LISTEN.
THINK.
SOLVE.®

VIRTUALIZATION FOR PROCESS AUTOMATION SYSTEMS

VIRTUALIZATION ALLOWS HARDWARE INDEPENDENCE, IMPROVES LONGEVITY, INCREASES FLEXIBILITY AND SCALABILITY AND INCREASES UPTIME

Rockwell Automation Publication: PROCES-WP007A-EN-P January 2013

Allen-Bradley • Rockwell Software

Rockwell Automation

Executive Summary

Computer virtualization is the process of constructing a virtual (instead of physical) computer hardware platform by executing software program (hypervisor) between the actual hardware and operating system(s). Virtualization allows users to abstract the operating system and application software from the real hardware. To be able to run in a virtual architecture users apply Virtualization software tools to create virtual machines that "act like a real computer with an operating system". One or many virtual machines, even with different types and classes of operating systems can be executed under that same hypervisor.

Virtualization has benefits that apply to both traditional enterprise IT and industrial automation such as server hardware consolidation, lower energy consumption, and reduced physical server footprint. However, there are several features that are extremely important for automation and especially process automation systems. By far, the most important is "hardware independence." This independence is at the core of many of the benefits virtualization provides. One of the most important being the ability to extend the lifecycle of a control system. Users are no longer tied to a specific hardware when virtualized and a virtual machine is supported for 10+ years given the generous support policy provided by VMware for their hypervisor. Virtualization provides features like High Availability and Fault Tolerance to help improve uptime of the process system and, therefore controlled application. The ability to take a "snapshot" of the current software configuration, implement changes, and revert to previous configurations if needed, decreases risk and improves start-up time. Features such as this decrease the risk of software upgrades, configuration changes, and operating system patching. Users are able to create templates of virtual machines and deploy Virtual Machines with their applications (if any) already installed and configured to their preference reducing engineering and deployment costs.

There are several leading providers of virtualization technology. Rockwell Automation chose VMware® as their technology provider due to its maturity and market leading position in virtualization. Herafter, we'll use virtualization terminology in context of VMware® virtualization.

This application note will describe how Rockwell Automation PlantPAx process automation system takes advantage of VMware vSphere™ virtualization technology. It will explain how to select hardware and build your virtual PlantPAx™ Process Control System. It will help process automation personnel understand IT hardware and software requirements for virtualization while also providing IT personnel an overview of virtualization as it is applied to process automation applications.

Table of Contents

Additional Resources

These documents contain additional information concerning VMware vSphere and related products from Rockwell Automation.

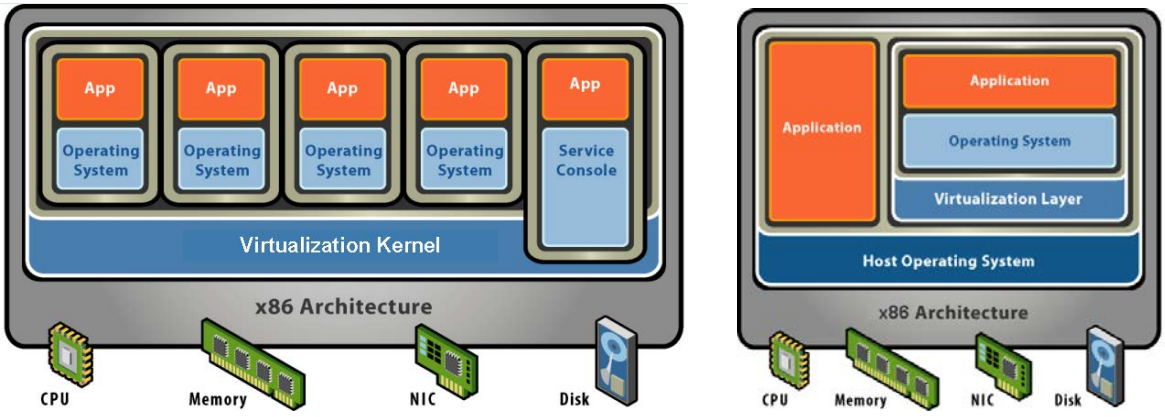
Resource	Description
VMware vSphere Basics, publication EN-000586-00	This document provides basic information on the features and functionality of VMware vSphere (ESXi 5.0, vCenter 5.0)
VMware View™ Optimization Guide for Windows 7, Publication VMW-WP-WIN7-USLET-20120112-WEB	Provides recommendations to enhance performance of Windows 7 based virtual machines within a VMware View solution. (pages 19-24)
PlantPAx Process Automation System Selection Guide, publication PROCES-SG001	Provides an overview of the three typical process architectures: independent, centralized, and distributed. Provides guidance on system requirements and equipment procurement.
PlantPAx Process Automation System Reference Manual, Publication PROCES-RM001	Provides PlantPAx guidance on system setup and configuration.

Virtualization: History and Technology Overview

Virtualization is a software technology that decouples the physical hardware of a computer from its operating system (OS) and software applications, creating a pure software instance of the former physical computer -- commonly referred to as a Virtual Machine (VM). A VM behaves exactly like a physical computer, contains its own "virtual" CPU, RAM, hard disk and network interface card, and runs as an isolated guest OS installation. The terms "host" and "guest" are used to help distinguish the software that runs on the actual machine (host) from the software that runs on the virtual machine (guest).

Virtualization works by inserting a layer of software called a "hypervisor" directly on the computer hardware or on a host OS. A hypervisor allows multiple OSs, "guests," to run concurrently on a host computer (the actual machine on which the virtualization takes place). It presents to the guest OS a virtual operating platform and manages the execution of the guest OSs.

Figure 1: Virtualization Types



Server or “Bare-Metal” Virtualization

Desktop or “Hosted” Virtualization

Rockwell Automation recommends that users make use of Server Virtualization, and VMware vSphere, when dealing with run-time production applications. Server Virtualization removes the dependency on a full host OS and provides a much more stable environment for critical applications. The Desktop solutions, such as VMware Workstation and VMware Player, provide virtual environments for engineers to develop and test virtual machines before deploying for production. Virtual Machines can be easily migrated from one environment to another using VMware vCenter Converter.

Rockwell Automation recognizes their customers' desire to make use of the opportunities that virtualization brings to process control applications and has worked closely with VMware to establish a technical relationship. Rockwell Automation supports its software suite in virtualized environments, and has developed a list of software products that are recognized by VMware as "VMware Ready." The VMware Ready status provides end users with the peace of mind that the applications will perform well and properly on VMware platforms.

Today, most Rockwell Automation configuration, human interface and information products are certified as VMware Ready, and Rockwell Automation is committed to supporting and testing all new software products in a virtual environment.

Why Virtualize an Automation System?

Virtual machines can be run on any virtualization-enabled physical server, creating a pool of computer resources that helps ensure your highest-priority applications will always have the resources they need.

Virtualization software allows virtual machines to access the physical hardware resources of the computer on which they reside. Having the ability to run multiple VMs on one physical computer allows for the optimization of server and workstation physical assets as most server-based computers are significantly underutilized. Organizations typically run one application per server to avoid the risk of vulnerabilities in one application affecting the availability of another application on the same server. Virtualization however allows users to retain this one application per server architecture model while allowing them to run as separate virtual machines on the same piece of server hardware.

Virtualization allows companies to create a scalable infrastructure, where new VMs can be added without the need to continuously buy new hardware and other physical devices. By having the ability to consolidate, users find they can buy and allocate the appropriate amount of resources for each VM, which reduces system maintenance and energy consumption costs.

During a planned outage, administrators can shift their workloads so the server can be taken down with no impact to the system. When the planned outage is complete, the server can be placed back into service. Since the VMs are not attached to a physical computer, the VMs can be migrated between servers while the system is still running.

Advantages of a Virtual Machine
- Hardware independence - Fault tolerance - Application-load balancing - Rapid disaster recovery - Recovery to non-identical hardware - Ability to pre-test OS patches or vendor updates - Ability to roll-back incompatible OS patches or vendor updates - Reduced TCO resulting from consistent datacenter environment - Reduced power usage

While virtualization may provide many benefits, there are certain scenarios in which it may not be compatible with a user's system. A server or workstation that is dependent on a specific hardware card (other than USB), such as a communication interface, cannot be attached to a virtual machine. USB devices can be attached to a Virtual Machine either through a remote access terminal (thin client) or directly on the server.

PlantPAx is based on open IT standards and networks meaning that all PlantPAx workstations and servers can easily be virtualized. Workstations for legacy systems that require special interface cards, beyond USB, are not supported in virtual environments at this time.

Virtualization Infrastructure

A complete VMware vSphere virtual solution consists of both virtualization software and hardware components. This section will highlight key software products and features in addition to physical hardware.

VMware Virtualization Software

A VMware vSphere solution is comprised of a number of different components and services (depicted in Table 1), which comprise the software platform that runs on the hardware to enable the virtualized system. ESXi is an infrastructure service, a hypervisor or basically a thin OS, that runs directly on the hardware. This is called a “bare-metal” design since there is no dependence on a general purpose operating system.

Table 1 - VMware vSphere Components

vSphere Components	Description
VMware ESXi	A virtualization layer run on physical servers that abstracts processor, memory, storage, and resources into multiple virtual machines
VMware vCenter Server	The central point for configuring, provisioning, and managing virtualized environments. It provides essential datacenter services such as access control, performance monitoring, and alarm management.
VMware vSphere Client	An interface that enables users to connect remotely to vCenter Server on ESXi from any Windows PC
VMware View	Virtual Desktop Infrastructure management software that provides services for managing the access of Virtual Machines through thin-client technologies.

There are a number of application services that makeup a complete solution but in Table 2, a few key services that provide particular value to a control system are highlighted.

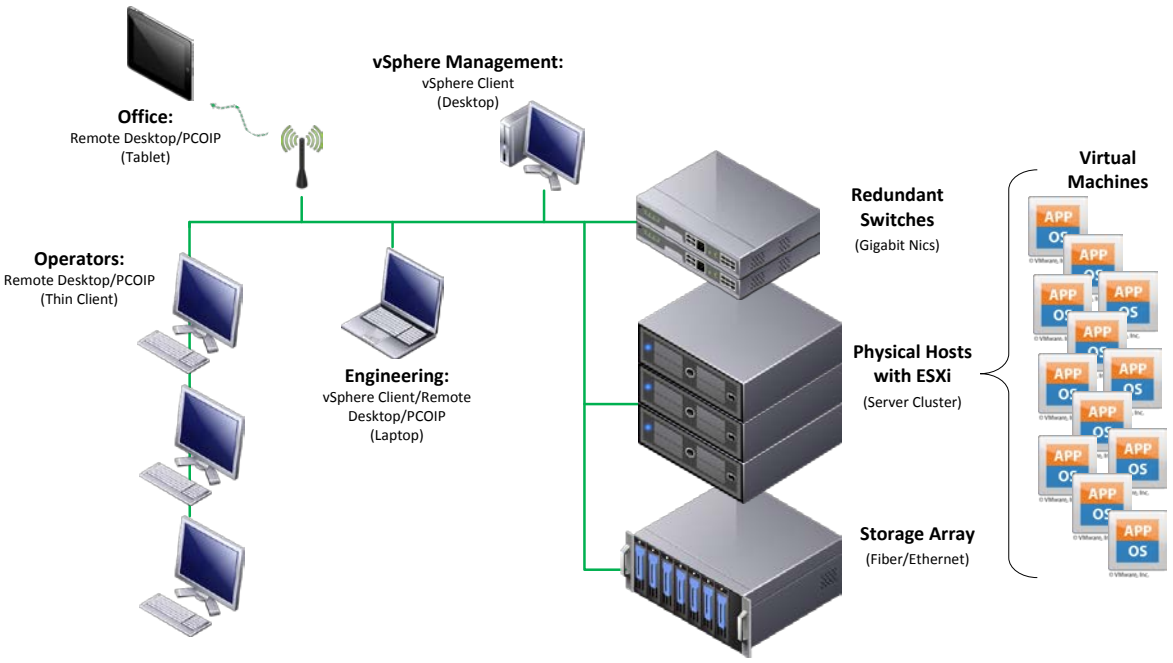
Table 2 - VMware vSphere Application Services

Key Application Services	Description
vSphere vMotion	Enables the migration of powered-on virtual machines from one physical server to another with zero down time, continuous service availability, and complete transaction integrity. Migration with vMotion cannot be used to move virtual machines from one datacenter to another.
vSphere Storage vMotion	Enables the migration of virtual machine files from one datastore to another without service interruptions. The virtual machine remains on the same host during Storage vMotion. Migration with Storage vMotion lets users move the virtual disk or configuration file of a virtual machine to a new datastore while the virtual machine is running. Migration with Storage vMotion enables you to move a virtual machines storage without any interruption in the availability of the virtual Machine.
vSphere High Availability (HA)	A feature that provides high availability for virtual machines. If a server fails, affected virtual machines are restarted on other available servers that have spare capacity.
vSphere Fault Tolerance (FT)	Provides continuous availability by protecting a virtual machine with a copy. When this feature is enabled for a virtual machine, a secondary copy of the original, or primary, virtual machine is created. All actions completed on the primary virtual machine are also applied to the secondary virtual machine. If the primary virtual machine becomes unavailable, the secondary machine becomes immediately active.
Distributed Resource Scheduler (DRS)	Allocates and balances computing capacity dynamically across collections of hardware resources for virtual machines. This feature allows users to define rules helping prevent specific VM's from inhabiting the same physical host.

Virtualization Infrastructure Physical Topology

A typical VMware vSphere based architecture consists of physical components including servers (Hosts), storage arrays, Ethernet networks, management PC, and desktop clients as seen in Figure 2.

Figure 2 - Infrastructure Topology (virtualized servers and desktops with HA/FT capabilities)



The Physical Hosts will run ESXi on “bare metal” and provide the CPU and memory resources for each of the Virtual Machines. For smaller systems, data storage is provided through HDD on the local Host. For larger systems and those requiring HA/FT, data storage is provided by the shared storage array. By grouping multiple physical hosts together in vSphere a user can create a server cluster, or resource pool. One of the advantages to virtualization is the ease of scalability. By simply adding another server to the cluster, the resource pool grows and more resources are available to the system to run additional virtual machines.

Storage arrays are connected to the server cluster and provide shared data storage for the entire system. By aggregating the data to a single array, a Virtual Machine can be run on any host (HA, FT, vMotion) because the compute resources are moving between hosts while the data is stored on the array, off the host.

Ethernet networks provide the backbone for the system. For systems requiring HA or FT, redundant switches are recommended. Multiple NIC’s allow each of the hosts and the VM’s they contain to access different VLANs (i.e. / Control System Networks, vSphere Management, Data Storage, etc.) through the use of Virtual Switches. VLAN planning will be discussed in the design recommendations section.

Management of your virtual environment is done through the vSphere Client. This is a PC with the vSphere Client software installed on a Windows Server Operating System. Physical hosts allow for some level of management on them directly, but for the most part are designed for headless operation. The vSphere Client provides a GUI for managing all components of the user's topology from a single point of contact. In order to do this, vSphere leverages a software component called VMware vCenter Server. VMware vCenter Server provides infrastructure services and data in regards to the different hardware and software components comprising a virtualization system. The vSphere Client(s) then subscribe to that service enabling users to visualize data/settings while also managing their system. VMware vCenter can be a physical server or it can be virtualized.

Operators are able to access their workstations through the use of thin clients, traditional desktops, or even tablets. One of the major benefits of virtualized operator workstations is that critical hardware is no longer exposed to plant conditions. If a thin client is damaged, it is easily replaced without any impact to the remote virtual machine. In the instance of a traditional workstation, if the desktop was damaged an engineer may have to rebuild (software, OS, application code) a replacement from scratch. This can often take a significant amount of time. If configured properly, an operator will not know that their workstation is even virtualized. For example, a thin client could link the local desktop login credentials to a specific virtual machine in the server cluster and use single-sign. When the operator logs in, it looks as if it was logging into the local machine. The use of thin clients will be discussed in greater detail in the Designing a Virtualized PlantPAx System section. For users that prefer to make use of existing desktop PC's, there is installable client software available from VMware that allows them to access the remote virtual machines in a very similar fashion.

If users are already making use of thin client technology, it can provide added benefits for engineering. As an engineer, a user could set-up permissions in the virtual environment such that their credentials provide them access to any number of virtual machines. As an example, an engineer may need to access Logix code for a particular application that is not available on the local operator workstation thin client. If the engineer were to login into that thin client, VMware would recognize that the engineer has permission to access a number of different virtual machines, one of which is an engineering workstation. That thin client is now converted from an operator workstation to an engineering workstation with the change of a login.

The use of virtual machines also enables users to make use of wireless tablets. Tablets do not have to have significant horsepower as they are not running the virtual machines, and instead are simply displaying it. Tablets act as a thin client connection to the system. This deployment is beneficial because the software and data are being run in a non-wireless system and the only thing being displayed to the tablet is a copy of the virtual machine display. The control software does not suffer from intermittent wireless communication.

Designing a Virtualized PlantPAx™ System

Before designing a virtualized PlantPAx System, readers should have a general understanding of the PlantPAx Control System architectures and sizing guidelines. Refer to the PlantPAx Selection Guide to learn how to properly size and build a system architecture. Reference the Selection Guide and Reference manual.

The sections below will discuss sizing calculations for Servers, Storage and Networking when creating a virtualized infrastructure from "scratch." If building from an existing system, there are a number of free tools available to measure existing system performance such as CPU and Memory Utilization in order to get an accurate sizing estimate. The Rockwell Automation Network & Security Services team provides services for the evaluation of an existing system and can provide system specifications and recommendations based on the findings. Please contact your local sales contact for more information.

Most importantly, before ordering any hardware, always be sure to check the VMware Hardware Compatibility List available at VMware.com.

> *VMware Hardware Compatibility List:*
> *http://www.vmware.com/resources/compatibility/search.php*

So what does a virtualized control system look like compared to a classic "physical" automation system? In a nutshell, there is a little more software and a lot less hardware depending on the target system size. The PlantPAx Control System software applications in a traditional system are still used in a virtualized system, but they are collapsed onto less hardware via the virtualization software.

In an extreme case it may be theoretically be possible to consolidate an entire simple automation system virtually on to one physical machine. This would be contingent upon having a sufficiently powerful processor and adequate memory, as well as an application that did not overtax the configuration.

In all practicality, a basic virtualized automation system would generally use three or more host physical machines, or servers. This is preferred to not only distribute the processing load, but more importantly to provide a pool of available hardware so that VMs could be restarted elsewhere in the event of a server failure. By increasing the available pool of servers, the user can extend the system into a higher availability configuration.

Server Recommendations

Rockwell Automation PlantPAx Characterization system data provides the following guidelines for server sizing. In order to use the information provided in the section, the user must have a known system architecture following the guidelines presented in the PlantPAx Selection Guide. For information in regards to SQL server sizing, refer to VMware best practices guides.

All numbers and figures in the following section should be referenced for initial sizing only. Actual performance may vary in final implementation. Once established as a system, VMware vCenter will allow users to observe and modify these settings to achieve optimal performance.

Number of Servers

The minimum number of servers recommended for systems making use of VMware FT or HA is 3. In the event that one server fails, the system will remain in a protected state across the remaining two servers. This also provides opportunities for one server to be taken offline for maintenance while maintaining protection. In both of these scenarios, the sizing of the servers must take into consideration that two servers must be sized to provide resources for the full system.

VMware limits the number of VM's that can be VMware FT protected to 4 per server. If additional machines require FT protection, additional servers will need to be taken into consideration.

When purchasing hardware, take into consideration future expansion plans by possibly adding an additional 20-30% of resources. VMware makes it very simple to scale the system size upward by adding servers in the future to provide additional resources.

CPU Calculations

Virtual Machines are always limited by the megahertz capability of the physical core. A common misconception is that a VM can utilize as much CPU megahertz as needed from the combined total available. A single vCPU VM can never use more megahertz then the maximum of one CPU/core. If a VM has 2 vCPUs, it can never use more megahertz than the maximum of each CPU/core.

Determine the number of physical cores required for a system by using the consolidation ratios in Table 3 in combination with the vCPU requirements documented in Tables 4 and 5 for a PlantPAx system with a known architecture.

Table 3 - CPU Consolidation Ratios

Server and Workstation Type	vCPU: Physical Core
Process Automation System Servers (PASS)	2:1
Operator Workstations (OWS)	6:1
Engineering Workstations (EWS)	2:1
AppServ – HMI	2:1
AppServ – Information Management	2:1
AppServ – Asset Management	2:1
AppServ – Batch	2:1
VMware vCenter	1:1
VMware View Server	1:1

Table 4 - PlantPAx Resource Requirements

PlantPAx System Elements (x64 bit OS)	vCPU	vRAM
Process Automation System Servers (PASS)	1	4 GB
Operator Workstations (OWS)	1	2 GB
Engineering Workstations (EWS)	1	4 GB
AppServ – HMI	1	4 GB
AppServ – Information Management	1	4 GB
AppServ – Asset Management	1	4 GB
AppServ – Batch	1	4 GB

Table 5 - VMware Component Resource Requirements

VMware Components	vCPU	vRAM
vCenter Server Sizing (Virtual, x64 bit OS)		
Less than 10 ESXi Servers	2	3 GB
10 to 50 ESXi Servers	2	4 GB
50 to 200 ESXi Servers	4	4 GB
VMware View Server (Virtual, x64 bit OS)		
Less than 25 View Desktops	2	4 GB
Between 25 and 50 View Desktops	2	6 GB
Between 50 and 75 View Desktops	2	8 GB

With the system requirements for physical cores calculated, divide the total system requirements by the minimum amount of servers that will be required to run the system at any given time. For example, with a 3 server system using VMware FT or HA the user should divide by two to help ensure that the system can continue to run with two servers should one server fail.

Memory Calculations

Using the data provided in Table 4, calculate the total resource pool size by multiplying the total number of each system element type by the number of resources recommended. The results provide a recommended amount of PlantPAx run-time resource needs.

Using the data provided in Table 5, calculate your VMware Infrastructure overhead resource requirements by adding up the recommended resources for 1 vCenter Server (depending on system size), 1 VMware View Server (if required).

Sample Sizing Calculation

Customer X's Process System Details:

Table 6 - Sample System Information

System Components	# of each	Total vCPU	Total vRAM
Process Automation System Servers (PASS)	1	1*1 = 1	1*4 = 4
Operator Workstations (OWS)	16	16	16 * 2 = 32
Engineering Workstations (EWS)	3	3	12
AppServ – HMI	3	3	12
AppServ – Information Management	1	1	4
AppServ – Asset Management	1	1	4
AppServ – Batch	1	1	4
VMware View Server	1	2	4
vCenter Server	1	2	3
	Total	30 vCPU	79 GB

Customer X requires a runtime memory resource pool of 79 GB to help ensure that all VM's have sufficient resources as shown in Table 6.

Calculate the runtime CPU resource pool requirements:

OWS = 16 vCPU / 6 = 3 physical cores

EWS, PASS, and AppServ = 10 vCPU / 2 = 5 physical cores

VMware Components = 4 vCPU / 1 = 4 physical cores

Customer X requires a total CPU resource pool of 12 physical cores.

Customer X would like to make use of 3 servers such that they have the ability to take a server offline for maintenance while maintaining redundancy between the remaining two. When purchasing servers, Customer X should size servers such that two can withstand the entire load.

Cores per Server = 12 Cores / 2 Servers = 6 Cores/Server

Memory per Server = 79 GB / 2 Servers = 40 GB/Server

Customer X would also like to allow for future expansion and assumes growth of 30%. In this scenario, Customer X would purchase 3 servers with the following specifications:

*Cores per Server = 6 Cores/Server * 1.30 = 8 Cores/Server*

*Memory per Server = 40 GB/Server * 1.30 = 52 GB/Server*

Storage Recommendations

Storage for the system will either be local to the physical host or on a separate network storage device that is shared between hosts. To take full advantage of a virtualized system (with VMware features such as HA, FT, vMotion, etc.) the user would need to make use of a shared storage device. For systems that require a single host where only a few virtual machines will be running, it would be more cost effective to run a local solution.

If a user desires a local storage device, be aware that software RAID controllers such as PERC S100 and S300 that are available with many servers are not compatible with the vSphere. Instead, make sure to choose hardware-based RAID controllers.

A Network Storage Array offers the greatest storage flexibility, and VMware can support a variety of options. Connection to the network storage can be via Fiber Channel (using specific hardware), iSCSI (over IP networks), or some other type of Direct Attached Storage. VMware allows storage via any of these methods to be allocated to each VM, but does not directly expose the VMs to the complexity of any one storage technology.

When sizing storage, the input/output operations per second (IOPS) and overall storage capacity must be determined. Rockwell Automation has investigated the values for VMs in various process control system elements and has developed characterized data. Users can utilize this baseline data to understand system requirements and to specify storage as needed.

Data storage on a storage area network (SAN) via the iSCSI protocol is highly recommended. iSCSI provides a reasonable compromise between cost and IOPS (I/O per second) performance. Fiber Channel can provide much higher IOPS performance (3x that of iSCSI) but may be cost prohibitive to many users. Direct Storage can only be configured to connect to a single host and is not recommended as it cannot make use of VMware features such as vMotion, FT and HA.

The characterized data in Table 7 assumes the user is following the PlantPAx guidelines for installing software, operating systems and configuration. The virtual machine virtual HDD disk size is also assumed to be near a certain size as noted in the figure. This data is for the operation of Rockwell Automation Software only. Use Table 8 to adjust the IOPS numbers in Table 7 if the components will require common software such as MS Office. Similar to the server sizing exercise, add up the IOPS requirement for each individual system element to derive your entire system need.

Table 7 - PlantPAx IOPS Requirements (Based on iSCSI SAN)

PlantPAx System Elements	Avg #IOPS	Avg # Reads/Sec	Avg # Writes/Sec
Process Automation System Servers (PASS)	40	35	5
Operator Workstations (OWS)	15	10	5
Engineering Workstations (EWS)	30	24	6
AppServ – HMI	40	25	5
AppServ – Information Management	100	20	80
AppServ – Asset Management	10	3	7
AppServ – Batch	10	3	7
VMware View Server	5	2	3
vCenter Server	15	10	5

Table 8 - Other Software IOPS Requirements

Other Software	Avg #IOPS	Avg # Reads/Sec	Avg # Writes/Sec
Anti-Virus	180	174	7
Microsoft Office	5	2	3
IE Browser	5	2	3

With the total IOPS/sec requirement for the system, reference figure X to understand IOPS/sec limitations based on RAID type and Disk speed. RAID levels offer varying levels of data and hardware protection. Higher levels of protection require additional disks to achieve certain levels of capacity and performance. Disk speeds are a tradeoff of performance vs. cost. The figure displays IOPS/sec capabilities for each disk. By adding disks, the system is able to accommodate more IOPS/sec capacity. In order to calculate the number of disks required, divide your IOPS/sec system requirement by the IOPS/disk capability associated with the desired RAID level and Disk speed preference.

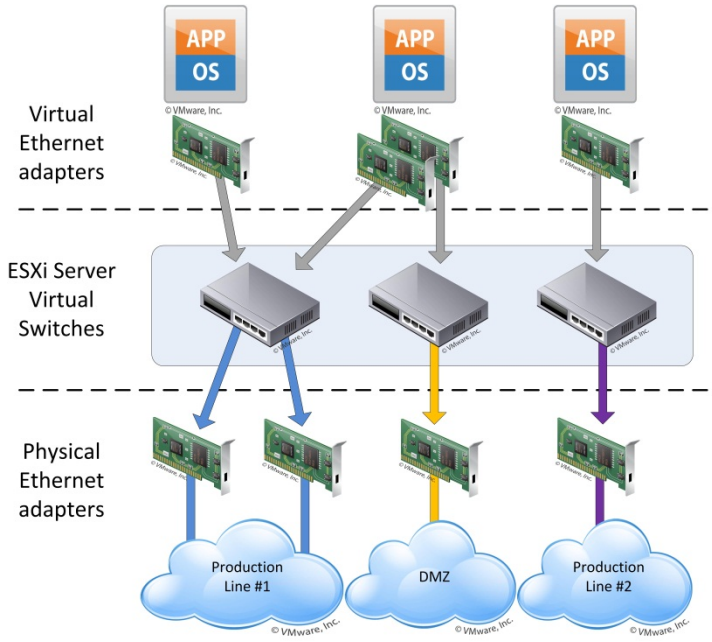
RAID Level	WRITE IO Penalty	Read s 15K	WRITEs 15 K	READ 10 K	WRITEs 10K	READs 7.5K	WRITEs 7.5K
RAID 0	0	150-170	140-150	110-120	100-110	70-80	60-70
RAID 1	2	150-170	70-80	110-120	50-60	70-80	35-45
RAID 5	4	150-170	30-45	110-120	25-25	70-80	15-25
RAID 6	6	150-170	30	110-120	15-25	70-80	10-15

With number of drives and speed, you can now select a storage solution. Manufacturers provide drives with varying amounts of capacity at each speed. Solutions are based on the number of drives and storage arrays that can be “stacked” to gain additional drive capacity and/or performance.

Network Recommendations

Virtualization makes use of Virtual Switches and Virtual Ethernet Adapters to organize network traffic in the virtual environment. Figure 3 shows a diagram depicting how these two virtual component work with the physical NIC on each server. The Physical NICs on each host act as trunks into the virtual environment for different VLAN’s. A virtual switch is placed at the end of the trunk that allows users to connect different VM's to that trunk or VLAN. This virtual switch is similar to a physical switch and provides many of the same capabilities.

Figure 3 - Virtual Networking Example



In order to determine how many physical NIC's are required, the number of VLAN segments must be determined. For every system the basic VLAN requirements include separation of VMware Management, Virtual Machine and Storage Networks. This is done to increase performance and stability while minimizing potential issues with bandwidth contention.

VMware Management networks are used by the virtual environment administrators to initiate moving virtual machines with vMotion, to communicate between the various hosts, and to collect system data, etc.

The storage network is set up to separate the high traffic read/write requests from the other networks. It is recommended that there are two NIC's per SAN device to help ensure adequate bandwidth for the VMs.

The VM networks will be the primary networks with which the VM's communicate. These VM networks are typically the same networks that the physical control systems utilize for the rest of the system communication.

In Table 9, an example is shown for the number of physical NIC's required by a server requiring access to every network.

Table 9- NIC Requirements

VLAN Types	Basic	Fault Tolerance (FT)
VMware Management (i.e. / vMotion, etc)	1	2
VMware FT (If FT required)	0	1
iSCSI Storage (if iSCSI used)	2	4
VM Networks	1	2
Production line 1	1	2
Production line 2	1	2
Firewall	1	2
Total NIC's required / host	7	15

Virtual switches represent Layer 2 switches in the PlantPAx architecture. The Virtual Switches provide networking between the various workstations and system servers. The Hosts and storage are all networked through gigabit NIC technology to a physical switch, or redundant switches. These physical switches supporting the virtual infrastructure are then uplinked to the Layer 3 switch for access to VM Network VLANs for Production Lines Firewalls, etc. The VLANs supporting VMware Management, VMware FT and storage are local to the switches supporting the virtual environment and do not require uplinks to the Layer 3 network.

Virtual Desktop Infrastructure (VDI) Recommendations

PlantPAx Characterization activities evaluated the use of thin clients with virtual environments (also known as Virtual Desktop Infrastructure) using VMware View. VMware View provides a management service for accessing VM's from thin clients. Administrators are able to associate log-in credentials with a specific VM or a group of VM's. If a group of VM's is enabled, the user will have the option of which VM they would like to access.

As an example, if an operator were to login, they would typically only have access to the Operator Workstation VM. If an engineer were to login to that same thin client, they could potentially access a variety of VM's including an Engineer Workstation VM. VMware View provides flexibility such that any user can access their desktop(s) from different locations using different devices.

VMware View makes use of two protocols for accessing VM's remotely, PCOIP (PC over IP) and RDP (Remote Desktop Protocol). RDP is an established and common Microsoft technology. RDP can be used for both desktop and server operating systems. PCOIP is available for desktop OS's only and provides more efficient transmission across the network for multimedia or video streaming. When used in the PlantPAx Control System, both RDP and PCOIP provide acceptable performance. The PlantPAx system does not push the network utilization enough to see the benefits of a PCOIP solution at this time. Selection of a protocol is up to user preference.

There are a wide variety of low cost thin client hardware devices that can be used to remotely access the VM's. Each piece of hardware contains a minimum amount of CPU and memory resources with a "thin" or embedded OS. Typically, there is no local storage. The user should confirm that there are sufficient USB and display connections available for connecting the appropriate interface technologies (i.e. / mouse, keyboard, monitors, etc).

Three solutions containing different operating systems were evaluated in the PlantPAx Characterization Lab in conjunction with VMware View. The solutions were Embedded XP (eXP), Linux, and Zero Client. All of these operating systems supply very basic functionality while requiring minimal resources to operate. Upon evaluation of these three solution types, none provided significant performance improvements over the other. Selection of a client type is up to the user preference.

Virtualized PlantPAx System Configuration

Once the basic architecture is developed, a virtualized PlantPAx™ system will benefit from a number of fundamental VMware configuration choices. Most of these choices start with automatic settings, with adjustments made as required to increase speed and improve redundancy.

System Configuration Recommendations

Servers

The latest Intel™ processors offer on-board virtualization support. The Intel Virtualization Technology in the BIOS must be switched on to take advantage of the performance gains. To use Windows 7 as a VM operating system, the host must be ESXi 4.0 Update 2 or ESXi 4.1 or later.

Hosts in the same cluster that have different processors should have Enhanced vMotion Compatibility (EVC) enabled to support the vMotion between hosts. EVC is enabled at the Datacenter/Cluster level. EVC is a fundamental technology that facilitates virtual machine migrations between different generations of CPUs, while vMotion is the utility used to make the migrations. The ability to migrate VMs between servers while they are running with the process completely transparent to any users is one of the leading benefits of virtualization.

Storage

Network attached storage uses a software network adapter to connect with iSCSI storage through Ethernet. Enable jumbo frames at the physical switch level and also at the virtual switch port level. Jumbo Ethernet frames carry up to 9,000 bytes of payload (as opposed to the normal 1,500) and can offer increased data through put with reduced CPU utilization, but the network must be configured to support jumbo frames from end to end.

When configuring the physical NICs on a host, setup NIC teaming in the Virtual Switch Configuration to enable greater bandwidth for storage traffic.

Each virtual hard drive on a network is assigned a logical unit number (LUN) to uniquely identify it. A LUN is a logical unit number of a virtual partition in a storage array. When assigning virtual hard drives from VM's to a LUN, be sure to balance intensive and non-intensive I/O applications. This will improve performance by balancing I/O traffic across multiple hard drives. A typical LUN size is between 400 GB and 800 GB. The maximum number of virtual machine hard disks(VMDK) on a LUN should not exceed 30, as more VMDKs could impact the performance because of disk queuing.

The LUN size is calculated by adding the total capacity (GB) of storage required plus VM Swap File requirements and finally additional room for VM Snapshots. When dividing the storage array into LUNs, the following equation can be used to determine appropriate sizing.

Calculated LUN Size = GB Capacity + VM Swap File Requirements + Snapshot Reservations

= 30(average VM virtual disk size) + 30*(average VM RAM) + 15% of (30 x average disk size).*

Networks

Connect VMs residing on the same ESXi server and same VLAN to use the same virtual switch. If separate Virtual Switches are used and connected to separate physical NICs, traffic will route separately through the wire and incur unnecessary CPU and network overhead.

Speed and duplex setting mismatches are common issues that will cause network problems. For ESXi, VMware recommends “Auto Negotiate” for both devices on the ends of a network link. It is also acceptable to set both ends for “1000 MB / Full Duplex” or “100MB / Full Duplex” if required by the network hardware. Never hard code settings on one device while choosing “Auto Negotiate” for the corresponding device, and never select half-duplex. Mismatches such as this can not only reduce performance, but may even cause connectivity problems.

VMware systems demand a high level of network performance by nature, so any methods to reduce bottlenecks should be explored. One such method is NIC teaming, where a single virtual switch can be connected to multiple physical Ethernet adapters. A team defined in this way can not only share the traffic load, but can provide a means of failover.

There are several options available for load balancing. The default is “route based on the originating virtual switch port ID”, where traffic from a given virtual Ethernet adapter is consistently sent to one physical adapter (unless there is a failover). Another option allows the Virtual Switch to load balance between multiple physical adapters. This is set by configuring EtherChannel link aggregation on the Cisco switch and the the load balancing setting is set to “route based on IP hash” in the Virtual Switch.

A combination of NIC teaming and the Cisco Switch load balancing settings are recommended for improved performance when accessing networked storage.

Virtual Machine Configuration and Optimization

VMs intended for use with Rockwell Automation applications should be configured to follow some basic recommendations.

VMware offers options for manually assigning CPUs to VMs, called CPU affinity. There may be situations that required this granular level of control, but a general practice should be to set VM CPU affinity only when necessary. Accepting default settings will generally result in the best performance.

If it is necessary to use a 32-bit guest operating system as a VM on a 64-bit server, select the CPU/MMU virtualization to use software for the instruction set, and Memory Management Unit (MMU) virtualization for improved performance.

Various options are available for hard drive controllers when provisioning a Windows 2008 VM, make sure to select the SCSI controller as LSILogic Parallel, since by default it will be LSILogic SAS. The hard drive is still virtually handled, but Parallel is the recommended setting.

While it is possible for VMs to communicate with each other via the host using the network layer, this adds communications overhead. A better option for VMs that must communicate frequently is to enable VM Communication Interface (VMCI) on each VM. VMCI is recommended for all PlantPAx System Element VM’s. VMCI offers fast and efficient communications between VMs, and can approach speeds that are five times greater than a normal internal network.

There is an option to specify a provisioning policy when a VM or virtual disk is created. The provisioning policy can be “thick” where the required disk space is initially allocated, or it can be “thin” where the disk space starts small and is allocated as needed. However, for a VM to be compatible with fault tolerance, it’s recommended that the VM use Eager Zero Thick Provisioning.

How snapshots and backups can be effectively used, are discussed later in this article. However, migrating a powered-on VM from one host to another that contains a snapshot is not a supported function.

Enable the hardware acceleration feature under the advanced graphical display settings to improve the mouse movement. Power options should be set for high performance, with no sleeping or hibernating.

System ion can be turned off, and the associated System Restore points removed. This frees disk I/O and CPU resources, and these functions can be superseded by VMware snapshots and backups. Encryption, backup, and defragmenter services are all examples of components that may be disabled.

VMware offers an optimization guide with a comprehensive list of services, along with recommendations on which to disable. This guide is called “VMware View Optimization Guide for Windows 7” and is listed in the reference documents of this paper.

Another key is to maintain VMware Tools up-to-date inside each guest operating system. When migrating or converting a VM from an older version ESX server, a best practice is to remove the old Tools and install the latest version.

Antivirus and Backup Recommendations

VMs are susceptible to virus attacks just like their physical counterparts. Of course, the same antivirus and malware applications used to help protect physical machines can be deployed on VMs. When it comes to antivirus, malware, and backup issues, VMs offer some significant benefits.

VMs are effectively “sandboxed” from each other and the host, but it is possible for services such as shared folders and network folders to facilitate VMs infecting each other or the host. By defending the guest systems, protection programs help ensure the integrity of the entire system.

In most installations, an antivirus package software program will be required. PlantPAx specifies Symantec Antivirus Software and is the only antivirus package that is qualified for use the system. The PlantPAx Recommendation Manual provides recommendations on how to install and configure Symantec antivirus software.

The antivirus software must be configured on the VM in an optimal way to maximize performance. The virus scans should be scheduled to take place during the off-peak hours, and staggered to avoid the collision of application requests for resources. Real-time virus scanning will greatly impact the performance of the servers, so this feature should be disabled if possible. Excluding files such as databases and swap files from virus scans will further improve performance.

VMware is capable of taking VM “snapshots”, which capture the entire state of the VM including the memory and files. Snapshots are not considered to be a proper backup strategy, but they can be used to restore a VM or file to a known “good” point during testing or development.

Snapshots can consume as much disk space as the VM itself, and using snapshots negatively impacts VM performance, so care must be taken with their use.

Since a VM is really just a series of bundled files, it is easier to back them up than it is to back up a physical machine. VMware backups to disk are fast to make as well as to restore. Options are available to back up VMs from the host level, or to execute full, differential and incremental backups from within the VM. If running the backup agent in the VM, it should be scheduled to run during off-peak hours.

Just like a physical system, in the event that malware damages files or causes data loss, the user will need to have a solid backup and restore plan in place to allow the VM or its contents to be reverted to a known “good” state.

VMware Converter Best Practices

In some cases, the virtualized automation system will be created from scratch, but in many other instances, migration from an existing PlantPAx system will be required.

VMware vCenter Converter is the software tool used to convert physical machines and third-party disk images into a VM format ready to deploy in a virtualized system. The latest version of VMware Converter should always be used. As detailed below, there are a number of steps and best practices to follow when making conversions.

Running vCenter Converter as a local administrator is fundamental to avert any permission issues. Remote conversions are possible, but one must still log in as administrator.

As with all software installations, it is recommended to stop as many running programs as possible. In particular, databases such as SQL should have their services and applications stopped in order to avoid data file corruption. Disabling real-time antivirus scanning is also recommend as it removes another possible cause of conflict during the process.

If the destination is an ESXi host, then connection to it should be made using the actual IP address instead of the DNS host name to circumvent any connection issues. The source disk needs at least 200MB of space to support snapshot features used by Converter, and if the source partition is larger than 256GB, then it’s necessary to increase the destination datastore’s block size above the 1MB default.

First, never convert diagnostic or recovery partitions, or unrecognized file systems. Next, refrain from modifying the recommended systems settings, such as resizing partitions or adjusting network interface card (NIC) quantities. Pay attention to the virtual disk type. Many times the conversion default is for the VM to use an IDE virtual disk, which can cause degraded performance or even an initial failure to boot. The solution is to convert the virtual IDE disk to a virtual SCSI disk. Follow detailed VMware Knowledge Base instructions (at kb.vmware.com, search for “convert virtual IDE to SCSI”) for the procedures. Finally, deselect any options to install VMware Tools or automatically powering on the virtual machine, as this can be done after a clean conversion.

Before running the application for the first time after conversion, adjust the number of virtual NICs, customize the computer name, and assign the IP addresses as needed for unique identification. Remove any unnecessary virtual devices such as COM ports, floppy drives, and USB controllers.

Start the VM in Safe Mode, and use the normal Windows functions to remove any unnecessary devices, drivers, and other items. The idea is to streamline the instance to the greatest extent possible. Restart in Normal Mode and check the Event Log for any error messages that need to be addressed.

With the newly converted VM up and running normally, install VMware Tools, and restart if required. For some systems it may be necessary to customize the VM's identity further through the use of the Microsoft SysPrep utility. In any case, ensure that the VM boots normally, and confirm any static IP addresses, as well as reconnect any disconnected virtual NICs.

Pay attention to the virtual disk type. Many times the conversion default is for the VM to use an IDE virtual disk, which can cause degraded performance or even an initial failure to boot. The solution is to convert the virtual IDE disk to a virtual SCSI disk. Follow detailed VMware Knowledge Base instructions (at kb.vmware.com, search for "convert virtual IDE to SCSI") for the procedures.

If any difficulties are experienced with the conversion process, try again but reduce the number of optional settings. The very latest specifics of VM converting can be found by searching the VMware Knowledge Base for topics such as "Converter Best Practices."

Licensing Considerations

VMware Licensing

The VMware licensing scheme is based on the number of physical CPUs (regardless of how many cores they contain), and the amount of virtual memory (vRAM) assigned to the VMs. vRAM "entitlements" are pooled on the system, and only powered-on VMs count against the pool.

Licensing is offered in "editions" purchased on a per-CPU basis, with each version allowing more vRAM per CPU and more features. A snapshot of some of the editions can be seen in Table 10. For smaller users, VMware offers entry level kits called "Essentials" and "Essentials Plus." These kits provide competitive entry level pricing with the sacrifice of not being scalable beyond the licensed limits. Users should take into consideration future expansion when purchasing licensing. There are a number of options available from VMware, and Rockwell Automation suggests that you talk to your local VMware distributor for the best solution.

Table 10 - VMware Licensing & Features

	Essentials	Essentials Plus	Standard	Enterprise
Physical CPU	3 servers, 2 proc.	3 servers, 2 proc.	8 proc. starter kit	6 proc. starter kit
vRAM Entitlement	32GB (192GB total)	32GB (192GB total)	32GB / CPU license	64GB / CPU license
Scalable	✘	✘	✔	✔
Thin Provisioning	✔	✔	✔	✔
Update Manager	✔	✔	✔	✔
Data Recovery		✔	✔	✔
High Availability		✔	✔	✔
vMotion		✔	✔	✔
vShield Zones				✔
Fault Tolerance				✔
Storage vMotion				✔
DRS/DPM				✔

Microsoft Windows Licensing

Licensing for Microsoft is tied to physical hardware and not to virtual machines. This traditional licensing model is of interest when a user tries to run multiple Virtual Machines on a single host.

For Microsoft Server Operating Systems, each host server must be entitled for the virtual machine “high water mark”, or maximum amount of Virtual Machines that host server will ever run at a given time using Microsoft Windows Server. There are various Microsoft Licenses, as seen in Table 11, and each allows the user to define a maximum amount.

Table 11 - Windows OS Licensing

Server Operating System	Entitlement
Windows Server Standard	1 Virtual Machine
Windows Server Enterprise	4 Virtual Machines
Windows Server Datacenter	Unlimited Virtual Machines.

Desktop licensing (Windows XP, Windows 7, etc) is also based on physical hardware. Each client device requires Windows Software Assurance, Intune, or Virtual Desktop Access Licensing. Each license enables the client hardware to use up to 4 Virtual Machines in the Virtual Datacenter and/or 4 Virtual Machines to run locally. These will also entitle the user to “roam” to other devices such as tablets.

Rockwell Automation Software Licensing

Virtualization does not change how Rockwell Automation Software is activated and licensed. The FactoryTalk Activation Server is fully supported in virtualized environments.

Conclusion

Virtualization is a powerful tool for improving the reliability and cutting the cost of Rockwell Automation Windows-based software applications in process plants. All of the software applications in the PlantPAx™ Process Automation System architecture can run in a VMware virtualized environment.

While the most obvious benefit of virtualization is reducing the number of required PCs, more important benefits are improved reliability, ease of upgrades and increased application longevity.

Although hardware costs are drastically reduced with virtualization, initial software investments and ongoing administration costs are increased. Even given these factors the benefits of virtualization will significantly outweigh the drawbacks for most process plants, particularly those simultaneously running a number of PlantPAx™ applications.

In the future, the relative advantages of virtualization over the traditional one application/one OS/one PC approach will increase as the technology becomes more widespread—as PC hardware, Microsoft Windows operating systems and PlantPAx™ applications become further optimized for operation in a virtual environment.