

Technical Case Study:
Patch Management

This is subsequent to Summary of Projects –

VMware - ESX Server to Facilitate:
IMS, Server Consolidation, Storage & Testing with Production Server



VAssure | Virtualization Labs | trRIMS | Offshore-QA | BI | Portals

<http://www.vassure.com>

PROJECT OVERVIEW

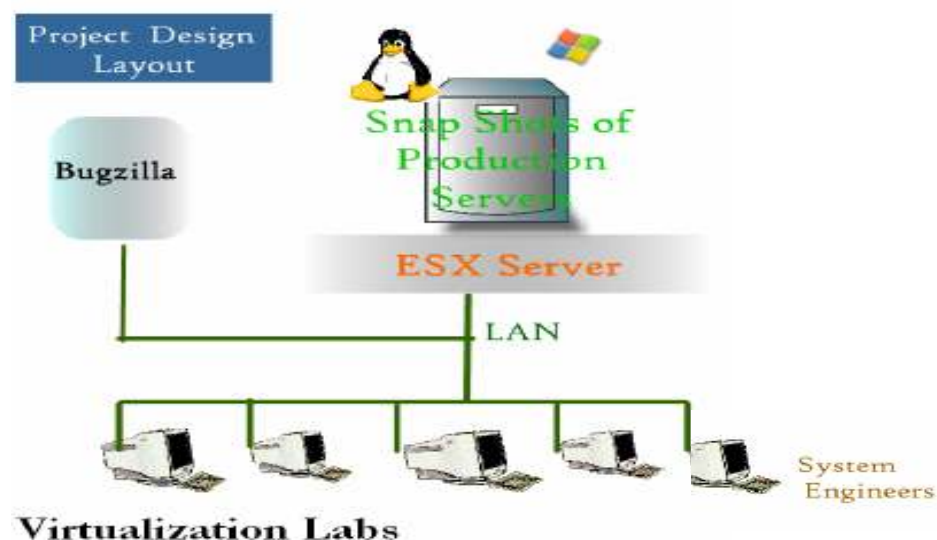
The Infrastructure Management Services project is made up of a set of hardware components, SAN and ESX server. Work together to provide IMS services and a system to storage applications. The project also involves testing of the storage application. The production server is built upon VMware ESX server running multiple operating systems. The main advantage of using the ESX server is for the server consolidation. The production server is connected to a SAN for storage management. If any problem occurs in the production server at the OS level, recovery server is used by client; a snapshot of the production server is taken and at virtual machine's lab it tested and modifications are to be done at the operating system level of the production's server. Client's applications are also tested at lab and if any bugs are found, the bugs are reported using Bugzilla. Applying required patches to the guest Linux kernel after successfully debugging and testing them in lab to improve the performance of the production server.



Patch Management:

During course of running, if any problem arises at production server or in a testing scenario the snapshot of the server is taken and snapshot is brought into the VAssure-Virtualization Labs (Systems from where System Engineers operate) making a clone of it. To rectify the problems, the required patches are developed in the lab. During the Patch Management, the bugs generated in client's applications will be rectified and the patches will be developed. The developed patches will be debugged and tested repeatedly. These patches will be deployed on the ESX server. After checking the functionality of these patches on the ESX server, the patches will be deployed on the production server.

To increase the performance of the Guest operating systems of the ESX server and to provide more features to the client the patches will be developed in the VM lab. The developed new patches will be debugged and the bugs will be cleared in the lab. After rectifying the bugs, the patches will be tested on the ESX server which is present in the VM lab. The patch which gives extra functionality to the kernel will be deployed on the production server.



This Document Addresses the Following Topics:

1. What is Patch Management?
2. Life cycle of Patch Management.
3. Types of Patch Management.
4. Benefits of Patch Management.
5. Implementation of Patch Management in IMS.

What is Patch Management?

Patch management is a process by which systems in network are secured by applying critical patches and updates, and kept free from vulnerabilities that exist in the Guest OS and software applications. Accurately identifying system vulnerabilities, detecting missing patches, testing them and then deploying patches to eradicate the vulnerabilities is the key to effective patch management. Here the Guest operating systems and software applications are on ESX server. It is imperative that every organization follows patching procedures and keeps systems up to date with the latest patches.

Life cycle of Patch Management:

The Patch Management Life Cycle consists of

1. Reach
2. Resolve
3. Research
4. Repair
5. Report

Any patch management process adopted in an enterprise will have to go through these 5 stages of the life cycle.

1. Reach: Discover and identify the servers and workstations in the network.
2. Resolve: Assess what vulnerabilities in the systems. Analyze what patches are missing and what are installed.
3. Research: Be up-to-date with the latest patch related information from various vendors and other websites. Develop or download patches and run extensive tests to validate the authenticity and accuracy of patches.
4. Repair: Schedule patches download and deployment of missing patches. Control deployment with flexible options like machine reboot. Verify and validate the accuracy and patch installation.
5. Report: View status reports of the different patch management tasks. Monitor patching progress in the enterprise.

Types of Patch Management:

The clients are working on the production server by remote login to the server. The Guest operating systems installed on the ESX server are Linux and Windows. Types of Patch Managements are.

1. Linux Patch Management:

The recently released Linux patches and depending on the client requirement newly developed patches are to be attached to the kernel to fulfill the client requirement and to increase the performance of the operating system.

2. Windows Patch Management:

Patch management for Microsoft Windows operating systems and other Microsoft software applications. This Patch Management is to discover and scan for missing Microsoft patches, analyzes the vulnerabilities, downloads and deploys patches and secures the Windows infrastructure in network.

Benefits of Patch Management:

Incorporating patch management in enterprise is very important. Here are some of the benefits:

1. Ensure that the most appropriate software available is installed.
2. Seal security loopholes in systems that can be exploited by malicious hackers.
3. Reduce system downtime.
4. Limit attacks that target known software vulnerabilities.
5. Be the last line of defense and secure networks from security threats.

Implementation of Patch Management in Infrastructure Management Services:

To provide the Infrastructure Management Services using latest technologies and procedures to the clients patch management implementation is necessary. To deploy the patches on production server, the snapshot of the production server is taken and a clone of it is made. The cloned Virtual Machine is brought to VM lab. The client's applications are tested using the debugging tools and testing tools like KGB, LCOV and GCOV for Linux and Winrunner, silk test and Load runner for Windows. The test reports are generated using the Testdirector and Bugzilla.

For Linux:

Create a Patch file for the newly developed patches in VM lab and the upgraded patches. For example,

```
diff -Naur | -u olddir newdir > new-patch  
- or -  
diff -Naur | -u oldfile newfile > new-patch
```

Make sure while creating a patch file same number of directories levels for both olddir path and newdir path.

Using the patch command:

Depending on the current working, use the following 'patch' command

```
patch -p0 <new-patch
```

```
patch -p1 <new-patch
```

Other method for calling the patch command using the standard input of patch:

```
cat new-patch | patch -p0
```

Levels in the Patch Command (-p0 or -p1?):

The -p option will optionally strip off directory levels from the patchfile.

For Ex: if you have a patchfile with a header as such:

```
--- old/modules/file
```

```
+++ new/modules/file
```

Using a -p0 will expect, from your current working directory, to find a subdirectory called "new", then "modules" below that, then the "file" file below that.

Using a -p1 will strip off the 1st level from the path and will expect to find (from the current working directory) a directory called "modules", then a file called "file". Patch will ignore the "new" directory mentioned in the header of the patchfile.

Using a -p2 will strip of the first two levels from the path. Patch will expect to find "file" in the current working directory. Patch will ignore the "new" and "modules" directories mentioned in the header of the patchfile.

In the code, line with neither a plus or minus would indicate that this particular line of code is just a reference point. The + would indicate that this particular line is to be added. The - would indicate that this particular line is to be removed.

For Windows:

The required and upgraded service packages for the guest operating system windows should be downloaded and installed in the VM lab.

The created and down loaded patch should be debugged and tested on the ESX server which is present in the VM lab. After checking the functionality and performance of the patch, it should be deployed on the production server. The selected up gradation patches are downloaded from the internet and stored in a particular location in the server. Then they are pushed to the production server virtual machines remotely using clone of the snapshot.

Compiled by: Gopinath.K – gopinath.k@vassure.com

This paper is not intended to be a definitive implementation guide. Many factors are not addressed in this document. Expertise may be required to solve logistical problems when the system is designed and built. VAssure team has not tested this procedure with all the combinations of hardware and software options available on all VMware products or guest OS variants. There may be significant differences in your configuration that will alter the procedures necessary to accomplish the objectives outlined in this paper.