THE 5 DOS AND DON'TS OF NETWORK VIRTUALIZATION

With increasing pressures on today's IT professionals to minimize resources, but still maintain a high-performing infrastructure, virtualization has become a go-to option for a low-cost, power-saving solution. In fact, CIO Insight recently reported that 70% of senior executives said virtualization had a significant impact on efficiency and cost savings for their organization. However, deciding what within your network infrastructure to virtualize, and how to actually do it, can be a challenge.

Here are **five dos and don’ts** to consider when virtualizing your systems.

01 **Do plan your virtualization based on the facts –** Before you start your virtualization project, evaluate your various applications‘ resource usage. Virtualizing systems without knowing their standard CPU/memory load, disk usage and network usage can lead to poor network performance and wasted resources. You want to ensure there are not too many virtual machines running on a single host, resulting in poor performance, or too few virtual machines running on a host which could result in wasted resources spent on unnecessary host servers.

02 **Don’t think of virtualization as one-size-fits-all –** Sure virtualization can be a cost-saver, but not all of your applications are good candidates for a virtual environment. For example, applications with heavy compute or data read/write loads are not good candidates for hypervisor virtualization. In order to identify which of your applications should remain on dedicated servers, and which can be moved to virtualized servers, you need to look at volume and character of transmissions to and from each of your applications.

03 **Do know your network’s status –** A highly virtualized environment lives or dies on the efficiency and dependability of its data network. Issues with your virtual machines (VMs) can originate from a host hardware failure or an issue with the operating systems. Set up sensors to monitor your VM host servers and operating systems to alert you when the status of either is not “normal,” so that you can minimize the impact of issues – like the failure of a Windows server – before they become critical to network and application availability.

04 **Don’t fail to establish a baseline for traffic patterns –** Virtualized environments cannot tolerate network overloads or switch failures. Ongoing, comprehensive traffic analysis will provide long-term usage projections and help you anticipate traffic increases and the need to enhance resources before they impact service levels.

05 **Do include your VMs in your unified monitoring practice –** Once you’ve moved your applications to virtual servers, you need to expand your overall network monitoring beyond physical devices to the virtual machines and the services and applications that are on those. Proactively monitor the performance of your virtualized infrastructure as part of a unified view of your workloads across both your physical and virtual tiers including applications, storage, operating systems, network, etc.

Unified monitoring to the rescue!

A unified monitoring solution is an essential part of a highly functioning, virtualized IT infrastructure and provides your IT department with a clear view of all network activities. Find out how Paessler’s PRTG Network Monitoring can support your virtualized environment by downloading a FREE TRIAL HERE.

PAESSLER PRTG NETWORK MONITOR

www.paessler.com