THE VIRTUALIZATION OF AN INTERNET SERVER

Cătălin MATEIAŞ[1], Adrian NICOLESCU[2]

For security reasons, the software used for building an Internet Server is not installed on a single computer, instead it is usually scattered on three or more computers. This paper presents how three computers have been replaced with virtual machines installed on a single server and how the data is transferred among the virtual machines and the hardware network, and the advantages and drawbacks of virtual machines versus hardware machines.

Keywords: virtualization, internet web server, database, communications

1. Introduction

The authors of the paper are working on developing a software platform using open source software, which will record data from sensors installed in locations that require constant monitoring, and make the data accessible to users using the Internet.

Locations that require constant monitoring are greenhouses, food warehouses, pharmacy storages, metrological laboratories, server rooms or any other locations that require constant monitoring [1].

The software application will store data like temperature, humidity, pressure, light intensity, air flow or any other measurable digtized elements [2].

The data will be available to users using web pages showing data in reports and graphs. Each user will be allowed to see only data from the sensors installed in the locations that he owns. For example in figure 1 the user (5) will see only data from the greenhouses (1) and (2) while the user (6) will see only data from the greenhouse (3).

This research was started as a substage for the development of a fully automatic system for a mushroom cultivation greenhouse, because commercial

[1] PhD student., University POLITEHNICA of Bucharest, Romania, e-mail: cata.mateias@gmail.com

[2] Prof., University POLITEHNICA of Bucharest, Romania

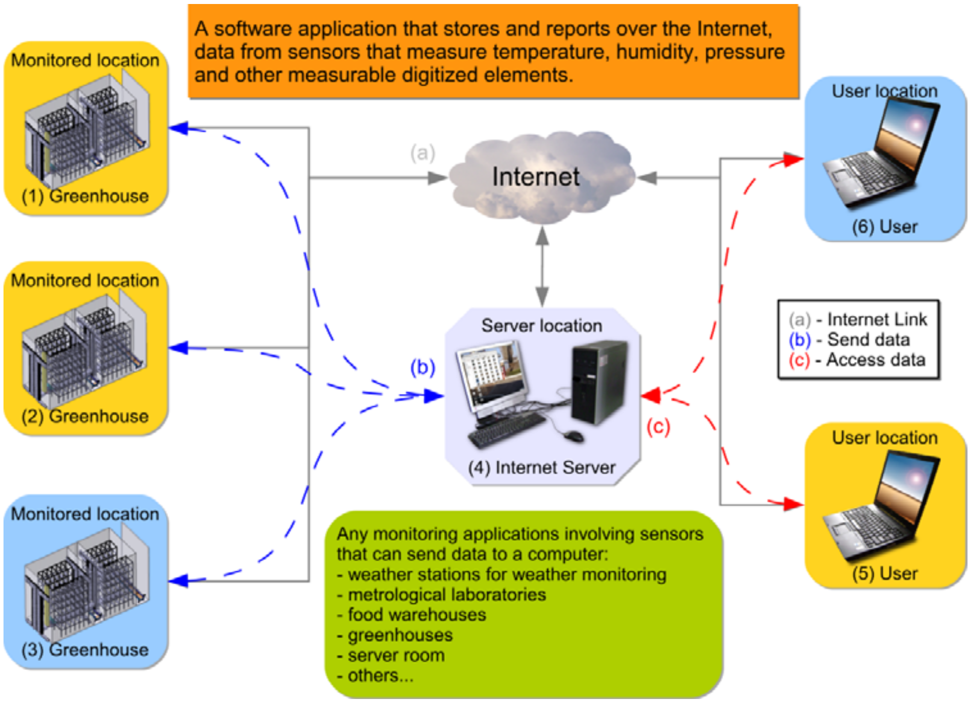
A software application that stores and reports over the Internet, data from sensors that measure temperature, humidity, pressure and other measurable digitized elements.
Monitored location
(1) Greenhouse
Monitored location
(2) Greenhouse
Monitored location
(3) Greenhouse
(a)
Internet
User location
(6) User
Server location
(4) Internet Server
(b)
(c)
(a) - Internet Link
(b) - Send data
(c) - Access data
User location
(5) User
Any monitoring applications involving sensors that can send data to a computer:
- weather stations for weather monitoring
- metrological laboratories
- food warehouses
- greenhouses
- server room
- others...

Fig. 1. Research description.

Table 1

Open source and freeware software used for development

Oracle	Database 11g XE
	Web Developing Application APEX
	Java Developer
Linux	Operating System Fedora Core and CentOS
	Firewall Shorewall
	DNS Bind
	Mail Server Postfix+Dovecot
	Web Server Apache HTTP
	Proxy Squid+SARG
	SNMP Communication Protocol
	Backup using Bacula

solutions of software for monitoring environmental parameters are too expensive or do not allow customization for graphs and reports to the mushroom cultivation greenhouse specifications [3][4].

In present, the software platform is recording the temperature, humidity, atmospheric pressure and dew point from one sensor once per minute every day. The application started recording from October the 2nd 2011. The data is stored in an Oracle XE database. The graphs and reports were designed using Oracle APEX and can display the measured values of temperature, humidity, atmospheric pressure and dew point in real time, or the average, maximum and minimum of temperature, humidity, pressure and dew point per minute, hour, day, month or year. To access data from the Internet the user must provide security credentials.

This paper will show the advantages and drawbacks between the current hardware infrastructure where the software platform is installed and the virtualization infrastructure planned for the software platform. The current hardware infrastructure of the Internet Server is presented in the 2nd section, “The hardware infrastructure”, while the 3rd section, “The virtualization infrastructure”, presents a virtual model designed using virtual machines, similar to the hardware infrastructure from section 2. Solutions for backup and restore of data for the virtual infrastructure are presented in section 4, “Backup”.

2. The hardware infrastructure

The hardware infrastructure of the software platform seen in figure 2 consists of three computers: the Firewall Server (4), a Domain Name Server (DMZ) (6) and the Database Server (10).

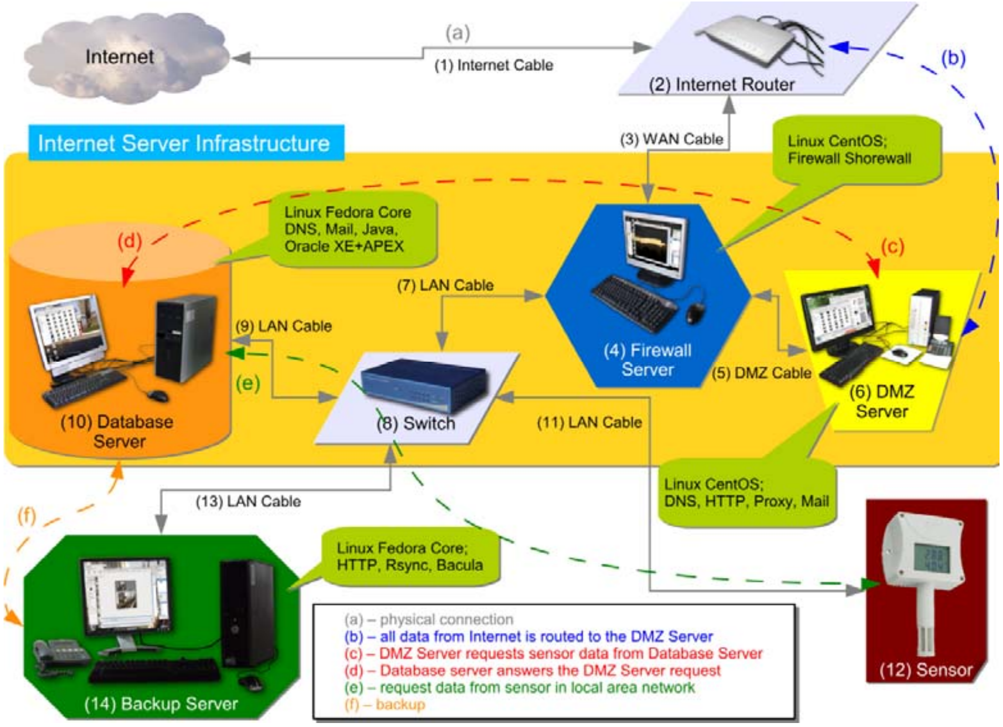

Fig. 2. The hardware infrastructure.

When a user from the Internet wants to see the sensor data, his request will reach the Internet router (2) which will forward the request to the Firewall Server (4). The Firewall Server (4) has three Ethernet network adapters: the 1st is for the connection to the Internet using WAN cable (3), the 2nd is for the connection to the Domain Name Server (DMZ) (6) using the DMZ cross cable (5), and the 3rd is for the connection to the local area network using the LAN cable (7). The Firewall Server (4) will forward the user request to the Domain Name Server (6) using the DMZ cable (5). The Domain Name Server (DMZ) (6) is the server that answers on the Internet when a user types the domain name in the Internet browser address bar. The HTTP web server is installed on the Domain Name Server (6), but the web pages and the sensor data are stored on the Database Server (10) inside the Oracle XE database. The HTTP web server connects to the Oracle XE database installed on the Database Server (10) using the DMZ cable (5) the Firewall Server (4) the LAN cable (7), the switch (8) and the LAN cable (9). The HTTP web server invokes procedures and generates the web pages with data in reports and graphs. Then the HTTP server will make the web pages available to the user from the Internet [5][6]. The sensor (12) with an Ethernet adapter is connected to the local area network using the LAN cable (11) to the switch (8). Important data from the Database Server (10), Domain Name Server (6) and Firewall Server (4) is stored on the Backup Server (14).

3. The virtualization infrastructure

The virtualization infrastructure in figure 3 consists of three virtual machines installed on a single hardware server. The hardware server has two ethernet network adapters : the 1st is for connetion to the Internet and the 2nd is for the connection to local area network. The hardware server, where the virtual machines are installed, is called HOST and the virtual machine is called GUEST. The virtual machines are connected to the hardware network using bridge networks. The virtual machines are connected among each other using internal networks.

A bridge network allows a virtual machine to connect to the hardware network using a hardware ethernet adapter found on the hardware server. The MAC address and IP address of the virtual machine bridge ethernet network adapter are different from the hardware server ethernet adapter, but the virtual machine IP address must be in the same IP address class as the hardware server ethernet adapter. For example to facilitate data transfer between the host and the guest, the host hardware ethernet has 193.168.1.33 and the guest virtual machine ethernet has 193.168.1.188.

An internal network is a virtual network where Oracle VirtualBox will act as a network switch among the virtual machines connected to the internal network. For example, three virtual machines with the IP addresses 10.10.10.1, 10.10.10.2 and 10.10.10.3 and with a netmask 255.255.255.0 will be able to transfer data among each other.

Bridge network and internal network are names of network types from Oracle VirtualBox.

On the Hardware Server (3) there are installed the operating system (4) (CentOS Linux), and a firewall (6) (Shorewall) that can also be used for routing (5) and for virtualization(11) Oracle VirtualBox is used.

In figure 3 there are installed three virtual machines : the Firewall Server Virtual Machine (12), the Name Server Virtual Machine (21) and the Database Server Virtual Machine (25).

The Firewall Server Virtual Machine (12) has three virtual ethernet network adapters : the 1st is for the connection to the Internet, WAN virtual ethernet (10) using Bridge network (9) to WAN hardware ethernet (2); the 2nd is for the connection to the local area network, LAN virtual ethernet (16) using

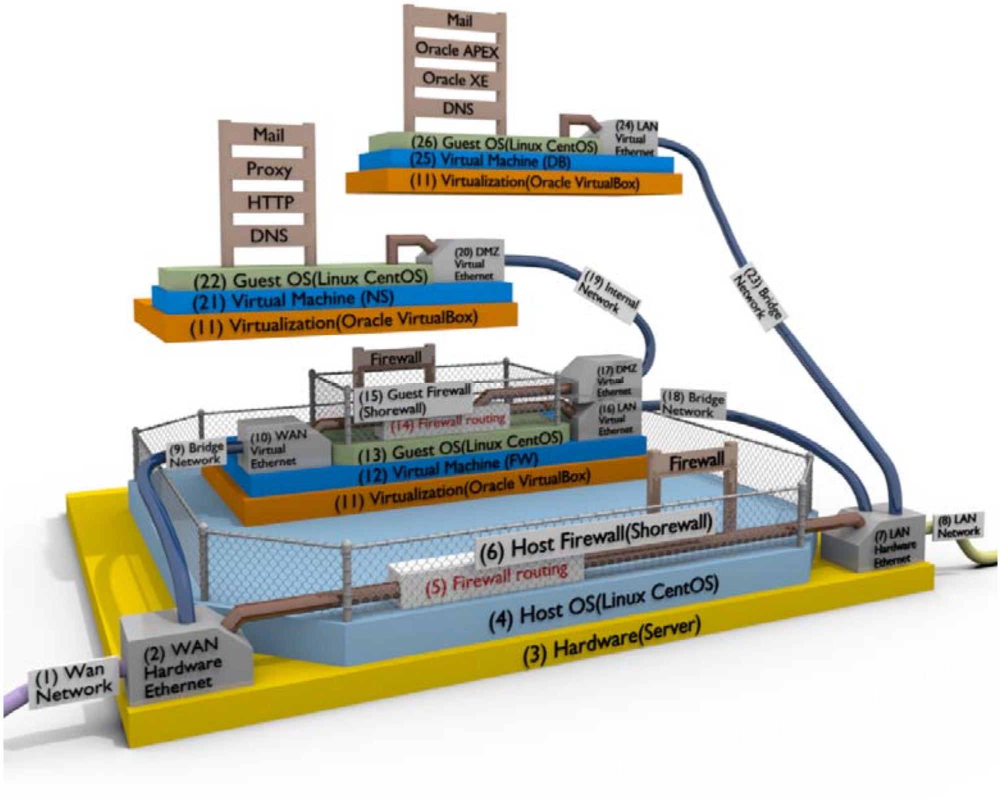
Mail
Oracle APEX
Oracle XE
DNS
(24) LAN Virtual Ethernet
(26) Guest OS(Linux CentOS)
(25) Virtual Machine (DB)
(11) Virtualization(Oracle VirtualBox)
Mail
Proxy
HTTP
DNS
(20) DMZ Virtual Ethernet
(22) Guest OS(Linux CentOS)
(21) Virtual Machine (NS)
(11) Virtualization(Oracle VirtualBox)
(19) Internal Network
(23) Bridge Network
Firewall
(17) DMZ Virtual Ethernet
(15) Guest Firewall (Shorewall)
(16) LAN Virtual Ethernet
(18) Bridge Network
(14) Firewall routing
(9) Bridge Network
(10) WAN Virtual Ethernet
(13) Guest OS(Linux CentOS)
(12) Virtual Machine (FW)
(11) Virtualization(Oracle VirtualBox)
Firewall
(6) Host Firewall(Shorewall)
(5) Firewall routing
(4) Host OS(Linux CentOS)
(3) Hardware(Server)
(7) LAN Hardware Ethernet
(8) LAN Network
(2) WAN Hardware Ethernet
(1) Wan Network

Fig. 3. The virtualization infrastructure.

Bridge network (18) to LAN hardware ethernet (7); the 3rd is for connection to the Name Server Virtual Machine (21), DMZ virtual ethernet (17) using Internal network (19) to DMZ virtual ethernet (20). The Firewall Server Virtual Machine (12) with the firewall(15) are needed because the Bridge networks (9) and (18) bypass the firewall (6) installed on the Hardware Server (3).

On the Name Server Virtual Machine (21) there are installed the operating system (22) (CentOS Linux), the DNS server, the HTTP server, a proxy server using squid, and the mail server. The Name Server Virtual Machine (21) can connect to the Internet through the DMZ virtual ethernet (20) using the Internal network (19) to DMZ virtual ethernet (17) of the Firewall Server Virtual Machine (12). The Firewall (Shorewall) (15) is routing (14) Internet from WAN virtual ethernet (10) to the DMZ virtual ethernet (17) and forwarding the HTTP, DNS, and Mail ports from the DMZ virtual ethernet (20) to the WAN virtual ethernet (10). The hardware server (3) is connected to the Internet using an Internet router (2) seen in figure 2. The Internet router(2) from figure 2 forwards the HTTP, DNS and Mail ports from WAN virtual ethernet (10) using Bridge network (9) via WAN hardware ethernet (2), WAN network cable (1). Note that the Internet router (2) from figure 2, the Hardware Server (3) and the Firewall Server Virtual Machine (12) have the same IP address class. The WAN network (1) of the Hardware Server (3) is a LAN network for the Internet router and the WAN network of the Internet router is the ISP Internet cable with the ISP static IP address.

On the Database Server Virtual Machine (25) there are installed the operating system (26) (CentOS Linux), the DNS server, Oracle XE database with Oracle APEX and the Mail Server. The Database Server Virtual Machine (25) is connected to the local area network through LAN virtual ethernet (24) using Bridge network (23) to LAN hardware ethernet (7).

When the Web server is accessed from the Internet, the Internet router will forward the request to the Firewall Server Virtual Machine (12) via WAN network (1), WAN hardware ethernet (2), Bridge network (9), WAN virtual ethernet (10). Then the Firewall (15) is forwarding the request to the Name Server Virtual Machine (21) via DMZ virtual ethernet (17), Internal network (19), DMZ virtual ethernet (20). The HTTP server connects to the Oracle XE database installed on the Database Server Virtual Machine (25) using DMZ virtual ethernet (20), Internal network (19), DMZ virtual ethernet (17) via Firewall (15), LAN virtual ethernet (16), Bridge network (18), LAN hardware ethernet (7), Bridge network (23), LAN virtual ethernet (24). The HTTP web server invokes procedures and generates the web pages with data in reports and graphs. Then the HTTP server will make the web pages available to the user from Internet.

The virtualization was done on a server with an Intel Xeon Quad Core CPU (4 cores with 2 threads per core), with 8 GB of RAM and three 500 GB hard disks, without any RAID configuration. On the 1st hard disk, was installed the Operating System (Host OS (4)) of the Hardware server (3), the firewall (Shorewall) (6) and Oracle VirtualBox (11). The files of the Firewall Server Virtual Machine (12) and the Name Server Virtual Machine (21) are stored on the 2nd hard disk.

The Database Server Virtual Machine (25) files are stored on the 3rd hard disk. The hard disks RAID setup was discarded because the virtual machines had poor performance when reading and writing data to disk. When using RAID 5 configurarion, the three hard disks act as one hard disk for the Operating System (4). The data transfer speed can be seen in table 2.

The Firewall Server Virtual Machine (12) and the Name Server Virtual Machine (21) load from the same physical hard disk because, after the operating systems of the two virtual machines have loaded, the Firewall Server Virtual Machine (12) does not read / write too much data to the hard disk unlike the Name Server Virtual Machine (21) and the Database Server Virtual Machine (25).

Tabelul 2

Data transfer speed among the virtual machines

Data transfer speed test	RAID 5 setup	No RAID setup
Copy data from one folder to another using the hardware server Operating System	50 to 130 MB/s	50 to 130 MB/s
Copy data from one folder to another on the same virtual machine	10 to 14 MB/s	21 to 32 MB/s
Copy data using SSH/SCP protocol from one virtual machine to another virtual machine using bridge or internal network	10 to 14 MB/s	21 to 24 MB/s

4. Backup

For the host server Operating System, only folder “/etc” is needed for data recovery, because all the necessary configuration files for the network and firewall are in “/etc”. This backup is necessary when the 1st hard disk of the server fails.

The files of virtual machines from the 2nd and 3rd hard disks are copied to an external hard disk. In case the 2nd or 3rd hard disk fails, the virtual machines files will be copied from the external hard disk to one of the other working hard disks and the virtual machines will be back on-line. For the Database Server Virtual Machine (25) it is also necessary to make a daily export of the Oracle XE database, because the data from the Oracle XE database inside the files of the Database Server Virtual Machine (25) from the external hard disk will be outdated.

5. Conclusions

In this paper, was presented how an Internet Server composed of three hardware computers has been re-built using virtual machines, each virtual machine replacing one of the hardware computers.

The main advantage of using virtual machines is that in case of failure (bad update of the Operating System of the virtual machine or any type of failure to the software running inside the virtual machine) the virtual machine can be put back on-line faster than a hardware machine that in most cases requires a full reinstall of the software running on the hardware machine.

A disadvantage is that if the hardware of the virtualization server fails (CPU or mother board failure) none of the virtual machines can be used any more, unless the virtual machines are started on another hardware server. If not using virtualization and instead using three hardware servers, and the Domain Name Server fails, the Firewall Server and the Database Server will remain on-line. The Internet Server will become inaccessible from the Internet, but the applications installed on the Database Server will remain accessible from the local area network to people working inside the company.

REFERENCES

[1] *Y.M. Hsieh, Y.C. Hung*, "A scalable IT infrastructure for automated monitoring systems based on the distributed computing technique using simple object access protocol Web-services", in Automation in Construction, 2008, pp. 424-433, Elsevier

[2] *R. Carniel, M.Cecca, O. Jaquet,* "A user-friendly, dynamic web environment for remote data browsing and analysis of multiparametric geophysical data within the MULTIMO project", in Journal of Volcanology and Geothermal Research, no. 153, 2006, pp. 80-96, Elsevier B.V.

[3] *C. Mateias, A. Nicolescu,* "Data Reporting on Internet from Sensors that Measure Environmental Parameters", in Annals of DAAAM for 2012 & Proceedings of the 23nd International DAAAM Symposium, Vienna, Austria, 2012, pp. 0075-0080, DAAAM International

[4] *C. Mateias, A. Nicolescu,* "Software Platform for reporting, on the Internet, data stored from Sensors used to Monitor Production Processes", in Proceedings of the World Congress on Engineering, 4-6 July, London, U.K., 2012, vol. 1, pp. 545-550, IAENG

[5] *T. Kimura, Y. Kanda*, "Development of a remote monitoring system for a manufacturing support system for small and medium-sized enterprises", in Computers in Industry, no. 56, 2005, pp. 3-12, Elsevier B.V.

[6] *C. Mateias, A. Nicolescu*, "Software Application for Storing and Reporting Data, over the Internet from sensors that Measure Environmental Parameters", in Proceedings of the 14th IFAC Symposium on Information Control Problems in Manufacturing, May 23-25, Bucharest, Romania, 2012, pp. 1814-1821, Elsevier B.V.