

Managing Servers and Network Equipment: KVM vs. Console Management

White Paper

Using Serial Console Management to Increase Efficiency in the Modern Data Center Environment

Introduction

In today's complex data center environment, there are many types of equipment, running many different operating systems and performing diverse functions. Increasing the amount of equipment and maintaining updates to software, while staying within departmental financial targets and staffing levels, requires increased efficiency on the part of all concerned, from management, to technical leads, to front-line support personnel. Practices that may have been prevalent by tradition do not always provide the highest efficiency and greatest return on investment. This paper reviews key technologies in the management of servers and equipment and evaluates their strengths and weaknesses.

Heterogeneous Environment, Multiple Management Choices

To achieve optimal efficiency in the data center environment it is necessary to look at the types of equipment commonly deployed and to identify what information is needed to effectively manage that equipment. In the main data center there are three different areas, often reflected in how IT departments are staffed. These are network equipment, UNIX/Linux® systems and Windows® systems. We will consider each of these areas in terms of monitoring (centralized and passive collection of information about system state) and management (updating of configuration and code, and mitigation of incidents).

Network equipment is typically monitored via SNMP and OSPF, with capabilities to effectively determine the state of the network, and thus what links are automatically propagated – up or down – between routing node. The major requirements for management are updating routing tables at specific nodes, and updating firmware to accommodate bug-fixes and security enhancements. While routing information can in principle be changed over a network connection, the principle of not changing the configuration of a given interface while being connected over it suggests use of the serial console port as the safest way for updating routing. Firmware updates can be applied over the network (as long as there is a console available in case of trouble), except when the network has to be disabled because of a security incident.

UNIX/Linux servers are typically monitored with a wide variety of methods, from port pingers to agent-based services running on the systems themselves. These methods are usually sufficient to monitor the state of applications running on the server. However, if a problem occurs which causes a system fault, panic, or other severe interruption of the underlying operating system, the only information given is that the system is non-responsive. Management of UNIX/Linux servers is usually handled through secured connections (HTTPS/SSH), either directly or through a console consolidator. Using a console connection is necessary when trying to recover a system from a fault, when performing an initial load, and whenever detailed logging of system changes is required. Direct network connections do not allow for non-repudiable logging of system changes as there is no independent audit function available.

Windows systems historically have required the use of a video console switch. The inability of video console, or Keyboard Video Mouse (KVM), to be effectively automated has been a limiting factor requiring IT departments to rely on expensive KVM over IP hardware to allow remote rebooting of the equipment.

Windows Server™ 2003 provides support for Special Administrative Console (SAC), allowing OS level installation and recovery to use serial console solutions, thereby eliminating the need for KVM over IP technologies.

Operator and Administrator: Two Roles, Two Interfaces

The Operator Interface to a system is the method by which changes are made to the lowest level of the computer and the operating system (BIOS and OS). Typically, operators seek to standardize and automate the process of monitoring and managing their equipment to ensure consistency and to minimize the amount of time they spend working with any individual system. For network equipment, UNIX/Linux systems, and now for Windows Server 2003, the lowest level and most reliable Operator Interface is a serial console port.

The Application Interface to a system is the method by which changes are made to the user applications that run on a given system. The Application Interface usually needs to provide access to all the features that users of the system need to run the applications. For GUI based applications, this interface is typically either video port or network based.

When to Use Serial Console

The serial console is best used to monitor the OS, to ensure that all low level changes to the underlying OS are captured and documented, to revert changes made in error, and to ensure that the OS can be trusted to track changes made at the applications layer. The most effective use of a serial console is when the serial port on the equipment is connected to another device that can provide logging capability to document changes to the system and alerting capability for errors and faults. To maintain auditing integrity, privileged access to the attached device should be managed separately from privileged access to the equipment to which it is connected.

When to Use KVM

KVM exists in two distinct forms. Direct KVM is often used in rack-managed server environments to allow someone in the server room to easily access nearby equipment. If workflow requires technicians to be on the data center floor, then this is an easy form of access. It does not, however, provide for a method of auditing changes if used for operator access.

KVM over IP provides (at greatly increased cost) the ability to manipulate the system through the video port at a distance. Typically, this function is better handled by a combination of serial console access (if available) and the appropriate network protocol – Remote Desktop/Terminal Services/VNC or X-Windows, depending on the OS of reference. The network protocols have the advantages of being less expensive to implement, offer better performance, and do not conflict with the easy application of direct KVM, if desired.

Maintaining Security

It is often said, correctly, that physical access to the equipment defeats any intended security policy. The best form of security (and best method to increase reliability of data center equipment) is to ensure that it remains undisturbed. Data centers should operate in a lights-out mode when possible. If access to the data center is required, cabinets with doors should be considered and physical access to the data center should be monitored. All connections to equipment in the data center, whether remotely while the data center is operating in lights-out mode, or during maintenance when technicians are on the floor, should be through auditable mechanisms. OS and agent software can be used to monitor application changes, but the underlying OS should be monitored in an agent-less manner, such as with a serial console solution.

<i>Serial Console Servers vs. KVM Switches</i>		
	<i>Serial Console Server</i>	<i>KVM Switch</i>
<i>Support</i>		
Serial Devices	Yes	No
Windows 2000	No	Yes
Linux	Yes	Yes
Sun	Yes	Yes
<i>Features</i>		
Distance	Unlimited	Server Room or Unlimited
Dial-Up Access	Fast	None or Slow
Logging	Excellent	Good
Multi-Users/Port	Yes	None or Limited
Bandwidth Requirements	Low	High

Source:
 Venture Development Corporation
 KVM and Console Switch Solutions: Global Market Demand Analysis,
 Volume II: Console Switches, May 2005 (Exhibit III-4)

Digi International
 11001 Bren Road E.
 Minnetonka, MN 55343 USA
 PH: 877-912-3444
 952-912-3444
 FX: 952-912-4952
 Email: info@digi.com
 www.digi.com

Digi International GmbH
 Joseph-von-Fraunhofer Str. 23
 D-44227 Dortmund
 Germany
 PH: +49-231-9747-0
 FX: +49-231-9747-111
 www.digi.de

Digi International (HK) Limited
 Suite 1703-05, 17/F.
 K Wah Centre
 191 Java Road
 North Point, Hong Kong
 PH: +852-2833-1008
 FX: +852-2572-9989
 www.digi.cn

© 2005 Digi International Inc.

Digi, Digi International and the Digi logo are trademarks or registered trademarks of Digi International, Inc. in the United States and other countries worldwide. All other trademarks are the property of their respective owners.

91001357
 A1/1105

