Managing the Virtualized Data Center

A PRACTICAL GUIDE TO
VMWARE OWNERSHIP

OVERVIEW

Many companies are implementing virtualization technology (most notably VMware®) to achieve a variety of benefits – including reduced capital spending on hardware, reduced power and cooling demands, and more flexible allocation of processing capacity.

Virtualization, however, creates many new management challenges. These new challenges arise from two basic causes:

1. Virtual servers by their nature need to be managed differently from physical servers, and
2. Data centers are only partially virtualized. That is, servers may be physical machines or they may be virtual servers sharing physical machines with other virtual servers.

The co-existence of virtual and physical servers in the data center adds a new level of complexity to management operations. As a result, IT managers must re-think the way they manage their increasingly dynamic mix of virtual and physical servers.

Avocent's management solutions are ideal for managing this emerging virtualized server environment. With Avocent solutions, IT organizations can:

- Access virtual and physical servers from a single interface
- Access virtual servers distributed across multiple VMware Virtual-Centers from a single interface
- Consolidate events and alerts from both physical and virtual servers
- Granularly control access rights to both virtual and physical servers in a common manner
- Maintain management assignments for virtual servers even as they are moved from one physical machine to another
- Granularly audit management operations performed on both virtual and physical servers

These are all essential capabilities that virtualization vendors do not themselves provide.

This document explains how virtualization will impact your management operations, as well as the role Avocent solutions can play in ensuring that your transition to virtualization is a successful one. It is based on the hard-won experience of early virtualization adopters. By taking the advice offered here to heart, IT organizations can avoid many of the pitfalls associated with VMware ownership – and maximize total business returns on their investment in virtualization technology.

WHY VIRTUALIZATION?

IT organizations are under constant pressure to do more with less. They are constantly being asked to roll out more applications, support more users, deliver higher service levels, and handle more intense processing workloads. And their budgets are rarely increased proportionally to these escalating demands.

Virtualization offers relief from these demands in several ways:

More efficient, "multiplexed" use of server hardware

Instead of having to devote individual servers to each application, virtualization allows multiple applications to be run on a single server – as long as those applications only utilize a relatively small percentage of the physical server's resources. This ability to run multiple applications on a single server can substantially reduce capital spending

on server hardware. Lifetime ownership costs may also be lower for a single large server than they are for multiple 1U rack units.

Respite from the physical limitations of the data center

Many IT organizations have maxed out the physical capacity of their existing data centers in terms of floor space, cooling capacity and/or power utilization. They would therefore not be able to add more servers without expanding or moving their data centers – which would be prohibitively expensive. Virtualization lets them postpone such a painful undertaking by allowing them to load more applications onto the server infrastructure they already have in place.

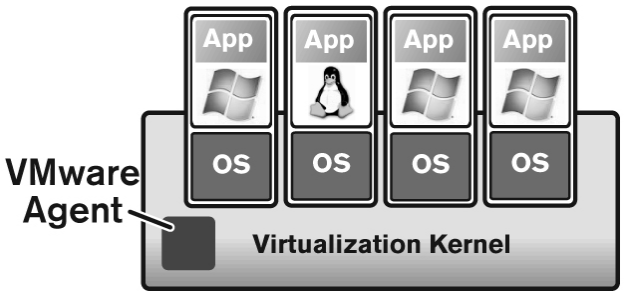
Cost-effective provisioning of high availability

With virtualization, IT organizations can provision failover servers far less expensively than they can with actual physical machines. Virtualization can also make it economically feasible for them to provision secondary servers so that they don't have to interrupt critical services while they perform maintenance or backup tasks on their primary servers.

Greater flexibility for meeting production and development requirements

IT organizations are often called upon to quickly provide servers in order to handle spiking workloads or support development projects. Doing this with physical servers can be expensive and slow – and fairly wasteful if the server is only needed for a limited amount of time. Virtualization, on the other hand, theoretically allows them to respond to these needs almost immediately without any incremental hardware cost.

These are just some of the reasons that IT organizations are introducing virtual servers into their data center environments. Some are actually using virtual servers as managed desktops that users access from PCs that only run thin clients. Others are using virtualization as a means of "cloning" configurations across departments and locations.



Every IT organization must have a clear sense of why it is implementing virtualization – and stay attuned to potential benefits it may have originally overlooked.

Key questions for IT managers include:

- *What primary benefits are driving your virtualization implementation? Reduced hardware costs? Faster response to business needs? Provisioning of high availability? Some other reason? A combination of reasons?*
- *Are you trying to reduce server hardware purchases or utility costs by a specific amount this year?*
- *Which applications are you initially targeting for virtualization? Why?*
- *How long are you hoping virtualization will enable you to defer expansion or relocation of your data center?*

VIRTUALIZATION IN THE REAL WORLD

As appealing as virtualization may be, IT organizations are introducing it into their environments with varying degrees of caution. Some are only starting to experiment with virtualization solutions in the lab. Others have begun to roll virtual servers out into production. But even the most enthusiastic early adopters of virtualization are only applying it to a certain percentage of their new production machines. And no one is overhauling their entire IT environment to make it entirely virtual.

In fact, for many applications – especially high I/O ones like email – virtualization is neither practical nor advisable. No data center will, therefore, ever be fully "virtualized." Different companies will implement virtualization to different degrees, but IT organizations will always have to deal with a mix of physical and virtual server resources.

The reasons for this include:

Investments in physical servers are significant. Companies have spent years buying server hardware, integrating those servers into their environments, and fine-tuning those servers to optimize application performance. They will not scrap those investments any time soon.

IT organizations are still figuring out how and when to implement virtualization. As they complete pilot projects, IT professionals are finding out that they have a lot to learn about virtualization technology. They're discovering that virtualization can cost them more CPU overhead than expected. They're discovering that application I/O can limit their ability to run multiple virtual servers on a single physical machine. These discoveries are causing them to be more disciplined and methodical in their roll-outs of virtual server technology.

They're running into management problems. Most of the business case for virtualization revolves around deploying infrastructure. But IT organizations spend a significant percentage of their budgets keeping infrastructure up and running. As IT organizations encounter first-hand the unique problems associated with managing virtual servers, they will have to figure out how to overcome those problems – and then re-consider the role virtualization will play in their long-term data center optimization strategies.

Adoption rates depend on many non-technical factors. Even if virtualization could fully live up to its hype – which it cannot – many other factors will slow adoption. IT organizations still have to come to terms with vendors. Potential investment in virtualization has to compete with other items on the IT to-do list. Application vendors have to deliver appropriate support for virtualization. And IT organizations may find other ways to overcome resource constraints, including open source and on-demand software.

For these reasons and others, virtualization will always occur in the context of phased implementation occurring in an environment that is either partially or – as is more likely – mostly physical. There are not now and there will be no 100% virtualized data centers. There will only be virtual servers that must be managed in conjunction with their still-physical counterparts.

Every IT organization must therefore understand the factors that constrain its implementation of virtualization technology. Key questions for IT managers include:

- *What percentage of your servers are virtual today? What percentage do you believe will be virtual a year from now?*
- *What percentage of all new servers being rolled out are now virtual? What percentage do you believe will be virtual a year from now?*
- *What is preventing you from rolling out virtual servers more aggressively?*
- *Are you concerned about how future virtualization moves by Microsoft may affect your company's long-term virtualization strategy?*
- *What is your biggest fear about virtualization?*
- *What technical issues have you run into in your initial implementations of virtual server technology?*
- *What other technologies are you considering to help you with your cost and flexibility issues?*
- *Have you run into any technical or logistical issues managing your virtual servers?*

THE IMPACT OF VIRTUALIZATION ON SERVER MANAGEMENT

Virtualization technology can help IT organizations significantly improve the economics of data center infrastructure. However, virtualization also introduces new complexities and challenges when it comes to managing that infrastructure. Some of these challenges arise from the nature of virtualization technology itself. Some of them arise from the fact that virtual servers must be managed in conjunction with all the servers in the data center that remain "unvirtualized." Together, these two sets of challenges significantly impact the way IT organizations must operate.

Challenges that arise from the nature of virtual server technology itself include:

Giving specific IT staff appropriate privileges for specific virtual machines

It can already be somewhat complicated to give specific IT staff access and appropriate operational privileges for specific physical servers. Authorized systems administrators, for example, may have to be given root access – while application specialists are only given access to the software running on the OS. When multiple virtual servers are running on individual physical machines, the administration of these rights becomes even more complex. To provide an application specialist with access to just one of the ten virtual servers running on a given physical machine, for example, an IT manager has to administer appropriate privileges on that physical machine's ESX Service Console – which is the management gateway for both the VMware virtualization layer – and the individual virtual servers running on the physical machine.

Matters get even more complicated as IT organizations implement more virtual servers. That's because they have to implement VMware VirtualCenter to manage multiple ESX servers. However, most IT managers don't want to give their systems administrators and application specialists access to VirtualCenter, because such access would potentially give them inappropriate control over the data center's virtual infrastructure. So, instead, they manually provide their technical staffs with the IP addresses and/or management URLs of the specific virtual machines for which they are responsible.

Maintaining management assignments as virtual servers move from one physical machine to another

This manual approach to the distribution of IP addresses and/or management URLs can create problems if and when virtual servers are moved from one physical machine to another. A company's VMware manager, for example, may choose to shift virtual servers between physical machines in order to balance workloads or handle utilization

spikes. However, this may leave application specialists temporarily in the dark until they can be provided with the new location of the virtual servers for which they are responsible. Even worse, VirtualCenter can be set up to automatically move virtual servers based on pre-defined business rules. If such an automatic move occurs without corresponding notification to all affected IT staff, technicians who don't have direct access to VirtualCenter may not be able to find their servers at all.

Accessing multiple virtual servers connected to different Virtual Centers

At this time, VMware doesn't enable IT staff to unify their views of multiple virtual servers residing on different physical machines, if the ESX Service Consoles of those different physical machines are connected to different VirtualCenters. Of course, each VirtualCenter can theoretically manage hundreds of physical servers. However, It organizations have generally chosen to deploy multiple VirtualCenters before they reach that threshold in order to segment their virtual environments by platform or location. So, if virtual servers in two locations support a single application, the application specialists in charge of that application can't view both servers from a "single pane of glass."

Protecting many virtual servers from component failure in a single physical server

With physical servers, there is a one-to-one relationship between component failure and application outage. When multiple applications are running on that same server, the stakes go up. Virtualization theoretically insulates applications and services from component failure by enabling IT organizations to run mirrored virtual servers and/or to quickly migrate virtual servers from one physical machine to another. But not all IT organizations have sufficient idle capacity on their other VMware-enabled servers to handle the workloads that would result from the simultaneous loss of twenty or more virtual machines due to the failure of a single physical machine. So IT organizations implementing VMware have to be particularly sensitive about the vulnerabilities created by multiplexing large numbers of virtual servers onto a single physical machine – and they must be sure they have the out-of-band access to those physical machines necessary to address BIOS- and hardware-level issues.

Exclusive use of Microsoft Active Directory

VMware uses Microsoft Active Directory exclusively to administer management rights and permissions. This can potentially be problematic for IT organizations that need to drive management access using technologies such as LDAP, RADIUS and single sign-on in order to support their broader infrastructure management architecture.

Challenges that arise from the fact that virtual servers must be managed in conjunction with all the servers in the data center that remain "unvirtualized." include:

Managing physical and virtual servers in a common manner

For virtualization to be truly transparent to technicians, virtual servers and physical servers must be managed in a common manner. That is, systems administrators, application specialists and others should not need to specifically know whether the server they have to manage is virtual or not. They shouldn't have to use an entirely different piece of software to access each type of machine. However, if they use VMwaretools alone, this is exactly what will happen. The VMware Remote Console is actually a client-side executable that responds to files with the .vxm file extension. So users will view the virtual servers for which they have management permission through the VMware Remote Console client, while they will use some other management application for their "regular" servers.

Consolidating events and alerts from both physical and virtual servers

In addition to accessing physical and virtual servers themselves in a common manner, technicians need to view management events from both sets of resources on a "single pane of glass." This is important for ensuring that all events are responded to in a timely manner and that multiple alerts stemming from a single root cause aren't handled in a fragmented manner. By itself, VMware only displays events from virtual servers and the physical servers that host them.

Administering access rights across both virtual and physical servers

The administration of access rights to physical data center assets is already a fairly complex affair. And, as noted above, the administration of access rights to virtualized server resources is itself likely to become increasingly complicated. If these two administrative tasks have to be performed entirely independently of one another, the overall complexity of access privileges will be overwhelming. It is therefore essential for IT organizations to come up with a single, streamlined method for authorizing, modifying and withdrawing access privileges on a granular basis across all physical and virtual resources.

Auditing management operations performed on both virtual and physical servers

As compliance pressures mount, IT organizations must be increasingly diligent about auditing staff access to servers that handle critical and/or security-sensitive data. They also have to be sure they can respond to inquiries from internal and external auditors.

These auditors expect all management operations relating to a given business function or application to be maintained in a single log. In fact, in some instances, the use of multiple audit logs may violate standard compliance practices. It is therefore essential for IT organizations to implement a common auditing mechanism for work performed on both virtual and physical servers.

The above are some of the initial management challenges that early adopters of VMware and other virtualization technologies are discovering as they roll out virtual servers in their data centers. There are likely to be others as well. The main point is that the emerging "partially virtualized" data center is even more complex to manage than conventional environments – and that VMware native management tools are insufficient for addressing this complexity.

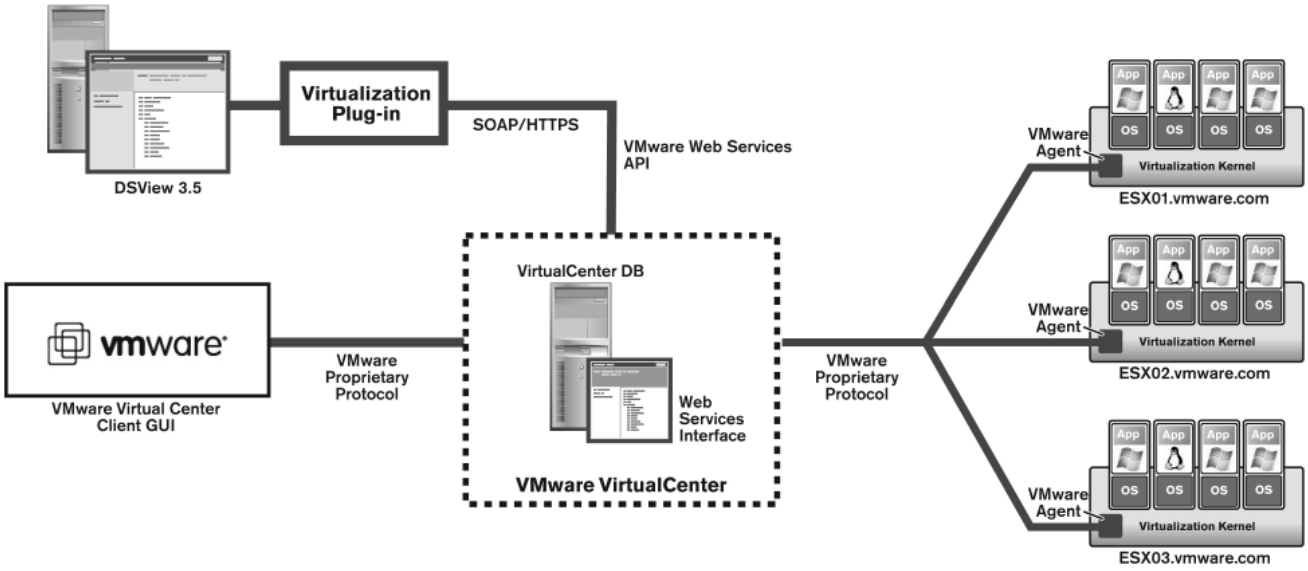
Every IT organization must ensure that it is fully cognizant of all potential management issues it will face as it embraces virtualization in the data center. Key questions for IT managers therefore include:

- How are you authorizing your staff to access virtual servers? How do you authenticate them at the server?
- What's your change process for both moving virtual servers and ensuring that the right people can still access that server once it's been moved?
- Are you giving everyone access to VirtualCenter? Why or why not?
- Have you implemented multiple VirtualCenters? Have you encountered any issues trying to manage resources across multiple VirtualCenters?
- How are you protecting your multiple virtual servers from failure of their shared underlying physical server? Are there specific virtual servers for which this is a greater concern than others?
- Are you using Active Directory across all of your management tools? If not, how are you going to integrate your Active Directory for virtualized servers into the rest of your management environment?
- Are you going to set up separate management teams for your virtual and physical environments? If not, is your goal to manage both in a common manner? What is your timeline for doing so?
- Do you want to collect events and alerts from both virtual servers and physical servers in a "single pane of glass?" How do you plan on doing this?
- Are you going to maintain separate audit trails for physical and virtual servers? If so, have you verified with your compliance managers that this is OK? If not, how are you planning to achieve audit consolidation?

AVOCENT: UNIQUE SUPPORT FOR VIRTUALIZATION

Avocent can play a central role in enabling IT organizations to meet the management challenges posed by data center environments that are partially virtualized. Avocent is doing this by:

1. Continuing to deliver the out-of-band remote management capabilities IT organizations need to maintain the health of their underlying physical server infrastructure – regardless of whether or not that physical infrastructure is hosting multiple virtual servers, and
2. Integrating DSView® 3 management software with VMware management tools so that IT staff can access virtual and non-virtual resources in a unified way

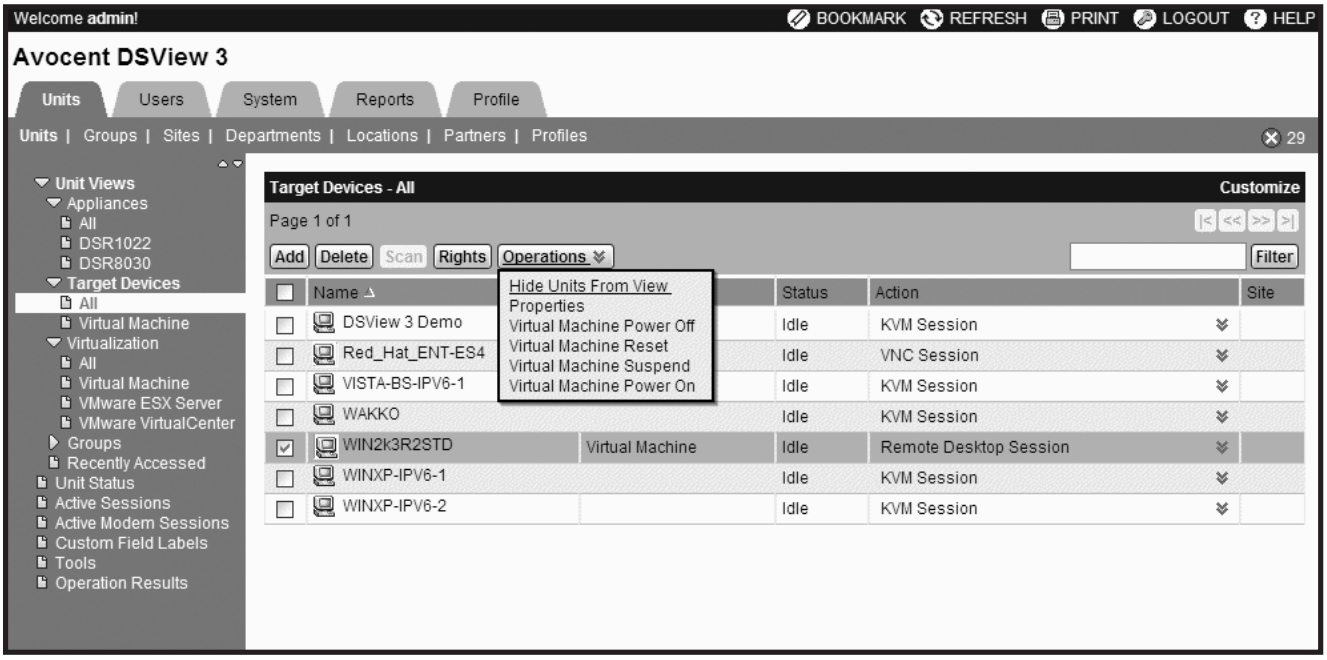


Specific functionality included in Avocent's initial VMware integration includes:

- *The ability to discover Virtual Centers, VMware ESX Servers and the virtual servers they support*
- *The inclusion of these virtual servers as Target Devices*
- *The ongoing synchronization/updating of the Target Device list as virtual machines are created, torn down or moved*
- *The ability to access virtual servers via the VMware Remote Console, a Web browser or RDP – as well as through the Virtual Infrastructure Client (VI Client) or Virtual Infrastructure Web Access of the VirtualCenter server associated with the ESX Server hosting the virtual server*

- *The ability to granularly administer management rights for virtual servers in a common manner with other target devices from the DSView 3 administration console – and to automatically replicate that permissioning in the corresponding ESX server*
- *The inclusion of events and alarms from VirtualCenter Management Servers and VMware ESX Servers in the DSView 3 event log for display and associated actions*
- *The capture of all management operations performed on virtual servers in the DSView 3 audit log*

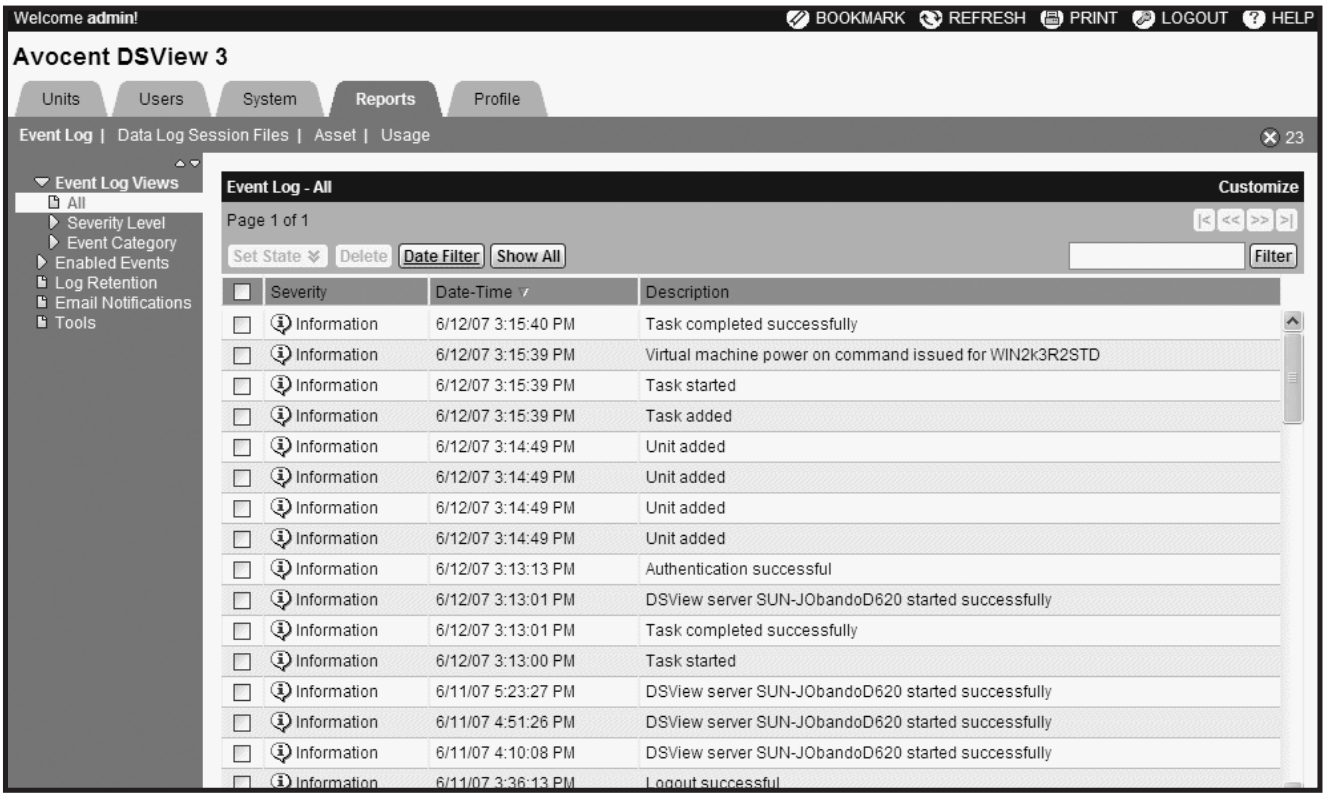
These new capabilities will provide IT organizations with several critical advantages as they move forward with their virtualization plans, including:



The ability to access physical and virtual servers from a single management application. IT staff will not have to know whether the device they need to access is physical or virtual. They will be able to pick any managed server from a single list of Target Devices.

The ability to access virtual servers from a single "pick list" regardless of which VirtualCenter it is associated with. IT staff won't have to search multiple instances of the VMware VirtualCenter management application to find a particular virtual machine. Also, virtual machines associated with any VirtualCenter can be included

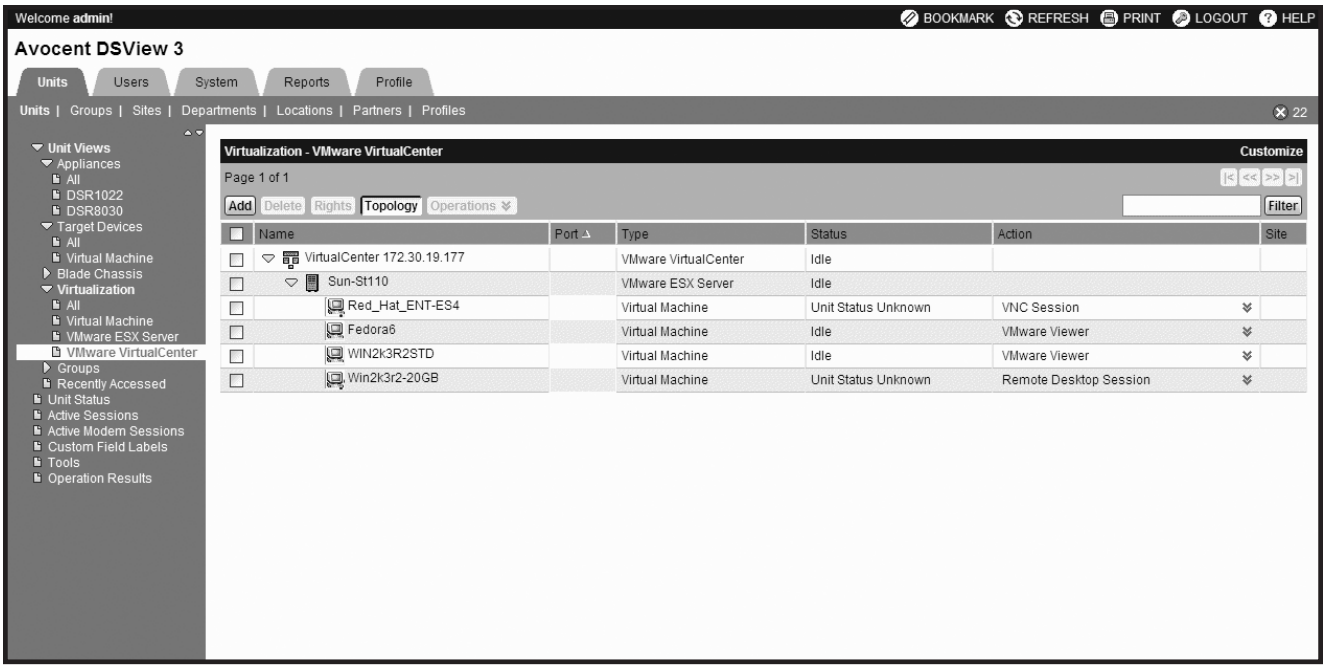
in the same "pick list" as physical servers anywhere across the enterprise – providing IT organizations with complete flexibility in assigning management responsibilities to technical staff.



A unified view of all server events and alarms, regardless of their source. By using DSView 3 software to consolidate data collected from virtual and physical servers, IT organizations can eliminate the need to "toggle" between multiple applications.

The ability to granularly assign management rights to technical staff across virtual and physical servers using any single directory solution-of-choice. DSView 3 software eliminates the use of separate administrative silos by allowing IT managers to allocate access and specific permissions for all servers across the "virtualized" environment from a single console.

A unified audit trail for all server management. By using DSView 3 software to access both virtual and physical servers, IT organizations can generate a single log for all remote management activity.



Simplified change management. Instead of having to manually re-distribute IP addresses or management URLs every time a virtual server is moved from one physical machine to another, DSView 3 software will automatically discover such moves – even if they occur across multiple VirtualCenters – and thereby keep IT staff's authorizations and individual "pick lists" up-to-date.

Improved security. DSView 3 software's authentication and encryption mechanisms are stronger than those provided by VMware – which is a particularly important consideration in light of the havoc an unauthorized user could wreak on multiple virtual servers if he or she gained access to an ESX Server's Remote Console or (even worse) a VirtualCenter Management Server.

These additional new capabilities are, of course, in addition to the current remote management functionality that DSView 3 software and Avocent KVM switching solutions provide – which continue to be essential for streamlining data center operations. In fact, those capabilities may be even more important now that the health and availability of multiple applications may now depend on the health and availability of a single physical server.

MAJOR BENEFITS FOR VIRTUALIZATION ADOPTERS

The previous section described the specific technical capabilities Avocent solutions offer IT organizations as they implement virtualization technology. However, it's important to understand how these capabilities actually benefit both IT organizations and the businesses they support.

In reviewing these benefits, it is important to maintain a good historical perspective on the introduction of new technologies into the enterprise. When PCs were first introduced into the corporate world, for example, they offered users the ability to be much more productive and to perform a wide range of new tasks. But they also had notoriously high total ownership costs, which ultimately undermined real return on investment (ROI). That's why LANs and PC management tools became so important in the late 80's. Internet and desktop browsers also offered enormous potential in the late 90's. But IT also had to move quickly to standardize browser versions, to limit non-legitimate web browsing, and to protect the enterprise from the flood of malicious code that Internet connectivity exposed it to.

Virtualization is a similar phenomenon. It offers a wide range of benefits in terms of data center economics. But, if it's not appropriately managed, it will quickly become a source of higher costs and bigger headaches.

Here, then, are key benefits that IT organizations should consider as they decide whether or not to take advantage of Avocent solutions as part of their overall strategies for the introduction of virtualization into the data center:

Lower cost of virtual technology ownership – and higher ROI

If IT organizations have to maintain a management "silo" for their virtual servers, the cost of owning those virtual servers will be higher than if those servers are managed in the same way as non-virtualized servers. It's also interesting to note that – because virtual servers have very low amortized hardware costs – management and administration comprise an even larger percentage of their total cost of ownership (TCO). By simplifying and unifying management of the "virtualized" data center, Avocent reduces TCO for virtual servers and therefore improves total return-on-investment for virtualization.

Faster responsiveness to business change

If it's not easy for IT organizations to keep technicians connected to the virtual servers they have to manage even as those virtual servers are moved from physical machine to physical machine, then they will be inhibited from making such moves. By automating these changes in virtual server access, DSView 3 software eliminates this inhibiting factor and ensures that IT organizations can take full advantage of the flexibility that virtualization promises.

Reduced risk

There are a variety of risks associated with implementing any new technology. In the case of virtualization, these risks include unanticipated management snafus, security exposure, and compliance issues. By subsuming the management of virtual resources into a server management solution with a proven track record in terms of control, security, and auditing, Avocent solutions mitigate many of these risks.

The ability to more broadly deploy virtualization

If virtualization lives up to its promises, then IT organizations will want to implement it more and more extensively. Unfortunately, those that have tried to do so start "hitting the wall" at about 1000 virtual servers – due to the limitations of VMware native tools. Because Avocent solutions overcome these limitations, they allow IT organizations to deploy as many virtual servers as they want.

Because many IT organizations have focused up until now on simply figuring out how virtualization works from a technical point-of-view, they may not have fully considered how to optimize its impact on the business over the long term. Key questions for IT managers therefore include:

- *Do you know what your TCO is today for your physical servers? Have you projected your TCO for virtual servers? What percentage of this TCO is related to management and administration? Would you like to reduce this number?*
- *How long does it take you to add or shift server capacity today? How quickly do you want to be able to do so with virtual servers? What factors might limit your ability to achieve these responsiveness goals?*
- *What do you consider to be the main risks associated with your virtualization rollout? What are you doing to mitigate those risks?*
- *What if virtualization is a success? How will you scale up your implementation?*

Virtualization will continue to evolve, and it is likely to become an integral aspect of every enterprise data center. This makes it critically important to implement management solutions that both address the immediate challenges presented by virtualization – and that come from a technology partner with a proven history of responding to ongoing changes in data center architectures. Avocent is clearly that technology partner.

Please visit www.avocent.com for additional complimentary virtualization technology information.

1007-SVDC_ENDUSER-AB-EN