

Design and Implementation of Construction System with High-Availability Application Service Environment

Yen-Jen Chen^{1*}, An-Liang Lo²

¹Department of Electronic Engineering, Ming Chi University of Technology, New Taipei City, Taiwan.

²Graduate School, Department of Electronic Engineering, Ming Chi University of Technology, New Taipei City, Taiwan.

* Corresponding author. Tel.: +886-2-2908-9899; email: yjchen@mail.mcut.edu.tw

Manuscript submitted October 15, 2015; accepted December 16, 2015.

doi: 10.17706/ijcee.2015.7.6.357-369

Abstract: This research is to use the virtualization technology to setup a network infrastructure and use it as a basis to design a system for constructing high-availability application service. The key to design lies in standardization of IT (Information Technology), which can be divided into 3 aspects of standardization: 1) Standardization of IT Infrastructure, which is used for defining standardization of network architecture, clustering, and virtualization; 2) Standardization of Settling Steps, which uses the standardized cluster and network architecture to define standardization of user parameter, service delivery and load balance; 3) Standardization of Controlling and Monitoring, which defines standardization of monitoring items and user controlling items. Finally, the design of the system for constructing high availability is realized through the way of implementation. It will obtain a complete construction system by continuously improving according to practical operation.

Key words: IT infrastructure, cloud technology, virtualization, clustering, high availability.

1. Introduction

Enterprises must build a stable IT Infrastructure to support business software, like PLM (Product Life Management), ERP (Enterprise Resource Planning), etc. [1]. PC, network equipment, servers, and databases are all under control of IT [2]-[4], which is wide and deep in technology, covering 1) operating system; 2) network 7-layer protocol; 3) database access; 4) information security; 5) antivirus; 6) quality of service (QOS); 7) network storage; 8) uninterruptible power supply (UPS); 9) cloud virtualization. Each of technologies cannot be obtained in a short time. However, it is hard to replace and control once the IT skills have been developed, so problems that all enterprises encounter are: 1) cost: Consideration of human quality and quantity; 2) confidentiality: IT Infrastructure administrators are easy to get confidential data; 3) rule of man: Ordinary IT staff is unable or not in the mood for documentation of technology and management details. Typically it has no standard operation procedures so that it is difficult to support or substitute for their jobs. Therefore, a round-the-clock IT Infrastructure with high availability shall be established to set up PLM and ERP systems, which is an assignment of high cost, secret worry, and being at the mercy of others. Availability represents a rate that a mechanism can be used in a period of time. For example, the availability of a mechanism is 99.98% in a year, and that means it allows 1.75 (= $365 \times 24 \times 0.0002$) hours to become invalid or stop in one year. Uptime Institute divides data centers into 4 grades. The availabilities of the 4 grades are respectively 99.67%, 99.75%, 99.98% and 99.99%. By this

standard, the highly available mechanism of the proposed scheme can reach grade 3 (99.8% availability). In order to reach such level, the mechanism must have the hot standby subsystem for taking over at any time so that the service will not interrupt. If IT administrations of standardization and regularization are automated, it will significantly mitigate the administrative workload of IT Infrastructure. Therefore, this study used the clustering and the virtualization [5] technologies of Linux authorized by the open source code to obtain a system platform [6] with high availability [7], scalability, flexibility and efficiency to support operation of business software.

Clustering refers to more than two similar equipment share one service and they can mutually support or share work. Obviously clustering technology can make the platform have a high availability and scalability. On the other hand, virtualization means an physical machine will become several virtual machines through virtualization so that hard resources can be sufficiently used and reach the so-called efficiency. Virtual machines can be transferred among different physical machines so that administrators can dispatch them flexibly and reach the so-called flexibility. Therefore, technology and intelligence administrated under IT Infrastructure are made into a settling and monitoring program, which is embedded into this platform. As a result, the above-mentioned three questions like cost, confidentiality and rule of man can be solved, and this also is an idea of IT administration automation.

This study designed a standardized application platform and developed a settling and monitoring system for an application based on this platform so as to reach the following: 1) setting of clustering and virtualization environment for settling applications; 2) providing an application with control of the virtual machine, like creation, deletion, modification, startup and shutdown, etc.; 3) monitoring if the application service is normal and using light signals to show statuses and the events to record errors. The 2nd section of this paper states work related to this study, the 3rd section states the research method and the design of the system mentioned, the 4th section describes the result implemented, and the 5th section summarizes this paper and raises the developable direction of the future.

2. Related Work

Some international cloud virtualized platforms differ from the system developed in this study. We now take a Taiwan system and an internationally famous system as an example. In 2014, "Gemini Cloud Computing Company" was established. This company is the first company to provide cloud system software and cloud application service platform in Taiwan. Its product "Gemini Open Cloud" provides enterprises or organizations with establishment of private cloud, which has been actually verified by National Development Committee Governmental Cloud, Easynet Public Cloud, Industrial Technology Research Institute Matlab Cloud, Tsinghua University Novatek Laboratory Matlab Cloud, New Taipei Government Monitoring and Analysis Cloud, and tested and verified by the Cloud Open Laboratory of the Institute for Information Industry commissioned by the Ministry of Economic Affairs. This product is commercially mature and internationally competitive. The OpenStack system is a cloud computing software jointly developed by the National Aeronautics and Space Administration and Rackspace company, authorized by Apache, and is a free software and project with open source code. OpenStack is IaaS (Infrastructure As a service) software, providing network system professionals with self-established and cloud computing services. Rackspace provides a private cloud service based on OpenStack and creates the revenue of USD 700 million and growth rate exceeding 20%. Gemini Open Cloud or OpenStack is a large-scale tool system, providing IT network system engineers with construction of IT infrastructure cloud, which differs from our study. This study does not have a large and professional engineering team as the former, so the target market takes middle and small-sized enterprises that are constructed network system as our object. Gemini Open Cloud or OpenStack has no preset network system architecture, so it needs professional engineers to

build the virtualized architecture. Therefore, enterprises also shall cost highly to purchase authorization and construction service of Gemini Open Cloud or OpenStack. The network system architecture designed by this study can be used in most of middle and small-sized enterprises, which is sold to customers in the form of hardware with highly available mechanism. Customers can use the virtual machines as a carrier to add their required application service system to the system platform through a simple interface. This process can be finished by non-professional IT infrastructure staff, so it can highly save customers' cost in IT administration.

3. Design of Construction System of Application Programs

In this paper, a construction system with high availability will be designed to settle and monitor application service. The key lies in standardization of the IT environment operated by the application, including standardization of IT Infrastructure, standardization of Settling Steps, and standardization of Controlling and Monitoring. Contents and principles of all standardizations will be described as following.

3.1. Standardization of IT Infrastructure

The standardization of IT Infrastructure is further divided into standardization of network topology, standardization of clustering and standardization of virtualization.

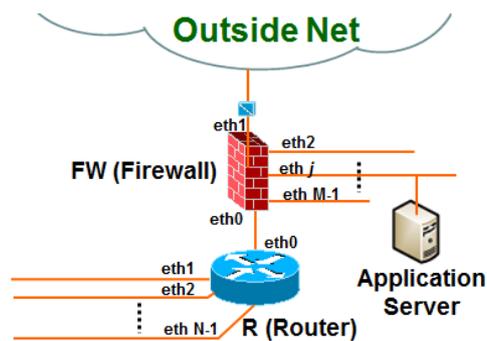


Fig. 1. Standardization of network architecture of IT infrastructure.

A network architecture consists of router, switch and firewall. In the process of virtualization, the three items are virtual machines. The switch is replaced by the virtual network built in the virtual operating system (Hypervisor). If you want to connect all virtual machines that they are placed together, you only need to bond their network interfaces to the same virtual network so that they will be connected together and become one LAN (Local Area Network); therefore, the standardization of the entire architecture lies in the domain cutting in the layer 3 of OSI (Open System Interconnection) model and the domain protection in layer 3~7). The former is realized by the router and the latter is realized by the firewall. By this idea, the standardized architecture for application operating environment is as shown in Fig. 1. The eth0 and eth1 interfaces of firewall are respectively connected to intranet and extranet. The eth j interface is used for settling the virtual machine where the application is installed and the application servers (as shown in the Fig. 1). The variable, j, refers to the application server that it can provide different network segments with different service items. The intranet has more than one network segment constructed by the router, R, which can be connected to the corresponding physical network so that users from different departments can link to the application server behind firewall through R.

The clustering can realize availability and scalability of the construction system, and its standardization is respectively applied to networks and servers. The dual-node clustering is used for various route-controlled equipment to reach HA (High Availability) [8], [9], i.e., at any time, one of the two nodes is the active node,

which is responsible for the connection path control, and other one is the standby node, which is responsible for backing up the active node. Servers providing application service use the multi-node clustering [10]. These nodes share incoming connections to reach the load balance [11] of the entire service. New nodes can be dynamically added or invalid nodes can be dynamically removed, which not only can reach the high availability and the scalability of the service.

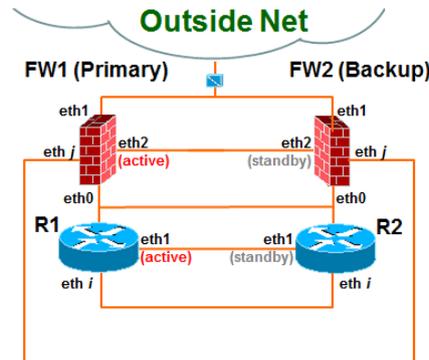


Fig. 2. Standardization of clustering of network equipment.

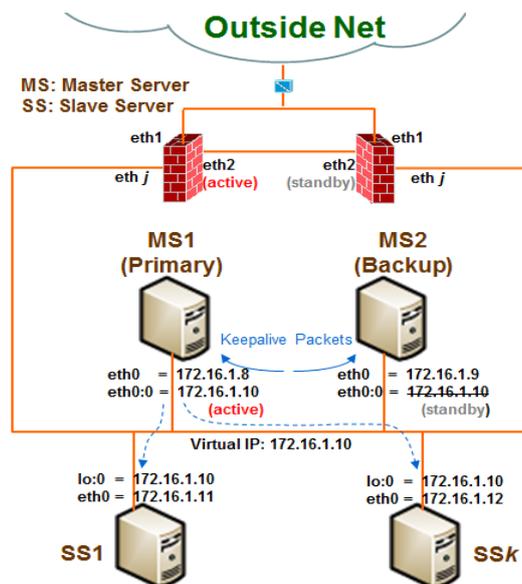


Fig. 3. Cluster standardization of application server.

Fig. 2 shows the standardized architecture of the network equipment, of which FW1 and R1 are in primary side, so it is preset as active node, and if it goes wrong, the standby node in the backup side will become active. Fig. 3 shows the standardized architecture of the application server [12], of which MS (Master Server) is responsible for externally representing the entire clustering to accept a user connection, and then the connection is introduced to SS (Slaver Server) that is actually responsible for service. The assignment method performed by MS is a simple round robin or advanced weight allocation system. MS1 and MS2 are in an HA cluster with high availability, of which one is active, and the other is standby. From SS1 to SS k (where $k > 1$), they form a LB (Load Balance) [13], [14] cluster. They are all active and wait and process connections introduced by MS. This architecture is called Direct Routing [15]. Its advantage is that MS is only responsible for redirecting connections. The response to connections is done by SS, which directly faces users and will not pass through MS. MS will not become the bottleneck of the entire load. In Fig. 3, the external address of application server cluster is 172.16.1.10, which is also called the virtual IP

address (virtual IP, VIP) of MS and SS. It is respectively realized in the eth0:0 interface of active MS and the lo:0 interface of all SS. This makes the real IP addresses in cluster invisible in the user end, so its transparency is perfect.

The virtualization standardization takes authorization of open source code and high operating efficiency as design factors. The former is the guarantee of cost and future program maintenance and use, and the latter is not only flexible but also efficient when applying to virtualization. On the aspect of virtualization operating system, i.e. Hypervisor, it plans to use the Linux system authorized by the open source code to construct the platform, so KVM (Kernel-based Virtual Machine) is selected as the constructor of virtualization environment. It is a part of Linux Kernel, so when making the virtualization control, it can directly use the hardware without additional control through kernel (since it is the kernel). Its efficiency performance can match with Xen (another Hypervisor of Linux), which is also the main factor considered. On the aspect of network operating system, it uses Vyatta [16] software router and firewall to realize the network system. As shown in Fig. 2, the system image files of FW1, FW2, R1, and R2 from Vyatta can be downloaded free, and their efficiency is quite good. On the aspect of the application server, it uses Linux Ubuntu to realize MS. As for SS, it can use Linux (e.g., Ubuntu, CentOS, Red Hat, Suse,...), Unix-like and Windows to realize it, which make almost any software can be settled in this standardized construction system.

3.2. Standardization of Settling Steps

When an application server SS cluster needs to be settled in the standardized construction system of this paper, users shall specify the following parameters:

- 1) Domain belonged: as shown Fig. 3, segment eth j the SS cluster belonging to shall be specified.
- 2) Number of application servers SS: as shown in Fig. 3, the quantity is k.
- 3) SS's basic parameters: CPU quantity, memory capacity, operating system, and system image file path.
- 4) Service protocol and address: protocol (TCP or UDP), extranet IP address, and service port number.

```
#sudo gedit /etc/keepalived/keepalived.conf
global_defs {
  router_id LVS_DEVEL
}
vrrp_instance VI_1 {
  state MASTER
  #state BACKUP
  interface eth0
  virtual_router_id 51
  priority 200
  #priority 100
  advert_int 1
  authentication {
    auth_type PASS
    auth_pass 1111
  }
  virtual_ipaddress {
    192.168.2.210
  }
}
virtual_server 192.168.2.210 8080 {
  delay_loop 1
  lb_algo wrr
  lb_kind DR
  persistence_timeout 60
  protocol TCP # Only TCP is implemented
  real_server 192.168.2.211 8080 {
    weight 1
    TCP_CHECK { #TCP healthchecker
      connect_timeout 10
      connect_port 8080
    }
  }
  real_server 192.168.2.212 8080 {
  }
  real_server 192.168.2.213 8080 {
  }
  real_server 192.168.2.214 8080 {
  }
}
```

Fig. 4. Master Server (MS) uses keepalived.conf file to set HA and LB mechanisms.

According to the said parameters, the system looks for an unused IP address in the domain to which the SS cluster belongs and returns the address to users. As the service's intranet IP address (i.e., the virtual IP address as shown in Fig. 3 and Fig. 4, VIP), intranet users use this IP address as the destination address for linking this application service. The construction system programs for settling the application service with high availability shall totally complete the four parts of setting functions as follows:

- 1) MS setting in the application server cluster (Fig. 3).

- 2) SS setting in the application server cluster (Fig. 3).
- 3) Firewall (FF) setting in the network cluster (Fig. 2).
- 4) Router (R) setting in the network cluster (Fig. 2).

When a set of SS clusters are added, the system firstly shall generate a VIP, which is used as the representative IP address of the SS cluster in intranet, and then the VIP shall be set in MS1 and MS2. Master Server (MS) uses `ipvsadm` and `keepalived` utilities [17] of Linux to realize HA (High Availability) between them (i.e. MS1 and MS2). MS also uses this two utilities to allocate user connections to the application server SS so as to realize LB (load balance) between SS servers. The mechanisms of HA and LB are all in the file `keepalived.conf` of the LVS `keepalived` utility, as shown in Fig. 4. A new VIP shall set a new HA Service Instance, and a new LB Scheduling shall be added to the SS cluster. After setting, the `keepalived` service shall be restarted.

In terms of the setting of the application server SS, it mainly sets the new VIP to `lo:0` interface of SS, and creates a route to the VIP in SS so that when a packet with the destination address of VIP received by SS, it can forward the packet to `lo:0`. Since the IP address of `lo:0` is VIP, SS receives the packet and processes it, and then responds to the source end of the packet, i.e., the user end.

Table 1. Translation Table for Address and Port Number of Application Server

PLM	192.168.2.215:8080 ↔ 192.168.100.210:8080
VNC AP1	192.168.2.215:5911 ↔ 192.168.100.250:5921
VNC AP2	192.168.2.215:5912 ↔ 192.168.100.250:5922
VNC AP3	192.168.2.215:5913 ↔ 192.168.100.251:5921
VNC AP4	192.168.2.215:5914 ↔ 192.168.100.251:5922
SSH AP1	192.168.2.215:2211 ↔ 192.168.100.211:22
SSH AP2	192.168.2.215:2212 ↔ 192.168.100.212:22
SSHAP3	192.168.2.215:2213 ↔ 192.168.100.213:22
SSHAP4	192.168.2.215:2214 ↔ 192.168.100.214:22

After setting the HA and LB mechanisms of SS cluster, the NAT (Network Address Translation) shall be further set for VIP of SS and extranet IP address. This mechanism shall be set in FW as shown in Fig. 2. In order to protect setters from setting complex configuration for operate the SS cluster, it shall automatically provide address translation of remote service VNC and SSH in addition to the address translation of its application service so that setters can control the application server SS through the remote desktop (by VNC) or text commands (by SSH). The use of SSH is because it needs SCP (Secure Copy) to encrypt the file transfer. SCP must work through the SSH channel, so the demand of SSH is not inferior to VNC. The adoption of VNC other than RDP (Remote Desktop Protocol) is because the KVM system holds one VNC port for each internal virtual machine in physical machines by default, so users can remotely control the corresponding virtual machine when they connect the IP address and VNC port of the specified physical machine distantly. Since it is the default function of KVM, the use of VNC can decrease many extra settling steps. Table 1 shows an example of using PLM (Product Life Management) as application service. It sets a cluster with 4 SS servers (named as AP1~4), of which address translations of PLM, VNC and SSH are as shown in Table 1. Per the corresponding intranet and extranet addresses of SS servers as shown in Fig. 5, the VIP of the SS cluster in this example is 192.168.100.210, the IP addresses of AP1~4 are 192.168.100.211~214. The extranet IP address 192.168.2.215 corresponds to the intranet VIP. The VNC connections are not connected to the virtual machines but connected to the physical machine IP addresses 192.168.99.250~251 (i.e. for Host A and B).

In addition, the protection policy of the SS cluster can be made into the filtering rule and set in the firewall FW or the router R. For example, connections from extranet can be divided into Internet

connections or subsidiary connections. Whether it is PLM or ERP, the direct access of Internet connections is not allowed. Therefore, if the SS cluster belongs to the network segment for FW's private service, it will prohibit Internet connections into FW's eth1 interface (Fig. 1 and Fig. 3) from being connected to the SS cluster. The joining of the SS cluster also will open or prohibit some intranet connections from being connected to the application service SS. These filtering rules shall be set in the network interface of the router R (Fig. 1).

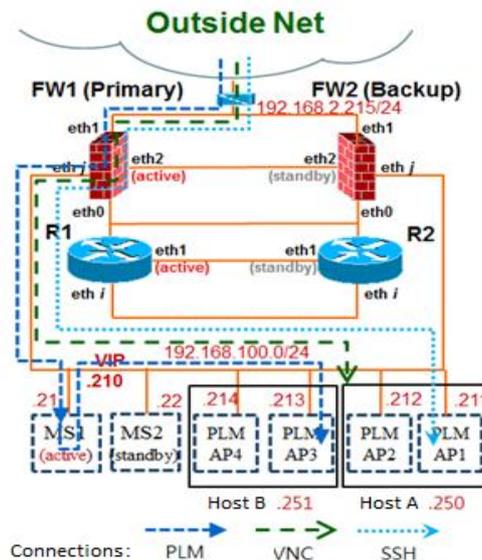


Fig. 5. Intranet and extranet IP addresses of application server and the related service connections.

3.3. Standardization of Controlling and Monitoring

The setter of the SS cluster shall completely control the virtual machine where the server is installed but shall not access or use other virtual machines, so a web-based control interface is designed in this paper to make the SS cluster setters control its virtual machine (VM) as below:

- 1) VM Operation: Create, Delete, Power On/Off;
- 2) VM Modification: Number of CPUs, Memory Size, System Image File Path;
- 3) Single Sign On: VNC Password Modifying.

```

itex@HostB:~$ virsh list --all
Id Name State
-----
 2 BService_MS2 running
 3 BXvr_PLMAP4 running
 4 BService_MS1 running
 6 BXvr_PLMTS2 running
 8 BService_Dual2 running
 9 BXvr_PLMAP3 running
10 BService_Dual1 running
45 BNetwork_Rtr running
46 BService_Monitor running
47 BNetwork_FW1 running
48 BNetwork_FW2 running

itex@HostB:~$ virsh net-list --all
Name State Autostart
-----
default active yes
Network1 active yes
Network2 active yes

itex@HostB:~$ virsh dumpxml BService_MS2 > a.xml
itex@HostB:~$
    
```

Fig. 6. Functions and demonstration of command virsh.

```

itex@HostB:~/monitor
itex@HostB:~/monitor
<domain type='kvm' id='4'>
  <name>BService_MS2</name>
  <uuid>bs850bad-4417-da62-4ea8-deb44f4d2e24</uuid>
  <memory>1048576</memory>
  <currentMemory>1048576</currentMemory>
  <vcpu>1</vcpu>
  <os>
    <type arch='x86_64' machine='pc-i.0'>hvm</type>
    <boot dev='hd' />
  </os>
  <features>
    <acpi />
    <apic />
    <pae />
  </features>
  <clock offset='utc' />
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/bin/kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' />
    </disk>
  </devices>
</domain>
itex@HostB:~/monitor$
    
```

Fig. 7. Parameter file in XML of virtual machine.

The VM operation mentioned above can be performed through the command virsh within the libvirt-bin function library. In addition, as for modification of the VM parameters, users also can directly modify the VM parameter file in the XML form. As shown in Fig. 6, it uses the virsh command to list all established VMs as well as all established virtual-network. Fig. 7 shows the parameter file of VM. This file contains the CPU quantity of virtual machine, memory capacity, and virtual machine's name in KVM environment.

In order to allow the SS cluster's setter to immediately know the cluster's health status, it automatically constructs the webpage to present the healthy light signal [18]. Green light means normal and red light means service error. There are three kinds of services (AS, VNC, and SSH), so the light signal is also divided into three types, as shown in Fig. 8, its AS (application service) takes PLM as an example. All VMs (online machines AP1~4 and test machines TS1~2) are brought into monitoring. Each service of each VM is designed with two light signals, which show the current status of the service. It uses Nmaputility [19] (an valid open source authorized network service scanning software) to scan the specified service port, and if it fails to get any response from the service port, the first light signal will turn to red, and if it fails to get any response of the service port within 3 consecutive periodical scans, the second light signal will turn to red. Fig. 8 shows the design of service health status. In addition, all errors will be recorded by events.

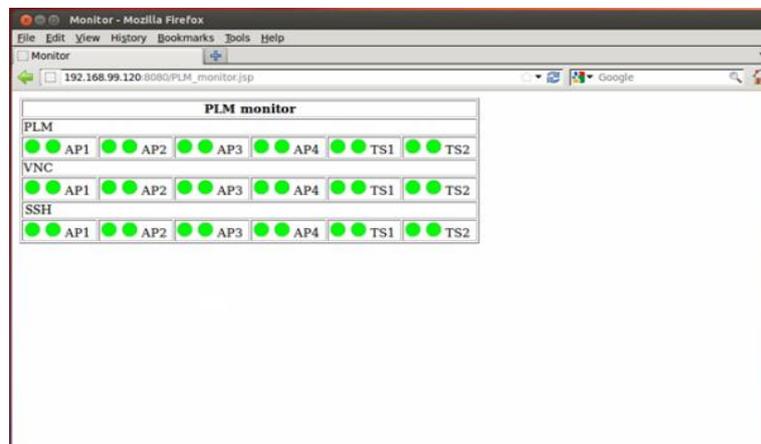


Fig. 8. Image design of service health status of application service.

4. Implementation and Results

The management of the actually operated virtual machine is as shown in Fig. 9, which shows the primary side mentioned in the previous section. Every item in the figure represents a virtual machine, and each virtual machine is created by KVM. As for its architecture, users can use Fig. 5 as a reference. In Fig. 9, virtual machines whose name is with "Network" use the software Vyatta to realize the firewall and the router. "MS" is the same as the MSas shown in Fig. 3, and it standardizes the cluster of the application service. Others are SS servers providing specific services.

Fig. 10 shows the cluster status visible in FW1. "Active" represents the system is in normal operation. If it does not particularly note "(standby)" next, it indicates this item plays the active role in the cluster. When there is a problem with the active one, it will automatically switches to the standby one. So far the construction system has been successfully formed to complete the standardization of IT Infrastructure and the standardization of Settling Steps stated in the previous section by using the virtual machine as the IT infrastructure.

The standardization of Controlling and Monitoring is realized by controlling the webpage, as shown in Fig. 11 to Fig. 15. From the top of Fig. 11, a menu mainly consists of 4 hyperlinks, Monitor, AP_Monitor, Hisotry and Contorl, of which the Monitor page is similar to AP_Monitor in the monitoring and exhibition method.

The red and green lights are used for monitoring the current state of the construction system. The difference is that AP_Monitor (See Fig. 8 for its form) is to monitor the server added into by users but Monitor is to monitor the default server and network objects in the standardized infrastructure. In the Monitor page, the monitoring item is further divided into 4 levels, which are respectively the Application, Network, Physical and Server. When the light signal going wrong turns to red from green, users can intuitively know which level of the construction system has problems. Press the hyperlink next to the light signal, it will show its related history under the log list, which shows the records for a specified object. However, the History page shows the comprehensive history of the construction system. Users can view the complete history and know the past running status. It is also helpful to debugging.

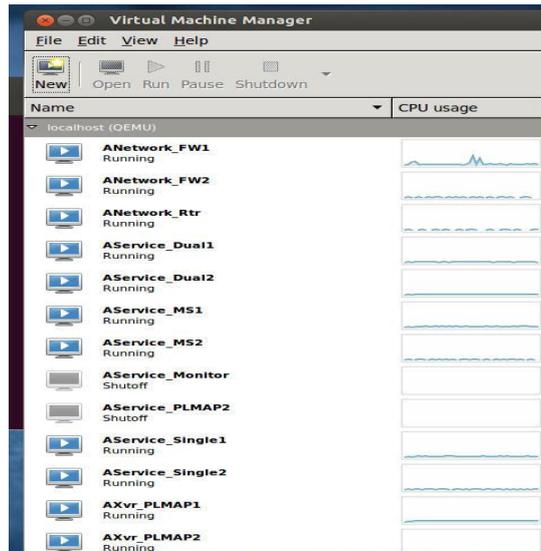


Fig. 9. Management screen of virtual machine in KVM.

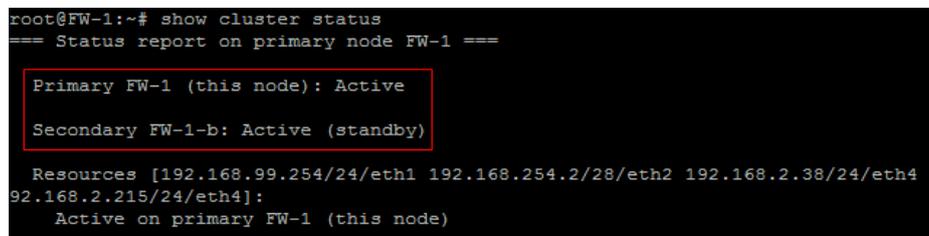


Fig. 10. Active and passive statuses of cluster.

Fig. 12 to Fig. 15 shows the control screens, which are used for controlling related settings of the construction system, and their functions include modification of user password, VPN user setting, startup and shutdown of virtual machine, creation and deletion of virtual machine. These functions shall be operated in such a manner that users manually enter or modify related parameters in the text interface mode. However, this design uses the webpage to provide a user interface to simplify the complex test operation mode.

Fig. 12 is the control screen of startup and shutdown of virtual machines. The startup and shutdown buttons are next to the corresponding virtual machines. When pressing the corresponding function, it will start up or shut down the virtual machine. The left half part is the default virtual machine and the right half part is the virtual machines newly added by users in the main frame. Thus users can completely control virtual machines.

Fig. 13 is the control screen of creating virtual machines. The left half part shows parameters for creating

virtual machines, including physical machine where virtual machines are installed, specified network segment, IP address, OS type and VNC password and the right half part is the details of the input parameter so that users can know the setting of the function.



Fig. 11. Monitoring screen.

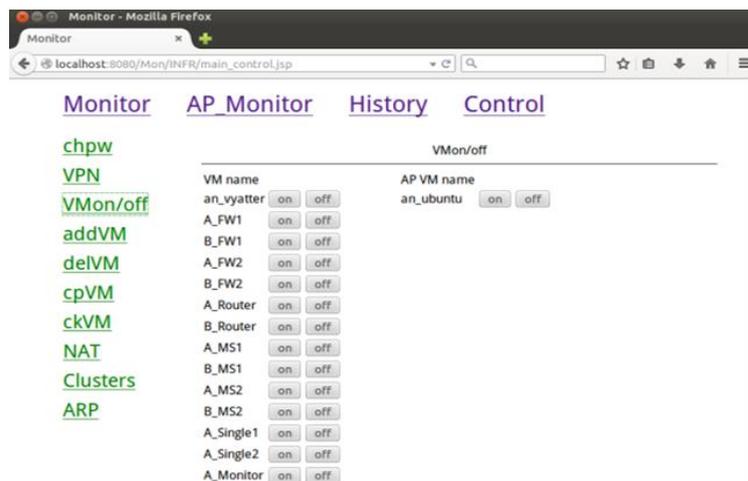


Fig. 12. Startup and shutdown of virtual machine.

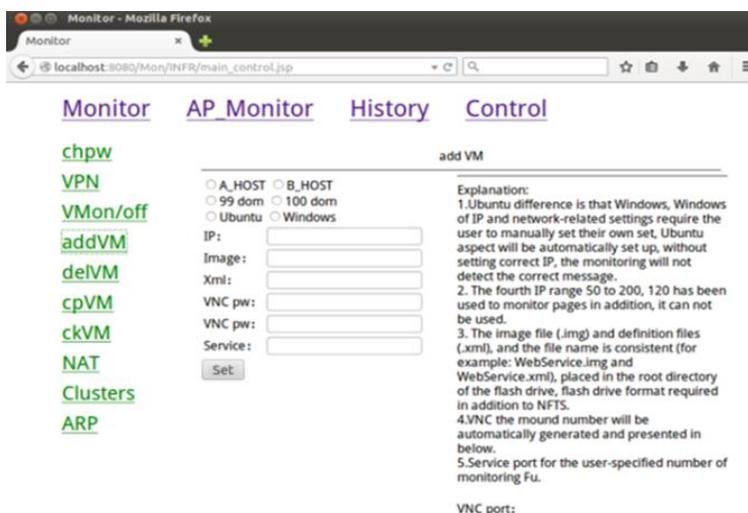


Fig. 13. Creation of virtual machine.

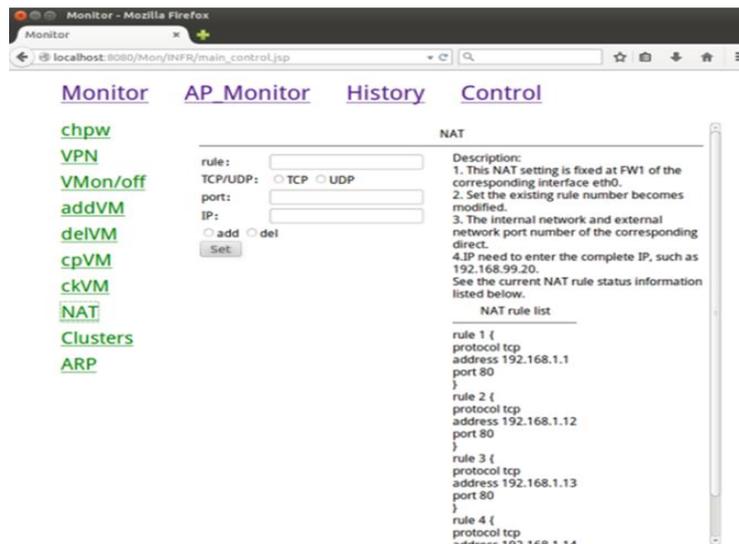


Fig. 14. Setting of NAT.

Fig. 14 is the control screen of NAT. The left half part is the required parameters and the top of the right half part is descriptions and its bottom shows the current NAT rule list for user reference. The NAT setting is defined as connection of intranet and extranet ports, so the input parameter is more simplified and convenient for users to implement input operation.

Fig. 15 is the control screen of clusters. Functions set by clusters are mechanisms of LB. One VIP is used as the representative number to allocate service to more than one real IP addresses. The upper left part is the input of the control parameters, and the upper right part is descriptions. The Public and the Private below respectively correspond to MS1 and MS2, showing the current settings of clusters for user reference.

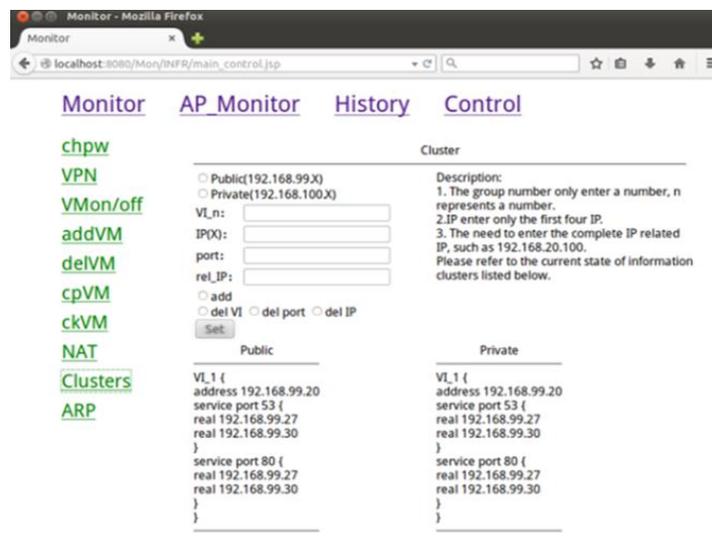


Fig. 15. Control of clusters.

5. Conclusions

In this paper, a construction system with highly available application service environment was designed and implemented to reach: 1) settle settings of creating clustering and virtualization environments required by applications; 2) provide the virtual machine where an application is installed with control, like creation, deletion, modification, startup and shutdown, etc.; 3) monitor if the application service is normal, and use light signals to show status and generate events to record errors. After being tested for about half a year,

and normally switching between primary side and backup side, it shows no any problems. The dispatching mechanism for load balance of MS to SS is normal, the entire system works normally, and the server service is also not disconnected. It has reached the high availability, so it proves that the virtualization of the network infrastructure is feasible under the current hardware environment. On the aspect of monitoring, the light signals shown by the webpage also can correctly show the status of the interface and the service so that users can visually know the full status of the construction system. On the aspect of control, users can add new service servers to the system and it also has no problems in operation. This proves that the construction system is scalable. However, the control function in webpage is not complete yet. Part of settings shall be completed manually.

The system still does not reach the completed status and needs to be adjusted and improved in the future. The primary purpose is that the webpage control interface shall be complete so that all controls can be finished in the webpage and the operability of the system is increased. Secondly the entire operation has already no problems but it is still not clear about the tolerances of a large amount of network traffic and disk access. Therefore, it shall be tested by the high traffic and data access before being improved. Finally the safety shall be taken into account. Information security is important to the system but very complex and difficult. It is a great challenge for standardizing and automating the security system.

References

- [1] Techtarget. (2015). Definition of high availability. Retrieved October 11, 2015, from <http://searchdatacenter.techtarget.com/definition/high-availability>
- [2] Cisco. (2007). *Cisco Data Center Infrastructure 2.5 Design Guide*. Cisco Validated Design.
- [3] Bitar, N., Gringeri, S., & Xia, T. J. (2013). Technologies and protocols for data center and cloud networking. *IEEE Communications Magazine*, 51(9), 24-31.
- [4] Cisco. (2015). Cisco data center high availability clusters design guide. Retrieved October 11, 2015, from <http://www.cisco.com>
- [5] Duan, Q., Yan, Y., & Vasilakos, A. V. (2012). A survey on service-oriented network virtualization toward convergence of networking and cloud computing. *IEEE Transactions on Network and Service Management*, 9(4), 373-392.
- [6] IT Today. (2013). Is high-performance computing for you? *IBM Systems Magazine, Power Systems*.
- [7] HP. (2014). Designing disaster tolerant high availability clusters. *HP Document*.
- [8] Araujo, J. A., Lazaro, J., Astarloa, A., Zuloaga, A., & Garcia, A. (2012). High availability automation networks: PRP and HSR ring implementations. *Proceedings of IEEE International Symposium on Industrial Electronics (ISIE)* (pp. 1197-1202).
- [9] Radhakrishnan, R., Mark, K., & Powell, B. (2008). IT service management for high availability. *IBM Systems Journal*, 47(4), 549-561.
- [10] Sharkh, M. A., Jammal, M., Shami, A., & Ouda, A. (2013). Resource allocation in a network-based cloud computing environment: Design challenges. *IEEE Communications Magazine*, 51(11), 46-52.
- [11] Lin, C. C., Chin, H. H., & Deng, D. J. (2014). Dynamic multiservice load balancing in cloud-based multimedia system. *IEEE Systems Journal*, 8(1), 225-234.
- [12] Liao, C. F., Chang, H. C., & Fu, L. C. (2013). Message-efficient service management schemes for MOM-based UPnP networks. *IEEE Transactions on Services Computing*, 6(2), 214-226.
- [13] Mahmood, A., & Rashid, I. (2011). Comparison of load balancing algorithms for clustered web servers. *International Conference on Information Technology and Multimedia (ICIM)* (pp. 1-6).
- [14] Membrey, P., Plugge, E., & Hows, D. (2012). *Practical Load Balancing: Ride the Performance Tiger* (1st ed.). Apress.

- [15] Lammle, T. (2013). *CCNA Routing and Switching Study Guide* (1st ed.). Sybex.
- [16] Vyatta. (2014). Vyatta community documentation. Retrieved August 15, 2014, from <http://www.vyatta.org/>
- [17] LVS. (2015). Retrieved October 11, 2015, from <http://www.linuxvirtualserver.org>
- [18] Ahmed, I., Auvenshine, J. J., & Blackburn, J. (2011). System for autonomic monitoring for web high availability. IBM Corp. US Patent 7996529 B2.
- [19] NMap. (2015). Retrieved October 11, 2015, from <http://www.nmap.org/>



Yen-Jen Chen was born in Taiwan. He received the B.S. and Ph.D. degrees in computer science and information engineering in 1989 from Tatung Institute of Technology and in 2000 from National Chiao Tung University (NCTU), Taiwan, respectively. From October 2000 to July 2001, he was an assistant professor under the collaboration project of NCTU and Cisco Systems Inc. for developing VoIP testing technology. From August 2001 to August 2002, he was a network design consultant in Unisys Corporation, Taiwan. Since August 2002, he is an assistant professor in the Department of Electronic Engineering, Ming Chi University of Technology, Taiwan. His research interests include traffic engineering and quality of service in computer networks, network management and system integration, Internet of things, and cloud virtualization.



An-Liang Lo was born in 1991. He received the B.S. degree from the College of Electronic Engineering, Ming Chi University of Technology (MCUT) and is currently pursuing the M.S. degree from the College of Electronic Engineering, Ming Chi University of Technology. His research interests include cloud computing, virtualization technology and so on.