

Proven Practice: 20 Questions from IT Security Professionals

Metadata

Title	Proven Practice: 20 Questions from IT Security Professionals
Version	VMware 02/SEP/2008 1.0
Author	 Steve Chambers schambers@vmware.com
Tags	security discussions why_vmwar EAL4 FIPS_140 DISA Gartner competition Citrix Xen Microsoft Windows ESX_Server ACE VirtualCenter
Location	http://viops.vmware.com/home/docs/DOC-1141
Context	<p>During adoption of VMware Infrastructure in enterprise IT organizations where there is a dedicated IT Security team, there will be a point where a discussion is required between the VCP and the IT Security professional.</p> <p>This discussion is a critical success factor of adopting VMware Infrastructure and is common to all organizations, and should be scheduled early the adoption cycle with continuous communication from that point on.</p>

	<p>The IT Security Professional will want to understand the risk profile of virtualization and VMware Infrastructure, and often compare VMware products to competitor products.</p> <p>The outcome of this discussion is normally a set of actions that will lead to an organization's IT Security team accepting and supporting VMware Infrastructure as a technology platform, incorporating it into their operational procedures.</p>
Actors	VMware Certified Professionals, IT Security Professionals
References	<p><u>On VIOPS</u></p> <p>Proven Practice: VI3 Security Risk Assessment from Xtravirt</p> <p>VI3 Hardening Guide and Updates</p> <p><u>External</u></p> <p>DISA Secure Technical Implementation Guide</p> <p>DISA Checklist for ESX Server</p> <p>CIS (Center for Internet Security) Benchmark</p>
Disclaimer	<p>You use this proven practice at your discretion. VMware and the author do not guarantee any results from the use of this proven practice. This proven practice is provided on an as-is basis and is for demonstration purposes only.</p>

How to use this document

This document provides guidance and references for the VCP and IT Security Professional discussion, as used by VMware staff and customers on successful VMware Infrastructure programs.

Ideally, both VCPs and IT Security Professionals should read through this document before their first meeting and use this as an objective discussion point for their organization-specific subject.

This document will be updated as experience from real discussions is added to it. If you discover a useful discussion thread that would improve this document, please add a comment and contact the author.

This document is intended to complement and provide a structured reference to the considerable material available on securing VMware Infrastructure.

20 Questions from IT Security Professionals

Before any discussions between a VMware Certified Professional (VCP) and an IT Security Professional (e.g. CISSP), it is important to clearly state the desired outcomes and constraints on both sides.

A VCP will normally be seeking to have IT Security "blessing" for the solution such that the VMware platform (e.g. VMware Infrastructure 3 in the datacenter) is accepted and supported by the IT Security team: this is usually a pre-requisite to hosting business applications like SAP on VMware Infrastructure.

To achieve this, the IT Security professional will normally follow a standard assessment procedure for the platform, collecting and analyzing information that will enable them to accept or reject the platform, and normally make recommendations on how to make the platform more secure without impacting business agility.

Although the procedure followed by IT professionals may vary (see the references for a risk assessment used by Xtravirt and many people in the industry), the following twenty questions are common:

1. What audits does VMware carry out on its software (independent and internal)?
2. What security framework do the VMware engineers work to?
3. Are VMware products secure by design?
4. Examples of when ESX Server has been compromised?
5. How do ESX Server security features compare to competitor products?

6. Examples of respected industry organizations using ESX Server?
7. What certifications (EAL, FPS) are assigned to which VMware products?
8. What do analysts say about VMware products (like Gartner and Forrester)?
9. What is VMware doing to continuously improve the security of their products?
10. What technology risks should we be concerned with?
11. What operational risks should we be concerned with?
12. How do we securely design ESX Server in our datacenter?
13. How do we securely deploy ESX Server in our datacenter?
14. How do we securely manage ESX Server in our datacenter?
15. What other organizations, similar to ours, are using ESX Server in their datacenter?
16. What compliance standards are applicable to VMware products?
17. Can we use ESX Server in our DMZ?
18. Where can we get help on security from VMware?
19. Where do we get VMware Security Advisories and Alerts from?
20. Where do I send my security questions to?

Each of these questions is discussed in the rest of this document. These questions will be updated and added to during the lifetime of this document, so keep checking for updates (use RSS) and let us know about your experiences so we can improve this document.

1. What audits does VMware carry out on its software?

VMware carries out both internal audits, by its security and engineering teams, and also periodical external audits by a leading security organization.

VMware, like other software companies, acts upon the results of these audits in a timely manner to ensure that its products are as secure as possible. Like other software companies, VMware does not disclose the results of these audits, but should updates be required to released products then a security notice and update will be released via the normal channels.

2. What security framework do the VMware engineers work to?

VMware engineers, such as those coding the the hypervisor, have security practices built in to their coding practices. In addition to automated tools imposing security best practices, engineers have guidelines to follow and review each others' code once checked in. VMware software engineers value security very highly and dedicate a significant amount of focus and effort on ensuring code is secure by design and implementation to reduce the risk of insecure code entering the product line.

3. Are VMware products secure by design?

"Thin" virtualization, found in software such as VMware ESXi 3.5, is the next step in virtualization, dramatically strengthening security and manageability.

- Reduced size makes the attack surface much smaller, and reduces the potential for vulnerabilities
- Independence from a parent partition or console based on a general-purpose OS means far fewer interfaces to exploit and less malware threats, especially important given the path of device drivers from the VM to the physical hardware
- Unstructured, console-based interaction for administration is replaced by authenticated and audited interfaces such as the VI Client and the Remote CLI

See [Security Design of the VI3 Architecture](#)

VMware products have security features at different levels of the product. Here are some examples:

- Virtual Machines running on an ESX Server are truly isolated from each other, they cannot see each others' CPU instructions, memory, network or storage, and they **do not** share a "parent domain" which is a full OS. The hypervisor can enforce more restrictive controls on a VM ethernet network by not allowing it to set its MAC to promiscuous mode, or change the MAC address, or forge the source MAC address. There are other controls on the interaction between a virtual machine and the hypervisor such as the ability to copy data between the guest and the host. Please see the [ESX Server hardening guide](#) for more information.
- The hypervisor in ESX Server is custom designed and written specifically to be a hypervisor - that's why ESXi is only 32MB in size. There is a common misunderstanding in the industry that "ESX Server is Linux based". This misunderstanding arises because the Console Operating System (COS) **is** Linux, but the COS **!=** Hypervisor. The COS is like a special virtual machine that runs **on top of** the hypervisor. It is a customized version of RedHat Linux and it's only purpose is to boot the hardware, pass control to the hypervisor, then provide administration features such as a command line. The COS has already been removed from ESXi. For this reason, the security profile of an ESX Server should be thought of as "COS Security" and "Hypervisor Security". Most of the Security Notices you see related to ESX Server are actually for the RedHat Linux programs in the COS, and due to the customized nature of the COS (e.g. COS does not run BIND) then most of these notices do not apply anyway (but always check

).

VMware advises that because of the administrative nature of the COS that its network port should be on a secure, separate management network (like other management devices) and not on the same network as virtual machines.

ESX Server Architecture

4. Examples of when ESX Server has been compromised?

ESX Server has a very good record of being secure and safe to run your business applications on, but no (serious) software company will ever claim that their products are impossible to hack.

There have been some unproven claims of being able to hack "VMware products" - often, these claims are against hosted (i.e. not ESX Server) products, where the compromise is actually in the host OS (e.g. Windows or Linux) rather than in the VMware software. See [Security Basics](#) for a comparison between Hosted and Bare Metal hypervisors (both are available from VMware, Workstation is an example of Hosted, ESX Server is Bare Metal).

- Read about [Blue Pill] <http://www.vmware.com/vmtn/blog/2006/08/#bluepillpoppers> [
- Chris Hoff, the well known IT Security Professional, [challenged such a claim at a recent industry event.](#)

5. How do ESX Server security features compare to competitor products?

Comparing ESX Server to competitor products is sometimes described as comparing apples-to-oranges because of the difference in implementation, capability, quality, and features.

- On major difference in the design of competitor products is the use of a **parent domain** in Hyper-V and Citrix Xen. Whilst in ESX Server the custom built hypervisor does all the heavy lifting, in these other products a full OS like Windows or Linux is used which significantly increases the security risk profile for all of your virtual machines who have to rely on this big footprint - will it be secured properly? What extraneous programs will be running in it? Who will be able to access it, and what will they do - will the admin **even realise this is a Hyper-V or Citrix Xen host?** This

could be a particular disaster as administrators fail to realise which machine they are on (human error is responsible for 40% of downtime according to Gartner) and make unfortunate changes, such as a reboot? ESX Server is a true virtualization appliance, much like a Cisco router or fabric switch - it has been built to do one thing, and **not** be a general purpose OS. Gartner is concerned that the Hyper-V architecture may cause reliability, vulnerability and maintenance issues because of its dependency on a single copy of Windows Server 2008, and they have stated that the Hyper-V architecture raises stability, vulnerability and maintenance concerns. Check Gartner Report ID:G00154925

- One other important difference is the **use of drivers**. Hyper-V and Citrix Xen claim that a superior feature of their product is that they can use **any driver** available for their host OS (windows or linux) thereby allowing their products to run on many more hardware configurations compared to ESX Server. However, outside of Microsoft and Citrix this is perceived as a weakness because the majority of windows blue-screens are caused by driver failures. The code quality of third-party drivers is much lower than inhouse at Microsoft or Citrix, and they just do not have the resources to certify all of those drivers, so the risk is significant. VMware has a limited, well established hardware and driver certification program that only restricts you to the most well known OEMs and the latest most suitable platforms for high-performance virtualization.
- VMware ESX Server is also **Evaluation Assurance Level 4 (EAL4)** accredited which our competitors do not have. Common Criteria is a public certification that holds great weight with many governments throughout the world.
- <http://www.cse-cst.gc.ca/services/ccs/vmware-e.html>
- We have level two and for ACE, FIPS 140.
<http://www.vmware.com/security/certifications/>
- **Roles and permissions** are very fine-grained in VMware Infrastructure, allowing for secure delegation of control - this isn't available in competitor products. See [Roles and Permissions](#)
- The next exciting addition to the VMware security landscape is **VMsafe** which allows security vendors to do "outside of VM" security operations. This virtual security technology provides fine-grained visibility over virtual machine resources, making it possible to monitor every aspect of the execution of the system and stop previously undetectable viruses, rootkits and malware before they can infect a system. See [VMsafe](#)

6. Examples of respected industry organizations using ESX Server?

VMware products like ESX Server have been used for years by recognized US military organizations, and around the world by all of the Fortune 100 organizations and beyond.

Use this [Case Studies](#) resource to find a reference by organization name (you can change this to find by product, solution and industry if you prefer).

See the [NSA Case Study](#).

[DISA](#) wrote the [STIG](#) for the [US DOD](#), and the US Marine Core at VMworld 08 in Vegas to show their global deployment of ESX Server.

7. What certifications (EAL, FPS) are assigned to which VMware products?

- ESX Server is EAL4 certified. <http://www.cse-cst.gc.ca/services/ccs/vmware-e.html>
- ACE is FIPS 140 certified. <http://www.vmware.com/security/certifications/>

8. What do analysts say about VMware products (like Gartner and Forrester)?

There are huge number of documents from Gartner and Forrester on virtualization, VMware and their competitors - but many of these are only available on a subscription basis and cannot be repeated here. However, there are some common statements from Gartner in the industry -

Gartner says that ESX Server is too expensive, but VMware customers get enormous TCO and ROI benefits from their deployments which makes this claim appear to be a simple comparison of ESX Server to Hyper-V and Citrix Xen on cost - as already stated, this is an apples-to-oranges comparison, but even on cost if you look at the per-VM cost then ESX Server, even ignoring the long list of features it has compared to the limited competition, then the cost is competitive because you can fit significantly more virtual machines on an ESX Server compared to the rest.

Gartner is concerned that the Hyper-V architecture may cause reliability, vulnerability and maintenance issues because of its dependency on a single copy of Windows Server 2008, and they have stated that the Hyper-V architecture raises stability, vulnerability and maintenance concerns. Check Gartner Report ID:G00154925

9. What is VMware doing to continuously improve the security of their products?

In addition to the inclusion of fine-grained security controls, such as roles and permissions, and granular controls on virtual machines such as ethernet controls, VMware is focused on reducing the security footprint and exposure of their products as well as innovating new features with partners.

To reduce the footprint, VMware recently released ESXi which shows that the custom built, "I was born to be a hypervisor" at the heart of ESXi, is only 32MB (compared to the bloated, 2GB+ fully-loaded OS's that act as the all-powerful "parent domain" in Hyper-V and Citrix Xen).

On the innovation front, VMware has worked with partners (e.g. allowing them access to the ESX Server source code as part of the [Community Source program](#)) to develop [VMsafe](#).

10. What technology risks do we have to be concerned with?

Introduction of a new management layer

Virtualization software, like all other infrastructure software, requires the ability to manage the components of the solution. This occurs through a management interface which connect together virtualization hosts, management servers, IP-based storage, and ancillary services such as authentication and monitoring. Since there is isolation between the virtual machines and the hypervisors interfaces, the most important step in securing a virtual deployment is to design and implement a strict separation for the management layer from any other network traffic. This greatest reduces the possibility of any attacks on a virtual machine affecting the virtualization layer or any other virtual machine.

Switches and Servers combined into one device

With VMware Infrastructure, not only can you create multiple VMs on a single host but also virtual networks as well. This is implemented using software layer-2 virtual switches with enterprise-class features such as VLANs and hardware NIC teaming for availability

and performance. Virtual networking provides a tremendous amount of flexibility and cost-savings. You can create a switch with as many ports as you need and you can create a large number of switches. However, there are several aspects of virtual networking that affect security:

- **Lack of intra-server network visibility:** Traditional network-based security tools rely upon access to the traffic traversing physical switches, typically through a hardware appliance. When the switch is virtual, new solutions must be employed that access virtual networking traffic, by running in a virtual appliance for example.
- **No separation-by-default of administration:** In a non-virtual infrastructure at a large enterprise, the server team is distinct from the network team, which might be distinct from the security team. With virtualization, a single administrative interface controls both virtual machines and virtual networks and the separation must be re-introduced through the proper definition of roles and privileges.
- **Elevated risk of misconfiguration:** The fact that it is possible to have more than one virtual switch on a host also represents a significant change. Now, instead of requiring you to physically unplug a network cable from one switch and insert into another, you can change the virtual switch of a VM with a simple drop-down menu. This flexibility of course brings about tremendous efficiencies, but it also elevates the risk of misconfiguration. This must be mitigated through familiar techniques such as strong change controls and meticulous log and event monitoring.

Information Leakage with VMotion

Some reports have claimed that, because it is possible to read information off a virtual machine that is in motion from one host to another, this represents a vulnerability. This misperception arises from ignoring the fact that virtualization inherently involves a management layer which sits underneath the production virtual machines. The most basic security best practices dictate that this management layer operate in a dedicated, isolated environment. Only by violating this fundamental rule would an environment open itself up to this kind of problems.

Learn more about the Security of VMotion

11. What operational risks do we have to be concerned with?

Ease of hardware consolidation

The ability to provision VMs quickly enables unprecedented IT responsiveness. But it also means you might quickly have a proliferation of systems with unknown configurations. This can be a big issue for large environments with hundreds or thousands of VMs. You can avoid this by setting up automated means to:

- Keep track of the configuration of the hosts, VMs, and other VMware Infrastructure objects, such as clusters, resource pools, folders, etc.
- Regularly audit event logs for suspicious or unexpected activity.
- Manage the lifecycle of virtual machines and build in an approval process for better IT governance

Other issues

- **Virtual Machine mobility:** The mobility of VMs provides a tremendous boost to service levels. With VMotion, you can move VMs with greater resource demands to more lightly-loaded server; DRS makes this load balancing automatic. However, most current security approaches assume that a server is located at a fixed location. For example, network-based security appliances that do stateful packet inspection look at traffic on a specific port for a particular server. This model breaks when you have VMs that can migrate across different physical servers, so new solutions must be employed which are compatible with this paradigm.
- **Virtual Machine Encapsulation:** Because a VM is encapsulated in a handful of files, making copies of them becomes quite easy. This enables standardization, and also much easier high availability and disaster recovery. However, many security tools, such as Antivirus and Patch Management, require that the server be up and running in order to push out updates, and hence this method not work for VMs that are turned off but may come online again in the future. New approaches can address this issue, such as offline patching with VMware Update Manager, or in the future, VMsafe-based host protection without any host-based agents.

For a better appreciation of the big picture of deploying and operationalizing VMware Infrastructure in the enterprise, read [Practical Implementation Strategies](#).

12. How do we securely design VMware Infrastructure in our datacenter?

There are well established best practices for designing VMware Infrastructure:

- Separate the COS network from virtual machines - make sure that the COS is connected through a dedicated virtual switch to physical NICs that are connected to a secure management network. This management network should not be available to virtual machines.
- Separate the vMotion network from virtual machines and the management network - make sure that the vMotion virtual switch is dedicated to this feature and is connected to a private, flat LAN that is not routable.
- Use storage security such as LAN zoning to isolate ESX Servers to reduce the visibility of LUNs and the impact of SCSI Bus Resets.
- Design roles and permissions correctly. See [Roles and Permissions](#).

OTHERS TO ADD

REFERENCES

13. How do we securely deploy ESX Server in our datacenter?

- Follow the [ESX 3.5 Hardening Guide](#)
- Deploy security notices to be displayed on all VMware products (VirtualCenter and ESX Server) such as "Message of the Day" banners.

OTHERS TO ADD

REFERENCES

14. How do we securely manage ESX Server in our datacenter?

- Send logs remotely to a syslog server
- Monitor ESX Server and ensure the alerts are (a) tested regularly, and (b) have incident management procedures assigned
- Use tools such as ConfigCheck from Tripwire to monitor configurations
- Enforce strict change control windows on Virtual Machines, VirtualCenter and ESX Servers. Any changes outside the window should be investigate and acted upon. Change windows should be changed to reflect new features such as zero-downtime maintenance with vMotion.
- Only deploy virtual machines from certified templates or via certified automated releases, do not allow uncontrolled deployment and configuration of virtual machines or hosts.

OTHERS TO ADD

REFERENCES

15. What other organizations, similar to ours, are using ESX Server in their datacenter?

Use this [Case Studies](#) resource to find a reference by name, product, solution or industry.

16. What compliance standards are applicable to VMware products?

VMware Infrastructure is used in environments where Payment Card Industry (PCI) and other compliance standards apply.

[Using VMware VDI and vmSight for Stronger and Sustainable HIPAA and PCI Compliance](#)

LATEST REFERENCES FROM CHARU'S WORK

17. Can we use ESX Server in our DMZ?

Absolutely. The [Choosing a DMZ Strategy](#) document explains your options.

[Chris Hoff](#) makes a great DMZ design point - [should you share storage between DMZ and non-DMZ?](#) - something often overlooked in the design stage. Although your virtual machines, if using virtual disks and not physical RDMs, will be using virtual disks (VMDKs) via the hypervisor and therefore have only limited read/write access so the risk footprint is small, you should check out your virtual machine configurations, your storage configurations and those of your fabric and arrays to ensure the best practices for LUN zoning and masking are in effect and that the networks are sufficiently isolated and protected.

18. Where can we get help on security from VMware?

VMware have provided an online [Security Center](#).

Check out the [VMware Knowledge Base](#) where you can search for "security" and other topics.

Read the [VMware Security Blog](#).

Subscribe to the [VMware Security Feed](#).

Security services are also available from [VMware Professional Services Organization](#).
Speak with your local VMware representative to find out more.

19. Where do we get Security Advisories from?

To get automatic notifications of new security articles from VMware, please subscribe to the Security Alert channel on [VMware's RSS feed](#). Whenever a new security article is published, VMware will announce it on the security channel.

The following pages are maintained by the VMware Security Team:

- Read [Security Advisories](#).
- Read [Security Alerts](#).

20. Where do I send my security questions to?

Post questions in the VIOPS [Security zone](#) , or send an email to security@vmware.com .