

# Why automated tools are required to audit virtual infrastructure

---

## Enabling virtualization

VM Informer provides an efficient and affordable mechanism to audit virtualized infrastructure. Unlike traditional audit tools, VM Informer is built purely for virtualization, it is agentless so no additional software is required and critically the output is relevant to the virtualization target.

VM Informer will immediately provide complete visibility of configuration settings against a variety of regulatory, industry security standards, or specific corporate requirement.

This assurance means you can expand your virtualization deployments with confidence.

### Policy templates

A sample of standard policy templates follows:

ESX hardening guides;  
ISO27001;  
PCI-DSS;  
DISA-STIG

This briefing note might have been titled *“What do you really know about your virtualization infrastructure?”* Most informed people would acknowledge that there are a lot of unknowns. As famously quoted, and paraphrased here, there are known knowns, known unknowns, and unknown unknowns; this is particularly true with respect to virtual infrastructure. The next few pages should provide some insight into how you can make known some of your unknowns, perhaps even the unknown unknowns.

Virtualization provides organizations with savings in computing processing and administration costs. Consequentially, most organizations have embraced virtualization as a technology to reduce their expenditure on IT. Despite the rapid uptake the full capacity of this technology has yet to be realised. Concerns around security, configuration and control restrain many organizations from achieving greater savings and particularly the purchase of on-demand (cloud) services for production computing.

You can only make good decisions with good information. This document is intended to explain how that visibility is provided by auditing virtual infrastructure. This will enable you to increase your virtualized deployment and consequently reap greater savings.

### What are the issues?

Firstly it must be stated that from a security or configuration perspective, a virtual machine is no less secure or difficult to configure than a physical device. The difference is that it is very easy, and quick, to make changes (small discreet variations or wholesale changes can be done with the same ease). Furthermore any virtualization administrator can make changes without reference to their colleagues in the infrastructure, network and provisioning teams, this is a tremendous benefit from the perspective of rapid provisioning - but it is also a weakness. Duties are not segregated in a virtualized environment – this is a very important issue and a common theme in this document.

At any point in time it is almost universally true, from the smallest business to the largest corporate enterprise, for cloud and hosting providers, that the full status of their virtualized infrastructure is unknown.

Despite the wide deployment of virtualization, many operators do not understand the hundreds of configurations settings that are available them.

Typically, deployments are delivered by systems integrators who take advantage of the easy setup mechanisms and default settings that allow rapid installation of virtual infrastructure. There are hundreds, often thousands, of settings that should be checked even in the smallest virtual environment. However, the volume of checks so large, and typically the initial deployments were so far within the corporate network, that detailed configuration checks were ignored or overlooked. As virtualized deployment moves from development to production systems, especially onto the DMZ of firewall segment the providence of each virtual machine and its host configuration becomes ever more important.

“Complete manual checking is so time consuming makes it prohibitively expensive”

Complete manual checking is so time consuming makes it prohibitively expensive. Stopping to thoroughly review configuration settings is not an option for IT departments under pressure to deliver production computing.

### Hundreds and thousands of security settings

There are in total about 200 settings to check the security of a vmware host, and about 30 settings per guest virtual machine. Even for a small business that operates, say ten ESX servers and 160 virtual machines, there are technically about 5,800 checks. The bad news is that some of these individual checks have multiple subsidiary checks (you could double the total quantity of checks required!).

Some will argue that many of these checks are unnecessary for a small business with a low risk profile. VMInformer contends that as a minimum 1/6th, or about 1000 checks, are required to provide basic assurance for an infrastructure of this size. What is obvious, even at this early stage, is that this is a process that should be automated.

### Checking configurations is not easy

Configuration settings need to be checked in the configuration file of each element of the virtualized infrastructure. These settings are written into the scripts that control the elements of the hypervisor, or its administration console. This is best described with a vmware example.

An element, of arguably medium risk, is the implementation of password policy. One part of this would be to determine if the global password settings are configured correctly. This is checked in vmware's ESX server's login.defs file. [This file is written to by ESX when the esxcfg-auth command is invoked to make changes to password policy. The ESX hardening guide recommends password changes every 90 days or less.] So you need to read the settings in the file, then login to the service console via ssh and run this command to remediate 'esxcfg-auth --passmaxdays=90' (or replace '90' with whatever is defined by your password policy).

If you are diligent you will go back and check your command was correctly registered. Human error rate is 1-2%. If you know the command structure in a thousand checks you might expect a minimum 10 oversights. You would expect a much higher error rate if a specialist is not employed to the task. Generally, the commands are not easy to implement. They are case sensitive; typically utilize double negatives in the syntax which makes checking a very precise and complex activity. At all times specialist skills are required. If you have these skills in house, you rarely want them deployed on something as mundane as checking configurations. If you do have the skills in-house you should, for obvious reasons, ensure that the person checking the settings is separate from daily operations to provide an impartial audit.

```
[root@esx41fulltesthost etc]# esxcfg-auth --passmaxdays=90
[root@esx41fulltesthost etc]# more login.defs
# Autogenerated by esxcfg-auth

CREATE_HOME      yes
GID_MAX          60000
GID_MIN          500
MAIL_DIR         /var/spool/mail
MDS_CRYPT_ENAB  yes
PASS_MAX_DAYS    90
PASS_MIN_DAYS    0
PASS_MIN_LEN     5
PASS_WARN_AGE   7
UID_MAX          60000
UID_MIN          500
UMASK            077
USERGROUPS_ENAB yes
[root@esx41fulltesthost etc]#
```

### Do you need to worry about security of virtual infrastructure if it is firewalled, virus protected?

Many of the security controls that are put in place in a virtual infrastructure are based on replicating the security deployment on physical servers. Most organizations have experienced an increased spend on security as more 'cheaper servers' are deployed within virtualized infrastructure. The default position (again due to the lack of visibility within the virtualized infrastructure) is to isolate each VM within a firewalled zone, the firewall in most cases being external to the virtual infrastructure. Sadly, despite this additional expense and inefficiency of design, it is very easy to bypass these controls by misconfiguring a setting in a virtual machine or its host. (This is particularly relevant if you are considering hosted, or cloud services, for any valuable computing work because you will be reliant on the controls and processes of the hosting provider).

Again, the lack of segregation of duties within a virtual environment is even more problematic, because all administrators of the virtual environment<sup>1</sup> must have the requisite networking and systems skills to recognize a security breach or configuration flaw. Of course the compounding factor is, how could anyone else pick up a misconfiguration when the console is populated with hundreds of elements? Once again, you cannot afford to audit because it is too time consuming, and even if it was perfectly configured at installation time.

### Risk analysis, worldwide standards and practical use

Risk profile and activity varies within organizations and across industry sectors and parts thereof. Risk has to be analyzed in context. For example, VMs connected to a DMZ network segment have to be hardened in a different manner to those on the intranet. Those holding customer data with credit card records have to be analyzed differently to those holding CRM records. It should be as easy when using an automated tool, to check against PCI-DSS requirements or ISO27001, or whether a specific setting - like build numbers are consistent. Configuration rules should be open, which means that users, and their auditors, can interpret existing policy templates, or tailor their own specialized checks. This allows you to tailor your checks to your needs or industry specific practice.

---

<sup>1</sup> It is worth checking who has access to administer your virtual infrastructure. It should be a distinct virtualization administrator group

### Visibility vs. frequency of auditing

You might be required to audit your IT infrastructure once a year, maybe twice. This frequency might be sufficient in a well-run physical IT environment. However, in a virtual environment with faster provisioning, but also with less visibility, less segregation of duties the frequency must be much greater. The good news is that the virtual environment lends itself to more frequent configuration checks. Tools to do these checks are inexpensive compared to their physical counterparts. To provide assurance, you should run tools like VMInformer, on the following rotations or requirements:

- On the initial deployment, followed by remediation (there are always surprises when a full audit completed); then:
- Develop your own audit policy for each trust zone;
- Depending on your risk profile audit, daily, weekly, monthly and remediate as required;
- Depending on regulatory, or statutory requirements, run tests against these requirements; and
- When changes to configurations are made, or build templates are changed, then audits should be re-run.

This might sound like a lot of work, but these checks if run automatically will be completed in about ten thousand times faster than a manual check. They can be run in the background and are very quick. VMInformer, for example, will check about 200 virtual machines, and the underlining infrastructure against three or four policies in about ten (10) minutes.

### Conclusion

Operators of virtualized infrastructure need visibility over their estate to make correct decisions. Thousands of information points need to be checked. This cannot be done accurately and affordably using manual process. You need an automated tool that is designed for virtualization to audit virtualized infrastructure (ones that audit the virtualized infrastructure as if they are physical servers will produce misleading results). It is also important that the exceptions and aggregated information is presented in a meaningful way.

Tools, like VMInformer, exist to audit virtual infrastructure quickly. These tools should allow you to tailor your checks to your own standards; network configuration; firewall zones; and relevant regulatory requirements. Basic checks against your standards should be run constantly. This will allow you to monitor for anything that may affect your security disposition, but also for changes that could degrade performance. You should check configuration changes when made are correctly applied. Finally, when templates are updated all machines should be reviewed irrespective of their power state.

Asia Pacific  
Suite 504, 75 Miller Street, North Sydney  
NSW, Australia T:+61 (0)2 8004 5422

Distributed by:  
C&RRUS Management Solutions Ltd  
Milton Park Innovation Centre, 99 Milton Park  
Abingdon, Oxfordshire. OX14 4RY  
Tel: +44(0)1235 854048  
Email: sales@cirrus-ms.co.uk  
Web: www.cirrus-ms.com