ABSTRACT

The system administration lab at the University of Cincinnati consists of 24 high-end desktop PCs, each loaded with client virtualization software. The lab is limited to 24 students per class and does not offer remote access to the virtual machines. The students must either wait for open lab hours or purchase their own high-end systems to work on their schoolwork. To expand the number of classes taught and enable remote access to the lab, the authors created a Microsoft-based private cloud accessible from any computer on the university’s network. VPN entry to the network allows students to login to the system using a web browser to access their VM’s from anywhere in the world.

Categories and Subject Descriptors
D.3.2 [Computers in Education]: Computer and Information Science Education.

General Terms
Management, Performance, Design, Reliability, Experimentation.

Keywords
System Administration, Networking, Virtualization, Capacity Planning, Cloud Computing.

1. INTRODUCTION

The current lab stores template VM’s locally on each lab system. Students make copies of these templates then load them on client virtualization software, such as VMware Workstation. Past publications describe this setup [6]. Currently, when a student needs to work on their lab outside of the scheduled class time he/she needs to copy the needed VM’s to a portable storage device to use on their own computer system. This requires the student to have a virtualization capable system.

The use of a private cloud makes the manual process of copying VM’s unnecessary while also granting remote access to the lab. Additionally, systems administration and networking classes would be able to be scheduled in other computer labs in addition to or in lieu of the expensive systems administration lab. Ideas and implementations of cloud-based solutions for such a lab environment are not new [1, 5, 7].

This paper, however, outlines the creation of a private cloud using Microsoft software, for which many academic institutions have site licenses available. Microsoft provides some documentation to assist in setting up such an environment [2, 3, 4].

2. METHODS

The project’s goal was to move the current networking/system administration computer lab to a remote solution that could be accessed from anywhere. The current lab has 24 client computers and a handful of servers for management purposes. The lab contains a domain controller to provide authentication and local profile support for each of the client computers. The student must sit at the same computer each time to continue working on their assigned lab work since storage of the large virtual machines is all local to each system.

The internal lab network is isolated from the university’s network with a firewall. The firewall prevents any unwanted network services implemented in the IT classes from disrupting the university network. Figure 1 shows the current infrastructure of the lab.

Figure 1. Current Lab Infrastructure

The private cloud must provide all of the existing functionality of the systems administration lab and allow for remote access to the lab resources. The authors determined that the system should be able to handle 100 concurrent users (3 classes of 24 students and approximately 30 students working remotely). The authors chose
to use all Microsoft software due to the university’s Enterprise License Agreement with Microsoft. Specifically Microsoft’s Hyper-V and System Center Virtual Machine Manager 2008 R2 (SCVMM) were used to achieve the remote access and virtual machine creation abilities required by students and professors.

The proof of concept consisted of 10 servers (4 Hyper-V hosts and 6 support/management servers). Each of the Hyper-V hosts contains a quad-core Intel processor and 8-16 GB or RAM. One of the servers was used to host System Center Operations Manager (SCOM) to allow prediction analytics. The limited number of viable Hyper-V hosts makes the installation of SCOM necessary to determine the required hardware to scale the environment to a production level.

2.1 Hyper-V

Hyper-V is Microsoft’s hypervisor solution that allows the guest operating system to share hardware resources with multiple VM’s. Hyper-V is available on any server running Microsoft Windows Server 2008 R2 that contains a virtualization capable processor. Hyper-V is installed using the Role Management Console within the Server OS.

In the proof of concept, Microsoft Windows Server Core 2008 R2 with Hyper-V enabled was used to minimize the resources used by the host OS and maximize the resources available to the private cloud.

2.2 System Center Virtual Machine Manager

System Center Virtual Machine Manager (SCVMM) is a centralized management console that provides fine-grained access control and functionality for the Hyper-V hosts. SCVMM manages all aspects of the private cloud including all Hyper-V hosts and virtual machines.

SCVMM has several components that can be installed on a number of various servers in the environment. The authors installed the Administration components, database, and Self Service web portal on different servers to prevent overloading a single server. Once the SCVMM Administration console has been installed and setup, Hyper-V hosts can be added. SCVMM will automatically deploy and install the administration client on all managed hosts. As part of this deployment Hyper-V will be enabled on the host if it is not already. Hosts should then be added to different Host groups with SCVMM to provide organization and permission control to individual hosts.

Microsoft packages a self-service web portal with SCVMM. This Self Service portal allows users to interact with the cloud environment from a web browser. The portal sits on a web server running IIS and uses web form authentication against the domain controller. Within SCVMM the administrator must create Self-Service User groups and members must be members of one of those groups to login to the Self Service portal. Each of the Self-Service User groups is completely independent of each other making it ideal for the systems administration lab replacement. Each class is setup as an individual User group and the templates required for each class are assigned to the group. When the students log into the portal, he/she can view their VM’s and create new VM’s based on the templates available to the User group. From the Self-Service Portal the student has complete control over the VM’s and can connect to the console of the VM.

2.3 Forefront Threat Management Gateway

To isolate the private cloud from the university’s network, a dedicated server was setup running Microsoft’s Forefront Threat Management Gateway (FTMG). FTMG is Microsoft’s firewall solution that can filter traffic based on protocol, source and destination IP. This allows the filtering of all harmful network services leaving the network such as DHCP and DNS while allowing safe traffic such as HTTP. The firewall ensures that any network service setup within the private cloud does not leak out and corrupt the services running on the university’s network. Since the self-service portal is hosted within the private cloud, a web listener was setup within FTMG that listens for HTTP requests on the external interface and forwards those requests to the appropriate web server.

3. RESULTS

The result was a fully functional private cloud. The authors achieved the deliverables of replicating the original network lab functionality while adding remote access. The authors achieved central administration and capacity planning with SCVMM and SCOM. The Forefront firewall was configured to properly limit ingress and egress traffic, while providing better bandwidth management than the current physical network (cached updates/patches as well as everyday web pages). Figure 2 shows the diagram of the cloud-based solution.

![Figure 2. Cloud Based Lab Infrastructure](image)

4. DISCUSSION

While the authors provided a fully functional private cloud, it was not able to scale to the capacity that would reflect production. This limitation was expected, but the system provided important usability metrics for its scale. The scale of a production environment system will have a similar up-front cost to creating a physical lab. This cost will be less over the long term than the current environment.

The physical lab currently requires replacement of thirty high-end desktops every three years, each desktop costing around $2,500 (price dependent on economy/market) plus licensing. With this
cloud solution, configuration virtual hosts would not require powerful CPU, RAM or disk. The system will just need enough RAM to scale to the program’s needs. The authors estimate 512MB of RAM per virtual machine and at least two VM’s per student on average. This metric equates to 50GB (512MB * 100 users) of RAM for the goal of 100 concurrent users.

It is recommended to use a minimum of two servers for redundancy. Using three servers with 25 GB of RAM each can save money. This will allow for one server to be down (for repair or maintenance) and still provide 100 percent uptime. At the time of writing this article, an HP server with 25GB of RAM lists at $5,500 (assuming $2,500 per desktop without licensing) to $16,500 for 3 servers for the cloud solution. The difference in this money would go to implementing a shared storage solution.

In addition to this up-front cost comparison, server hardware is designed to last longer than desktops and will not need to be replaced as often. New hardware will only need to be added to scale to meet the demands of the student/class.

5. REFERENCES


