

Auditing a Virtual Environment

Risk and Control Considerations

Phil Culleton – Director, Barclays Internal Audit

Chris Avent – Associate Director, Barclays Internal
Audit

Purpose and Agenda

PURPOSE

To provide you with an overview of virtualisation, the risks and some recommendations on how to audit it.

AGENDA

1. What is virtualisation?
2. Why should I worry?
3. How do I audit virtualised environments?
4. Q & A

What is Virtualisation?

Virtualisation allows you to run more than one operating system simultaneously and independently on the same hardware. Hardware resources are dynamically allocated to achieve optimal performance.

Stalled operating systems are automatically restarted. Where hardware is in a High Availability cluster, all workloads on failed hardware can be automatically restarted within the cluster.

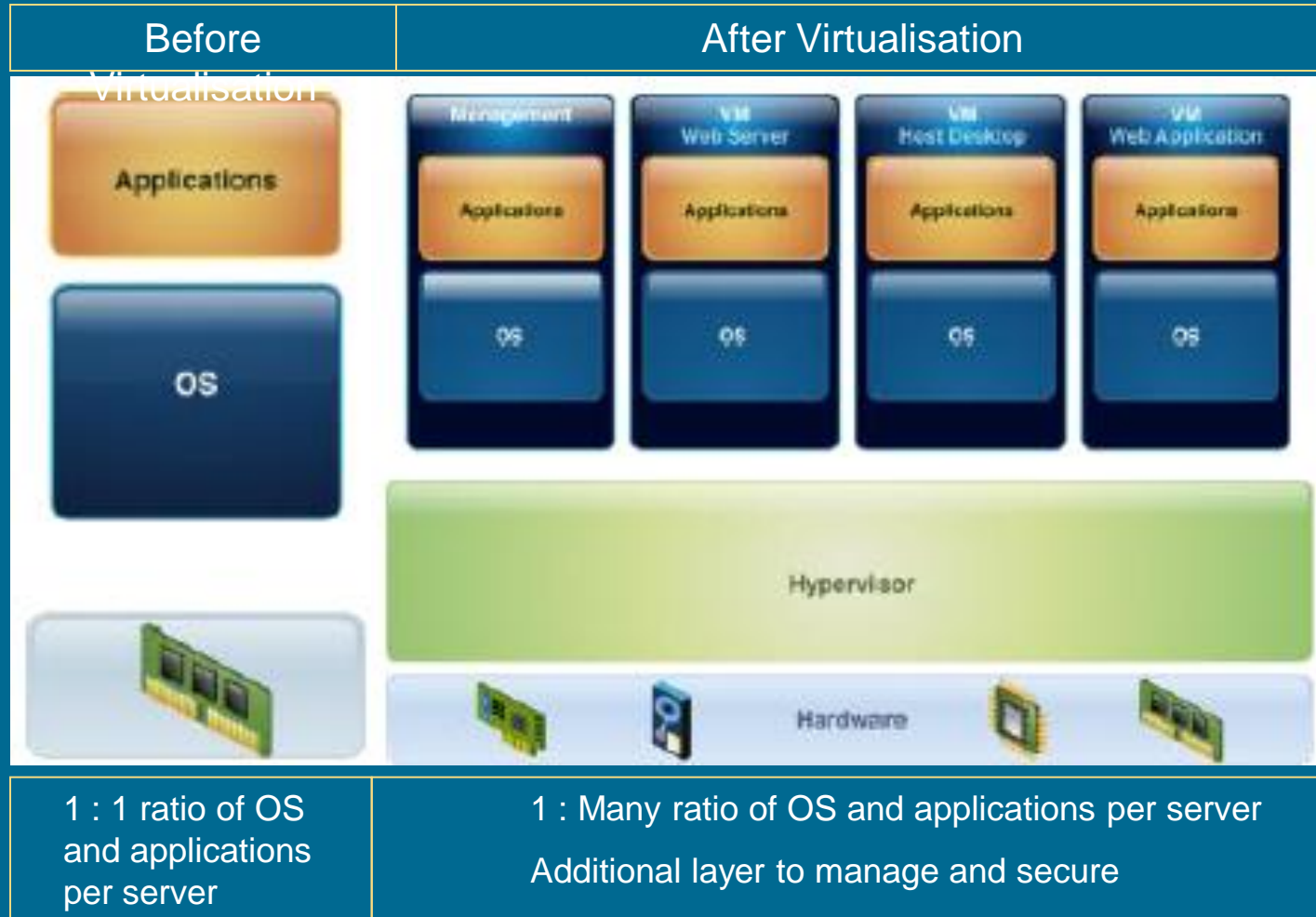
Some key drivers for virtualisation are:

1. Reduced time to market
2. Improved service uptime
3. Improved performance management
4. Ability to support legacy operating systems and applications
5. Reduced support and energy costs
6. Reduced data centre space requirements

New Complexities and Security Challenges

New Complexities:

- Dynamic relocation of VMs
- Increased infrastructure layers to manage and protect
- Multiple operating systems and applications per server
- Elimination of physical boundaries between systems
- Manually tracking software and configurations of VMs



Virtualisation Terms and Concepts

- **Virtual Machine (VM):** An isolated guest operating system instance
- **Host:** Physical machine where the VMs run
- **Hypervisor:** software installed on the host which presents a virtual operating platform to guest operating systems and manages their execution
- In familiar terms, a virtual machine is a folder containing configuration files and large virtual disk files. These folders, just like regular directories, can be copied, moved or deleted. RAM and processor access are values in a configuration file.
- Unlike multi-tasking, which also allows applications to share hardware resources, the virtual machine approach using a hypervisor isolates failures in one operating system from other operating systems sharing the hardware.

Key Risks of Virtual Environments

- **Misconfigured Hosts:** The host should be configured to remove default vulnerabilities; any configuration issue will be magnified across all the Virtual Machines on that host. Hosts can be appliances or blade systems with an underlying commercial operating system.
- **Access Controls:** Host administrators have full rights over the host infrastructure, including the ability to copy VM memory – virtualised Domain Controllers pose a particularly high risk.
- **Single Point of Failure:** A host failure could bring down a set of key applications; this magnifies the effect of any failure. The need for adequate recovery strategies is a key area to consider.

Key Risks of Virtual Environments

- **Rogue Virtual Machines ('sprawl')**: Large numbers of unauthorised VMs can be quickly deployed. Over time these pose a risk to the environment as they may not be securely configured or patched. Licensing issues may also arise.
- **Internal Skills**: Host administrators are required to define and maintain underlying parameters for both the network and operating systems
- **Network Segmentation**: Production and management traffic using the same segment coupled with weak root access control could enable an internal attacker to gain administrative privileges.

How do I audit virtualisation?

Risk Area	Consideration
Asset Management	Creation/destruction of VMs
Secure Build & Hardening	Gold copy for new hosts and guest O/Ss
Virtual Networks	Access controls using the virtual network
Segregation of Applications	How many key applications run on the same host; avoid mixing confidentiality needs
Change Management	Changes tested before being applied
Privileged Access	Adequate privileged access controls in place
Capacity Management	Each VM has pre-allocated resources and is prevented from impacting other VMs

Additional Areas to Consider

- Virtualisation needs a dedicated work programme (can be added to platform audits but will require time for specific testing)
- The audit team needs specific training on virtualisation technologies
- There are some commercial tools that can be used to test the configuration of the hosts (hypervisors). Also possible to script GET commands using PowerShell.
- The audit team should consider the risk created by combining different criticality VMs into a single Host (confidentiality, integrity and availability)

Security Techniques & Controls

- Misconfigured Hosts:
 1. Documented build standards for the hosts
 2. Approved deployment scripts to implement the build standards consistently
 3. Compliance monitoring

Security Techniques & Controls

- **Access Controls:**

1. Roles in management tool (e.g. VMware's vCenter) assigned to inappropriate users
2. Weak password controls for host root access could lead to privilege elevation
 - Access should be accountable, logged and high risk activities monitored, e.g. copying of domain controller VMs
 - Typically the roles of host administrator and guest administrator should be segregated

- **Single Point of Failure** – ensure High Availability is correctly configured; this can reduce the impact of many other virtualisation specific risks

Security Techniques & Controls

- **Rogue (Sprawl), Possibly Misconfigured Guests:**

1. A mature, documented, change control policy and process with authorisation, testing, communication and roll-back requirements for every guest creation, change, removal, or relocation
2. A mature, documented asset inventory process with accurate recording integrated with the change management process
3. Periodic independent assessment of the authorised asset inventory of guest deployments to the actual deployments in the organisation
4. Include authorised (gold image) and dormant guests in patch, anti-virus, configuration monitoring and other security processes

Security Techniques & Controls

- **Internal Skills** - if the networking capabilities enabled by the hypervisor are in the hands of staff untrained in networking concepts or, conversely, if the networking team is given administrator rights on the host, those privileges may be outside their expertise... specific training is required.

Security Techniques & Controls

- **Network Segmentation:**

- Segregate production and management traffic on separate network segments
- Restrict access to workload migration traffic (e.g. VMware's vMotion) as the traffic is unencrypted by default
- Leave default vSwitch promiscuous mode in default "Reject" mode
- Install redundant Network Interface Cards for continuity

Questions