CHAPTER

APPLICATION MANAGEMENT IN VIRTUALIZED SYSTEMS

5

When customers start using virtualization, they have a preliminary notion of what virtualization is. But, once they get in and start using it, they see it's like a Swiss army knife, and they can use it in many different ways.
Raghu Raghuram

A Day in the Life at Acme Manufacturing: A Little Cooperation Goes a Long Way!

Meet Bruce. He is an IT manager at Acme Manufacturing. As part of Acme's program to encourage professional development of their employees, Bruce does some teaching at the local community college. Lately, he became aware of a plethora of ***IT service management (ITSM)*** *jobs in the area and a shortage of IT service management student recruits. To respond to this shortage, he created a new course in ITSM for the upcoming semester. Bruce is excited about the employment opportunities that this type of course will offer to the community college students upon graduation. However, there's one big stumbling block: the community college does not have the funds to purchase the expensive ITSM software to offer the students the hands-on experience Bruce feels is critical to supplement the learning modules he developed. He wants to differentiate his students from those at nearby colleges and universities when they apply for their first ITSM job after graduation, and he knows that being software-proficient will set them apart from the rest.*

After a few sleepless nights he realizes that he might have the answer. In his job at Acme, Bruce uses a well-respected ITSM software package and Acme's IT organization recently completed a large server virtualization implementation. Bruce thinks it's time to set up a meeting with Amanda, his CIO.

Application Performance Management (APM) in the Digital Enterprise. http://dx.doi.org/10.1016/B978-0-12-804018-8.00005-X

Meet Amanda. She is CIO at Acme. She agrees to meet with Bruce, who arrives armed with recent statistics about the lack of ITSM college courses and the consequent lack of skilled ITSM student interns and college recruits. During the meeting, Amanda is impressed by the innovative approach Bruce is proposing. She agrees that partnering with the community college is an excellent idea and agrees to provide the resources that Bruce needs to create a virtual disk image by which the students can access the much-needed software. Amanda is very interested the outcome of Bruce's project and asks him to report back to her at the end of the semester.

Next, Bruce schedules a twice weekly one-hour time slot to access the ITSM software and registers the email address of each of student with Acme's IT services department. Once a virtual desktop is created for each of the students to log into at the specified times, the course is ready to go live.

Meet Kurt. He is a second-year student who is majoring in information systems. He has enrolled in Bruce's new ITSM course and at first, Kurt isn't sure whether this new course is right for him. Initially, he found the textbook material a little boring, but once he is exposed to the "really cool" virtualized desktop that he gets to use each week, Kurt is much more motivated and never misses a class! By the end of the semester, Kurt is pulling an "A" and is quick to tell others that he's really glad that he took the course. He also has an interview with Acme and is hoping that it will lead to his very first job in ITSM.

At the end of the course, Bruce submits his report to Amanda. Thanks to the power of virtualization and a little cooperation between practice and academia, he is proud to report that the partnership was a huge success. His students are proficient in using a well-respected ITSM software package, understand how ITSM works in a real-time environment, and have even learned a little about the benefits of

working in a virtualized environment. And there's already a waiting list for the next offering of the course!

Amanda is excited, too. The partnership with the community college not only provided Acme with a pool of skilled ITSM students from which to recruit, like Kurt, but Amanda was also invited to sit on the college IS Board of Advisors. It's a position she's wanted for some time and she looks forward to identifying other opportunities for Acme to partner with the college.

INTRODUCTION TO VIRTUALIZATION

The concept of **virtualization** is not new, but it is revolutionizing the world of computing. First introduced in the mid-1970s when IBM began shipping virtualized mainframes, its purpose is to provide multiple **logical representations of resources** that allow a system to represent more resources than the actual **physical resources** available. For example, virtual memory allows a system to use more memory than is actually physically available.

In the 1990s, the concept of **virtual machines (VMs)** became mainstream with the introduction of X86 systems, which allow one physical machine to support one or more virtual machines. In some cases, 20 or more VMs could be hosted on one physical machine. This allowed for not only reduced hardware requirements and power and cooling needs, but also enabled and required a whole new way of managing systems.

Now, virtualization is the norm in today's business, thanks to the new opportunities that it created at every level of IT **application management**, from maintenance improvements to operational and capital savings. These savings often equate to 20–50% of the cost of servers, data center power, and personnel.

WHY VIRTUALIZE?

Before we begin exploring the different aspects of virtualization, it is useful to first understand why an organization would consider virtualization as an option to simplify its application management. We will begin by looking at the hardware on which **applications** exist. Most traditional servers are inherently inefficient. Typically, to ensure consistent **performance**, servers run at far less than full capacity of the peak application loads they are designed to handle; on average, they operate at only 10–15% capacity of their peak **application performance** requirements.

Next, the flexibility of applications must be considered. Having just one **operating system (OS)** on a server severely limits this flexibility, and there are also potential conflicts between applications running on the same server. To avoid this, server administrators must run each application on a separate server. This is not an efficient way to manage IT resources since this leads to not only substantial equipment costs, but also a considerable amount of funds being spent on power, cooling, storage, maintenance, and personnel. The good news is that there is a better way, and it is virtualization.

In a virtualized environment, each VM has its own operating system and application and, thanks to specialized software known as a **virtual machine manager (VMM)**, or **hypervisor,** each is totally unaware it is sharing hardware with other operating systems and applications (see Fig. 5.1).

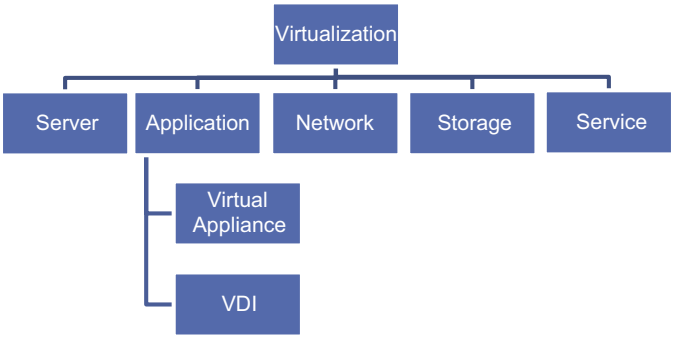

FIGURE 5.1

The many facets of virtualization.

Transforming physical servers into VMs addresses some of the sustainability concerns faced by many organizations by "greening" their data centers to achieve significant energy savings. Each individual VM instance is commonly referred to as a guest, and the computer that runs all the VMs is known as the host.

In this way, the world of virtualization significantly reduces operating costs and allows greater business agility and scaling, as well as better data protection and improved compliance with industry and corporate standards. This type of architecture equips application managers with new **management** techniques and tools that lead to increased flexibility and control, help reduce downtime, and promise better usage efficiencies not normally possible in a nonvirtualized environment. The following sections will cover the various facets of virtualization that enable these huge savings in **total cost of ownership**.

SERVER VIRTUALIZATION

The most common aspect of virtualization is server virtualization. Now considered a mainstream technology, server virtualization benefits organizations by allowing server consolidation. A single physical server allows support for multiple VMs, which in turn allow support for applications that normally require dedicated servers. In this way, resources can be shared on a single server. Ultimately, this practice reduces unnecessary server hardware costs. It is no wonder that recent estimates show that most organizations have virtualized over half of their production workloads to facilitate the mobility of applications and application systems. Fig. 5.2 shows how applications and their underlying operating systems in a virtualized environment are completely independent of the physical host machine. In their new **configuration**, a layer of specialized software known as the VMM or hypervisor creates a separation layer between the applications and the underlying hardware. The hypervisor provides an **abstraction software layer** to disconnect direct reliance of the applications on specific hardware capabilities and communicates instead with the generalized virtual hardware interface in the hypervisor. This allows applications to run on literally any hardware system that can run the same hypervisor.

A key benefit on the server side of applications is that new **virtual servers** can be activated in hours, if not minutes, to meet the need for new applications or applications that require additional capacity.

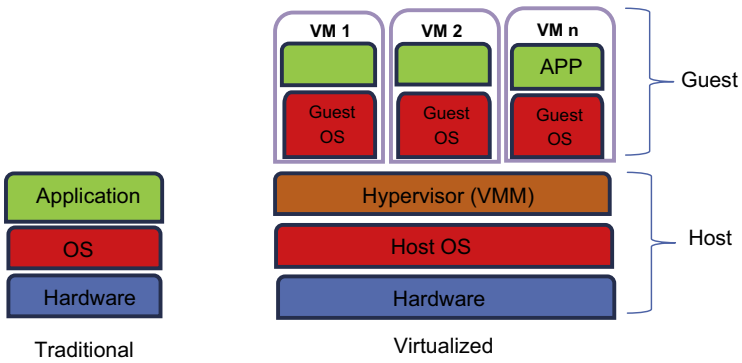

FIGURE 5.2

Comparison of traditional versus virtualized architectures.

Prior to virtualization, if a new application or an existing application needed more capacity, the only answer was to order new hardware and then physically install, test, and provision it. In some cases, this could take weeks or months. In a traditional IT architecture, it is not uncommon for an organization to be faced with the need to upgrade power requirements or build a new data center to meet their requirements. Neither option is easy, efficient, or inexpensive. With virtualized servers, these extreme measures are no longer necessary.

Applications that rely on specific hardware functions are less mobile than other applications that do not have hardware-specific feature dependencies. When applications need direct hardware access for performance reasons, those applications are also less portable. Virtualization can run most applications with little performance degradation, as if they were run natively on a server. However, it is best to avoid deploying applications with hardware-specific dependencies whenever possible.

Server and desktop virtualization also creates new ways to package, deploy, and manage applications. Single and multitier applications can be installed on a system with all of it dependent on libraries and **services**. A copy of that virtual disk image can then be saved as a file along with metadata about the image, which can be reused or cloned for future deployments.

Another advantage of virtualized servers is the ability to make a copy of the disk image of the system. This allows application managers to make a replica of a system, with all of its operating systems and application components that can be deployed when another VM instance is needed. These images may be in various formats, depending on the platform. For example, VMware uses virtual machine disk, Microsoft and others use virtual hard drive, and Amazon Cloud uses **Amazon Machine Image**.

A packaging format for these images called **open virtualization format (OVF)** was created to provide an industry standard to link to the VM image, along with **metadata** about the VM(s). For example, VMware packages their metadata in a VMX file that contains description and resources requirements for the disk image to be loaded and booted. In multitier applications, the metadata may include information about the machines like the sequence by which the machines should be started. Although these image formats are different, there are several tools that allow you to easily convert one format to another. And, although the conversion is not always perfect, it's close enough to get you going! In addition to the disk image format there is associated metadata (OVF will be covered in greater detail in Chapter 16).

Using metadata along with the disk images allows for a much quicker installation of new applications since disk images are distributed without running the install process and applications are often up and running in minutes instead of hours or days. Of course, there is a certain amount of configuration/customization that may need to be done before the application or application system is fully functional. This is normally done via some user prompts and configuration wizards. Many products today are delivered as VM images. This process also ensures that the necessary software dependencies were already installed at the appropriate level for the distributed application.

Virtualized server images are also used by **cloud** service providers to offer machine images or **templates**. These templates can provide prepackaged applications and services such as a web server, database server, or a load balancer. In this way, cloud server providers for either **public** or **private clouds** can offer their customers a comprehensive menu of preinstalled packaged application services for their use. Customers can also be assured that all the required components and dependencies were installed in the image. Templates also allow for version control of the applications and services. If and when newer versions of the software become available that are safer, faster, and provide the latest functions, templates also allow for control of end-of-life versions of the software.

APPLICATION VIRTUALIZATION

Application virtualization provides organizations with the best return on investment. Applications that are distributed across multiple **personal computers** present the single biggest problem for IT organizations. Preparing a complex application for deployment can take as much as 10 days; when there are hundreds of applications to manage, this can be a daunting task. As new versions of the application are released, the deployment process must be repeated ad nauseam. Instead of taking control of an application's Windows Installer-based installation, application virtualization grabs the running state and delivers it to each desktop. In essence, this means that applications no longer need to be installed because they can simply be copied. Any virtualized application will run on any version of Windows, so there is no need to revisit applications when they are moved or upgraded from one Windows version to another.

In addition to providing a single image that can be shared by many users, application virtualization also improves **patch management** of end-user applications and can eliminate the need for wasting hundreds, if not thousands, of hours upgrading systems.

A core concept of application virtualization is **application streaming**, or the ability to stream applications from a central point to multiple PCs. Similar to video or audio streaming, application streaming buffers content when an application is launched by a user and begins playing the selected content as soon as enough content is available. The rest of the application content is then delivered in the background. The beauty of application streaming is that the process is transparent to the end users.

Another concept that gained a lot of attention relative to virtualized applications is **ThinApp**. Developed by VMware, ThinApp encapsulates application files and registries into a single packet that can be easily deployed, managed, and updated independent of the underlying OS. With this approach, applications can be run on a physical PC, a shared network drive, a virtual desktop, or a USB stick without installing them on the local machine. This technique provides several features, including portability, reduced help desk costs, ease of updating, stronger endpoint **security**, and the ability to run multiple versions of the application on the same machine. This capability is now offered by a number of vendors and provides considerable cost savings, along with improved management and control.

All in all, virtualizing applications provides for greatly simplified application management by eliminating complex software deployment infrastructures and installation processes. It also provides an improved ability to customize individual user application delivery through a transparent **user experience**.

VIRTUAL APPLIANCES

One of the most efficient ways to deploy a server or test a server-based application is by using a **virtual appliance (VA)**. A VA fundamentally changes the way an application is delivered, configured, and managed. The VA is essentially a VM image (VMI), which is a large file that a VMM can use to create a VM that can be duplicated and moved between VMMs. In contrast to an application that is deployed in a nonvirtual environment, the focus of the VA is on the application. The VA includes a single application and its appropriate operating system, libraries, and services already configured and tuned for the specific application. This enables a user to simply download a single file to run an application. VAs can be open or closed. A **closed VA** is always packaged, distributed, maintained, updated, and managed as a single unit. An **open VA** allows customers to make modifications. Some examples of VAs include **WAN** optimization controllers, application delivery controllers, **firewalls**, performance monitoring solutions, enterprise applications, and web applications.

From a management perspective, there are a number of important benefits to be gained from using VAs. These include the following:

1. Significant reduction in application deployment time because the focus is on the application. The VMI incorporates everything necessary to run the application in a virtualized environment. It is configured and tuned for the specific application, streamlining its deployment.
2. Reduced resources required for maintenance. There are less services and drivers to maintain, fewer patches to keep the operating system up to date, less bandwidth, and less storage requirements.
3. Reduced cost of deploying a software-based VA compared to its nonvirtual, hardware-based counterpart.
4. Greater economies of scale when a VA is deployed to multiple individuals by eliminating the need to expend necessary costs to acquire additional hardware-based appliances.
5. Problem solutions associated with heterogenous hardware and operating systems by focusing on the application prepackaged with its single appropriately configured operating system.
6. Facilitated management of network applications by deploying and managing VAs at remote sites where there are limited resources.
7. Accelerated evaluation of new applications. Vendors offer a VA with a new application preinstalled on its appropriate operating system.

VIRTUAL DESKTOP INTERFACE

Another important aspect of application virtualization is the **virtual desktop interface (VDI)**. Desktop virtualization focuses on centralizing the management of complete desktops or individual desktop applications. This centralization process simplifies management operations by allowing IT organizations to

perform maintenance across various virtualized desktops. The two primary forms of desktop virtualization include client-side application/desktop and server-side application/desktop.

Client-side application virtualization focuses on allowing applications to be streamed on-demand from central servers by a client's device. The primary challenge of managing desktop virtualization is acquiring and maintaining optimal bandwidth to achieve a good user experience. Alternatively, in server-side virtualization, a client's device acts as a terminal that accesses an application or desktop hosted on a centralized server. This method can be achieved in one of two ways: a server-based computing or virtual desktop infrastructure (VDI).

While the cost of traditional PCs and storage has decreased, the operational cost of managing individual physical desktop computers increased due to rising labor costs and the escalating complexity associated with maintenance of individual physical PCs. Implementing VDIs reduces this total cost of ownership since users connect using just a keyboard, monitor, and mouse connected to the hosting virtual desktop server via PC over IP. Overall, the management of the physical PC lifecycle consumes a large amount of IT resources, whereas a VDI solution can shortcut and even eliminate many of these desktop management tasks, thus significantly reducing the associated operational costs. It also provides a much more streamlined application management approach by centralizing all management tasks. In a large company, these savings can be multiplied by hundreds or thousands of users, resulting in huge savings. In addition, a VDI greatly reduces security risks and the power and cooling requirements of the enterprise.

The virtualized desktop enables a broad range of **mobile devices** to allow users to launch their applications safely and securely on smartphones and tablets, and accommodates the seamless integration of cloud-based applications. Mobile and cloud-based applications are discussed further in Chapters 4 and 6.

NETWORK VIRTUALIZATION

To avoid the complexities of traditional network configuration and provisioning and fully realize the benefits of virtualization, a virtualized network must be used. Traditional networks simply cannot withstand the strain placed on them by the increasing demands of applications, servers, and the large bandwidth requirements of virtualization. With a virtualized network, the same agility, reduced costs, and business continuity that were enabled in the hardware/software environment by server virtualization can be realized.

In many organizations, nonvirtualized networks are still anchored to the hardware and their configurations are spread across multiple physical and virtual network devices. Despite IT's ability to deploy virtual applications within minutes, a network can delay their use for days or weeks. This growing demand to provide multiuser network services that enable each user to specify, deploy, and control their own virtual network presents a golden opportunity to revise network management strategies, making sure that the complexities and failings of the traditional network are not repeated in the virtual network. For example, the focus must be on required network functionality rather than on infrastructure configuration and control.

As with other virtualization offerings, the virtual layer must be decoupled from the infrastructure and be efficient, scalable, and highly available. It is also important to consider the dynamic nature of **virtualized data centers** where endpoints are created, deleted, and migrated. Some recommend the

development of network blueprints to determine and verify the network functionality specifications and allow the complete application lifecycle to be managed independently of the endpoint lifecycle.

STORAGE VIRTUALIZATION

Legacy storage systems are ill-suited to meet today's business needs. Deployed in storage silos, these systems do not have the ability to fully address virtualization needs or to deliver economies of function and scale in modern data centers. To capture new data from various media sources, such as mobile, social media, and the cloud, IT managers need a storage architecture that is scalable, focuses on business-critical workloads, and offers lower storage total cost of ownership (TCO). To harness and manage all of this, new data managers are turning to storage virtualization strategies. These strategies enable them to save money on basic storage functions, apply those funds to new business-critical workloads, and take advantage of its capability to enhance data analytics functions by dynamically moving data from system to system.

Storage virtualization achieves these benefits by pooling physical storage from multiple network storage devices into what appears to be a single storage device that is managed from a central console. Converting to virtualized storage helps solve a number of storage-related problems such as improving capacity utilization to improve the 40–50% capacity utilization rates that are typical in most IT organizations. This benefit is amplified in situations where storage is mirrored to other sites. Storage virtualization can also facilitate disaster recovery efforts by replicating data without having to provide a matching host or disk at the disaster recovery site. It can also eliminate bottlenecks created by communication between agents on the application server and the backup server by taking a snapshot of a file system, thus eliminating the need for a backup window and simplifying the management of storage throughout the application management lifecycle. These snapshot capabilities provide online data copies that allow the system to roll back to a time before file corruption or loss occurred. Other benefits of virtualizing storage include:

- Faster data migration between heterogenous platforms
- Automatic capacity expansion
- Easier and safer application testing using a replicated data set
- Improved database performance by sharing an expensive solid-state disk
- Higher availability by separating the application from its data storage to insulate an application from its server failure

Storage virtualization also helps the storage administrator perform the tasks of backup, archiving, and recovery more easily and in less time by disguising the actual complexity of the **storage area network (SAN)**. Users simply implement virtualization through software or hybrid hardware/software appliances on different levels of its SAN.

SERVICE VIRTUALIZATION

The last piece of the virtualization collage is **service virtualization**. This facet of virtualization increases agility throughout the **software development lifecycle (SDLC)**, which allows for the testing of interconnected applications earlier in the development process, enables faster deployment of higher quality

applications, and reduces project risk. It is particularly useful if there are complex applications with multiple dependencies. With its ability to simulate complex test environments, service virtualization is truly a game changer that drastically improves the way software can be managed throughout its lifecycle.

The goal of an IT manager is to deliver high quality, high performing applications on time and under budget. Service virtualization moves this goal closer to reality by reducing testing bottlenecks. It achieves this by emulating unavailable application components to allow end-to-end testing of the application as a whole. By using these **virtual services** instead of production services, testing can be done earlier and more frequently throughout the SDLC. These virtual components can be constructed by monitoring the network traffic of the service or by reading service specifications that describe the operations offered by a service, including the parameters and data outputs. In this way, service virtualization can dramatically alter the economics and flow of the entire application lifecycle.

Let's face it: most applications have "bugs" when they are released—it is a fact of life in the IT industry. However, the later in the application lifecycle that these defects are found, the more expensive they are to fix. By using service virtualization, organizations can identify problems and fix them with fewer consequences to timelines and budgets by testing frequently throughout the process. Service virtualization can also be used to fix defects. If a defect is found in testing, it can block the application from performing properly. However, service virtualization can be used to emulate its correct functionality so that further testing can proceed. It is best to begin using service virtualization incrementally to realize "quick wins," for example, virtualizing components that are the most stable and the most expensive to test. Next, ask these questions to determine the need for service virtualization:

- How much downtime does the development team experience during testing because they cannot access dependent system components?
- How many dollars does this downtime represent?
- How often is access to third-party interfaces needed prior to scheduling a test?
- What are the costs associated with gaining access to third-party interfaces?
- How many defects are typically found in the various stages of the SDLC?
- What is the cost of resolving these defects?
- What is the cost of customer dissatisfaction due to these defects?

Next, consider the costs that will be incurred to implement service virtualization, e.g., software licenses, implementation costs, and training costs to bring developers up to speed on the new tools. A comparison of need versus costs, particularly for those organizations that struggle with testing complex applications or are dependent on third-party services, can result in significant cost savings. It is easy to see why a growing number of organizations have made service virtualization a key part of their testing strategy throughout the application lifecycle.

VIRTUAL INTEGRATION

The most effective way to manage virtualization is to adopt an integrated, full-stack approach. This was initially addressed by the notion of **converged systems**, which emerged as a way to easily handle individual components of hardware setups. The range of hardware pieces controlled in a converged infrastructure generally consists of servers, networking equipment, and storage devices. A converged infrastructure can be likened to a number of components networked together topped by a management layer.

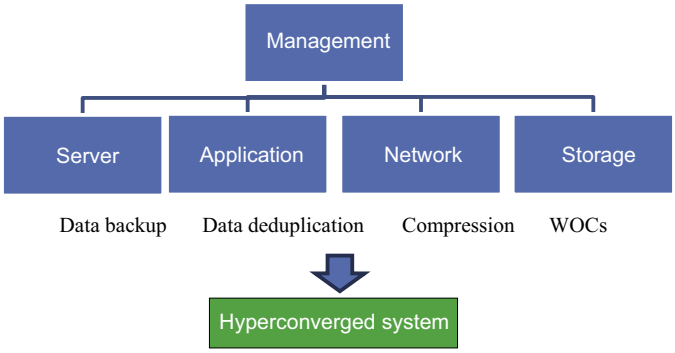

FIGURE 5.3

Virtualization integration through hyperconvergence.

However, greater efficiencies could be gained from streamlining IT architectures even more by integrating not only compute, storage, and management, but also compression, data deduplication, data backup, and WAN optimization through the higher concept of a **hyperconverged system** (see Fig. 5.3). Hyperconverged systems and converged systems are similar in many instances, but hyperconvergence increased the integration of IT resources to enable easier and more comprehensive management.

Hyperconverged systems rapidly gained momentum and acceptance as a way to address VM sprawl caused by incremental adoption of virtualized servers, applications, networks, and storage services. To simplify the operational issues related to this siloed approach to virtualization, a converged infrastructure evolved as multiple vendors combined their technologies into an integrated full stack containing servers, storage, and networking.

Hyperconverged systems advance the integration concept even further by combining the physical components of servers, storage, and networking into a single form-factor server that uses direct-attached storage in place of more expensive SAN-based storage. A natural progression in virtualizing IT could be to follow server virtualization with a hyperconverged approach as the standard for deploying new workloads. Hyperconverged systems can be delivered as **appliance-based systems** or software-only systems. Appliance-based systems are delivered as a VA that contains both hardware and software. Software-only systems are just that: software with no hardware. If an organization has a good relationship with its hardware vendor, a software-only system on existing hardware may be ideal. The downside is that diagnosing specific problems may be more difficult than if the hardware and software were deployed as a single unit.

The benefits of hyperconvergence include reduced operating costs and time to market, enhanced flexibility, and better application performance. For example, a hyperconverged system can be installed and spun up in less time than a large-scale virtual server solution. This is particularly appealing to smaller organizations that do not have experienced staff to carry out the installation. From a cost perspective, although hyperconverged systems are not significantly cheaper to deploy than a custom virtual server system, operating them definitely is. This is typically where significant cost savings can be realized. Managing a hyperconverged system is definitely easier thanks to vendors that improve monitoring functions to facilitate proactive support for their products. Whether organizations are just embarking on a virtualization exercise or have one well underway,

hyperconvergence can help. For small organizations just beginning the virtualization journey, it represents an easy, inexpensive way to update all data centers simultaneously. For larger organizations, hyperconvergence can address costs and complexity of storage and data protection as the organization progresses through the different facets of virtualization.

VIRTUAL MACHINE MIGRATION

The movement of VMs from one resource to another, such as from one physical host to another physical host, or data store to data store, is known as VM migration. There are two types of VM migration: cold and live. **Cold migration** occurs when the VM is shut down. **Live migration** occurs while the VM is actually running. This amazing new capability is particularly useful if maintenance is required on the part of the physical infrastructure and the application running on that infrastructure is mission-critical. Before the availability of live migration applications, managers were stuck with the choice of either causing a planned outage, which in some global corporations is not always feasible, or waiting and not taking the system down, which risks an unplanned outage in the future. Needless to say, neither of these choices is optimal.

With live migration, a running system is copied to another system and when the last bits of the running system's state are copied, the switch is made and the new system becomes the active server. This process can take several minutes to complete, but is a great advantage over the two previous options.

Earlier versions of live migration were limited to moving VMs within the same data centers. That restriction was removed and it is now possible to perform live migrations between different data centers. This capability provides an entirely new set of options and availability, including the ability to move workloads from a data center that may be in the eye of a storm to another data center outside of the target area. Again, these application moves can be accomplished without any application outages. There are several products on the market today that provide some form of live migration. These products and platforms may have some guidelines and requirements to provide the capability. If an organization is considering live migration as an option, it is recommended to check with the virtualization software vendor to understand those requirements, particularly for the data center.

WORKLOAD BALANCING

Virtualized applications and servers provide a new level of mobility. Virtualized servers can be moved in a live migration mode as described earlier, or they can be moved in a stopped state. It is always good to remember that a physical server may have 20 or more virtual servers running on it. With live and static migrations, VMs may be moved to provide a workload balance. For the sake of example, let's say that a physical web services application server has 10 highly busy VMs running, and a physical line-of-business application server has little or no activity on the VM that it is hosting. In this case, it would make sense to move some of the workloads from the web services application server to the line-of-business server to balance the workload.

SCALING USING VIRTUAL SYSTEMS

One of the great things about virtualized systems is that it is not necessary to order lots of new hardware to gain increased capacity. Instead, a copy of the application server(s) can be made to easily and quickly deploy one or more additional servers. Cloning an existing VM saves time and reduces the amount of errors that may occur if each machine is created from scratch.

Those new machines can be spun up and—with the help of a load balancer—can quickly add capacity to an application. There are several tools and types of clones, but the basic idea is to create multiple instances of an application and then use some sort of load balancer to distribute the requests to a pool of servers. As there are different types of clones, there are also different types of load balancers. Some allow the selection algorithm criteria for the load balancer to be configured using a round robin approach to limit the time each process can run, or by sending the request to the server with the least number of current connections. Of course, it is important to make sure the parent of the clones was configured for optimum performance. Whatever inefficiencies were in the clone parent will be propagated to the child clones.

One other great advantage to scaling in this fashion is that when it is time to upgrade the server image, operating system, application software, or the configuration, it could be done to one server, then tested and then cloned again and replaced on the existing running images.

IMAGE CHECKPOINT AND ROLLBACK

Another nice facility provided by most virtualization vendors is the ability to create a checkpoint for a VM. This is a handy capability for developers when making changes to a VM, as it allows the developer to roll back the image to a previously known image without having to keep an entire copy of each image. A VMI can be several gigabytes in size, so creating a backup every time a change is made would require a lot of disk space. With check pointing, the system stores only the deltas of the change so it can roll back an image quickly and easily. This technique can also be used when making complex changes to a production server.

CHALLENGES OF MANAGING A VIRTUAL ENVIRONMENT

While virtualization solves some problems and offers amazing capabilities, it also intensifies some traditional application management challenges and creates several new ones.

SECURITY

Security concerns are consistently identified as one of the top five issues for senior-level IT managers and the security of virtualized servers, and infrastructure is high on their list of security concerns. Although a virtualized infrastructure is not inherently any less secure than that of a traditional infrastructure, it still has to be patched and maintained in the same way that a nonvirtual infrastructure does to keep abreast of potential vulnerabilities. As discussed earlier, virtualization adds an additional layer

(VMM or hypervisor) between the operating system and the applications to manage multiple VMs on a single host, and it is theoretically possible for hackers to attack the VMM specifically or hijack a VM and use it to attack other VMs. While there are security risks associated with the VMMs beyond accepting vendor patches and keeping VMMs maintained, these VMs are primarily reliant on vendor support to keep them secure. However, there are also a number of other server and network virtualization security issues that can and should be controlled by IT departments. Let's explore some of these virtualization security issues now to understand how they can be managed.

Host/platform configurations. In the case of virtual servers, configuration issues are magnified. The host platform can vary in the type of configuration options, depending on system architecture. To secure these systems, a number of best practice configurations can be implemented, such as setting file permissions, controlling users and groups, and synchronizing logs and times. To assist with this, a number of configuration guides are available free of charge from virtualization platform vendors, the Center for Internet Security, the National Security Agency, and the Defense Information Systems Agency.

VMM or hypervisor security. The VM manager is a piece of software. Since software is often released with "bugs" that need to be patched and maintained, it is important to maintain the latest service packs for both guests and hosts in a virtualized environment. This action is necessary to guard against any vulnerabilities and to apply the latest security roll-up patches if and when a virtual software vendor supplies them.

Least privilege controls. Creating separation of duties and providing the least amount of privilege necessary for users to perform their authorized tasks are basic tenets of information security that apply to both physical and virtual resources. For example, the director of marketing would not need access to a VM that runs a payroll application.

To address this issue, a system of checks and balances with processes to split functions and enforce dual controls for critical tasks must be put into place, and approval processes should be set up for creating new VMs and moving new applications to new VMs. Audit logs for VMs should be monitored for usage activity in the data center and on the endpoints. VMware monitoring tools that also monitor in nonvirtual environments to compare and report performance, per the least privileges policy, are also useful. Additionally, so are host-based firewalls and host intrusion prevention tools. To maximize the success of least privileges controls, it is important to involve all stakeholders in defining access levels and allocate access to specific roles, rather than individuals, and establish an annual review process to check that access levels remain consistent with business needs.

Failure to integrate into application lifecycle management. Managing vulnerabilities and patches across virtual systems can cause problems, and so can failing to conduct system integrity checks for a virtual system. However, with the appropriate combination of controls, you will be able to manage VM lifecycles more easily than their physical environment. An easy fix for this is to deploy appropriate tools that have these management capabilities. VMware vendors and third-party tools scan for weaknesses in VMs and work independently of and with the VMM.

Raising IT staff awareness. If IT staff do not know about an issue, they cannot manage it. Internal and external IT auditors need to be provided with a complete understanding of the virtualization infrastructure deployed, the data within the systems, and the policies that are put in place to govern the lifecycle of system instance creation, use, and end of lifecycle. Assessment of risk, compliance with relevant regulations, and even software licensing agreements are impacted when new VMs are dynamically deployed, temporarily retired, or eliminated. Traditional approaches to risk assessment and analysis, such as assessment questionnaires, may be inadequate in a virtual environment.

Risk must be assessed and analyzed at the onset of new virtualization projects, and risk management staff must be involved with changes in the virtualization infrastructure that may affect the level of risk. Educate risk management and compliance groups about virtualization capabilities and limitations, and consider involving compliance staff in critically shaping security policies for the virtual infrastructure in accordance with relevant regulations.

Traffic monitoring. One of the biggest security issues that may be faced in a virtualization environment is the lack of visibility into traffic among guests. Unlike the physical computing environment where a host platform has an internal virtual switch that each guest connects to, in the virtual environment, all VM traffic on a host is contained entirely within the host's virtual switching components. This severely compromises visibility and security. To get around this, mirror ports need to be created on the built-in Layer-2 switching controls that are provided by most virtualized solution vendors to monitor traffic.

Controlling user-installed VMs. Central IT staff may not recognize the existence of VMs on endpoint systems. Even if they do, there may not be any policies in place to control the use of these technologies by end users. Licensing and patching issues may also need to be resolved and appropriate policies instituted to address desktop applications on virtual endpoints that may be operated by unsophisticated users.

In anticipation of (or in response to) user-installed VMs, a new set of management capabilities should be created that allow IT desktop support, security operations, and help desk staff discover virtualization in use throughout the organization's endpoints, set and monitor policy, and gain visibility into the status of VMs running on desktop systems. An internal usage policy and network and endpoint security should be established that are VM-aware enough to locate and identify VMs and report them. To enable this visibility and control, endpoint security management needs to develop discovery protocols for virtual systems running on endpoints.

Lack of integration with existing tools and policies. Many common practices used in securing physical servers, such as hardware firewalls and intrusion sensors, either are not available or are extremely difficult to configure in virtual environments because the data is crisscrossing a system backplane, not an IP network. Unfortunately, hardware security tools that work in physical environments do not always work smoothly in a virtual environment. Instead, careful network configuration is required to help to avoid security issues related to VM failures, maintenance issues, and application removal. The good news is that security and network management vendors are moving to make their tools virtual-aware. To guard against some of these security issues, it is advisable to mirror standard security software including antimalware, host intrusion prevention, endpoint security software, and host firewalls on the VMs. Remember, a good number of traditional security and management vendors are adding functionality that addresses virtualized resources, so it is important to evaluate options for deploying system and file integrity tools, intrusion prevention systems, and firewalls as VAs with a vendor before purchasing new tools. Partnerships also enable maximum coverage at minimal cost.

DISASTER RECOVERY

It is necessary to have a disaster recovery plan to address a major outage in the data center. Before virtualization, applications were more hardware-dependent. Often, duplicate equipment would need to be purchased and staged in another location. Virtualization reduces the hardware dependencies for most applications and provides cost-effective disaster recovery site alternatives.

It is imperative for a good disaster recovery plan to be developed, regularly tested, and updated as new applications and technologies are deployed in the data center. Application managers need to ensure there is a plan in place and that mission-critical applications are part of the plan and tests. Virtualization greatly reduces the amount of work involved to make the backup and to activate it in the case of a disaster.

When any changes to the application systems and/or VMs are made, they need to be backed up and ready for deployment at the disaster recovery site. One of the challenges in restoring systems to a backup site is the time and effort involved in deploying and configuring data storage, networks, and correct versions of the machine images. A good disaster recovery plan and regular testing will greatly reduce the amount of downtime that may occur in the case of a disaster. In other scenarios, such as a data center in the path of a hurricane, the disaster recovery plan must be executed even though the data center is still functioning. In other scenarios such as an earthquake, there may not be time to prestage the disaster recovery site and the recovery could take more time.

The bottom line is that even though virtualized systems provide some handy ways to clone and move workloads, effective disaster recovery starts with good planning and requires constant testing and updating.

AVAILABILITY

Unlike traditional IT, virtualization relies on network connectivity and a centralized infrastructure in which numerous end users, from front-end connection brokers to back-end servers, share the same application and desktop delivery infrastructure. Consequently, while the failure of a physical desktop PC or application impacts only one user, a failure within the shared infrastructure of a virtual application and desktop deployment can impact the entire user population. To avoid this, the infrastructure design must protect against potential site-level outage failures, as well as individual component failures.

SCALABILITY

One of the main issues faced by application managers is VM sprawl, which can occur when administrators create VMs without regard for the resources the VMs consume or the possibility of overwhelming the host server's resources. The phenomenon of virtual sprawl introduces new management challenges as more and more VMs are created, and tracking VMs and their consumption of resources throughout their lifecycle become more difficult for the application manager. This issue is akin to discovering and monitoring applications in a traditional IT environment, but on a much larger scale. As systems can easily be created and cloned, the actual number of new servers, both virtual and physical, are constantly expanding. Therefore tracking, monitoring, and retiring servers is a constant challenge. The combined proliferation of virtualized servers, VMs, and **VLANs** places a significant strain on the manual processes used to manage physical servers and the supporting infrastructure.

To prevent VM sprawl, organizations should develop a **virtual machine lifecycle management (VMLM)** plan to empower administrators to oversee implementation, operation, delivery, and maintenance of all VMs throughout their entire lifecycle. A VMLM ensures accountability for the creation of each VM, monitoring throughout its lifecycle and systematic decommissioning at the end of its lifecycle.

PERFORMANCE MONITORING

Other traditional management challenges that are magnified in a virtual environment include **performance baselining**, **application profiling**, and response time analysis. All these activities are important because they help detect and resolve performance issues before they impact an organization's end users by providing a reference point to measure service quality and application delivery effectiveness. They also lead to an understanding of how critical applications are behaving. In a virtual environment, this becomes even more critical since the systems are less visible and are more difficult to track.

STORAGE ACCESS

While live VM migration can add significant value, it can be challenging to ensure that the VM retained the same level of storage access. Tracking the location of VMs and associated shifts in network traffic add even more complexity to the troubleshooting process and significantly complicate it.

LEGAL

Another important issue that requires close monitoring is tracking license entitlements for the ever-increasing number of servers and applications. Failure to do this can create a huge liability with fines and legal action if license entitlements are exceeded. Fortunately, there are a plethora of tools that can assist with managing virtualization deployments and the associated security risks.

SUMMARY

Virtualization adds a great deal of tools and capabilities as well as some unique challenges. Leveraging these technologies, taking advantage of new mobility, and scaling capabilities can improve application performance and uptime. Understanding this technology will help organizations be aware of some of the pitfalls to avoid. In the following chapters, we will build on the virtualization concepts as we take a look at **application lifecycle management** in **containerization** applications, cloud, mobile, web-based, componentized, and **agile** computing.

KEY TAKEAWAYS

- Virtualizing applications makes it easier to manage the application lifecycle while providing a transparent experience to end users.
- Virtualization overcomes the dependency on operating systems.
- Server virtualization addresses the gross underutilization of server capacity and enables IT managers to better manage their budget.
- VM sprawl can be controlled by implementing a VMLM plan.
- Virtualization has evolved from simple server virtualization to hyperconverged systems to streamline the process for companies of all sizes.
- Hyperconverged systems are useful to small organizations that are just embarking on their virtualization experience and to large organizations that are in the midst of virtualization, but are experiencing some issues.