A RESEARCH PAPER ON TIVOLI ENDPOINT MANAGER

Prateek Rana[1], Anurag Chauhan[2], Tarang Bhalotia[3], Mrs. Indu[4]
[1,2]B.tech Student Department of Computer Engineering,MVSIT Sonipat
[3]Asst. Professor Department of Computer Engineering,MVSIT Sonipat
Mahavir Swami Institute Of Technology, Sonipat Haryana-131030

Abstract: Data is any type of stored digital information. Security is about the protection of assets. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, personal databases and websites. This RLO is ment for System Administrator(SA) audience. The RLO is ment to teach SA the basics of TEM, understand the architecture at a high level, and demostrate to them how to run Patch Management and Security/Compliance management to their servers. TEM will allow SA to centrally administer their servers, and provide a standard, consistent method of doing their tasks. In doing this we hope to reduce the SA workload, and increase effeciency and reliability in our services to our customers.

Example: Joe from the office is a Windows Administrators, and has 20 Servers he needs to manage for company ABC. Joe's duties include making sure the servers are at latest patches, which means he has goto Microsoft site for each flavour of Windows he has (Windows 2003, Windows 2000, Windows 2008 etc) and the applications that run on them like SQL, Exchange etc.. and download the latest patches. Then Joe needs to transfer the files each machine manually and install the patches and do checks. With TEM, Joe just needs to log into TEM console, the patches are automatically available for Joe for each his systems and applications. Joe just needs to select whcih machines needs to be patched and execute.

Another duty Joe has is Security/Compliance. Joe has ensure that each server meets certain criteria for security compliance like password complexity, password expiry, log file management, OS security settings etc.. Joe has to revalidate and set these setting on all his servers on a regular basis. To be compliant means the revalidation on a continous basis. With TEM, Joe can select his compliancy rules and send the fixlet(TEM small code runs on the TEM Agent) to all his machines he wants, and the fixlets will run continously and if broke will report and fix the problem automatically.

I. INTRODUCTION

IBM BigFix formerly IBM Endpoint Manager, Tivoli Endpoint Manager (TEM) and before that, BigFix, is a systems-management software product developed by IBM for managing large groups of computers running Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOSand Android.[1] IBM BigFix provides system administrators with remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory functionality.

TEM(Tivoli Endpoint Manager) earlier known as BigFix Enterprise Suite integrates the assets acquired with BigFix into the IBM portfolio.

TEM combines endpoint and security management into a single solution.

TEM Server Software Requirements

Operating Systems

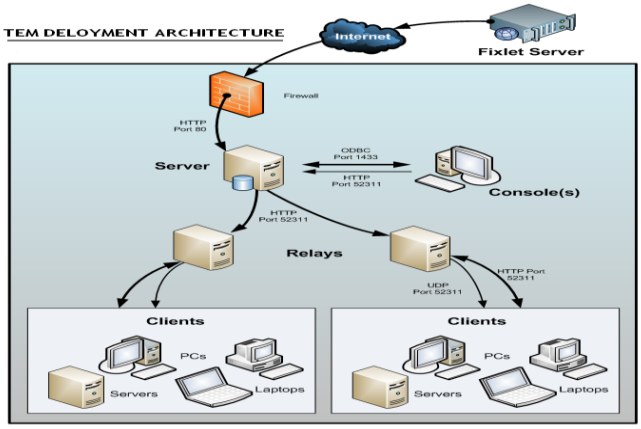
- Windows 2008 (x86, x64) Enterprise - Tivoli Endpoint Manager (BigFix) 7.1 or later
- Windows 2003 (x86, x64) Enterprise - Tivoli Endpoint Manager (BigFix) 6.0 or later

Databases

- SQL Server 2008 R2 (x86, x64) Enterprise - Tivoli Endpoint Manager (BigFix) 8.0 or later
- SQL Server 2008 (x86, x64) Enterprise - Tivoli Endpoint Manager (BigFix) 7.2 or later
- SQL Server 2005 (x86, x64) Enterprise - Tivoli Endpoint Manager (BigFix) 6.0 or later

TEM Server Hardware Requirements

- CPU : 2-3 GHz - 4 Cores
- Disk Space :200 - 250 GB
- Memory :32 GB
- Hard Disks: Three Physical Array (Recommended) or three LUN from SAN



Components of TEM

1. Tivoli Endpoint Manager Clients
2. Tivoli Endpoint Manager Server
3. Tivoli Endpoint Manager Relays
4. Tivoli Endpoint Manager Console
5. Web Reports

 Copyright 2019.All rights reserved.

1. Tivoli Endpoint Manager Clients
   - To be installed on every computer which is to be managed
   - Accesses a collection of Fixlet messages that seek out security problems, vulnerabilities and deviations from the desired operating environment.
2. Tivoli Endpoint Manager Server
   - Collections of interacting server applications that form the heart of TEM system.
   - Coordinates with the flow of information to and from individual clients and store the results in database
3. Tivoli Endpoint Manager Relays

Increases the efficiency of the system. Instead of requiring every networked computer to directly access the TEM server, relays can be used to offload much of the burden.

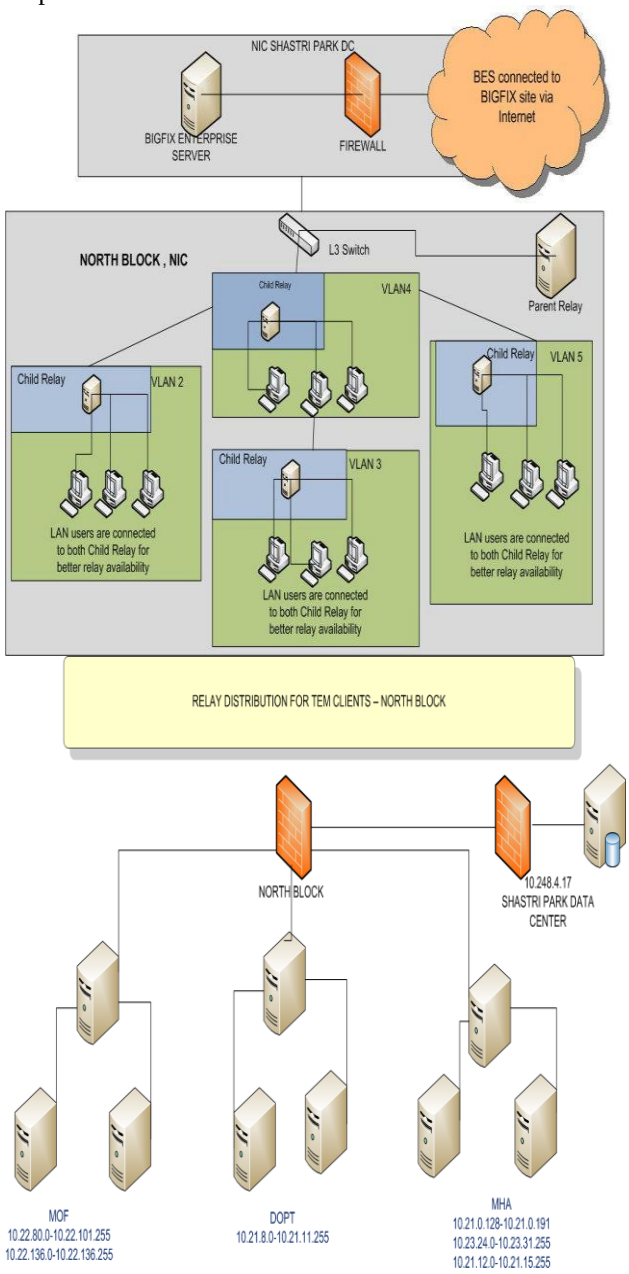
Relay Server requirements

Hardware Requirements
- Minimum CPU: Pentium 2, 400 Mhz
- Minimum RAM: 128 MB
- Minimum Free HD Space: 2 GB
- Internet Explorer 4.01 or higher is required for proxy authentication

Software Requirements
- Windows NT SP6a/2000/XP/2003 (x86/x64) -- BigFix 4.1+
- Windows Vista (x86/x64) -- BigFix 7.0+
- Windows Server 2008 (x86/x64) -- BigFix 7.0.9+
- Windows Server 2008 Core (x86/x64) -- BigFix 7.2.1.357+
- Windows Server 2008 R2 -- BigFix 8.0+
- Windows Server 2008 R2 Core -- BigFix 8.0+
- Windows 7 (x86/x64) -- BigFix 8.0+
- Windows 2003 (x86/x64) - BigFix 6.0+
- Windows 2003 R2 (x86/x64) - BigFix 6.0+
- Solaris 10 (x86/SPARC) -- BigFix 8.0+
- RHEL 4 (x86/x64) -- BigFix 8.0+
- RHEL 5 (x86/x64) -- BigFix 8.0+
- RHEL 6 (x86/x64) -- BigFix 8.2+
- SUSE 11 (x86/x64) -- BigFix 8.2+
- AIX 5.3 -- BigFix 8.2+
- AIX 6.1 -- BigFix 8.1+
- AIX 7.1 -- BigFix 8.2+

4. Tivoli Endpoint Manager Console
   - Ties TEM Client, Server and Console together to provide a system wide view of networked computers along with their vulnerabilities and suggested remedies.
5. Web Reports
   - Enables the Administrators to produce charts and graphs of the data.
   - Allows to get an overview of relevant Fixlet messages and any subsequent remediation efforts.
   - Summarized charts can be created for administered computers and vulnerabilities.

Proposed Architecture

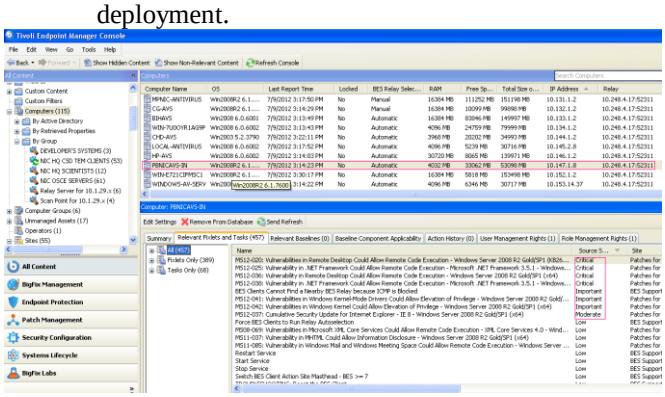


Key Solutions of TEM
- Patch Management
- Asset Discovery and Inventory
- Software Distribution
- Endpoint Protection Status
- Vulnerability Status

Patch Management
- Deployment of Relevant Patches on the severity basis of OS Vendors, Application vendors and category.
- Deployment of patches on the basis of vulnerabilities listed in CVE.
- Deployment of patches on single or multiple computer(s) with a single click.
- Presets can be used to aware user regarding patch

 Copyright 2019.All rights reserved.

deployment.



TEM Console

Gives consolidated overview of :

- TEM Server Status
- Analyses
- Patches and Fixlets
- Endpoint Protection status and many more……

TEM Console Components

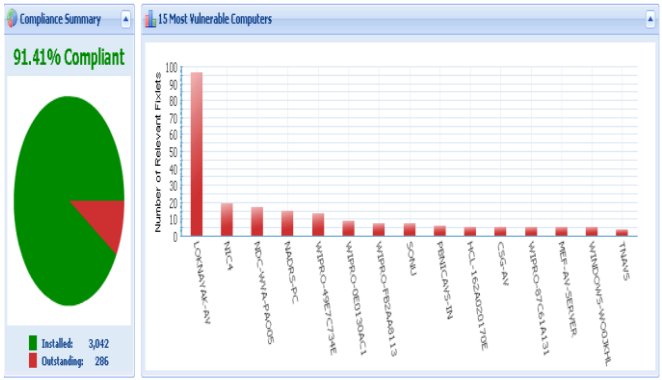
- Domain panel
- Console Toolbar
- List Panel
- Context Menu
- Domain Buttons
- Work Area Toolbar
- Work Area

Important Features of Console

- Fixlets Deployment
- Analyses and Tasks Activation
- Actions Status
- Computers and Groups
- Dashboards

Web Reports- Asset Management

Web Reports- Compliance Summary



REFERENCES

[1] https://www.techopedia.com/definition/1773/decryption
[2] www.computerhope.com/jargon/d/decrypti.htm
[3] https://en.wikipedia.org/wiki/Cryptography
[4] https://www.techopedia.com/definition/25403/encryption-key
[5] http://searchsecurity.techtarget.com/definition/private-key
[6] https://www.tutorialspoint.com/cryptography/cryptography_tutorial.pdf

 Copyright 2019.All rights reserved.