I J C T A, 10(8), 2017, pp. 689-695 ISSN: 0974-5572

Compliance Using BMC Blade Logic Server Automation

Shraddha Ramteke[1, 3], Saurav Siddhartha[1, 4], Tanvi Shah[1, 5], Tejas Shah[1, 6], Suresh Balla[2] and Varsha Powar[1,7]

ABSTRACT

BMC Blade Logic Server Automation (BBSA) is the industry-leading solution for automated management, control, and enforcement of server configuration changes in the data center and in the cloud. The Compliance module of BBSA enables to analyze servers and measure compliance with corporate policies or industry standards. This project describes the typical tasks that one performs while analyzing compliance through BMC Server Automation. Full life cycle management: Focal point of control for entire server life cycle, simplifying compliance, provisioning, configuration, patching, and reporting. Using the Compliance module, any number of server configurations can be scanned across multiple data centers for adherence to the relevant policies or sets of compliance rules. Compliance analysis is performed based on two types of BMC Server Automation objects: components and component templates. Components: Encapsulate portions of server configuration, enabling simple yet powerful compliance jobs. Component templates: Contain relevant compliance rules that are required to be adhered to the servers.

Keywords: BBSA, Compliance, Rules, Automation, RSCD agent, tmp, var, var/log, nodev, nosuid, noexec, cron, ssh

1 INTRODUCTION

Years ago, the system administrators faced a lot of problem due to the repeated execution of the same work. Later on, a group of system administrators came up with the idea of ad-hoc type of activity which included combining of libraries to execute common tasks. Server Automation is the solution for managing, configuring massive number of servers and ensuring automated provisioning, patching of the servers. It enforces configurational changes in data centers and in cloud with great ease.

2 NEED

The Applications which we use, highly depend on data centers' servers. So managing, configuring, patching and provisioning manually becomes a huge overhead for the system administrators as it is a tedious job for them to repeat the same task. BBSA (BMC Blade Logic Server Automation) helps to overcome all the above issues by providing a policy-based approach to manage data centers with fast speed and consistency. BBSA also offers a core capability which is compliance which enables to analyze servers and measure their compliance with industry set standards. The compliance module of server automation is used to check the fulfilment of requirements set by the standardized organizations.

3 COMPLIANCE

In BBSA, compliance is basically the process which is determining whether the system meets the industry set standards [5]. Two properties of compliance which are analysis and remediation are performed on two types of BBSA objects: components and component templates. Component templates are created by writing rules and compliance is measured using a standard known as scoring. A scoring status indicates whether

[1] Information Technology, MIT Pune, India,

[2-7] BMC Software, *Email: suresh_balla@bmc.com*; *Emails: shraddharamteke10@gmail.com; saurav_siddhartha@hotmail.com; tanvis544@gmail.com; shahtejas2401@gmail.com; varsha.powar@mitpune.edu.in*

compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring status are used in this benchmark:

- Scored: Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.
- Not Scored: Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

3.1. Rules

There are two types of configuration files defined by the LTS Benchmark based on which the rules are written [5]. They are as follows:

- Level-I: Rules defined in this profile aim to be:
- Be practical.
- Provide security benefits clearly.
- Not hamper the usefulness of the technology beyond acceptable means.
- Level-II: It extends the "Level-I" profile. The rules defined in this profile have the following characteristics:
- Are important for the environments where security is of prime importance.
- May negatively hamper the usefulness or performance of the technology.

In order to check whether the system is compliant according to the given standards following set of rules are implemented:

3.1.1. Patching and Software Updates

This section describes about the security enhancements in terms of patches which may not be available through the full update[5]. It is always recommended that the latest software patches should be used to take advantage of the latest features.

3.1.2. Filesystem Configuration

Directories that are used for all the system administration functions are protected by placing them on separate partitions[5]. Partitions are known as file systems. A user partition is a filesystem that has been defined for the use by the users and does not contain software for system operations. Compliance for the filesystem consists of checking the rules related to partitioning the files such astmp, var, var/log, home. It also consists of setting options such as nodev, nosuid, noexec for files. It also consists of setting Sticky bit for write able directories and also binding mount and disabling mount of file systems.

3.1.3. Secure Boot Settings

These settings basically provide root privileges to the owner and prevents the non-root users from changing the files[5].

3.1.4. OS Services

This section is to check which services are not important for the normal system operation. The services which are not required are disabled[5].

3.1.5. Special Purpose Services

This section describes the services that are needed to be installed on servers which are significantly needed to run these services[5]. If any of these services are not mandatory then it is recommended to either disable or delete them.

3.1.6. Network Configuration and Firewalls

The Networking vulnerabilities are the most exploited vulnerabilities by attackers[5]. To stop networking based attacks, the server needs to be compliant with the company standards. To do so, certain network based files and connections need to be audited and if any of these files or connections found to be prone to malicious activity and not in accordance to the standards, then the permissions of those particular files or connections must be modified.

3.1.7. Logging and Auditing

This section is used to describe how to configure logging, log monitoring, and auditing[5].

3.1.8. System Access, Authentication and Authorization

This section helps in keeping intact the authenticity and authority of the system[5]. The various procedures include allowing the access to cron (daemon) jobs if and only if the user is the owner, checking the password strength while someone sets a password and number of attempts allowed for entering correct password before temporary locking of accounts and proper ownership of the ssh files which allows connections using protocols like FTP, Telnet, etc. If these are not monitored properly the system is prone to attacks from malicious party which can tamper the state of the system and make it unavailable for use even by the authorized personnels.

3.1.9. User Accounts and Environments

This section basically helps to set up secure default values for system and user accounts[5].

3.1.10. Warning Banners

Presenting a warning message prior to the normal user login may assist the action of trespassers on the computer system[5]. Changing some of these login banners also has the side-effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

3.1.11. Verify System File Permissions

There are various files in the system which contain highly sensitive data which if falls in wrong hands can do a lot of damage[5]. Therefore, it is mandatory to protect the files from unauthorized access of write. If attackers can gain read access to the password file, they can easily run a password cracking program against the hashed password to break it. So the permissions to this file should only be restricted to specific group of users. And to verify the users authentication Ubuntu does various checks. The user file contains a list of all the valid userIDs defined in the system, but not the passwords. Administrator needs to set the right to this file to root users only.

3.1.12. Review User and Group Settings

Over time, system administration errors and changes can lead to changes in groups' definition[5]. This section basically provides guidance about the security feature of the user and groups.

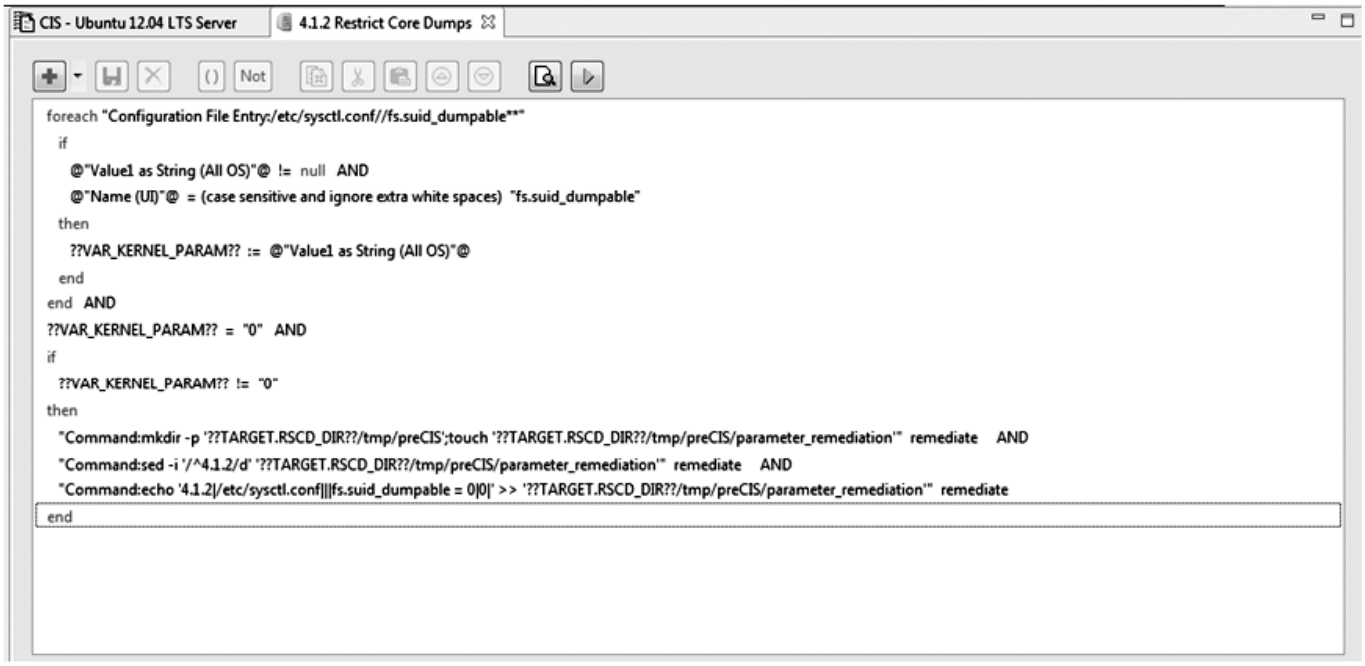

Figure 1: Rule of Restricted Core Dumps

The Fig. 1 encompasses the rule description. The core dumps are the memory segment of a program which dictates why the program failed. It contains some sensitive data which can be used by attackers to tamper the machine. So as mentioned in the above figure the condition is fs.suid_dumpable is set to 0 so that no program is able to dump the core.

4. WORKFLOW

The workflow of our project can be illustrated with the help of following steps:

1. Add Ubuntu server with RSCD Agent installed to the console
2. Create component template
3. Create rules
4. Check compliance
5. If the rule is compliant then generate report
6. If the rule is non-compliant then remediate and repeat 4 and 5
7. The generated report contains the entire information of the compliant & non-compliant rules. It should be stored in the database

5. ARCHITECTURE

The Fig. 2 elaborates how the various servers such as Console Terminal Server, Application Server, File Server and Database server communicate with each other in order to deploy jobs on the targeted servers. The communication occurs by the end points known as ports and each server has a unique port for communication, i.e. for Console Terminal Server port number 9840 is used, for Application Server port number 4750 is used, for Database Server either port number 1521 is used or port number 1433 is used depending upon whether Oracle or Microsoft SQL is used respectively.

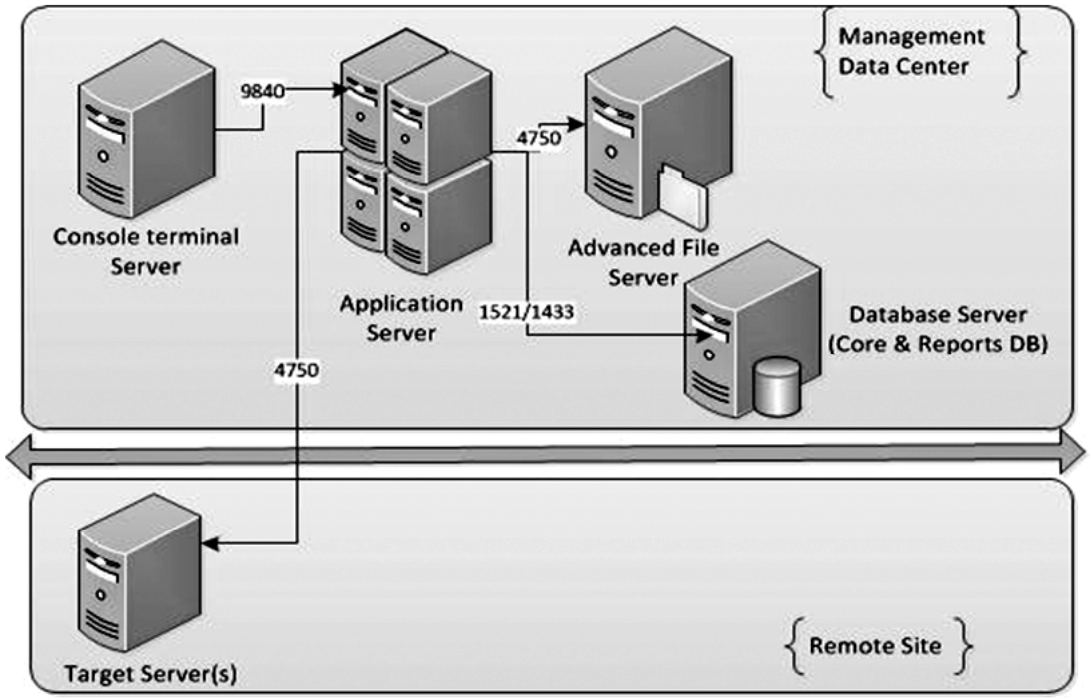

Figure 2: Architecture of BBSA

6. SOFTWARE REQUIREMENTS

6.1. Web service

"CIS UBUNTU 12.04 LTS Web Server" is the server on which the RSCD agent is installed. Incase if a rule is not compliant according to the industry standard then it can be remediated by firing commands on the terminal.

"Microsoft 2008 Server R2" is a server operating system developed by Microsoft. It is the first 64-bit-only operating system which was released from Microsoft.

"Microsoft SQL Server" is a relational database management system which is developed by Microsoft. It is basically a software product whose main function is to store and retrieve data as per the requirement by the applications which either run on the same computer or computer across a network.

6.2. Tools

6.2.1. BMC BladeLogic Server Automation Console

The BMC BladeLogic Server Automation Console is the user interface which is used to create component templates on which compliance can be checked. We can live browse through the contents of the target machine on which RSCD Agent is installed. The server needs to be added to the console. Rules can be remediated using this front end tool.

The Fig. 3 shows us the various window panels. The panel on the top left has the template folders, servers, etc. Here we can select the template we want to work on and the target server. The panel to the top right is where we create our rules and live browse the server. The RSCD agent needs to be installed in order to work on the server.

The Fig.4 does not differ much from the figure 3 as only the top right panel where we select the compliance tab and on the bottom right panel the various rules appear marked in order. Here we can choose the specific rule to work upon.

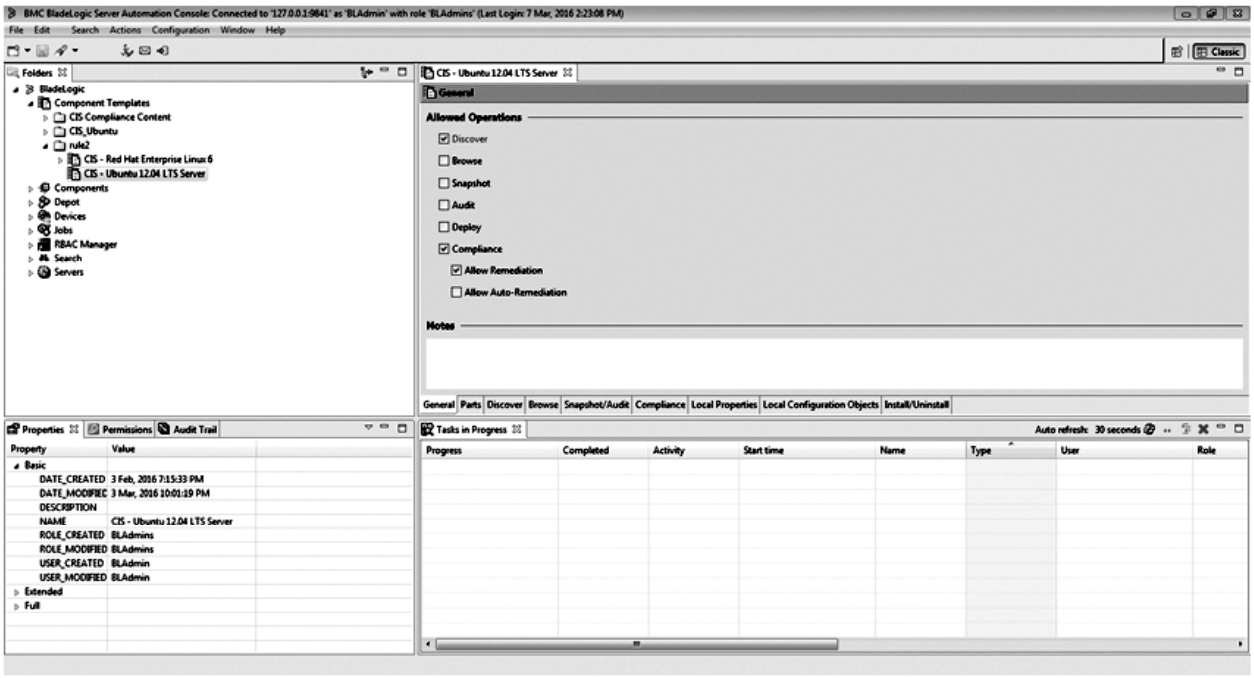

Figure 3: BBSA Console

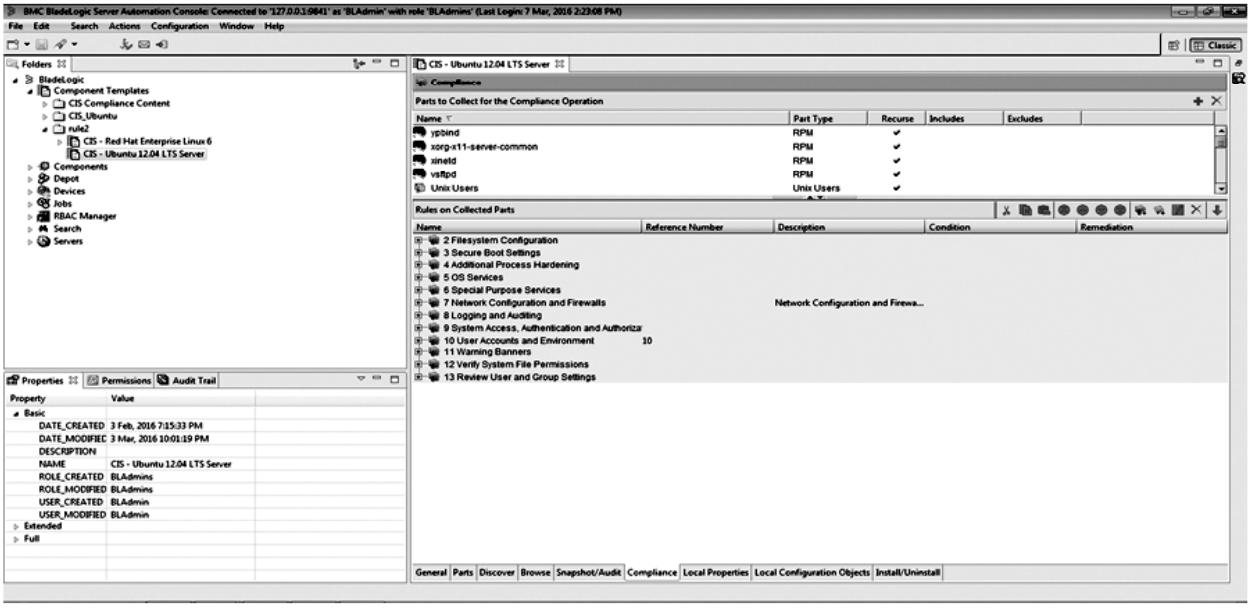

Figure 4: BBSA Console

6.2.2. Application Server

Application Server acts as a middleware between the BMC BladeLogic Server Automation Console and the Ubuntu Server (target machine).

7. REPORT GENERATION

After the creation of component template is done and all the required rules are written, a report is generated at the end which contains information about all the compliant as well as non-compliant rules. We can test the compliance of rules individually by manual testing and if we want to check the compliance of all the rules together then we can generate report.

8. CONCLUSION

BMC BladeLogic Server Automation has the capability to reduce vulnerabilities and maintain operation efficiency. With the help of BBSA, security policies can be ensured. Also provisioning, vendor-supplied patches and configuration. Physical, virtual and cloud servers can be maintained.

REFERENCES

[1] https://docs.bmc.com/docs/display/public/bsa85/Analyzing+system+compliance

[2] http://documents.bmc.com/products/documents/27/36/242736/242736.pdf

[3] http://www.bmc.com/it-solutions/intelligent-compliance.html

[4] http://www.ktsl.com/bmc-automation

[5] CIS Ubuntu 12.04 LTS Server Benchmark pdf