Realtime publishers

The Definitive Guide™ To

Virtual Platform Management

sponsored by

Anil Desai

Chapter 8: Virtualization Policies and Processes....165
The Need for Policies and Processes....165
Aligning IT and Business....165
Understanding Processes....166
Understanding Policies....167
Benefits of Policies and Processes....167
Defining Roles and Responsibilities....168
Virtualization Management Issues....169
Managing Virtual Machine Deployment....170
Developing Virtual Machine Deployment Processes....170
Implementing Configuration Management....171
Standardizing Virtual Machine Configurations....171
Implementing a Quality Assurance Process for Virtual Machines....175
Managing Virtual Machine Placement....176
Implementing Data Protection Policies and Processes....177
Determining Recovery Requirements....177
Identifying Important Data....178
Implementing Backup Processes....178
Performing Guest-Level Backups....178
Performing Host-Level Backups....179
Choosing Storage and Backup Destinations....179
Developing Backup-Related Policies....180
Developing Virtualization Security Policies....180
Virtualization Security Benefits....180
Virtualization Security Risks....182
Security Policies for Protecting Virtual Infrastructures....182
Policy and Process Best Practices....185
Identifying Overall Goals....185
Identifying Process Candidates....185
Keeping Policies and Processes Up to Date....186
Automating Policies and Processes....186
Summary....187

Copyright Statement

Chapter 8: Virtualization Policies and Processes

The focus of this chapter is on identifying the benefits of implementing policies and processes in IT environments that have deployed virtualization technology. Although some of the same standards designed for physical machines still apply, virtualization also brings some unique concerns and considerations. After enumerating benefits of policies and processes, I'll present specific ways in which policies can help. The areas of focus include deployment, configuration management, security best practices, and data protection. Finally, I'll conclude with best practices for enforcing policies and processes in a busy IT environment.

The Need for Policies and Processes

Some of the benefits of virtualization are undeniable—simplified manageability and decreased costs usually top the list. In some cases, however, technology can make tasks "too easy." For example, users and systems administrators may be able to create and deploy new virtual machines without the benefit of careful configuration reviews or oversight from IT staff. The virtual machines could contain any of a wide variety of guest OSs. Compare this with the process of deploying physical machines: IT is usually responsible for purchasing equipment, configuring it according to best practices, and deploying it to the data center. Deployment, along with a long list of other concerns, raises the importance of establishing policies and processes for organizing IT operations. This section focuses on ways in which organizations can benefit from implementing policies and processes and how they can implement them.

Aligning IT and Business

A common challenge faced by many organizations is that of keeping IT departments aligned with the rest of the enterprise. In the past, it was common for technology departments to work in a vacuum, and only on internal projects with low visibility. As technology has taken on a strategic role for most companies, it's important to ensure that all areas of the organization are coordinated in their goals. The direct benefit is that the entire enterprise will be able to identify those initiatives that can provide the most positive impact to overall operations. Successful policies and processes extend beyond the borders of the data center and need to involve representatives from throughout the organization. For example, when defining a process for deploying virtual machines, IT managers should work with business managers to determine acceptable timeframes for the steps that are required. Steps might include determining which applications and OSs are supported, along with ways in which configurations can be customized.

Understanding Processes

A process can be defined as a set of tasks or actions that is designed to meet a specific goal. Often, a process defines the roles and responsibilities of the individuals involved, along with rules for how they should interact. Figure 8.1 provides an example of the types of steps that might be included in a change management process that involves reconfiguring virtual machines. The actual change that is requested can vary from the relatively simple (such as increasing the amount of memory that is allocated to a virtual machine) to more complicated (for example, moving a workload or making copies of a production virtual machine).

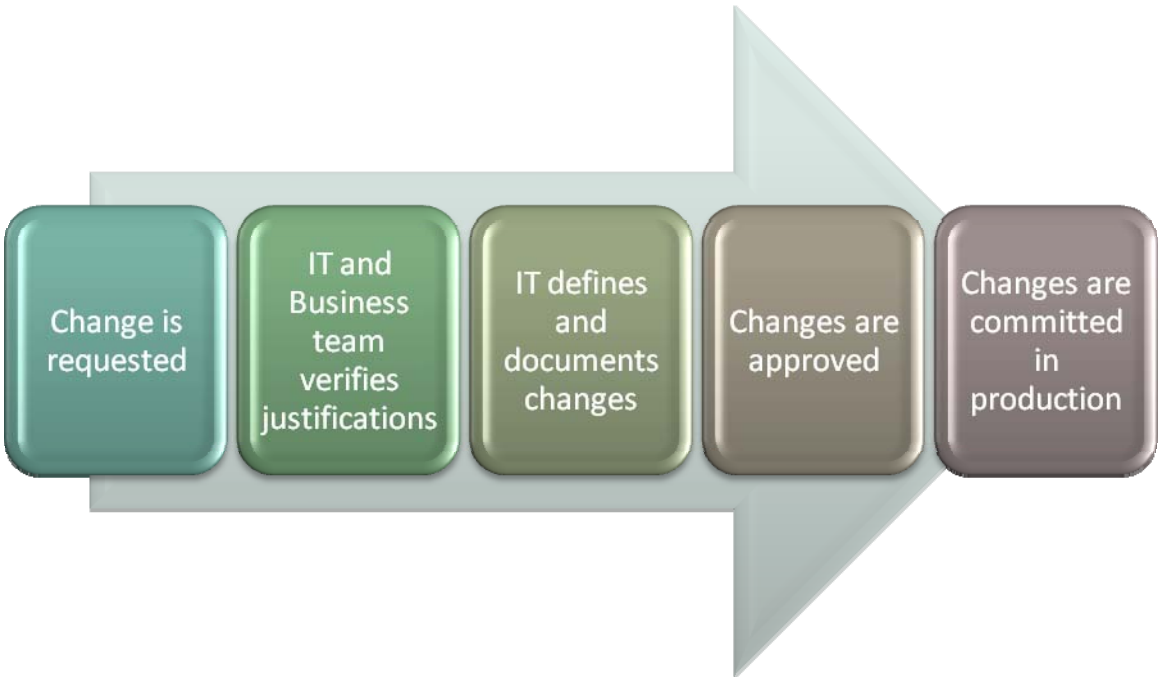

Figure 8.1: An example of a change management process for virtual machines.

The process begins with a change request that is usually generated by a business unit or a potential user of the virtual machine. The request is then reviewed by a team of business and technical staff that has the authority to determine whether the justifications are in line with the entire organization's goals. Issues might include technical considerations (such as host resource capacity and availability) and business requirements. Assuming that the configuration change is approved, IT staff can begin to create and configure the virtual machine based on requirements. An important step prior to deployment is for the IT department to ensure that the configuration meets the requirements defined in policies. Specific considerations might include validation of security settings and ensuring that all applicable patches and updates are installed. Finally, the change is committed in the production environment. Overall, the steps in this process prevent important technical and business tasks from being overlooked.

Understanding Policies

With respect to IT organizations, a policy is used to define rules related to various tasks and operations. Policies include details about which actions can be taken and who can perform the actions. They can also be used to specify standards for areas such as security and configuration management. Many IT organizations have numerous staff members that have overlapping permissions. When guidelines and responsibilities are not clearly defined, it is difficult for the team to consistently perform critical tasks. The same applies outside of IT—without policies in place, the rest of the organization will have a difficult time determining what exactly to expect.

Benefits of Policies and Processes

Many IT environments work in an ad-hoc and reactive fashion. A loosely defined process might involve a business manager's direct request to a systems administrator for more resources. The administrator would then provide the resources, without oversight from the rest of the organization. The end result is that new deployments might not completely meet business and technical needs or be aligned with the organization's overall strategic goals. A much better approach would involve input from throughout the organization and would include well-defined steps that should be followed to ensure consistency and quality.

Policies and processes take time and effort to implement and enforce. In some cases, completing an entire process (such as a simple configuration change) can take as little as a few minutes to complete. For example, if relevant personnel are all present at a meeting, the added time for approvals might be negligible. However, in dynamic environments that routinely work with configuration change requests, the process might add a noticeable delay. Therefore, it is important to recognize that there is a potential cost that must be considered when instating new rules or procedures.

The primary benefits of implementing policies and processes are consistency and repeatability. Performing the same tasks in the same way helps identify potential problems and areas for improvements in efficiency. When compared with ad-hoc methods in which every systems administrator performs tasks in their own way, this provides tremendous benefits. For example, when all system configurations are compared with a well-defined security policy, the IT team can be assured that new deployments adhere to the organization's best practices.

In addition, there are staffing advantages: When operations are well documented, the need for specialists for each of the types of guest and host OS (and the virtualization platforms they're running) is lessened. The end result is that even IT generalists and systems administrators are able to meet the operational needs of a virtualized infrastructure. Finally, a common cause of downtime and data loss issues is related to human error or a lack of coordination. Environments can minimize risks related to changes by ensuring that the necessary approvals and oversight are implemented as part of a well-engineered process.

Defining Roles and Responsibilities

An important characteristic of well-defined policies and processes is the inclusion of roles and responsibilities. Figure 8.2 shows an example of a process that includes details related to which people are responsible for each step.

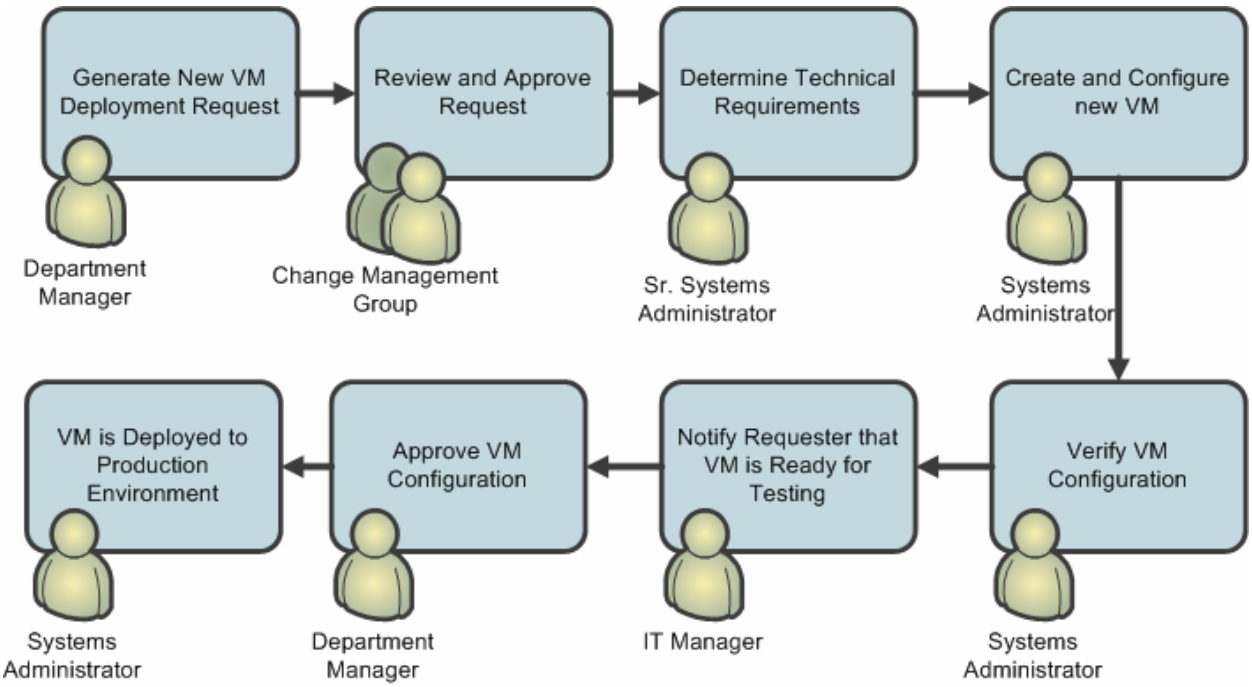

Figure 8.2: Defining roles for a virtual machine deployment workflow.

At any given point in the process, it is clearly known which groups or individuals are responsible for completing a task. These are the "owners" of the overall process at that point in time. More complex processes might include branching paths and cycles that involve additional reviews prior to ultimate deployment. The most important point is that, at all given steps, responsibilities are clearly identified.

Virtualization Management Issues

So far, the chapter has focused on the details and benefits of implementing policies and processes in general. Although these approaches apply directly to all aspects of an IT department, the deployment of virtualization raises some unique challenges. Figure 8.3 provides an overview of the issues that IT organizations must consider.

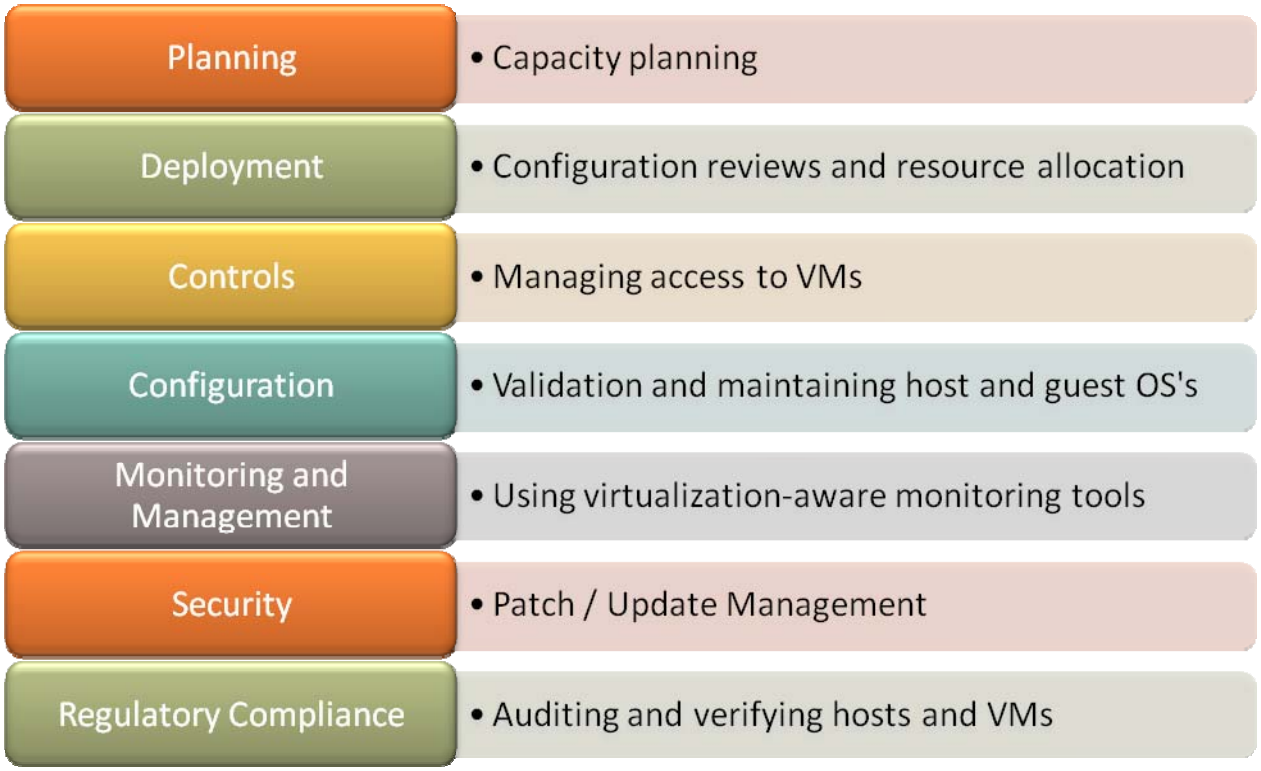

Figure 8.3: Potential challenges related to managing virtual environments.

These challenges affect all areas of the standard management life cycle for virtual machines. Considerations start with planning and deployment—determining where and when to use virtualization. Once virtual machines are in production, it's important to monitor and validate configurations to ensure that they adhere to best practices. Security and regulatory requirements force administrators to keep their systems up to date and to perform regular audits of their systems. There are other considerations that should be kept in mind, as well. For example, IT departments will often find that they are supporting a wide array of guest OSs, each of which must be appropriately managed in a production environment.

All of these areas of the management life cycle can be addressed through the use of policies and processes. In the remainder of this chapter, I'll present examples and details.

Managing Virtual Machine Deployment

Left unmanaged, many organizations find that they are suffering from a problem known as "virtual machine sprawl"—the rapid proliferation in the number and types of virtual machines that IT must support. The deployment phase is one area in which IT organizations can often dramatically improve the manageability of their environments. This section presents ways in which policies and processes can help.

Developing Virtual Machine Deployment Processes

To ensure that new virtual machines meet the IT organization's standards, a deployment process should be developed. Figure 8.4 provides an example of typical steps that are included.

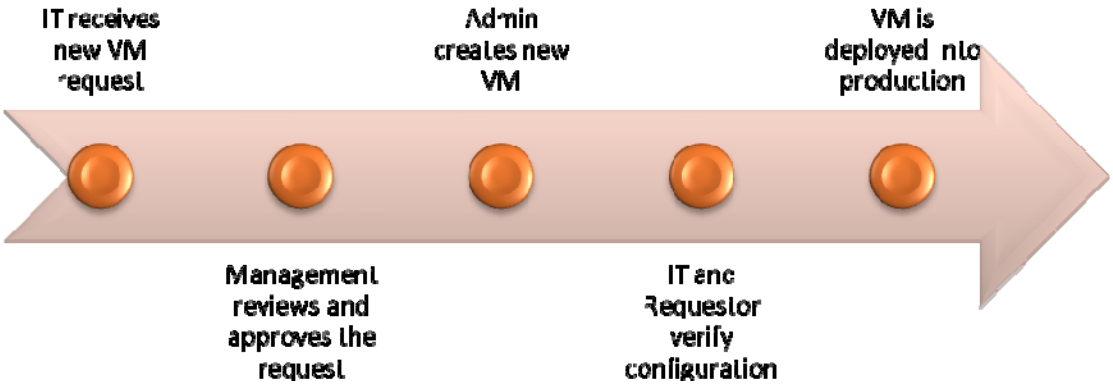

Figure 8.4: A process for new virtual machine deployments.

The process begins with a new deployment request that originates from a business manager, end user, or other department leader. In some cases, additional capacity is needed to support new applications. In other cases, systems might be used for test and development purposes. The request is then reviewed by a team that includes business and technology managers. It's possible that changes to the request will be made at this time in order to adhere to IT or business policies. Once the request is approved, technical staff can create the new virtual machine based on best practices. Prior to deployment, it is important for systems administrators and the original virtual machine requester(s) to ensure that the virtual machine meets the requirements. Assuming it does, the new virtual machine can be deployed into production.

Although the overall process might result in some deployment delays, the benefits usually outweigh the inconvenience. For example, the process requires business and IT representatives to verify that the configuration meets their needs, thereby reducing additional work that must be performed to fix configuration errors. The steps place technical responsibilities in the hands of the experts (the IT staff), while ensuring that business stakeholders are involved.

Implementing Configuration Management

In the world of IT, complexity often leads to management issues. Virtualization technology allows users and systems administrators a significant amount of freedom related to what their virtual machines contain. Most IT organizations have standard configurations that are supported on their physical machines. These requirements are driven by hardware compatibility and supportability concerns. Most virtualization platforms, however, have the ability to support hundreds of different OS versions. And many OS platforms include various versions and update levels. This resulting diversity, along with the ease of deployment, can make it very difficult for IT departments to ensure that their systems meet security and regulatory compliance requirements. In addition, providing support for a broad array of different systems is beyond the expertise of most systems administrators. Fortunately, organizations can address some of these issues by developing configuration management policies and processes.

Standardizing Virtual Machine Configurations

One useful method for reducing systems administration effort for virtual machines is that of standardization. Although this practice is common in the world of physical computers, IT organizations often find it difficult to exercise the same control over virtual machines. Instead of allowing end users and systems administrators to create their own configurations, the IT department can establish specific supported guest OS platforms and versions that will be allowed in production. A good way to implement these restrictions is for the IT department to create a sample configuration of base virtual machine images. Figure 8.5 provides examples of typical configurations. Most virtual machines will require additional configuration, such as the installation of additional services or applications. However, IT departments can more easily verify the production readiness of virtual machines by limiting variations. The specific numbers and types of supported configurations will change over time and must be able to meet the basic needs of users and applications.

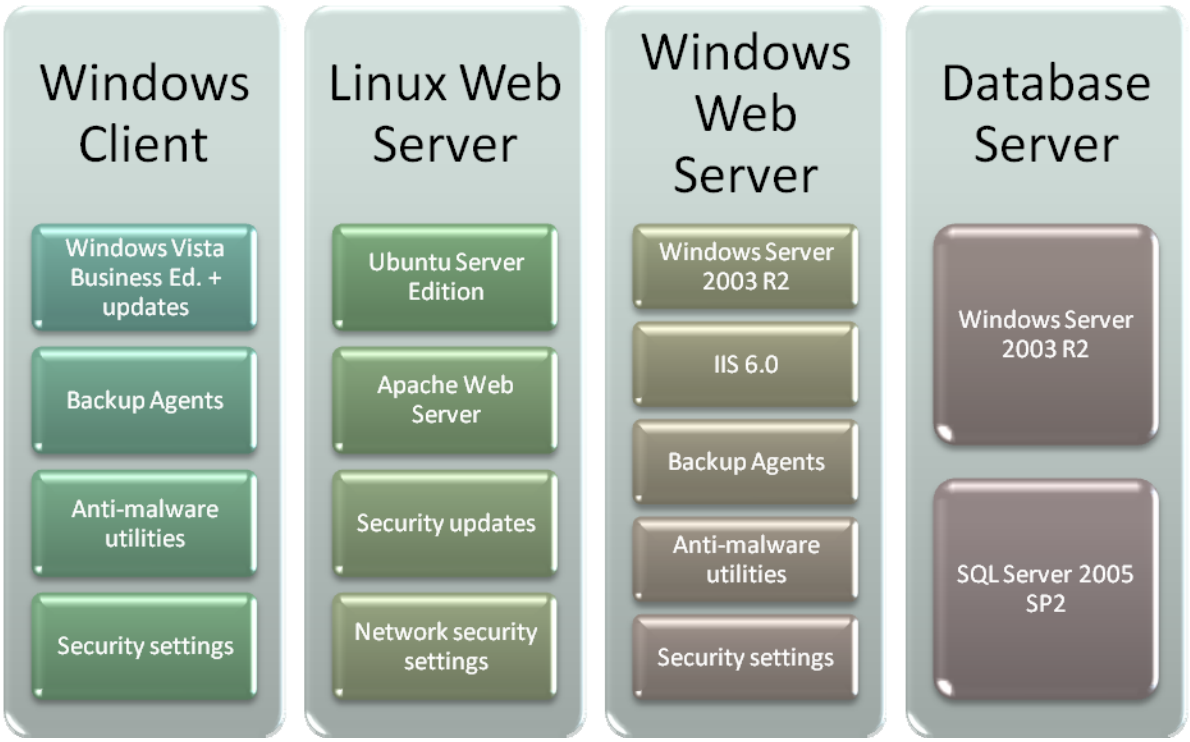

Figure 8.5: Examples of base virtual machine images that might be located in a virtual machine library.

Each of the illustrated virtual machine configurations is designed to meet a large proportion of typical deployments. For example, a standard Web server configuration might be used by many different departments for internal and external hosting purposes. By starting with an IT-approved image, certain best practices can be enforced. After customizations are made, security experts can ensure that the system is still following the IT department's policies. Each virtual machine configuration is often referred to as an "image" because it includes all the contents of one or more virtual hard disks. All the images together can be combined into a "virtual machine library"—a collection of images that have been approved by the IT department and are ready for use in configuring new virtual machines. A standard deployment process involves making a copy of an image from the virtual machine library and deploying it into production. Once the copy has been made, however, the production virtual machine must be maintained and kept up to date.

Designing and Maintaining Base Images

A potential challenge related to the development of a virtual machine library is that of determining the specific configuration of each base virtual machine image. Perhaps the most important aspect to realize is that no list of base virtual machine images will meet the needs of 100% of the user population. And, as new OS versions are released, it's likely that additional images will be needed. A good initial approach is to aim to meet the needs of 80% of total deployments using standard base images. The most common configurations will likely be the same as those that are running on current physical desktop and server machines.

Another consideration is in determining when to create new images. For example, if there is a request for a new database server configuration, should the IT department manually modify a standard base server configuration? Or should they create a new standardized image that can be used in the future? Although saving the image for reuse is helpful, the new base image must also be kept up to date over time. There is no right answer to this question, and the details will be based on the expected number of times the image will be used in the future.

From a technical standpoint, it's necessary to maintain base images over time. For example, as new OS updates and security patches are released, they should be added to base images. One method of updating base images is to boot a specific virtual machine, make the modifications, and then save the virtual machine. This process can be time consuming and tedious, though. Third-party utilities are available for directly connecting to virtual hard disk files and opening them without first attaching them to a virtual machine.

The final issue to consider is in relation to running multiple virtual and physical platforms. For example, IT departments might use several virtualization solutions in their production data center. Generally, virtual machines are not compatible between different platforms. This raises the question of whether IT departments should create separate images for each virtualization platform. That approach is possible, but creating more images translates to performing more maintenance. An alternative is to use virtual machine migration tools to simplify the process. Some third-party solutions also support the creation of system images that can later be deployed to physical or virtual machines as needed. These images are designed to be hardware-independent and can be easily deployed to various targets (both physical and virtual). Virtualization conversion tools are available for performing the following types of migrations:

- Physical-to-Virtual (P2V)—Converting a workload from running directly on physical hardware to running within a virtual machine
- Virtual-to-Physical (V2P)—Moving a workload from a virtual machine to running directly on a physical server
- Virtual-to-Virtual (V2V)—Converting a virtual machine that is running on one virtualization platform to run on another version or platform
- Image-To-Virtual (I2V) and Image-To-Physical (I2P)—Using a hardware-independent image to deploy to virtual or physical systems

Regardless of the technical approach, IT departments should create policies and processes for maintaining their base virtual machine images to ensure that they continue to meet security requirements and the needs of their users.

Benefits of Standardization

I have already listed some of the benefits of standardizing virtual machine configurations, but it is helpful to keep in mind all the ways in which this effort can pay off:

- Consistency—By starting with IT-approved images, guest OSs can follow best practices. The specific configuration details will vary for each supported OS platform and version, but standard updates are usually installed based on the organization's policies. If configuration issues are found, it is easier to isolate and resolve them on consistent systems.
- Security—End users often overlook important security considerations and lack the knowledge to address potentially serious problems. A virtual machine that does not meet basic security requirements can be a major liability if it is deployed into a production environment. Base images follow IT security policies because they are configured by experts.
- Convenience and efficiency—It's much quicker and easier for users to start with a pre-built guest OS image than it is to start installing the OS from scratch. The convenience aspects help ensure that the deployment polices are followed.
- Resource utilization—IT departments can remain in control of the resource utilization settings that are allowed for virtual machines. This helps ensure that virtual machines don't monopolize host servers or use too much physical memory.
- Licensing—Keeping track of guest OS and application licensing is an important concern from a compliance standpoint. IT departments can ensure that new virtual machines adhere to current license agreements and policies.

Of course, support for a broad array of guest OSs and versions is one of the most useful aspects of virtualization technology. For these reasons, it's inevitable that some users will need to run unsupported configurations. Any exceptions to the standardization guidelines would require explicit approval by IT management. In some cases, guest OSs that are unsupported may be placed in a test environment or on an isolated network.

Implementing a Quality Assurance Process for Virtual Machines

Software development teams often rely upon Quality Assurance (QA) staff to ensure that their products meet the intended specifications. Earlier in this chapter, I mentioned the importance of having IT approvals and oversight into production deployments. Systems administrators can implement a QA process to ensure configuration quality in the same way. Figure 8.6 lists common tools and approaches that can be used to analyze virtual machines prior to and after deployment.

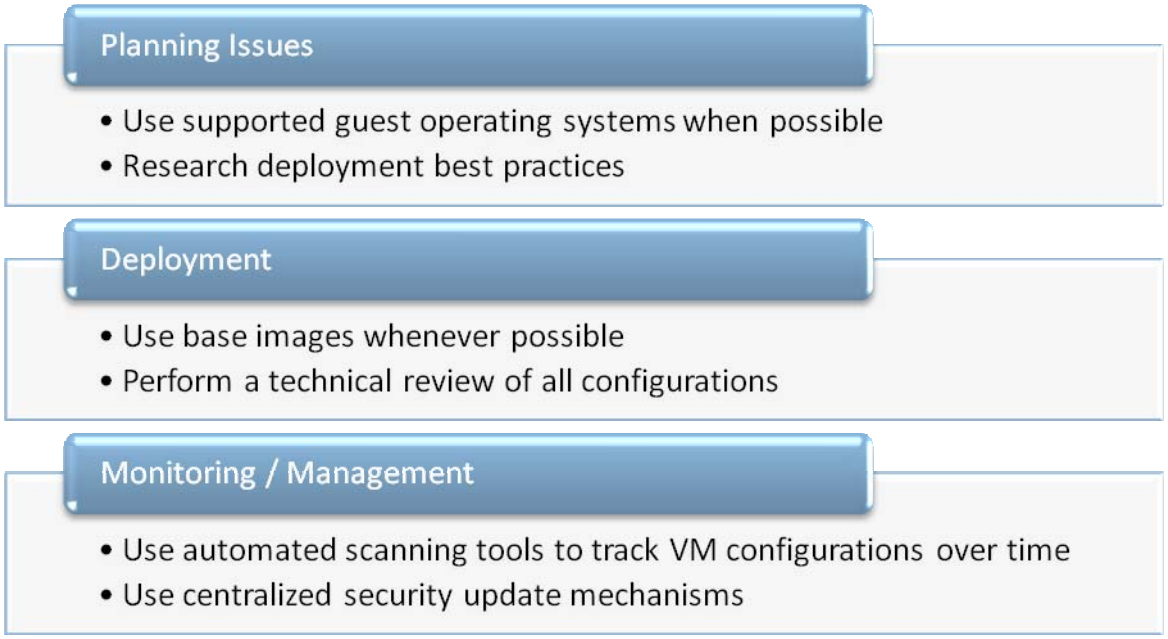

Figure 8.6: Methods of ensuring virtual machine "quality."

The overall QA process should start in the planning phase for a new virtual machine deployment. Often, end users or department managers will request a new production virtual machine configuration that does not conform to the IT department's supported OS list. In some cases, it might be possible to substitute the requested configuration with another compatible one that is supported. For deployment, base images should be used for as many cases as possible. The technical review process will usually involve a checklist of items that should be verified before the virtual machine is placed onto a production host system. Finally, once the virtual machine is in production, administrators should use automated tools to monitor their status. This helps ensure that all virtual and physical systems are up to date at all times.

Managing Virtual Machine Placement

Over time, workload performance characteristics can change. By implementing performance monitoring and optimization (a topic covered in Chapter 6 and Chapter 7), administrators can decide whether they need to move a virtual workload to another host server. Virtual machines are unique in that their complete configuration is based not on their underlying physical hardware but instead on a virtual hardware configuration. Resources such as hard disks, network settings, allocated memory, and other details are most often stored in configuration files. Virtual machines might also depend upon virtual networks and other settings that are defined at the level of the host OS or the virtualization layer. Figure 8.7 provides an overview of common types of settings that pertain to host and guest OSs.

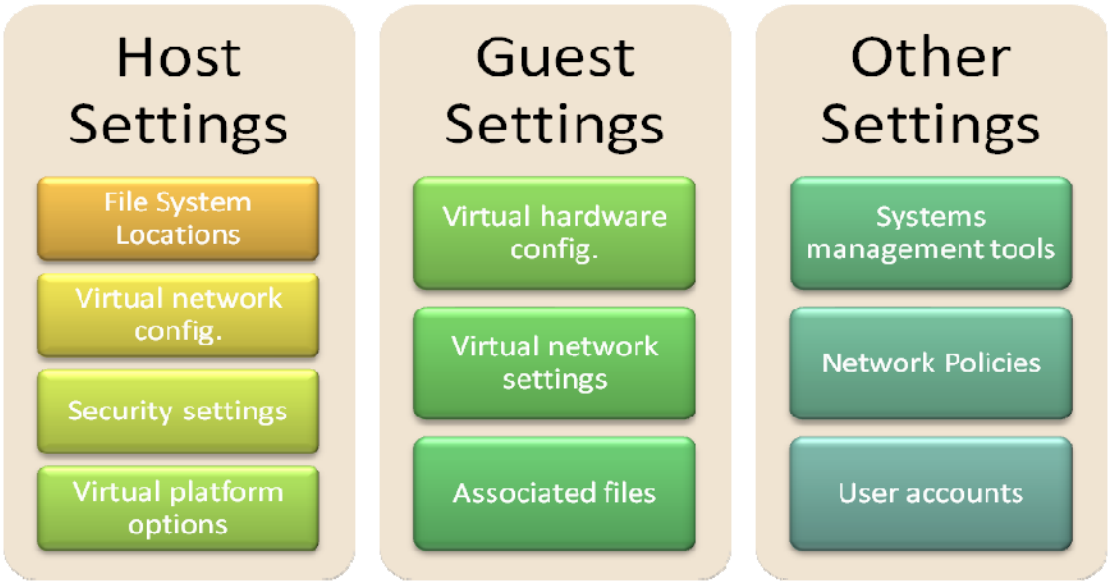

Figure 8.7: Configuration settings related to virtual machines.

Sometimes, seemingly minor changes to the configuration of a virtualization layer or to a virtual machine can have significant impacts on overall security. For example, if a virtual machine is currently connected to a private virtual network called “Default Virtual Network” on a particular host, it might be prevented from accessing the Internet or other computers on the organization’s network. The same network name might be used on another host computer to refer to a network that does have external access. Simply moving the virtual machine without considering these changes can lead to unexpected consequences.

To ensure that security and other configuration settings are maintained when moving virtual machines, IT departments should develop a standard practice for performing these steps. This is particularly important because it is easy for administrators (especially those that do not have virtualization management expertise) to overlook some of the steps. Important aspects to keep in mind include documenting the initial configuration of the virtual machine prior to making any changes. These details should be used as a checklist to verify that the migration to another system has been successful. Other steps might include a configuration review and approval from senior administrative staff.

Implementing Data Protection Policies and Processes

As organizations move mission-critical workloads into virtual environments, important issues related to data protection are raised. This section will explore details related to how organizations can develop data protection policies and processes.

Determining Recovery Requirements

An often overlooked concept is that the primary purpose of performing backups is to allow for the recovery of important information and systems. Accordingly, it's a good idea to start the development of a backup policy by defining the recovery requirements. Important constraints to consider include:

- Acceptable Data-Loss—In the case of a serious failure, the organization must decide how much information may be lost. Although business leaders are likely to initially state that no data loss is acceptable, costs and other practical limitations make this level of reliability difficult to achieve for all systems.
- Acceptable Down-Time—The process of restoring data can be time-consuming, and fail-over processes might not be automatic. Organizations should decide how long, in a worst-case scenario, systems can be unavailable for production use. Some organizations might have contractual or legal obligations to consider, while less-critical resources might have only minimal internal impacts.

One of the most important characteristics of developing backup policies is the involvement of decision makers from throughout the organization. Due to the importance of data protection, this is not the type of task that can be determined by IT departments alone.

The details will vary widely for different types of workloads, so IT departments can benefit from creating different levels of backup policies. Figure 8.8 provides some examples.

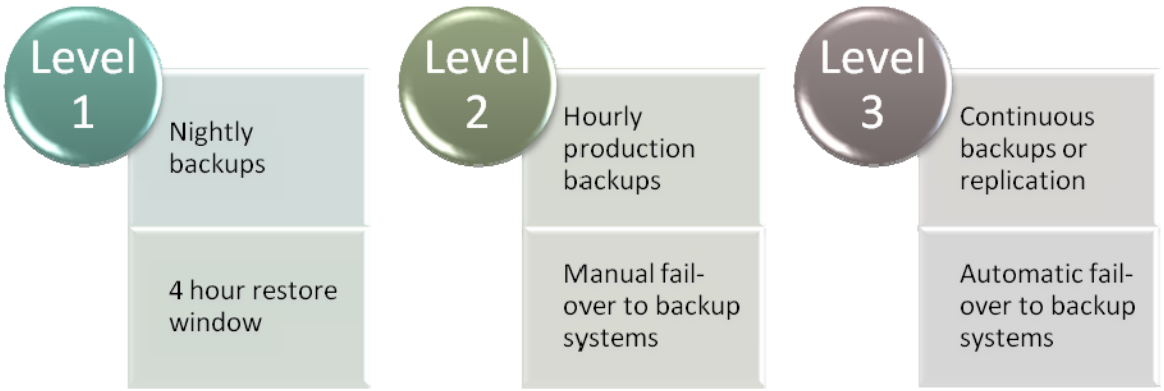

Figure 8.8: Policies for different levels of data protection.

Once the various levels are defined, each virtual and physical system can be categorized based on the most appropriate level. The goal should be to provide a balance between the level of data protection and the costs related to implementation of that level.

Identifying Important Data

In an ideal world, IT departments would create multiple real-time copies of all the data stored on production systems. Real-world constraints place limitations on what can be reasonably protected. Physical and virtual machines include OS files and application files, both of which can be recovered using installation media. User data files, databases, and configuration settings are more difficult (or impossible) to recreate. To reduce the size of backups, organizations must decide whether they should focus on backing up entire virtual machine or just important data files. With relation to virtual machines, at least the following types of information should be included in a standard virtual machine backup:

- Host server configuration data
- Virtual hard disks
- Virtual machine configuration files
- Virtual network configuration files
- Saved state and rollback files

Generally, virtual hard disks will take up the most storage space.

Implementing Backup Processes

When implementing data protection for virtual machines, systems administrators have two main approaches to performing the tasks. In this section, I'll present details related to implementing guest- and host-level backups.

Performing Guest-Level Backups

When performing backups from within a guest OS, the general approach is to treat virtual machines as if they were physical ones. The technical implementation generally involves the installation of backup agents that are then able to communicate with a central backup solution. In order for this to work, the guest OS must be supported by the backup solution.

The primary benefit of this approach is the ability to identify which data must be protected (thereby limiting backup sizes). The drawback, however, is that restore operations can be complicated. Instead of simply moving or copying the relevant virtual hard disk files to another computer, a suitable OS environment must be available for the restore process. In some cases, a new virtual machine can be created quickly from a base OS image. However, there will be complexity in ensuring that the configuration settings for the virtual machine are identical to those of the original machine.

Performing Host-Level Backups

Virtual machines are self-contained sets of files, so it makes sense to perform backups of their entire contents from within the host file system. As long as the relevant configuration and data storage files are all included, this approach can greatly simplify the recovery process. Generally, all that is required to recover from a complete host failure is to restore the virtual machine files to another suitable host. In cases in which failover times must be minimized, it can make sense to keep a "warm" backup copy of the virtual machine running on another server or at another site.

The primary disadvantage to backing up entire virtual machines is the total volume of storage space that will be required. A full virtual machine backup will comprise the entire guest OS, including program files and other binaries, so the virtual hard disk files tend to be very large. Technical limitations in data transfer speeds can limit the number and types of backups that can be made.

The other major issue with making virtual machine backups is the fact that virtual machine files are locked as in-use while they are running. In order to make a reliable backup copy, there are three main approaches that can be implemented (see Figure 8.9).

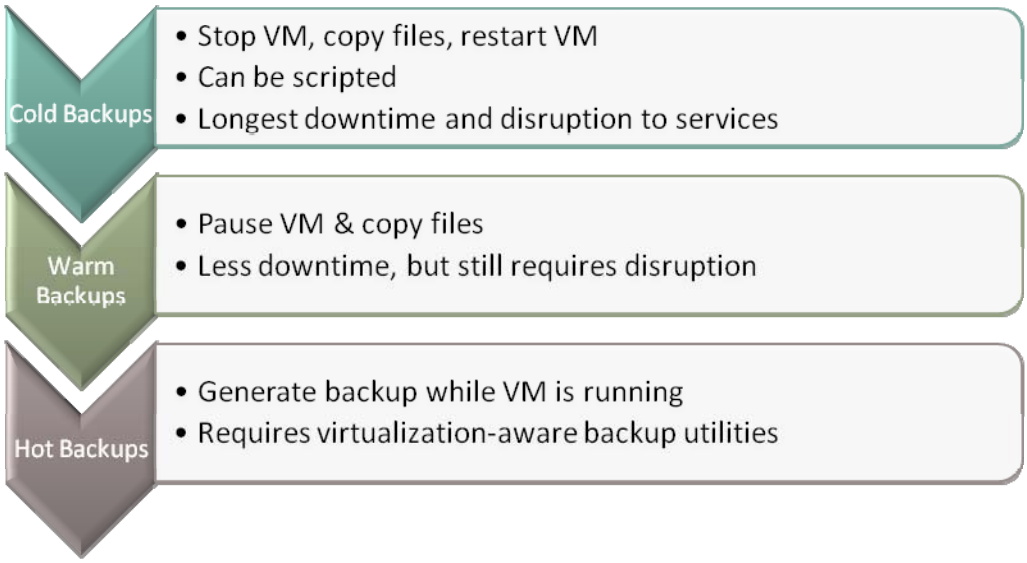

Figure 8.9: Host-level backup options.

The ideal configuration is the use of hot backups, as it involves no downtime. Organizations will need to invest in virtualization-aware backup tools and features in order to use this approach.

Choosing Storage and Backup Destinations

The default option with most virtualization platforms is to use local storage for storing virtual hard disk files. IT departments can use network-based storage options in order to simplify backup operations and to improve performance. By centrally managing storage and using high-speed, low-latency connections, they can support large, distributed virtualization environments. Figure 8.10 provides an overview of the major types of storage technologies.

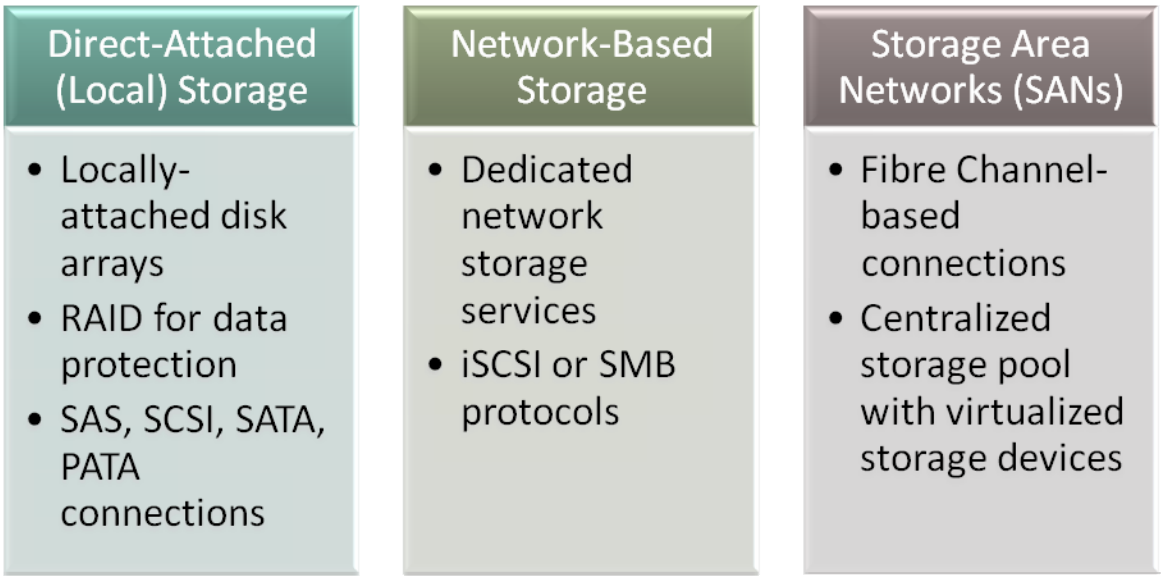

Figure 8.10: Storage options for virtual machine files.

The best option for a given environment will vary based on storage requirements, current infrastructure, and the recovery-related requirements mentioned earlier in this section.

Developing Backup-Related Policies

The purpose of a backup policy is to define the data protection requirements for a particular workload or system. The statement of the policy should be based on recovery requirements and technical data protection details. Most importantly, the terms of the policy should be clearly communicated and agreed-upon across the entire organizations. This helps avoid unwanted surprises should data loss or downtime occur.

Developing Virtualization Security Policies

Security is an important concern for all production deployments—both physical and virtual ones. In many ways, the primary concerns are the same. OSs that run on physical hardware and those that run within virtual machines need to be patched and kept up to date over time. Additionally, it's important that every system adheres to the IT department's security policies and standards. This section covers details that need to be understood in order to ensure that virtual machines remain protected.

Virtualization Security Benefits

The use of virtual machines can provide inherent benefits over physical deployments with relation to security. Figure 8.11 enumerates some of the areas in which virtual machines have potential advantages over physical OS deployments.

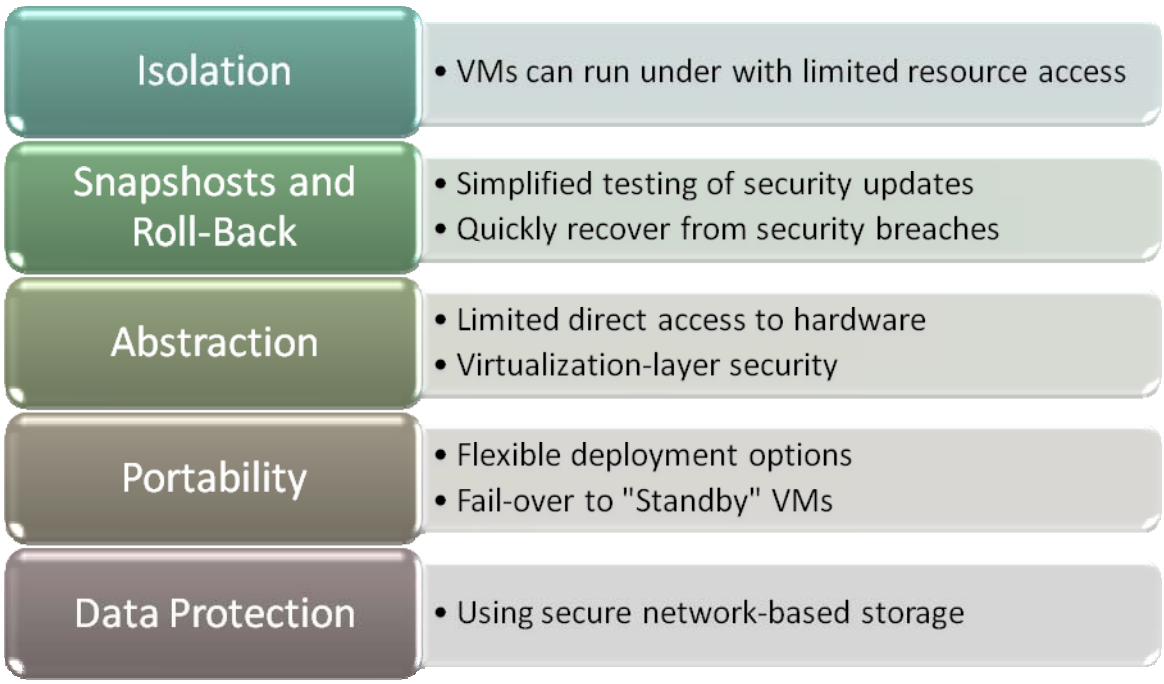

Figure 8.11: Security-related benefits of virtual machines.

The primary architectural advantage that virtual machines have is that they run in isolated environments that do not have direct access to hardware. For this reason, they can be configured to have only limited access to a host computer's resources. For example, virtual hard disk files can be located on only certain partitions and folders. The guest OS cannot access other locations, so even if the virtual machine is compromised, it should not be able to access host data.

Virtual machines can also be configured with limited access to physical networks and can be restricted to communicating only with each other (wherever the workload's requirements allow this). Other features, such as the ability to roll back the state of a virtual machine can be helpful in combating malware, virus, and other infections. In the case of a failure of a host server, virtual workloads can be restored from backups and can run on another host system with minimal reconfiguration. Finally, virtual hard disk files themselves can be stored securely using network-based storage solutions.

Virtualization Security Risks

Although there are benefits to using virtual machines, there are also risks that organizations should understand:

- Host OS vulnerabilities—Different virtualization approaches rely on different host OSs (or, at least, a thin Hypervisor layer that is responsible for coordinating hardware requests). If a host computer is compromised, it could provide direct access to all the virtual machines on the server. An intruder could reconfigure, move, or copy the virtual machines, allowing him to make copies of potentially sensitive data.
- Virtualization layer vulnerabilities—Theoretically, if an unauthorized or malicious user were to compromise the virtualization layer, she might be able to gain access to all the virtual machines on a specific host computer. Most production host computers run many virtual machines, so this possibility can increase security risks.
- Guest OS resource utilization—Malware infections or viruses that cause increased resource utilization within a guest OS can adversely affect the performance of other workloads on the same server.
- Managing offline virtual machines—In a typical data center, all production servers are running and connected to the network at all times. Virtual machines, however, can be quickly and easily shut down. This makes it difficult to use automatic network scanning tools to verify that all virtual machines are sufficiently patched.
- Tracking virtual machines—Virtual machines are portable, so they can be relocated to other host computers. They can also be copied to make what might look like an identical copy of an existing system.

To address these issues, IT departments must invest in virtualization-aware security solutions. These solutions should have the ability to uniquely identify virtual machines as they are moved between systems. In addition, they should be able to connect to a host computer and enumerate which virtual machines are present.

Security Policies for Protecting Virtual Infrastructures

Standard security policies apply equally to virtual and physical machines. One such recommendation is to use the philosophy of assigning minimal permissions. Permissions and capabilities can apply to standard users and systems administrators as well as to physical machines and virtual machines. With relation to virtual machines, organizations should limit the capabilities of a virtual machine based on the minimal needs of the workload that it is intended to support. Important questions to ask are shown in Figure 8.12.

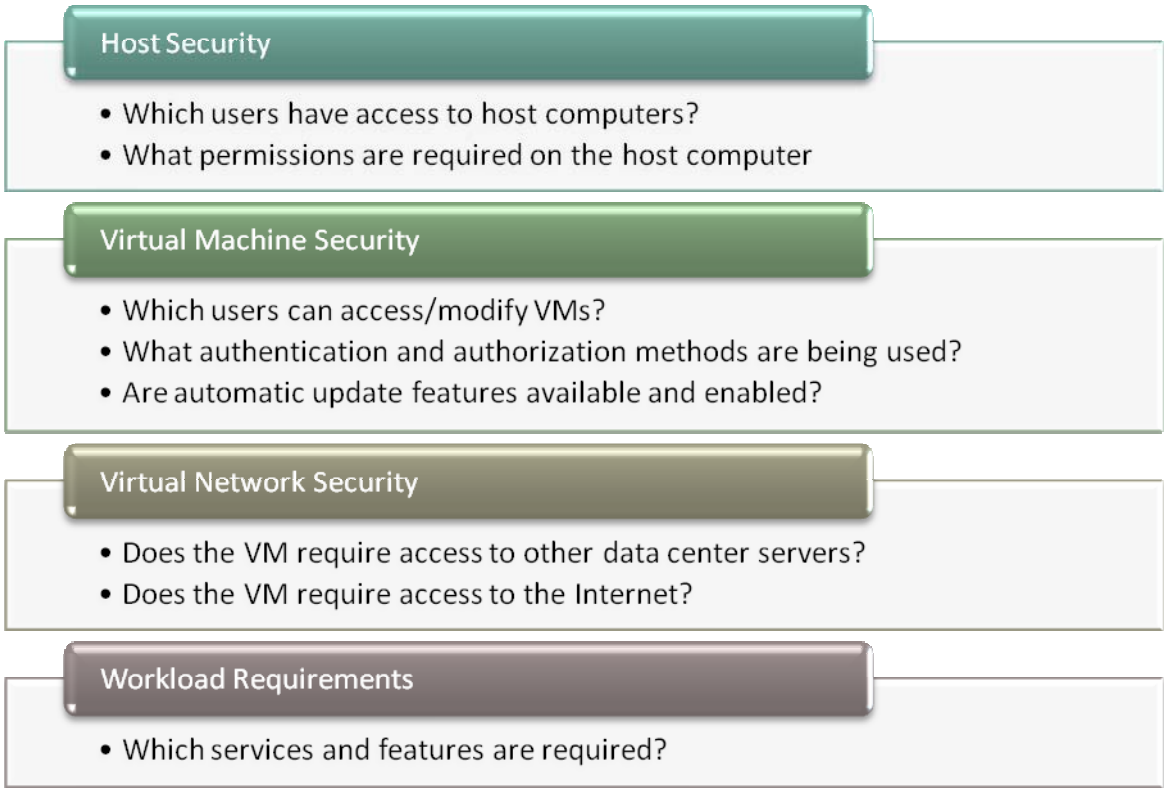

Figure 8.12: Questions related to designing virtual machine security policies.

A successful IT security policy should address all of these areas using a principle of least privilege. That is, the default configuration of a virtual machine should be to provide basic OS functionality. Users that require additional functionality (such as access to other systems or virtual machines) should be required to provide specific justifications. Often, systems administrators will find that their virtual workloads need only minimal access to the rest of the environment. By isolating virtual machines, security concerns can be decreased.

Applying Minimal Permissions

Virtual infrastructure permissions need to be considered at several levels. Multiple OSs can run concurrently on the same hardware, so the host, guest, and network permissions must all be part of a comprehensive security policy. Figure 8.13 provides a list of the typical types of permissions that should be considered.

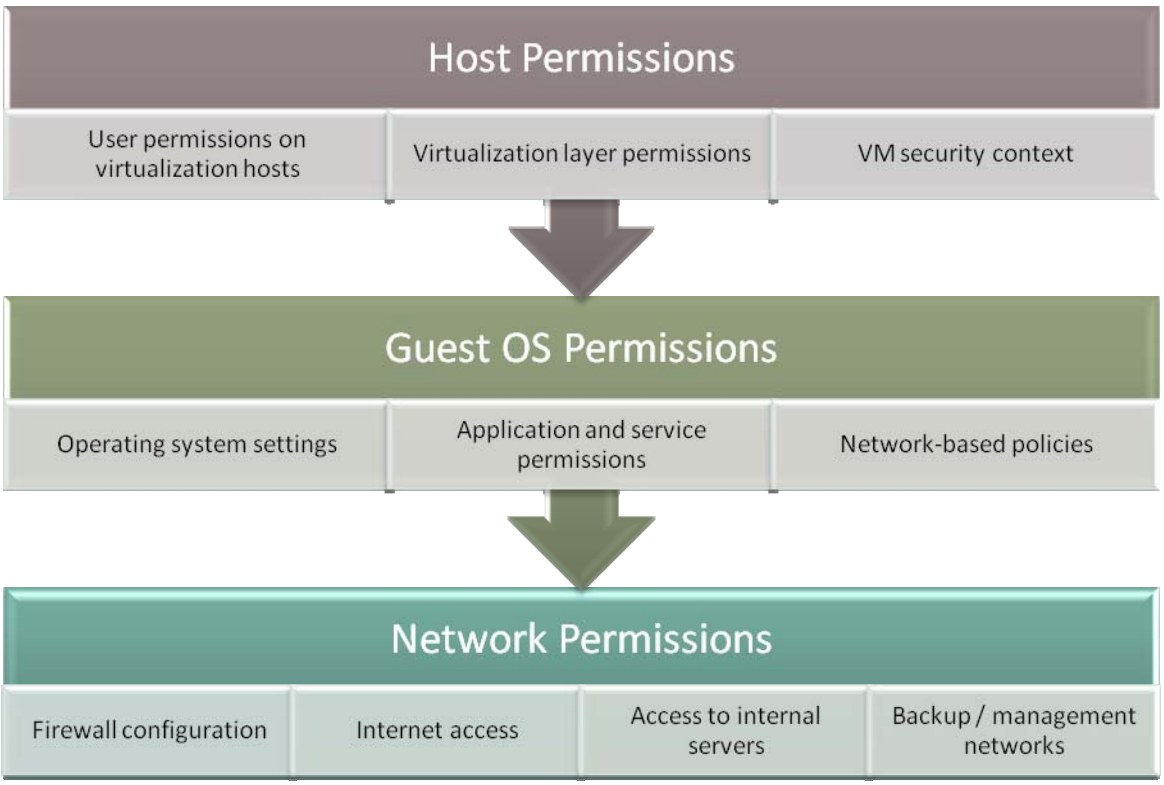

Figure 8.13: Security permissions related to virtualization.

The specific details will vary significantly based on the virtualization platform, the guest OS, and the host OS. Therefore, standard IT security policies should not be focused on a specific technology. Examples might include the types of permissions that user accounts should have within virtual machines and how IT will control access to critical systems.

Automating Security Management Processes

Organizations that have deployed virtual machines often find that they are quickly faced with supporting hundreds of new OSs. Virtual machines are quick and easy to deploy, so this situation becomes difficult to manage manually. IT departments that already use in-house automated patching methods can generally extend those systems to protect virtual machines. In some cases, upgrades to the update servers and supporting network infrastructure might be required in order to provide the additional capacity. Another caveat is that the update management system should protect as many different types and versions of guest OSs as possible. Those that are unsupported will need to be managed manually.

Keeping track of security in a dynamic virtual infrastructure is complicated by the frequent types of changes that can occur. Unlike physical machines, virtual machines can be relocated or reconfigured in a matter of seconds and without physical access to the data center. Automated scanning tools can query virtual machines that are running on the network to determine which ones might be out of compliance with IT policies. In addition, these solutions should be able to query host servers to monitor virtual machines that are offline or that have been moved to other systems. Overall, security management tools must be virtualization-aware in order to address the most important issues.

Policy and Process Best Practices

At the beginning of this chapter, I presented details related to the purpose and benefits of implementing policies and processes. In the subsequent sections, I covered specific details and examples of how these approaches can help manage complex virtual infrastructures. To conclude the discussion, this section will present ways in which organizations can decide how to implement and enforce policies and processes.

Identifying Overall Goals

Before organizations start implementing new policies or developing new processes, it's important to keep in mind the ultimate goals of these initiatives. Some of the justifications might be obvious due to current problems. For example, the issue of "virtual machine sprawl" and inconsistent configurations can directly affect supportability for the entire IT department. Clearly, steps need to be taken in order to reduce administrative complexity and efforts.

Good solutions include developing a deployment process and standardizing virtual machine configurations. Other goals might be more proactive in nature. For example, security and data protection concerns are important reasons to look into virtualization-specific policies and practices. Overall, it is important for the entire organization—ranging from business leaders to technical management to end users—to realize the importance and value of adding organization to the environment.

Identifying Process Candidates

Although the technical details related to policy definitions and process steps can vary significantly, there are some characteristics that organizations should keep in mind when managing virtualization. When choosing which types of operations should be included in a process, organizations should look for the following characteristics:

- Tasks that are performed frequently
- Tasks that have limited subjectivity and that can be organized into discrete steps
- Tasks that involve numerous individuals
- Tasks that involve interactions of people with different job roles

Processes that address these types of operations can provide the most value to the entire organization. However, tasks that involve a high degree of subjectivity or that are simple for one or a few people to accomplish might not benefit from the added overhead.

Keeping Policies and Processes Up to Date

As many employees can easily attest, there are potential drawbacks to implementing new policies or requiring processes to be followed. The first major risk is that of inefficiency. Sometimes managers that are out of touch with operations and the problems that they are intending to solve compound the issue by creating inefficient and reactive processes. The end result is decreased productivity and increased frustration on behalf of everyone involved. To avoid these problems, representatives from various user and administrator groups should be included in the development of new management approaches. This involvement also helps with enforcement, as staff members are much more likely to following decisions that they were a part of rather than those that are developed with a "top-down" approach.

Another major risk with implementing processes is the issue of keeping them up to date. Many organizations have examples of outdated procedures and practices that no longer have relevance to typical jobs. Often, steps make otherwise simple tasks needlessly complex. Consequently, the entire processes are ignored altogether or significant delays are introduced. To avoid these problems, organizations should regularly review and update their process definitions and policy statements. All affected members of the organization should be encouraged to provide feedback into areas for improvement.

Automating Policies and Processes

The primary challenges related to implementing new processes and policies are the time, cost, and effort involved. When performed manually, policy and process enforcement can be difficult. Important issues are related to communications and the coordination of efforts. Fortunately, automation can be used to simplify the required steps. Figure 8.14 provides an example of how an enterprise management solution can be used to ensure that policies and processes are being followed.

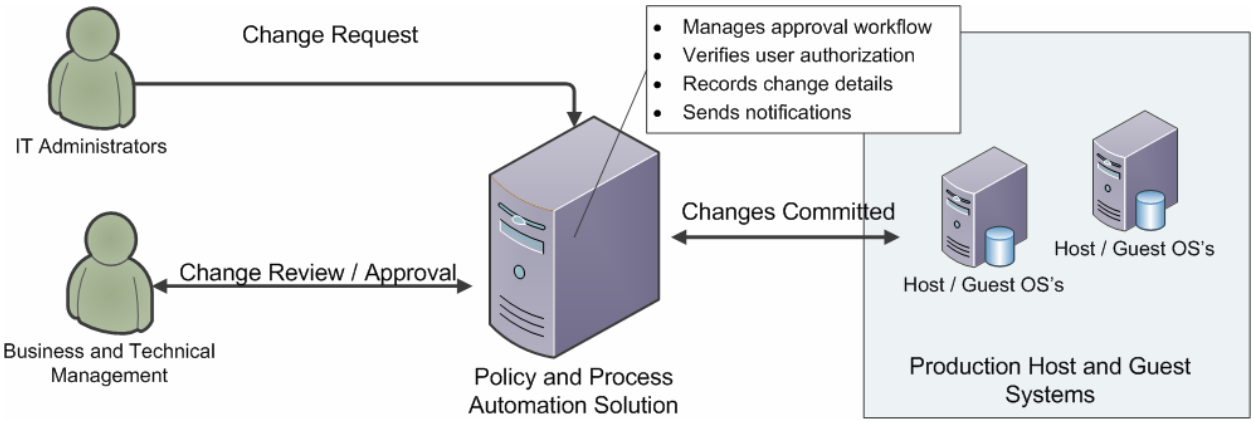

Figure 8.14: Automating policy enforcement.

For many types of operations (such as the deployment of a new virtual machine), a systems administrator will focus on just the technical tasks at hand. The organization, however, might require approvals before a new virtual machine is deployed. In order to ensure that these rules are followed, the management solution can automatically send notifications and collect the necessary approvals. Business and technical management will have a single place from which to view and organize requests.

This automated approach also provides other benefits. The system enables increased security because only the automated solution needs direct access to resources such as host servers, virtual machines, network equipment, and other devices. By minimizing permissions on these systems, departments can reduce potential security issues. Additionally, an automated policy and process enforcement solution can perform tasks simultaneously on dozens or even hundreds of virtual and physical systems. This allows changes to be done during off-peak hours without requiring additional effort from the IT staff. All the configuration changes are automatically tracked and logged so that they can be reviewed at a later date. When compared with performing these tasks manually, automation can provide tremendous advantages to a well-managed IT department.

Summary

This chapter focused on identifying ways in which policies and processes can be used to better manage heterogeneous physical and virtual environments. I began by describing the need for and benefits of implementing these management methods. Details included the involvement of the entire organization and defining roles and responsibilities. Based on these goals, I presented several scenarios and methods that could benefit from the definition of policies and the implementation of processes. The areas included the deployment of new virtual machines, standardizing virtual machine configurations, implementing security, and managing data protection. Although standard IT best practices generally apply equally to virtual infrastructures, there are additional considerations that should be kept in mind. Automated solutions can be used to simplify the creation and enforcement of policies and processes.

Overall, organizations that are struggling with managing virtualization can use a variety of approaches to address the most common problems. With these solutions in place, IT departments can gain the cost, performance, and management advantages of virtualization while still maintaining order and sanity in the data center.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.