

Centralized Management Software: Best Practices to Control Your Data Center

How to achieve secure access to any server or network device from a single interface

Centralized Management Software: Best Practices to Control Your Data Center

Table of Contents

3	Executive Summary
4	Introduction
4	Centralized Access and Control
4	Tracking the Tools
5	Integrating Many Into One
5	Avocent Data Center Management Tools
6	KVM Server Management
6	Serial over IP
7	Power Management over IP
7	Full Remote Access
7	Conclusion



Executive Summary

Distributed enterprises and network operating centers require powerful, centralized, and remote control of computer systems, serial-based devices, and power distribution products such as UPS and power strips. To effectively manage all of these disparate devices from a single console, a comprehensive user interface is necessary to provide point-and-click connectivity and enforce strong access and control.

A good centralized management platform easily provides a solid return on investment in many ways. It lets you control multiple devices from a single system, helping to reduce complexity and downtime by giving users a fast and easy method to complete a variety of tasks. And, it lets you quickly take control or log on to a piece of network hardware from a single interface, one that is accessible from anywhere.

The Avocent family of management solutions handles all of these problems and more. DSView® 3 management software, used in conjunction with Avocent appliances, provides you with secure, browser-based remote access to any server or network device, all from a single interface.

Centralized Management Software: Best Practices to Control Your Data Center

Introduction

Today's data centers contain a wide range of devices including application servers, email servers, database servers, Web servers, and e-commerce servers. These servers may consist of Intel-based servers, RISC servers, and even legacy minicomputers and mainframes. These servers run many operating systems including Windows, UNIX, Linux, and others.

The data center also includes numerous communication devices, such as routers, gateways, VPNs, and firewalls. And, all of these components require power, which is often managed by UPS devices, surge protectors, and power strips.

Business computing needs will always grow, which in turn increases the complexity of systems the IT administrator is responsible for managing. As an administrator, you have to add new hardware and systems as business needs require without sacrificing your existing management platform; you have to maintain additional servers without creating additional support problems.

In any medium to large organization, it's rare for all of the network service components to be in one location. Branch and remote office environments often require key network components to be dispersed to many locations, sometimes all over the world. This can present an access problem for IT administrators.

Budget constraints usually mean that branch locations have very little in the way of IT support. It is often up to the IT administrator at the central office to troubleshoot and fix problems with systems that may reside hundreds or even thousands of miles away.

Centralized Access and Control

To be most effective, IT managers need a centralized management solution that gives them full remote access to all of the components regardless of their location. And, centralized management should mean more than just controlling each component from one desk. You should be able to see a combined view of all your connected servers and devices on a single computer monitor, in a single interface.

Network data systems are made up of disparate components from many different vendors. A useful remote management solution must be able to handle the needs of several different operating systems. It will not only provide control for PC-based systems, but also serial devices and AC power solutions.

Underlying all of these requirements is the need for security. Your management platform should secure access to your devices by leveraging the directory system you already have in place, allowing you to use a single user name and password repository. You should

be able to assign device-level rights based on a user's name so that administrators have access to more devices than an entry-level technician. Auditing and logging of all activity is also important so that you can keep track of "who does what" with your network infrastructure and all the devices attached to it.

Tracking the Tools

Most vendors have a way of remotely accessing and managing their equipment, but each tool is different. As the number of devices that need to be monitored, managed, and maintained grows, finding the right management tool or utility can be a chore.

For example, the typical enterprise will have network switches in racks that are normally managed using a Telnet session—either over a physical serial connection or via IP. Other devices, such as firewall and security appliances, are monitored and managed over an IP network using Web-based or Telnet-based management or through a third-party SNMP monitoring platform.

Intelligent Platform Management Interface (IPMI) technology allows IT administrators to monitor and control mechanical elements of their servers' hardware, such as temperature, fans, and power supplies. Add keyboard, video, and mouse (KVM) switches and other commonly used tools such as remote management software, and the issue of access and control becomes quite complex.

Multiple tools mean multiple interfaces, multiple systems to learn, and no single point of management. Because there is no integration between the tools and no single interface to work from, you will have to connect using a method specific to that piece of equipment on your management console. This means you have to maintain multiple software clients, IP address lists, physical serial connections, and possibly other special hardware in order to connect to a device.

With multiple tools, the administrator has to become an expert on each different management solution. Learning curves are further exaggerated because each piece of hardware is a stand-alone piece of equipment that shares little or nothing with the other systems in the enterprise.

Without a centralized management console, there is no centralized user access management between each system. Each connection type must maintain its own user and password list—no sharing of information. A good centralized management platform should provide the benefits of single sign-on, where a secured authentication provides the necessary authorization and tracking for all of the tools, interfaces, and utilities that a specific IT administrator needs.

Integrating Many Into One

By combining your miscellaneous management tools into a single integrated platform, you can not only centralize your access control to each device, but also provide a smoother, more streamlined interface (see diagram).

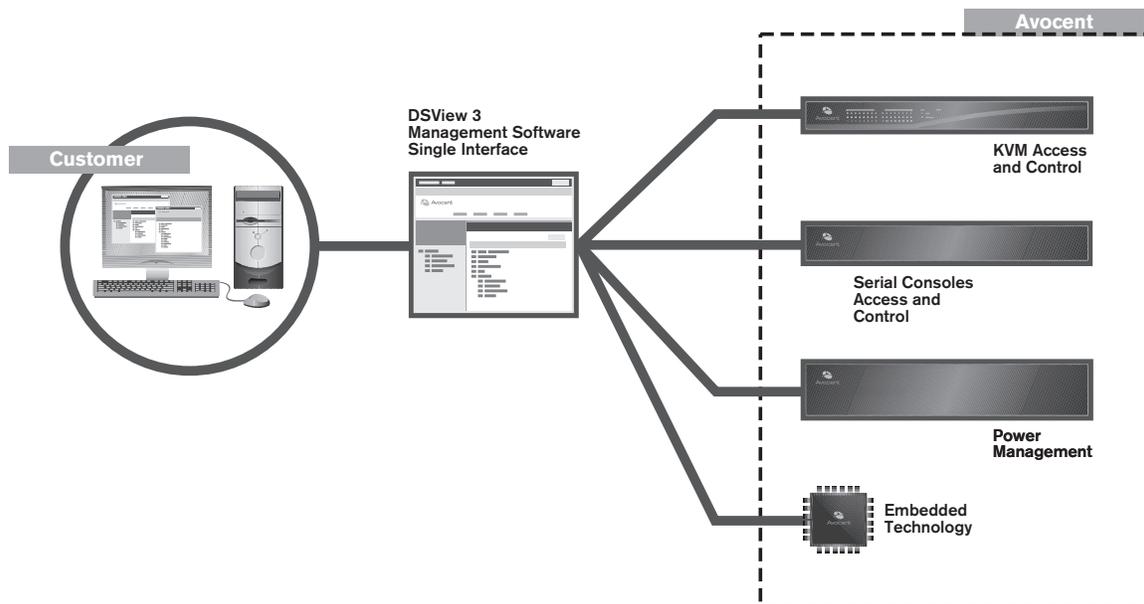
An effective solution must have access to all of these tools and components even when the network, server hardware, or the installed operating system is having problems. That means out-of-band management options that provide redundant access, because your management platform has to work all of the time.

Console management appliances must provide out-of-band access via dial connectivity. The right console management solution should let the appliance act as a PPP server. And it's important that the appliance supports authentication and access control on dial connections. An integrated management solution speeds up the diagnostic process. Gathering information about a problem and then fixing that problem can be accomplished faster when the IT administrator can turn to a single console with a unified interface. When systems are diagnosed, repaired, and brought back online quickly, users experience very little downtime. They are more productive, the company runs more efficiently, and the organization is more successful.

Avocent Data Center Management Tools

Avocent has the right combination of hardware, software, and embedded technology to provide you with a unified interface, centralized user management, and connectivity to all of your servers and devices. The need to learn and manage multiple software systems is eliminated with the comprehensive Avocent solution.

Avocent KVM switch products and serial console appliances work in conjunction with DSView 3 software to offer a complete data center management solution from a single graphical user interface (GUI). Power control is accomplished through embedded IPMI or through power strips which are also integrated into this single interface. It's an arrangement that offers you complete access and control over all aspects of your IT infrastructure.



Centralized Management Software: Best Practices to Control Your Data Center

KVM Server Management

KVM solutions can reduce management costs while providing enhanced access to servers. With a KVM solution, administrators can control hundreds of servers and serial devices from a single console.

To meet the needs of remote management, some companies have installed remote control software on target servers. Such software lets network administrators both issue commands and retrieve performance and other information. However, these software-only solutions require that the device is online and the operating system is already loaded. Often the most important time a user needs access to a server or other device is when there is a problem. How can you connect and resolve a device problem when it doesn't respond to a ping or the operating system is simply hung? That is when the addition of an out-of-band solution can provide many more remote management options.

Avocent KVM solutions do not depend on any type of software agent on the host system, so you have complete access to the server as if you were sitting at its console without interfering with the system itself. And, that direct access is not dependent on the operating system or services that may or may not be running. A true out-of-band connection will allow access even when network connectivity of the remote server is disabled or the network switch to which it is attached is un-routable.

The most visible benefit of a KVM solution is the elimination of keyboards, monitors, and mice from each server. Servers need not be homogeneous; despite substantial differences, Windows, UNIX or Linux devices can be controlled from the same KVM solution.

Digital KVM over IP switching leverages the power of your existing infrastructure by using standard Ethernet connections to transmit KVM signals rather than relying on proprietary cabling. Avocent invented KVM over IP. KVM over IP solutions make several advanced features possible including sophisticated access controls, user authentication, and activity logging.

By leveraging the existing network infrastructure, Avocent IP-based KVM switches can span multiple server sites and are highly scalable. With KVM over IP, IT administrators need not be on-site with the servers they manage. No need to leave their desks to walk, drive, or fly to the server. They have complete control whether the servers are across the hall or halfway around the world. Embedded KVM solutions provide even greater control of hardware and are growing in popularity among standard rack servers and many blade servers.

Embedded KVM solutions from Avocent can provide access to power controls and monitoring functions through the

Baseboard Management Controller (BMC). This controller is described in the IPMI specification and performs management operations independent of the main system processor. These solutions provide more direct access to out-of-band system performance data and efficient integration with system-level monitoring information.

Where a traditional KVM switch requires the operator to have physical access to the console, the Avocent KVM solutions give administrators browser-based control of all local and remote servers. You have complete access through a single interface.

Virtual media further enables administrators to achieve increased operational efficiency in remote server management by allowing them to remotely load software by mapping a local removable media or mass storage device to a remote server. It eliminates the need to physically load a CD directly to the server to perform data-related functions. The ability to remotely conduct file transfers and other tasks from a CD makes for a more efficient environment and helps keep IT administrators at their desks.

Again, this feature is available through a standard USB connection to the server and does not require any drivers or software to be downloaded. This out-of-band connection even allows for remote file transfers when the remote server is offline or not responding to normal network requests.

Serial over IP

The Avocent serial console appliances provide secure, remote access to the serial console and configuration ports of a wide variety of equipment—including headless servers, network equipment, telco, storage devices and power units—through local or remote IP connections. With secure, in-band and out-of-band connectivity, it ensures quick access to critical devices whether the network is up or down.

When used with DSView 3 software, you can remotely control serial devices from a single interface. The newest appliances offer a full range of console management features, including tools for console redirection such as IPMI and Serial over LAN (SoL).

The Avocent serial console appliances let you connect to your critical network devices in the following ways: VT100 terminal (through dedicated local port), modem (using built-in modem string handling for external modem), terminal emulation (direct connect or dial access), PPP (Telnet or SSH in the appliance via the serial port), and through IP forwarding (the SoL interface).

Power Management over IP

Power distribution and control is a requirement in every data center. Avocent IPMI appliances integrate with DSView 3 software for a single interface to securely monitor and control power and system health on IPMI-enabled servers. Emergency control and access through SoL and power control are also centralized in the software, providing a single point for access and control of all systems in your IT network.

Looking at the list of servers and serial devices in the DSView 3 software interface, a user can click on a server name and the “power state” is presented with three options: on, off or reboot. Using DSView 3 software, the same secure single interface is used to manage KVM, serial, embedded technologies, and external power devices, including smart power strips.

Full Remote Access

The Avocent DSView 3 management software lets you remotely control all of your network connected devices using a simple point-and-click interface. DSView 3 software uses IP connections, so you can remotely manage or even reboot a server from the data center, your desk or from anywhere you can get on the Internet.

With DSView 3 software, you can have a multi-window display of your devices. This lets you control multiple devices at the same time without having to shut down a session to start a new one. Avocent systems can leverage the existing IP network and take advantage of your current architecture and security model, thus minimizing training and support costs. Other cost-justification criteria include control, scalability, security, space utilization, and even employee recruiting and overtime costs.

Network administrators must examine migration capabilities to accommodate network and other advancing technologies. Some other solutions may work well today but are unable to cope with technology advances without forklift upgrades. By contrast, IP will be a communications standard for the foreseeable future.

When combined with DSView 3 software, Avocent systems also enhance security despite the openness of IP networks. With KVM over IP, serial over IP, and power management over IP, a device and its controlling console can be miles apart. To prevent performance degradation and maintain session security, the client software implements data encryption and compression along the entire path.

Encryption, bolstered by multiple levels of centralized network control, provides network-level security. Permissions and access levels can be set per user down to individual devices, and detailed user logs provide audit trails for added security.

The flexibility of these Avocent solutions means they can add value to any type of environment. They are not limited by distance, operating system or number of devices to be managed. They can be installed and used by IT technicians in various environments.

Data Center Environments. IT administrators are able to manage the systems from their desks without having to travel to the server room, saving time, especially if the data center is in another building or across a corporate campus.

The scalability options provided by these solutions generate other ROI benefits. For example, these solutions can easily accommodate growth in devices and users without time-consuming and costly reconfiguration. And, they are compatible with the devices that you already own. For enterprise users down to small and medium businesses, you can implement Avocent solutions for complete system access.

Branch Office Environments. You achieve centralized control with Avocent solutions. No longer do technicians have to be dispatched to remote locations for service or other action. Out-of-band solutions allow for more reliable troubleshooting and help reduce the time necessary to identify problems at remote locations. This can dramatically reduce the total time needed to identify and resolve common network and operating system issues.

Conclusion

Unfortunately, administrators are not always in the data center when a failure occurs. Factors such as downsizing, business travel, multisite facilities, branch offices, lights-out policies, and 24/7 operations increase the likelihood that failures will occur when administrators are not present.

Keeping up with your remote maintenance chores can be a real burden, especially when your enterprise spans server racks, buildings or even continents. It's reassuring to know there is a solution that provides a unified platform for all of your remote management needs.

With Avocent, you have a single, comprehensive user interface for all of your remote access and control requirements. Avocent offers a point-and-click interface for device control and user-rights management that is completely integrated with the remote hardware. Security and ease of use are key components to the Avocent solution. But most of all, it's the total consolidation of KVM, serial, embedded technologies, and power management into one platform that makes the difference.

About Avocent Corporation

We believe IT complexity should never stand in the way of achieving a business goal.

Avocent is a leader in open, modular software and hardware solutions that rapidly enable our customers to better tackle the chaos of their information technology environments. Our innovations drive lower costs, lower risks and greater agility, enabling IT to meet more and more demanding service levels. It's no wonder that some of the world's leading brands depend on Avocent technology to simply manage their mission critical IT resources. www.avocent.com

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE:EMR), is the global leader in enabling Business-Critical Continuity™. The company is the trusted source for adaptive and ultra-reliable solutions that enable and protect its customers' business-critical technology infrastructures.

Through its Embedded Computing business, Emerson Network Power enables original equipment manufacturers (OEMs) and systems integrators to develop better products quickly, cost-effectively and with less risk.

Emerson is a recognized leading provider of products and services based on open standards such as AdvancedTCA®, MicroTCA™, AdvancedMC™, CompactPCI®, Processor PMC, VMEbus and OpenSAF™. Our broad product portfolio, ranging from communications servers, application-ready platforms, blades and modules to enabling software and professional services, enables OEMs to focus on staying ahead of the competition.

Manufacturers of equipment for telecommunications, defense, aerospace, medical and industrial automation markets can trust Emerson's proven track record of business stability and technology innovation. Working with Emerson helps them shift more of their development efforts to the deployment of new, value-add features and services that create competitive advantage and build market share. Emerson's commitment to open, standards-based solutions goes back over 25 years and our deep understanding of the embedded computing needs of OEMs provide the foundation for the market to look to us for leadership and innovation.

Emerson Network Power.

The global leader in enabling *Business-Critical Continuity™*.

■ AC Power

■ Embedded Computing

■ Outside Plant

EmersonNetworkPower.com

■ Racks & Integrated Cabinets

■ Connectivity

■ Embedded Power

■ Power Switching & Controls

■ Services

■ DC Power

■ Infrastructure Management & Monitoring

■ Precision Cooling

■ Surge Protection