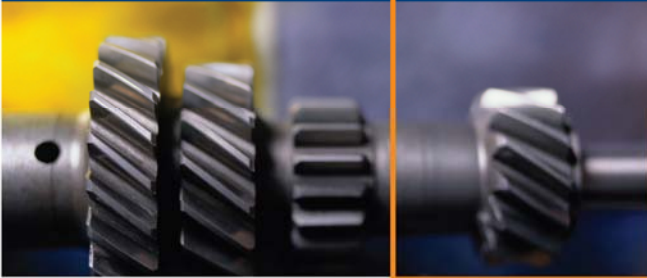


WHITE PAPER



VMware Infrastructure 3

Security Best Practices

VIRTUAL TECHNOLOGIES...REAL RESULTS

www.foedus.com

Contents

Contents.....	1
Overview	2
Target Audience	2
Prerequisite Knowledge	2
VMware Virtual Infrastructure 3 Architecture Overview	3
VI3 Operational Security Challenges	5
Applying a Sound Security Design to Virtual Infrastructure	5
User Accounts and the Least Privilege Principle	5
Auditing and Logging	6
Secure Networking for VI3.....	6
Shared Storage	7
Services.....	8
Management.....	8
Patching	8
Best Practices for Securing VI3	10
ESX Server Hosts.....	10
ESX Server Best Practices.....	10
VirtualCenter Management Server.....	10
VirtualCenter Best Practices	11
ESX Server Operational Practices to Avoid	11
VirtualCenter Server Operational Practices to Avoid	11
Appendix	12
ESX Server Services and Ports	12
VirtualCenter Services and Ports	13
About the Authors	15

Disclosure

The collaborative effort of several Foedus engineers, this whitepaper draws on three years of extensive experience designing, implementing, and troubleshooting VMware based virtual infrastructures for SMB and Enterprise customers.

This paper neither necessarily reflects VMware Inc.'s position, nor is it endorsed by them.

Overview

VMware ESX Server and VirtualCenter Server Virtual Infrastructure platform technologies provide a powerful yet flexible layer between a system's physical hardware and operating system. The timely development and publication of implementation and deployment best practices has been challenged by the rapid rate of VI adoption as organizations increasingly seek the business benefits it is capable of delivering.

Foedus developed this whitepaper to help network administrators, server administrators, and other individuals specifically focused on security, understand and address the many security implications of Virtual infrastructure. It provides objective guidance for integrating VMware Virtual Infrastructure 3 (VI3) and IT infrastructure without compromising security in the process.

Since ESX Server host default installation is inherently secure this whitepaper is not intended to describe how to harden VI3 as is commonly understood, rather to convey the requisite knowledge and proper planning necessary to prevent unintentionally relaxing security controls when granting operational access to VI administrators and operators. This whitepaper will explain how to deploy VI3 in a secure manner without compromising security in the process.

Target Audience

- Chief Security Officer or Chief Information Officer
- Network/security administrator
- System/server administrator

Prerequisite Knowledge

- Basic network security
- Basic authentication and authorization practices in Windows and Linux

VMware Virtual Infrastructure 3 Architecture Overview

A brief overview of the architecture of VI3 is a fundamental prerequisite to an understanding of the security concerns surrounding VMware Virtual Infrastructure. VMware ESX Server 3 and VirtualCenter 2 constitute the VI3 architecture's major software components. VMware ESX Server is a robust, proven virtualization platform that abstracts processor, memory, storage and networking resources into multiple virtual machines.

VMware ESX Server consists of four major components (see Figure 1. ESX Server Components):

- **The Virtualization Layer (or VMKernel)** Kernel software designed by VMware to run virtual machines, it controls the hardware resources utilized by ESX Server hosts and schedules their allocation among the virtual machines.
- **Virtual Machines** The containers in which applications and guest operating systems run. All VMware virtual machines are isolated from one another by design. Virtual machine isolation is transparent to the guest operating system.
- **The ESX Server 3.0 Service Console** The service console provides an execution environment to monitor and administer the entire ESX Server host. It is a limited distribution of Linux based on Red Hat Enterprise Linux 3, Update 6 (RHEL 3 U6).
- **The Virtual Networking Layer** The virtual network devices through which virtual machines and the service console interface with the physical network.

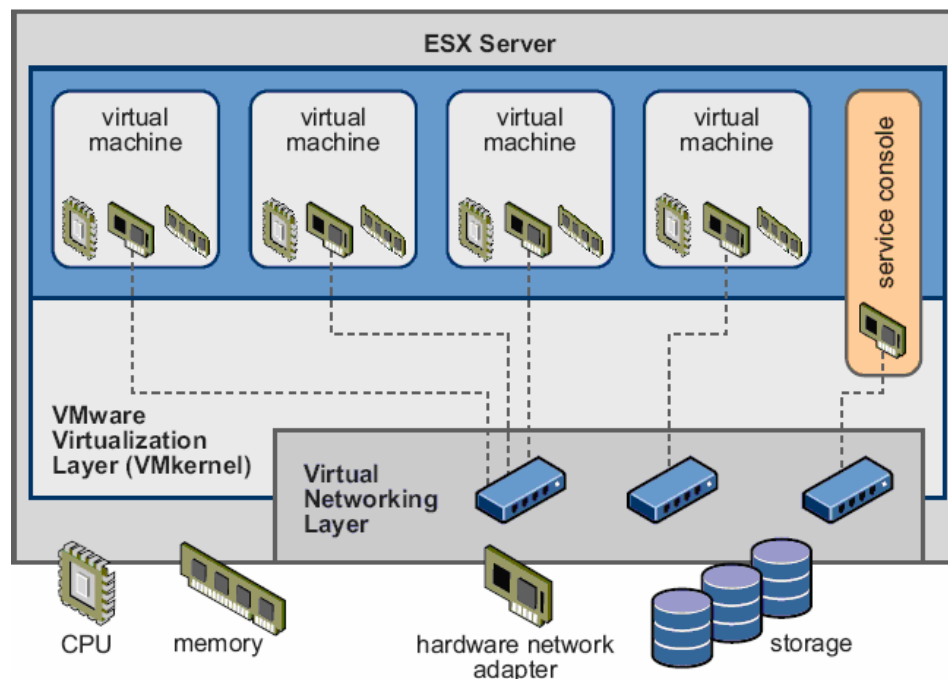


Figure 1. ESX Server Components

The ESX Server management interface or Service Console is a customized, enhanced security version of Red Hat Enterprise Linux 3. The Service Console is a specialized virtual machine used to interface to and manage the

VMKernel, not to be confused with the base operating system of hosted virtualization products (e.g., VMware Server) which run on Microsoft Windows or Linux OS.

The ESX Server management interface comprises four main components (ref. Figure 2: ESX Server Management Interface):

- **VirtualCenter Management Server** The central control node for configuring, provisioning and managing virtualized IT environments. The Management Server runs as a service on Microsoft® Windows 2000, Microsoft® Windows XP Professional, and Microsoft® Windows Server 2003.
- **VirtualCenter Database** Stores persistent information about the physical servers, resource pools, and virtual machines managed by the VirtualCenter Management Server. The database resides on standard versions of Oracle, Microsoft® SQL Server, or Microsoft® MSDE.
- **Virtual Infrastructure Client** Allows administrators and users to connect remotely to the VirtualCenter Management Server or individual ESX Servers from any Windows PC.
- **VMware License Server** Enables the management of all VMware software licenses with an embedded FlexNet licensing server and a single license file.

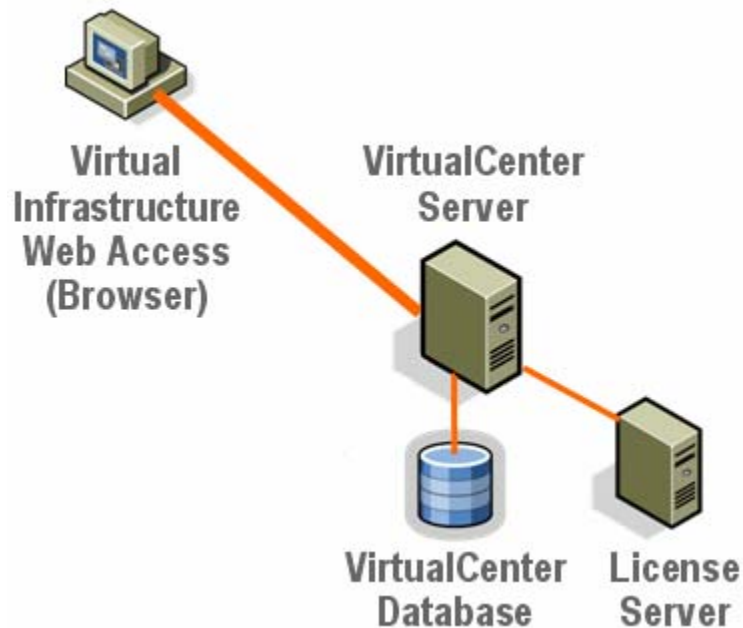


Figure 2: ESX Server Management Interface

Identification of the high-level components of VMware Virtual Infrastructure reveals the attack surface or inventory of system weak points, and the means by which security best practices and education can address each security concern.

VI3 Operational Security Challenges

The design of VMware virtual infrastructure components enables integration into heterogeneous environments with little to no significant design changes. This ease of use can easily lead to an open, insecure implementation of virtual infrastructure analogous to removing the door to one's physical datacenter because it is easier just to walk in. Avoiding this is the primary challenge facing an IT professional planning for security around VMware Virtual Infrastructure.

Applying a Sound Security Design to Virtual Infrastructure

Virtualization does not eliminate the need for security controls. With a measure of advance planning, administrators can successfully apply the basic principals of security planning and implementation to virtual infrastructure. This section explores such security planning for VMware Virtual Infrastructure implementations.

User Accounts and the Least Privilege Principle

When using the default ESX Server installation routine (rather than a scripted installation), one can set only the *root* account password and logon with this one account. The *root* account has the highest privilege within the service console of an ESX Server host, and has access to all configuration and operational settings. By default *root* is allowed logon access only from the physical server console (**ssh** access is not permitted by default). Similarly, the default installation of VirtualCenter assigns the hosting Windows server's local *Administrators* group the VirtualCenter role of "Administrator", which has the highest privileges within a VirtualCenter installation. This role grants full administrative control over all managed ESX Server hosts. When the VirtualCenter Windows server is a domain member, all members of the *Domain Admins* group automatically inherits these elevated privileges within the virtual infrastructure.

To enable multiple administrators to use and manage virtual infrastructure, one must create new accounts and explicitly assign them to individuals. The privileges of these accounts are associated with their responsibilities and are managed through the use of roles. VirtualCenter's granular permissions design allows one to create roles with specific permissions that are associated with Active Directory users or security groups. By leveraging this architecture, one can assign administrators only what permissions are required to fulfill their responsibilities and no more.

There are only two available account authorities for user authentication within the virtual infrastructure platform: local and Active Directory. By using a uniform directory service, such as Active Directory, one can enforce user security policies such as password strength and age. One has the ability to configure ESX Servers to use Active Directory for user authentication, create custom roles on the ESX Server, and assign them to Active Directory accounts.

Advanced configuration and troubleshooting of ESX Servers may require local privileged access to the service console. Under such circumstances, one should setup **sudo** (superuser do) to allow controlled and logged execution of privileged commands. One can grant or revoke **sudo** access to commands on an as-needed basis.

Weak user controls typically pose the greatest threat to a virtual infrastructure platform. One should make sure to apply strong user account controls by observing the following recommendations:

- Set a strong root password for one's ESX Server hosts, and control access to it
- Require administrators to use accounts specifically assigned to them to logon to the ESX Server service console, and require them to use **sudo** for privileged command execution
- Change the default role assignments in VirtualCenter to use a specific Active Directory group created just for VirtualCenter administrators
- Apply the least privilege principle to limit assignment of permissions
- Perform periodic audits to determine who has permissions to access what virtual infrastructure components

Auditing and Logging

Establishing logging for administrative changes to the virtual infrastructure platform is critical to maintaining security, and ensuring the veracity of the log entries requires a common standard for system time. Ensuring that all systems are time synchronized facilitates tracking and correlating an intruder's actions when reviewing the relevant log files. VirtualCenter features extensive logging of events and system activities, and one should consider establishing a centralized `syslog` service to consolidate one's ESX Server syslogs. To ensure secure and consistent logging of system events and accurate time synchronization for auditing and operational purposes, follow these recommendations:

- Configure the network time daemon (`ntpd`) on ESX Server hosts to synchronize with an internal ntp clock source which is in turn synchronized with a stratum-1 clock source
- Set the Windows time service on the VirtualCenter server to the same or similar clock source as the ESX Server hosts
- Configure the VMware tools service within the virtual machines guest OS to perform time synchronization between the service console and virtual machine
- Periodically verify the time is correct and consistent on all systems
- Establish a central syslog service, and configure ESX Server hosts to forward entries
- Review and archive log entries on a regular basis

Secure Networking for VI3

There are several different types of network traffic routed through the virtual networking layer:

- **ESX Server management** connections such as service console and VI Web Access
- **VMkernel ports** such as VMotion, iSCSI, and NFS traffic
- **Virtual** machine guest OS network connectivity

Though the ESX Server management communication is encrypted it should be secured, and it is recommended that these connections occur on a management VLAN or isolated network, separated from other, less secure network traffic.

VMotion network activity is not encrypted, so as a best practice this traffic should occur on a dedicated VLAN or connection and kept secure from network sniffing, as the running memory state of a virtual machine traverses the VMotion network and will likely contain privileged information. Hardware based SSL encryption is an option for securing VMotion networks in high security deployments.

iSCSI traffic should always be located on a separate physical network. Encryption is not available for Disk I/O, consequently this connectivity, if used, should be treated with high security.

NFS traffic can take on two purposes; NFS mounts can be used to store only ISO files and other support files (such as ESX Server patches), or used to store templates and virtual machine state files. In the former case, secure handling of this traffic may assume the same urgency as that which surrounds the NFS server. In the latter case treat the traffic with the same policies as iSCSI traffic.

Virtual machine network connectivity is essentially functionally equivalent to network connections to physical switches with directly attached physical servers. Virtual switches (vSwitches) support 802.1Q VLAN trunking, consequently attaching multiple VLAN trunks to the same virtual switch creates no more potential for routing loops and compromised network traffic than traditional physical switch trunks. Virtual machines have no visibility to any other VLAN traffic other than their own since the vSwitch will only forward packets destined to a particular virtual machine's MAC address, just as with physical switch architecture.

Shared Storage

ESX Server's virtual machine file system, VMFS, enables multiple systems simultaneous access to shared storage. File locking mechanisms prevent two systems from accessing the same file in read-write mode, but virtual machine files can be put into read-only mode (referred to as 'undoable mode') thus allowing another system to make a copy of a running virtual machine's disk(s). Configure zones within the SAN fabric to prevent unauthorized systems from accessing VMFS LUNs and vmdk files directly, paying special attention to templates. Since templates can easily be converted to virtual machines and booted, a malicious user could install software on a template for later exploit when a virtual machine is deployed from the compromised template.

iSCSI SANs allows one to make efficient use of existing Ethernet infrastructures to provide ESX Server hosts access to storage resources that they can dynamically share. As such, iSCSI SANs provide an economical storage solution for environments that rely on a common storage pool serving numerous users. One should consider iSCSI SANs as potential targets of security exploits as with any networked based system. One can take several measures to minimize security risks when configuring iSCSI on an ESX Server host. One should use a separate physical network infrastructure for connectivity to the iSCSI targets: allowing virtual machines to share virtual switches and VLANs with one's iSCSI configuration potentially exposes iSCSI traffic to misuse by a virtual machine attacker, since neither the hardware iSCSI adapter nor the ESX Server host iSCSI initiator encrypts the data they transmit to and from the targets (exposing the data to sniffing attacks). Ensure that none of one's virtual machines can see the iSCSI storage network to prevent intruders from listening to iSCSI transmissions. One should also configure authentication between the ESX Server host (or initiator) and the iSCSI device (or target) whenever the host attempts to access data on the target LUN.

Recommendations for securing shared storage:

- Use SAN fabric zoning to limit exposure to fibre attached storage
- Implement a separate Ethernet storage network for iSCSI datastores
- Do not allow virtual machines to access the virtual switches and VLANs of one's iSCSI storage network
- Configure initiator/target authentication between the ESX Server and iSCSI storage

Services

Only enable required services in the service console, such as NTP, PAM; management agents (HP SIM, IBM Director, Dell OpenManage, EMC Navagent); backup products (esXpress, Commvault). Do not treat the service console as a Linux host. Only install software supported by VMware. One should also consider and provide for potential negative interactions that can occur when layering applications and services (such as the need for additional log file space in the /var partition).

Management

Recommended management practices for ESX Server hosts and VirtualCenter servers:

- Create accurate and complete documentation for all aspects of the virtual infrastructure platform, including system configuration, network and storage connections, and administrative information. Keep this documentation current with all changes.
- Incorporate the virtual infrastructure platform in one's organization's monitoring systems and establish alerts for system issues and exceeding performance thresholds. Use the same process for monitoring virtual machines as physical machines whenever possible.
- Implement a change management process governing the review and approval of all configuration changes to the virtual infrastructure platform

An additional consideration bearing on operational security is the securing of virtual machine snapshots. One can create a complete snapshot of one's virtual machine, including its configuration state and application data, and treat the resulting snapshot like a collection of files using the add-on licensed product VMware Consolidated Backup or other available third-party backup products. This virtual machine snapshot can be mounted and booted on any compatible version of ESX Server. Some third-party backup products afford the capability to create encrypted backups that prevent restoration without the private key or password.

Patching

Applying patches to software is a critical part of a successful and secure operational strategy for all software systems today. VMware releases software patches for ESX Server and VirtualCenter as needed to address security issues and to fix bugs (it is not uncommon for several months to elapse between patch releases). The recommended software update strategy includes these practices:

- Determine whether an update is necessary for one's environment. Security fixes and critical fixes are typically the most essential.
- Analyze the risk factor of applying the update.

- Minimize the change to one's software environment whenever possible.
- Apply only those updates that address known issues in one's environment.
- Keep one's environment as current as possible.

The process of applying software updates to an ESX Server system has become complex and time-consuming. Each new update introduces changes into the existing system, and it is crucial to apply only the required updates in order to stay current with security fixes and minimize the changes to one's software environment while doing so.

ESX Server 3 provides a new software update model to address the challenges outlined above. This update model facilitates selective application of software updates specific to a particular environment. It also provides the flexibility of staying current with security and critical updates and allowing deferred application of non-critical updates. This new maintenance tool is named *esxupdate*, and must be run within the service console using root or root equivalent privileges. The *esxupdate* tool enables the virtual infrastructure administrator to list, query, validate, and apply updates to ESX Server hosts. The recommendations for patching one's virtual infrastructure environment are as follows:

- Apply the recommended practices for updating software, particularly ESX Server hosts and VirtualCenter servers
- Test patches on equivalent test hardware before applying the patches to production systems
- Keep aware of current security related information by regularly visiting the VMTN Security Center at <http://www.vmware.com/vmtn/technology/security/> and by subscribing to the security alerts at <http://vmware.simplefeed.net/subscription/>
- Apply VMware security related patches as close to release time as possible (after testing)
- Never apply standard Red Hat Linux patches to the service console OS
- Include any additional software installed in the service console (such as management agents) within the scope of software update cycles

Best Practices for Securing VI3

ESX Server Hosts

Adding ESX Server hosts is the most common method used to increase virtual infrastructure platform operational capacity. Most of the effort for securing VI3 must be applied to the ESX Server host layer through the following best practices as well as the ESX Server installation procedures.

ESX Server Best Practices

1. Use a strong password for the ESX Server host root account, and limit the number of people that know the password and that can use the root account.
2. Establish clock synchronization with an external, reliable clock source. The validity and value of audit trails is wholly dependent upon a timestamp standard, and using a common directory service for authentication requires a consistent time baseline. Configure the NTP service on every ESX Server to synchronize with a reliable NTP source that provides the time for the rest of the network.
3. Create a local non-privileged user account to enable local login to the ESX Server host for troubleshooting purposes.
4. Configure the ESX Server host to use a directory service to authenticate user accounts (such as LDAP or Active Directory).
5. Configure the **sudo** command for executing service console commands requiring elevated (root equivalent) permissions. **sudo** allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while logging the commands and arguments.
6. Create a separate group for VI administrators (as opposed to using the default **sudo** group named 'wheel').
7. Deselect the option to create a default virtual machine port group during ESX installation. (This option will create a virtual machine port group on the same network interface as the service console.)
8. Use a separate VLAN or physical network for the service console and VMotion network connections. (VMotion traffic is neither encrypted nor secured.)
9. Perform regular security audits and review log files.
10. Have virtual machine owners use RDP or VNC to administer their guest operating systems instead of using VirtualCenter or VI Web Access

VirtualCenter Management Server

The Windows OS affords potential exploitable security vulnerabilities and as a consequence the VirtualCenter Management server is the most likely target for an individual seeking to compromise virtual infrastructure security.

VirtualCenter Best Practices

1. Harden the VirtualCenter Windows server operating system by remaining current with both Windows OS and VirtualCenter application patches.
2. Create the VirtualCenter database on a separate physical server. Create a dedicated account for the VirtualCenter service, and set DB owner privilege for this account only during installation. After installation, one can reduce these privileges to just Invoke/Execute Stored Procedures, Select/Update/Insert, and Drop.
3. Create Active Directory (or LDAP Directory) Security groups matching the VirtualCenter security roles, and create the group and role association in VirtualCenter. Change the default association of the server's local administrator group with VirtualCenter's VirtualCenter Admin role to avoid making all members of *Domain Admins* VirtualCenter *Administrators*.
4. Replace the default VMware VirtualCenter SSL certificate with an appropriate certificate from one's organization. This will reduce the risk of the risk of compromising a VirtualCenter user account via login session replay attacks.
5. Treat the VirtualCenter datacenter container as a top level security boundary, and only assign permissions at this level to the individuals that require access to everything beneath it. (One can create folders below the datacenter and cluster containers and assign permissions there)
6. Ensure the supporting staff is adequately trained in VI3 operations prior to granting access to VirtualCenter
7. Establish or maintain policies and procedures for workflow relating to virtual infrastructure and ensure good change management controls are in place and complied with.
8. Perform periodic audits to ensure compliance with established polices and procedures.

ESX Server Operational Practices to Avoid

1. Do not treat the ESX Server service console as a standard Linux host. The ESX Server service console is more a management appliance than a true Linux host. Do not install any software in the service console that does not secure or improve ESX Server host management.
2. Do not expose the service console or VMKernel interfaces directly to the Internet or publicly connected networks.
3. Do not enable unnecessary services in the service console (e.g, NFS).
4. Do not enable direct **ssh** access for the *root* account. Rather, use a common account authority such as Active Directory and use **sudo** when elevated privilege is necessary.

VirtualCenter Server Operational Practices to Avoid

1. Avoid exposing the VirtualCenter Server to risky activities e.g. web surfing or email client installation. Do not expose the VirtualCenter server to the public internet.

Appendix

ESX Server Services and Ports

The following table lists the pre-configured services available in the VI Client, with corresponding TCP/UDP ports and the default status of the service. These services can also be enabled/disabled using the `esxcfg-firewall -e` and `esxcfg-firewall -d` commands.

Service Name	Description	Incoming Port(s)	Outgoing Port(s)	Default
AAMClient	EMC AAM Client	TCP/UDP 2050-5000 TCP/UDP 8042-8042	TCP/UDP 2050-5000 TCP/UDP 8042-8042	Enabled
CIMHttpServer	CIM Server	TCP 5988		Enabled
CIMHttpsServer	CIM Secure Server	TCP 5989		Enabled
CIMSLP	CIM SLP	TCP/UDP 427	TCP/UDP 427	Enabled
commvaultDynamic	CommVault Dynamic	TCP 8600-8619	TCP 8600-8619	
commvaultStatic	CommVault Static	TCP 8400-8403	TCP 8400-8403	
ftpClient	FTP Client		TCP 21	
ftpServer	FTP Server	TCP 21		
LicenseClient	VMware License Client		TCP 27000, 27010	Enabled
nfsClient	NFS Client		TCP/UDP 111, 2049	
nisClient	NIS Client		TCP/UDP 111, 0-65535	
ntpClient	NTP Client		UDP 123	
smbClient	SMP Client		TCP 137-139, 445	
snmpd	SNMP Server	UDP 161	UDP 162	
sshClient	SSH Client		TCP 22	
sshServer	SSH Server	TCP 22		Enabled
swiSCSIClient	Software iSCSI Client		TCP 3260	
telnetClient	Telnet Client		TCP 23	
TSM	Tivoli Storage Manager Agent	TCP 1500	TCP 1500	
veritasBackupExec	Symantec BackupExec Agent	TCP 10000-10200		
veritasNetBackup	Symantec NetBackup Agent	TCP 13732, 13783, 13720, 13734		
vncServer	VNC Server	TCP 5900-5964		
vpxHeartbeats	VMware VirtualCenter Agent		UDP 902	Enabled
vmware-authd ¹	VMware VI Client communication	TCP 902, 903 ²		Enabled

¹ The vmware-authd service is not configurable through the VI Client nor the esxcfg-firewall command. This service is referenced here to simply identify the communication port.

² TCP 903 is used for communication between the VI Client and the hosting ESX Server for VM Console sessions to virtual machines.

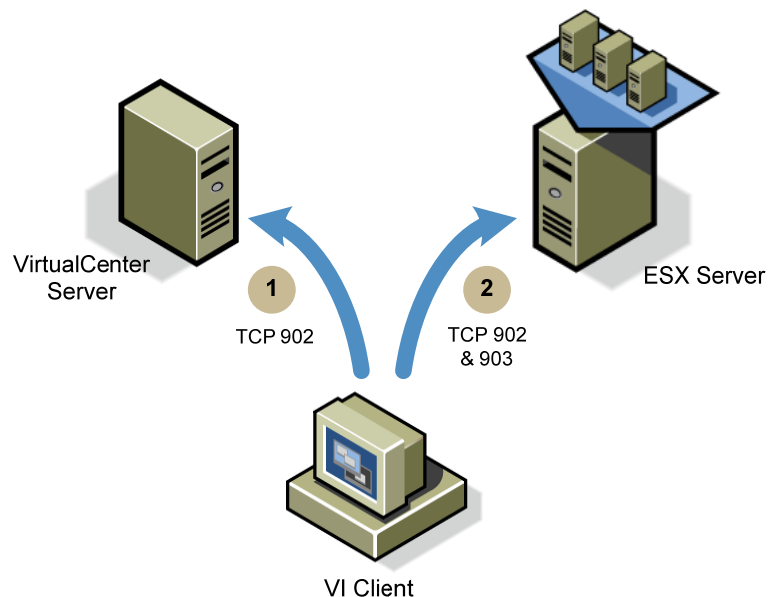
VirtualCenter Services and Ports

The following table lists and describes the services installed by VirtualCenter, and the corresponding listener ports created by these services.

Service	Listening Port(s)	Description
VMware License Server	TCP 27000, 27010	ESX Servers communicate with the VMware License Server on these ports
VMware Virtual Infrastructure Web Access	TCP 8005, 8006, 8086	Internal communication ports within the VirtualCenter server
VMware VirtualCenter Server	TCP 80, 443	Web-access ports for communication from client web browsers
	TCP 902	VI Client communication
	UDP 902	ESX Server virtual machine heartbeat communication from the vpxHeartbeat service
	TCP 8083, 8085, 8087	VirtualCenter diagnostic ports for internal service diagnostics

VI Client Communication

The VI Client connects directly to the ESX Server for the purpose of VM Console communication even when VirtualCenter manages ESX Servers. The relationships between the VI Client, VirtualCenter and ESX Server is illustrated below



The VI Client establishes communication with the VirtualCenter Server via TCP 902 to manage the virtual infrastructure.

The VI Client connects to the hosting ESX Server over TCP 902 to establish the session upon opening a virtual machine VM Console, and then opens a new TCP session on port 903 for the VM Console communication.

Default Firewall Configuration on ESX Server

The following tables represent the default ESX Server firewall, in regards to open communications ports for both incoming and outgoing traffic.

Incoming Connections

From	To	Protocol	Port(s)	Action	Related Service
Any	Any	TCP	902	Permit	vmware-authd
Any	Any	TCP	80	Permit	vmware-webAccess
Any	Any	TCP	443	Permit	vmware-webAccess
Any	Any	UDP	67-68	Permit	bootps/bootpc
Any	Any	TCP	2050-5000	Permit	AAMClient
Any	Any	UDP	2050-5000	Permit	AAMClient
Any	Any	TCP	8042-8045	Permit	AAMClient
Any	Any	UDP	8042-8045	Permit	AAMClient
Any	Any	UDP	427	Permit	CIMSLP
Any	Any	TCP	427	Permit	CIMSLP
Any	Any	TCP	22	Permit	sshd
Any	Any	TCP	5989	Permit	CIMHttpsServer
Any	Any	TCP	5988	Permit	CIMHttpServer

Outgoing Connections

From	To	Protocol	Port(s)	Action	Related Service
Any	Any	UDP	53	Permit	DNS Query
Any	Any	TCP	902	Permit	vmware-authd
Any	Any	UDP	67-68	Permit	bootps/bootpc
Any	Any	TCP	2050-5000	Permit	AAMClient
Any	Any	UDP	2050-5000	Permit	AAMClient
Any	Any	TCP	8042-8045	Permit	AAMClient
Any	Any	UDP	8042-8045	Permit	AAMClient
Any	Any	UDP	427	Permit	CIMSLP
Any	Any	TCP	427	Permit	CIMSLP
Any	Any	TCP	27000	Permit	LicenseClient
Any	Any	TCP	27010	Permit	LicenseClient
Any	Any	UDP	902	Permit	vpxHeartbeats

About the Authors

John Dodge, VCP, MCSE, CCNA, is a Managing Partner of Foedus Group, LLC. John primarily spends his time designing and implementing virtual infrastructure platforms for Fortune 500 companies and has over twenty years technical and management experience in IT infrastructure. John is also a highly regarded subject matter expert for Pharmaceutical Virtual Infrastructure qualification.

Michael Burke is a Senior Virtual Infrastructure Engineer for Foedus LLC. Mike has over five years experience working with VMware products, has written several technical articles, and was a technical editor for the book "VMware ESX Server: Advanced Technical Design Guide"

Rob Daly is a Senior Systems Engineer for Foedus. A VMware Certified Professional (VCP), Rob has worked in the IT industry for 9 years. Over the last four of those years, Rob has concentrated his focus on virtual infrastructure, having designed and implemented a wide variety of VMware ESX solutions for companies throughout the US, including several listed within the Fortune 100.

fo  dus

Virtual Technologies...Real Results

30 International Drive
Portsmouth, NH 03801
877-2-foedus tel
603-431-2662 fax

www.foedus.com