WHITE PAPER: BACKUP AND RECOVERY

Implementing Virtualization:

Techniques and Tools for Microsoft® Windows® Conversion

White Paper: Backup and Recovery

Implementing Virtualization: Techniques and Tools for Microsoft Windows Conversion

Contents

Introduction

Most IT professionals know or suspect that virtualization of computer systems may have an important role in their organization's evolving infrastructure—though where and how are likely under investigation. Some organizations will decide that virtualization isn't necessary. Others will find that they want to implement it in places, but not across the board. Still others will move to implement it on a large scale.

For those who decide to implement virtualization, the question is how to do it. Many people are not aware that a number of conversion tools and techniques are available now in the Microsoft Windows environment. This paper focuses on these tools and techniques and presents a variety of scenarios for using them.

First, however, there are several misconceptions to be pointed out. As a general rule, virtualization does not save on the cost of software. It may or may not save on the cost of hardware. The biggest economic driver is probably the efficiency it enables in terms of administration and management.

With regard to hardware, in most cases the savings aren't a huge part of the total economic benefit. That's because any group of devices being retired have to be replaced with a more sophisticated and therefore more expensive single system. In fact, running a large virtual environment effectively may very likely require implementing a storage area network (SAN), with all the ensuing costs and complexities.

In terms of management and administration, however, virtualization can deliver significant economic benefits. For example, consider a computing environment with 20 separate physical servers, each in a different physical location performing different tasks, and each running mid-level hardware and separate applications. Several questions come to mind. First, how do you keep track of them all? Second, does new software, when implemented, usually need to be run on independent servers?

With computer system virtualization, all 20 servers can exist virtually on a single high-performance system. Only one physical device needs to be managed instead of twenty. And, you can manage it in a way that makes it easy to automate more tasks on all the virtual systems.

When you need more resources, instead of procuring them you can simply allocate them on the main physical system. After all, even though the 20 servers probably are relatively identical in terms of their hardware capabilities, their applications don't use identical amounts of memory, processors, disk space, or other resources. Some applications may be very intensive. Others may use hardly any of the resources built into the server.

With physical hardware, balancing and managing resource utilization can be time consuming. In a virtual environment, however, you can quickly and easily reassign resources to the applications and operating systems that need them most.

Virtual and physical conversion

One of the biggest uncertainties about virtualization in IT organizations is how to get there; i.e., conversion. This process involves swapping out the architecture that underlies applications and operating systems and converting them to run in a different environment, whether that means a totally different physical environment or a different virtual environment.

When you use virtualization for your IT operations, you are making an important decision. You are taking all of your eggs from separate baskets and putting them all into one basket. It's absolutely essential to have access to physical-to-virtual and virtual-to-physical conversion tools that you can rely on.

Many organizations treat their virtualization strategies as experimental. After going virtual, they may find that the approach doesn't work as well for a particular application or system essential to them. Or, they may discover that they prefer having their systems more physically distributed. They might then decide to go back to running in a physical environment. A best-practices approach should always provide for conversion back to physical when desired or required.

Benefits and issues

If you're doing a true, or permanent, migration of systems from physical to virtual, then all changes and operations afterward will be done on the virtual system. The physical system can be retired or repurposed. The virtual system becomes the production system, maintained just as though it were a physical server. The applications and patches, which are not even aware that they're running on a virtual system, can continue to be licensed and managed as if they were on physical hardware.

Converting just one or several systems to virtual is neither difficult nor terribly time consuming. For example, if your chosen platform is VMware, you can do conversions with a free and easy-to-use VMware tool. If, on the other hand, you need to convert a large number of systems, then you would want to employ automation so that the overall task is not so arduous. This approach is beyond the scope of free tools, and would require the purchase of third-party conversion software that's more powerful.

The main difference between free tools and purchased third-party tools is that the free tools are used solely for physical-to-virtual conversion and have no system recovery (virtual-to-physical conversion) capabilities. Free tools are also generally not as automated and may not deliver the best performance.

Those who are already creating virtual systems for backup purposes can also provide for redundant failover of the original physical system—without purchasing additional physical servers. Simply implement a strategy wherein a new physical-to-virtual conversion, or copy, of the physical system is periodically created. In the event that the original physical server fails, this copy can be brought up at a moment's notice and used for disaster recovery.

Tools and environments

To provide users with the greatest value, conversion tools must be able to perform two primary operations. First, they need to create a copy or *image* of the full system and data partitions and then store this copy in a virtual file. Second, they need to know and address the critical system drivers required to use the hardware on the target system. A VMware virtual server, for example, uses Intel IDE.sys and VMSCSI.sys as storage drivers. For network drivers or NICs, VMware uses VMxnet.sys or AMDpcnet.sys.

In a typical conversion, additional applications allow the client or guest system to communicate, configure, or work seamlessly with the physical hardware. There's also the question of moving a new virtual system to a new physical location where it can be hosted. For example, VMware ESX Server software uses a Linux® kernel and a Linux file system. Before a physical system is fully converted for use by ESX, it has to be moved onto the file system where it will be accessible to that virtual infrastructure.

In simpler environments, such as VMware Workstation, the new virtual system might run natively on Windows and wouldn't require anything to be imported into a different file system. There's still a need, however, to port those bits into a format that the virtualization platform will understand.

Consider Microsoft's virtualization platform, where the virtual system resides in a Virtual Hard Disk (VHD) file—literally a single file that includes the operating system, application, data and everything that makes up that system. Converting into that file type is the secondary step. When completed, the result will likely be a very large file with—in the case of Microsoft—a .VHD extension. VMware converts in the same way to a file type having a .VMDK extension.

Conversion types

Physical to virtual (P2V)

Physical-to-virtual conversion is performed on an operating system that is installed directly on hardware. This conversion effectively takes the physical system up a level in abstraction. Thus, instead of the operating system running directly on hardware, it runs on a virtual system that is running on hardware.

Virtual to virtual (V2V)

In a virtual-to-virtual conversion, one virtual system that's running on a virtual platform is converted to another virtual system running on a different virtual platform. This type of conversion is less commonly done than P2V.

Virtual to physical (V2P)

This conversion type allows conversion back from a virtual system to a physical system. This tool is essential when performing conversions, because it lets you revert to the physical system you started with.

Physical to physical (P2P)

Physical-to-physical conversion can be very useful when doing a hardware upgrade or replacement. However, it doesn't have anything to do with virtualization *per se*.

Backup and disaster recovery considerations

An additional benefit of virtualized systems is that a copy or image of the virtual system can be used for disaster recovery or full system recovery. Then, even if a physical or virtual system becomes corrupt, you can boot the recent virtual copy and have your production system up and running again quickly.

Many IT professionals have discovered this to be a viable system recovery approach. It does not provide immediate failover, as clustered servers do. However, with servers in scenarios that do not justify the cost of clustering, it can be used to provide disaster recovery at a very reasonable cost.

Because of this, it's wise to consider a system recovery solution when evaluating conversion technologies. Some recovery solutions provide conversion capabilities and some conversion tools provide recovery tools. The most useful all-around solutions are likely to provide capabilities for both system recovery and virtual conversion.

Conversion scenarios

Conversion should be a main focus of any virtualization strategy. In general, conversion scenarios involve taking a system in one environment and going, or converting it to, another environment. The two environments we are concerned with here are physical and virtual, and there are four main variations, not all of which are commonly known or understood:

- Going from a physical environment to a virtual environment
- Going from one virtual environment to a different virtual environment
- Going from a virtual environment back to a physical environment
- Going from one physical environment to a different physical environment

There are several software tools available to help you perform these conversions. This paper describes different use cases and scenarios where the conversion tool of choice is Symantec Backup Exec™ System Recovery.

Going to virtual

P2V or physical-to-virtual conversions

P2V is the best known and most commonly used type of conversion. It's typically used to convert from a physical to a virtual environment either for permanent migration into a virtual environment or for temporary conversion, such as disaster recovery or testing an environment.

In computing environments where Symantec Backup Exec System Recovery is already running and being used to create images for backup or other purposes, converting from physical to virtual is quick and easy:

1. The user opens the Symantec Backup Exec System Recovery conversion wizard and chooses any existing .sv2i file.
2. The user then chooses a virtual output format—either VMware or Microsoft Virtual Server—and clicks Finish.
3. If the user chooses VMware, they are given the option of copying the file to a VMware ESX server once it has been converted.
4. Within minutes, a copy of the image file is created in the desired virtual format—either a .VMDK file in the case of VMware, or a .VHD file in the case of Microsoft Virtual Server.

With Symantec Backup Exec System Recovery, an .sv2i file is a small reference file, created from the most recent image capture, that points to an entire image set. It knows which are the most recent .v2i and .iv2i files, and knows whether the image capture included multiple partitions. So, for example, if both the C and D drives were last captured, then by pointing to the .sv2i file, the conversion will automatically include both the C and D drives in the virtual file.

Here it's important to note several points. First, after performing this P2V conversion, the original image files will still exist. There will just be another instance of the system in the virtual format in addition to the .v2i images. Second, the image files are going to take up approximately the same amount of space as they did on the original disk. In other words, using the C and D drive example, if they were compressed to about 10GB during image creation, then you can expect when they're converted to virtual they're going to be uncompressed and take up approximately twice the space, or 20GB.

In terms of time, a good rule of thumb is that the full conversion will take approximately 60 to 90 seconds per gigabyte. Of course, performance will vary depending on hardware resources, network performance, and other variables. Once the file is converted, it will be ready to be launched with either VMware or Microsoft Virtual Server, depending on the virtual application you chose.

A P2V conversion of this sort can be described as a *full clone*. In this case, the entire image is converted to the desired format. Another P2V option, however, is a *linked clone*. Symantec partnered with VMware to create linked clones, which are designed for temporary conversions. Linked clones do not convert an entire image into VMware format, but merely the descriptor file or disk configuration file. They also create a small .VMDK file to which changes are written. This .VMDK file continues to reference the original Backup Exec System Recovery image (or .v2i file) on an ongoing basis. As a result, a linked clone does not perform as efficiently as a full clone in a virtual environment, but the conversion is very fast—in fact, nearly instant.

A linked clone is the optimal choice if you simply want to run some quick tests in a virtual environment. For example, suppose you'd like to see how a new patch affects a Microsoft hot fix. A linked clone allows you to do this without affecting the production system at all. The image file won't be affected either, because any changes written are stored in the .VMDK temporary file and discarded once the system is turned off.

Linked clones are very easy to create. Simply open the VMware Workstation application, go to the File menu and choose Open. A pull-down menu allows you to browse for the desired .sv2i file. Once you've chosen the file image, the application dynamically creates .VMX and .VMDK extensions, allowing changes to be written and the system to be loaded quickly.

V2V or virtual-to-virtual conversions

While it is not used as often as P2V, V2V is a necessary and important conversion process. It allows you to convert from one virtual platform to another, even from the same vendor. For example, you can convert from Microsoft Virtual Server to VMware Workstation—or from VMware Workstation to VMware ESX Server. With V2V conversion, you can even migrate a virtual platform from one VMware ESX Server instance to another.

There are also other reasons for doing V2V conversions, such as retiring or repurposing a virtual server. The virtual environments running on that old system have to be moved over to another virtual server. This kind of V2V conversion is obviously a maintenance and management task.

Sometimes it can be to a vendor's advantage to provide free or inexpensive conversion tools, and this is true for VMware and V2V conversion. VMware provides an internal V2V conversion capability that allows users to convert easily from a VMware Server platform to a VMware ESX Server platform. The free VMware Server product was designed for running just one or a few virtual systems in small, simple virtualization environments. But even if one starts out running a small number of virtual systems, they may end up being taken into an environment with large numbers of virtual machines, or with machines that have heavier performance requirements.

In that case, you'll want to upgrade to a VMware ESX Server platform. VMware has made it easy, using straightforward VMware utilities that convert any existing VMware Workstation or VMware Server files into VMware ESX Server files.

Going to physical

Whether converting from virtual to physical or physical to physical, you use the same type of process with the same steps. Either way, in a conversion to a physical environment, a number of variables have to be dealt with.

When converting to virtual environments, the requirements are much simpler. You address the driver set and file system and other considerations to make the operating environment function in the selected virtual environment. Take VMware, for example. The virtual environment is a static environment. It provides a static platform to reside on, meaning that the driver set is static, and the storage controllers used are the same storage controllers. Providing just one storage controller driver during the conversion process makes it possible to address VMware's virtual environment. As far as network or NIC drivers are concerned, VMware uses just two. Provide them both and you're covered for conversion to that virtual environment.

When converting to a physical environment, the physical system to which you're converting or restoring can have any number of different drivers that may be unknown to you. For example, suppose you order a new server from the factory. It could have a completely new storage controller on it, a new NIC, a new hardware abstraction layer, a new chipset—in short, many different hardware devices, all requiring drivers that are new. This is a much more challenging conversion.

Obviously, there needs to be a way to dynamically address and provide those different drivers in real time during conversion, so that the system can be functional on the new hardware. For example, a storage controller driver has to be in place in order for the disk to be recognized—and so that the operating system on that disk can function. If the required critical drivers are not added in real time during the conversion process, the system will never boot on the new hardware.

Both V2P and P2P require this type of capability. Fortunately it exists, though few are aware of it, in the form of the Symantec Recovery Disk (SRD) provided with the Backup Exec System Recovery application. This disk runs the Microsoft Windows PE operating system and contains a large driver database. When Windows PE boots, it loads the Windows services required to access the restored system and to plug in drivers dynamically. This is the tool to use for both V2P and P2P conversions.

V2P or virtual-to-physical conversions

There exist fewer options for doing V2P conversions than P2V conversions. But options do exist, and they work well. They should be considered as part of any organization's conversion strategies, especially when virtualization is being used both for its own sake and as part of a disaster recovery or failover strategy.

In fact, those are the most common scenarios for V2P conversion: where virtualization is implemented due to failover or used during disaster recovery. Once disaster has been averted or replacement hardware for lost systems has been procured, there remains the need to migrate efficiently back to the previously operating physical environment.

There are several other common use cases for V2P. For example, an organization might decide running a system in a virtual environment is not the best use of that system, and may want to do a permanent migration back to physical hardware. Still another scenario might apply to virtual servers with many virtual guest systems. These are, by definition, very centralized systems, but perhaps the user now needs to break them down and distribute them.

Using the Symantec Recovery Disk, V2P conversion is greatly simplified. Once the disk boots, it loads all the Windows services and drivers necessary to restore the system, either from a locally attached disk or a network attached disk. Menus and prompt screens guide the user. One option asks if Restore Anyware (restoring to dissimilar hardware) is desired. If that option is selected, the recovery disk environment will automatically search its own huge, built-in driver database, automatically locating the appropriate critical drivers (storage controller, kernel, hardware abstraction layer devices, and so forth) so that the system image will function on the new hardware. If any critical device drivers are not found in the database, the user is prompted to browse for them, by driver type. The user then accesses a Windows-like browse environment with which to locate the drivers.

P2P or physical-to-physical conversions

P2P conversions are required in scenarios where a computer or server fails. The disks or controllers may no longer function, or perhaps the server has just reached its end of life. In any case, the computer or server must be replaced.

Unless the machine failed practically out of the box, it's unlikely the user will be able to replace it with the same or even similar hardware as originally purchased. Typical computer lifetimes are between three and five years. Some organizations have even gone the very expensive route of purchasing identical hardware to restore to, but in most cases that is not necessary. Businesses should simply buy whatever system fits their current needs, taking advantage of all advances in technology and hardware—and then do a P2P conversion with the Symantec Recovery Disk. If Symantec Backup Exec System Recovery is already being used, there will be an image, or recovery point, ready to restore to that new hardware. The conversion process is identical to that described above for V2P conversions.

Another case, called *hardware lease* or *migration*, occurs when the hardware is still functional but needs to be upgraded or retired. If you own the server, you may want to repurpose it, or retire it completely and move to the latest and greatest new hardware. If it's leased, it may simply be time to turn it over.

Any of these scenarios can be addressed by taking the existing image and converting it to the new hardware. The slow way of doing this is to install the operating system and all the core components and applications, then change all the settings and configurations and migrate your data to the new system. This is an extremely painful and slow process, and it's not even likely to

result in the same environment that existed before. However, if a P2P conversion is performed with Backup Exec System Recovery, the result will be a system identical to the one that ran on the older hardware, but which is now running on the newer hardware and able to take advantage of all its benefits.

Backup and recovery

Backup and recovery needs vary from organization to organization. In the event of a physical failure, some small organizations with non-critical data can afford to be down for a day or two, or even longer. At the other end of the scale are critical power grid–type systems that millions of people depend on. When it comes to backup and recovery, virtualization can provide a solution and a path for both these types of organizations—and all those in between.

Consider an organization that cannot afford to stock extra hardware just to make sure it will be on hand whenever it's needed. A more affordable solution would be a single, more powerful system capable of hosting several virtual systems. In the event of an emergency, a virtual copy of that system could be waiting in the wings and brought up immediately, with no wait necessary to replace the hardware.

Immediate failover in clustering technologies can be very expensive, requiring duplicate hardware and intelligent software applications that are continually monitoring for failover. With virtualization, however, something similar can be achieved at a much lower cost.

In addition, when there's a hardware failure in a physical environment, the problem isn't just that another server is needed to run the application. The problem also includes the time it will take to restore the backup to that system, to switch all the physical components and connections, to configure the system, and to make it look as much as possible like the former live production system.

If a company has to go out and buy hardware at such a time, it's not likely to be much of a bargain. Also, under a time deadline, you'll have to take what you can get in terms of hardware. Unfortunately, many backup and recovery approaches require that the replacement be the same hardware or else they will not work. Or, alternatively, you'll need to install the operating system from scratch before you can even begin to restore the backup application.

When combined with virtualization, some newer technologies can recover nearly instantaneously, making business continuity affordable for everyone—even in unexpected situations.

One recent example was an airport outage where all the server systems that reported incoming and outgoing flights were unrecoverable. Also affected were the reservation systems, which enabled ticketing, boarding, and deplaning. Amazingly, the entire system was back up and running within 15 minutes. What made this possible was a fluke: A physical copy of the airport's backup solution had been saved without much thought to a small USB drive. It took only minutes before the whole airport was functioning again, using some of the conversion techniques discussed earlier for a physical-to-physical recovery.

Conclusion

Virtualization is a powerful way to deal with a number of the challenges that IT organizations face. These include the need to increase operating and administrator efficiency, to control server sprawl, and to ease disaster recovery.

To be successful, virtualization strategies need to make use of readily available tools that simplify conversion between physical and virtual environments. A few, such as Symantec Backup Exec System Recovery, conveniently bundle a complement of such features, not only providing comprehensive backup and recovery, but also facilitating reliable, quick conversions within Windows environments. The Symantec Recovery Disk makes it easy to perform even the most complicated conversion: going from a virtual environment back to a physical one, where the destination hardware and drivers are not similar to the original.

When combined with virtualization, the latest hardware and software technologies are making nearly instantaneous disaster recovery much more affordable and available for all organizations. Tandem implementation of strategies for both disaster recovery and virtualization is likely to yield the most efficient and economical overall results.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

07/07 12419875