VM AUTOMATION IN THE
Private Cloud

CHAPTER 1: Best practices for automated VM deployment   BY MIKE LAVERICK

BEING ABLE TO automatically deploy virtual machines to users is one key advantage of the private cloud. Creating and enforcing strict policies and objectives will keep VM provisioning—and over provisioning— under control.

Best practices for automated VM deployment

CLOUD COMPUTING, which delivers resources to virtual machines (VMs) on-demand based on a pool of CPU and memory requirements, is evolving. Many enterprises are now looking to the private cloud because this model facilitates the automatic deployment of VMs to users. Creating a private cloud is a turning point for moving VMs into an environment that resides outside the traditional data center, and it gives enterprises more control over their data than they have using a third-party hosted service.

That's just one advantage of the private cloud. Creating a private cloud also allows enterprises to meet internal auditing requirements through established and defined policies and objectives.

■ Un-muddying the waters of the private cloud

The difference between a virtualized data center and the private cloud may seem fuzzy. Essentially, a virtual data center is a technology; a private cloud is a conceptual IT model.

Virtualization is the key enabler for the private cloud because it unshackles the business and the IT department from the rigid models of provisioning computer resources in the physical world. In the past, server administrators were responsible for scoping out physical servers. More recently, however, duties have shifted to monitoring virtual servers.

A private cloud alleviates some of the complexity involved in creating and deploying new computing resources—virtual machines. For example, the private cloud adds another level of abstraction between the application

owner and the VM. Application owners should be able to dial up a VM from the private cloud on-demand as they can with an external provider such as Amazon's Elastic Compute Cloud (EC2). This prevents admins from getting bogged down with day-to-day operational issues of the virtualization layer. It also eliminates the possibility of human errors when provisioning new VMs.

Several pressures drive enterprises toward automation and workflow management. Businesses moving into more advanced virtualization techniques are taking the next logical step—building a private cloud so users can dial up VMs without needing a team of people to first create and define them. In the private cloud, those teams will instead need to create and enforce policies and automation workflows that give users easy access to new VMs.

■ Defining policies: A new admin headache?

Defining VMs and associated policies isn't easy; problems can occur. Many administrators still over-spec virtual machines, assigning them with too much memory and disk resources. Over-allocation wastes precious resources and further complicates matters when you have to reclaim them.

Technically, it's easy to reduce RAM and CPU allocations on a VM, but a downgrade such as this is likely to annoy the user. If the administrator initially created a virtual disk that was too large, reclaiming it requires third-party tools such as VizionCore's vOptimizer. And this is often an intrusive process.

Although newer virtualization technologies have accelerated the VM provisioning process, internal business processes remain unmodified. Changing existing processes is mired in politics; many IT departments look for ways to automate workflows to avoid getting tangled in corporate red tape. Automation also reduces the possibility for human errors. A lack of automation can lead to VMs being defined in multiple and inconsistent ways.

■ Setting enterprise-wide VM creation policies

Before you look into technology to build new policies and workflows, you need to become familiar with what already exists in your organization. Doing so helps you identify possible inefficiencies.

Then you can start to examine the manual processes involved in provisioning new VMs to understand which steps are mandatory and which steps are merely options. It's also worthwhile to reacquaint yourself with the virtualization vendors' best practices so you can include those rules in your policies and workflow later on. This also allows you to determine which settings could cause conflicts or incompatibilities with other technologies from the same vendor.

ASSIGN VM CLASSIFICATIONS. One way to simplify the steps needed to create VMs is to have different "classes" of virtual machines in the automation engine. Many customers deploy VM classifications of *Platinum, Gold, Silver* or *Bronze*.

The more CPU and RAM a VM receives, the higher its classification. The option to create a custom VM will always be there, but these categories can help create a standard to which all VMs conform. They also allow IT teams to attach a cost to each type of VM to dissuade users requesting a new virtual machine from always selecting one that's the most resource-rich.

ESTABLISH FILE NAMES. In addition to determining a VM classification hierarchy, you should establish a valid naming convention to properly identify virtual machines. Make sure that VM names are unique and make logical sense. In my experience, most companies adopt a naming convention that matches the "hostname" or "NetBIOS" name (in Windows)

> Once you've determined internal policies for VM creation, you can begin automating workflows to put these policies into place.

as the basis for their VM names. The theory behind this is that giving the VM a name that's different than the operating system can cause confusion.

■ Automating workflows to enforce policies

Once you've determined internal policies for VM creation, you can begin automating workflows to put these policies into place. After naming your virtual machine in the user interface, you'll need to set the standard for how the VM will connect to the wider network.

Setting a connection precedence is particularly important. A VM that's patched into the wrong network could lead to security breaches. Enable permissions in the management layer to prohibit this from happening. The permission should filter the network options at least to the site location where the VM will reside.

Next, select where the VM will be stored. In a multiprotocol environment that approves the use of Fibre Channel storage area networks (SANs), iSCSI SANs and network file systems (NFS), you may want to look into the per-gigabyte cost of each storage type and tie this to VM classes. For example, you may want to set it up so that a platinum-level VM defaults to being stored on a high-end, low-latency Fibre Channel SAN while a VM in the bronze class defaults to a more cost-effective NFS that was built in-house.

You should also consider if you want to include local storage as part of your policy. Local storage can cause several headaches. For example, if a VM is stored locally, it will be excluded from enterprise functions such as VMotion or Live Migration as well as from certain clustering technologies.

Storage decisions don't end with simple protocol decisions. There may be different types of disks—Fibre Channel, SATA and SSD—within a selected array that can be used to create varying storage tiers. Additionally, the array LUNs or volumes may not be replicated, so you may need to decide if the VM is mission-critical and should be replicated to a disaster recovery site.
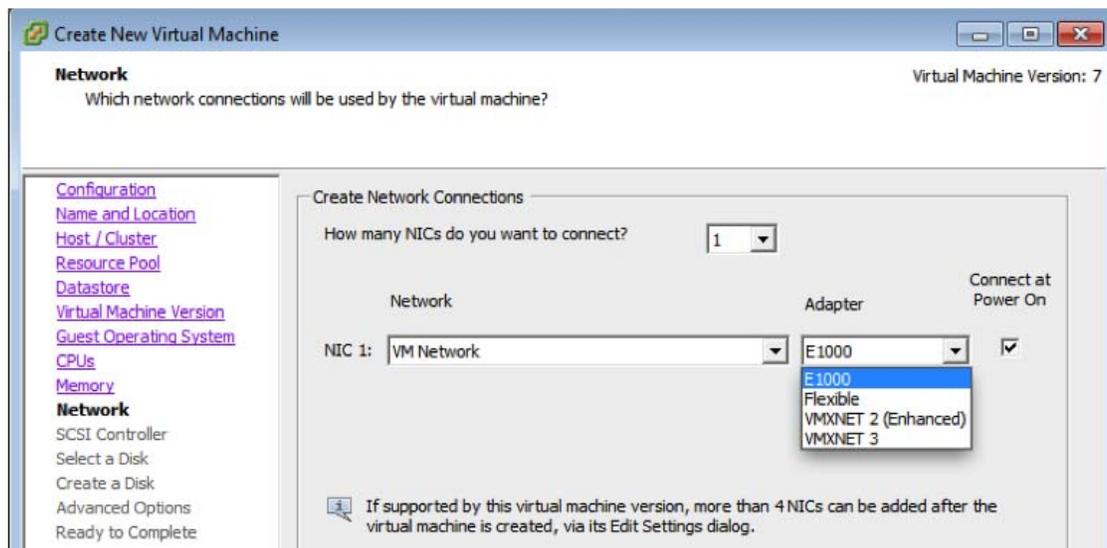
▪ Putting it into practice with VMware vSphere 4.1

Let's take a step forward and apply VM automation in the real world. I looked at whether it's better to create a VM from scratch or use vendor-supplied templates in VMware vSphere 4.1. The answer, it seems, is to incorporate a little bit of both options.

I selected the **DataCenter** object in vCenter and used the **Create New Virtual Machine** wizard in vSphere 4.1's **Custom** mode. The Create New Virtual Machine wizard has about 12 parts. Within each of these 12 divisions are countless options—with at least 26 individual choices—not including selecting the correct OS from a long list of supported vendors.

Many administrators blindly accept the default settings, assuming that VMware chooses the best options. But this isn't always the case. Frequently, VMware selects an option by default simply because it appears first in the alphabet (**Figure 1**).

FIGURE 1: *When creating a new virtual machine in VMware vSphere 4.1, the Create New Virtual Machine wizard lists settings in alphabetical order.*

BEST PRACTICES FOR AUTOMATED VM DEPLOYMENT

It might seem that the best way to narrow down choices is to use supplied VMware templates. And to some degree, this is true. Templates store both the installation of the OS to a virtual disk and the settings that define the VM. Most virtualization vendors store these settings in a separate text file; VMware stores them in a .vmx file.

Although templates are useful, you still need to manually customize them for each VM. For example, suppose that you make a template that defines a VM with 2 vCPUs, 2 GB of RAM and a 40 GB boot disk. What happens when these resources don't suit your application? What if you have a new application that requires more (or fewer) virtual resources? Since VMware didn't separate the definitions held in the .vmx file from the virtual disks, it's impossible to have a template for every configuration.

To change settings, an administrator must first clone a template and then, once it's complete, use the Edit Settings dialog box to dial up or dial down required resources.

It would seem that a simple solution would be to have a template for every possible configuration, but this would waste disk space and increase complexity. The more templates you have, the more work you have to do to keep the OS consistent and up to date.

> Having fewer templates than necessary can lead to problems where the default template setting is used several times by different systems.

However, having fewer templates than necessary can lead to problems where the default template setting is used several times by different systems. This occurs when organizations don't review settings after the cloning process has completed. I recommend creating a range of templates, each configured with more resources. For example, the first template can have 1 vCPU and 1 GB of RAM, while the final template in the set contains 8 vCPU with 32 GB of RAM.

During virtual machine creation, VMware recommends that you select a vmxnet.sys driver as the interface for the virtual machine to optimize performance. Therefore, in the dialog box, select the Flexible, VMXNET2 or VMXNET3 options. It's tempting to make the latest driver version the default choice, but that driver isn't compatible with vSphere 4.1's Fault Tolerance feature.

Selecting VMXNET3 as part of your policy and workflow makes it more difficult to enable fault tolerance on the VM. The only way to rectify this is to power off the VM, remove the offending NIC and then add a compatible NIC back in. The problem is that a guest OS may see this as a new device and your IP settings may be lost.

This is a classic example of how virtualization vendors develop two features that will be at odds with each other. As part of your policy creation process, decide which feature has higher priority and enable that in your environment.

A similar situation may confront operators when selecting a virtual disk type. In this case, the operator has a choice of thick, thin or fault tolerance-enabled virtual disk types. While it's possible to convert from one type to another, enabling fault tolerance on either a thick or thin-format virtual machine requires you to power down the VM. It also may entail a lengthy conversion process.

Thin virtual disks may save you a great deal of space, but there continues to be concern about their performance. Although VMware has made efforts to reassure customers that the thin virtual disk types provide equal performance, some customers remain cautious, setting thick virtual disks as the default for new virtual machines. ∎

> Thin virtual disks may save you a great deal of space, but there continues to be concern about their performance.

ABOUT THE AUTHOR:

Mike Laverick *is a professional instructor with 15 years of experience in technologies such as Novell, Windows and Citrix, and he has been involved with the VMware community since 2003. Laverick is a VMware forum moderator and member of the London VMware User Group Steering Committee. He is also the owner and author of the virtualization website and blog RTFM Education, where he publishes free guides and utilities aimed at VMware ESX/VirtualCenter users. In 2009, Laverick received the VMware vExpert award and helped found the Irish and Scottish user groups. He has had books published on VMware Virtual Infrastructure 3, VMware vSphere4 and VMware Site Recovery Manager.*

- **Virtualizing Storage within Cloud Computing Infrastructures Using VMware vSphere 4.0 and Dell EqualLogic iSCSI SANs**

- **VMware vSphere 4: The Best Platform for Building Cloud Infrastructures**

- **Private Clouds for SMBs: Building the Business Case**

About Dell and VMware:
Dell Inc. (NASDAQ: DELL) listens to customers and delivers innovative technology and services they trust and value. Uniquely enabled by its direct business model, Dell is a leading global systems and services company and No. 34 on the Fortune 500. For more information, visit www.dell.com, or to communicate directly with Dell via a variety of online channels, go to www.dell.com/conversations. To get Dell news direct, visit www.dell.com/RSS.