Virtualization Best Practices
Jesus Vigo, Network Infrastructure District Technician, Miami-Dade County Public Schools

CEU-approved for A+, Network+, Security+, Cloud+, CSA+ and CASP
Agenda

• What is virtualization?

• Virtualizing server infrastructure: reality vs perception
  – Hardware requirements
  – Application limitations
  – Performance & uptime

• Managing expectations: concept vs execution
  – Isn’t it just cramming a few servers into one big one and calling it a day?
  – More like Wi-Fi or BYOD initiatives - only worse

• 4 takeaways to virtualization nirvana
  – Plan, plan, and plan some more...Did I mention how important it is to plan?
  – Configure your virtual machines accordingly, then continue tweaking them
  – Manage your host servers and guest OSes by monitoring them constantly
  – Security (physical, logical, and data) is the most important piece of the puzzle
What is Virtualization?

• Creating a version of something which logically divides the system resources from the software, simulating the hardware so that the operating system and applications may run unmodified.

• While multiple types of virtualization exist, the most common type found supported by modern hypervisors is hardware-assisted virtualization.

• By utilizing the processor extensions found in more recent CPUs from Intel and AMD (post-2006), calls made from the virtual machines (VM) to the underlying hardware are more efficiently performed through the hypervisor, allowing for better cooperation between the hardware and software. This greatly alleviates performance overhead that occurs when using CPUs that do not fully support VT-x/AMD-V.
Virtualizing Server Infrastructure: Reality vs Perception

• Hardware specifications for existing physical servers do not apply on a 1:1 ratio (most of the time) for their virtualized instances to run properly.

• Application limitations - including requirements - play a big role in how well it will function as a VM. Just because an app can be virtualized does not mean it should be.

• VM performance and service uptime will vary widely between organizations for any number of reasons, but will depend mostly on the physical-to-virtual (P2V) conversion process, the resources allocated to the virtualized instances, and ongoing monitoring & optimization.
Managing Expectations: Concept vs Execution

• Communication is the key that will enable stakeholders to get on the same page in understanding the ups and downs to virtualizing assets.

• The line between how virtualization is conceptualized by different stakeholders and what it will take to implement it, and how it will work going forward are often blurred by misguided expectations.

• The aim - with regards to stakeholders is simple: Avoid unexpected surprises that could otherwise delay the project, or experience extended periods of downtime without a plan to fall back on.
Isn’t it just cramming a few servers into one big one and calling it a day?

• In a word: No. Not if you want your virtualization project to fail miserably before it can even start. Planning is the order of the day.

• Procuring a server powerful enough to support your needs isn’t a matter of buying the most expensive one you can afford. Other dependencies include the needs of your organization, the server roles of the VMs...

• And optimizing the resources allocated. This does not occur “automagically,” but as a direct result of continuous monitoring and management by IT.

• Virtualizing a server does not shield it from attacks nor protect data in a cocoon. It just introduced another vector for security-related concerns.
More like Wi-Fi or BYOD Initiatives – Only Worse

• (Concept) Users were used to open networks, or hot spots, which allowed them to just connect and go online. No security or limitations.

• (Execution) Wi-Fi had IT scrambling to not only procure access points to provide wireless Internet access, but also to obtain the hardware and software necessary to manage networks securely and efficiently.

• (Concept) BYOD users jumped at the chance to bring their personal devices to work instead of using obsolete hardware or equipment they were less familiar with at work.

• (Execution) IT begrudgingly caved-in and allowed non-managed devices on company networks, but access is subject to the same standards and limitations as company-owned devices to keep managed assets protected.
4 Takeaways to Virtualization Nirvana

• Plan, plan, and plan some more...Did I mention how important it is to plan?

• Configure your virtual machines accordingly, then continue tweaking them.

• Manage your host servers and guest operating systems by monitoring them constantly.

• Security (physical, logical, and data) is the most important piece of the puzzle.
Planning

- Baseline physical servers to gain an idea of the resource usage per system (peak/off-peak) prior to being virtualized.
- Perform capacity planning to determine how many virtual instances a host can support, based on the requirements of the physical servers to be virtualized.
- Make determinations based on baselines, trend reports, and application-specific requirements as to whether or not a system is a good candidate for virtualization.
- Expenditures associated with virtualization aren’t limited to new hardware purchases. Add-ons from licensing to maintenance contracts to training will hike costs.
Configuration

- “Right-size” your VM instances so as to not over allocate (or under commit) resources to your hosted systems.
- Evaluate and understand the various server roles and their unique requirements when configuring VMs. Consult vendor white-papers for guidance.
- Physical-to-virtual (P2V), or captured servers may contain data, applications, and/or hardware profiles that can be detrimental to the stability of the VM.
- Virtual-to-virtual (V2V), or VMs converted from one type of virtual machine to another, may require reconfiguration when powering on the existing VM on a new host.
Management

• Whether managing 1 or 100 VMs - management consoles are required to setup, configure, and troubleshoot issues.

• Ongoing optimization for virtualized systems is a task that should be constantly monitored in order to achieve an optimal consolidation ratio.

• Keeping up-to-date with software patches to the hypervisor, guest operating systems, and the software run by these systems is just as imperative on virtualized systems as it is on physical servers.

• Don’t forget to manage yourself by keeping your skill sets updated by learning the nuances of virtual infrastructure management.
• Don’t skimp on the physical or technical security of the host - or it’s VMs. It’s just as important to virtualized systems as traditional physical servers.

• Adhere to all security principles and best practices for servers. This goes hand in glove with host-based security implementations specific to virtualized environments.

• Implement (and test) Disaster Recovery Plans (DRP). Virtualized systems are subject to the same data loss and compromises as their non-virtual counterparts - with some virtual-only attacks mixed in for fun.

• Apply network security standards to the virtual switches that connect VMs to the physical network to prevent unauthorized access and protect data.
Questions?
Thank you!