Lunch Break SERIES

Windows 7 Migration & System Center Configuration Manager

Better Windows 7 Migration with Microsoft System Center Configuration Manager (SCCM)

An IT Pro's Guide to Virtualization and Windows 7

SPONSORED BY

BDNA
IT Visibility. Solved.™

Redmondmag.com

RVP
REDMOND VENDOR PROFILE

BDNA: IT Visibility. Solved.

What is BDNA? BDNA provides the most thorough and accurate view of your entire IT infrastructure, including data centers, desktops, and enterprise architecture. The key to its value proposition is BDNA Technopedia, the world's largest catalog of IT product information, with more than 90,000 enterprise IT products and more than 14 million market data points. From IT administrators to executives, BDNA delivers the business-relevant information required to accelerate key corporate initiatives.

BDNA's IT Visibility Solutions Link Your Entire IT Infrastructure Directly to Your Business Goals.
Using patented technologies and leveraging the industry's most comprehensive hardware and software catalog, BDNA delivers the visibility that drives corporate IT initiatives.

From enterprise processes such as license compliance and asset/service management, to time-critical projects such as data center consolidations and Windows 7 migration, BDNA provides the ultimate solution for complete and accurate IT visibility.

- **Technopedia™** Run a reality check on your entire IT infrastructure with Technopedia's complete catalog of over 90,000 hardware and software products augmented with over 10 million market data points.
- **BDNA Discover™** Gather a comprehensive, accurate, and immediate inventory of all your known and unknown assets without having to deploy any software agents.
- **BDNA Normalize™** Leverage the strategic value of your existing network discovery and management tools quickly and easily, by normalizing and enriching the raw data trapped within them.
- **BDNA Normalize as a Service (BDNA NaaS™)** Combines the market-leading capabilities of BDNA Normalize with the convenience and efficiency of a service, thus guaranteeing a reliable, scalable and secure normalization solution.
- **BDNA Normalize for SCCM™** Integration with SCCM helps SCCM professionals automatically transform data into real-world information, without having to leave the SCCM environment.

BDNA
IT Visibility. Solved.™

For more information, please visit www.bdna.com

BY BRIEN M. POSEY

Better Windows 7 Migration Planning with Microsoft System Center Configuration Manager

Anyone who has ever performed a large-scale desktop operating system migration knows just how challenging the process can be. Microsoft's System Center Configuration Manager can help to make migrating to Windows 7 easier, but you are still going to have to do quite a bit of planning before you ever begin the migration process. As such, I'd like to familiarize you with some of the strategies that you can use when preparing for such a migration.

When contemplating a migration, the main decision that network administrators must make is in regard to the level of desktop preservation that needs to be achieved. In many larger environments, it is perfectly acceptable to wipe the workstation hard drives and perform a clean Windows installation because no user data is stored on the workstation hard drives.

In other cases, administrators might need to preserve the existing desktop configurations throughout the migration process. The most common reason for doing so is to preserve user profile data that resides on the PC. Even if the PCs do not contain any profile data, it might sometimes be advantageous to preserve the PC's configuration in an effort to avoid having to reinstall applications and drivers.

Preserving the User State

If your goal is to preserve any user state data that exists on the PCs, then your best bet is to use version 4.0 of the User State Migration Tool to transfer the user's data from the old operating system to the new one. The User State Migration Tool is part of the Windows Automated Installation Kit, and is included with System Center Configuration Manager.

In some situations this might seem like overkill. For example, if you are going from Windows Vista to Windows 7 then you might be able to perform an in-place upgrade and avoid using the User State Migration Tool altogether. However there are a few problems with taking this approach.

First, there is an element of risk associated with an in-place upgrade. If the upgrade fails then there is a chance that the user state data could be lost.

Another problem with performing an in-place upgrade is that it won't work if you are switching architectures or if you are downgrading Windows Editions. For example, if you are going from a 32-bit version of Vista to a 64-bit version of Windows 7, then you won't be able to perform an in-place upgrade. Finally, you can't perform an in-place upgrade if you need to migrate from Windows XP to Windows 7. You might be able to get away with performing an in-place upgrade from Windows XP to Vista and then from Vista to Windows 7, but this type of upgrade isn't officially supported.

If you decide that you need to preserve user state data, then the easiest way to do so is to use the System Center Configuration Manager to create a package for the User State Migration Tool. If you are using version 4.0 then you don't have to worry about creating separate packages for 32-bit and 64-bit systems. A single package will do.

After you have created a User State Migration Tool package you need to copy the package to a distribution point and then install it to the PCs that you plan to migrate to Windows 7.

In the past, one of the big challenges with working with the User State Migration Tool was that backing up the user state required a lot of storage space. With the 4.0 version, it is possible to back up the user state data to the same volume in which it currently resides. This process involves the use of pointers and therefore requires less than a gigabyte of free disk space.

Deploying an Image File

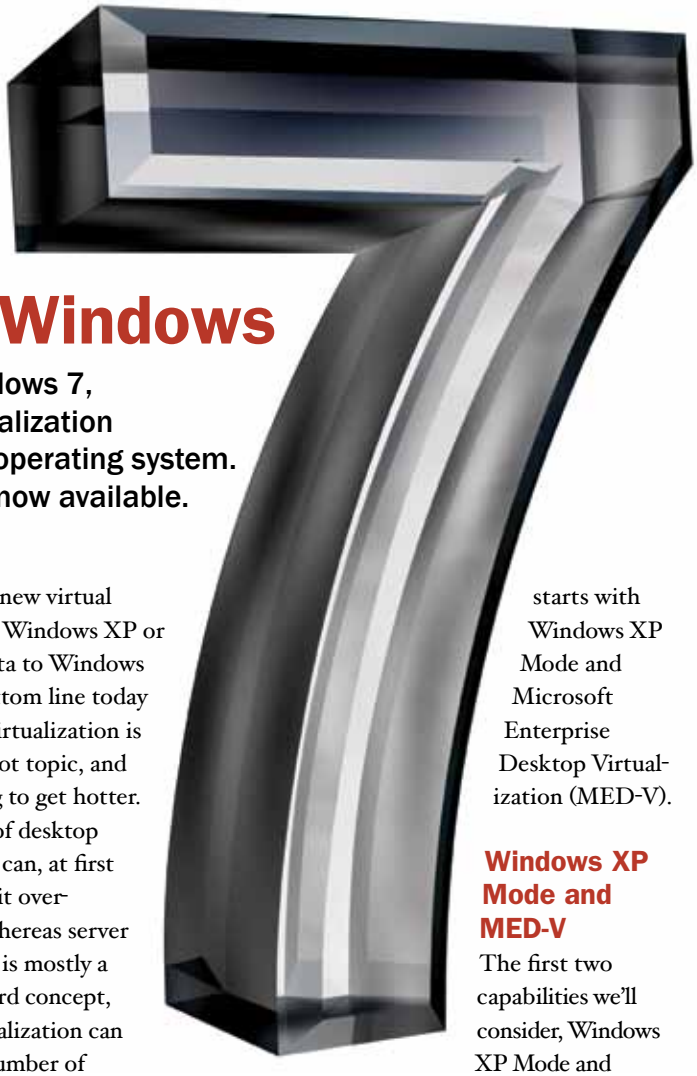
If you do not have to worry about preserving user state data on the PCs, then it may be easier to perform the migration by using an image file. The problem with deploying an image file is that there is a good chance that not every desktop in your organization is identical. As such, you must either create multiple images or you will have to create a single image that contains the operating system, core applications, software updates, and drivers, and then add anything that is missing from the individual PCs once the image has been deployed.

Regardless of which technique you choose, the process works the same way. The first thing that you will have to do is to use the System Center Configuration Manager to create a package based on the Windows 7 installation DVD. Once the package has been created, you can copy it to a distribution point. Repeat this process to create packages for any applications that you want to install on the operating system. You can then build a task sequence that deploys the operating system and the applications.

Once everything is in place, you can use System Center Configuration Manager to build and capture a reference machine. This process uses the task sequence that you have created to deploy Windows and your application set to a new machine. When the deployment is complete, System Center Configuration Manager will create a WIM image. You can then build an OS image package from the WIM file and use it to deploy Windows to all of the machines that you need to migrate.

You can find step-by-step instructions for the process at: http://blogs.technet.com/b/gborger/archive/2010/10/11/getting-started-creating-a-windows-7-capture-image-using-sccm-osd.aspx

BY J. PETER BRUZZESE AND LEE OWENS



Virtualization and Windows

As companies prepare to migrate to Windows 7, IT professionals can implement new virtualization capabilities provided in the new desktop operating system. We offer a primer on the various options now available.

Virtualization is just about everywhere in IT these days: there's network virtualization, storage virtualization and, of course, server virtualization. For now, server virtualization stands in the spotlight, providing numerous benefits to IT administrators including cost savings, server consolidation, ease of administration and deployment, and enhanced security and compliance. Now such advantages are rapidly sparking interest in bringing the benefits of virtualization down to the desktop level.

The growing attention to desktop virtualization will no doubt continue to expand, perhaps even more so now that Windows 7 is becoming widely deployed. For some IT shops, the proliferation of Windows 7 may very well mark the right time to make the switch to virtualization on the desktop. Such a move may have been put on the back burner for a year or more to avoid the pain of going through a migration from a physical to a virtual platform, with the knowledge that the migration would have to be immediately followed up by a conversion of those new virtual systems from Windows XP or Windows Vista to Windows 7. But the bottom line today is: Desktop virtualization is becoming a hot topic, and it's only going to get hotter.

The topic of desktop virtualization can, at first glance, be a bit overwhelming. Whereas server virtualization is mostly a straightforward concept, desktop virtualization can involve any number of different concepts and technologies—especially with the virtualization options presented by, and to, Windows 7. Therefore, IT professionals and decision makers need to know which virtualization options are available to them in order to make informed decisions as to whether a virtual Windows 7 deployment is the right fit for their environment.

With that in mind, we're going to examine the gamut of desktop virtualization options available for Windows 7 deployments—whether a company is rolling out a single desktop or thousands in the enterprise. It all starts with Windows XP Mode and Microsoft Enterprise Desktop Virtualization (MED-V).

Windows XP Mode and MED-V

The first two capabilities we'll consider, Windows XP Mode and MED-V, are similar in their overall purpose and general functionality. Both allow older applications to operate virtually running under their supported OSes, thus removing the application incompatibility barriers that could prevent an OS upgrade to Windows 7. Both deliver applications to the Windows 7 desktop (Professional version or higher) from a Windows Virtual PC running Windows XP in a way that's completely seamless and transparent to the user. These published applications will appear and operate just as if they were installed on the Windows 7 desktop itself, even

The latest Dell Optiplex desktop PCs support the company's new Flexible Computing Framework, which includes Dedicated Remote Workstation and Virtual Remote Desktop solutions.

allowing users to pin them to the task bar for easy access.

While these two solutions are comparable in purpose, their usage scenarios are what really differentiate them. In general, Windows XP Mode is targeted for use primarily by individuals or small workgroups, whereas MED-V is intended to provide the additional capabilities required for deployment in the enterprise. Windows XP Mode uses a preconfigured Windows XP virtual machine (VM) that must be manually downloaded and installed on each workstation. MED-V allows IT administrators to centrally deploy an IT-managed virtual Windows XP environment that can be customized and rolled out automatically, and do so based on Active Directory user accounts and group membership. MED-V bridges third-party application incompatibility gaps. It also enables automatic redirection of Web requests on the Windows 7 desktop that require Internet Explorer 6 or newer to IE on the virtual Windows XP environment, thus eliminating browser-version incompatibilities. In short, MED-V helps IT pros deploy, provision, control and support virtual environments.

Who can use these products? Windows XP Mode is available to anyone running Windows 7 Professional, Ultimate or Enterprise. It utilizes Windows Virtual PC and does require the hardware to support virtualization. MED-V is a core component of the Microsoft Desktop Optimization Pack (MDOP), which is available only as a subscription for Software Assurance customers. For more details on Windows XP Mode and MDE-V, and to download Windows XP Mode, visit the Microsoft Web site.

Now, let's turn our focus to the options available for running Windows 7 virtually.

Virtual Desktop Infrastructure

We should start by defining what Virtual Desktop Infrastructure (VDI) is. Put simply, VDI gives users access to a desktop computing environment that runs as an independent VM on a server-based hypervisor, typically in the datacenter. When discussing VDI, it's important to understand that it's a complete solution, not a single, standalone product. Therefore, evaluating VDI solutions requires an understanding of the many factors that must be taken into consideration. These factors include parts of the entire infrastructure, including hardware and software choices at the desktop and server level, centralized storage considerations, and even the implications such a solution would have on the network. But don't let any of that scare you away from the thought of deploying Windows 7 on VDI.

While VDI may not be for everyone, it certainly does offer many of the benefits of virtualization in general, and it can be especially useful in providing business solutions for specific scenarios. What are some of the benefits offered by VDI?

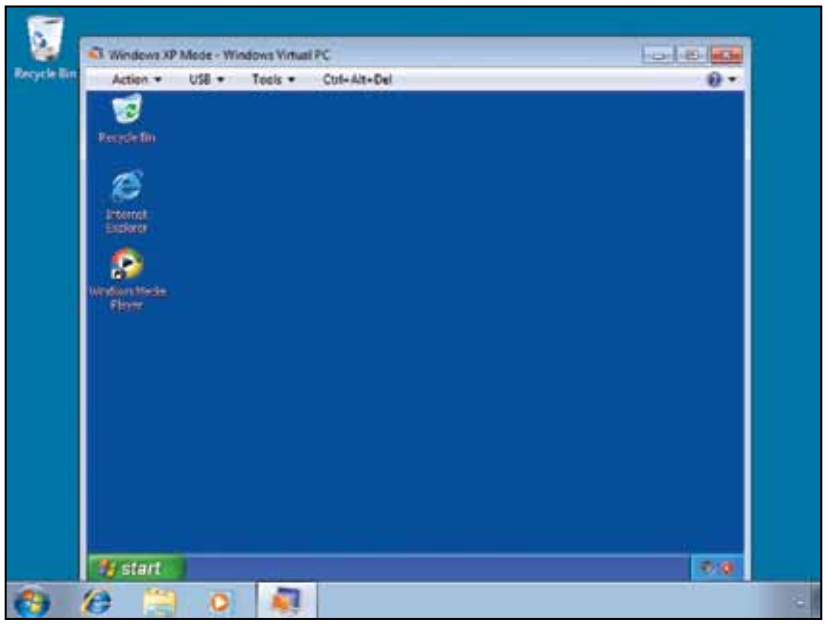
- VDI as a server-based computing model provides the following benefits: improved data security, as all data remains in the datacenter; potential for savings on hardware expenses; ease of management and greater efficiency due to centralization; and the ability for users to move around without being tied down to one desk or physical machine.
- VDI also offers benefits derived from the distributed computing environment. With VDI, each user still has his own "PC" (at least his own OS) running as an independent VM. So, while there may be dozens of such guest VMs running on a single

hypervisor host server, each user has complete control of his VM and can install applications or reboot without causing any issues for other users.

- Because VDI runs on a virtualization platform, you get the same benefits that are offered by server virtualization, such as improvements in stability and performance, high availability with automatic failover and recovery, and fast and easy VM provisioning—which, for VDI, can even mean automatic deployment of new desktops as needed.

So, what are some of the IT challenges that can be met by the benefits of VDI solutions? Among them are the following:

- By deploying VDI, it's possible to extend the lifetimes for legacy PCs already on the desktop. Such older hardware—which would've needed upgrading in order to run a new OS such as Windows 7 or an intensive application—can remain in place and serve, in effect, as a thin client for providing connectivity to a user's new VM desktop.
- Because of the benefits of virtualization technology, VDI can be used as an effective business-continuity solution in order to meet disaster-recovery requirements. By utilizing VM portability and dynamic provisioning as part of a VDI solution, a standby datacenter with VDI configured can be ready to take over in case of a serious outage due to a disaster, whether the disaster is a physical occurrence or the result of a pandemic.
- Because VDI is centralized, organizations that have outsourced business functions can provide VMs to remote users and yet retain control of the desktop environment and any internal data that must be accessed by these workers.



Windows XP Mode is available with Windows 7 Business, Ultimate and Enterprise editions.

- Organizations that have already deployed virtualization solutions for their server infrastructure can deploy VDI to align their desktop and server processes while leveraging a common platform. This can allow IT shops to do more with fewer physical resources, which may provide some needed relief to busy IT pros and support staff.

Now let's look at what it takes to implement VDI.

Components of VDI

As noted earlier, VDI is a complete solution that encompasses many components, and for each component there are numerous product offerings from numerous vendors. However, the primary components of an overall VDI architecture can be broken down as follows:

- **Server-Based Hypervisor Platform** This is where it all starts for VDI, which is also the same starting point for server virtualization. In this component category, there are typically two leading vendor solutions, from Microsoft and VMware Inc. The Microsoft solution is built on Windows Hyper-V Server 2008 R2. The current VMware solution offering for VDI is VMware View 4, which is integrated with vSphere. Naturally, there are other vendors in this arena, perhaps most notably Citrix Systems Inc., which not only offers its own solutions but has also partnered with Microsoft to extend and enrich the client experience on the Hyper-V platform.
- **Guest VM Running the Client OS** In the end, VDI is all about providing a stable, secure, easily manageable and—most importantly—enjoyable desktop computing environment for your end users. What could be a better fit than Windows 7? Of course, VDI allows for all sorts and flavors of client OSes. If you need to run a few Windows XP VMs for legacy apps, or

even a Linux workstation or two, then those options are available as well.

- **Client Access Device** There are two basic choices in this area. The first is to use a regular PC to connect to the VM, via either a standard Remote Desktop Connection or some other client software. While this can allow you to extend the lifetime of your desktop hardware, it does still mean having to manage the OS at the desktop level. For this reason, and others, many choose to go with another option—thin clients. A thin client is a solid-state desktop device with an embedded OS that provides access and connectivity to the virtualized desktop, also using either Remote Desktop Protocol or another client. Many thin-client models have no hard drive, fan or other moving parts, which means they can have a longer lifetime than standard fat-client computers and can also use significantly less power than PCs. Thin clients offer enhanced security, easier deployment and manageability, and a high level of reliability. That's not to say that thin clients provide limited capabilities; rather, they're feature-rich devices offering expansion, I/O ports and even dual-monitor capability. The industry leader in thin clients is Wyse Technology Inc., but many vendors, such as IBM Corp., Hewlett-Packard Co., NEC Corp., Fujitsu Ltd. and Oracle Corp. (via its Sun products business)., to name just a few, have thin-client offerings.
- **Connection Broker** In a static VDI environment, there's a one-to-one relationship between an end user and a specific virtual desktop assigned to that user. This usually works well for smaller VDI implementations. However, many larger enterprises will want to deploy a dynamic VDI environment. This will require a connection broker, which is used to assign users to any available virtual desktop, to suspend and resume VMs based on state, or even to dynamically provision a new virtual desktop if none is available. Connection brokers allow for higher VM-to-user utilization rates and system concurrency by utilizing dynamic allocation of virtual resources, which will usually result in a cost savings. VDI connection broker software products are available from Microsoft (Remote Desktop Connection Broker in Hyper-V 2008 R2), VMware (View Manager as part of the View 4 solution), Citrix and Quest Software Inc., as well as from other vendors.
- **Management Software** The management component is going to serve as the window into your VDI world. A centralized management console will allow you to manage the physical servers, the guest VMs and the client connections all from one place. For a Microsoft Hyper-V solution, there is System Center Virtual Machine Manager. VMware offers View Manager and vCenter Server to manage its solution.

Select HP business PCs will be certified to run the forthcoming Citrix XenClient bare-metal hypervisor.

Those are the big pieces. Of course, the component list for a complete VDI solution doesn't end there. There are also components involving security, workflow automation, application virtualization and so on. How can you make it all come together? Once you decide on a vendor for your hypervisor virtualization platform, you'll be able to take advantage of that vendor's third-party partnerships to round out your solution. And by following the partners' and vendor's recommended best practices, you can make all of the pieces to your VDI puzzle fall into

place—like one big virtual picture.

Alternatively, because VDI essentially makes the desktop a service, there's another option to consider: Service providers are now offering subscription-based virtual desktops as a hosted solution—located either locally in the customer's network, or in the cloud at the service provider's datacenter. Such a hosted solution can reduce the complexities and capital expenditure costs required for a successful VDI implementation. Is outsourcing the desktop—whether internally or out to the cloud—something that everyone should consider? No, and that's not what we're suggesting here. However, for some organizations, it will make sense. Therefore, if you're interested and think it may make sense for your organization, you may want to check out the offerings from IBM (Smart Business Desktop Cloud), Secure-24 Inc., I-Land Internet Service, ICC Global Hosting or Desktone Inc. (Virtual-D Platform), to name just a few.

Client-Based Hypervisors

When it comes to hardware virtualization engines, or hypervisors, there are two categories: Type 1 and Type 2. We referred to Type 2 client-based hypervisors when discussing Windows 7 XP Mode. A Type 2 hypervisor is really an application, like Windows Virtual PC, which runs on top of a full-featured OS such as Windows 7—and there are more out there, including VMware Workstation. Such Type 2 virtualization engines for desktop computers have been around for some time now.

A Type 1 hypervisor runs natively on the bare metal of a computer system, whether a server or a desktop, and in effect becomes the OS—thus this type is often referred to as a "bare-metal" hypervisor. Microsoft Hyper-V and VMware ESX are examples of Type 1 server-based hypervisors. While server-based offerings have been available for some time now, it's only recently that Type 1 bare-metal, client-based hypervisors have become available for the client, and many are still in development. The first to market was Virtual Computer Inc. with its NxTop solution. Of course, VMware and Citrix are working on getting their offerings to market in the near future; the forthcoming Citrix XenClient is now in beta.

We know what kind of evolution has taken place in the server arena with Type 1 virtualization. Will bare-metal, client-based hypervisors have the same impact? Only time will tell. The implications of such technology at the client will offer a multitude of benefits, however, and that alone should be enough to add bare-metal, client-based hypervisors to your list of possible virtualization solutions for deploying Windows 7.

We've looked at the options out there to run virtualization on Windows 7, as well as how you can run Windows 7 on virtualization. By leveraging the benefits of the Windows 7 OS and virtualization technology, you can enjoy a new level of administrative ease and enhanced security, as well as a dynamic infrastructure.

J. Peter Bruzzese (peter@trainsignal.com), Triple-MCSE, MCT, MCITP: Messaging, is a longtime contributor to Redmond and an Exchange instructor for Train Signal Inc. Lee Owens, Triple-MCSE and MCITP: Messaging 2007, has more than 13 years experience in the IT field and is currently an enterprise systems engineer focused on Active Directory, Exchange, mobility and virtualization technologies.