HYPER-V VIRTUALIZATION AT ALS HIGH LEVEL ACCELERATOR CONTROL*

C. Ikami, T. Kellogg, C. Lam, G. J. Portmann, H.Nishimura
Lawrence Berkeley National Laboratory, Berkeley, CA 94720, U.S.A.

Abstract

In an effort to more efficiently support the High-Level Controls System (HLC) at the Advanced Light Source (ALS), a virtualized computer infrastructure has been implemented. The functionality of this infrastructure was selected to address the operational issues that most impacted the support of previous ALS control system consoles. In order to reduce the burden of physical machines the majority of these support servers, consoles and context stations have been virtualized. The issue of high availability to these services, the servers, consoles, developer stations, context stations, has been addressed by placement into a failover cluster configuration. The current work will discuss the methods and findings from this study.

GOAL

The ALS Control System upgrade has been completed at the application software domain in HLC [1], the focus has been in the HLC computer infrastructure. The priorities that were set for the improvement of the associated support infrastructure are listed below.

- **Console Consistency.** In order to build each individual console, several steps were required for the installation of HLC applications, libraries and system environment configurations. This led to variations from station to station due to version control issues.
- **Recoverability**. Due to the time required for a build a single console, the replacement for a down system could take days.
- **Development Machines**. The Control System Developers require several test consoles, servers and workstations. The time required to specify, order, install operating system and control system software on physical machines required many hours of support staff time.
- **Context Machines**. Single purpose machines, (e.g. monitoring systems) were usually placed on older machines that had both software and hardware maintenance issues associated with out-dated technologies.
- **Remote Access.** The need for Control System Consoles to access outside services or for users outside the filtered router to access resources within the Control System was awkward, slow, posed security risks and was platform limited.
- **Security**. In addition to the conventional issues of security that would be addressed by the privileges and permissions of the Active Directory (AD) [2] domain controllers, the control system subnets are located behind a filtered router. Access to and from the HLC system through the router was limited, difficult and posed security risks. Machines inside the filtered router environment were blocked from accessing the Microsoft update servers.
- **High Availability**. Servers, Consoles, Development Stations, Context machines, Server roles and features that were consolidated on a single machine or in a single server room were subject to service interruption by system upgrades, power outages or hardware failure.
- **Cross Platform.** Virtualization should support both Windows and major Linux releases.

STATUS

We have adopted the Windows 2008 Server R2 [3] to use the following roles and features to resolve the issues mentioned above.

Windows Deployment Services

- **Console Consistency**. The primary physical consoles are not virtualized but cloned from a single master image by using the Windows Deployment Service (WDS) [4]. This methodology establishes absolute assurance of identical software capabilities to each WDS HLC control room console at the time of deployment.
- **Recoverability**. Due to the rapid deployment feature of WDS, the creation of a new or replacement control room console is reduced from days to less than one hour, requiring no detailed knowledge of console creation. Rapid deployment not only addresses routine system replacements but also has security implications for situations such as console contamination by virus outbreak.

Hyper-V

Hyper-V[5] is a hypervisor that manages virtual clients.

- **Development Machines**. There are several types of development machines; server-side development for infrastructures including web, EPICS [6], and database services. On the client side; they are for EPICS client software development, instrumentation, and database clients. For the most part, these systems have been virtualized. Each system has been created to be as singularly purposed as possible. In the case of the client software development, we have only one

*Work supported by the U.S. Department of Energy under Contract No. DE -AC02-05CH11231

ISBN 978-3-95450-115-1

on-premise physical PC. Most of these virtual machines have read-only access to the control system via the EPICS Gateway, therefore making them an ideal location to develop controls software during normal accelerator operation avoiding the risk of interference. Development machines, including workstations, servers and consoles, can now be on a stable and consistent hardware platform that greatly reduces maintenance in terms of operating system support (drivers, BIOS updates, system patches, application deployment). These platforms occasionally require changes in their hardware configurations. Changes to the amount of memory, size of the disk drive, and/or the number of CPUs/cores can now be done in the time it takes to edit the Hyper-V settings and reboot.

- **Context machines**. These single purpose machines were normally relegated to placement on older machines. By using virtual machines they can be properly maintained in terms of up to date operating systems with High Availability.
- **Cross Platform.** Hyper-V also supports several Linux systems and we have installed CentOS, Ubuntu and SUSE version on Hyper-V clients without any major problems.

Remote Desktop

- **Remote Access.** Remote Desktop (RDP) [7] using Network Level Authentication (NLA) [8] can provide secure access to both the physical and virtual machines through the filtered router. RDP clients are available on all Windows Operating systems since XP and in the Apple Macintosh environment. Windows 7 also supports Xmanager [9] to connect to Linux applications.

Inside / Outside (secured server pairs)

- **Security.** The ALS domain AD privileges works with file and group permissions as well as in conjunction with other system services such as operating system firewalls. Using these security measures, a server on an open subnet can have trusted access to another server placed inside the filtered router environment. Using this method of secured paring, a control room console can enable a remote desktop session that can access the full resources of the entire Internet (e.g. email, updates, procedures, documents, websites etc.). Since none of the protected virtual machines are exposed to the open Internet to get these services, these control room console machines have a greatly reduced risk of compromise. Another example would be the shadowing of the Windows Server Update Services (WSUS) [10]. This paired service allows machines, virtual and physical, within the secured control system environment to receive the latest patches for the operating system, layered products and anti-virus software without the risks posed by a direct connection to the outside Internet. Still another example would be using a gateway virtual machine with NLA RDP on the outside server to provide secure access from outside networks.

Failover Clusters

- **High Availability.** When demand for and reliance upon the virtual machines and virtual services increased, an expansion into a clustered environment was implemented. Existing Hyper-V farms and newly acquired servers became joined nodes in a cluster type known as “Failover” [11]. The Failover cluster allows for Hyper-V machines to migrate from one physical platform to another. A single VM can be moved to another node to better utilize resources such as memory or CPU. An entire node can be cleared to allow for maintenance of that physical platform (system or hardware upgrades). Migrations can be performed on actively running machines without loss of data. This feature is called “Live Migration”[12]. Live Migration can be done manually or automated to occur during an unexpected outage of a node, thereby providing nearly continual availability of services, such as EPICS, which are critical to the operation of the ALS Virtualized control room consoles have been tested in a failover cluster. The control system consoles, which contain the EPICS clients, were able to perform live migration without problem.

REMAINING WORK

We are continuing the migration of existing web and database servers, as well as existing Hyper-V developer workstations to the Data Center Failover cluster. We are in process of creating an Enterprise failover cluster for service within the control system filtered router environment. A second storage server has been acquired for backup. We are evaluating software options for the conversion of the backup storage server into a failover storage server.

CONCLUSION

By following industry standards for the enterprise, we were able to apply these Windows 2008 R2 Server roles and features for the HLC effort, accommodating the project need for a virtualized computer infrastructure placed within the operating restrictions of our secured networks. Of the five roles we have implemented, Active Directory, Windows Deployment Services, Windows System Update Service, Hyper-V and Failover Cluster, each has been shown to be a practical and stable tool to provide a wide range of services to the control room consoles and system developers. Each server role and feature mentioned here is included in the license for Windows 2008 R2 Server (Data Center or Enterprise). Using our existing ALS Computer Support Group staff, we were able to implement a virtualized computer infrastructure support facility consisting of two failover clusters, each with two nodes, for an infrastructure-wide capacity of 256 virtual servers and workstations.

AKNOWLEDGEMENTS

We thank to the ALS managers, D. Robin, A. Biocca, and J. Kekos, for their support. The collaboration with the machine operations group was also crucial, especially with W.Byrne, M. Beaudrow, S. Stricklin and P. Bloemhard.

REFERENCES

[1] G. Portmann et al, "High-Level Controls Upgrade at the ALS", Proceedings of PAC09, p.4805-4807, Vancouver, BC, Canada, 2009.
H. Nishimura et al, "ALS Control System Upgrade in C#", Proceedings of PAC09, p.4803-4804, Vancouver, BC, Canada, 2009.
[2] http://www.microsoft.com/en-us/server-cloud/windows-server/active-directory.aspx
[3] http://www.microsoft.com/en-us/server-cloud/windows-server/default.aspx
[4] http://technet.microsoft.com/en-us/library/cc731439%28v=WS.10%29.aspx
[5] http://technet.microsoft.com/en-us/library/cc753637(v=WS.10).aspx
[6] L.R. Dalesio, et al., ICALEPCS '93, Berlin, Germany, 1993.
[7] http://www.microsoft.com/en-us/server-cloud/windows-server/remote-desktop-services-overview.aspx
[8] http://technet.microsoft.com/en-us/library/cc732713.aspx
[9] http://www.netsarang.com/
[10] http://technet.microsoft.com/en-us/windowsserver/bb332157
[11] http://technet.microsoft.com/en-us/library/cc732181(v=WS.10).aspx
[12] http://technet.microsoft.com/en-us/library/dd446679(v=ws.10)
[13] http://www.microsoft.com/en-us/server-cloud/system-center/default.aspx

ISBN 978-3-95450-115-1