

Moving beyond KVM: the evolution OF SERVER REMOTE CONTROL

Robert Waldie, VP business development UK, Opengear, looks at how lights-out management and virtualisation has changed out-of-band server management in the data centre.

Data centres were once dominated by crash carts, careening down the aisle in a scramble to resuscitate the latest system to have lucked out in the MTBF lottery. Once the server was located and the crash cart's CRT, keyboard and mouse were cabled up, then troubleshooting and remediation could begin. By today's standards, the downtime was geological in scale.

Over time, the data centre has developed complementary strategies and technologies to minimise the impact of such failures. Through virtualisation, hosted application resources and their operating environments are no longer tightly coupled to physical server infrastructure. Redundant power and networking design has eliminated many single points of failure.

Like the crash carts that preceded them, external KVM over IP devices are cabled directly into the server's VGA,

PS2 and USB ports, and operate independently of the server. Historically, KVM over IP devices served the KVM stream over the network using the RFB protocol, but unlike the related VNC, these devices give remote operators BIOS-level control of server systems even with a crashed OS.

KVM over IP switches became an important tool for remediation during outages, acting as remote access concentrators for the high-density server installs typically found in the data centre, serving KVM connections from many servers at the one network endpoint.

Today's data centres have become a complex and diverse ecosystem of interdependent infrastructure. Maximising MTBF and reducing MTTR requires remote management of a multitude of systems, including networking infrastructure, back up power and power distribution equipment, and environmental sensors. This has given rise to sophisticated data

centre infrastructure management (DCIM) appliances, that go well beyond the remote presence capabilities of KVM over IP switches.

Infrastructure management appliances offer a wider variety of physical connectivity, including RS232 serial, USB, and dedicated management Ethernet ports, and a suite of monitoring, logging and alarm notification features. In some instances, these appliances have merged KVM over IP switch and traditional serial console server into the one appliance. However the KVM over IP component in these appliances has been all but deprecated by virtual KVM, which has emerged by way of two key technologies.

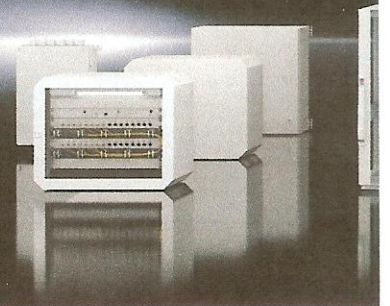
The first of these is the proliferation of service processors and lights-out management (LOM) controllers, such as IMM and RSA from IBM, iLO from HP and DRAC from Dell. Lights-out management controllers are secondary embedded computers housed inside

50 YEARS
Rittal. Power and Vision!

Rittal – The System.

Faster – better – worldwide.

**IT infrastructure
from smallest to largest.**



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL



the server chassis, running independently of the server's main CPU (or CPUs). With direct access to the video and IO via the system bus, they enable KVM without the mouse sync and video quality issues that plagued external KVM over IP switches – IP connectivity is via a secondary or sideband network port, available regardless of OS or primary network state.

Unlike external KVM over IP, integrated lights-out offers IPMI power control for remote server power cycling, and hardware health monitoring – arguably the true killer features. This allows IPMI-enabled infrastructure management appliances to alert operators when monitored health metrics hit warning and critical levels, and provide a unified interface for remote power control in environments that mix different makes, models and versions of lights-out interfaces.

With the growing adoption of ISO 27001 for Information Security, infrastructure

management appliances are proving invaluable as a means to isolate and secure management traffic to interfaces such as lights-out management controllers. Encrypted remote access and integration with data centre authentication systems addresses the vulnerability of leaving a management back door ajar.

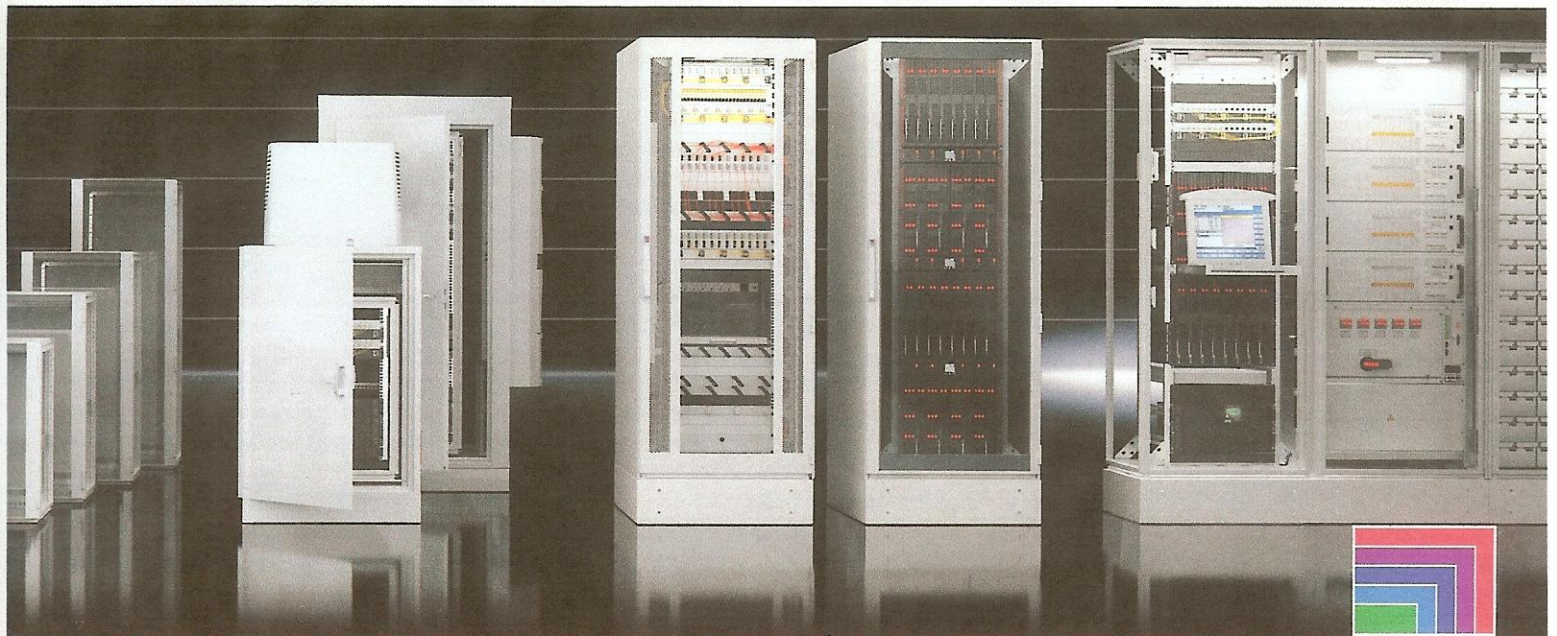
The second technology that has displaced traditional KVM over IP is virtualisation. Guest virtual machines lack physical hardware ports, so KVM connectivity to each guest is purely virtual, served via the VM management software. This trend also speaks of the strengthening delineation between systems management and infrastructure management. Operating environment and systems management has been pushed up the stack, with OS deployment, policy and patch management taken care of using specialised tools such as Dell KACE and Microsoft SCCM.

Today's data centres have become a complex and diverse ecosystem of interdependent infrastructure. Maximising MTBF and reducing MTTR requires remote management of a multitude of systems, including networking infrastructure, back up power and power distribution equipment, and environmental sensors.

This leaves the infrastructure management appliances to focus on the bare metal server itself. The hypervisor, whether it be XenServer, Linux Kernel-based Virtual Machine or VMware ESX, offers BIOS-redirection and low level CLI out-of-band control via an RS232 serial console. The serial console connection is network connected via the infrastructure management appliance's console server, using standard secure protocols such as SSH and HTTPS.

Among the advantages of CLI console management, is remote access becomes orthogonal across disparate infrastructure, such as servers, routers, switches and SAN devices, and like KVM over IP, managed infrastructure remains accessible during primary network outage. All management traffic can be logged in plaintext, providing an audit trail and notification when malicious or anomalous patterns are detected. It also facilitates the development of scripts to automate common configuration and troubleshooting tasks.

The combination of real-time monitoring with management control of a wide range of infrastructure, enables scriptable actions to be triggered in response pre-defined environmental, time, or service availability conditions. This has given rise to a further shift away from the traditional scenario where electromechanical systems notify, and human operators manually remediate via an out-of-band management channel such as crash cart or KVM over IP. The next generation of smart infrastructure management appliances now provide a platform to develop sophisticated self-healing solutions that automatically remediate blocking outages.



IT INFRASTRUCTURE

SOFTWARE & SERVICES



www.rittal.co.uk