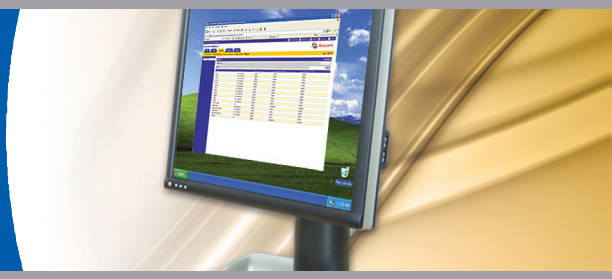
DSView® 3 Management Software

Unique Support for VMware Environments



Companies are implementing VMware's virtualization technology to reduce capital hardware costs, limit power and cooling demands, and more flexibly allocate 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) No data center is 100% virtualized – so virtual servers and their "conventional" physical servers must be managed in some common manner

The long-term success of any company's virtualization strategy thus depends to a large degree on how well it meets these two core management challenges.

MANAGING VIRTUAL SERVERS

The first set of challenges companies face as they implement virtualization arise from the nature of the technology itself. These challenges include:

Giving specific IT staff appropriate privileges for specific virtual machines
Because multiple virtual servers run on each physical machine, administration of privileges is more complex than it is with physical servers. To provide someone with access to just one of the ten virtual servers running on a given machine, for example, a manager has to administer privileges on both that physical machine's ESX Service Console and the individual virtual server. Things get even more complicated when VMware's VirtualCenter is used to manage multiple ESX servers.

Managing privileges as virtual servers move between machines
As virtual servers are moved from one physical machine to another in order to balance workloads or handle utilization spikes, new administration issues arise – especially if technicians are "in the dark" about the new location of the virtual servers for which they are responsible. This problem can become even worse if VirtualCenter is set up to automatically move virtual servers based on pre-defined business rules.

Accessing multiple virtual servers connected to different Virtual Centers
VMware doesn't currently enable IT staff to unify their views of multiple virtual servers connected to different VirtualCenters – which is what usually happens as IT organizations 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. So IT organizations have to be particularly sensitive about the vulnerabilities created by running multiple virtual servers on a single physical machine – and must have the out-of-band access necessary to address BIOS- and hardware-level issues on those machines.

Exclusive use of Microsoft Active Directory
VMware uses Microsoft Active Directory exclusively to administer management privileges. This can be problematic for IT organizations that use technologies such

Here are some important questions to ask as you determine how you're going to manage the virtual servers in your data center:

- *What percentage of your servers are virtual today? What percentage do you believe will be virtual a year from now?*
- *What's your change process for both moving virtual servers and ensuring that the right people can still access that server once it has been moved?*
- *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 VMware 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?*
- *What is your TCO for your physical servers? Have you projected your TCO for virtual servers?*
- *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?*

as LDAP, RADIUS and single signon to support their broader infrastructure management architectures.

MANAGING VIRTUAL AND "CONVENTIONAL" PHYSICAL SERVERS TOGETHER

The second set of challenges that companies face as they implement virtualization arise from the fact that it is inefficient to manage virtual servers as a separate "silo" from other servers. These challenges include:

Managing all servers in a common manner
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.

Consolidating events and alerts from both physical and virtual servers
Technicians must be able to view management events and alerts from both set of resources on a "single pane of glass." This is important for ensuring that infrastructure issues are responded to in a timely manner and that multiple alerts stemming from a single root cause aren't handled in a fragmented way.

Administering privileges for both virtual and physical servers
IT organizations need a single, streamlined method for authorizing, modifying and withdrawing privileges on a granular basis across all physical and virtual resources. Otherwise, the administration of privileges will become unacceptably complex and costly.

Auditing management operations performed on both virtual and physical servers
As compliance pressures mount, IT organizations must be increasingly diligent about auditing access to servers that handle critical and/or security-sensitive data. Auditors want the audit information maintained in a single log. In some cases, use of multiple logs may itself constitute a compliance failure.

AVOCENT AND VMWARE

Avocent's solutions are extremely useful for addressing the full range of management challenges posed by the partial virtualization of the data center. That's because:

1) Avocent delivers the out-of-band remote management capabilities necessary to maintain the health of the physical server infrastructure that host virtual servers

2) Avocent's DSView® 3 management software integrates with VMware tools so IT staff can access virtual and physical servers 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
- 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 tools, a Web browser or RDP
- Granular administration of virtual server permissioning
- Inclusion of events and alarms from VMware in the DSView 3 Event Log
- Capture of all management operations performed on virtual servers in the DSView 3 Audit Log

These capabilities provide several critical advantages for IT organizations as they move forward with virtualization, including:

Access to all physical and virtual servers from a single management application. IT staff won't have to know whether a server is physical or virtual. They can pick any managed server from a single list of Target Devices.

Access to all virtual servers from a single "pick list" across all VirtualCenters. IT staff won't have to search multiple instances of the VMware VirtualCenter management application to find a particular virtual machine.

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 use 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 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. DSView 3 software automatically discovers virtual server moves – even if they occur across multiple VirtualCenters – and keeps privileges and "pick lists" up-to-date. This eliminates the need to manually re-distribute IP addresses or management URLs.

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

These operational advantages translate directly into bottom-line business benefits, including:

- **Lower cost of virtual technology ownership – and higher ROI**
- **Faster responsiveness to business change**
- **Reduced risk**
- **The ability to more broadly deploy virtualization**

Virtualization will likely to become an integral aspect of every enterprise data center. This makes it critically important to implement management solutions that address the immediate challenges presented by virtualization itself – as well as the long-term challenges that will arise from managing a dynamic mix of virtual and non-virtualized servers. By uniquely addressing both sets of challenges, Avocent offers compelling value for today's IT organization.

0907-DSV-VRTShort-AB-EN