>

---

## Removing components from the chassis

It is important that you remove the components from the chassis regardless of whether you purchased the chassis already installed in racks. Removing the components will:

- Decrease its overall weight, making it easier to install in a rack (assuming your chassis were not purchased with racks).
- Re-seat components that might have shifted during product transit. Re-seating ensures proper component connectivity.

---

### Attention

- Always observe static handling precautions to prevent damage due to a static discharge.
- 

**To remove components from the chassis, complete these steps before supplying power to the rack or chassis:**

- 1 Make a note of each of the component's current location so it can be reinstalled correctly
- 2 Pull the colored handles to remove the components.
- 3 Remove the bezel from the front of the chassis.

### Next steps

If you purchased your chassis with racks, proceed to “Connecting the BladeCenter S to networks and power”. Otherwise, complete the tasks in the next section, “Install the BladeCenter S chassis in a rack”.

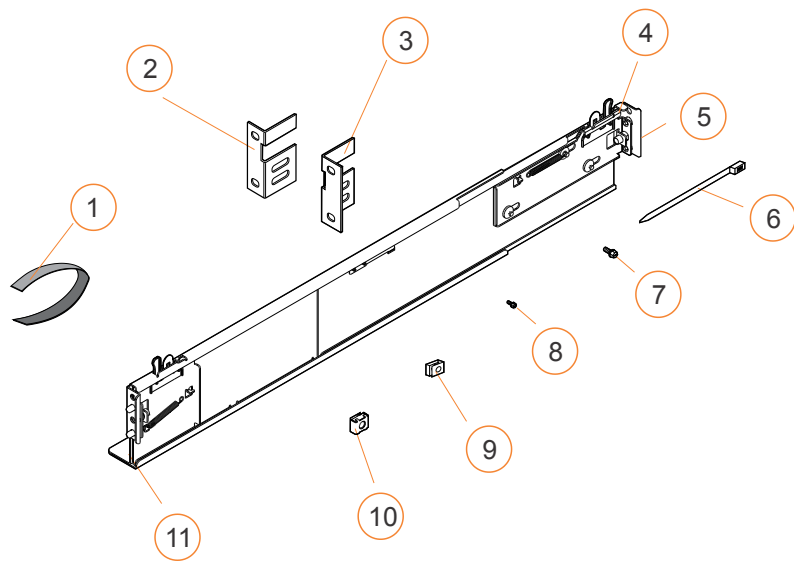
# Install the BladeCenter S chassis in a rack

This topic provides detailed guidelines on how to install the BladeCenter S chassis, from checking the installation parts to connecting networks.

**Attention**  
Always observe static handling precautions to prevent damage due to a static discharge.

1. Make sure you have all of the parts for the rack installation kit that are needed to install the BladeCenter S chassis in a rack ( see below). If any parts are missing or damaged, contact Honeywell Support.
2. Make sure you have more than one person available to lift the BladeCenter S chassis.

**Tip**  
Note: Left and right shipping brackets are required only when the BladeCenter S chassis is shipped while it is installed in a rack cabinet. An initial set of shipping brackets is provided in the rack installation kit. If you need to order additional shipping brackets, you must order the miscellaneous parts kit.

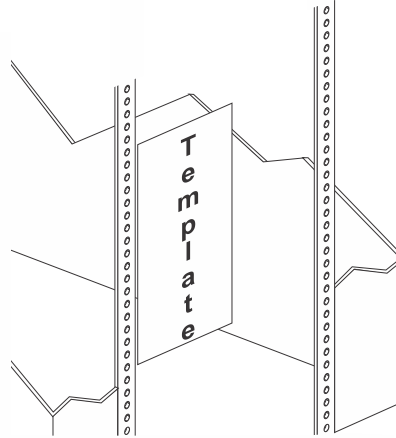


Callout	Description
1	Cable strap (6)
2	Upper left shipping bracket
3	Upper right shipping bracket
4	Rail (2)
5	Rear of rail
6	Cable ties (6)
7	M6 screws (14)
8	M5 screws (4)
9	Clip nut (6)
10	Cage nut (6)
11	Front of rail

### Position the mounting rack template

1. Position the rack-mounting template that is supplied with your BladeCenter S system on the rack so that the edges of the template do not overlap any other installed devices.

2. Line up and select the holes on the front and rear of the rack in the locations that are indicated by the arrows on the template.



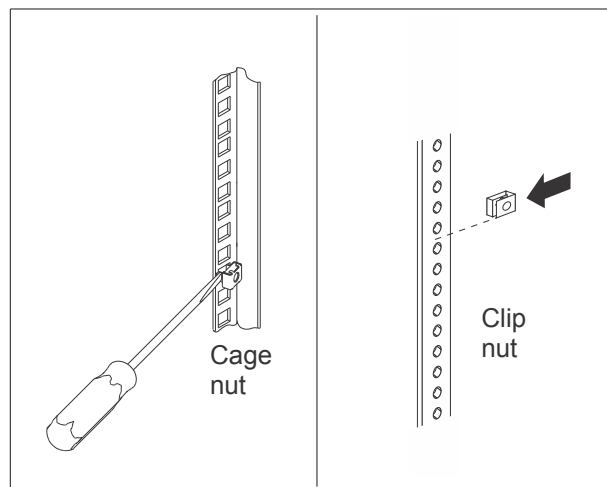
### Installing the cage nuts

1. Use a screwdriver to install the cage nuts or clip nuts, as required for your rack, in the locations indicated on the template.



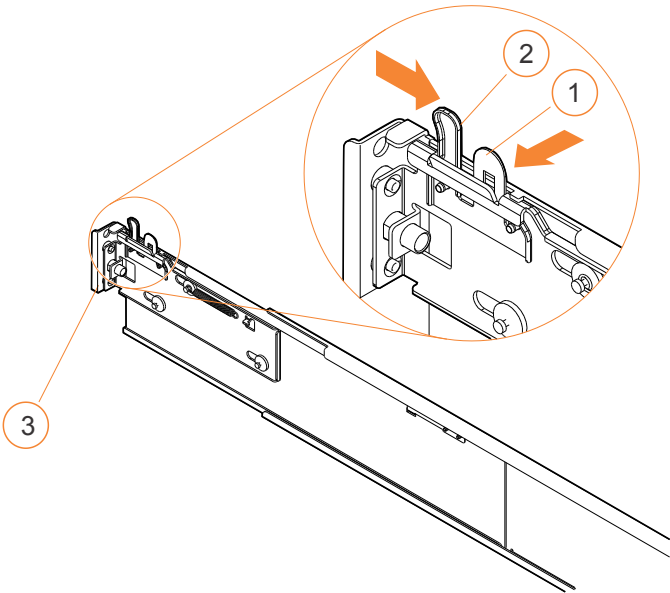
#### Tip

For racks with square holes, use the cage nuts. For racks with rounds holes, use the clip nuts.



### Retract rail pins


1. Before you install the rails in the rack, fully extend each rail. A set of rail pins and a mounting flange are on each end of the rail. Retract the rail pins by pressing in the rail latch pulling the finger pull 1 and then 2 toward the center of the rail.
2. Pull each end of the rail away from its center until the rail is fully extended. A locking mechanism prevents the rail from being extended too far.



Callout	Description
1	Rail latch
2	Finger pull
3	Mounting flange

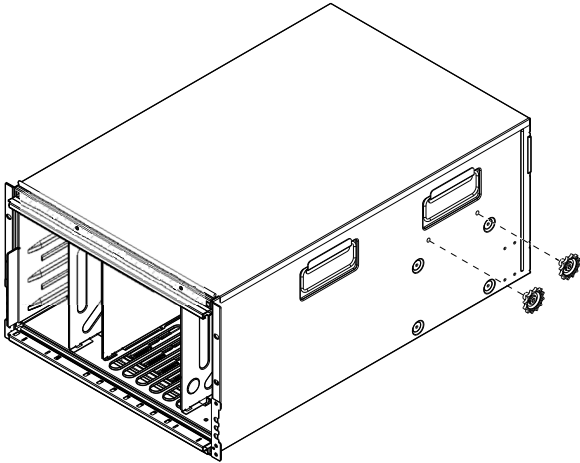
**Position rails**

- 1. Position the rail in the desired location on the rack and align the pins on each end of the rail with the applicable holes on the rack.
- 2. Release the rail latches and finger pulls on each end to allow the rail pins to pass through the rail and the mounting flange.
- 3. Repeat for the other rail.

 **Tip**  
Make sure that the rail pins protrude through the mounting flanges and the rack cabinet rails.

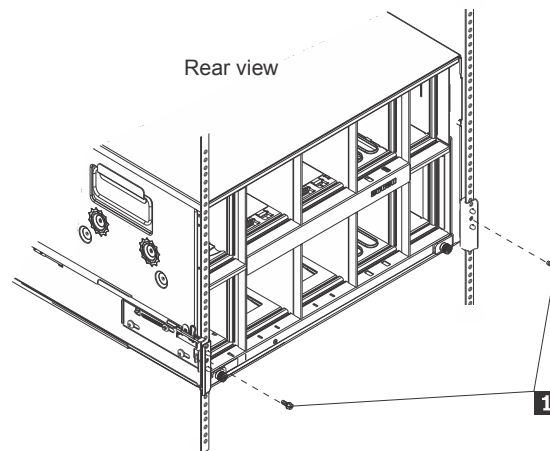
**Remove shipping screws**

- 1. Remove the two blue shipping screws from each side of the BladeCenter S chassis.

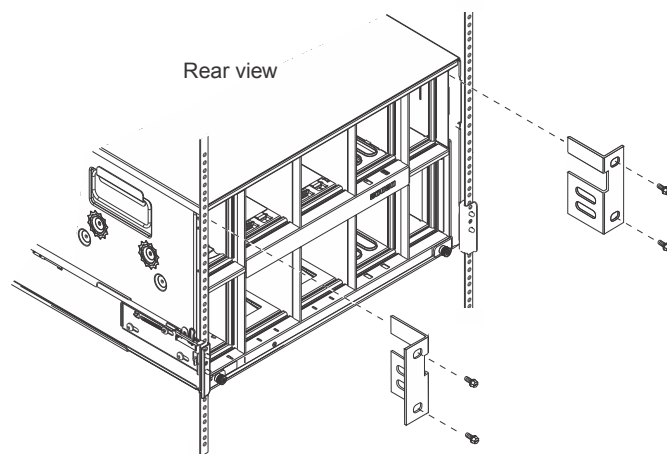


### Secure chassis

1. Slide BladeCenter S chassis into the front of the rack.
2. Insert one M6 screw (1) in the center hole of each rail in the rear of the rack cabinet.



3. Optionally, install the shipping brackets. There is a set of shipping brackets provided in the BladeCenter S chassis rack installation kit.

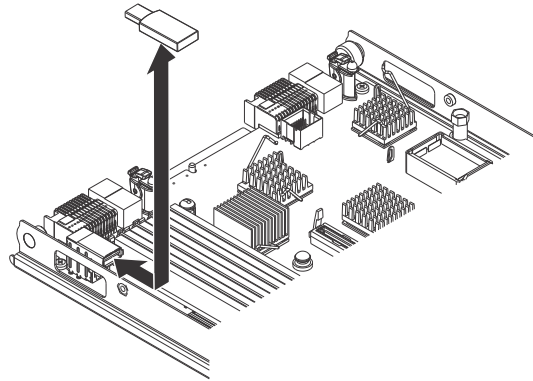


4. To install the upper right shipping bracket (if you are facing the rear of the BladeCenter S chassis):
  - a. Align the first shipping bracket so that the bottom of the shipping bracket will fit into the slot to the right of power module bay (1). Insert the shipping bracket into the slot.
  - b. Align the holes in the shipping bracket with the holes in the rack cabinet.
  - c. Secure the shipping bracket to the rack cabinet with the screws that are provided.
5. Repeat these steps for the upper left shipping bracket.
6. Secure chassis and reinstall components by inserting four M6 screws in the front of the chassis to secure it to the rack cabinet.

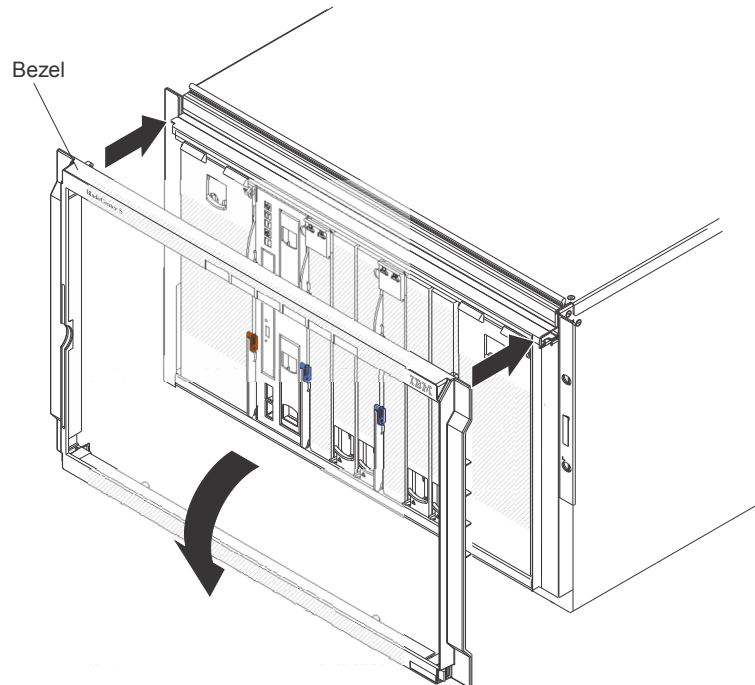
### Re-install components

1. Re-install the components that were removed prior to installing the chassis in the rack. If Experion is licensed with a USB security dongle, then connect the dongle to each Blade that will host Experion server workload prior to re-installing the Blade server to the chassis.
2. Remove the cover of the Blade server in order to expose the USB port. To open the Blade server cover:
  - a. Lay the Blade server on a flat, static-protective surface, with the cover side up.
  - b. Press the Blade server cover release on each side of the Blade server and lift the cover open.

- c. Lay the cover flat, or lift it from the Blade server. Use the image below to locate the port for USB insertion



3. Return the cover to the Blade server and re-install in the chassis.
4. If the BladeCenter S chassis is not fully populated with Blade servers, insert a filler into each empty Blade slot. This is required for cooling of the chassis.
5. Install the bezel on the front of the BladeCenter S chassis.





## Connecting the BladeCenter S to networks and power

This topic describes how to connect the BladeCenter S to networks and power sources, and how to use the LED panel to monitor the power up process.

Power is supplied to the BladeCenter S chassis by connecting a power cord to a power connector on the rear of the BladeCenter S chassis (see *Understanding the chassis hardware features - Back view*) and the other end of each power cord to a power distribution unit (PDU) or appropriate electrical outlet. There is no power switch on a BladeCenter S chassis. It is recommended that each PDU be connected to separate power circuits to optimize the BCS provisioning that sets the policy to manage power usage from redundant power sources.

### Connecting to networks

1. Use the figure in *Network requirements for management* to connect the appropriate ports from the I/O modules on the back of the BladeCenter S chassis to the external management routers (L2.5 routers).



#### Tip

When using the Honeywell supplied rack for the Premium Platform, it is recommended that the network cables route from the IO Modules 1 and 2 to the cable management mechanism panel mounted below each chassis. All of the network cables should route through the cable management panel, then down the left side of the chassis. It is important to keep the network cables separate from the PDU power cords to prevent interference.

2. Use the figure in *Network requirements for DCS architecture* or *Network requirements for SCADA architecture* to connect the appropriate ports from the I/O modules on the back of the BladeCenter S chassis to the external production switches.

### Connecting to power

1. Connect the power cords from power supplies 1 and 2 to the 110 V ac or 220 V ac PDU of the first power source. On the Honeywell supplied rack, use the top PDU to connect to the Power Supplies 1 and 2 (left side).



#### Tip

When using the Honeywell supplied rack for the Premium Platform, two PDUs are mounted above each chassis. The PDU cords are connected to the PDUs and therefore ready for connection to the power supplies as described above. The power cords are anchored to the right side of the rack and are routed to minimize interference with fan module replacement.

2. Connect the power cord from power supplies 3 and 4 to the 110 V ac or 220 V ac PDU of the second power source. On the Honeywell supplied rack, use the bottom PDU to connect to the Power Supplies 3 and 4 (right side).
3. When the power is connected, verify that the following LEDs are lit:
  - The power-on LED on the system LED panel. This is found on both the front on the media tray and rear of the chassis below I/O modules 1 and 2. (see image below.)
  - DC power and AC power LEDs on each power module.
  - OK or Power LED on each I/O module.

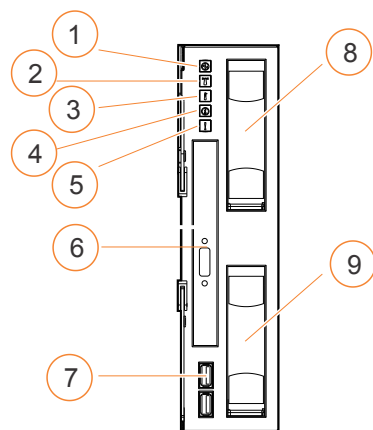


#### Tip

The power up (top) LED for each Blade server should be blinking fast while the Blade initiates.

You might see blinking amber LEDs on the SAS Connectivity Module in bays 3 and/or 4. The LEDs will turn green when you complete the AMM configuration wizard.

The following image shows the System LED panel on media tray on the front of the chassis.



Callout	Description
1	Power-on
2	Location
3	Over-temperature
4	Information
5	System error
6	CD-RW/DVD-ROM drive
7	USB ports
8	Battery backup unit 1
9	Battery backup unit 2

# Configuring hardware to work with Experion virtualization



## Attention

If you have not done so already, contact Honeywell Support for assistance if any of the following are true:

- You are unable to use the provisioned management subnet 10.100.0.xx
- You have existing devices with duplicate MAC addresses to those identified on the BladeCenter S chassis label
- You have existing physical nodes with duplicate IP addresses to those identified in Management IP Addresses  
Honeywell Support must adjust the provisioning in your chassis prior to continuing with the remainder of the configuration tasks described in this document.

## Related topics

“Establishing remote web console connection to the BladeCenter S” on page 44

*This topic guides you through connecting to the Advanced Management Module, which is used to configure and manage BladeCenter S components.*

“Configuring the site specific management properties” on page 46

*This topic guides you through configuring the site specific management properties of the Advanced Management Module.*

“Adjusting the production network properties” on page 47

*This topic guides you through adjusting the production network properties of the Intelligent Copper Pass-thru Module (ICPM) if one or more of the Blade servers is connected to uplink switches that do not auto-detect. An example uplink would be FTE switches that only support 100 Mbps, Full.*

“Backing up the AMM configuration” on page 48

*This topic guides you through backing up the AMM configuration in case the AMM needs to be restored, such as in the case when you need to install new AMM firmware.*

“Setting the RSSM password” on page 49

“Verifying the hypervisor boot” on page 50

“Configuring an ESXi host” on page 52

*This topic details the some extra configuration tasks necessary to ensure correct operation of your Blade server.*

“Preparing the vCenter server” on page 54

*This topic lists the steps involved in preparing the vCenter Server, including first creating a virtual machine to host vCenter Server and other components.*

“Organizing your VMware inventory objects” on page 55

*This topic contains a recommended hierarchy for your VMware inventory objects.*

“Creating and updating high availability clusters” on page 56

“Creating and managing virtual machines” on page 59

## Establishing remote web console connection to the BladeCenter S

This topic guides you through connecting to the Advanced Management Module, which is used to configure and manage BladeCenter S components.

The remote console connection to the BladeCenter S is through the Advanced Management Module (AMM). To connect to the AMM you will need a client computer that is connected to the management network. The IP address of client computer and the AMM must reside in the same subnet.

### To establish remote console connection to the BladeCenter S:

- 1 Using the table of IP addresses defined in “Allocation of Management IP addresses”, in the *Network requirements for management* section, locate the IP address of the AMM for your BladeCenter S. For example, if you are installing your first chassis, then the IP address of the AMM is 10.100.0.20.
- 2 Open a web browser on the client computer and direct it to the IP address of the AMM for the chassis.
- 3 Enter the default Supervisor user name, (**USERID**), and the default password, (**PASSWORD**) (note the number zero, not the letter O, in PASSWORD) on the **Welcome to the Advanced Management Module** display.
- 4 Select **login** to start the remote session. Since this is the first time the AMM has been accessed, you will be prompted to change the password. When the new password is confirmed and accepted, follow the instructions for desired session parameters.
- 5 Select **Continue** to complete the remote console connection.

Referring to the example below, the display shown has two panes: the left pane contains the menu hierarchy; the right pane displays the results depending on the menu item selected.

IBM BladeCenter S Advanced Management Module

Welcome USERID About Help Logout IBM

Bay 1: BCSC01

- Monitors
  - System Status
  - Event Log
  - LEDs
  - Power Management
  - Hardware VPD
  - Firmware VPD
  - Remote Chassis
- Blade Tasks
  - Power/Restart
  - Remote Control
  - Firmware Update
  - Configuration
  - Serial Over LAN
  - Open Fabric Manager
- I/O Module Tasks
  - Admin/Power/Restart
  - Configuration
  - Firmware Update
- Storage Tasks
  - Configuration
- MM Control
  - General Settings
  - Login Profiles
  - Alerts
  - Serial Port
  - Port Assignments
  - Network Interfaces
  - Network Protocols
  - Chassis Int Network
  - Security
  - File Management
  - Firmware Update
  - Configuration Mgmt
  - Restart IMM
  - License Manager
- Service Tools

**System Status Summary**

The following links can be used to view the status of different components.

- [Blades](#)
- [I/O Modules](#)
- [Storage Modules](#)
- [Management Module](#)
- [Power Modules](#)
- [Power Module Cooling Devices](#)
- [Chassis Cooling Devices](#)
- [Media Tray](#)

**Blades**

Click the icon in the Status column to view detailed information about each blade.

Bay	Status	Name	Pwr	Owner**		cKVM*	I/O Compatibility	WOL*	Local Control			
				KVM	MT*				Pwr	KVM	MT*	BEM*
1	On	BCSC01-BS01	On				OK	On	✓	✓	✓	---
2	On	BCSC01-BS02	On				OK	On	✓	✓	✓	---
3	On	BCSC01-BS03	On				OK	On	✓	✓	✓	---
4	On	BCSC01-BS04	On				OK	On	✓	✓	✓	---
5	No blade present											
6	No blade present											

\* MT = Media Tray (CD/USB), WOL = Wake on LAN, BEM = Blade Expansion Module  
 BSE1 (BSE2, BSE3) = Blade Storage Expansion 1st Generation (2nd Generation, 3rd Generation)  
 PEU1 = PCI Expansion Unit 1st Generation, PEU2 = PCI Expansion Unit II, BPE3/BPE4 = PCI Express Expansion Unit  
 cKVM = Concurrent KVM Expansion, BIE = Blade I/O Expansion, BPR = Blade Processor Expansion, BGE = Blade Graphics Expansion Unit, MEU = Memory Expansion Unit

\*\* You can change the KVM and Media Tray ownership on the Remote Control panel (under Blade Tasks).

I/O Modules

Trusted sites | Protected Mode: Off | 100%

Figure 9: The Advanced Management Module interface

**Tip**

The default USERID account has full access rights to the AMM configuration. Honeywell has provisioned the AMM specifically for this BladeCenter S chassis

When accessing the AMM with this account, make only those changes documented in this guide or suggested by Honeywell Support. When you have completed the Honeywell required changes, it is strongly recommended that you terminate the remote connection to the AMM with the default (SUPERVISOR) account. Use the Operator account to monitor your BladeCenter S chassis as described in Monitoring the BladeCenter S.

Lastly, if a blocked web site prompt is displayed for *http://*, we recommend either clicking **Close**, or clearing the **Continue to prompt when website content is blocked** check box to disable the prompt.

---

---

## Configuring the site specific management properties

This topic guides you through configuring the site specific management properties of the Advanced Management Module.

### Prerequisites

“Establishing remote web console connection to the BladeCenter S”.

### To configure site specific management properties

- 1 From the menu pane of the AMM console, expand the **MM Control** option.
- 2 Select the **Network Interfaces** option from the **MM Control** list.
- 3 In the **Management Module** section within the results:
  - a Verify that the Hostname is the name associated with the IP address of the AMM for this chassis.
  - b Enter the domain name for this AMM IP address.
  - c Click **Save**.
- 4 Select the **General Settings** option from the **MM Control** list.
- 5 In the **MM Date and Time** section with the results pane, select **Set MM Date and Time**.  
Two sections appear in the results pane: *MM Date and Time* and *Network Time Protocol (NTP)*
- 6 Verify that the time and date values in the **MM Date and Time** section are accurate for your site.
- 7 In the **Network Time Protocol (NTP)** section within the results pane:
  - a Set **NTP auto-synchronization service** to **Enabled**.
  - b Enter the fully qualified hostname or IP address of your NTP server.
  - c Set the **NTP update frequency** (in minutes). The recommended frequency is **30**.
  - d Set **NTP v3 authentication** to **Disabled**.
  - e Click **Save**.

### Next steps

Add the IP address and the name of the AMM to the DNS.

---

## Adjusting the production network properties

This topic guides you through adjusting the production network properties of the Intelligent Copper Pass-thru Module (ICPM) if one or more of the Blade servers is connected to uplink switches that do not auto-detect. An example uplink would be FTE switches that only support 100 Mbps, Full.

### Prerequisites

“Establishing remote web console connection to the BladeCenter S”.

- 1 From the menu pane of the AMM console, expand the **I/O Module Tasks** option.
- 2 From the **I/O Module Tasks** list, select the **Configuration** option to view the **I/O Module Configuration** details. Use the tabs along the top of the configuration page to select one of the configuration options: **IPv6 Support**, **Slot 1**, **Slot 2**, **Slot 3**, and **Slot 4**.
- 3 Select the **Slot 1** tab, then select the **Port Configuration and Status** link to connect production workload on the primary network (through vmnic3). The results pane is updated with **I/O Module 1 – Intelli, Copper PM: I/O Port Status**.
  - a For any Blade that is hosting non-FTE workload, map to the appropriate port as shown in *Network Requirements for DCS architecture* or *Network Requirements for SCADA architecture*. For example, if Blade 6 is hosting non-FTE workload, then use port 13.
  - b Change the value in the **Setting** list from **Auto** to **100 Mbps, Full**
  - c Click **Save**.
- 4 Repeat step 3 for Slot 2 to connect production workload on the secondary network (through vmnic1). The results pane is updated with **I/O Module 2 – Intelli, Copper PM: I/O Port Status**.

---

## Backing up the AMM configuration

This topic guides you through backing up the AMM configuration in case the AMM needs to be restored, such as in the case when you need to install new AMM firmware.

### Prerequisites

“Establishing remote web console connection to the BladeCenter S”.

- 1 From the menu pane of the AMM console, expand the **MM Control** option.
- 2 Select the **Configuration Mgmt** option from the **MM Control** list.
- 3 In the **Backup Configuration to File** section within the results:
  - a Select **Backup**.
  - b In the **File Download dialog box**, click **Save**.
  - c Navigate to the desired location to save the AMM backup file. For example, *Documents\AMM Backups*. (You may need to create this folder if it does not already exist.)
  - d Rename the *asm.cfg* file to represent the purpose of the backup. For example, *preupdatebackup\_MMDDYY\_asm.cfg*.
  - e Press **Save**.
  - f In the **Download Complete dialog box**, click **Close**.
  - g Insert removable media in the client node.
  - h Open Windows Explorer and browse to same folder identified in *step C*
  - i Copy the archived file from *step D* to the removable media. It is also recommended that you keep a copy of the usernames and passwords for each AMM login account with the backup file.
  - j Un-mount the removable media and store in a secure location.



## Setting the RSSM password

To change the password on your RSSM you need to change the passwords on two components in each of the IO modules residing in bays 3 and 4 of a Blade Center-S: the SAS switch and the RAID controller.



### Attention

- Note for both the SAS Switch and RAID Controller the factory default password is "PASSWORD" (note that zero is used in place of an O).

### Prerequisites

Access to a Telnet client.

### Identify the correct IP addresses

- Provisioned IPs for Blade Center S Chassis 1
  - a SAS Switch for I/O Bay 3: **10.100.0.28**
  - b SAS Switch for I/O Bay 4: **10.100.0.29**
  - c RAID Controller for I/O Bay 3: **10.100.0.38**
  - d RAID Controller for I/O Bay 4: **10.100.0.39**
- Provisioned IPs for Blade Center S Chassis 2
  - a SAS Switch for I/O Bay 3: **10.100.0.48**
  - b SAS Switch for I/O Bay 4: **10.100.0.49**
  - c RAID Controller for I/O Bay 3: **10.100.0.58**
  - d RAID Controller for I/O Bay 4: **10.100.0.59**

To determine provisioned IPs for subsequent chassis, simply add on 20 to the last byte of the IP address, as shown by the example above for chassis 2 compared to chassis 1 2.

### To change the password on your SAS switch:

- Using a Telnet client on the management network, connect into the SAS switch using its IP address.
- From the telnet prompt issue the following command: **command setadminpassword USERID newpassword.**
- Repeat for other SAS switches.

### To change the password on your RAID Controller:

- Using a Telnet client on the management network, connect into the RAID Controller via its IP address.
- From the telnet prompt issue the following command: **command chpasswd -cli -oldpasswd xxxxxxxx -newpasswd yyyyyyyy** Where **xxxxxxx** is the old password, and **yyyyyyy** is the new password.
- Repeat for other RAID Controllers.

## Verifying the hypervisor boot

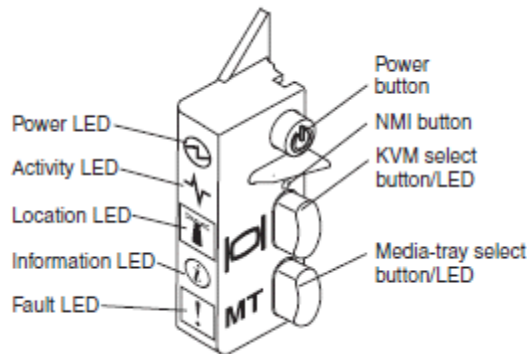
Powering on the Blade servers boots the ESXi hypervisor from shared storage. After the initial hypervisor boot, you need to make several site specific configuration changes to the hypervisor.

### Prerequisites

- You have installed the Java Runtime Environment on the client node used to remotely access AMM. The minimum version required is Sun JRE 6.0 update 10.
- You are logged into the AMM console using the Supervisor account (USERID). See *Establishing remote web console connection to the BladeCenter S*.
- You have the DNS related network details for each Blade server.

### To power on the Blade servers

- 1 From the menu pane of the AMM console, click **Blade Tasks**.
- 2 Select the **Power/Restart** option from the **Blade Tasks** list. All Blade servers are listed **Blade Selection** and **Status** table. The **Pwr** status of each Blade is **off**. The **Management Network** status for each Blade server is green.
- 3 Select each Blade that you want to power on.
- 4 Select **Available Actions > Power On Blade**.
- 5 Select **Perform Action** to power on the selected Blade servers.  
The **Pwr** status of each Blade changes from **off** to **on**.



Use this image and the Blade chassis information card (front side of the chassis in the slot on lower left) to verify that the Blade server is operating normally.

### To manually power on a single Blade server

- 1 Locate the Blade control panel for the Blade server you want to power on. If the Power LED exhibits a quick flash LED, then the Blade server is in a state that will prevent the power control button from responding, and you will not be able to turn it on manually. When the Power LED transitions to a slow flash, the power control button is active and can be turned on.
- 2 Press the Power button on the Blade control panel. A solid Power LED means that the Blade server has power and is turned on.

### To configure hypervisor for your site

- 1 From the menu pane of the AMM console, click **Blade Tasks**.
- 2 Select the **Remote Control** option from the **Blade Tasks** list

- 3 In the **Start Remote Control** section of the display, click **Start Remote Control**.

**Tip**

You need to turn off pop-up blockers to allow the Remote Control function to be invoked. The first time you try to access Remote Control, a **Publish Trust** dialog box is displayed. To proceed, select the **Always trust content from this publisher** option and click **Run**.

- 4 Perform the following steps from the **Remote Control** window, referring to the example below:
- Select the target Blade server from the drop down list
  - If the hypervisor is running, a black screen with grey text is displayed. Otherwise, wait for the Blade to initialize and start the hypervisor.
- 5 Change the hypervisor password
- With the cursor over the **Remote Console** window, click once, then press **F2**. The console changes color.

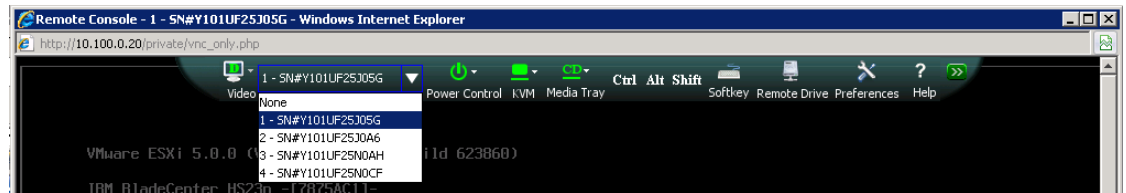


Figure 10: The Remote Console window

**Tip**

Press the left **Alt** button to re-display the Remote Control menu bar if it is not visible at any stage.

- Press **F2** again to display the **Login** dialog box. Enter **root** in the Login Name and **PASSWORD** (note the number zero) in Password.
  - Configure Password** is highlighted at the top of the screen. Press **Enter** to select.
  - Provide the old and new passwords, then press **Enter**.
- 6 Configure the Default Gateway, DNS, and Host names
- Use the arrow keys to select **Configure Management Network** and press **Enter**.
  - Use the arrow keys to select **IP Configuration** and press **Enter**
  - Use the arrow keys to select **Default Gateway**
  - Type the default gateway address.
  - Press **ESC** to exit IP Configuration.
  - Use the arrow keys to select **DNS Configuration** and press **Enter**.
  - Use the arrow keys to select **Use the following DNS server addresses and hostname** and press the spacebar.
  - Enter the primary server, an alternative server (optional), and the host name, (Make sure the host name includes your local domain reference *hostname.domain.local*) then press **Enter**.
  - Press **ESC** to go back to **Direct Console main menu**.
  - Press **ESC** to exit Direct Console.
  - Repeat this procedure for each Blade server, starting at step 4a.

## Configuring an ESXi host

This topic details the some extra configuration tasks necessary to ensure correct operation of your Blade server.

Honeywell has provisioned each Blade server with most of the necessary configuration. This section lists the remaining configuration items necessary for each Blade work properly within your management network:

- Configuring the ESXi host time synchronization. ESXi hosts require time synchronization within the whole infrastructure. Ensure that you have determined the time source for all ESXi hosts and configured the time configuration.
- Updating vSwitch1 and/or vSwitch2. This might be necessary if your production workload runs at a speed higher than 100mbps. This is necessary for non-FTE production workload.

### Prerequisites

- You have installed vSphere Client on a physical node that is connected to the management network.
- You have the IP address or host name of the NTP Server for each Blade server.
- You have the IP address for each Blade server. See *Allocation of management IP addresses* for more information.

## Configuring the ESXi host time synchronization

- 1 Connect to the Blade server using the vSphere Client.
- 2 Click the **Configuration** tab.
- 3 Click **Time Configuration**.
- 4 At the top right of the page, click **Properties**. The **Time Configuration** dialog box appears.
- 5 Click **Options**. The **NTP Daemon (ntpd) Options** dialog box appears.
- 6 Click **NTP Settings**, and then click **Add**. The **Add NTP Server** dialog box appears.
- 7 Type the IP address or host name of the NTP time server and click **OK**.
- 8 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 will see an event in the vSphere Client recent tasks status bar stating *update service activation policy*. The **Time Configuration** dialog box appears.
- 9 Click **OK**. You will see an event in the vSphere Client recent tasks status bar stating *update date or time*. Within 15 minutes, the ESXi host time should synchronize with the NTP time server.
- 10 Repeat these steps for each Blade server in the chassis.

## Updating vSwitch1 and/or vSwitch2 configuration

If the Blade server is hosting FTE production workload that is connected from the Intelligent Copper Pass-thru Module (ICPM) to uplinks running at 100 Mbps, use the FTE Yellow and FTE Green virtual switches as provisioned. However, you must adjust the port speed on the ICPM as instructed in “Adjusting the production network properties”.

If the Blade server is hosting production workload that is connected to a network other than FTE, use the information in this section to update the configuration of vSwitch1 and vSwitch 2 (see Blade 6 in Figure 6 or Blade 1 in Figure 7). In this case, the settings for speed and duplex for vSwitch1 are correct. Since vSwitch2 is not needed, remove the provisioned value of vmnic1 from the uplink adapter and add NIC teaming on vSwitch1 between vmnic3 and vmnic1. The settings for vSwitch0 must remain as provisioned.

If the Blade server that is hosting the non-FTE production workload is connected from the ICPM to uplinks running at 100 Mbps, adjust the port speed on the ICPM as instructed in “Adjusting the production network properties”.

**To update vSwitch1 or vSwitch2 configuration settings**

- 1 From the vSphere client, select the ESXi host from the inventory panel.
- 2 Select the **Configuration** tab, then select **Networking**.
- 3 Select **vSwitch1** and click **Properties**. Change only the properties as identified in the table below.

Virtual switch	Virtual machine port group	Uplink Adapter	VLAN ID	Speed value	Duplex Value
vSwitch1	Replace FTE Yellow with an alternative network identifier.	Use the provisioned value of vmnic 3. Add vmnic 1 by following the <i>NIC teaming</i> instructions below (connect to ports within range of 8-13 on ICPM in I/O 1 and ICPM in I/O 2 respectively as shown in <i>Planning the Network Architecture</i> )	No change	No change	No change
vSwitch2	No change	Remove the provisioned value of vmnic 1.	No change	No change	No change

**To configure NIC teaming**

- 1 On the vSphere Client, (within the **Home > Inventory > Inventory** view), locate the ESXi host. Click the **Configuration** tab, and then under the Hardware group, click the **Networking** link.
- 2 Locate the vSwitch1 virtual switch, and then click the associated **Properties** link. The **vSwitch Properties** dialog box appears.
- 3 To construct a NIC team (connecting redundant network adapters to vSwitch1):
  - a Click the **Network Adapters** tab and then click **Add**. The **Add Adapter Wizard** dialog box appears.
  - b In the **Unclaimed Adapters** group, select the vmnic1 adapters (NICs) that need to be connected to the vSwitch1, and then click **Next**.
  - c Click **Move Up** and **Move Down** as needed to move the selected vmnic1 adapter into the **Active Adapters** group box.
  - d Click **Next**.
  - e Review the information and then click **Finish**.
- 4 To set the NIC teaming policy exceptions:
  - a Click the **Ports** tab, select the vSwitch configuration, and then click **Edit**.
  - b Click the **NIC Teaming** tab.
  - c Set the following policy exceptions:

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

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

**Attention**

The settings for vSwitch0 must not be changed.

## Preparing the vCenter server

This topic lists the steps involved in preparing the vCenter Server, including first creating a virtual machine to host vCenter Server and other components.

On the Blade server that will run the management workload, you need to create a virtual machine to host the vCenter Server (and vCenter Update Manager).



### Tip

Before preparing the vCenter Server, make sure you have completed the tasks in the *Planning your workload distribution* section.

### To prepare the vCenter Server

1. Confirm the existence of a Windows Domain Controller.

A Windows domain must exist before you create the vCenter Server. Ensure that there is a physical or virtual domain controller for the vCenter to communicate with, otherwise you will need to install a new Windows domain controller on the same network as the management workload.

The Windows domain controller:

- Performs the role of a DNS server
- Uses reverse lookup zones for all subnets in the infrastructure
- Uses DNS HOST A and PTR records to the Forward and Reverse lookup Zones for each of the ESXi hosts, using their management network IP address.

For more information about setting up a Windows domain controllers, see the *Window Domain and Workgroups Implementation Guide* available from the Honeywell Process Solutions Support web site (<http://www.honeywellprocess.com/>).

- Enables the creation of Domain service accounts when separate SQL installation is required.
2. Install vCenter Server, SQL Server, and Update Manager on the virtual machine.

For more information about installing these products, refer to the *"Installation and configuration of SQL server and vCenter server"* white paper, available from the Honeywell Process Solutions web site (<http://www.honeywellprocess.com/>).

3. Install extra applications, if appropriate (only applicable when using virtual machine replication).

When virtual machine replication is used, the vCenter Server requires extra applications to be installed. Installing these applications during the initial installation and configuration phase of the vCenter server will prevent possible restarts later when this type of interruption may not be acceptable. Refer to "Replicating a virtual machine" in the *Virtualization Planning and Administration Guide* for an overview of this functionality and requirements in the vCenter Server.

---

## Organizing your VMware inventory objects

This topic contains a recommended hierarchy for your VMware inventory objects.

A logical grouping of inventory objects will help you more easily locate ESXi hosts, HA Clusters and virtual machines within vCenter Server. You should first identify this logical grouping, and then create the required inventory objects in vCenter Server, such as datacenters and folders, before adding the Blade Servers to vCenter Server inventory.

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

## Creating and updating high availability clusters

### Related topics

- “Creating an HA cluster” on page 56
- “Adding a new host to an HA cluster” on page 56
- “Migrating a VM to an HA cluster” on page 57
- “Configuring the HA cluster VM options” on page 57
- “Adding alarms to an HA cluster” on page 57

### Creating an HA cluster

- 1 From the vSphere Client, navigate to the hosts and clusters view.
- 2 Right-click on the folder or Datacenter object that will contain the new cluster and select **New cluster** to display the **New Cluster wizard**.
- 3 Type a name for the new cluster in the **Name** field, and select the **Turn on vSphere HA** option.
- 4 Click **Next**.
- 5 Select the **Percentage of cluster resources reserved as failover spare capacity** option, and set both the **CPU** and the **Memory** values to **50%**. Values as low as 30% can be applied based on the availability requirements for your clusters outlined in the workload distribution planning section.
- 6 Click **Next**.
- 7 Leave the Virtual Machine options as provided, and click **Next**.
- 8 Leave the Virtual Machine monitoring set to disabled, and click **Next**.
- 9 Leave the VMware EVC set to **Disable EVC**, and click **Next**.
- 10 Leave the Virtual Machine Swapfile location as provided, and click **Next**. The Ready to Complete page displays a summary of your options.
- 11 Click **Finish** to create the cluster.
- 12 From the vSphere Client, navigate to the hosts and clusters view.
- 13 Right-click on the new cluster in the tree and select **Edit settings>Datastore Heartbeating**.
- 14 Select the **Select any of the cluster datastores** option.
- 15 Click **OK**.



#### Attention

Host monitoring should be disabled when performing any network maintenance that might disable all heartbeat paths between the hosts within the cluster. This is especially important whenever maintenance is to be performed on the management network. This will prevent HA from determining that the maintenance action is a failure and from consequently triggering the isolation responses.

To disable host monitoring, right-click on the new cluster in the tree and select **Edit settings > vSphereHA**. Uncheck the **Enable Host Monitoring** check box.

If there are changes involving the management network, it is advisable to reconfigure HA on all datacenters after the maintenance action is completed.

### Adding a new host to an HA cluster

- 1 From the vSphere Client, right-click on the cluster and select **Add Host** to display the **Add Host wizard**.
- 2 Enter the fully qualified domain name of the ESXi host in the Host field, and enter the **root** user name and password in the Authorization fields.



- 3 Click **Next**. If the Security Alert dialog is displayed, click **Yes**. The **Host Summary** page is displayed.
- 4 Click **Next**.
- 5 Select the applicable vSphere License, then click **Next**.
- 6 Ensure that **Enable Lockdown Mode** is selected, then click **Next** to display the **Ready to Complete** page.
- 7 Review the summary, and click **Finish** to add the host to the cluster.

## Migrating a VM to an HA cluster

- 1 Ensure that the VM is running on a Datastore that is available on all hosts in the HA cluster.
- 2 Use the mouse to drag and drop the virtual machine onto the target ESXi host inside the HA cluster. The **Migrate Virtual Machine dialog box** is displayed.
- 3 Ensure that **High Priority** is selected, then click **Next**.
- 4 Review the **Ready to Complete** page, then click **Finish** to complete the migration. The VM is vMotioned to the target host within the HA cluster.

## Configuring the HA cluster VM options

You can configure the VM options to change the restart order of the VMs in the HA cluster, or to disable restart on some VMs. For example, the most important VMs should have a high VM restart priority. Similarly, when a lower availability cluster exists on the same system, its VMs might require the VM restart priority to be disabled to ensure that they are not restarted when an HA failover occurs.

### To configure the HA cluster VM options

- 1 From the vSphere Client, navigate to the hosts and clusters view.
- 2 Right-click on the new cluster in the tree and select **Edit settings > Virtual Machine options > VM Restart Priority > Host Isolation Response**.
- 3 Leave **Host Isolation Response** as **Leave powered on for all virtual machines**.
- 4 When the HA cluster is being configured for lower availability (see *Planning your Workload Distribution*), set the VM Restart Priority option for any VMs with inherently redundant applications to **Disabled**.
- 5 Set the VM Restart Priority of the VMs by selecting **High**, **Medium**, or **Low** depending on which VM should be started first. The default VM restart priority is:
  - High: Experion Servers and Domain controllers
  - Medium: Console Stations and ACE
  - Low: Flex Stations and Other workload

## Adding alarms to an HA cluster

HA clusters have five alarms to monitor the status of the cluster. Two additional alarms are recommended: *vSphere HA failover resources are insufficient*, and *vCenter Server is unable to find a master vSphere HA agent*.

### To add alarms to an HA cluster

- 1 From the vSphere Client, select the parent object in the tree (the vCenter name).
- 2 Select the **Alarms** tab, then click **Definitions**.
- 3 Right-click in the white space to the right of the existing definitions and select **New Alarm**.
- 4 In the **Alarm name** field, type **vSphere HA Insufficient Failover Resources**.
- 5 Select **Clusters** as the **Monitor** value.
- 6 Select the check box to **Enable** this alarm.

- 7 Select the **Triggers** tab, and click **Add**.
- 8 From the list in the **Event** column, select **vSphere HA Failover resources are insufficient**.
- 9 Click **OK** to create the alarm.
- 10 Right-click in the white space to the right of the existing definitions and select **New Alarm**.
- 11 In the **Alarm name** field, type **vSphere HA Cannot find master**.
- 12 Select **Clusters** as the **Monitor** value.
- 13 Select the check box to **Enable** this alarm.
- 14 Select the **Triggers** tab, and click **Add**.
- 15 From the list in the event column, select **vCenter Server is unable to find a master vSphere HA agent**.
- 16 Click **OK** to create the alarm.

---

## Creating and managing virtual machines

You have successfully built your virtual infrastructure, and you are now ready to create and deploy virtual machines to your virtual environment.

For guidance creating, deploying, and managing virtual machines, see the “Creating new Experion Virtual Machines” section in the *Experion Software Installation Users Guide*.

The preferred method for virtual machines to access media is via ISO files on the datastores or via a network share. If use of ISO files is not possible, then the preferred method is to utilize the CD/DVD drive on the physical node that hosts your vSphere client.

However, it is possible but discouraged to use the Blade Server chassis CD/DVD drive directly from a virtual machine. You must, however, use caution when switching the drive from one Blade server to another.

### Connecting the virtual machine to a CD/DVD drive

- 1 Edit the settings of the virtual machine to use the local host option. If this is successful, you should see a *vmhba* number (for example, `mpx.vmhba32:C0:T0:L0`).
- 2 Use the AMM to select the Blade server to be connected to the CD/DVD drive.
- 3 Open the console of the virtual machine on that host and connect the CD/DVD drive to the **host device**. The host device selected should show the same *vmhba* number as identified in step 1.
- 4 Use Windows Explorer within the virtual machine to verify that the CD/DVD is mounted.



#### Attention

Before connecting the BladeCenter S chassis CD/DVD drive to another Blade in the chassis, you must first disconnect the CD/DVD drive from the host device in the current virtual machine that is using the CD/DVD server.

---



# Administering the BladeCenter S system

## Related topics

“Monitoring the BladeCenter S” on page 62

*This topic describes how to use the Advanced Management Module to monitor the status of the BladeCenter S and view event logs.*

“Moving a USB security device” on page 63

“Shutting down the chassis” on page 64

“Starting up the chassis” on page 66

“Removing and replacing modules” on page 67

---

## Monitoring the BladeCenter S

This topic describes how to use the Advanced Management Module to monitor the status of the BladeCenter S and view event logs.

You can monitor the BladeCenter S from the Advanced Management Module (AMM).

### Prerequisites

You are logged into the AMM console using the Operator account (OPERATOR). See *Establish remote web console connection to the BladeCenter S*.

### To monitor the BladeCenter S

- 1 From the menu pane of the AMM console, click **Monitors**.  
The **AMM Console** is displayed. The system status is the default view, and shows a status section for each of the chassis components.
- 2 Use the System Status Summary links, or scroll to the desired section. Click on the ? icons to display more information about each section.
- 3 When you have finished setting up the BladeCenter S, you can monitor the Blade servers and datastores from vCenterServer. The vCenterServer is the primary source of status information. Use the AMM Console as a backup to vCenterServer when vCenterServer is not available or you need to drill down to the root cause of a BladeCenter S problem.

From the **Monitors** option, you will primarily use the **System Status**, **Event Log**, **LEDs** and **Power Management** options to view status. The remaining options may be used when working with Honeywell Support.

### To view an event log

- 1 From the menu pane of the AMM console, click **Monitors**.
- 2 Select **Event Log** to display a consolidated view of logs stored on the AMM.
- 3 Click on the link in the Event ID column to view the event description and recommended action for the event.



#### Tip

The log has limited capacity. When the log becomes full it wraps, causing the oldest entries to be deleted. The AMM monitors the state of the log and reports events when it is 75% or 100% full. The event log is provisioned to include these events.

---

## Moving a USB security device

If an Experion virtual machine uses a USB security device (dongle), you may need to temporarily move the virtual machine to a different Blade server when:

- The Blade server requires maintenance
- The Blade server fails in a High Availability (HA) cluster

Additional USB ports are available in the media tray, so you will need to move the USB security device to one of the shared USB ports on the media tray.

### To move a USB security device during maintenance

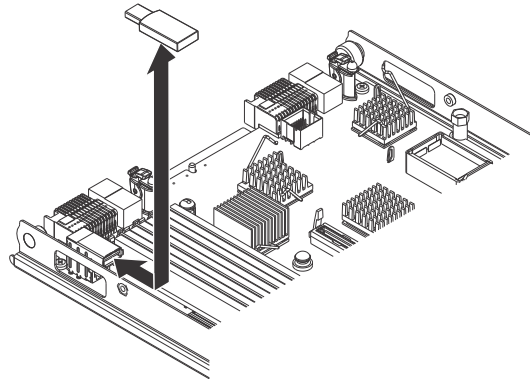
- 1 Ensure that the Experion server is running normally with no copy protection system alarms.
- 2 vMotion the Experion server virtual machine to the destination Blade server. No copy protection system alarms should appear.



#### Tip

Any other workload required during maintenance will also need to be vMotioned according to your vMotion plan.

- 3 Remove the USB dongle from the original Blade server and insert it in the media tray. A copy protection system alarm, stating that the server will be shutdown in 60 minutes, should appear.



- 4 Edit the virtual machine settings on the Experion server virtual machine and remove the original USB device. Then, add the new USB device to the virtual machine.



#### Tip

It may take several minutes for the USB device to be recognized by the destination Blade server.

The Experion server recognizes the USB device and no additional copy protection system alarms appear.

### To move a USB security device during Blade server failure in a HA cluster

- 1 Remove the USB dongle from the original Blade server and insert it in the media tray.
- 2 Press the Media Tray Select Button on the front of the Blade server to associate the media tray with the Blade server.
- 3 Edit the virtual machine settings on the Experion server virtual machine and remove the original USB device. Then, add the new USB device to the virtual machine.



#### Tip

It may take several minutes for the USB device to be recognized by the destination Blade server.

The Experion server recognizes the USB device and no additional copy protection system alarms appear.

## Shutting down the chassis

Use this procedure to shut down the BladeCenter-S chassis. Repeat the procedure for each chassis in the system.

The order is determined by type of workload on the Blades across all chassis' in the system. The Blade or Blades that host vCenter Server should be shut down last, and the Blade or Blades hosting the L2.5 Domain Controller (DC) should be shut down next to last. It is highly recommended that you back up all virtual machines prior to shutdown.

For each ESXi host that has host lock down mode enabled, you need to log into the ESXi host console and disable the host lock down mode. For more information, see the instructions in the “To configure hypervisor for your site” procedure of the *Verifying the hypervisor boot* section.

### To shut down the BladeCenter S chassis

- 1 From vCenterServer, disable each HA cluster within the chassis.
- 2 For each Blade on the chassis that does not contain vCenterServer or L2.5 DC:
  - a Use vCenterServer to re-enable the startup order for the Blade (ESXi host).
  - b Use vCenterServer to shutdown the workload (use the reverse order as identified in the auto start)
  - c [Option for shutting down a single chassis in multi chassis deployment] If resources are available, use the Migrate option from the vCenter Server to move workload to other Blades that do not reside within the same chassis.
  - d [Option to force manual restart of VMs on chassis startup] Use vCenterServer to put the Blade in maintenance mode. This forces you to validate that all virtual machines are shutdown. However, when you power the Blade back up, the auto restart will not execute. You must manually restart the virtual machines.
  - e Use AMM to shutdown the Blade using the option to shutdown the operating system first.
  - f Repeat steps a through e for each Blade that does not host the L2.5 DC or the vCenter Server.
- 3 For the Blade containing the L2.5 DC:
  - a Use vCenterServer to re-enable the virtual machine startup and shut down order for the Blade (ESXi host).
  - b Use vCenterServer to shut down the workload (use the reverse order as identified in the auto start, skipping the vCenterServer if it is on this Blade).
  - c [Option for shutting down a single chassis in multi chassis deployment] If resources are available, use the Migrate option from the vCenter Server to move the workload to another ESXi host that does not reside within the same chassis.
  - d If vCenterServer resides on this Blade, go to step 4.c
  - e [Option to force manual restart of VMs on chassis startup] Use vCenterServer to put the Blade in maintenance mode. This forces you to validate that all virtual machines are shut down. However, when you power the Blade back up, the auto restart will not execute. You must manually restart the virtual machines.
  - f Use AMM to shutdown the Blade using the option to shut down the operating system first.
- 4 For the Blade containing the vCenterServer:
  - a Use vCenterServer to re-enable the startup order for the Blade (ESXi host).
  - b Use vCenterServer to shut down the workload (use the reverse order as identified in the auto start leaving out the vCenterServer).
  - c Disconnect the vSphere client from vCenterServer and reconnect directly to the Blade server (ESXi host) where vCenterServer resides.
  - d Shutdown vCenterServer virtual machine.



- e [Option to force manual restart of VMs on chassis startup] Use vSphere Client to put the Blade in maintenance mode. This forces you to validate that all virtual machines are shut down. However, when you power the Blade back up, the auto restart will not execute. You must manually restart the virtual machines.
  - f Use AMM to shut down the Blade using the option to shutdown the operating system first.
- 5 When the disk activity on the drives has stopped, use AMM to shut down both RAID controllers at the same time. Make sure the status of both controllers is **Off** before powering off the chassis.
  - 6 Pull the power cords, if required.

## Starting up the chassis

Use the following procedure to perform an orderly startup of a BladeCenter-S chassis. Repeat the procedure for each chassis in the system. The startup order is determined by type of workload on the Blades across all the chassis' in the system. For example, the Blade or Blades that host the domain controller of the primary or secondary DNS server should be first, followed by the Blade hosting vCenterServer.

### Prerequisites

Before you power up make sure that:

- Network routers/switches are up and running (implies cabling is re-established).
- Time source is up and running. This includes any physical piece of hardware that serves as the NTP server. If all of your domain controllers are virtual machines, you need only to start up the external time source that is required in this case. For more information, refer to the “Planning for Time Synchronization” topic in the *Virtualization Planning and Implementation Guide*.
- If your DC that hosts the primary or secondary DNS of the virtual workload resides on a physical node, bring the node(s) up and validate that they are running properly.
- If your vSphere client resides on a physical client node on L2.5, bring up the node and validate that it running properly.
- NAS is connected to the management network and powered on. This assumes that the NAS was set up by following instructions in the “Configuring and connecting backup devices” section.

### To start up the BladeCenter S chassis

- 1 Connect the power cords on the chassis to the power supplies. Wait at least 10 minutes to let the chassis components startup and synchronize. Note that the Blades do not start up simply as a result of supplying power to the chassis.
- 2 From a client PC on the management network, connect to the AMM of the chassis to which power has just been restored. Use the instructions in the “Establishing remote web console connection to the BladeCenter S” section. Note that you need to provide the current password rather than the default password.
- 3 When a connection is established, click **Monitors** in the navigation pane, and move through each item to validate that the chassis is operational.
- 4 Determine the startup order of the Blades depending which workload is considered the most critical to get up and running.
- 5 Use the AMM to start the Blades one at a time. Note that if the Blades are in maintenance mode you can start them all at the same time because there is no workload to start up.
- 6 For each Blade in maintenance mode, direct connect to the Blade hosting the vSphere client (direct connect using IP address of the host and host user/password). Verify that each virtual machine on that Blade is powered off. Start up the virtual machines in the desired startup order.  
For example, if the Domain Controllers that host the primary or secondary DNS are virtualized, then you must start those virtual machines first, followed by vCenterServer.
- 7 Use vSphere client that is connected to your vCenterServer to validate that the hosts and virtual machines are all running.
- 8 Re-enable HA on all hosts in those chassis that participate in HA.
- 9 Verify that the backup schedule is active, and that the backup devices are functional.
- 10 Re-enable host lock down mode when you are satisfied your startup has completed successfully.

## Removing and replacing modules

The BladeCenter S platform is designed for maximum availability. Its many redundant features are designed to better protect against a single, catastrophic fault taking down the entire system. A single fault may result in an unplanned removal or replacement of a module. There may also be situations that call for planned removal or replacement of a module. For example, the recommended Honeywell support response to an Advanced Module message may be to re-seat one or more modules to ensure proper connectivity. Another example of planned removal of redundant modules may be to validate system availability prior to commissioning a system for production. In all cases, you must be familiar with proper removal and replacement guidelines to avoid loss of data or configuration. Failure to adhere to these guidelines may require system re-configuration and/or module replacement.

Components with a blue or orange handle can be removed and replaced without disconnecting the BladeCenter S system from the power source.

A blue handle indicates that you can remove the component but you should gracefully shut down any software that is running on the module. This applies primarily to Blade servers. Therefore, you should shutdown virtual machines followed by a graceful shutdown of the ESXi hypervisor. If only a single Blade needs to be shut down and it participates in an HA cluster, then you need only shutdown the ESXi hypervisor. The virtual machines will automatically move to the other Blade in the cluster. However, if a Blade server must be shut down for maintenance purposes, then HA should be disabled prior to the shutdown. All workload must then be manually moved to the backup host.




### CAUTION

**With the exception of individual hard drives and Drive Storage Modules (DSMs),** an orange handle indicates that you can remove the module without any prior software or hardware shutdown.

Furthermore, since the shared storage solution uses RAID 10 with mirroring, removal of healthy, running hard disk drives or DSMs could corrupt the storage configuration and require a rebuild, which can take up to 48 hours.

Carefully follow the guidelines below when removing or replacing modules. To maintain chassis cooling, each module should not be physically out of the chassis for more than 1 minute.. When a module is disconnected from the mid-plane of the chassis, leave the module (or its replacement) in the chassis in a disconnected state for the time periods indicated in the following table:

Module	Procedure
Hard Drives	<p>Remove a failed hard drive from the DSM by lifting the orange handles and pulling on the drive. Insert the replacement hard drive in the same slot from which the failed drive was removed.</p> <p>Healthy running drives should not be removed.</p> <div>  <b>Tip</b>            Depending on system configuration and load, it may take 24 – 48 hours for the storage array to return back to a normal state.         </div>
RSSM RAID Controller	<p>The disk pools, volumes and ESXi hosts are provisioned by Honeywell to avoid data loss. If a healthy RSSM is removed, wait at least 5 minutes before re-inserting into the chassis. This allows background safety checks, redundant controller communication, and RAID system settling to occur.</p> <p>Prior to inserting a pulled RSSM, review the RAID controller logs to confirm that the running RAID controller is the Primary controller, and that it is in a healthy state.</p> <p>No rebuild occurs after inserting a pulled RSSM.</p>
HS23 Blades	<p>Blade servers should only be removed after workload has been accounted for, the ESXi hypervisor has been shutdown, and the Blade is powered off.</p> <p>Hot removal of a running Blade server with installed software is likely to cause corruption to the hypervisor and/or the virtual machines.</p>

Module	Procedure
Intelligent Copper Pass Through Module (ICPM)	Assuming that the network connections have been completed according to the instructions in “Planning the Network Architecture”, a single ICPM can be removed with no impact to the system. Wait at least 5 minutes before re-inserting an ICPM.
Power Supplies	Power supplies can be removed at any time and re-inserted after a minimum of 5 seconds. The Honeywell provisioned Power Management policy allows for two power supplies to be removed without causing Blade servers to shutdown.
Chassis Fans	Chassis fans can be removed at any time and re-inserted after a minimum of 5 seconds. Only remove a healthy chassis fan when the chassis temperature is normal or below normal. Do not remove fans if the chassis temperature is elevated and/or the fans are running at near full speed.
Battery Backup Module for the RAID controller	A single battery backup module for the RAID controller can be removed at any time and re-inserted without any delay.  If both modules are removed, the system will transition from <i>write back</i> to <i>write through</i> cache mode, resulting in a significant decrease in performance. Normal performance is restored when at least one battery module is available to the RSSMs.
Media tray	The media tray for the BladeCenter S is a module that consists of the system LED panel, optical drive, two USB 2.0 ports, and two battery backup module bays for the SAS RAID Controllers. The main ambient temperature sensor is also located in the media tray. If the media tray is removed, the battery backup modules are not accessible. The media tray removal also causes the blowers/fans to run at a maximum speed.  You can remove the media tray while the BladeCenter S system is powered on. Make sure that the USB ports and the DVD drive are not in use before removing the media tray. To remove it, open the release handles and slide the media tray from the BladeCenter S chassis.
Advanced Management Module (AMM)	If the AMM that is currently installed in the BladeCenter S chassis is functioning, make sure that the configuration file has been saved prior to removal. See “Backing up the AMM Configuration” for information about how to save the AMM configuration file.  To remove the AMM while the BladeCenter S system is powered on, disconnect all cables, open the release handle, and slide the AMM out of the BladeCenter S chassis. When you remove the AMM, the fan modules will start running at full speed.  Wait at least 5 minutes before re-inserting the AMM. Re-insert the AMM prior to powering up any Blade server that was not operating prior to or during the time that the AMM was removed.

# Glossary

Definition of terms and acronyms used throughout this guide.

<b>AMM</b>	An acronym for Advanced Management Module.
<b>Advanced Management Module</b>	A hot-swappable BladeCenter S module that you use to configure and manage all installed BladeCenter S components. The AMM provides system management functions and keyboard/video/mouse (KVM) multiplexing for all Blade servers in the BladeCenter S unit that support KVM. It controls a serial port for remote connection; the external keyboard, mouse, and video connections for use by a local console; and a 10/100 Mbps Ethernet remote-management connection.
<b>Battery Backup Unit</b>	Provides backup for the SAS RAID controller module cache. BBUs can provide enough reserve power to store data in your BladeCenter S SAS RAID Controller Module memory cache for 72 hours in the event of an interruption of power.
<b>BBU</b>	An acronym for Battery Backup Unit
<b>BC-S</b>	An acronym for BladeCenter S
<b>Blade</b>	A processing module that occupies a slot in the BladeCenter S Chassis. Blade servers can contain components such as microprocessors, memory, Ethernet controllers, and hard disk drives. They receive power, network connection, and I/O devices (such as DVD drive, keyboard, mouse, video port, USB ports, and a remote monitoring port) from the BladeCenter S chassis.
<b>BladeCenter S</b>	The BladeCenter S is a high-density, high-performance rack-mounted server system. It supports up to six Blade servers that can share common resources, such as power, cooling, management, and I/O resources within a single BladeCenter S chassis. In addition, it provides support for up to twenty four 2.5-inch, SAS hard disk drives.
<b>COA</b>	An acronym for Certificate of Authenticity
<b>datacenter</b>	<p>A datacenter is the primary container of inventory objects, such as hosts and virtual machines. A vCenter Server can contain multiple datacenters.</p> <p>For large virtualization implementations, datacenters can be used to represent organizational units within the enterprise. In addition to providing a container, the datacenter also serves as a boundary when using advanced features including vMotion.</p> <p>For Experion virtualizations, a datacenter is used to contain all of the Experion virtual machines.</p>
<b>datastore</b>	Logical containers that hide the specifics of each storage device and provide a uniform model for storing virtual machine files. Datastores can also be used for storing ISO images, virtual machine templates, and floppy disk images.
<b>Drive Storage Module</b>	A storage module and the hard disk drives installed in that storage module are commonly referred to as integrated shared storage because this storage is integrated in

the BladeCenter S chassis and shared among the Blade servers in the BladeCenter S system. You can install a maximum of two storage modules in the BladeCenter S chassis and each storage module contains hard disk drives.

<b>DSM</b>	An acronym for Drive Storage Module
<b>ESXi</b>	<p>A virtualization layer that runs on physical servers (hosts) that allows the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system.</p> <p>Through ESXi, you can run virtual machines, and you can install operating systems, run applications, and configure the virtual machines. Configuration includes identifying the virtual machine's resources, such as storage devices.</p>
<b>ESXi host</b>	<p>A host is a computer that is running ESXi virtualization software to run virtual machines.</p> <p>Hosts provide the CPU and memory resources that the virtual machines use and give virtual machines access to storage and network resources. Multiple virtual machines can run a host at the same time.</p>
<b>guest operating system</b>	An operating system that runs inside a virtual machine. For example, Microsoft Windows Server 2008 or Windows 7.
<b>host memory</b>	The total amount of physical memory on a physical server (host).
<b>ICPM</b>	An acronym for Intelligent Copper Pass-through Module
<b>IFM</b>	An acronym for IBM Fabric Manager
<b>Intelligent Copper Pass-through Module</b>	A hot-swappable I/O module that provides 14 RJ45 100Mbit/1Gbit operations on uplinks. Each module exposes 2 ports for each Blade Slot. Port 7 and 14 of I/O bay 1 also provide connectivity to SAS RAID controllers.
<b>production ESXi host</b>	An ESXi host that is assigned production workloads.
<b>production workloads</b>	Workloads (that is, virtual machines) associated with the Experion system and process, and encompasses both the application operational workloads and process operational workloads. However, it does not include the management workloads.
<b>management ESXi host</b>	An ESXi host that is assigned management workloads.
<b>management node</b>	A virtual machine, or physical machine, running management workloads, such as vCenter Server, Windows domain controller, and so on. Some management nodes, such as vDR, can only be virtual machines.
<b>management workloads</b>	Workloads (that is, virtual machines) associated with the administration of the virtual infrastructure.
<b>memory over commit</b>	Allocating more memory to the virtual machines than the physical memory available on the ESXi host.
<b>RAID</b>	An acronym for Redundant Array of Independent Disks. A storage technology that combines multiple disk drive components into a logical unit. Data is typically distributed across the drives in one of several ways called <i>RAID levels</i> , depending on the level of redundancy and performance required.
<b>RAID SAS Switch Module</b>	The BladeCenter S SAS RAID Controller Module consists of an integrated SAS Switch combined with a RAID Controller which provides an embedded RAID storage solution with advanced SAN features to the BladeCenter-S chassis.

<b>RSSM</b>	An acronym for RAID SAS Switch Module
<b>SAS RAID Switch Module</b>	The SAS RAID Controller Module provides fully-integrated RAID Storage Area Network (SAN) functionality, inside your IBM BladeCenter S chassis. The SAS RAID Controller Module consists of an integrated SAS Switch combined with a RAID Controller which provides an embedded RAID storage solution with advanced SAN features to the BladeCenter-S chassis
<b>SM</b>	An acronym for Storage Module. See DSM for more information.
<b>SRSM</b>	An acronym for SAS RAID Switch Module
<b>vCenter Server</b>	<p>The central point for configuring, provisioning, and managing virtualized IT environments.</p> <p>The central administration service for VMware ESXi hosts that are connected to the management network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESXi hosts).</p> <p>vCenter Server runs on the management node and connects to the ESXi hosts through the management network.</p>
<b>virtual machine</b>	A virtual machine is a software implementation of a physical computer, which runs an operating system and applications.
<b>virtual network</b>	A virtual local area network that is shared by virtual machines running on the same host.
<b>virtual switch</b>	A virtualized network switch that manages network traffic between virtual machines and physical network adapters on an ESXi host.
<b>VM</b>	An acronym for virtual machine.
<b>vSphere Client</b>	Application that remotely connects to the vCenter Server or ESXi from a Windows computer that is connected to the management network.
<b>vSwitch</b>	An acronym for virtual switch.





# Notices

## **Trademarks**

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

## **Other trademarks**

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

## **Third-party licenses**

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third\_party\_licenses on the media containing the product, or at <http://www.honeywell.com/ps/thirdpartylicenses>.

---

## Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

<http://www.honeywellprocess.com/support>

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

[hpsdocs@honeywell.com](mailto:hpsdocs@honeywell.com)

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

---

## How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

<https://honeywell.com/pages/vulnerabilityreporting.aspx>

Submit the requested information to Honeywell using one of the following methods:

- Send an email to [security@honeywell.com](mailto:security@honeywell.com).
- or
- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

---

## Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, <https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx>.

---

## Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see <http://www.automationcollege.com>.

