Global Knowledge®

Expert Reference Series of White Papers

Where to Go Once Your Servers Are Virtualized

Where to Go Once Your Servers Are Virtualized

John Hales, Global Knowledge VMware Instructor, A+, Network+, CTT+, MCSE, MCDBA, MOUS, MCT, VCP, VCAP, VCI, EMCSA

Introduction

At VMworld in August 2013, VMware said that there are three basic phases of virtualization, namely:

- **Basic Virtual Machines (VMs)**, where test and development, and non-production critical VMs are virtualized. Most companies today have at least gotten to this stage (most reliable accounts put this in the 60 percent to 80 percent range today).
- **Mission critical VMs**, where the critical servers that the company runs (such as SQL, Exchange, Oracle, and SAP), are virtualized. According to VMware's research, about 54 percent of companies are in this stage today. They also noted that half of all Oracle and SAP servers and three-quarters of Microsoft servers in this category are virtualized today.
- **IT-as-a-Service (IaaS)**, the phase where we use cloud computing (private, public, or a hybrid of the two). IT provides the resources and controls, but the VMs may be anywhere. Again, according to VMware, 21 percent of companies are in this stage today.

It is interesting to note in the roughly 10 years that VMware has been pushing server virtualization how the number of VMs-per-administrator has changed. In the first phase, where there typically are more, smaller physical servers, the number of VMs per administrator averages around 120 (across companies of all sizes), while in phase two, it is 170, and in the IaaS phase, the current average is 363. To manage that number of VMs well, IT has to have better tools to control what is deployed and where, the governance to control data security and access, and the ability to manage and monitor such a diverse set of assets.

So what do you do—which technology or technologies should you look at once you've virtualized all or most of your environment? What can you look at to drive down costs and increase efficiency? This white paper discusses several possible "next moves" and how they can make your business more agile and, at the same time, reduce costs.

The technologies to consider next that are discussed in this white paper include the following:

- The Software Defined Data Center (SDDC) (via Software Defined Networking [SDN] using NSX and Software Defined Storage [SDS] via VSAN)
- Desktop virtualization (VDI with the Horizon Suite)
- Cloud computing (vCloud Hybrid Service [vCHS], vCloud Director [vCD], and vCloud Automation Center [vCAC]
- Operations Management (vCenter Operations Manager [vC OPS], VCenter Log Insight, and the IT Business Management [ITBM] Suite)

You can choose to implement any or all of the technologies listed to optimize your environment. VMware's offerings are designed to integrate with each other, making it easier to deploy any combination that works in your environment. That type of integration will only deepen with upcoming product releases.

The Software Defined Data Center

If you have looked at VMware's marketing campaign and website, you have probably noticed lots of references to the Software Defined Data Center (SDDC). How is that different from what you have now? Most organizations have a Hardware Defined Data Center (HDDC) today, where networking is implemented by various switches and routers and storage via either Storage Area Networks (SANs), or Network Attached Storage (NAS).

In both cases, the networking and storage is often locked into a specific vendor with experts on staff in those vendor's products. The expertise of IT is in many brittle, vertical silos where the storage team only understands storage and the network team only understands networking, which leads to lots of finger pointing when an issue arises between these teams, the application teams, and the virtualization teams. These solutions are often very expensive to purchase (i.e., they require a large CapEx or capital expenditure) in the first place and the cost a lot to maintain and monitor through the expertise of the specialists on each team (i.e., they require a large, ongoing OpEx, or operational expenditure). Often, due to these investments, the organization is locked into a particular vendor and the costs to migrate to a new solution are often cost prohibitive. What can be done to alleviate these issues?

Two big areas are emerging in this regard—Software Defined Networking (SDN) and Software Defined Storage (SDS). They can be implemented independently or together. The basic idea is to do for networking and storage what virtualization did for computing. To some people, this is a radical idea, but then again, so was virtualization when VMware introduced it. While you may not be ready to implement either at the moment, you should start considering if they make sense and start planning for their implementation. **Note**: At this point, larger, more complex organizations will probably benefit most from SDN, while SDS can be utilized cost effectively by organizations of all sizes and complexities.

Software Defined Networking (SDN)

Let's start with SDN. The basic premise is that we separate or abstract the networking needed by your virtual machines from the actual networking that provides it. It takes the average organization about 30 days to provision the required networking for a new application (VLANs, QoS, routing between networks, firewall rules, etc.). This is not very quick or inexpensive to the business, in terms of the time it takes to make the application available as well as the IT costs to make the needed changes. What if that time could be reduced to minutes or less? What would emerge is a much less expensive, more agile environment. Now let's take that a step further—what if the IP addresses used in development could also be used in QA and production? Think of the time savings and the agility gained in moving things into production without worrying if a rule had been forgotten or an extra rule added that might break things between environments. What if, instead of having firewall rules based on the IP addresses of individual machines, the rules were applied to containers of VMs based on what the VM did and the networking and security requirements it had? Firewall rules then would automatically be updated as VMs were added to or removed from the containers. These rules could also follow VMs no matter where they were migrated to, as could their IP addresses, even across datacenters.

VMware's solution in this area is NSX and it allows (at a kernel level, not generally through Virtual Appliances [VAs] which have a greater performance impact [though some third-party solutions are implemented as VAs]). It provides the ability to handle switching (Layer 2), routing (Layer 3), Firewalls, and load balancing natively, and third parties can extend these capabilities with enhanced capabilities or even replace a native solution with one of their own. In all cases, networking performance is not limited by the hardware you own, but rather by the

compute you have; scaling is as simple as deploying a new host and adding it to NSX and the appropriate configurations will automatically be deployed to the host. These capabilities are all created, managed, and deployed through the vSphere client you all ready know.

But wait, it gets even better! If your organization is subject to laws or regulations, such as HIPPA, PCI, etc., VMware has predefined templates that can determine what you have and automatically place the appropriate VMs in the appropriate containers with the correct access permissions, firewall rules,and so forth. These rules are (or in some cases—are—in the process of) being certified by the appropriate regulatory bodies, so implementation is as simple as deploying the templates, having the systems automatically tagged and placed in the correct containers, verify firewall rules and access permissions, and turning the solution over to auditors for approval.

The same concept holds for antivirus (AV) solutions. The vendor can create a quarantine container and when a VM is found to be infected, it is automatically tagged as infected and moved into the quarantine container; once the problem has been remedied, it can be rescanned, no longer tagged as infected, and returned to its original container where it resumes normal operations.

In this model, network administrators spend much less time at a command prompt typing obscure commands, but instead spend their time monitoring the network, verifying the gateways between the physical and virtual worlds are functioning as expected, troubleshooting any issues that crop up, and designing for the future. In this world, the physical switches don't need a lot of intelligence, just the ability to forward packets where they are told, greatly reducing, if not eliminating, vendor lock in.

NSX was announced at VMworld 2013 and went general availability (GA) in October. It is not available as a download to the general public yet as VMware gets the necessary documentation, reference white papers, and such created and available, but it is expected to be available in the future.

Software Defined Storage (SDS)

Vendor lock-in on the storage side is probably even greater due to the expense of getting the SAN or NAS array (often in the hundreds of thousands to millions per array), not counting the expertise required to operate the array, tune it, and do the necessary provisioning, monitoring, and optimization tasks. In addition, with the cost per gigabyte dropping rapidly, purchasing storage well in advance is expensive (and would be cheaper if purchased just before it was needed), but that can lead to a "death by a thousand cuts" syndrome of constantly having to go back to management and ask for another few disks (relatively inexpensive), a new shelf (somewhat more expensive), or even an entire new array (very expensive). Up until now, the cost was deemed worth it to ensure high availability, shared access across hosts, low latencies, and so forth. These features will still probably be required for large, complex companies and probably will for years to come to one degree or another, but how about the storage required for these use cases:

- Tier 2/3 storage needs
- VDI (where storage can easily be 40-60% of the cost of implementation)
- DR (at the backup site)
- DMZ servers, especially where an air gap is required between internal and DMZ storage
- Management clusters, which need the usual SAN capabilities, but often don't justify the costs of those capabilities
- Remote Office / Branch Office (ROBO) sites, where a SAN or NAS device is not feasible and/or cost justified.

For these and other use cases, VMware created VSAN, which was announced at VMworld 2013 in August and was in public beta from then until early March, when it went GA. VSAN is implemented at the kernel level, and

thus doesn't suffer from the performance disadvantages of the Virtual Storage Appliance (VSA), which was (and is) a VA. VSAN takes local storage in individual servers and turns it into shared storage that can be used by HA, vMotion, DRS, etc.

VSAN is implemented at the cluster level, similarly to HA and DRS. It can be enabled in just two clicks, though there are many advanced options that can be set, along with storage policies to provide the needed availability at the best cost. The nice thing about this product is that you can scale up by adding additional storage within an ESXi host and you scale out by simply adding another ESXi host into the cluster.

VSAN has the following requirements:

- 3–32 hosts per cluster
- HA must be enabled for the cluster
- 1 SSD and 1–7 magnetic (spinning) disks, which create a disk group
- Best practice is that 10% of the space in each disk group be SSD
- 1–5 disk groups per ESXi host
- 1 GbE minimum, with 10 GbE recommended
- vSphere and vCenter (5.5 or higher)

While some may question performance, both of the solution and the CPU performance cost, VMware has tested and shown nearly one million IOPS in a single cluster (read only; roughly half that in a mixed read/write scenario) and at that level only a 10% hit to CPU performance. While the 10% may sound like a lot, most ESXi servers today are running closer to 50% utilization, so the extra 10% hit will not likely affect VM performance.

Desktop Virtualization

Desktop virtualization (often called Virtual Desktop Infrastructure or VDI for short) is similar in concept to server virtualization, in that you take the desktops and run them in VMs as you do with your server VMs currently. However, unlike server virtualization in which you reduce the number of servers in the organization, desktop virtualization will not reduce the number of desktops—everyone will still need one. The device the user uses to connect may be different than using a physical desktop or laptop—they may use an iPad, Android tablet, Windows-, or Mac-based computer, or even a thin or zero client; VMware even announced in February 2014 a partnership with Google to support Chromebooks using just an HTML5 browser (as a side note, Chromebooks took 30% of the notebook market in 2013, so you may want to start experimenting with them now if you haven't already), but each user will still require some kind of endpoint device. Users can continue to use their existing devices (desktops or laptops) and keep them running longer (as the connection software does not require much computing power), or you may replace them with a thin or zero client (which will add to the CAPEX costs in the short term, but will likely decrease costs in the longer term, as they have an average life span of eight years instead of three to four years and usually require just a few watts of power).

The server count will increase, however, to host the new virtual desktops, and a storage upgrade may be required to hold all the new VMs (though in many cases, VSAN can be used instead at a fraction of the cost). The big payback is in reduced OPEX via better security by storing no company information on the user's device, backup of all data in the datacenter, including all user data, DR capabilities after an event that affects your primary datacenter or the location from which your employees work, and simpler helpdesk tasks. If a device fails, just replace it with another device, and the user is instantly productive again.

VMware's solution to VDI is the Horizon Suite, which is made up of four Horizon components:

- Horizon View
- Mirage
- Workspace
- ThinApp

A fifth area around Mobile Device Management (MDM) was recently announced with the acquisition of AirWatch. The capabilities will be integrated in a future version of the Horizon Suite providing device to desktop management as well. As this is recently announced and not yet available, this set of features will not be described here.

Horizon View

VMware's original product for VDI, View is still available and being enhanced. View provides a true VDI environment. That is, while you could just virtualize desktops, access to those desktops would have to be done via native mechanisms, such as SSH or RDP. This isn't possible with most thin or zero clients, nor with tablets and smart phones in many cases. View provides a client that can be installed on a Windows, Linux, or Macintosh computer, an iOS- or Android-based tablet or smartphone, access via a thin or zero client, or, new in version 5.2 and later. A virtual desktop can even be accessed by any HTML-5-compatible browser with no client installation at all (e.g., the aforementioned Chromebook). It supports Windows XP (though that is at EOL and really shouldn't be deployed or used any more), Vista, 7, and 8 (including 8.1) only, and provides for a simplified, authenticated experience to login from any of the previously mentioned devices, providing the best end user experience possible, including making touch work better on an OS that was not built for it (e.g., to use an iPad to connect to Windows 7 via a feature called Unity Touch). It even allows the same client to connect not only to a desktop VM, but also to a physical computer or a Windows Terminal Services desktop, providing a single client access to many desktop sources. Licensing from Microsoft to do VDI is expensive and complicated, so new in View 5.3 and later, Windows 2008 server can be deployed as well and configured to look and feel like a desktop which can dramatically cut licensing costs (when used with the Datacenter edition which is licensed per physical host instead of per VM) while providing the familiar look and feel.

View has many advances to make the administrator's control and manageability as well as the user's experience as close to physical as possible.

Administrators can deploy pools of VMs to which users can connect (either always to the same VM or to a random VM each time) with a few clicks, and then configure their preferences, settings, and data to follow them wherever they login from. Data is maintained at the datacenter, and, thus, can be secured and backed up in much the same way that a server is. Administrators can deploy applications, upgrade them, and remove them as desired. Access can be secured both internally as well as from outside the corporate network with all data encrypted by SSL. VMware has added performance-enhancing features, such as the ability to leverage SSD drives, set aside some RAM in the ESXi server for caching frequently accessed data, and allowing the desktop VMs to leverage a physical graphics card to dramatically reduce the load on the CPU by handling graphics rendering in hardware instead of software, allowing for much better consolidation ratios. They have also added space-saving features to reduce the amount of disk space required. Furthermore, the settings for View itself, as well as many of the configuration options for the virtual desktop, can be configured via Group Policy in Active Directory, making centralized management much easier and simpler.

From the user's perspective, VMware has made the environment simple to access their desktop from any device from any location. It will automatically discover and make available any printer to which the end point device has access without the need to install any drivers in the virtual desktop. Performance is optimized for access from all

kinds of networks from DSL to LAN speeds, and to handle WAN latency well in most cases, allowing VMs to be run from 3G (or preferably) 4G networks. VMware also allows a desktop to be "checked out" from the datacenter and run locally while a user is disconnected from the network, for example while they are on an airplane, at a customer's site, or other locations where network access is not possible. In addition, the local copy of data is encrypted and controlled by policy from an administrator and synchronized with the datacenter in case the laptop is lost or stolen.

In short, VMware has optimized their environment for everyone and continues to make great strides in providing a simple to use infrastructure for users that is also easy to manage and secure for administrators.

Horizon Mirage

Mirage is the second tool in the Horizon family of products. Mirage works by logically dividing a computer into multiple layers, some controlled by the administrator (OS, drivers, etc.) and some by the user (e.g., their data). In addition, applications can fall into either category, with some that are controlled by the administrator and some by the user if desired. Data can be backed up and restored separately from the OS, so an administrator could upgrade a computer automatically, and the user would still have all of their data. The administrator is happy because he or she has control of the OS, patching, etc., and the data is all backed up centrally. The user is happy because the user controls their own data and it is backed up in case it needs to be restored later.

Mirage can also take the image of a physical computer that it normally makes and turn it into a VM, perfect for when a user's laptop crashes or is stolen: just grab a replacement from IT (or a favorite retailer), or even use a tablet, and connect to the device to View and continue working while a permanent replacement is worked out.

Horizon Workspace

Workspace is the third major tool in the Horizon family. It allows an administrator to manage applications, deploying them to physical or virtual machines, as well as to mobile devices. It includes the ability to pass through a user's credentials to many Software-as-a-Service (SaaS) applications, such as Sales Force, to allow single sign-on for many applications used in the cloud. Not only can applications be deployed using this tool, but it is done on a self-service basis, so a user simply needs to log in to the portal, pick the needed apps (from the list an administrator makes available), and the apps get deployed to the device(s). It also tracks the applications deployed across the entire organization to assist with license compliance.

In addition, it can function much like SharePoint in giving you a shared space to share files, both internally and externally to the organization. Permissions can be set to control who is allowed to share data externally or internally and optionally with whom. All data stored in Workspace is always encrypted—on the Workspace server, over the network, and on any end user devices (PCs, Macs, iPads, Android devices, etc.), so the data is always secure. The administrator always maintains the ability to remotely remove the information from any of the devices as well in case the device is lost or stolen or the user leaves the company.

ThinApp

ThinApp is included with all of the products in the Horizon Suite individually, as well as a standalone product (it was supposed to no longer be available standalone, but VMware decided to keep selling it this way as well as part of the Horizon Suite) and allows application virtualization. Similarly to how server or desktop virtualization separates the OS from the hardware, application virtualization separates the application from the OS. This allows you to install an application once and deploy it to many systems. It works with both physical and virtual OS deployments. Application virtualization lets you install an application on one OS and run it on another (usually as long as the other OS is more recent than where it was originally installed). It also lets you run multiple versions of the same application side-by-side. For example, you could run Internet Explorer 6, 7, 8, 9, and 10 all on the same computer at the same time, making it much easier for web developers or help desk personnel to troubleshoot issues across browsers or browser versions without requiring many VMs or desktops.

ThinApp allows applications to deployed via Horizon Workspace, Horizon View, from web servers or file servers, by locally installing it on a machine, and even to run it on a locked down PC from a USB key. Over 90% of all applications can be virtualized, allowing for broad application of the technology.

VMware has recently released a major upgrade to ThinApp, version 5, replacing the 4.x versions that have been available for years. There are many changes to ThinApp 5, but the biggest and the one with the most far-reaching consequences is the ability to capture and deploy 64-bit applications, which the previous version could not. They have better support for Office 2010 and 2013, IE 10 as either a native browser with ThinApp-based plugins, or a completely ThinApp-based browser with any necessary plugins. They also have improved the manageability of ThinApp via GPO policies in .adm or .admx files. They have also integrated support between AppSense and ThinApp so that settings in one environment (virtualized or native) can be used in the other.

Conclusion

You can buy View, Mirage, and Workspace as individual products (each includes ThinApp as well), or you can buy the Horizon Suite that includes all three in a bundle for a package price. Any of the Horizon offerings can be purchased individually (i.e., without including any vSphere licenses) or can include the desktop license of vSphere, which includes vCenter Standard and ESXi Enterprise Plus licensed for desktop VMs and View infrastructure only.

One other thing that VMware provides with the Horizon Suite which is a great advantage to all who deploy View as part of the Horizon Suite (not the standalone View product only), is that vC OPS for View is now included in the price. This tool provides 11 custom dashboards of information on how the View environment is functioning; that is a great aid for all View administrators. More about vC OPS will be described in greater detail later.

Cloud Computing

Cloud Computing is here to stay. Whether it is a major or minor part of your environment, most companies today use cloud computing in some form or another. It might be for email and web-hosting via Office 365, or to run an application such as Sales Force. It can even be used for such mundane tasks as file sharing with Dropbox. Regardless of the use, cloud computing is a reality today.

Cloud computing can be much more than these simple uses, however important to the business, however. Cloud computing can dramatically reduce the time it takes to create a new VM or set of VMs, whether for testing, production, or even just to have the ability to normally run locally (at your normal location) but burst into the cloud when demand soars. It can be used to deploy a group of VMs for a developer who needs to run a domain controller, a SQL server, and an app server, along with three test VMs with different operating systems, for example. The tools to create and manage cloud infrastructures can have approvals built into the process and the ability to charge back (or at least show back) to show to departments the value of the IT services provided without sending a bill. This is the power, flexibility, and agility that cloud computing provides.

Most of the tools discussed here are related to Infrastructure-as-a-Service (IaaS), not the other cloud types, though VMware and other providers have solutions for other cloud types as well. All start with the vSphere you use today, and then extend in different directions.

VMware has several products that are designed for the cloud-computing arena, namely:

- vCloud Hybrid Service (vCHS)
- vCloud Director (vCD)
- vCloud Automation Center (vCAC)

vCloud Hybrid Service (vCHS)

vCHS is VMware's product designed to make it easy to migrate workloads between your on-premises vSphere implementation and a cloud-based vSphere implementation hosted by VMware. This product is available from VMware directly and is based on their data centers in Dallas, Santa Clara, Las Vegas, and Sterling, Virginia (greater Washington, D.C.). vCHS has a release cycle of every 6 weeks to keep up with the rapidly changing world in the cloud, but these changes occur without any outages to customers using standard vSphere technologies.

vCHS is designed to allow for common networking, including keeping the same IP address onsite as well as in the cloud using a stretched Layer-2 network between a company's location and the cloud provider's. It also allows for common management, security, and support, allowing you to leverage your existing vSphere skills and design, and simply extend them into the cloud. It takes just a few clicks to move a VM into or out of the cloud. The hybrid cloud pieces (local and cloud) are managed via the standard vSphere Web Client.

It will also enable DR-as-a-Service (DRaaS), integrating with SRM, as well as Desktop-as-a-Service (DaaS), integrating with Horizon seamlessly through VMware's purchase of Desktone. For many businesses without multiple locations, the DRaaS capability may be very helpful in creating and maintaining an off-site backup that can be spun up into VMs quickly in case of an outage at the normal production site.

vCloud Director (vCD)

The original product in VMware's line up for cloud offerings was vCD. It is designed to make self-service provisioning easy and secure for end users while at the same time providing tools for vSphere administrators to manage the physical network, storage, and compute resources. The tool has billing support natively, as well as integrates with third-party billing tools and lets customers define the resources that they need to access in the cloud.

vCloud Director is built to support multiple tenants, whether they are different companies, departments, projects, and so forth. This support for complete isolation between tenants makes it a very powerful tool to create public clouds, and is, in fact, where this product is heading. In a public cloud, the absolute security between clients is the highest priority, followed by ease of use then features in most cases, and vCD has implemented its features in this order.

On the other hand, if you want to extend your existing vSphere infrastructure into other hypervisors, either on-premises or in the cloud, the two options just mentioned aren't very helpful, as they only work with vSphere; enter vCAC.

vCloud Automation Center (vCAC)

vCAC is based on a tool VMware purchased from DynamicOps, a company that was created as a spin off from Credit Suisse, based on their need to automate virtualization. vCAC is designed to provision machines on physical servers, various virtualization platforms, or in the cloud. It supports provisioning new machines in any combination of the following platforms:

- **Physical:** Dell, HP, and Cisco UCS
- **Virtual:** vSphere, Red Hat / KVM, Microsoft Hyper-V, and Citrix Xen Server and Desktop
- **Cloud:** vCloud Director (vCD), vCloud Hybrid Service (vCHS), Red Hat / OpenStack, and Amazon Web Services (AWS)

In Version 6, released in December 2013, many changes were made, including a complete overhaul of the UI and support for XaaS (where X is anything, from database as a service to a custom onboarding app). The traditional IaaS components are still strongly tied to the Windows platform and leverages .NET, IIS, and Active Directory to do the actual provisioning work, but can provision machines with virtually any OS. It can even provision

hypervisors on bare metal, preparing them for use in deploying VMs. Other areas of the platform, including Single Sign-On (SSO) are supported via a VA based on Linux.

vCAC is a great infrastructure tool for administrators to use to pull together all of the hypervisors in use across the organization and make them available in a simple, manageable way to end users. It has many of the features of self-service provisioning that vCD offers as well as basic billing capability (but not the deep integration or depth of options that vCD offers, as it is aimed at use within a company instead of at cloud service providers); however, this capability is accessible via integration with the IT Business Management (ITBM) Suite (described later).

Administrators can also have multiple tiers of storage and can define costs for them as well, thus creating a cost structure that end users can understand and consider in making choices of what platform a particular project requires. They also have the ability to require approvals, either in all situations, or only if certain threshold are surpassed, providing control while not adding a lot to the workload of the IT staff for routine requests.

When creating machines using the IaaS capabilities, administrators create blueprints that define the details of what machines can be created on which platforms and then assign permissions to end users to use the blueprints they need. Multi-tier solutions can also be created that span multiple environments or include sub-components in a vCD environment that get deployed as a single package with just a few clicks. Leases and maximum durations can also be created, if desired, automating the life cycle of a development project for example; approvals can be added to extend the project if needed or desired. Multiple levels of administrators with varying abilities within the system are defined; an administrator can belong to any or all of them, depending on the size and complexity required by the organization.

Users get a simple deployment interface via a web-based GUI to create, manage, and delete machines. The tool provides a machine console for vSphere-based VMs in addition to also making accessible access via the underlying platform (e.g., RDP) to provide connectivity to the machine. It does make it easy for end users to expire machines they no longer need, take snapshots of them for quick recovery, or to roll back a testing environment, control the power status of the machine, reboot it, or reprovision it (i.e., change the configuration of it, such as to add CPU or memory to it). The actual capability the user has depends on the platform the machine is installed on and the capabilities that an administrator has assigned to the user.

Reporting is available, detailing what is deployed, what can be reclaimed due to non-usage, how much of each resource (example: physical servers or cloud space) is deployed, and what is currently allocated. A chargeback report provides details of the costs of the deployed environment. Dashboards are also provided to give high-level information quickly and succinctly.

With this product, VMware is moving beyond the commodity hypervisor and hypervisor management space that it pioneered to the management of your environment, no matter who the underlying virtualization vendor is or even if it is a physical or cloud-based design (or any combination of the three). Thus, you may use Hyper-V or AWS for test and development, but still run production on vSphere, for example.

Conclusion

VMware would prefer you to have an all-VMware shop based on vSphere, but understands that as your organization grows, you may wish to grow into the cloud. If you wish to stay in the VMware family and continue using VMs and vCenter, and you don't really need the ability to have strict security between departments, divisions, etc., and self-provisioning, then vCHS is probably the best solution. If you want the broadest support for the cloud with the best billing, costing, security, and self-service options possible, then vCD is your best bet. Finally, if multiple hypervisors, physical environments, and cloud platforms are what you need to deal with, then vCAC is just the tool for the job. No other VMware components are required with vCAC, though they will, of course, be leveraged if you have them.

One note on vCD vs. vCAC that is important comes from an announcement at VMworld 2013 and documented in this blog post from VMware: http://blogs.vmware.com/vsphere/2013/09/vcloud-director-convergence-and-transition-plan-whats-the-scoop.html. It discusses the future of vCD and vCAC and the recommended path to take for various situations. Please review this document and see which product will be a better fit for your organization.

Operations Management

Management of a virtualized environment is important and it can be time- and resource-consuming. As you layer VDI and/or cloud computing on top of the existing server, virtualization what you have already done, and you add to the complexities of managing your environment, making a solution for managing a complex environment that much more important. There are needs within the organization to manage the environment for issues and problems, to plan for future needs, to analyze the environment looking for under- and over-utilized VMs, hosts, and so on. Each component adds to this complexity by generating its own set of logs with operational, performance, and/or security information. How does one sift through all of this data and pick out the nuggets of information that will help you resolve the root cause of problems, spot trends, etc.?

VMware as an organization has the same issues you do as they have operations globally, have many hardware and storage platforms, and have a virtualization infrastructure with data in the public and private clouds, as well as being a public cloud provider for others. As such, they turned to software and their knowledge of the virtualization and cloud environments to make it simpler and easier to manage and then partnered with server, storage, and networking companies to extend this capability to the rest of the ecosystem. They have two major tools in this arena, as well as a cast of supporting tools that can be used.

- vCenter Operations Manager (vC OPS)
- VCenter Log Insight

In addition to all of the technical tools a third tool, which is available from VMware to help in costing and service quality management. This enables managers to run IT more like a business, seeing the areas that are working well, as well as highlighting areas that can be improved. It also has a benchmarking feature that can be used to compare a company's costs compared to various other industries and geographies to provide relative performance metrics as well. The business management product is:

- IT Business Management Suite (ITBM)

These tools can help you simplify the management, both technically as well as from a business perspective, of environments of all sizes and complexities.

vCenter Operations Manager (vC OPS)

vC OPS is a tool that is designed to analyze your environment, figure out what "normal" is and alert you when abnormalities occur. These abnormalities can be at the VM or host, cluster, or data-store levels. They can be reported on at the particular node level experiencing the abnormalities as well as bubbled up to see the impact on the wider configuration. vC OPS is designed to help you find both undersized and oversized VMs as well as wasted resources as part of a broader ability to assist with capacity planning to prevent vastly oversizing the environment, as well as to showing when additional resources are needed. It can help you spot issues early and provides root-cause analyses for the issues detected, directing you where to look or what action to take to fix problems. If you also have vCenter Configuration Manager (vCM—part of the vC OPS Management Suite), it can correlate events that occurred in the environment with results (such as performance changes) in the VM, host, etc., to look for those relationships that are often difficult to find, such as a patch in the OS causing a CPU spike.

vC OPS will gather data over time and dynamically set thresholds based on what is normal for that time of day, day of the week, week in the month, etc., and report back when they are exceeded. vC OPS is designed to alert you when things are not normal but not bother you about the little events and minor abnormalities that are normal (and probably common) in your environment.

Most environments with more than a few servers and a few dozen VMs need vC OPS (or a similar tool). There are just too many things going on and too few administrators to watch all that is happening to effectively manage issues, not to mention all of the false alarms raised for things that may be normal in your environment, such as a server using a lot of CPU during a backup. This could be fixed by adjusting alarm values for those VMs, but that requires a lot of data gathering and analysis to figure out what is "normal" for each VM. Then you must implement those custom alarms on all affected VMs, leading to management by exception. In addition, alarms don't support different values at different times of the day, so you'll need to either set one value that works all of the time, or create a scheduled task to programmatically change it for different times of the day, days of the week, etc.

vC OPS does what computers do best: it gathers data and analyzes it, alerting you to abnormal conditions. You can then fight the real fires by doing what people do best. The costs of not managing an environment well are unplanned outages, capacity limitations that lead to performance degradation, and, if left unchecked, possible outages, lack of resources when a failover event occurs, or no disk space, freezing all the VMs on any datastore in such a condition.

As of vSphere 5.1, the Foundation edition of vC OPS is included in the package for free, so there is really very little reason to not have at least a basic level of monitoring in place. Note that you still need to download and install the product (it comes packaged as a Virtual Appliance [VA]), but there is no additional cost associated with it; higher versions of vC OPS with greater capabilities (most features beyond basic health monitoring) are separately licensed, either a la carte or with various bundles.

According to VMware, the following are some of the benefits of deploying vC OPS (though not all are available with the Foundation edition):

- A 36% reduction in downtime at the application level
- A 26% reduction in the time it takes to diagnose and resolve a problem
- A 40% increase in capacity utilization
- A 37% increase in consolidation ratios (the number of VMs hosted per ESXi server)

VCenter Log Insight

VCenter Log Insight is designed to import large quantities (potentially in the hundreds of gigabytes or even terabytes) of unstructured text-based log data, analyze it, and automatically highlight issues. It natively reports on vSphere logs and is extensible to include operating system, application, storage, and networking logs as well. In fact, just about any type of text-based logs from any device, application, etc. can be analyzed—including even network traces and firewall logs for example. It is deployed as a Virtual Appliance (VA) and can scale out across multiple VAs easily, potentially residing on different ESXi servers and/or storage locations for better performance.

Log Insight can be used by itself or it can be used with vC OPS for richer data analysis and reporting. It can help find anomalies and predict where things will be in the future. It is extensible via content packs from VMware, third-party vendors, and partners, as well as the community at large. A content pack provides dashboards, saved queries, field definitions for commonly searched data, and alerts, and is usually based on input from the vendor's developers and product support personnel on what they think is most useful and most often helpful in solving issues. Currently View and NSX have content packs available from VMware; other content packs are available

from EMC, NetApp, Cisco, and VCE, among others. These and others are available on the Solution Exchange (http://solutionexchange.vmware.com/store/loginsight).

VMware described the data contained in logs as follows:

> *Log data [is like] the Twitter feed of the datacenter – each piece of software and hardware emits a constant chatter of status updates. These status updates (short text messages called log messages) provide rich information on the state of the environment, and the actions of individual components within that environment.*
> *Source*: http://cto.vmware.com/introducing-vmware-vcenter-log-insight/

The analogy is perfect and describes very accurately the great value, as well as the great quantity, of information the logs provide. The problem is how to extract that data and find the nuggets of relevant information buried among informational data that is just noise. Log Insight is easy to deploy and very easy to configure to collect vSphere Logs (just a single step in the wizard for this). Via the content packs, other data sources are likewise very easy to collect and analyze.

Among the use cases are troubleshooting and root-cause analysis, security, and compliance. Log Insight is needed as larger and larger distributed architectures with more nodes, more devices, and more complexity are integrated with increasing numbers of layers in the application and infrastructure stacks. It is designed to remove complexity and find hidden value in the many often-ignored logs. It is simple and easy to use (just click and highlight to select words, click Extract field, and it is now query-able like a field in a database). These queries can even be graphed, including how often a particular event (log entry) has occurred historically to help set proper thresholds; email alerting can be configured when these thresholds are exceeded.

IT Business Management Suite (ITBM)

The IT Business Management (ITBM) Suite is designed to give a holistic view of the costs and service level agreements(SLAs) surround IT. There are four main components to the tool, namely:

- Financial Management (Costing – Part 1)
- Business Management for the Cloud (Costing – Part 2)
- Benchmarking (Costing vs. others in various industries, geographies, etc.; Costing – Part 3)
- Service Quality Management

Let's look at each of these areas and see how ITBM can help in both costing and SLA management.

CIOs don't know or have a very good grasp of the cost of IT. Yes, they know how many dollars were spent on servers, storage, salaries, and so on, but what does that mean? For example, how much did it cost last year to have email handled in house? To know that, you'd need to know the cost of the servers (or portions thereof if virtualized), storage costs (percentage used by email vs. total capacity in terms of both IO rate and space), cost of networking, cost of licenses for the email platform and the fraction of the virtualization platform's and OS' costs attributable to Exchange—and then do the same thing for salaries of the network, storage, virtualization, security, and application teams. Then you'd have to figure that cost over the lifespan of the various components, add in services needed to implement it, etc. to come up with a true TCO (Total Cost of Ownership). ITBM can do that for you (of course you will need to input some of these costs as well, such as how much you paid for the servers, storage, etc.), and then produce a report on the top consumers of IT resources. It can also track actual vs. forecasted rates to spot trends early and take corrective action sooner. It also has the ability to look for usage and suggest cost-saving measures, such as tiering, virtualization, consolidation ratios, and so on. These features are all part of the Financial Management part of the suite.

That still leaves the question of whether or not a public cloud offering is cheaper than what the current costs to the business of doing things internally (a private cloud). ITBM's Business Management for the Cloud offering addresses that. Using the financial data from the Financial Management part of the suite and the costs of various public cloud providers (such as Amazon and Azure), the system will look at existing machine costs and inform you of the costs of various competitors. It can also do what-if modeling to see the impact of various options or changes in demand and what the costs associated with each would be. It integrates with vCAC, vCD, and vCenter out of the box to gather usage data of existing VMs. It can also look at a proposed deployment and predict the cost of each through vCAC and the options available there. That is the second part of costing.

The third area in costing is how your specific business costs compares to your peers' costs. You can then decide where to focus on cost savings or better SLAs or whatever with the costs you peers are paying to help ensure you stay competitive. The benchmarks are in the same areas that the Financial Management functionality in the suite tracks—software and hardware costs, personnel costs, etc. and are available for different industries and geographies.

Finally, none of the costing information, while important, covers the costs of downtime and the impact of downtime to users, customers, etc. For this, you need SLA management. This area of the suite allows you to track when an SLA or Key Performance Indicator (KPI) is in jeopardy of not being met, and this information can be compiled into monthly reports on performance to track what the agreements call for vs. what is being delivered. It also allows you to track and manage the vendors' invoices vs. contract terms and actual spending and SLA levels. Thus, costs can be managed and justified or contract terms adjusted if the service levels needed are not being met.

Conclusion

One of the things that most of these technologies share is that they reduce operational expenses (OpEx), not capital expenses (CapEx) that has traditionally been the focus of virtualization. Many companies implemented virtualization with the goal of saving money in the form of fewer servers to buy with the side benefit of reducing the footprint of the servers and lowering the required power and cooling. Most of the savings were in capital; do not expect the same thing with many of the technologies listed here. Some may even require some additional capital expenditures (at least for software) in order to save on the day-to-day operations of IT. The bigger cost in running an IT department is in the OpEx category anyway, so savings there are recurring savings. VSAN and NSX may be the exceptions where CapEx savings may be seen (though licensing costs are associated for these products).

It's also important to note that you can implement any or all of the four categories as mentioned at the start of this white paper. Each brings a different set of requirements and overhead to solving the challenges you experience in your environment.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through authorized VMware training.

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

John Hales (A+, Network+, CTT+, MCSE, MCDBA, MOUS, MCT, VCA-DCV, VCA-Cloud, VCA-Workforce Mobility, VCP, VCP-DT, VCAP-DCA, VCI, EMCSA) is a VMware instructor at Global Knowledge, teaching all of the vSphere and View classes that Global Knowledge offers. John has written a book called Administering vSphere 5: Planning, Implementing, and Troubleshooting published by Cengage, as well as other technical books—from exam-preparation books to quick-reference guides, as well as custom courseware for individual customers. John lives with his wife and children in Sunrise, Florida.