Control Server Core - High Availability (HA) Maintenance Guide

Feb 2019
These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Public Information – This document contains non-sensitive information approved for public disclosure.

GE provides the following document and the information included therein as is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Revised: Feb 2019
Issued: March 2017


* Indicates a trademark of General Electric Company and/or its subsidiaries. All other trademarks are the property of their respective owners.

We would appreciate your feedback about our documentation. Please send comments or suggestions to controls.doc@ge.com
Document Updates

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Maintenance and Troubleshooting</td>
<td>New section containing recommended maintenance schedule and common failure modes, indicators, and recovery steps</td>
</tr>
<tr>
<td>A</td>
<td>Datastore File Maintenance</td>
<td>Added this section containing the procedures to access and maintain Datastore files</td>
</tr>
</tbody>
</table>

Acronyms and Abbreviations

- AD: Active Directory
- CA: Certificate Authority
- DNS: Domain Name System
- HMI: Human-machine Interface
- HTTPS: HyperText Transfer Protocol Secure
- ISA: International Society for Automation
- IP: Internet Protocol
- PDH: Plant Data Highway
- RADIUS: Remote Authentication Dial-In User Service
- RAID: Redundant Array of Independent Disks
- RBAC: Role Based Access Control
- SIEM: Security Information and Event Management
- SSH: Secure Shell
- UDH: Unit Data Highway
- VFA: Virtual Field Agent

Related Documents

<table>
<thead>
<tr>
<th>Doc #</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6840</td>
<td>NetworkST 3.1/4.0 for Mark VIe Controls Application Guide</td>
</tr>
<tr>
<td>GEH-6844</td>
<td>Control Server System Overview</td>
</tr>
<tr>
<td>GEH-6846</td>
<td>Control Server Installation and Startup Guide</td>
</tr>
<tr>
<td>GEH-6848</td>
<td>Control Server Hand-over Guide</td>
</tr>
</tbody>
</table>
Safety Symbol Legend

**Warning**
Indicates a procedure or condition that, if not strictly observed, could result in personal injury or death.

**Caution**
Indicates a procedure or condition that, if not strictly observed, could result in damage to or destruction of equipment.

**Attention**
Indicates a procedure or condition that should be strictly followed to improve these applications.
Control System Warnings

**Warning**

To prevent personal injury or damage to equipment, follow all equipment safety procedures, Lockout Tagout (LOTO), and site safety procedures as indicated by Employee Health and Safety (EHS) guidelines.

**Warning**

This equipment contains a potential hazard of electric shock, burn, or death. Only personnel who are adequately trained and thoroughly familiar with the equipment and the instructions should install, operate, or maintain this equipment.

**Warning**

Isolation of test equipment from the equipment under test presents potential electrical hazards. If the test equipment cannot be grounded to the equipment under test, the test equipment’s case must be shielded to prevent contact by personnel.

To minimize hazard of electrical shock or burn, approved grounding practices and procedures must be strictly followed.

**Warning**

To prevent personal injury or equipment damage caused by equipment malfunction, only adequately trained personnel should modify any programmable machine.

**Warning**

Always ensure that applicable standards and regulations are followed and only properly certified equipment is used as a critical component of a safety system. Never assume that the Human-machine Interface (HMI) or the operator will close a safety critical control loop.
Attention

The procedures and methods described in this document apply to the standard Control Server product as originally designed by GE. However, there may be deviations from the standard feature set installed and configured at the time of shipment. Please reference plant-specific documentation provided by your GE representative at the time of installation and commissioning for alternative or supplemental maintenance instructions for your application.

Note

1. Disconnect the equipment from the power supply by removing the plug from the socket-outlet, which is installed near the equipment and easily accessible.

2. There are no serviceable parts. Replace faulty sub-assembly and return defective material to GE Automation & Controls.

Waste Disposal: This mark or symbol on any electrical or electronic product indicates that this product cannot be disposed of in a trash bin. Such products must be returned to the original vendor or to a properly authorized collection point. The black bar under the waste bin symbol shows that the product was placed on the market after 13 August 2005.

Batteries are not meant to be replaced by an operator. A coin cell battery is included in the servers and in the firewall device, and the original manufacturer documentation should be referenced for any applicable end-of-life removal instructions.
1 Overview

The Control Server consists of a product line that can be combined in different configurations to meet the needs of individual sites. The basic architecture consists of one or more server class computers each running a hypervisor. The Virtual Machines (VMs) that run on the hypervisor(s) perform the site functions.

The Control Server product architecture consists of two layers. Within each layer multiple products are available to meet a site's feature, redundancy, size, and workload requirements.

The Control Server Core is the lower architectural layer. It includes the server hardware and the hypervisor software that runs on the server to provide the platform for hosting virtual machines. Various core architectures and options are available to meet a site's redundancy and performance requirements.

The Control Server Module is the upper architecture layer. Various modules supply different types of virtual machines to meet the site's application requirements, and multiple modules can be supported at the same time. Within each module there are typically options for the number and size of VMs supplied, such as the number of Human-machine Interface (HMI) VMs supplied, the number of Virtual Field Agent (VFA) VMs supplied, or the number of Thin Client Terminals that must be supported.

The following sections provide additional information on the Control Server Cores and Control Server Modules that are available.

1.1 Control Server Core

The Control Server Core is the lower architectural layer. It includes the server hardware and the hypervisor software that runs on the server to provide the platform for hosting virtual machines.

There are two Control Server Core architectures available:

- **Simplex Core**: This core supplies a single server where all the Virtual Machines run. Various options are available controlling the size of this server. This core is typically used when the functions that it provides do not need to be redundant.

- **High Availability (HA) Core**: This core supplies a pair of redundant servers and a high-speed interconnection between them to support both manual and automatic failover capability. Virtual Machines can be migrated between the servers, and if one server fails or is shut down then the VMs will run on the remaining server.

A site's redundancy requirements tend to drive the Core selection (Simplex or HA), and its anticipated workloads tend to drive the selection of Platform and Options within the selected Core.

The following sections provide additional information about the Control Server Core products.

1.1.1 Simplex Core

The Simplex Core provides a single server class computer upon which to run VMs. The VMware ESXi hypervisor is used to host one or more VMs to meet the site's application needs.

The Simplex Core product is further subdivided into the Platform and Options available:

- The **Platform** selects the base type of server used. The Platform selection tends to focus on the features and expandability that is available in the platform. Low end platforms may not supply redundant power supplies, and may be more limited in their expandability. Higher end platforms tend to include redundant power supplies and have greater flexibility and range with respect to the CPU power, memory, and disk drive capacities available.

- Various **Options** are available within any one Platform selection. These options control items such as the CPU power, memory, and disk drive capacities available. The site's anticipated workload (number and types of VMs) typically drive the sizing option selection.
1.1.2 High Availability (HA) Core

High Availability (HA) Core supplies a pair of redundant servers and a high-speed interconnection between them to support both manual and automatic failover capability. The VMware ESXi hypervisor is used to host one or more VMs to meet the site's application needs.

Various Options are available to control items such as the CPU power, memory, and disk drive capacities available. The site's anticipated workload (number and types of VMs) typically drive the sizing option selection. Both physical machines must have the same options selected to support the failover options.

The VMware Virtual SAN product is used with the high-speed interconnection between the servers to mirror the virtual hard drives used in each VM on each server and provide failover capability. VMs can be migrated from one host to another without clients even recognizing that a transfer has taken place. In case of a sudden server failure preventing graceful migration, the client may need to reconnect to the VM after it restarts itself on the remaining host - a process that typically takes 15-30 seconds for a typical HMI. Depending upon the platform sizing options selected, a single server running all the VMs may exhibit reduced performance over the normal case of both servers in operation and the site load distributed between them.

1.2 Control Server Modules

The Control Server Module is the upper architecture layer. Various modules supply different types of virtual machines to meet the site's application requirements. Multiple Modules and/or multiple instances of a single Module are supported, with the platform sizing and performance requirements being the limiting factor. There are three basic modules available, and within each module there are typically options on the number and type of VMs supplied.

1.2.1 Domain Services Module

The Domain Services Module provides a pair of redundant Domain Controller VMs and a Certificate Authority VM to establish a Microsoft Active Directory domain at the site. The domain provides for centralized management of users and roles and typically all Windows based VMs are joined to this domain. Computer Hardening is accomplished by joining computers (or VMs) to the domain and using domain Group Policies to apply the hardening policies. Services in the Domain Controllers and Certificate Authority are also used by devices outside of the domain for user identity management and access control.

The Domain Services Module supplies the following Virtual Machines:

• DC1: This is the primary Domain Controller. It provides the domain services listed below.
• DC2: This is the backup Domain Controller. It provides the same features as the primary Domain Controller.
• CA1: This is the Certificate Authority. It provides the Certificate and Public Key Infrastructure (PKI) services listed below.

The Domain Controllers provide the following domain services:

• Microsoft Active Directory Domain Services
• Microsoft RADIUS Server
• Microsoft DNS Server
• Microsoft DHCP Server

The Certificate Authority supports the following domain services:

• Microsoft Active Directory Certificate Authority
• Microsoft Network Device Enrollment Service

The Domain Services Module does not have options for the number and type of VMs supplied, a pair of redundant Domain Controllers and the Certificate Authority (three VMs total) are always supplied.

The Domain Services Module does not have any other core or module dependencies, although using this module in a Simplex Core environment prevents splitting the redundant Domain Controllers across multiple servers.
1.2.2 Thin Client HMI Module

The Thin Client HMI Module provides one or more Virtual Machines typically used for supervisory level control. This includes the HMI, Historian, and Gateway VMs used to configure, monitor, and operate the control system. The VMs in this module are normally accessed by using Thin Client Terminals as the user interface.

The Thin Client HMI Module supplies the following types of VMs:

- **Engineering Workstation (EWS):** This VM type supplies the programming tools and typically acts as the master repository for the control configuration information. (See below for more details)

- **HMI:** This VM type is used for the Operator Interface. In addition to the Operator Interface software it also has the full programming and communication capability. There are typically multiple HMI VMs at a site for redundancy or to segment the operator displays for handling separate plant areas.

- **Historian (HST):** This VM type supplies the Proficy Historian with the Proficy Historian Analysis package. If required, there is typically only one VM of this type at a site.

- **Gateway:** This VM type is used as an interface between control systems or DCS layers. It provides the communication interface between control systems using an agreed upon standard protocol, such as Modbus, GSM, OPC DA, OPC AE, or OPC UA. If required, there are typically two of these VMs supplied for redundancy.

- **Application Server (AppServ):** This VM type is used as a host for control applications, such as a Configuration Management System or an Alarm Server. This VM comes with the communication layers needed to exchange control information, but not the Operator Interface tools or Configuration Tools.

- **Windows Server (WinServ):** This VM type is essentially a Windows Server VM with antivirus software. It has no additional control software on it for communications and is available for loading any site specific applications.

The EWS VM type is unique in that this VM includes software that is typically only installed on one VM at a site. This VM also has a special IP address that, in conjunction with the NetworkST 4.x access control lists, allows it to communicate with and configure network equipment that other VMs cannot reach. The functions that are typically supplied only on this VM type include:

- CMS Server: This provides the central repository for the Configuration Management System (CMS) and the CMS Server that clients use to access it.

- Proficy Licensing Server: This provides the licensing server that coordinates the GE Proficy licenses across all other VMs.

- Microsoft Terminal Services License Server: This (optional) component is used to coordinate licenses across all instances of Terminal Services across all other VMs. This is only required in Many-to-One configurations (see definition below).

- Thin Client Configuration Server: This provides the programming tools, services, and files needed to configure Thin Client Terminals. This includes the Thin Client Terminals firmware and configurations. For some Thin Client Terminal types this information is pushed from this VM to the Thin Client Terminals, in others the Thin Client Terminals are configured to pull the information from this VM.

- Thin Client Module Information: This VM holds a set of sharenames that provide scripts and online documentation for the Thin Client Module.

There are typically two schemes used for connecting Thin Client Terminals to the Thin Client HMI VMs. The selection is typically made based upon the site size, cost targets, redundancy requirements, and the desired relationship between the number of Thin Client Terminals and the number of VMs:

- **One-to-One:** This scheme supports a single Thin Client Terminal logged into a VM at any one time. Multiple Thin Client Terminals are supported, but each VM can only support one logged in user at a time.

- **Many-to-One:** This scheme supports multiple Thin Client Terminals to be logged into a single VM concurrently. The maximum number of Thin Client Terminals that can be logged in is determined by performance and the sizing of the VM, and enforced by the Terminal Services Licensing.

The Thin Client HMI Module supports many options for defining the number and type of VMs to be supplied. The options to select are based upon each site's requirement as to the number and type of VMs along with its One-to-One or Many-to-One configuration. In the Many-to-One configurations, the CPU power and memory to be allocated to each VM may be adjusted within the total limits imposed by the Platform Options selected. This balancing can be done after the initial creation of the VMs and is not required at the time of placing the order. Verify that the Platform Options supply sufficient resources, and those resources can be reallocated or balanced between VMs at any time.
The Thin Client HMI Module requires that the Domain Services Module be installed as it makes extensive use of the Domain Services that it provides. All VMs in this module must be joined to the Domain Services domain.

### 1.2.3 Virtual Field Agent Module

The Virtual Field Agent (VFA) Module provides one or more VMs used for hosting Predix™ applications. The VMs in this module primarily interact with the control system, but applications may also provide an interface (such as a Web Server) for direct access. Various network connectivity options are available to meet the needs of site applications and to address site security policies.

The VFA Module supports the creation of multiple VMs, each running their own Predix applications. This split may be done for performance reasons, or the applications may be split among multiple VMs due to the data that they are dealing with, segmenting different plant areas into their own VMs. The maximum number of VMs is defined by the resource demands of the applications that are run within the VM versus the platform options and the site's performance requirements.

The base VFA Module does not have any other core or module dependencies, but individual Predix applications may add their own dependencies. These may include items such as additional security capability through the Domain Module, or a user interface accessed through the Thin Client Module.
2 Theory of Operations

The Control Server Core provides the hardware and software platform on which to run VMs to perform site functions. The HA Core provides a pair of servers with a high-speed interconnection between them to support both manual and automatic fail-over of VMs between servers.

The following sections provide additional information about the Control Server HA Core product design.

2.1 Hardware

The hardware supplied with the HA Core consists of two layers:

- The Platform selection defines the particular server class computers that are used for the two virtualization servers. These are typically identical in their configuration.
- The Platform Options define the various sizing options available within the Platform selection. Platform Options are typically chosen to accommodate the site's requirements for CPU power, memory, and drive capacity.

2.1.1 Platform

There are three server class computers supplied with the HA Core:

- Two virtualization Host Servers (HS1, HS2) are supplied to host the VMs that perform the site application functions.
- A single Management Computer (MC2) is supplied to host two special VMs supporting the HA architecture:
  - The Hypervisor Witness (HW1) VM is used to arbitrate between the two host servers, defining which is the master in the case of network fragmentation.
  - The Management VM (MC3) is not required under normal operating conditions but contains diagnostic and management tools that can be used to restart the core in case of a complete shutdown and to rebuild certain portions of the core if necessary.

Additionally, one VM runs within the two Host Servers that is used to manage the HA environment. The Hypervisor Control (HC1) VM hosts the VMware vCenter Appliance, which is used to monitor, configure, and otherwise manage the VMware HA environment.

The decision to use the HA Core (instead of the Simplex Core) is typically made to meet site redundancy requirements. Once the decision is made to use the HA Core, the Platform selection addresses the basic features of the host servers.

The Platform selection defines the model of computer used for the host servers, such as:

- Support for redundant power supplies (most platforms used with the HA Core support redundant power supplies)
- Upper limit on the number of CPU slots that are supported, and the type of CPUs that can be used to populate each slot
- Maximum amount of memory that can be added to each server
- Number and type of drive bays available
- Number of expansion slots available for items such as network adapters

Due to its limited and predefined functions, the Management Computer (MC2), which hosts the HW1 and MC3 VMs, does not require any Platform selection or Platform Options. A single configuration of MC2 covers all Control Server HA Core Platforms independent of the Platform and Platform Options chosen for the host servers (HS1, HS2).
2.1.2 Platform Options

Once the base Platform has been selected, it can be customized using Platform Options to control the resources available in each server. The host servers are typically sized to be able to support the entire loading of the site so that in the event of a single host failure all VMs can be hosted on the remaining server. While not a technical requirement, the Platform Options on both servers are typically identical, making the servers interchangeable.

The following Platform Options are typically available on all host server Platforms:

- **The CPU Selection** defines the number of CPUs and the number of cores per CPU. The Platform selection controls the number of CPU sockets that are available. Each CPU socket can be populated by a CPU. The CPU selection controls items such as the speed of the CPU, the amount of cache it possesses, and the number of cores in the CPU. Multi-socket CPU platforms use the same CPU selection for each socket. The most common criteria for CPU selection is the number of cores in the CPU. With Hyperthreading enabled, each CPU core is recognized by the host server as two processors. Each VM is configured with the number of processors that it is allowed to use.

- **The Memory Selection** defines the amount of memory in the host server. Each VM is configured with the amount of memory it is allowed to use.

- **The Network Selection** defines the number of Ethernet ports available to the host (not including the special high-speed interconnections used between the host servers). There are typically a fixed number of Ethernet ports on the host server motherboard, with additional expansion adapters added which contain multiple (typically 2 or 4) additional ports. For redundancy, each network that the host must make available to the VMs uses two ports. Each VM is configured with the networks over which it must communicate, with all VMs within a host server sharing the same physical port connections to that network. Thus, the number of ports required for the host server is the union of all the networks that the VMs require, times two (x2) for redundancy.

- **The Drive Selection** defines the number and type of disk drives in the host server. The Platform selection defines the number of drive bays available in the server and the Drive selection defines the number and type of drives installed in the bays. Refer to the section *Virtual SAN* for details on the type and size of drives and how that correlates to the drive capacity available to the VMs. Each VM is configured with the drive space it is allowed to use.
2.2 Software

The Control Server HA Core uses the VMware ESXi hypervisor to provide the hosting environment for the VMs. In addition to the base hypervisor, two special features are also included:

- The Virtual SAN subsystem is provided to create multiple copies of each VM across multiple servers and keep the images up-to-date in real time.
- The High Availability (HA) option is provided to support migrating VMs between the host servers either manually or automatically upon a hardware failure.

2.2.1 Hypervisor

The VMware ESXi hypervisor provides the base platform on which to run the VMs. It handles the allocation of host resources between VMs (such as CPU, memory, and drive usage) and provides each VM with an environment equivalent to it running on its own separate hardware.

VMware ESXi is a Type-1 bare-metal hypervisor, meaning the computer boots directly into the ESXi hypervisor and it controls the direct access to the hardware in the server. Hardware added to the server must be on the VMware Hardware Compatibility List (HCL) with the associated drivers loaded into the ESXi hypervisor. The hypervisor then exposes the equivalent functionality as virtual devices in each VM. If a VM wants access to the host server hardware, the hypervisor must be configured to pass connectivity through to that VM. For example, if a VM wants to be able to access the DVD drive on the host server, the hypervisor must be configured to map that physical DVD drive as a virtual DVD drive in the VMs.

Care must be taken when mapping a physical device on a host server to a VM. Mapping a physical device to a VM makes that VM ineligible for migration from one host to another since the other host will not have that same hardware mapping or connection. These physical mappings (such as DVD or USB flash drives) should be done only for short periods of time while the device is actively being used, and the mapping should be removed as soon as it is no longer needed. Long term mapping to devices such as a USB flash drive are best served by using an auxiliary device that can be accessed from both hosts, such as creating a sharename from a Thin Client terminal or by using a special Ethernet based USB port hub. Those solutions provide the long term mapping capability while still allowing VMs to migrate from host to host as needed.

2.2.2 Virtual SAN

The Virtual SAN subsystem is designed to keep multiple copies of all VMs disk files on separate servers, and keep them up-to-date in real time. By keeping multiple copies present, it adds a level of redundancy and a recovery path in case of failures.

Virtual SAN is different from a typical server's RAID drive configuration in the following ways:

- A BIOS-level RAID configuration uses additional local resources (drives) to protect against local drive failures. The extra information needed to recover from a failure is all local within that one host.
- Virtual SAN uses a special high-speed interconnection between hosts to keep additional full copies of all files on multiple hosts.

For Virtual SAN to orchestrate the multiple copies of all disk files, it must take over as the interface layer to the drive hardware. The drives to be used under Virtual SAN must not be part of any RAID array at the host computer level.

There are two types of drives in a Virtual SAN environment:

- **Capacity drive** is a drive that is used for storage of VM files. A Capacity drive may be a solid state drive (SSD) or a hard disk drive (HDD).
- **Cache drive** is a drive that is used to cache the latest drive operations. Updates to the Cache drives are the largest part of the traffic across the high-speed interconnection between the hosts. Cache drives must be SSDs to handle the speed and volume of updates.
  - Cache drive sizes are not used to determine the amount of drive capacity available to the VMs.
  - Normally, 70% of a Cache drive is used as a Read cache and 30% is used as a Write cache. If all Capacity drives are SSD then 100% of the Cache drive is used as a Write cache since there is no performance loss by reading all data directly from the Capacity drive.
The two types of drives (Cache and Capacity) are combined into a Disk Group. Each Disk Group consists of one Cache drive and one or more Capacity drives. The Control Server typically uses two Disk Groups in each server.

Adding drive capacity to the host can be accomplished in a number of ways, including:

- The size of each of the capacity drives may be increased. This has no other resource issues, but the non-linear pricing of SSDs may cause this to be a more expensive option than other methods.
- An additional capacity drive can be added to each Disk Group. This requires an available drive bay (one per capacity drive or two total for a normal dual Disk Group server) for each added drive. The advantage of this scheme is it can be used on existing systems to increase capacity without losing any information already on the server. Once the drives have been added to the Disk Groups (an online operation) they will automatically be used as additional capacity.
- Additional Disk Groups can be created. This requires both a Cache drive and a Capacity drive for the new Disk Group, so two drive bays will be required in each server.

The Control Server Platform Options balance the above concepts to meet site needs. As the disk capacity needs of a server increases, it is first addressed by using larger drives as capacity drives, then by using multiple capacity drives per disk group. The current Platform Options have not yet expanded to a point where an additional disk Group has been required, but architecturally that is an option. (The number of available drive bays tends to favor using two Disk Groups with multiple capacity drives per group over additional Disk Groups.)

Virtual SAN uses the concept of Failures To Tolerate (FTT) to determine how many copies of each file are required. If the system is defined to be able to support \( n \) failures, then \( n+1 \) copies of each file are spread among the hosts. The Control Server is the simplest case where there are two servers and FTT is set to 1. With an FTT of 1, Virtual SAN will keep two copies of each file, one on each host. This means that each host in the system will have a copy of every VM at all times, available to be run should the other host fail or be shut down.

The Virtual SAN requires a high-speed connection between the hosts for exchanging Virtual SAN disk updates. This must be a 10 Gbps link (or faster) when using an all SSD configuration. The Control Server uses a special high-speed point-to-point interconnection between the two host servers instead of incurring the added expense of a high-speed network switch. This interconnection uses an expansion card in each host server to provide two point-to-point network connections. Two connections are used for redundancy, and the state of these two connections is set to Active/Active (as opposed to Active/Standby) to allow the hypervisor to orchestrate the flow of network traffic. The two servers should never be operated without these high-speed interconnections - loss of both links at the same time will confuse the Virtual SAN subsystem. Restarting both servers in the presence of the Witness VM (and waiting for them to arbitrate which host is to run which VM) should recover from this condition.
2.2.3 HA

The HA subsystem is designed to allow VMs to migrate between the hosts and to automatically restart VMs should there be a failure of one of the hosts. When combined with the Virtual SAN subsystem, which makes sure there are copies of each VM on both hosts, it provides a high level of redundancy to address site availability requirements.

There are two methods for controlling which host runs which VMs:

• If both hosts are currently running, the VMware vMotion feature can be used to move a VM from one host to another. Since both hosts are running they can coordinate the handoff to make it essentially transparent to the VM and any clients connected to the VM. The Virtual SAN subsystem keeps the disk contents intact, and the vMotion subsystem copies the memory from the running VM to a standby VM on the other host. After getting the standby copy up-to-date in both memory and disk, the two hosts coordinate shutting down the VM on one host and enabling it on the other. Since the disk and memory contents have been copied, the VM picks up right where it left off. It does not lose client connections, and most software cannot even tell that a transfer has taken place.

• If one host suddenly fails, the host that is still functional will detect that the other copy is no longer running and it will restart the VM using its Virtual SAN disk images for that VM. Since it could not obtain the memory contents from the other host, it cannot pick up where it left off and will appear as if the VM has restarted. Clients will need to reconnect to the VM after it has been started. Software will detect that the VM was restarted and can take the appropriate action.

The HA subsystem, which needs to restart VMs upon a partner host failure, can be configured to restart the VMs in a priority order. VMs can be defined with High, Medium, or Low restart priority which controls the relative order in which the VMs are restarted. In the Control Server, where the systems have typically been designed to handle the entire load, this only impacts the order in which the VMs are restarted. In systems where there may not be enough resources to restart all the VMs, the VMs will be started in the priority order until there are not enough resources left to start the remaining VMs. VMs that were already running on the host will not be stopped in favor of higher restart priority VMs, this only controls the VMs that HA must restart on the remaining host.

The HA subsystem attempts to monitor the resources remaining on the hosts and warn if there is a condition where there would not be sufficient resources to handle another failure. Unfortunately, the HA subsystem is not aware of the Virtual SAN subsystem when it performs its disk space calculations. To the HA subsystem, if a host fails then all the files on its drives must be migrated over to another host; it is not aware that Virtual SAN already has a copy of them on the other host. As a result, whenever there is more than 50% utilization of the total Virtual SAN disk space, the HA subsystem will warn of the next failure running out of disk space. This warning can be ignored since there will be no impact on the disk space used because Virtual SAN already has a copy on the other host and a fail-over will not require any additional disk capacity on the remaining host.
2.3 Configuration

2.3.1 Account Management

Control Server Core HA includes the VMware vCenter Appliance VM that is used to form a VMware cluster. A cluster is a collection of individual hosts that share common settings and, when used with Virtual SAN, share a common disk storage space across all hosts in the cluster.

To perform these functions, the vCenter Appliance includes all the items needed to form its own domain, complete with a Certificate Authority. This domain includes the definition of user accounts, security groups, and privileges that combine to determine which users are allowed to perform various functions. As with any identity management system, there are settings that control various password management features, such as password complexity requirements and password expiration. These settings may need to be updated to match site security requirements.

The Control Server does not make extensive use of the VMware domain, as normal operational procedures do not require the definition of multiple classes of users with different privileges. This is not precluded, however, and sites are free to make use of the security groups and local accounts to implement a multi-tier Role Based Access Control (RBAC) scheme of their own. Normally, the Control Server delivers a single administrative level account in the vsphere.local domain for administering the hypervisor hosts.

VMware does have the ability to request identity services from a Microsoft Active Directory system, such as any Control Server with Domain Services or SecurityST available. Since both of these are optional components and Control Server traditionally only requires one level of administrative access, by default the VMware domain is not associated with any Microsoft Active Directory domain. This can be done on site if desired, but a local (vsphere.local) account must be retained for emergency operation. Be careful to avoid a situation where the hypervisor must authenticate a user by contacting a domain controller running in a VM in order to be able to start that domain controller VM.

2.3.2 Networking

The ESXi hypervisor supports the concept of virtual switches. A virtual switch is used similar to a physical network switch but it is used to connect the VMs running in a host server together on an internal Ethernet network. Optionally it can be used to connect that network to a physical network port that is connected to the hypervisor host. In this way, any network that is connected to the hypervisor host can be bound to a virtual switch, and then any number of VMs can have virtual Ethernet adapters that connect to that virtual switch.

Ethernet network redundancy is accomplished at the hypervisor layer. When a virtual switch is created, the configuration of the virtual switch includes options on whether to connect that virtual switch to any physical connections or not. If no physical host connections are included then the virtual switch is used to communicate between VMs within that host and is not available outside of the host. If the virtual switch is connected to at least one physical host port then the virtual switch traffic will be exposed on the external network. Connecting the virtual switch to more than one port provides network redundancy.

Virtual switches support multiple physical connections to support redundant network connections. When multiple connections are used for redundancy there are options on how to address the redundancy. The primary options are:

- **Active/Active**: This scheme allows messages to flow over each network connection concurrently. Ethernet packets are not sent over both ports at the same time; instead they are sent over one port or the other. This means that the total bandwidth available to the system is the sum of the bandwidth available over each port connection. The high-speed Virtual SAN connection between the two hosts uses an Active/Active configuration, allowing the Virtual SAN subsystem to determine how to utilize the additional bandwidth.

- **Active/Standby**: This scheme uses one network connection or the other for communications. Ethernet packets are not sent over both ports at the same time; instead one port is used until it is deemed to have failed at which time the traffic switches to the other port. The total bandwidth available is the bandwidth of each port, they are not additive. This scheme is used for most control zone networks where the redundant networks are used for fail-over availability and not additional bandwidth. This scheme ensures that the total traffic does not creep to the point where both ports are required to support site operation, meaning that if one port (either one) fails, the site will not have adequate network bandwidth. By using a fail-over scheme there is no loss in performance during periods where one port is unavailable. All traffic is simply routed over the other port.
Applying network redundancy at the virtual switch level means that individual VMs only need to have one network adapter per network defined and configured. The VM does not need to implement any network teaming software, it all handled at the virtual switch level.

The network interface can be summed up as follows:

- A network (such as the UDH or PDH) defines a set of interconnections and an IP address range for a specific purpose.
- Networks are often implemented using redundant physical switches and cables to provide redundancy.
- Each hypervisor physical port is connected to a different switch to provide redundancy.
- The hypervisor uses a single virtual switch connected to multiple physical Ethernet ports to provide fail-over redundancy.
- Each VM connects to the virtual switch with a single network adapter, but has the benefit of the external network redundancy defined at the virtual switch layer.
3 Security and Secure Deployment

This chapter introduces the fundamentals of security and secure deployment.

3.1 What is Security?

**Security** is the process of maintaining the confidentiality, integrity, and availability of a system:

- **Confidentiality**: Ensure only the people you want to see information can see it.
- **Integrity**: Ensure the data is what it is supposed to be.
- **Availability**: Ensure the system or data is available for use.

GE recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take appropriate care in securing their GE products and solutions.

Different sites will have different needs and requirements surrounding these concepts. Follow the site's requirements when building, deploying, and using systems, keeping in mind the impact that decisions and procedures will have on the site's security posture.

3.2 I have a firewall. Isn’t that enough?

**Firewalls** and other network security products, including Data Diodes and Intrusion Prevention Devices, can be an important component of any security strategy. However, a strategy based solely on any single security mechanism will not be as resilient as one that includes multiple, independent layers of security.

Therefore, GE recommends taking a *Defense in Depth* approach to security.

3.3 What is Defense in Depth?

*Defense in Depth* is the concept of using multiple, independent layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability, but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs to find a way to circumvent both the firewall and the username/password authentication.
3.4 General Concepts

There are a number of concepts that are used throughout this document that provide many of the building blocks used to improve a site's security posture. This section describes these basic concepts.

**Authentication** is the act of determining or verifying the identity of a user or element that is requesting access to a resource or requesting that a particular action be taken.

- Example: The Microsoft® Windows® Operating System typically defines a username to establish an identity for a user and a password to verify that the user is in fact who they claim to be.
- Example: Many communications schemes use a Certificate to verify the identity of the endpoint (or endpoints) of that communication. As part of the initiation of the communication link one or both sides provide their certificate to verify their identity.

**Authorization** is the act of determining what identities are allowed (authorized) to access a resource or perform an action. Most authorization schemes support multiple levels of authorization, such as a distinction between the ability to view an item versus the ability to modify an item.

- Example: The Microsoft Windows Operating System supports multiple levels of access on items (such as ReadOnly versus ReadWrite access to a file) and a set of operating system privileges to control actions that users may take.
- Example: The Mark VIe controller in Secure State uses a user's certificate to determine the level of commands that the user can perform, such as Read, Set (write), and Download (reconfigure).

**Access Control Lists (ACLs)** are often used as a method of binding together the requester's identity with the level of access allowed. These ACLs are defined on a per-item basis, so different items may have different ACLs.

- Example: The Microsoft Windows Operating System supports ACLs on files and devices to define which users have what access rights to those items.
- Example: The network switches support ACLs on their administrative interfaces to define which elements of the system have the right to access the administrative functions.

**Note** When done at the operating system level, ACLs protect an item no matter what tool (program) is used to attempt access - this is called authoritative security. This is a stronger level of protection than when the tool being used determines whether to allow access or not - this is called cooperative or client-based security. Cooperative security can be bypassed by using a different client to access the resource, authoritative security cannot be bypassed as easily.

The concept of **Least Privileges** states that each user should be granted only the access rights and privileges that they need to perform their work function. This protects items and configurations against inadvertent changes by users, possibly because of malware that the user has inadvertently triggered.

- Example: The Microsoft Windows Operating System supports the concept of Administrator level access for making changes to the operating system and software running on the computer. If a user is running with administrative access, any malware that they trigger could alter the operating system or any program in any way that it desired. If the user is running in a non-administrative account it is limited in the changes that it can make.
- Example: The ToolboxST* subsystem supports a Users and Roles concept to define what operations a user is allowed to take, such as forcing variables, issuing alarm acknowledge and reset commands, or downloading configurations to controllers.

The concept of **Role Based Access Control (RBAC)** is a consolidation of using the user's identity (authentication) and their allowed rights (authorization) in a slightly easier to maintain manor. An intermediate concept of a user's Role is introduced, which defines a collection of users with shared access rights and privileges. This simplifying scheme has a number of benefits:

- Authorization (done on a per-item basis) is done not to a set of user identities, but instead to a Role - it's ACL is not a list of usernames but a (much smaller) list of Roles. As users are added and removed from the system the ACLs on each item do not have to change since they were tied to the Roles and not the users, making updates very fast and efficient.
- Reporting on the members of a single Role is quick and easy compared to having to visit all items and examine their individual ACLs.
• If a user's Role changes (their job requirements change) it is a simpler task to assign them to a new role, and perhaps change it back again if the change was only temporary.
• New roles are typically easy to define as the site's operating procedures change and different classifications of users are required or different sets of privileges are identified.
• Example: The Microsoft Windows Operating System has a single security group that grants Administrative access to computers - the Administrators group. Adding or removing a user to the Administrators group will grant or revoke the user's administrative privileges and the individual ACLs on all files and devices does not have to be changed.
• Example: The ToolboxST subsystem supports a Users and Roles concept, which defines what rights and privileges are given for each Role. If a site decides to change whether the Operators role is allowed to force variables, granting or revoking the Force privilege to the Operators role is all that is required - there is no need to change each user's privileges.

3.5 What is Hardening?

Hardening a system includes taking steps to reduce attack surfaces that may be used in an attack on the system. These steps include removing functions that are not essential and changing system settings to help deter attacks. Each section in this manual includes information on how to help harden each component, but the following concepts apply to most all products:

• Disable unused Servers and Services on each device.
• Create and maintain the list of users and their rights. Disable or remove a user's account as soon as the person is no longer granted access rights to the equipment.
• Implement the site's password policies, where possible by configuring the equipment to reject passwords that don't meet the standards automatically.
• Remove all as shipped accounts or (if the account is to remain) change all passwords as soon as feasible during the site commissioning process. Implement strict site policy and controls to limit the exposure of passwords.
3.6 General Recommendations

The following general recommendations should be used to improve the security posture at the site:

• Provide physical security for all devices - many, if not most, devices can be compromised by an attacker that has physical access to the device at startup/boot time or direct access to non-volatile media that the device can boot from (hard drive, flash memory, and such). Access to network equipment (switches, routers) can allow for introduction of new devices onto the networks, including network monitoring equipment.

• Disable unused services on devices to reduce the mechanisms available for attacks.

• Wherever possible, configure the site's password requirements (length, complexity...) into the devices or operating systems to have each device enforce them automatically. If it cannot be automatically enforced it must be done procedurally.

• Implement Role Based Access Control wherever available, and keep the list of users and roles current.

  − Some system components allow for logging (auditing) failures, use these if available - preferably logging to a centralized site SIEM (if available) for both convenience and pattern analysis across devices.

• Implement a site-wide scheme for applying software patches, especially those defined as security patches.

• Implement a site-wide scheme for supplying anti-virus software wherever appropriate, including a method to keep the anti-virus signatures up-to-date.

• Implement a Network Intrusion Detection scheme for communication traffic where appropriate, especially traffic that crosses an electronic security perimeter.

Limiting visibility to the control system is a strong defense-in-depth approach to help prevent attacks. This is accomplished by using separate communications networks (Virtual Local Area Networks or VLANs) to isolate different types of equipment, then tightly controlling the network traffic that can cross from one VLAN to another. There are various schemes and recommendations (ISA-99, IEC-62443) that include network segmentation and they should be followed when making any networking changes or while introducing new equipment to the control system.

• Consider using a dedicated point-to-point link instead of a shared network for dedicated functions within the same network zone. Never bridge network zones using a dedicated link, always go through a router that provides controlled access (and optional logging).

• Consider using an additional firewall even within a network zone to add additional constraints on traffic, especially if the traffic includes a protocol that does not support authentication.

• Consider using the Windows Firewall IPsec settings in an HMI or Engineering Workstation to protect protocols that do not support authentication (such as Modbus or GSM). This adds an extra layer of protection in that clients that do not know the IPsec keys will not be able to connect.

  − This is stronger protection than using just the Windows Firewall IP address or MAC address filter, as both IP addresses and MAC addresses can be spoofed.

  − If a site requires encryption of protocols that do not support encryption the Windows Firewall IPsec layer can be used to encrypt the traffic (in addition to providing client-server authentication).

Visibility into the control system is not limited to just communication links, it also includes removable media. There are many instances of malicious software delivered to control systems via USB (thumb or pen) drives as well as via CDs and DVDs.

• Verify the source and integrity of media before placing it into site equipment.

  − Software distributions should be verified by whatever method the manufacturer supports, such as signed installation files or a separate web site that lists the hashes for the files on the distribution media.

  − Use of password protected media does not ensure that the media is free from malicious software, but it does help prevent the media from being infected while left unattended.

• Make sure that the AutoRun option in the Windows Operating System is disabled to help prevent software from being automatically run when the media is inserted into the computer.

• Typically all USB ports cannot be disabled on an HMI or Engineering Workstation as they are used for peripherals (keyboard, mouse, speakers) and hardware license keys. If these functions can be supported by using internal USB ports, it may be possible to disable the external USB ports if desired.

• Consider using hardware USB port locks to prevent access to the USB ports, and/or pulling the front or rear USB port connectors coming from the computer's motherboard.
Consider using additional software packages (such as the Sophos™ Anti-Virus package supplied with the SecurityST product) to control access to the USB ports on computers.

Consider blocking the use of USB ports on all but one or two computers (often the Engineering Workstation[s]) to limit USB exposure, then use the internal network to transfer the information to the computers that need it.

3.7 Specific Recommendations

The VMware vCenter Appliance includes the definition of a domain used by the VMware components to form a cluster. This domain supports full Role Based Access Control (RBAC) through the use of individual user account, Roles, and assigned permissions.

- Update the VMware password policies to match the site password policies.
- Consider using individual user accounts if accountability is a site requirement.
- If multiple levels of user access are required, such as a set of users that may need to start and stop VMs but should not be allowed to create or destroy VMs, consider setting up full RBAC. This would include:
  - Setting up Roles (or using existing predefined Roles) and assigning users their appropriate Role.
  - Assign the privileges required to the Role, limiting the privileges granted to only those required to meet the Role's job functions.
  - If required, use the VMware capability to grant users or Roles privileged access to certain VMs while restricting access from other VMs.

Various networks are typically available at a site, which leads to decisions about the networks made available to each host server and then to the VMs that are running within the server.

- For network security purposes, host servers are typically connected only to networks within one network zone at the site. Routing of communications between zones should be done via external routers, not within the Control Server. Keeping all communications within one network zone prevents the ability to cross network zones due to potential vulnerabilities in the hypervisor software.

**Note** Even if networks in multiple zones are available to the host server, individual VMs should not be configured with network connections to multiple zones.

- The network connections provided to each VM should be limited to only the networks that the VM requires.
- VMs should never be configured to bridge networks.
- In no case should a virtual switch inside a host server bridge multiple networks. There should be one virtual switch defined for each network, and if VMs require access to multiple networks they should be created or configured with multiple network adapters.
- Care should be taken deciding which network should be used for the host server's hypervisor management network.
  - If available, a separate limited access hypervisor management network should be used.
  - The management interface should not have a default gateway (or static route) defined which would allow access to it from outside of its native network zone unless that is a site requirement. If that is a requirement, consider the use of routers and firewalls to limit management access to only the devices, ports, and protocols required.

The ESXi hypervisor supports a management console for diagnostic and maintenance purposes. This console is available locally (a connected monitor and keyboard) or over a Secure Shell (SSH) network connection on the management network.

- Knowledge of the username and password required for hypervisor console access should be limited to only those with a valid need to know.
- The local console should only be enabled when needed for maintenance or diagnostic operations, and should be disabled as soon as they are completed.
- The SSH console should only be enabled when needed for maintenance or diagnostic operations, and should be disabled as soon as they are completed.
- The hypervisor management network should not have a default gateway or static route defined which would make the SSH console reachable from outside the management network itself. If the management network is made routable it...
should be protected by a router and/or firewall where the SSH port (22) is not included in the routable protocols unless it is an absolute site requirement.

- When an SSH connection is established, the client will receive the server certificate as part of the initial handshake. The SSH client should present the server certificate information to the user and ask if the server should be trusted. The site should provide a mechanism for users to determine if the server should be trusted based upon its certificate, and users should be warned not to provide login credentials to devices that are not trusted. This helps prevent man-in-the-middle attacks from obtaining the hypervisor login credentials.

Physical access to the host servers should be controlled:

- Users with physical access may be able to boot the servers off of foreign media, potentially compromising the server.
- Users with physical access may be able to swap the contents of physical devices (DVD drives, USB drives) that are connected to the VMs.

The host server USB ports are available for mapping to VMs, but care should be taken using these ports for that purpose:

- Use of host server USB ports will require physical access to the host servers.
- Mapping a physical device (DVD or USB) to a VM will make it ineligible for migration from one host to another. This may impact the availability of the VM.
  - The device should be unmapped from the VM as soon as the required operations have been completed.
  - If multiple VMs require access to the contents of media (such as DVD or USB drives) consider mounting the media on one VM and copying the contents to that VM. That VM can then create a sharename which can be used by all other VMs to access the content without having to mount the media in each VM or leave it connected to the VM long term. The sharename can be set to read-only for security, and can be removed when the content is no longer needed. This method is often used for site software or anti-virus signature updates.
  - If one or more VMs require long term access to media, consider mounting the media on a Windows based Thin Client terminal (if present) and making the content available via a sharename. This scheme allows the VMs to access the content while still being able to migrate from host to host as needed.
  - If one or more VMs require long term access to media, consider mounting the media on an Ethernet based USB port concentrator. This scheme allows a single VM to access the content as if it was mounted to that VM while still allowing the VM to migrate from host to host as needed.
## 4 Maintenance and Troubleshooting

### 4.1 Maintenance Recommendations

The following table provides maintenance procedures that users should perform for the Control Server and the recommended frequency.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Maintenance Item</th>
<th>Maintenance Procedure</th>
</tr>
</thead>
</table>
| Daily     | Check for Alarms on Control System Health (CSH) Viewer | Open the Control System Health Viewer and disposition all items not in OK (green) state. 
*Refer to Figure 1 CSH Alarm Viewer Components with OK State.* |
| Monthly   | CimView Restart  | 1. Close all CimView screens.  
2. From the Start menu, open CIMPICITY* Options within the Proficy HMI SCADA group.  
3. From the Projects tab, select the currently running project and click Stop.  
4. Click OK to save the setting and close the window.  
5. Reopen CimView screens normally.  
*Refer to Figure 2 CIMPICITY Options.* |
| Quarterly | Reboot Thin Clients | 1. Disconnect from the currently selected VM.  
2. From the Windows VM Start menu, click the Power icon (top right corner) and select Disconnect.  
3. From the Thin Client operating system, select Restart. |
| As Needed | Restart Windows VMs as required when applying patches | Patches indicate the need to restart the VM. Restart may need to be done manually or the patch may automatically restart the VM. Reconnect to the VM after restart. |
Figure 1 CSH Alarm Viewer Components with OK State
4.2 Common Failures Modes, Indicators, and Recovery

The following table lists common failures and events in the Control Server and provides failure indicators and recovery instructions.
## Failure Indication and Recovery Instructions

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Event</th>
<th>Impact</th>
<th>Indicators</th>
<th>Recovery Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>HS# Failure</td>
<td>Host is unavailable due to a hardware failure, ESXi crash, or loss of power</td>
<td>VMs on the affected host will be migrated to the remaining host in the cluster. The affected host is not available to participate in the VSAN quorum and the loss of the remaining host or HW1 results in total loss of all VMs.</td>
<td>CSH alarms indicate the loss of the host. Refer to Figure 3 Alarm Viewer Host Loss Alarm, Figure 4 Host Loss in CSH Diagnostics Tab, and Figure 5 Host Loss in CSH Status Tab. vCenter alarms indicate a loss of power and/or network connectivity. Refer to Figure 6 VCenter Host Loss Alarms. ESXi displays a purple crash window when the user connects a VGA monitor directly to the affected host. Thin Clients connected to the VMs hosted on the affected host are disconnected after a 30-second timeout period. The client exits to the Thin Client desktop.</td>
<td>1. Reboot the affected server. 2. Once the affected server is returned to operation, migrate VMs back to the server per the 4108 to balance the VMs across the system.</td>
</tr>
<tr>
<td>Thin Client Session Drop</td>
<td>Thin Client drops the remote session to the VM</td>
<td>The user is no longer connected to the VM.</td>
<td>The Thin Client stops updating the screens and graphics for 30 seconds, then returns to the Thin Client desktop.</td>
<td>Reboot the Thin Client and relaunch the session into the VM.</td>
</tr>
<tr>
<td>HC1 Failure</td>
<td>HC1 powers off or crashes</td>
<td>HC1 is unable to access the vCenter client to observe or modify the VM infrastructure.</td>
<td>CSH alarms indicate the loss of the VM. vCenter Client is not accessible.</td>
<td>Reboot HC1 (wait ~20 minutes to access the Web Client).</td>
</tr>
<tr>
<td>MC2 Failure</td>
<td>MC2 is unavailable due to hardware failure, ESXi crash, or loss of power</td>
<td>Loss of VMs on MC2 (MC3 and HW1). HW1 is not available to participate in the VSAN quorum and the loss of HS1 or HS2 results in total loss of all VMs.</td>
<td>CSH alarms indicate the loss of a host and, by extension, the loss of a VM (HW1 and MC3). Remote sessions to MC3 are disconnected.</td>
<td>1. Reboot MC2. 2. Reconnect remote sessions to MC3.</td>
</tr>
<tr>
<td>HW1 Failure</td>
<td>HW1 and/or MC2 powers off or crashes</td>
<td>HW1 is not available to participate in the VSAN quorum and the loss of HS1 or HS2 results in total loss of all VMs.</td>
<td>CSH alarms indicate the loss of HW1 or loss of connectivity to HW1.</td>
<td>1. Check if MC2 has failed. 2. Reboot HW1 (and/or MC2).</td>
</tr>
<tr>
<td>MC3 Failure</td>
<td>MC3 and/or MC2 powers off or crashes</td>
<td>MC3 is unavailable. S and R share drives are not available on all VMs.</td>
<td>CSH alarms indicate the loss of MC3. Remote sessions to MC3 are disconnected.</td>
<td>1. Check if MC2 has failed. 2. Reboot MC3 (and/or MC2).</td>
</tr>
<tr>
<td>Subsystem</td>
<td>Event</td>
<td>Impact</td>
<td>Indicators</td>
<td>Recovery Steps</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Loss of Network Connection to</td>
<td>Single network connection is lost to a 1GB NIC on the Control Server</td>
<td>There is no immediate impact to operations. However, a second failure could prevent communication to and from all VMs on that host and the host itself.</td>
<td>CSH alarms indicate loss of 1GB network. Refer to Figure 7 1GB Network Loss in CSH Diagnostics Tab and Figure 8 1GB Network Loss in CSH Status Tab.</td>
<td>Resolve the network connection.</td>
</tr>
<tr>
<td>Control Server</td>
<td></td>
<td></td>
<td>vCenter alarm indicates a loss of network connection. Refer to Figure 9 VCenter 1GB Network Loss Alarm.</td>
<td></td>
</tr>
<tr>
<td>Loss of 10GB Link Across Servers</td>
<td>Single network connection is lost to a 10GB NIC on the Control Server</td>
<td>There is no immediate impact to operations. However, a second failure could prevent replication of VMs between hosts and prevent VMs from migrating efficiently.</td>
<td>CSH alarms indicate loss of 10 GB network on both hosts. Refer to Figure 10 10GB Network Loss in CSH Diagnostics Tab and Figure 11 10GB Network Loss in CSH Status Tab.</td>
<td>Resolve the network connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vCenter alarms indicate a loss of network connection on both hosts. Refer to Figure 12 VCenter 10GB Network Loss Alarm.</td>
<td></td>
</tr>
<tr>
<td>Loss of Disk</td>
<td>Single disk failure occurs from a single host</td>
<td>The datastore is reduced in overall capacity</td>
<td>CSH alarms indicate disk failure. Refer to Figure 13 Alarm Viewer Disk Failure Alarm, Figure 14 Disk Failure in CSH Diagnostics Tab, and Figure 15 Disk Failure in CSH Status Tab.</td>
<td>Reseat or replace the failed drive.</td>
</tr>
<tr>
<td>VM Migrate</td>
<td>VM is migrated from one host to another</td>
<td>There is no direct impact to operations. Operations is made aware that the VM is now hosted on a different server.</td>
<td>WorkstationST Alarm Viewer indicates an event. Refer to Figure 16 Alarm Viewer VM Migrated Alarm.</td>
<td>Make sure that the VMs are balanced between the hosts to achieve maximum availability in the event of a host failure.</td>
</tr>
<tr>
<td>VM Powered Off</td>
<td>VM is powered off</td>
<td>With the VM powered off, remote connections and other services for that machine are not accessible.</td>
<td>CSH alarms indicate that the VM is powered off. Refer to Figure 17 VM Powered off in CSH Diagnostics Tab and Figure 18 VM Powered off in CSH Status Tab.</td>
<td>Restart the VM using vCenter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Remote sessions to that VM are disconnected. All communication services for that VM are lost.</td>
<td></td>
</tr>
</tbody>
</table>
Figure 3 Alarm Viewer Host Loss Alarm
Figure 4 Host Loss in CSH Diagnostics Tab
Figure 5 Host Loss in CSH Status Tab
Figure 6 VCenter Host Loss Alarms
Figure 7 1GB Network Loss in CSH Diagnostics Tab
Figure 8 1GB Network Loss in CSH Status Tab
Figure 9 VCenter 1GB Network Loss Alarm
Figure 10 10GB Network Loss in CSH Diagnostics Tab
Figure 11 10GB Network Loss in CSH Status Tab
Figure 12 VCenter 10GB Network Loss Alarm
Figure 14 Disk Failure in CSH Diagnostics Tab
Figure 15 Disk Failure in CSH Status Tab
<table>
<thead>
<tr>
<th>Device Time</th>
<th>Type</th>
<th>Alarm State</th>
<th>Class</th>
<th>Active</th>
<th>Primary Language Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-01-30 13:25:1...</td>
<td>Event</td>
<td>Active (0 → 1)</td>
<td>Virtual...</td>
<td>No</td>
<td>Virtual Machine CRM10SVR has been migrated to Server ControlServer1_HS1</td>
</tr>
<tr>
<td>2019-01-30 13:25:0...</td>
<td>Event</td>
<td>Active (0 → 1)</td>
<td>Virtual...</td>
<td>No</td>
<td>Virtual Machine CRM10SVR has been migrated from Server ControlServer1_HS2</td>
</tr>
</tbody>
</table>

**Figure 16 Alarm Viewer VM Migrated Alarm**
Figure 17 VM Powered Off in CSH Diagnostics Tab
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The configured device type of the virtual machine</td>
<td>Workstation</td>
</tr>
<tr>
<td>The Name of the Server Currently Hosting this Virtual Machine</td>
<td>HS2</td>
</tr>
<tr>
<td>The overall Virtual Machine status reported by VM ware</td>
<td>OK</td>
</tr>
<tr>
<td>The Power state of the Virtual Machine. 0=Off, 1=On, 2=Suspended.</td>
<td>Powered Off</td>
</tr>
<tr>
<td>The virtual machine is critical. Alarms will be generated when the machine is not available.</td>
<td>True</td>
</tr>
<tr>
<td>Virtual Machine Description</td>
<td></td>
</tr>
<tr>
<td>Virtual Machine overall status. 0=OK, 1=Warning, 2=Error.</td>
<td>Error</td>
</tr>
</tbody>
</table>

*Figure 18 VM Powered Off in CSH Status Tab*
5 Common Procedures

The following sections outline some of the common procedures used in the Control Server Core — HA environment. These instructions reference the Architecture Specification for the product being installed for detailed settings, making these instructions applicable for many different Control Server Modules (Domain, Thin Client, VFA, and so forth).

5.1 VM Creation

There are two different methods used to create the VM:

- **Create VM**: Use this procedure to create a new VM. The next step in the process is typically to boot off of operating system installation media to install the operating system and build the system up from there.

- **Import VM**: Use this procedure to import a VM that has been previously built and exported from another system. The files imported are the *.ova or *.ovf files, which define the configuration and content of the VM.

Follow the procedure that is most appropriate for the VM that you are creating or importing.

5.1.1 Create VM

This section provides the procedure to create the VMs using the vCenter Web Client interface.

➢➢ To create a Virtual Machine

1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with administrative privileges.
3. From the Home screen, select Hosts and Clusters.

   **Note** You may need to expand the Tree view for the items to become visible.

4. Expand Datacenter1, then expand Cluster1 and select the desired host.
5. Right-click on the host and select New Virtual Machine, then select New Virtual Machine.
6. From the Select a creation type dialog box, select Create a new virtual machine and click Next.
7. From the Select a name and folder dialog box, perform the following steps:
   a. Enter the VM name.
   b. Select the Datacenter1.
   c. Click Next.
8. From the Select a compute resource area, choose the desired host (it will default to the one you right-clicked on to start this process) and click Next.
9. From the select storage dialog box, accept the default, and click Next.
10. From the Select compatibility dialog box, accept the default and click Next.
11. From the Select a guest OS dialog box, select Microsoft Windows Server 2012 (64-bit) and click Next.
12. From the Customize hardware dialog box (starting on the Virtual Hardware tab), perform the following steps:
   a. Set the CPU field to the appropriate value.
   b. Set the Memory field to the appropriate value.
c. Set the **New Hard disk** field to the appropriate value.

d. **[Single Network]** If the VM has a PDH address but no UDH address, set the **New Network** field to **PDH**.

e. **[Dual Network]** If the VM has both a UDH and a PDH address, perform the following steps:

   i. Set the **New Network** field to **UDH**.

   ii. From the **New Device** drop-down menu, select **Network** and click **Add**.

   iii. For the **New Network** option just added (at the bottom of the list), select **PDH** and ensure that the **Connect…** option is enabled (checked).

   ______________________________

   **Note** It is very important to set the **FIRST** adapter to UDH and the **SECOND** adapter to PDH - do not reverse this order!

   ______________________________

f. If a copy of the operating system installation DVD has been uploaded to the appropriate Datastore, perform the following steps:

   i. Set the **New CD/DVD Drive** field to **Datastore ISO File**.

   ii. Expand the **Build Datastore**, select the directory with the ISO image, select the ISO file, then click **OK**.

   iii. Enable (check) the **Connect…** option on the **New CD/DVD Drive** option line.

g. Expand the **Video Card** entry and set the **Number of Displays** and **Total video memory** fields to appropriate values.

h. Select the **VM Options** tab.

   i. Expand the **Boot Options** entry and set the **Firmware** field to **EFI**.

   j. Click **Next**.

13. In the **Ready to complete** dialog box, click **Finish**.
### 5.1.2 VM Import from OVA or OVF File

Virtual Machines can be created by importing copies of other VMs. This procedure is often used for VMs that are *Appliance* VMs - one copy duplicated multiple times or across multiple sites. This procedure provides the procedure to create a VM by importing an OVA or OVF file.

**Note** An OVA file is a single .zip file container that includes VM settings as well as the content of all hard drives for a VM. An OVF file contains the VM settings, but must be accompanied by other files in the same directory (typically *.vmdk) to supply the contents of its hard drive(s). There are utility programs available to convert between a single self-contained OVA file and the set of OVF and supporting files - there is no functional difference and you can use either type of distribution when creating the VM.

➢➢

To import a VM from an OVA or OVF file

1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with administrative privileges.
3. From the Home screen, select Hosts and Clusters.

   **Note** You may need to expand the tree view for the items to become visible.

4. Expand Datacenter1, then expand Cluster1 and select the host you want to use to host the new VM (standard: https://172.16.199.8).
5. Right-mouse click the selected host and select Deploy OVF Template.
6. From the Select source dialog box, perform the following steps:
   a. Select Local File, click Browse, navigate to the OVA or OVF file, select it and click Open.
   b. Click Next.
7. From the Review Details dialog box, click Next.
8. From the Select name and folder dialog box, perform the following steps:
   a. In the Name field enter the desired VM name.
   b. In the Select a folder or datacenter field select Datacenter1 as the destination.
   c. Click Next.
9. From the Select storage dialog box, perform the following steps:
   a. In the VM Storage Policy field select vsanDatastore.
   b. Click Next.
10. From the Setup networks dialog box, perform the following steps:
    a. For each network defined, set the Destination column to the desired network for the associated Source network.
    b. Click Next.
11. From the Ready to complete dialog box, click Finish.
12. In the Recent Tasks display, the Status column indicates the progress of the VM creation.

**Note** Wait until the status displays Completed. Depending upon the size of the VM hard drives, this can take 10 to 20 minutes (or more).
13. Select the VM just created (in the tree view).

14. Right-click the selected VM, select **Edit Settings**, and perform the following steps:
   a. Set the **CPU** field to the appropriate value.
   b. Set the **Memory** field to the appropriate value.
   c. Set the **Hard disk** field to the appropriate value.
   d. For each **Network adapter <n>**, verify that the correct network is selected and the **Connect at power on** check box is enabled.
   e. Set the CD/DVD drive 1 to **Client Device**.
   f. Expand the **Video Card** entry and perform the following steps:
      i. Set the **Number of Displays** field to the appropriate value.
      ii. Set the **Total video memory** field to the appropriate value.
   g. Select the **VM Options** tab, expand the **Boot Options** entry, and set the **Firmware** field to the appropriate value.
   h. Click **OK**.
5.2 VM Powerup

➢ To power on a VM
1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with administrative privileges.
3. From the Home screen, select Hosts and Clusters.
4. Expand the tree view, locate and right-click on the desired VM, select Power, then select Power On.

5.3 VMware Integration Tools Installation on Microsoft Windows Operating Systems

➢ To install VMware integration tools on Microsoft Windows operating systems
1. Log into the Management VM (MC3).
2. Open a vSphere Client Console Connection to the VM's host server.
3. From the main Inventory page, select the VM on which you want to install the tools.
4. Select the Console tab for the VM and make sure you are logged into the VM using an Administrator account.
5. Minimize any open windows (such as the Initial Configuration Task window) to make the installation dialogs visible.
6. Right-click on the VM in the tree view and select Guest, then select Install/Upgrade VMware Tools.
7. When the AutoPlay dialog box displays in the VM console window, select Run setup64.exe.

Note If you miss this timed dialog box, open a Windows Explorer window, navigate to the pseudo-DVD drive with the label VMware Tools, and double-click on it.

8. Select Typical installation, then click Next.
9. Select Install.
10. Click Finish at the end of the installation.
You will be prompted to restart the VM.
5.4 VMware Tools Upgrade

*Note* Upgrading the VMware tools in a VM will require a reboot of the VM.

➢ To upgrade the VMware tools in a VM

1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with Administrative privileges.
3. From the Home screen, select **Hosts and Clusters**.
4. Expand the tree view and locate and select the desired VM.
5. Select the **Summary** tab.
6. The **VMware Tools** line indicates the current status of the VMware tools:
   - **Current** status indicates that the VM is at the current tools level and no upgrade option is available.
   - **Upgrade Available** status indicates that the tools can be upgraded to the current tool revision.
   - A VM that is not running may display a status, but needs to be started before the upgrade option can become available.
7. To upgrade, right-click on the VM in the tree view and select **Guest OS**, then select **Upgrade VMware Tools**.
   a. From the **Upgrade VMware Tools** dialog box, select **Automatic Upgrade**.
   b. Click **Upgrade**.

After the tool upgrade is complete, the VM will automatically restart. After restart, the Summary tab displays that the VMware Tools are current.

*Note* You may need to refresh the Summary tab to see the VMware Tools state as **Running**.
5.5 Console Connections to a VM

A VM console is the equivalent of connecting a monitor, keyboard, and mouse to a physical computer. It is typically used to manage a VM, and is the only option available prior to establishing the Ethernet networks required for remote login.

Note Using the current software, the vSphere Client Console tends to work much better than the vCenter Web Server Console. GE recommends using the vSphere Client to establish a console connection to a VM even on Core HA systems where both are available.

5.5.1 Establishing a vSphere Client Connection to a Host

➢➢ To establish a vSphere client connection to a host
1. Log into the Management VM (MC3).
2. Launch the vSphere Client Application by double-clicking the VMware vSphere Client icon on the desktop.
3. In the IP address field enter the host's IP address.
4. In the User Name field enter the username for an administrative account.
5. In the Password field enter the associated password.
6. Click Login.
7. In the Security Warning dialog box, click Ignore.
8. If you are directed to the Home Page, click Inventory to go the main screen used to configure and monitor the hypervisor.

5.5.2 Establishing a Console Connection to a VM

➢➢ To establish a console connection to a VM
1. Use the vSphere Client to connect to the host and open the Inventory page.
2. Right-click on the desired VM and select Open Console.

5.5.3 vSphere Console Commands

➢➢ To capture the keyboard and mouse: click anywhere inside the console window.

➢➢ To issue a [CTRL] + [ALT] + [DELETE] sequence: press [CTRL] + [ALT] + [INSERT].

➢➢ To release the keyboard and mouse capture: press and release [CTRL] + [ALT].
5.5.4 Disconnecting from the VM Console

Disconnecting a console from a VM does not log the console session out. Another person connecting to the console would inherit the session from the previous user. You should always lock the screen (if supported) or log out from the VM prior to disconnecting the console.

➢➢ To disconnect the console connection
1. (Security Recommendation) Lock the VM screen or log out from the VM.
2. Close the console window by clicking the red X in the upper right hand corner.

5.6 Enable or Disable SSH Interface on ESXi Host

➢➢ To enable or disable the SSH interface on an ESXi host
1. Log into the vSphere web client using an account with Administrative privileges.
2. From the Home screen, select Hosts and Clusters.
3. Select the host (HS1, HS2, MC2, or HW1) that you want to configure.
4. Select the Manage tab and the Settings group.
5. In the System section, select the Security Profile pane.
6. Scroll down past the Firewall table to the Services table, then click Edit on the Services table header line.
7. Select the SSH entry.
8. Click Start to start the service, and Stop to stop the service.
9. Verify that the state of the SSH service matches the selection made in the previous step (Stopped or Running).
10. Click OK to exit the Edit Security Profile dialog box.

Note The main page will not automatically refresh the service status. To confirm the SSH service state, click the Refresh icon in the Services table header line.
5.7 Enter SSH Commands on Hosts

➢ To enter SSH commands on a host
1. Run the following program on MC3: C:\Program Files (x86)\PuTTY\putty.exe.
2. In the Host Name (or IP address) field, enter the PDH IP Address of the host to which you are connecting, then click Open.
3. A PuTTY Security Alert window displays the certificate thumbprint of the host to which you are connecting. Verify that the certificate is from the correct host (trusted), then click No to continue with the connection.
4. When the main PuTTY window displays a login as: prompt, enter the username and the password for an administrative account.
5. Enter the desired Command Line Interface (CLI) commands.
6. When finished, enter the command exit to end the session and close the PuTTY window.

5.8 Setting Password Policies

The VMware domain maintained by the vCenter Appliance has a set of password policies (such as length, complexity, and expiration) that may need to be modified to meet the site security policy.

➢ To view or change the Password Policy
1. Log into the management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with Administrative privileges.
3. From the Home screen, select Administration.
4. In the Single Sign-On section, select the Configuration pane.
5. Select the Policies tab and the Password Policy group to view the current password policies.
6. To change any of the displayed password policies, click Edit….
   a. In the Edit Password Policies dialog box, update the various values to match the site security policies.
   b. Click OK.
7. If the site has specific lockout policies, repeat this procedure for the Lockout Policies group.
5.9 Setting VM HA Restart Priorities (VM Overrides)

When the HA subsystem needs to restart multiple VMs it will examine HA Attribute entries in the VM Overrides table to determine the priority-based order in which to start VMs.

➢ To adjust the HA Attributes for the VMs

1. Log into the management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with Administrative privileges.
3. From the Home screen, select Hosts and Clusters.
4. Expand Datacenter1, then select Cluster1.
5. Select the Manage tab and the Settings group.
6. In the Configuration section, select the VM Overrides pane.
7. To add a new entry to the VM Overrides table, click on Add…
   a. Click the Select virtual machines icon (plus sign), select the desired VM(s), and click OK.
   b. In the VM restart priority field, select the appropriate priority from the drop-down menu.
   c. Click OK to complete the add operation.
8. To change the value for an existing entry, select the desired entry and click on Edit.…
   a. In the VM restart priority field, select the appropriate priority from the drop-down menu.
   b. Click OK to complete the edit operation.
9. To remove an existing entry, perform the following steps:
   a. Select the desired entry and click Delete.
   b. In the Delete VM Overrides dialog box, select Yes.
5.10 Migrating VMs Between Host Servers

VMs can be migrated from one host server to another host server, which is often done to change the load balancing between the hosts or to move all VMs off of a specific host for server maintenance or repair.

There are many places in the vCenter Appliance where the VM migration can be triggered. In the Hosts and Clusters display, a right-click on any VM in the Tree view will display the Migrate... option. It is typically more convenient to customize the cluster-wide VM display to add the Host column, then perform the migrations from there. This has another advantage in that multiple VMs can be selected and migrated together in one operation.

➢➢ To migrate VMs between the host servers

1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with administrative privileges.
3. From the Home screen, select Hosts and Clusters.
4. Expand Datacenter1, then select Cluster1.
5. Select the Related Objects tab and the Virtual Machines group.
6. If the columns shown do not include the Host column, perform the following steps:
   a. Right-click anywhere in the column header line and select Show/Hide Columns....
   b. Select (enable) the Host column.
   c. You may wish to remove (deselect) columns that are of limited interest to allow all columns to fit without requiring horizontal scrolling.
   d. Click OK.
7. If desired, you can click on most column headers (including Name and Host) to sort by that column.
8. Select the VM(s) that you want to migrate.
   a. A block of continuous VMs can be selected by clicking on an entry and then [SHIFT] clicking on a second entry. The two entries and all entries between them will be selected.
   b. Multiple VMs can be selected by clicking on the first entry, then [CTRL] clicking on each additional entry.
   c. The previous two options can be combined, a block of entries can be [SHIFT] selected, and then individual items within the block can be deselected by using [CTRL] clicking. [CTRL] clicking toggles the selection state of an item.
9. Right-click on any of the selected entries and select Migrate....
10. If multiple entries were selected, a confirmation dialog box displays asking for verification that you want to take this action on multiple VMs. Click Yes.
11. From the Select the migration type dialog box, select Change computer resource only and click Next.
12. From the Select a compute resource dialog box, select the host you want to which to migrate the VMs and click Next.
13. On the Select network dialog box, verify that the networks align with the desired networks (they should, both servers should have identical networks) and click Next.
14. On the Select vMotion priority dialog box, accept the default of Schedule vMotion with high priority and click Next.
15. On the Ready to complete dialog box, verify the settings and click Finish.
16. Watch the Recent Tasks list and the updating main display to monitor the state of the VM migration.
5.11 **Mapping Host Physical Devices into VMs**

*Mapping* is the act of making a physical device on a host server (such as a DVD drive or a USB flash drive) accessible to a VM. Physical devices appear as virtual devices inside the VM, and can be treated the same as physical devices. There may be some additional limitations imposed by the mapping, such as a DVD drive may be marked as read-only instead of being writeable.

5.11.1 **Mapping a host DVD Drive to a VM**

The DVD drive on the host server can be mapped to one (or more) VMs. The DVD drive access will be limited to read-only operation. Be aware that while the DVD is mapped to the VM the VM cannot be migrated off the host to another host. A DVD does not have to be loaded into the host DVD drive in order to establish the mapping.

➢ To map the host DVD drive to a VM

1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with Administrative privileges.
3. From the Home screen, select **Hosts and Clusters**.
4. Expand **Datacenter1**, then expand **Cluster1** and select the VM you wish to use.
5. Select the **Summary** tab to identify the host server on which the VM is currently running.
   a. If the host server is acceptable then this is the host where the DVD should be mounted.
   b. If the host server must be changed, perform the procedure *To migrate VMs between the host servers* to move it to the desired host server.
6. Right-click on the desired VM and select **Edit Settings**....
   a. In the **CD/DVD drive 1** field, select the **Host Device** option.
   b. Select the **Connected** check box.
   c. If the host server has multiple DVD drives (unlikely) expand the CD/DVD drive 1 entry and select the desired device from the CD/DVD Media drop-down menu.
   d. Click **OK** to close the **Edit Settings** dialog box.
7. Disconnect the map network drive for the DVD drive when finished, as the VM will not be able to migrate between the hosts while the DVD is mapped.
### 5.11.2 Mapping a Host USB Drive to a VM

The procedure for mapping a host USB drive to a VM is similar to that of mapping the host DVD drive, but since the USB device is not a predefined device in the VM a USB controller may need to be added before adding the USB Device. The actual USB device must be connected to the host server prior to establishing the connection to the VM.

➢ **To map a Host USB Drive to a VM**

1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: `https://172.16.199.7`) using an account with Administrative privileges.
3. From the Home screen, select **Hosts and Clusters**.
4. Expand **Datacenter1**, then expand **Cluster1** and select the VM you wish to use.
5. Select the **Summary** tab to identify the host server on which the VM is currently running.
   a. If the host server is acceptable then this is the host where the USB device should be connected.
   b. If the host server must be changed, perform the procedure **To migrate VMs between the host servers** to move it to the desired host server.
6. Insert the USB storage device into the host server USB slot.
7. Right-click the desired VM and select **Edit Settings**....
   a. If the settings do not include a **USB Controller** device, perform the following steps:
      i. In the **New Device** field, select **USB Controller** from the drop-down menu and click **Add**.
      ii. Click **OK** to close the **Edit Settings** dialog box and perform the operation to add the device.
      iii. Reopen the dialog by right-clicking the appropriate VM and selecting **Edit Settings**....
   b. In the **New Device** field, select **Host USB Device** from the drop-down menu and click **Add**.
   c. If there are multiple Host USB Devices available, select the desired device from the **New Host USB device** drop-down menu.
   d. Click **OK** to close the **Edit Settings** dialog box.
8. Disconnect the map network drive for the USB device when finished, as the VM will not be able to migrate between the hosts while the device is mapped.
5.12 Checking the Virtual SAN Health

View the Virtual SAN Health pane to check the health status of the Virtual SAN subsystem.

➢➢ To view the Virtual SAN Health

1. Log into the Management VM (MC3).
2. Open the vCenter web page (standard: https://172.16.199.7) using an account with Administrative privileges.
3. From the Home screen, select Hosts and Clusters.
4. Expand Datacenter1, then select Cluster1.
5. Select the Monitor tab, the Virtual SAN group, and the Health pane.

The Virtual SAN help report is displayed. The following information may assist in the analysis of this report:

• On ESXi Version 6.0, the Data health entry will show a status of Failed. Expand the Data health item and select the (failed) Virtual SAN object health entry. It will show that all data items are marked as inaccessible. This false indication of inaccessibility appears to be caused by using point-to-point interconnections between the hosts, and can be safely ignored. Items other than inaccessible should be investigated.

• The Virtual SAN HCL health entry may be showing one or more warnings. The following warnings may be present but will not impact normal operation:
  − If the Hardware Compatibility List (HCL) is more than 90 days old it will show a warning for the Virtual SAN HCL DB up-to-date entry. This will not impact operation, but it is a reminder to check for updates to drivers and other subsystems.
  − If a newer recommended version of a driver is available from VMware, the Controller Driver entry may show a warning. The determination on whether to update to a newer driver or remain with the existing driver is outside the scope of this document.

5.13 Datastore File Maintenance

The Virtual SAN, MC2, and HW1 support file systems that are accessed by both the VMs and the hypervisors. The vCenter web page supports the maintenance of the files and directories in the Datastores, including creating and deleting directories and uploading files to or deleting files from the Datastore.

➢➢ To access a Datastore

1. Log into the vSphere web client using an account with Administrative privileges.
2. From the Home screen, select Storage.
3. In the left hand pane, expand the tree view and select the appropriate Datastore.
4. Select the Manage tab and the Files group.

It may take some time for the vCenter Appliance to retrieve the directory listing from the host server for the Datastore.

Tip ➢ You may need to expand the Datastore item in the data pane to see the top level directories in the Datastore.
➢ To create a directory
1. Access the list of files in the Datastore (refer to the procedure To Access a Datastore).
2. Select the parent directory for the directory that you wish to create (where you want the directory created).
3. Click the Create a new folder icon (folder with plus sign located in the icon section above the directory listing).
4. From the Create a new folder dialog box, enter the name for the new directory.

   Note Directory and file names are case sensitive.

5. Click Create.

The directory listing displays the new directory.

➢➢ To upload a file
1. Access the list of files in the Datastore (refer to the procedure To Access a Datastore).
2. Select the parent directory for the file that you wish to create (where you want the file created).
3. Click the Upload a file to the Datastore icon (disk with up arrow located in the icon section above the directory listing).
4. From the Open dialog box, click Browse and select the file to be uploaded, then click Open.

The file should begin uploading to the Datastore. A progress table below the directory listing indicates the progress of the file upload. Upon completion, the directory listing shows the file uploaded.

➢➢ To delete a file
1. Access the list of files in the Datastore (refer to the procedure To Access a Datastore).
2. Navigate to the parent directory of the file(s) that you want to delete and select the file(s).
3. Click the Delete selected file or folder icon (red X located in the icon section above the directory listing).
4. From the Confirm Deletion dialog box, click Yes.

A dialog box indicates the progresses of the delete operation. Upon completion the directory listing should show the file(s) removed.
Glossary

**Hardened** is the state of a computer or network device that has been configured through settings or application installations to be less vulnerable to security-related attacks.

**Hypervisor** is a piece of computer software, firmware, or hardware that creates and runs virtual machines.

**Plant Data Highway (PDH)** is a plant-level supervisory network connecting the HMI server with remote viewers, printers, Historian applications, and external interfaces.

**Secure Shell (SSH)** is a cryptographic network protocol for secure data communications.

**Unit Data Highway (UDH)** is the portion of the network that carries controller-to-controller or controller-to-HMI data.