Break Vendor Lock-in Using White Box Management
Dispelling the Management Myth

Today, many organizations have grown accustomed to the hardware layer management interface sold by traditional brand-name legacy server manufacturers which in turn have provided vendor lock-in mechanisms to keep customers hooked. Hardware layer management is a key tool for system administrators that has traditionally come as costly additional hardware and software licenses. When businesses consider moving to white box servers, there is a misconception that the same tools are not available, or the same quality, as what they have in their current systems. White box server manufacturers are now able to offer the same remote hardware management features. This paper focuses on dispelling the myth that the current generation of white box servers do not offer the same manageability as traditional brand-name legacy server manufacturers.

History

With new technologies like real time analytics, big data, and content delivery there has been an explosion in compute needs. The massive growth in compute means customers are deploying more servers than ever. It is common for medium to large businesses to have a thousand servers or more while the largest enterprises easily top 10,000 servers. Operating with that many servers creates challenges around managing, monitoring, and alerting over the entire infrastructure. In the past, customers would walk down to the data center and plug in a monitor, keyboard, and mouse to work on a server. Today, enterprise and large users often have multiple lights-out datacenters with administrators who could be thousands of miles away.

Legacy hardware manufacturers have traditionally provided remote management solutions, for a significant fee, to support growing customers through mostly proprietary interfaces. These remote management interfaces typically offered a GUI that allowed admins to see the server status and gather basic details including BIOS, firmware, sensor status, and other hardware related metrics. In addition, remote management interfaces included common communication protocols like serial over LAN, SSH, and APIs providing administrators better scripted access for larger server inventories. A major addition to remote management came with the remote Keyboard, Video, and Mouse (KVM) capability providing remote screen access without needing to be physically in front of the server.

Initially, white box manufacturers avoided the expensive proprietary remote management interface to keep end-customer system costs low and used alternative methodologies including hardware appliance based KVMs. Appliance-based KVM worked well when server counts were relatively small. With the boom of the Internet and massive server growth, white box manufacturers shifted strategy to include more standardized remote management features in the server. Unfortunately, the shift was not quick enough and white box servers became synonymous with “difficult to manage”. But this has changed!
Management Software Today

In general, all of the components in a server are commodity parts. Processors, memory, hard drives, fans, power supplies, network cards, etc. are all standard design and made by companies other than the traditional legacy or white box server vendor. In the same sense, the server management interface has become a commodity item that all server vendors can now offer. The server management interface contains two key pieces, on-board hardware management devices and the software that provides the interface.

The Baseboard Management Chipset (BMC), which is the hardware portion of the management interface, is a standardized design manufactured by a few companies. Motherboard manufacturers purchase the chipset from one of the BMC manufacturers and integrates it into their motherboard design. All BMC chipsets follow a standards-based design and are either included in the motherboard or developed as a removable module that may cost extra. In general, all BMCs can perform the same tasks from a hardware standpoint.

Historically, the software that runs on the BMC is where traditional legacy server manufacturers have created a difference through features that entice companies to use their equipment. The different feature sets have also helped traditional legacy server manufacturers create vendor lock-in through the creation of proprietary features and command sets. To provide a complete solution and compete in the larger server sales market, white box manufacturers and their partner motherboard manufacturers have worked to develop similar remote management software to run on the BMC. The gap in “value-add” features provided by traditional legacy server vendors is continually shrinking when compared to what white box server manufacturers now offer, making it more difficult for traditional legacy server vendors to charge a premium for what are now considered standard features.
Standard Features

There are three standard feature sets that all remote management interfaces support to provide access to the BMC: 1 - a GUI interface, 2 - Remote KVM access, and 3 - multiple CLI and API connection methods. Combined, these three feature sets offer the ability manage, monitor, alert, and report on all aspects of the server hardware. In addition, some traditional legacy and white box server vendors have developed external software that goes beyond reporting on the individual servers. The additional software includes roll-up management software as a data gathering point for multiple servers and host agents that collect information available from the OS and applications running on the server. When combined, the additional software can help construct a more complete picture of the server health beyond just the hardware layer.

GUI

The GUI interface to the BMC offers many monitoring and configuration features to help server administrator's setup and manage their servers. The GUI interface can be broken into three distinct feature sets; configuration, reporting, and management. The configuration feature includes both configuration of the BMC software as well as configuration of the server itself. The BMC software typically includes key features such as SMTP and SNMP alerting based on thresholds, integration into Active Directory or LDAP for security purposes, and secure connections like SSL. The BMC also enables server configuration features including setting fan speeds and sensor thresholds.

Reporting through the BMC focuses on the server hardware information and metrics. Information on the components installed in the server like motherboard, memory, and processor are quickly accessible through the GUI. Metrics collected through the BMC include system health attributes like power consumption, fan speeds, temperature readings, and include access to key hardware logs that record power activities, physical intrusions, and component failures.

The management tools in the BMC wrap up the three interfaces in the GUI feature set. The management tools allow administrators to take actions based on server needs. The BMC provides access to power management including resetting and turning off/on the power to the server. In addition, access to features like updating firmware or BIOS without downtime enable administrators to ensure their servers are always running the latest code in a 7/24/365 environment.

KVM

Remote access to the keyboard, video, and mouse is arguably the feature that took remote management from a valuable feature to a must-have capability for every server. Remote KVM works by redirecting the keyboard, video, and mouse to the administrators local PC allowing the administrator the same access to the server as if they were sitting in front of the box. Unlike remote desktop sessions, that use individual sessions for each user, remote KVM displays the main server video output exactly as if the administrator connected physically to the server. The administrator can monitor boot screens to see errors and gain access to the video output, even if the OS has locked up and is not operating properly. With additional features of KVM, like remote media, an administrator can load and configure the OS and applications without ever being in front of the server. In fact, administrators are rarely in the same room as the hardware and quite often not even in the same city.
The API or CLI connections available in the BMC enable remote access to the server without the use of a GUI enabling scripted or programmatic control. Both traditional legacy and white box server vendors support the same standard CLI and API communication protocols including Serial over LAN, SSH, and the Intelligent Platform Management Interface (IPMI) API. The communication protocols, command set, and responses are relatively similar between all server vendors allowing scripting and command line communications to remain largely similar no matter what server brand the administrator has accessed. One exception to this standardization is that most traditional legacy server vendors have modified the IPMI API in a proprietary fashion so scripts that work with one vendor may not work with another. The modifications to IPMI means administrators of traditional legacy servers have to use additional proprietary intermediary tools to translate commands to and from IPMI, locking companies into a single vendor for simplicity. White box server manufacturers have left IPMI in the standardized state allowing direct access to the API without additional translator software.

One area where traditional legacy server manufacturers have continued to invest to create value-add over white box is in the server management roll-up tools. These tools allow administrators to visualize, monitor, and manage large amounts of servers through a single GUI or CLI. Until the boom of cloud computing and the Internet of Things, developing customized software to report on servers was a time consuming and costly effort which was reflected in the oversized fees traditional legacy server manufacturers charged for their management interface and tools. In addition, the server management tools facilitated vendor lock-in, as they were proprietary and used proprietary APIs that would not work with other third party tools.

Today, lightweight remote monitoring and management applications that run in the cloud or on premises are readily available and take advantage of standards based communication CLI's and API's including SSH, IPMI, and REST APIs. Beyond third party monitoring tools, the Open Source movement has produced several free or very low cost management tools that offer many of the same features as the traditional legacy manufacturer tools. The third party tools can be more flexible than those of traditional legacy server vendors and enable similar functionality no matter what server is being managed. The tools also help reduce vendor lock-in at the hardware level by removing any proprietary functionality or features at the software layer.

Another area where traditional legacy server manufacturers have developed features that create vendor lock-in through proprietary features is the use of host agents. Most OS and application vendors did not develop standard API's in their products. Host agents worked around these limitations by creating executables that ran on the server and polled the OS or application sending back the collected data to the management software.

Host agents were unavoidable in the past, but they had many challenges including causing the very OS or application they were monitoring to crash or perform poorly. In addition, they mimicked the actions of hackers and Trojan horses by collecting key data and transmitting it back to a central location setting off many security and virus monitors. Finally, host agents were challenging to manage, especially in large environments where it could take months to test and roll-out a single version update to the entire server infrastructure only to start the process again immediately due to a new agent release.
Today host agents are outdated technology, which challenges traditional legacy server manufacturers to justify their high priced management interface. Many operating systems and applications now include external open APIs that provide the same level of data that host agents once gathered. In addition, the open source movement has created standards based data collectors for many parts of the datacenter including the server that are more friendly to use and manage than the traditional proprietary host agent.

The New Reality

For many years, white box server manufacturers have talked about the future of management that will put their tools on par with traditional legacy server vendors. Today, that future is a reality with the relatively recent release and adoption of two key standards in the server management layer: Redfish and OpenBMC. These two open standards have helped commoditize some of the last proprietary features in the BMC software. With the availability of standard management solutions, companies must ask their legacy vendors why they are paying for expensive features that are now typically included in low-price white box servers.

Redfish

Redfish, and its closely related storage version Swordfish, is an open standard based REST API protocol to facilitate communication, monitoring, alerting, and reporting on the BMC. DMTF - the standards organization that brought other popular standards to the industry including the Common Information Model (CIM), Systems Management Architecture for Server Hardware (SMASH), and Web-Based Enterprise Management (WBEM) - has developed Redfish as a new standard REST API protocol for server management. Redfish will replace the outdated IPMI API allowing any third party to connect to any server management port to provide true unencumbered management in a multi-vendor environment. All traditional legacy server manufacturers and many white box companies support Redfish helping the standard come to the market quickly across all server platforms. More information on Redfish can be found at http://www.dmtf.org/standards/redfish.

OpenBMC

OpenBMC is a standards-based open source software that runs on the BMC. OpenBMC replaces the proprietary BMC firmware that has allowed traditional legacy server manufacturers' limit management of servers to their and their partner's software only. OpenBMC originally developed by Facebook and supported by many companies including Google, IBM, and Apple, helps companies break away from vendor lock-in tools and expensive management software. Currently, most traditional legacy server manufacturers do not support OpenBMC as it affects their ability to charge for their proprietary software and hardware. However, white box manufacturers and their partner motherboard manufacturers currently support OpenBMC on most solutions. More information on OpenBMC can be found in this informative post: https://code.facebook.com/posts/1601610310055392/introducing-openbmc-an-open-software-framework-for-next-generation-system-management/.
Breaking your Vendor Lock-in and Moving to White Box Servers

This whitepaper provided important information to those who are concerned about the ability to manage white box servers when moving from traditional legacy servers. Although traditional legacy server manufacturers initially paved the way for server management through the BMC and associated software, the fees for these features in current servers are continuing to increase, while white box manufacturers are offering the same features at no additional charge.

In addition, the lock-in effect of traditional server manufacturers makes it difficult for companies to purchase lower priced white box servers from multiple vendors. Companies must use multi-vendor white box server flexibility to cost-effectively grow their infrastructure.

The key take-away: White box server manufacturers now offer the same management features and functionality as traditional legacy server manufacturers at a much lower price with no vendor lock-in.

You owe it to your organization to explore these new white box management solutions.