Realtime
publishers

Maximizing Your Desktop and Application Virtualization Implementation

The Essentials Series

sponsored by

vmware®

David Davis

Desktop and Application Virtualization Management Best Practices 1

Image Management Best Practices 1

Desktop and Application Virtualization in BYOD and Physical Environments 3

Managing and Monitoring Your Environment 3

Desktop Provisioning Considerations 5

Summary 5

Copyright Statement

Desktop and Application Virtualization Management Best Practices

The delivery, management, and automation of virtual desktop infrastructure (VDI) can be challenging if the implementation is not well planned and maintained.

Desktop virtualization administrators should be prepared to answer the following critical questions as they plan out a desktop implementation.

- How will the operating system (OS) images be managed in the environment?
- How will the OS be patched and upgraded when needed?
- Where will applications be stored, how will they be upgraded, how will they be entitled, and how will they be delivered to end users? What about end user customizations/profiles/personas?
- How will customizations/profiles/personas from the OS image and applications be separated to ensure that these three distinct pillars of an end user VDI virtual machine (VM) image are siloed?
- How will performance and capacity be managed?
- How will you troubleshoot VDI when problems occur?
- How will you automate the environment to run smoothly and efficiently?

Let's look at best practices in these areas to help you answer these critical questions.

Image Management Best Practices

As part of desktop virtualization delivery, you will need to know what VDI solution you will use, what the end user devices will be, what remoting protocol you will employ to deliver the end user experience, and how you will manage the virtual desktop images that you plan to deliver to your end users.

As mentioned earlier, the three distinct pillars of an end user VDI VM image are:

- OS
- Applications
- End user personas

Taking these one at a time, the OS challenge is usually met with desktop virtualization. To save disk space, a golden image is created and then cloned. Those clones are linked back to the main image such that only the changes from the golden image require disk space. In most cases, the OS is also separate from the applications and end user personas (profiles) so that the OS can be updated as needed without affecting the applications or end user data.

The application challenge is handled in a variety of ways, as discussed in the first article. You might install applications inside the VDI image or you might insert links to virtualized versions of your applications (which can be updated independently), you might use an application distribution technology, or you could leverage hosted applications.

Finally, end user profiles/personas could be simply stored on a file share or stored separately using your VDI product. Although most VDI products include some form of persona management, many customers choose to leverage a more advanced third-party end user persona management application. No matter what you use, the end result is the same: end user personas are kept separately and can be applied to whatever OS or device to which the end user connects (see Figure 2.1).

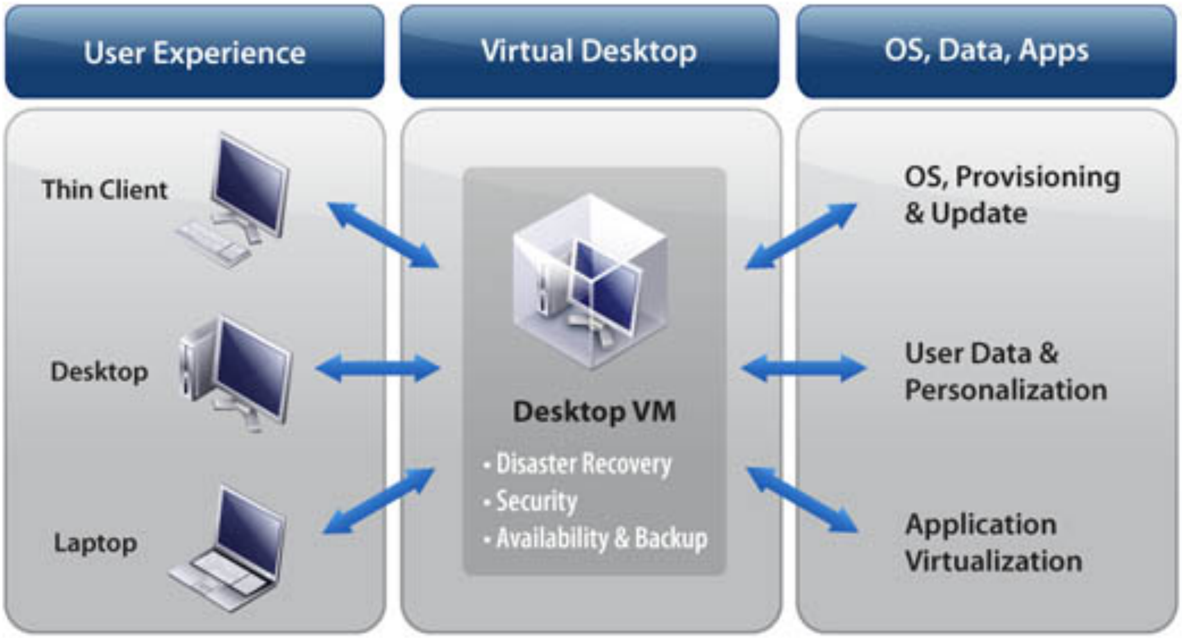


Figure 2.1: Separation of OS, applications, and personas.

By separating these three components of the end user VM image with VDI, you can upgrade the OS or applications at any time, without affecting end user personalization, performance, or end user productivity. VDI solutions that allow you to silo the OS, applications, and personas for easy patching and updates are the ideal solution for enterprises of all sizes.

Desktop and Application Virtualization in BYOD and Physical Environments

More and more companies are moving to a policy where end users are allowed to bring their own device. The Bring Your Own Device (BYOD) policy takes a huge burden off IT to purchase, support, and troubleshoot a variety of devices. However, it also introduces issues, the main concern being security. If BYOD end users were able to access the company's network, applications, and data from their own device and if that device had a virus or contained malware, the virus could spread and/or the malware could access the company data. The way around this challenge is to keep BYOD devices in a secure DMZ (that is, off the relatively unprotected company network) and allow them to access only a VDI desktop or simply the specific the set of applications they need.

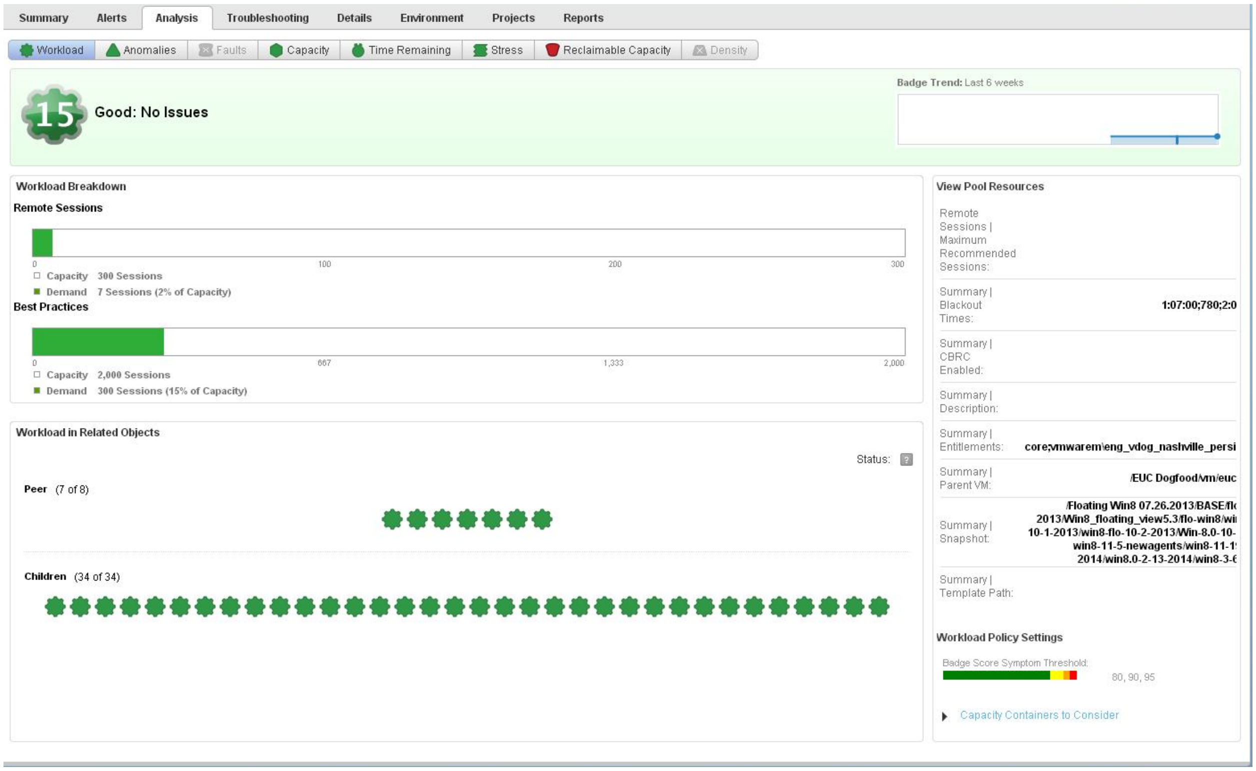
When the VDI OS, applications, and personas are siloed, the virtualized or remote applications can be delivered independently of the OS to BYOD end users. This solution is optimal for keeping the BYOD OSs from accessing the corporate network.

Many companies still have and will continue to have physical desktops or laptops because they have remote or mobile users that don't have full-time network access. As a result, these users have their own local OS image, applications, and personas. However, IT still needs to keep those physical machines up to date. Ideally you could keep them up to date with the same siloed OS image, application images, and end user personas employed in your VDI environment. The latest end user computing solutions are making this possible, providing many of the benefits of VDI to physical devices. When combined with a virtual desktop container on the endpoint, these next-generation image management solutions can also be applied to a BYOD environment with encryption, expiration, and locked down policy controls.

Managing and Monitoring Your Environment

Although virtualization administrators might be used to managing performance and capacity in virtual server environments, undertaking performance and capacity management in VDI environments is a very different task. VDI has different resource utilization characteristics, such as much heavier storage I/O utilization and very unpredictable storage I/O patterns.

Thus, desktop virtualization administrators need performance and capacity tools that are designed specifically for desktop and application virtualization environments (see Figure 2.2) Additionally, you don't want performance and capacity tools that provide only statistics such as Input/Output Operations Per Second (IOPS). Although it's important to have access to these types of raw statistics, what is more critical is that your tool gives you complete visibility into the end user environment and provides useful information such as the overall health, performance, and efficiency of your end user environment.,. The tool must be able to optimize the VDI environment to ensure that VMs aren't oversized or undersized as well as be able to quickly identify performance/capacity bottlenecks. Ideally, your performance/capacity tool should be able to prevent problems before they occur. However, when troubleshooting is necessary, you should be able to identify the root cause quickly and have the tool provide recommendations for remediation.



Good: No Issues

Workload Breakdown

Remote Sessions

□ Capacity 300 Sessions
■ Demand 7 Sessions (2% of Capacity)

Best Practices

□ Capacity 2,000 Sessions
■ Demand 300 Sessions (15% of Capacity)

Workload in Related Objects

Peer (7 of 8)

Children (34 of 34)

View Pool Resources

Remote Sessions | Maximum Recommended Sessions:

Summary | Blackout Times: 1:07:00;780;2:0

Summary | CBRC Enabled:

Summary | Description:

Summary | Entitlements: core;vmwarem\eng_vdog_nashville_persi

Summary | Parent VM: /EUC Dogfood/vm/euc

Summary | Snapshot: /Floating Win8 07.26.2013/BASE/flo
2013/Win8_floating_view5.3/flo-win8/wi
10-1-2013/win8-flo-10-2-2013/Win-8.0-10-
win8-11-5-newagents/win8-11-1
2014/win8.0-2-13-2014/win8-3-

Summary | Template Path:

Workload Policy Settings

Badge Score Symptom Threshold: 80, 90, 95

Figure 2.2: Virtual infrastructure performance and capacity tool for desktop and application virtualization.

End users expect their virtualized desktops and applications to perform as reliably as their physical desktops did. The last thing that you want is your end users having to report their own problems to IT. You must prevent problems before they happen, or at least know about them before the end user does. You need a tool that offers you the fastest time to value for your environment, lowers your overall operational costs, and helps you provide the optimal end user experience.

Desktop Provisioning Considerations

All too often, the last thing enterprises consider is automating desktop provisioning. This is unfortunate because if you can capture your most common tasks and orchestrate and automate them, you can immediately become more efficient. Examples of common tasks that you might consider include:

- Deploying patches to a company application
- The workflow associated with requesting and approving new desktops
- Adding new virtual desktop users
- Entitling a common application to an existing VDI user

Automation and orchestration tools allow you to automate many of the common tasks that you perform for your virtual infrastructure. Large-scale automation tools can take these common automations to a higher level by interfacing with physical infrastructure, cloud services, and other hypervisors while applying company policies and managing the complete lifecycle of VMs and applications. Additionally, these high-level automation tools allow you to deploy any application "as a service" and/or deliver applications and VMs from a self-service catalog. In the end, orchestration and automation will drive greater IT operational efficiencies and deliver greater return on investment (ROI).

Summary

No desktop or applications virtualization project can be successful if not planned and maintained well. The reliability, availability, and performance of your environment depend on the proper time investment, upfront—and the right tools to keep it running smoothly over time. You must ensure that your performance and capacity tool is well versed in the unique demands of desktop and application virtualization to ensure that you can predict bottlenecks before they happen. Finally, by automating tasks the first time you do them, you won't have to reproduce them. Although it sounds simple, many administrators never invest their time in this automation and orchestration process. The small investment required for automation will result, in the long term, in much greater efficiency for you, as an administrator, and for your company.