Data Center Infrastructure Management for System Administrators

The role of Access and Control in DCIM
Table of Contents

1. Executive Summary ........................................................................................................... 3
2. Server Access & Control .................................................................................................. 4
   2.1 Remote Access Tools and Out-of-Band Management .................................................. 4
   2.2 IPMI and Baseboard Management Controllers (BMC) ............................................. 4
   2.3 Remote Light-Out Management Tools ......................................................................... 4
3. Data Center Infrastructure Management (DCIM) .............................................................. 5
   3.1 What is DCIM? .............................................................................................................. 5
   3.2 DCIM Evolution ........................................................................................................... 5
   3.3 The role of Access & Control technology in DCIM ..................................................... 5
4. Your DCIM and Command & Control Action List ............................................................... 6
   4.1 Eliminate Out-of-Band Hardware redundancy ............................................................... 6
   4.2 Start on the road of DCIM ........................................................................................... 6
   4.3 Process Automation ...................................................................................................... 6
5. Ten Reasons to Consider Tenduit RIMCenter ................................................................... 7
1. Executive Summary
This document brings Intelligent Platform Management Interface (IPMI) and Data Center Infrastructure Management (DCIM) in context so that IT Managers and System Administrators understand how traditional Access & Control tools will evolve with emerging technology and market trends to Close the Loop in Infrastructure Management.

The Business Issue
Until recently, IT was focused on the goal of providing reliable levels of service to support business functions. To a large degree, that is mission accomplished, now. Besides improvements across all data center technologies, virtualization and cloud computing enables us to build scalable infrastructures with high level of resilience and availability. Business is now demanding higher levels of accountability, agility, and efficiency from the data center. Servers running at 15% utilization, inability to identify the business service supported by a given element in the IT infrastructure, power consumption that far exceeds the active IT load, are all part of a “availability at any cost” scenario that is still a commonplace, but is no longer acceptable.

The Solution and Benefits
The solution requires changes, in both the IT organization and in the leveraging of tools and technology. DCIM (Data Center Infrastructure Management) consists of a set of tools, methodologies and organizational changes to manage data center elements as a shared infrastructure to support business functions. IPMI (Intelligent Platform Management Interface) is a technology embedded in the servers you buy today, it enables DCIM, allows us to eliminate clutter in the datacenter rack, and facilitates the reduction of manual intervention and automation of IT operations. The benefits are reduced costs (in labor, power, equipment), improved efficiency (through polling of resources, optimization, elimination of waste) and increased service levels (reduction of errors caused by manual intervention).
# Server Access & Control

## 2.1 Remote Access Tools and Out-of-Band Management

In order to manage the server infrastructure, System Administrators need to be able to access the infrastructure “as if they were there” next to the rack in the data center. One could think that, since all servers are network-connected, they could just connect over the production network and access servers for management.

But remote access is also and specially important when there is a service disruption. If the network is down or if the server Operating System is down, connectivity using the data network (“in-band”) are not available. So, System Administrators have traditionally relied on Access & Control (also called “Out-of-Band”) technologies that provide connectivity through alternative channels that don’t rely on the server Operating System or the data network connections. Those tools allow access to the operating system console and often include the ability to access the pre-OS console (to set BIOS parameters, change boot options, reconfigure hardware, etc.) and reset and power control the equipment. The out-of-band network is often also used to monitor and collect operational and environmental data that is useful for infrastructure management.

In order to support those out-of-band channels, data centers today use an array of equipment that is installed in every rack: KVM Switches, Serial Console Servers, Intelligent Power Distribution Units, Management Gateways, Data Collection Appliances, etc. This equipment is usually considered part of the active IT infrastructure, but they don’t directly support business workloads and consume a considerable portion of the cost, power, space budgets.

## 2.2 IPMI and Baseboard Management Controllers (BMC)

During the early 2000’s, under pressure of some of the large financial companies (the most advanced users of IT), several of the IT vendors (including major server OEM, led by Intel) developed the standards for a technology that would take the functionality of the out-of-band infrastructure and embed it into every server, eliminating the need for redundant external hardware. That technology, Intelligent Platform Management Interface (IPMI), is now a standard on virtually all datacenter servers.

Think of slicing all the external support equipment (KVM, Serial, Power, Sensors, etc) and pushing them inside the servers. The Baseboard Management Controller (BMC) is a microcontroller embedded in virtually all servers you buy today. They all follow the IPMI standard, but vendors market them as “features” under names like HP iLO, Dell iDRAC, IBM IMM, Sun ALOM.

The BMC sole function is to collect platform level sensor information, monitor the operation of the main CPUs, and provide external connectivity for management functions using standard IPMI protocol. As long as the server is connected to power, the BMC is active, even when the main processor is not running, is powered down, and when the OS is not functioning.

IPMI adoption was spotty for a long time, but more than 10 years and at least 3 data center refresh cycles later, IPMI 2.0 is in virtually every server in a modern data center.

## 2.3 Remote Light-Out Management Tools

Customers have already paid for the BMC inside servers and it is there sitting on the motherboard collecting data and waiting to be used. Why do people continue to buy external equipment, deal with cabling, external temperature and air flow sensors, extra money, power, network capacity, and rack space requirements?

In part it is because ubiquity of IPMI is a relatively recent reality. System Administrators want to use the same tool to do the same task independent of the age or manufacturer of the server and the minimum common denominator was external appliances. The second reason is that all Lights-Out Management Tools were provided by either the server OEM or a vendor of Out-of-Band Management equipment (those vendors have a vested interest in keep selling you the extra hardware).

While many of the DCIM solutions are still being provided by the same hardware vendors, the DCIM proposition requires hardware-agnostic tools and the market is evolving towards software-based solutions that work with any server vendor and does not require additional redundant hardware because they fully utilize the capabilities of the embedded BMC.
3. Data Center Infrastructure Management (DCIM)

3.1 What is DCIM?
Until recently, IT infrastructure was organized in vertically integrated silos. A business demand triggered the need for an IT workload. An application was selected and then the resource stack all the way down to the physical computing infrastructure was allocated. Servers in the data center had a business owner, IT was responsible for keeping it running, and nobody else could touch it. As the business evolved, the IT workload becomes obsolete. Lack of communication and accountability perpetuated the maintenance of the IT resource stack in the data center.

That resulted in a data center were it is common to find large sections of infrastructure that are consuming power, space and other resources, but nobody knows what is running on it. Even in well managed data centers, server utilization levels are typically under 20%.
Virtualization technology allowed the decoupling of applications and operating systems from the underlying data center infrastructure. Business owners care about IT services and there is no static relationship between those services and the underlying infrastructure.
It is now possible to manage the datacenter as a shared resource pool managed as a true infrastructure. DCIM is the set of methodologies, organization, tools and technologies that enable that holistic view of the Data Center Infrastructure and enable the automation and optimization of its management.

3.2 DCIM Evolution
DCIM is a holistic and systemic view of the infrastructure and ultimately aims to manage an automated infrastructure capable of responding and adapting to variation of input conditions and output demands in real-time.

Because the first step in managing an infrastructure is taking control of its elements, most DCIM implementations start with Discovery, Asset Management and building a comprehensive physical model of the infrastructure.

Most datacenters have also started to deploy sensors (temperature, humidity, air flow, movement, etc) so that they can monitor some of the most critical infrastructure parameters.
By comparing the design models with the measured reality, DCIM tools can “close the loop” and deliver predictive models and a truly autonomic system that is optimized for efficiency.

3.3 The role of Access & Control technology in DCIM
While the goal of DCIM is an autonomic system, the current design models are static and reactive. Most data centers (including the best managed ones) still deploy equipment first, then document where the equipment is and try to keep track of it using manual audits and spreadsheets or modeling tools.
Data Collection and monitoring is not integrated to a predictive model. In almost all cases, sensors deployed in the data center are there to trigger events and alarms when parameters deviate from the design parameters and call for human intervention to avoid catastrophic failure.
Human intervention invariably occurs through Command & Control tools. That is how the management loop gets closed today. That is why, to deliver on its value proposition, DCIM has first to integrate with Command & Control technologies and let human operators act within the context of infrastructure management. Then we need to gradually integrate the monitoring elements, implement predictive analysis, and reduce the need for human intervention.

4. **Your DCIM and Command & Control Action List**

Now that we looked at how DCIM and Command & Control fit together, we can list a series of actions in execution order to “close the management loop” in DCIM:

4.1 **Eliminate Out-of-Band Hardware redundancy**
A BMC is embedded in every server for the purpose of collecting environmental and operational data and providing management connectivity to enable remote operation. Using external KVM switches, Serial Switches, IPDUs, Sensors, Gateways, Appliances is a waste of power, space, money and resources. Adopting Software-based Lights-Out Management not only eliminates that waste, but also prepares you for the evolution in the years ahead, when we will able to close the management loop in DCIM leveraging both the Command & Control and Monitoring capabilities of BMCs.

4.2 **Start on the road of DCIM**
There are several emerging DCIM frameworks from multiple vendors. It is beyond the scope of this paper to help you select the right solution. But if you are using spreadsheets and the only way to find something in your datacenter is a manual audit on the data center floor, it is time to start in the road of DCIM. The first steps are to take inventory and modeling your current infrastructure and implement a Change Control system that helps you keep track of its dynamic evolution.

4.3 **Process Automation**
Automating the wrong process only make things worse. Before you automate, implement processes in infrastructure management (your DCIM tools should help you on that). Make sure IT managers and System Administrators have the Access & Control tools that provide a holistic view of all equipment, independent of geographical location and vendor. Once you have real-time models and monitoring in place, consider automating the process. You are on the path to close the loop in infrastructure management.
10 Reasons to consider Tenduit for Your Remote / Out-Of-Band Management

1. It Works!
Let’s be honest. When it comes to IT systems management tools, most are as painful to use as the problems they are meant to solve. You need something that makes your job easier. Our customers love Tenduit because... it just works.

2. Complete Remote Access & Control
A complete server remote access and power control tool for enterprise and mid-enterprise data centers. Install Tenduit without long deployment cycles, project teams, or expensive professional services. Software installs in minutes and can be deployed to hundreds of servers in a single day.

3. Power Management
An idle server wastes 40%-70% of its peak power usage. How many of your servers can be switched off over night or over the weekend because they are not mission critical or not in use? Make use of RIMCenters ‘power-scheduling features’. Switch off and on servers at pre-defined times and save thousands in energy costs.

4. Enterprise Ready
Integrates with Active Directory for user / server authentication for ease of setup. Providing 256-bit AES encryption for ultimate security. It’s also easy to add servers that are not within the Active Directory structure.

5. Affordable
Save 50% or more compared to alternative remote access solutions such as iLO (HP), iDRAC (Dell) or iMM (IBM) and appliance based legacy KVM and PDUs.

6. Scalable
Whether you have 5 servers or 5,000 servers, Tenduit scales with you. Simply add managed node licenses as your site grows.

7. Easy to use
No lengthy training or professional services required for deployment or maintenance. No baby-sitting or time-consuming administration needed.

8. Who is Tenduit?
Tenduit Software is the creator of RIMCenter, a complete remote console (BIOS and Operating System) and power control solution that is entirely software-based. It leverages the embedded Baseboard Management Controller (BMC), which virtually every modern server contains. It works by using the IPMI 2.0 standard and works and is a powerful, affordable and easy-to-use system for remote access and control of your servers – enabling efficient lights-out management - without the cost, hassle, and limitations of hardware-based products.

9. Proven team
Tenduit’s leadership has extensive backgrounds in remote systems and out-of-band management. Their prior company was the leader in the KVM/IP and embedded management space.

10. True “All-in-one” Server Access & Control
A single software tool, that easily scales, to manage and control all of your servers across all vendors and platforms. Get secure and immediate access to your critical resources for system recovery and service restoration. Manage your energy and cooling costs by turning off unused resources and restoring them when needed.

Contact us to arrange a free, no obligation trial
www.tenduit.com