GEH-6852A

Control Server Core - Simplex Maintenance Guide

July 2017

For public disclosure

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 – This document is 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: July 2017
Issued: April 2017

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

Document Updates

Location	Description
Datastore File Maintenance	Added this section containing the procedures to access and maintain Datastore files

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
TCP/IP	Transmission Control Protocol/Internet Protocol
UDH	Unit Data Highway
UDP/IP	User Datagram Protocol/Internet Protocol
VFA	Virtual Field Agent

Related Documents

Doc #	Title
GEH-6840	NetworkST 3.1/4.0 for Mark VIe Controls Application Guide
GEH-6844	Control Server System Overview
GEH-6846	Control Server Installation and Startup Guide
GEH-6848	Control Server Hand-over Guide

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.

Contents

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 Simplex Core provides a single stand-alone server to host all VMs.

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

2.1 Hardware

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

- The **Platform** selection defines the particular server class computer that is used for the virtualization server.
- 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

The decision to use the Simplex Core (instead of the HA Core) is typically based upon a site's limited redundancy requirements. Once the decision is made to use the Simplex Core, the Platform selection addresses the basic features of the host server.

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

- Support for 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 the server
- Number and type of drive bays available
- Number of expansion slots available for items such as network adapters

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 the server.

The following Platform Options are typically available on the host server platform:

- 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. 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. The host server always uses a RAID array of drives to survive a single drive failure, using RAID-1 for two drive configurations and RAID-5 for more than two drives. For a configuration with *n* drives, the total drive capacity is *n-1* times the size of each drive. Each VM is configured with the drive space it is allowed to use.

2.2 Software

The Control Server Simplex Core uses the VMware ESXi hypervisor to provide 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.

2.3 Configuration

2.3.1 Account Management

The ESXi hypervisor supports a local Role Based Access Control (RBAC) scheme within the hypervisor itself. The Control Server does not make extensive use of the local Roles, 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 local accounts and Roles to implement a multi-tier RBAC scheme of their own. Normally, the Control Server delivers a single administrative level account for administering the hypervisor host.

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.
- **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 is 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.

Notes

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 ESXi hypervisor uses local accounts for authentication and authorization. The hypervisor supports full Role Based Access Control (RBAC) through the use of individual user accounts, Roles, and assigned permissions.

- 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 as it requires physical access to the server and limits access to one VM at a time. Instead of using a host port, consider using one of the following options:

- Use a USB port on a Windows Thin Client (if available) and assign it a share name with appropriate permissions. This allows multiple VMs to access the USB device concurrently while providing user-based access control (ReadOnly or ReadWrite).
- Use a USB port on a Linux™ Thin Client (if available) as a point-to-point connection to the currently logged on host.
- Use an Ethernet-based USB port concentrator to allow a single VM to access the content as if it was mounted to that VM.

4 Common Procedures

The following sections outline some of the common procedures used in the Control Server Simplex Core environment.

4.1 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.

4.1.1 Create VM

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

➢ **To create a Virtual Machine**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the main *Inventory* page, right-click on the top level of the tree view (host IP Address) and select **New Virtual Machine**.
6. From the *Configuration* dialog box, select **Typical**, then click **Next**.
7. From the *Name and Location* dialog box, enter an appropriate VM name and click **Next**.
8. From the *Storage* dialog box, accept the default Datastore and click **Next**.
9. From the *Guest Operating System* dialog box, select the appropriate operating system and click **Next**.
10. From the *Network* window, perform the following steps:
    a. If the VM is connected to only one network:
        i. Select **1 NIC**.
        ii. For NIC 1, select the appropriate network, select the **E1000** adapter, and verify that **Connect at Power On** is checked (selected).
        iii. Click **Next**.
    b. If the VM is connected to two networks (typically the PDH and the UDH):
        i. Select **2 NIC**.
        ii. For NIC 1, select the first network, select the **E1000** adapter, and verify that **Connect at Power On** is checked (selected).
        iii. For NIC 2, select the second network, select the **E1000** adapter, and verify that **Connect at Power On** is checked (selected).
        iv. Click **Next**.

11. From the *Create a Disk* dialog box, set an appropriate **Virtual Disk Size**, select **Thick Provision Lazy Zeroed**, and click **Next**.

12. From the *Ready to Complete* window, enable the check box **Edit the virtual machine settings before completion**, then click **Continue**.

Note If you see **Finish** instead of **Continue**, the **Edit the virtual machine settings before completion** check box was not enabled.

---

13. From the *Virtual Machine Properties* dialog box, define the following additional settings:

    a. Set the **Memory** setting to an appropriate value.

    b. Set the **CPU** setting to an appropriate value. Leave the **Number of virtual sockets** value at one (1) and set the **Number of cores per socket** to an appropriate value.

    c. Click the **Video Card** entry and define the following settings:

        i. Set the **Number of displays** to an appropriate value.

        ii. Set the **Total Video Memory** to an appropriate value

    d. If you want to map the CD/DVD drive to an ISO image in the Datastore, perform the following steps:

        i. Click **New CD/DVD (adding)**.

        ii. Select **Datastore ISO file**.

        iii. Click **Browse** and navigate to and select the appropriate ISO file.

        iv. Enable (check) the **Connect at Power On** check box (located near the top of the dialog box).

    e. Select the **Options** tab.

    f. Select the **Boot Options** tab and set the **Firmware** field to an appropriate value (EFI is the preferred boot method, but not all VMs support EFI boot).

    g. Click **Finish** to create the VM.

14. Verify that the VM displays in the tree view in the left pane.

4.1.2 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 a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the main *Inventory* page, select **File**, then select **Deploy OVF Template…**.
6. From the *Select the source location* dialog box, perform the following steps:
   a. Click **Browse**, navigate to and select the appropriate OVA or OVF file, then click **Open**.
   b. Click **Next** to continue.
7. From the main *OVF Template Details* dialog box, click **Next**.
8. From the main *Name and Location* dialog box, enter an appropriate name for the VM in the **Name** field and click **Next**.
9. From the main *Disk Format* dialog box, accept the defaults and click **Next**.
10. From the main *Network Mapping* dialog box, set the **Destination Networks** field(s) to match the appropriate network(s) and click **Next**.
11. From the main *Ready to Complete* dialog box, click **Finish**.
    The VM will be created and the contents of the OVA/OVF file will be transferred to the host. This may take some time depending on the size of the hard drives (10 to 20 minutes or more is not uncommon; an estimate will be provided).
12. From the *Completed Successfully* dialog box, click **Close**.
13. From the main *Inventory* page, right-click the VM just created in the tree view (left hand pane), select **Edit Settings**, and perform the following steps:
    a. Set the **Memory** setting to an appropriate value.
    b. Select the **CPUs** setting and set the **Number of cores per socket** value to an appropriate value.
    c. Click the **Video Card** entry and define the following settings:
       i. Set the **Number of displays** to an appropriate value.
       ii. Set the **Total Video Memory** to an appropriate value
    d. If you want to map the CD/DVD drive to an ISO image in the Datastore, perform the following steps:
       i. Select the **CD/DVD drive 1** entry.
       ii. Select **Datastore ISO file**.
       iii. Click **Browse** and navigate to and select the appropriate ISO file.

iv. Enable (check) the **Connect at Power On** check box (located near the top of the dialog box).

e. If you do not want to map an ISO image in the Datastore, set the **Device Type** to **Client Device**. Do not leave this as *Host Device — CD/DVD drive <n>*.

f. Select the **Hard disk 1** entry and set the **Provisioned Size** to an appropriate value.

g. If there are additional **Hard disk <n>** entries, set them to appropriate values.

h. For each **Network adapter <n>** present, perform the following steps:

i. Select the **Network adapter <n>** entry.

ii. Verify that option **Connect at Power On** is enabled (checked).

i. Select the **Options** tab.

j. Select the **Boot Options** tab and set the **Firmware** field to an appropriate value (EFI is the preferred boot method, but not all VMs support EFI boot).

k. Click **OK** to save the settings.

14. Verify that the VM displays in the tree view in the left pane.

4.2 VM Powerup

➢ **To power on a VM**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. Expand the tree view, locate and right-click on the desired VM, select **Power**, then select **Power On**.

4.3 VMware Integration Tools Installation on Microsoft Windows Operating Systems

➢ **To install VMware integration tools on Microsoft Windows operating systems**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the main *Inventory* page, select the VM on which you want to install the tools.
6. Select the **Console** tab for the VM and make sure you are logged into the VM using an Administrator account.
7. Minimize any open windows (such as the *Initial Configuration Task* window) to make the installation dialogs visible.
8. Right-click on the VM in the tree view and select **Guest**, then select **Install/Upgrade VMware Tools**.
9. Click inside the *Tap to choose what happens* window to display the *AutoPlay* dialog box.
10. 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.

---

11. Select **Typical** installation, then click **Next**.
12. Select **Install**.
13. Click **Finish** at the end of the installation.

You will be prompted to restart the VM.

4.4 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 a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page, expand the tree view and select the desired VM.
6. Select the **Summary** tab.
7. The *VMware Tools* line indicates the current status of the VMware tools as follows:
   a. **Current** status: the VM is at the current tools level and no upgrade option is available.
   b. **Out-of-date** status: the tools can be upgraded to the current tool revision.
   c. A VM that is not running may show its status, but needs to be started prior to its offering the upgrade option.
8. To begin the upgrade, right-click on the VM in the tree view and select **Guest**, then select **Install/Upgrade VMware Tools**.
9. From the *Install/Upgrade Tools* dialog box, select **Automatic Tools Upgrade** and click **OK**.

During the upgrade process, the Summary tab should display an **Active Task** of **Initiated VMware Tools install or 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*.

4.5 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.

4.5.1 Establishing a vSphere Client Connection to a Host

➢ **To establish a vSphere client connection to a host**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
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 display the main *Inventory* page used to configure and monitor the hypervisor.

4.5.2 Establishing a Console Connection to a VM

➢ **To establish a console connection to a VM**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page, right-click on the appropriate VM and select **Open Console**.

4.5.3 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]**.

4.5.4 Disconnecting from the VM Console

Attention

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.

4.6 Enable or Disable SSH Interface on ESXi Host

➢ **To enable or disable the SSH interface on an ESXi host**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. Select the top-most entry in the tree view (the server), then select the **Configuration** tab.
6. From the *Software* group, select the **Security Profile** pane.
7. From the *Services* section, click **Properties** and perform the following steps:
   a. Select the SSH entry and click **Options**.
   b. From the *Service Commands* group, click **Start** or **Stop** to get to the desired running state, then click **OK**.
   c. Click **OK**.

4.7 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 without saving the certificate.
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.

4.8 User Management

The server supports a set of local users with the intention of each user being assigned a Role with the privileges appropriate for that role. This section describes some of the procedures for defining users, assigning them to Roles, and removing users.

4.8.1 New User Account

➢ **To Create a New User Account**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page, select the top-most entry in the tree view (the server), then select the **Users** tab.
6. Right-click anywhere in the user pane, select **Add…**, and perform the following steps:
   a. In the *Login* field, enter a username for login.
   b. (Optional) In the *User Name* field, enter the user's full name.
   c. In the *Password* and *Confirm* fields, enter a password to assign to this username and re-enter the password to confirm it.
   d. Click **OK** to add the user.
7. Select the **Permissions** tab.
8. Right-click anywhere in the Permissions pane, select **Add Permission…**, and perform the following steps:
   a. In the *Users and Groups* group, select **Add…**.
   b. Select the user to whom you want to assign permissions for (Role), click **Add**, then click **OK**.
   c. Select the newly added user, select the Role for this user from the *Assigned Role* group's drop-down, and click **OK**.
9. Verify that the user has been added to the Permissions pane with the desired Role.

4.8.2 Modify User Role

➢ **To modify a user's Role**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page, select the top-most entry in the tree view (the server), then select the **Permissions** tab.
6. In the *Users and Groups* group, double-click the user's entry to change the assigned Role.

4.8.3 Remove User Account

➢ **To remove a User account**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page, select the top-most entry in the tree view (the server), then select the **Users** tab.
6. Right-click on the desired user account and select **Remove**.
7. When the confirmation dialog box displays, click **Yes**.

4.8.4 Change User Password

➢ **To Change a User's Password**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page, select the top-most entry in the tree view (the server), then select the **Users** tab.
6. Right-click on the desired user account and select **Edit**.
7. Select (enable) the **Change password** check box.
8. In the *Password* and *Confirm* fields, enter a new password for the user and re-enter the password to confirm it.
9. Click **OK** to save the password change.

4.8.5 New Roles and Privileges

➢ **To create a new Role and assign Privileges to the Role**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If you are not automatically directed to the *Home* page, click **Home** in the address bar to display the *Home* page.
5. Click **Roles**.
6. Right-click anywhere in the Roles pane and select **Add…**.
7. In the *Name* field, enter a new name for the Role.
8. In the *Privileges* field, enable the privileges that should be assigned to the Role.
9. Click **OK** to apply the changes.

4.8.6 Modify Roles and Privileges

➢ **To change the privileges associated with the Role after its creation**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If you are not automatically directed to the *Home* page, click **Home** in the address bar to display the *Home* page.
5. Click **Roles**.
6. Right-click on the Role and select **Edit Role…**.
7. In the *Privileges* field, modify the privileges assigned to the Role.
8. Click **OK** to apply the changes.

4.9 Setting VM Startup Options

The server can be configured to start and stop VMs automatically when the server is started and stopped. It is common to have the server configured to automatically start all VMs upon powerup to allow for unattended operation.

➢ **To configure VM automatic startup and shutdown**

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page, select the top-most entry in the tree view (the server), then select the **Configuration** tab.
6. From the *Software* group, select the *Virtual Machine Startup/Shutdown* pane.
7. In the header line of the pane, click **Properties**.
8. If it is not already enabled (selected), enable the **Allow virtual machines to start and stop automatically with the system** check box.
9. Select the desired VM and use the *Move Up* and *Move Down* command targets to move the selected VM into the correct startup category, placing it in an appropriate position relative to the other VMs.
10. Repeat step 9 for each VM that needs its startup option changed.
11. Click on **OK** to apply the configuration.

4.10 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.

4.10.1 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. 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 a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. From the *Inventory* page tree view, right-click the appropriate VM and select **Edit Settings**.
6. Select the **CD/DVD drive 1** option.
7. Map a host physical DVD drive as follows:
   a. Select the **Host Device** option.
   b. From the **Host Device** drop-down menu, select the physical DVD drive to map.
8. Map an ISO image in the Datastore as follows:
   a. Select the **Datastore ISO File** option.
   b. Click on **Browse**, navigate to and select the directory containing the ISO image, select the ISO image, and click **Open**.
9. Click **OK** to close the *Virtual Machine Properties (Settings)* dialog box.

4.10.2 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.

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the *Home* page displays, click **Inventory** to display the main *Inventory* page.
5. Right-click the appropriate VM and select **Edit Settings**.
6. If the settings do not display a **USB Controller** in the machine, perform the following steps:
   a. Click **Add…**.
   b. Select **USB Controller** and click **Next**.
   c. Accept the default Controller Type and click **Next**.
   d. Click **Finish**.
7. Connect the USB device as follows:
   a. Click **Add…**.
   b. Select **USB Device** and click **Next**.
   c. Select the USB you want to connect and click **Next**.
   d. Click **Finish**.
8. Click **OK** to close the *Virtual Machine Properties (Settings)* dialog box.

4.11 Datastore File Maintenance

The hypervisor supports a file system that is accessed by both the VMs and the hypervisors. The vSphere Client supports the maintenance of the files and directories in the Datastores, including creating and deleting directories as well as uploading files files to or deleting files from the Datastore.

➢ To access a Datastore

1. Log into a computer with the VMware vSphere Client installed (such as MC3).
2. Double-click the VMware vSphere Client icon on the desktop to launch the vSphere Client application.
3. Enter the IP address of the server (typically 172.16.199.8) and log in using an account with administrative privileges.
4. If the Home page displays, click **Inventory** to display the main *Inventory* page.
5. Select the top-most entry in the tree view (the server), then select the **Configuration** tab.
6. From the *Hardware* group, select the **Storage** pane.
7. Right-click on the desired Datastore entry and select **Browse 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 *New Folder* dialog box, enter the name for the new directory.

Note Directory and file names are case sensitive.

---

5. Click **OK**.

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).
   a. Select either of the following options:
      - Select **Upload File...** to upload a single file.
        - In the *Open* dialog, click **Browse** and select the file to be uploaded, then click **Open**.

      Or

      - Select **Upload Folder...** to upload an entire directory. When you select a folder to be uploaded, a new folder with the same name will be created in the location that you selected as the destination. In other words, the directory that you select as the source will be created in the directory that you selected as the destination.
        - In the *Open* dialog, click **Browse** and select the directory to be uploaded, then click **OK**.

b. If an *Upload/Download Operation Warning* dialog box displays indicating that files will be overwritten if duplicate filenames are found, click **Yes** to continue.

An *Uploading...* dialog box indicates the progress of the file upload. Upon completion, the directory listing shows the file(s) 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).

- Press [Shift] and click to select a block of items.
- Press [Ctrl] and click to toggle the selected state of a single item.

3. Click the **Delete selected items icon** (red X located in the icon section above the directory listing).

4. From the *Confirm Delete* dialog box, click **Yes**.

A dialog box indicates the progresses of the delete operation. Upon completion, the directory listing shows the file(s) removed.

Note If you delete the currently selected directory, you should select a new directory in the tree view to refresh the display. If you do not, it may hang, showing as *Loading...*, and not complete by itself.

Notes

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.

Notes