Article published on November 28th 2011 | Internet

A few years back in history, organizations were worrying that their virtual machines will have management issues, problems in its performance, security and also its staff. That was because of VM sprawl. Now another problem is haunting them and it is the VM stall.

VM stall has the tendency of putting the converted non-production type low-risk systems to a standstill. The virtualization projects that organizations keep localized or confined in certain areas of the physical network will hit a wall; a wall that they would hit every time they decide to secure each thing they need. At start experts would conduct security tests and pen testing to know what this wall is all about and what could have been done to avoid it. They have found out that this virtual wall could have been avoided if they have deployedvirtualization securities that have the ability to enable dynamic virtualized networks without compromising the security.

VM stall is indeed a problem, but there are available solutions nowadays that can be used in surmounting that wall and erase the fears an worries of losing control on the system or degrading its performance. Continuing the phases in virtualization of an organization will lead to a faster server provisioning as well as management.

It is a stated fact that companies are hesitant when they allow non-administrators or non-pros to conduct certain testing on their systems such as pen test; much more if they allow them to maintain their VMs. There are chances that these systems will be misconfigured or not maintained properly and it could lead to open vulnerabilities to the system.

Solutions that are used implementing VM will enforce other technology that exists today. Furthermore, these solutions will allow organization to mix workloads, turn on the VMotion as well as get better ratios in VM-to-host compressions without the added risk on the VM security. Virtualization-specific security also helps overcome the wall of VM stall and at the same time it mitigates ROI's arguments.

The practical example of virtualization-specific security's impact on the ROI is this. If a certain customer has 3 VM hosts as well as 30 VMs; 10 VMs are used for various applications of thehost business while the 20 are for 2nd tiered VMs. If we assume that the max capacity of each of the host is only 20 VMs, the customer shall protect as well as limit the access to the critical VM by using VLANs. For instance, 5 VMs is allotted to 1st host, 5 VMs allotted to the 2nd host and 20 VMs to the 3rd host. Since the 3rd host is maxed out, the customer will need to add additional non-critical VMs, deploy additional hosts since the 1st and 2nd hosts are isolated even if they aren't maxed out. The logic behind this is that it is possible to achieve security without mixing the workloads and physically isolating the critical VMs to any VLN. However, this happens at the expense of the ROI â€“ thus there is a stall.

A 2nd example is a customer who used granular security in each VM, the customer can mix the workloads; obtain departmental isolation as well as security without reducing the host's VMs. Thus the customer can load 10 VMs in every host as well as have headroom for the additional 30 VMs that are spread throughout the existing host. That is the power of servervirtualization-specific security and ROI.

Virtualization security helps the security and the ROI concerns which related to the reticence of the

deployment. It is important that the security packages have been evaluated and that they have the needed features to provide granular isolation as well as have the required automated security.

There are some few things needed to consider when searching for the solution. It must have layered defenses like firewalls, AV software, IDS and penetration testing tool kits. It must have vCenter integration to make the solution for the security aware in the changes of the network. VM Introspection that provides X-ray view to know what is installed in each VM. It also must have compliance enforcement to alert or quarantine the VMs that have failed the compliance checks. An auto-VM security that is used for brand new VMs is needed to automatically apply the security policy that is given for each VM type. Finally, VM image enforcement is needed to monitor each of the VM images for the compliance of the right configuration.

Article Source:
http://www.articleside.com/internet-articles/virtualization-specific-security-the-elixir-of-vm-stall.htm - Article Side

Eccuni - About Author:
The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in penetration testing.

More information about EC-Council is available at www.eccouncil.org, a pen testing, a pen test, a penetration testing

Article Keywords:
Virtualization, pen test, penetration testing, pen testing, Elixir, VM Stall, VM sprawl, physical network, security tests, virtualized networks, VM-to-host, VM security, VLN, ROI, automated security, AV software, IDS, E-Commerce