V-LAB REPORT FOR FALL 2012

REPORTER: LE (LARRY) XU

ADVISOR: DIJIANG HUANG

SECURE NETWORKING AND COMPUTING (SNAC) RESEARCH GROUP

SCHOOL OF COMPUTING INFORMATICS & DECISION SYSTEMS ENGINEERING (CIDSE)

12/20/2012

ARIZONA STATE UNIVERSITY

Table of Content

1. Executive Summary

In Fall 2012 semester, V-Lab system has served 234 unique students in 10 laboratories of 4 courses. Totally 481 virtual machines and VLANs are created to allow students perform experiments in a virtualized environment, and help instructors and teaching assistants evaluate and grade the experiment results.

At the beginning of Fall 2012, the development team of V-Lab incorporated multiple new technologies and improvements to the system.

- A new Web-GUI was built based on Drupal to integrate with ASU's LDAP authentication system, which allowed students to sign-in using their ASU credentials.
- The new Web-GUI integrates with a newly developed certificate management system to issue authenticated students ID and resource access certificates that are used for Single-Sign-On (SSO).
- The V-Lab system has been migrated from a IPTABLEs-based port forwarding solution to OpenVPN-based system to provide scalability and secure communication. OpenVPN servers can be deployed at run-time in V-Lab system to increase the networking capability at run-time.
- The storage and backup system of V-Lab has been migrated from NFS-based file system to iSCSI-based block system to increase the storage capacity and availability.

During the Fall 2012 semester, V-Lab has encountered a few problems as follows.

- The OpenVPN-based solution only has preliminary scalability capability on the client side, which cannot be dynamically reconfigured at run-time. Also the client side solely depends on a random function that lacks a central control for load distribution.
- The virtual machines in V-Lab system are created using a pre-configured template and thus have same credentials when they first boot up. This may become a security issue when the virtual machine users forget to change the password.
- As a block storage system, iSCSI lacks the file system control of NFS. While NFS has full control on the file operations, iSCSI only grants read write privileges to accessing parties without any controls. This means the external party may damage the iSCSI data content without protection.

More details are described in the rest of the report.

2. V-Lab Usage Statistics

This section presents the V-Lab usage statistics.

2.1. Supported Courses and Laboratories

The table below shows the laboratories and projects that have used V-Lab system in Fall 2012:

Course	Lab Name	Instructor	Course Name
468/598	Packet Filtering Setup	Tianyi Xing	Computer Network Security
468/598	Secure Web Service Setup	Tianyi Xing	Computer Network Security
468/598	Intrusion Detection and Penetration Testing using Snort, Syslog and Openvas	Tianyi Xing	Computer Network Security
468/598	OpenFlow Programmable Network Control	Tianyi Xing	Computer Network Security
545	Software Security Lab	Stephen Yau	Software Security
545	OpenFlow Programmable Network Control	Stephen Yau	Computer Network Security
465/598	Authentication-based Web Server Lab	Ahn Gail-Joon	Information Assurance
445/598	Web-based Application Development and State Management Lab	Yinong Chen	Distributed Software Development
445/598	Service-Oriented Software Development Lab	Yinong Chen	Distributed Software Development
445/598	XML and Related Technologies Lab	Yinong Chen	Distributed Software Development

2.2. Students Usage

The table below shows the numbers of students that have used V-Lab in Fall 2012.

Course	Lab Name	Total Students	Grad students	Undergrad Students	% of Grad	% of Undergrad
468/598	Packet Filtering Setup	67	23	44	34%	66%
468/598	Secure Web Service Setup	67	23	44	34%	66%
468/598	Intrusion Detection and Penetration Testing using Snort, Syslog and Openvas	67	23	44	34%	66%
468/598	OpenFlow	67	23	44	34%	66%

	Programmable Network Control					
545	Software Security Lab	74	23	51	31%	69%
545	OpenFlow Programmable Network Control	74	23	51	31%	69%
465/598	Authentication-based Web Server Lab	54	0	54	0%	100%
445/598	Web-based Application Development and State Management Lab	39	39	0	100%	0%
445/598	Service-Oriented Software Development Lab	39	39	0	100%	0%
445/598	XML and Related Technologies Lab	39	39	0	100%	0%
		587	255	332	43%	57%

3. Improvements and New Features

This section presents the improvements and new features that have been developed and integrated with V-Lab system during Fall 2012 semester.

3.1. Certificate-based User Authentication System

At the beginning of Fall 2012 semester, the V-Lab system was integrated with a self-developed certificate management system, which was an extension to MobiCloud research project. The system can work with ASU's LDAP authentication server to issue certificates to currently enrolled ASU students and allow them to access internal resources of V-Lab.

The certificates include information for both user Identity and access control. The accesses to internal services of V-Lab such as OpenVPN and SSH can be issued as tickets with expiration timestamp. The default expiration time for tickets is one semester.

To allow students create and manage their certificates, V-Lab system provides a web-GUI that incorporates with ASU's LDAP-based authentication system. The web-GUI allows only currently enrolled ASU students to login and create their own certificates. After that, students can download the certificates and use them to provide single sign-on (SSO) for accessing all kinds of internal services of V-Lab system based on the user's privilege.

The system has been used in the whole Fall 2012 semester and very few students have had issues with using the system.

3.2. OpenVPN-based Secure Remote Experiment with High Availability

V-Lab system has been migrated from an IPTABLEs-based port forwarding solution to an OpenVPN-based remote access solution at the beginning of Fall 2012.

The IPTABLEs-based solution has been used in the past 2 years. The major problems of it are as follows:

1. Scalability issues: The IPTABLEs-based solution assigns each networking port to one communication channel. Typically each student in the V-Lab system may occupy 3-5 ports at the same time, and thus can exhaust the entire available port pool quickly. Also, the port forwarding mechanisms are maintained by IPTABLEs, which may have performance issues with a high number of concurrent connections.
2. Non-secure communication: The ports are open to the Internet and do not require a setup of secure communication to connect. If the application layer communication does not have encryption, the sensitive information over the channel maybe compromised.
3. Management issues: The port forwarding solution puts a high management overhead on V-Lab system where the admins have to reassign a port from one student to another when the student has finished using the system. Also, when changing the port assignment, the IPTABLEs must be restarted, which may affect connected users.

To solve the above problems, V-Lab system uses eight OpenVPN servers and deploys one for each XenServer. On the client side, the OpenVPN client uses a built-in round robin mechanism to randomly choose one server to connect. This allows an even distribution over clients so each OpenVPN server can server a small portion of clients. This eliminates the management issues as well because there is no need to maintain a port mapping on the server side. The OpenVPN servers may be turned off, or more servers may be added to the system to dynamically adjust the system networking capacity. Lastly, the OpenVPN establishes a secure channel each time, regardless of the networking protocol used on the application layer. This ensures the security over the communication channels.

3.3. iSCSI-based Virtual Machine Storage and Backup for XenServer

V-Lab system has been migrated from NFS-based storage solution to iSCSI-based storage and backup system at the beginning of Fall 2012. The NFS-based storage system has been used for 2 years and the major problem is networking performance. Because NFS is a file system that does not offer any internal mechanisms for high-availability networking, it is completely dependent on the underlying operating system and the Infrastructure to provide some means of making sure that network connectivity is assured. While iSCSI is in many ways dependent on the operating system, it allows for multi-path to be configured,

effectively using multiple data-links as individual paths that data may take to reach the target. By using iSCSI, the overall V-Lab system performance has been improved.

4. System Capacity and Estimation

4.1. Overview

The current V-Lab system has 8TB iSCSI storage for virtual machines. There are 4 XenServers with 24 CPUs and 64GB memory, and 4 XenServers with 16 CPUs and 32GB memory. Thus the total memory is 384GB, and the total numbers of CPUs is 160.

4.2. VM Templates

Each laboratory in V-Lab system consists of one or multiple virtual machines. The virtual machines are built based on pre-configured templates. Current system contains the following templates that are available to be created for laboratories:

- Ubuntu 10.04: 256MB Memory and 8GB Storage
- Windows XP: 512MB Memory and 8GB Storage
- Windows 2008 Server: 1GB Memory and 24GB Storage
- Windows 7: 1GB Memory and 24GB Storage

CPUs are not dedicated to VMs and thus need not to be included.

4.3. Estimated Capacity for Laboratory Hosting

Based on the current capacity of V-Lab, the approximate number of virtual laboratories that can be hosted in V-Lab is calculated as follows.

A typical Ubuntu-based laboratory assigns 3 VMs for each of 50 students:

Resource types	Resource per student	No. of students	Total Resources	No. of labs supported
Memory	256MB	50	12.8GB	30
Storage	8G	50	400GB	**20**

A typical Windows XP-based laboratory assigns 2 VM for each of 50 students:

Resource types	Resource per student	No. of students	Total Resources	No. of labs supported
Memory	512MB	50	25.6GB	**15**
Storage	8G	50	400GB	20

A typical Windows Server 2008-based laboratory assigns 1 VM for each of 50 students:

Resource types	Resource per student	No. of students	Total Resources	No. of labs supported
Memory	1GB	50	50GB	7
Storage	24G	50	1200GB	**6**

A typical Windows 7-based laboratory assigns 1 VM for each of 50 students:

Resource types	Resource per student	No. of students	Total Resources	No. of labs supported
Memory	1GB	50	50GB	7
Storage	24G	50	1200GB	**6**

The above calculations are based on the assumption of 100% resource usage. In the real world situations, V-Lab system has to retain 20% resources for redundancy or administration purpose, and thus the real number of laboratories that can be hosted by V-Lab system will be slightly less.

To sum up, the V-Lab system can support roughly 8 Ubuntu-based laboratories and 4 Windows-based laboratories at same, where each laboratory serves roughly 50 students.

5. Issues and Discussions

This section presents the issues found in V-Lab system with discussions.

5.1. Client-side OpenVPN Scalability

The OpenVPN solution supports client-side load distribution by using a random selector on the internal OpenVPN servers. While this provides certain level of load balancing, it still lacks the flexibility and reconfigurability for V-Lab system to dynamically add more OpenVPN servers and update the server list on the client side.

A better solution is to use a load balancer on the V-Lab gateway, and allow it to distribute client connection to available OpenVPN servers. There is also an alternative solution, which uses DNS server to manage and distribute workloads. These features are to be developed for next semester.

5.2. Lack of User Account Management on Virtual Machines

Currently the V-Lab system provides user management on the Web-GUI and OpenVPN. But it lacks user management for each virtual machine. By default, each virtual machine is created based on a template, and thus they all have same login credentials. This could be a secure issue when the default password may be used to login newly created virtual machines. To solve the problem, V-Lab system needs to extend the user management, which allows students to setup and manage the credentials of their virtual machines through Web-GUI.

5.3. Issues with iSCSI Storage System

The iSCSI storage system provides better networking performance than NFS. However, there are disadvantages to iSCSI system as well. As a block storage system, iSCSI lacks the file system control of NFS. While NFS has full control on the file operations, iSCSI only grants read write privileges to accessing parties without any controls. This means the external party may damage the iSCSI data content without protection.

Also, the performance advantage of iSCSI is very slight and requires enabling multi-path. In the future networking environment where 10Gbit or 40Gbit become more common, the advantage will be much less.

6. Development and Enhancements of V-Lab In Spring 2013

The existing V-Lab Web-GUI has a self-developed JavaScript-based Web canvas that can be used for students to create and customize virtual resources for each experiment. The canvas was developed without native support for Web 2.0, and thus lacks the Ajax features for dynamic pulling and updating. It also does not work well with V-Lab's new Website, which is implemented in Drupal.

The new Web canvas is developed based on an open-source project jGraph, which comes with community support. The canvas can work closely with the backend Websites and databases to provide a user-friendlier Web-GUI to future V-Lab users. The development is in process.

References

[1] V-Lab: http://vlab.asu.edu