QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Virtualizing Network Services: Practical Perspectives

Emad H. Al-Hemiary
Networks Engineering Department, College of Information Engineering, Al-Nahrain University – Baghdad - Iraq
emad@coie-nahrain.edu.iq

ARTICLE INFO

Article History:

Received: 18 March 2017

Accepted: 1 April 2017

Published: 10 April 2017

DOI:

10.25212/lfu.qzj.2.2.47

Keywords:
Virtualization, virtualized network services, open-source datacenters.

ABSTRACT

The work in this paper focuses on creating virtualized network services for datacenters based on open-source software and explains the preliminary and mandatory requirement associated with. Datacenters are necessity for organizations to maintain their workflow and processed data as well as fast and secure data retrieval. The current and future design emerge virtualization as key technology in efficient and manageable datacenters. Therefore, the design proposal is based on virtualizing physical servers to the required services following infrastructure as a service. The designed and implemented network use open-source operating systems and software exclusively. Different types of services like web, email, eLearning, databases, and Cloud ready are included and tested. The runtime for the implemented datacenter clearly supports this proposal and confirms the direction of use open-source software over closed-systems for building highly customized network services and reduce overall cost.

1. INTRODUCTION

Datacenter is a combined electrical, mechanical, and civil infrastructures within an organization, city, country or worldwide level. Whether it is centralized or distributed, many requirements are listed by specialists for efficient and powerful datacenters [1,2]. These requirements include specialized rooms containing networking devices and servers secured by special equipment and maintained operational most of the time using backup electrical systems supporting power failure situations. The main function of datacenters is the store and process of data as well as network services. Every organization; small, intermediate, or enterprise have their own datacenter where it keeps and centralize its information technology (IT) communications within one or more physical geographical area. Storing data coming from within the organization or remotely from other connected sites is associated with security measures. Therefore, IT specialists link data storage servers with security access [3].

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

When datacenter network requires more servers to be added in order to increase capacity or add new type of service, physical hardware servers increase and large number of servers becomes an issue which need more management, control and operational power. This where virtualization [4] takes place. Virtualization is the process of exploiting server's power through creating smaller virtual servers, services, or functions. Imagine a hundred service and each counted service requires a standalone server with (x_s, y_s, z_s) where the latter symbols represents (processing speed, dynamic memory, permanent storage). If one physical server have (x, y, z), then approximately, a new virtual machine (VM) could be created as long as:

$$y_a > y_s | x, z \qquad (1)$$

Where y_a is the available memory given by:

$$y_a \cong y - y_{os} \qquad (2)$$

and y_{os} is the required memory for the operating system running virtualization and the symbol | represents conditional relation on x and z. As long as the x and z (central processing unit supports virtualization and the permanent storage is dynamically allocated and adequate) are satisfied, the virtual machine is related to the available memory. According to that, the number of VMs can be counted approximately as:

$$Number\ of\ VMs \cong \frac{y_a}{\sum_i^n y_{si}} \qquad (3)$$

Thus, the major requirement for creating virtual machines within physical sever is the capacity of its dynamic RAM (random access memory). For the previous calculations, the one hundred server's example could be distributed over five, ten or twenty physical servers depending on the server's power and capacity. Whenever the cost and space is a problem, virtualization is the solution. Many management software called Hypervisors [5] allow many guest operating systems to run on the same physical server machine. Kernel Virtual Machine (KVM) [6], VirtualBox [7], Xen [8], and VMWare [9] are examples of widely used hypervisors. Since the focus of this work is based on open-source, Linux-based software are used exclusively. The rest of the paper is organized as follows: Section 2 discusses network services and their practical implementation requirements and section 3 gives the implemented virtualized network layout. Conclusions are given in section 4 and finally references are listed in section 5.

2. NETWORK SERVICES AND THEIR PRACTICAL PERSPECTIVES

The aim of this work is to highlight the practical requirements to establish an open-source datacenter supporting small business organization and based on virtualizing network

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

services. Basically, Domain Name System (DNS), Web, and Email are main services required to establish datacenters. The following sections explains these services in details.

2.1. DNS

The naming strategy followed since the Internet becomes globally wide helps end users to use names instead of numbers in web browsing and servers connections. This is better remembered since numbers; referred to IP (Internet Protocols) addresses, are difficult to remember and might change according to organization network updates. Therefore the naming strategy (DNS) is essential whenever web, email, multimedia or other types of services are operational. Shortly, DNS functionality is to map names to IPs and vice versa. But this is not the only functionality it possesses! DNS is actually the key to other services especially when ownership and authentication is required for the domain it serves. To highlight this function, figure 1 shows a typical DNS network services or protocols hosted by an organization denoted by local site. As the figure shows, an authoritative-only DNS (responds only to queries about domains or subdomains configured inside by the network administrator) with master-slave configuration to ensure continuous operation and this should be physically separated and not in the same geographical area and also not logically addressed by the same subnet to isolate any power or network failure and keep service operational. The DNS server consists of two zones: forward and reverse. The forward zone configures the domain name like anydomain.com and lists all the required records within a file known to the DNS process called forward zone, while the reverse zone is required for IP-Name verification, this is explained later on. As shown in figure 1, the master (primary) DNS service updates its slave (secondary) with zone records periodically or when the zone file serial number is changed, and in this way the slave becomes an updated copy from the master.

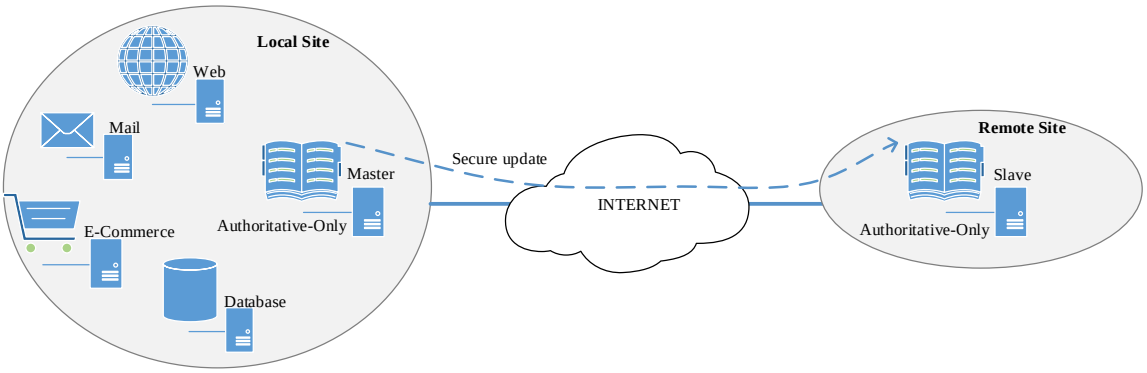

FIGURE 1. Master-Slave practical implementation for reliable DNS operation.

When a request from the Internet targeted one of the services (Web, Mail, etc.) in the local site, the DNS receives a query for the IP address of the server hosting this service from the requester (the operation is actually a series of requests and replies [10]). The DNS server through its service contacts its local database and reads the forward zone A record (The A records maps domain or subdomain names to their assigned IP address) as shown in figure 2. It is important to mention here that the local site may have its own DNS's for serving local clients and these DNS's are not what figure 2 shows. As the reader recalls, the main IP version 4 TCP/IP settings requires four IP numbers to work: IP address of the machine, subnet mask, default gateway (first router the client connects to) and the primary DNS to contact for web requests. The latter one is called non-authoritative and responds to any query

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

through its local cache. On the other hand, DNS holds authentication records for verification purposes. As an example, the google site verification is a TXT record issued by Google for a specific domain to verify its ownership and this is used typically for verifying domain mail server as it will be shown later on. Table 1 shows authentication records and their functionality.

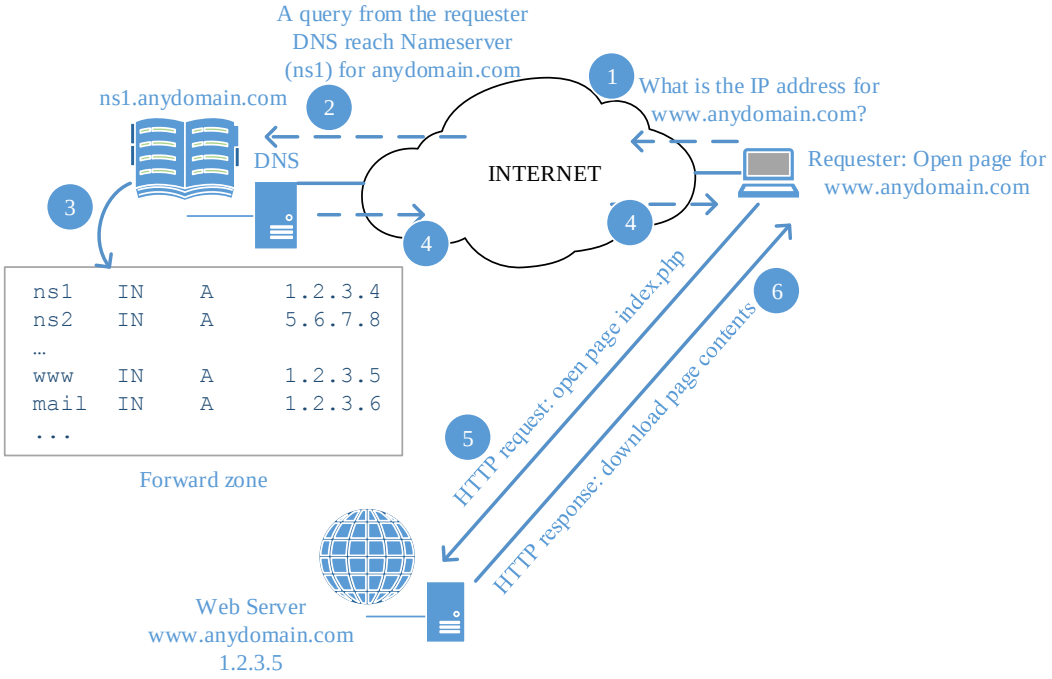

FIGURE 2. DNS response to queries. All messages are exchanged over UDP port 53.

2.2. MAIL

One of the main services required by an organization for exchanging messages is the electronic mail. E-Mail service is composed of many protocols for sending and receiving messages. The E-Mail server uses Simple Mail Transfer Protocol (SMTP) [11] either unsecured (port 25) or secured (Secure Socket Layer - SSL port 465 or Transport Layer Security – TLS port 587) to send messages to another server. The receiving protocols are mainly Post Office Protocol or simply POP3 (Unsecured port 110 or SSL port 995) and Internet Message Access Protocol or simply IMAP (unsecured port 143 or SSL port 993). Due to the fact that email is a source of Spams and Viruses, ownership and authentication of the sending mail server is required by the receiving mail server. The process involves a trace back from the recipient Mail Server to the sender as shown in figure 3. When an email is send from some mail server to another one, the recipient mail server contacts the ISP (Internet Service Provider) of the sender's mail server asking for reverse lookup of its IP address to its name. If a match is found then the email is accepted, otherwise the recipient mail server establish a reject policy regarding the sender's mail server and its IP address. The case becomes worse when the recipient mail server is Yahoo, Gmail, Hotmail or other free web-based global mail servers. This is due to the 'SPAMHAUS Project' [12] where IP addresses are stored as black listed. Therefore, for practical perspectives, any mail server should contact SPAMHAUS database to ensure and verify senders.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

As figure 3 reveals, the role of DNS is clearly mandatory in the process of sending and receiving email. Without the authentication mechanisms shown in table 1 and figure 3, the email sender cannot sustain his eligibility and thus considered as Spam.

TABLE 1: Authentication records required for practical authoritative-only DNS servers

Record	Type	Typical form record	Function
SPF	TXT	"v=spf1 +a +mx +ptr +ip4:1.2.3.6 include:mail.anydomain.com ~all"	"Identifies which mail servers are permitted to send email on behalf of anydomain.com. The purpose of an SPF record is to prevent spammers from sending messages with forged from addresses at your domain."
Google domain verification	TXT	google-site-verification=-Aqw1jSo8lsOZwbwd-cQ5bQvtm-M1DqVEHEIKXZ1z6U	Unique security token provided in the Google Admin console's verification instructions. The token is a 68-character string that begins with google-site-verification=, followed by 43 additional characters.
Domain Keys	TXT	"v=DKIM1; p="domain public key"	Define DomainKeys policy and public encryption keys for a domain name. Each email message will be signed by domain's public key.
DMARK	TXT	_dmarc.anydomain.com IN TXT v=DMARC1; p=none	The goal of DMARC is to build on this system of senders and receivers collaborating to improve mail authentication practices of senders and enable receivers to reject unauthenticated messages.

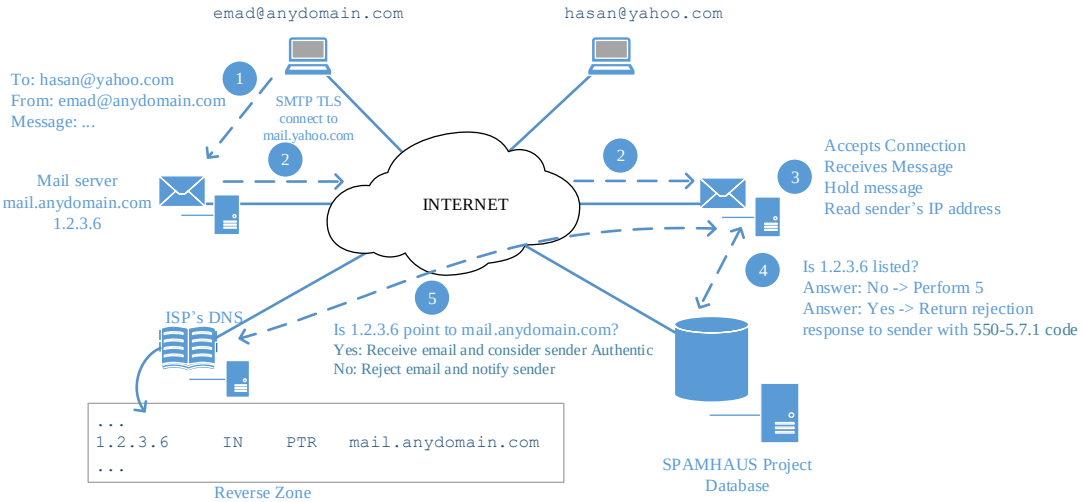

FIGURE 3. Sender's mail server authentication mechanism. PTR refers to pointer as it points IP address to name

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

2.3. WEB, DATABASE AND OTHER SERVICES

Most of the Internet services requires web access using Hypertext Transfer Protocol (HTTP or HTTP over SSL – HTTPS). The process involves a mechanism of requests and responses messages between the Web client and Web server to download and view the page contents using an application layer software like Internet Explorer. The pages forming the dynamic website normally store its contents in databases for future retrieval. Many websites can be hosted on the same Web server using software like Apache2 which is an open-source platform for hosting web contents. The websites themselves are written using server-side scripting languages like PHP5 combined with HTML and Javascript and data are stored within the server's permanent storage using language like SQL (Structure Query Language); Finally, datacenters include many other services like multimedia streaming, voice managers, Cloud for private use, workflow, human and financial systems and other useful related services.

3. NETWORK SERVICE VIRTUALIZATION USING OPEN-SOURCE

In the previous sections, network services are explained with highlights on their practical implementation. All of these services can be virtualized using one or more physical server entity characterized by high dynamic RAM as it has been explained in section 1. Therefore, this work considers an HP ProLiant DL380 G8 Server with 32GB DDR3 Registered Dual in-line Memory Module (DIMM) and Intel(R) Xeon(R) CPU E5620 @ 2.40GHz, 16 cores. This physical server runs UBUNTU 14.04.3 Linux operating system and virtualized using VirtualBox hypervisor and controlled by the front end web interface called PHPVirtualBox and divided into VMs hosting the network services shown in table 2. The network interface card of the server is configured in bridged mode to assign different IP addresses to each VM. The detailed network diagram is shown in figure 4 where multiple sites cooperates to maintain DNS's databases as previously explained.

In the network shown in figure 4, the master DNS located in the college of Information Engineering / Al-Nahrain University is synchronized with its slave DNS installed in the department of Research and development at the Ministry of Higher Education and Scientific Research. Both of these servers run NSD (Name Server Daemon) software and encrypt their synchronous updates with private key. Whenever a request reaches the Master DNS (identified by its parent DNS), the master DNS responds back with query answer unless it is unreachable and consequently the slave DNS responds back on behalf. Figure 4 shows also the reverse DNS location in the network of SatGate ISP for proper email server ownership. The whole network is operational without problems and it is completely built using open-source software as indicated in Table 2. Maintaining virtualized services running requires periodic monitoring and backup and these are also managed using available open-source software like Nagios [13] and Amanda [14].

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

TABLE 2: List of virtualized network services using open-source software

Service Name	Software	VM
Master DNS	NSD [15]	512 Mbyte of RAM, Single CPU, 4GByte dynamic storage
Mail Server	Postfix [16], Dovecot IMAP/POP3 [17], MySQL Database [18], SpamAssassin Mail Filter [19], amavis [20], Roundcube [21], Apache 2 [22], PHP5 [23]	2000 Mbyte of RAM, Single CPU, 100 GByte dynamic storage
Web Server	Apache 2, PHP5, MySQL Database	(10 VMs) Depends on Application
E-Learning Server	Moodle [24], Apache 2, PHP5, MySQL	2000 Mbyte of RAM, Single CPU, 100 GByte dynamic storage
Workflow	Apache 2, PHP5, MySQL	4000 Mbyte of RAM, Single CPU, 100 GByte dynamic storage
File Sharing and Data Storage	ownCloud [25]	4000 Mbyte of RAM, Single CPU, 500 GByte dynamic storage
Other services	-	Depends on Application

4. CONCLUSIONS

In this paper, practical perspectives in network service virtualization are highlighted. Different types of services like DNS, Web, and Mail are explained and critical issues running them are pointed out. The work is implemented using open-source software features no cost (low cost when support is needed), reliability and high availability. It has been shown that physical servers can be divided into multiple VMs using hypervisors software like VirtualBox to exploits its resources, and each VM is considered as a dedicated server with assigned amount of memory that is considered the key to virtualization. Therefore, the amount of memory decides how many running VMs a hypervisors can produce as it has been shown by the approximate equations in section 1. The work shows practical implementation of multiple site-to-site cooperation to achieve the required ownership, authentication and verification for domain and mail services. Finally, the use of virtualization easily expands network services as the process involves adding virtually and not physically.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

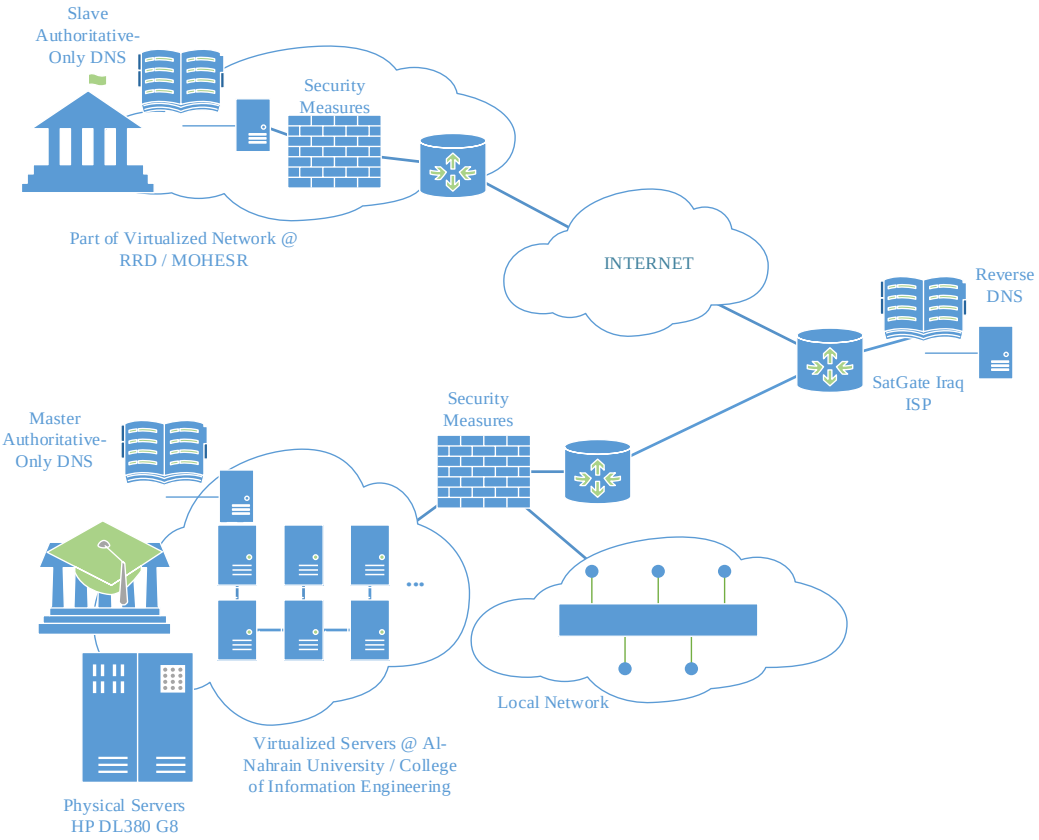

FIGURE 4. Network diagram showing virtualized services distributed over multiple sites

5. REFERENCES

[1] M. Rahman, and A. Esmailpour, "A Hybrid Network Architecture for Data Centers," *in IEEE First International Conference on Big Data Computing Service and Applications (BigDataService)*, 2015, pp. 7-13.

[2] G. Schulz, *The Green and Virtual Data Center*, Boston MA, USA:Auerbach Publications, 2009.

[3] M. Ammar, M. Rizk, A. Abdel-Hamid, and A. Aboul-Seoud, "A Framework for Security Enhancement in SDN-Based Datacenters," *in 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2016, pp. 1-4.

[4] N. Jain, and S. Choudhary, "Overview of virtualization in cloud computing," *in Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016, pp. 1-4.

[5] A. Kivity, Y. Kamay, D. Laor, U. Lublin, and A. Liguori, "kvm: The linux virtual machine monitor", Proc. Linux Symp., vol. 1, 2007, pp. 225-230,

[6] Kernel-Based Virtual Machine (KVM), https://www.linux-kvm.org, (Accessed: 17th March 2017).

[7] Oracle VM VirtualBox, https://www.virtualbox.org, (Accessed: 17th March 2017).

[8] The Xen Project (Xen), https://www.xenproject.org, (Accessed: 17th March 2017).

[9] Virtual Machine Software (VMWare), http://www.vmware.com, (Accessed: 17th March 2017).

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

[10] RFC1034,1035 - Domain Names - Implementation and Specification – IETF, https://www.ietf.org/rfc/rfc1034.txt (rfc1035), (Accessed: 17th March 2017).
[11] RFC 5321 - Simple Mail Transfer Protocol - IETF Tools, https://www.ietf.org/rfc/rfc5321.txt, (Accessed: 17th March 2017).
[12] The Spamhaus Project, https://www.spamhaus.org, (Accessed: 17th March 2017).
[13] Network Monitoring, Nagios, https://sourceforge.net/projects/nagios/, (Accessed: 17th March 2017).
[14] Amanda: Open Source Backup, http://amanda.zmanda.com, (Accessed: 17th March 2017).
[15] Name Server Daemon (NSD), https://www.nlnetlabs.nl/projects/nsd/, (Accessed: 17th March 2017).
[16] Mail server, Postfix, http://www.postfix.org, (Accessed: 17th March 2017).
[17] Secure POP3 and IMAP server for Linux, Dovecot, https://www.dovecot.org, (Accessed: 17th March 2017).
[18] Open source database, MySQL, https://www.mysql.com, (Accessed: 17th March 2017).
[19] Apache SpamAssassin Project, http://spamassassin.apache.org, (Accessed: 17th March 2017).
[20] Amavis Virus Scanner and Checker, https://www.ijs.si/software/amavisd/, (Accessed: 17th March 2017).
[21] IMAP client, Roundcube, https://roundcube.net, (Accessed: 17th March 2017).
[22] The Apache HTTP Server Project, https://httpd.apache.org, (Accessed: 17th March 2017).
[23] PHP scripting language, http://php.net, (Accessed: 17th March 2017).
[24] Moodle, https://moodle.org, (Accessed: 17th March 2017).
[25] OwnCloud, https://owncloud.org, (Accessed: 17th March 2017).