

Project Report on

**Server Lifeboat, Nagios Monitoring**

**Submitted by**

**Kaustubh Deochake: 240344223008**

**Kiran Patil: 240344223024**

**Rupesh Modi: 240344223019**

**Ujjwal Shelke: 240344223037**

Under the guidance of

**Mr. Sandeep Walvekar**

**In partial fulfillment of the award of** **Post Graduate Diploma in**

**IT Infrastructure, Systems and Security**

**(PG-DITISS)**



**Sunbeam Institute of Information Technology,**

**Pune (Maharashtra)**

**PG-DITISS -2023**

**DECLARATION**

We declare that this written submission represents our ideas in our own words and where others’ ideas or words have been included; we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed**.**

Place: Pune

Date:

**Kaustubh Deochake Kiran Patil Rupesh Modi**

**(240344223008) (240344223024) (240344223019)**

**Ujjwal Shelke**

**(240344223037)**

**CERTIFICATE**

This is to certify that the project report entitled **“Server Lifeboat, Nagios Monitoring”**, submitted by **Kaustubh Deochake** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

**CERTIFICATE**

This is to certify that the project report entitled **“Server Lifeboat, Nagios Monitoring”**, submitted by **Kiran Patil** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

**CERTIFICATE**

This is to certify that the project report entitled **“Server Lifeboat, Nagios Monitoring”**, submitted by **Rupesh Modi** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

**CERTIFICATE**

This is to certify that the project report entitled **“Server Lifeboat, Nagios Monitoring”**, submitted by **Ujjwal Shelke** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

**APPROVAL CERTIFICATE**

This Project II report entitled **“Server Lifeboat, Nagios Monitoring”** by **Kaustubh Deochake(240344223008)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

**APPROVAL CERTIFICATE**

This Project II report entitled **“Server Lifeboat, Nagios Monitoring”** by **Kiran Patil (240344223024)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

**APPROVAL CERTIFICATE**

This Project II report entitled **“Server Lifeboat, Nagios Monitoring”** by **Rupesh Modi(240344223019)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

**APPROVAL CERTIFICATE**

This Project II report entitled **“Server Lifeboat, Nagios Monitoring”** by **Ujjwal Shelke (240344223037)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

**CONTENTS**

|  |  |
| --- | --- |
| **TITLE** | **PAGE NO** |
| **Declaration** |  |
| **Certificate** |  |
| **Approval Certificate** |  |
| **Abstract** | 1 |
| **1.INTRODUCION** | 3 |
| 1.1 Applications | 4 |
| 1.2 Organization and Project Plan | 4 |
| **2. LITERATURE SURVEY** | 5 |
| Paper 1 | 5 |
| **3. SYSTEM DEVELOPMENT AND DESIGN** | 7 |
| 3.1 Proposed System | 7 |
| 3.2 Flow Chart | 8 |
| 3.3 Technology used | 8 |
| 3.3.1 Web Server | 8 |
| 3.3.2 Database Server | 9 |
| 3.3.3 Mail Server | 9 |
| 3.3.4 Rsync Command | 9 |
| 3.3.5 Git | 10 |
| 3.3.6 Snort | 10 |
| 3.3.7 Nagios | 10 |
| **4. PROJECT OUTPUT** | 11 |
| **5. CONCLUSION** | 14 |
| 5.1 Conclusion | 14 |
| 5.2 Future Scope | 14 |
| **REFERENCES** | 15 |

**ABSTRACT**

For today’s organization, data is the blood through which every organization in the flow. Hence, it is imperative to guarantee the availability and completeness of this information as a way of supporting business processes. This is where a good backup solution comes in handy as a way of protecting data and ensuring that new data will be created. This abstract discusses steps that involve installation of a backup server in Linux environment in order to ensure that categorized data from web, database and mail servers are safe and encrypted backups executed in the original servers recorded in the remote machine.  
The proposed solution includes installing three indigenous Linux machines where one machine will be used for hosting Web Server, second Machine will be used for hosting Database Server and the last Machine will be used for hosting mail server. On each machine, backup script settings are provided to copy all data of the server and make backups periodically. The script makes use of rsync, a tool commonly used for remote backups, whereas tar is used for carrying out differential as well as full backups and does not consume a lot of time when backing up due to the pseudo-remote nature of the backup.  
For instance, to encrypt the backup data, the script uses GPG or SSH in order to transmit the backup data securely to the remote machine. The remote machine is another backup server, corresponding servers that receive and store the encrypted backups from three servers.  
Another and equally important function in this context of the backup server is to perform backup retention and delete according to specific business rules to keep and maintain the backup repository clean. Moreover, the backup server is a monitoring script that is charged with the responsibility of monitoring the backup process and notifying whenever there is an occurrence of an error or failure.  
With the help of this solution, organizations can guarantee that data is stored in a manner that allows it to be accessed independently of the hardware, software, or mistakes. Linux as the fundamental base grants steady and secure environment for the backup structures; the utilization of the open-source tools, including rsync and tar, safeguards effectiveness and reliability in terms of the costs.  
In conclusion, this abstract provides a holistic method on how a backup server can be set up on Linux to ensure information from web, databases, and mail servers is backed up. Through the ideas incorporated in this paper, particularly through the automation of backups, application of encryption methods, and the implementation of the retention policy, organizations will be in a position to secure their data and proceed with business as usual once an unpredictable event occurs.

1. **INTRODUCTION**

In the modern digital landscape, the integrity and availability of data are critical for organizational success. This introduction outlines a robust backup server configuration involving three Linux machines-dedicated to web, database, and mail servers-designed to ensure data protection through systematic backup processes. The architecture leverages VMware for virtualization, with a remote machine featuring for enhanced data redundancy and reliability.

The primary objective of this setup is to automate the backup process, ensuring that all critical data from the web server, database server, and mail server is regularly captured and securely transmitted to a remote backup server. To further enhance the security and integrity of the backup process, the solution incorporates a fifth machine running Nagios and Snort. Nagios serves as a monitoring tool, providing real-time insights into the health and performance of the entire infrastructure, while Snort acts as an intrusion detection and prevention system, monitoring network traffic for potential threats. The backup process utilizes efficient tools such as rsync for file synchronization, ensuring that only changes are transmitted, thereby optimizing bandwidth usage. Additionally, the backups are encrypted during transmission to maintain confidentiality and protect sensitive information.

By implementing this comprehensive backup solution, organizations can ensure the resilience of their IT infrastructure, minimize the risk of data loss, and maintain operational continuity. This approach not only secures essential data but also fosters a proactive stance towards data management and disaster recovery, ultimately contributing to the overall efficiency and security of the organization’s digital assets.

1.1 Application:

* Data Protection: Automates regular backups to protect critical data hosted on web, database, and mail servers.
* Remote Backup Storage: Leverages a remote VMware machine for redundancy and fault tolerance.
* Monitoring and Security: Integrates Nagios for monitoring server health and Snort for intrusion detection.
* Disaster Recovery: Enables quick recovery of services by restoring from regularly scheduled backups.
* Compliance: Helps maintain compliance by securely backing up data and providing an audit trail.
* Cost-Effectiveness: Uses open-source tools and Linux servers to reduce licensing costs compared to proprietary solutions.
* Data Integrity: Employs encryption during backup transmission to protect sensitive information from unauthorized access.

1.2 Project Plan Table: Activities Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr.**  **No.** | **ACTIVITY** | **WEEK** | | | |
| **1** | **2** | **3** | **4** |
| 1 | Project group formation |  |  |  |  |
| 2 | Project work to be started in respective labs |  |  |  |  |
| 3 | First review with PPT presentation |  |  |  |  |
| 4 | Design Use-Case view as per project |  |  |  |  |
| 5 | Design Block diagram as per project |  |  |  |  |
| 6 | Second review with PPT presentation |  |  |  |  |
| 7 | Selection |  |  |  |  |
| 8 | Final review with PPT presentation |  |  |  |  |
| 9 | Implementation coding as per project |  |  |  |  |
| 10 | Testing, Troubleshooting with different techniques |  |  |  |  |
| 11 | Created Soft copy of project and then final hard copy |  |  |  |  |

**2. LITERATURE SURVEY**

1. The importance of the data generated and retrieved is referred to as data integrity and availability.

Key Concepts: Describe how availability and integrity of data are critical components of organizational continuity concerning numerous servers, including web, database, and mail servers.

Studies that are pertinent: Look for studies and publications that provide instances of data integrity concerns along with the goal of helping the reader comprehend how companies have suffered as a result of data loss scenarios.

2. Technologies and Backup Plans

Key Concepts: Different backup facilities (on-site, off-site, and cloud storage) and backup methods (full, incremental, and differential) are covered.

Relevant Studies: Analytical articles that examine the benefits and limitations of these strategies based on firsthand experience implementing them in various settings, providing an examination of automation and disaster recovery.

3. Backup System Automation

Important Ideas: Talk about when the backups are completed, where automation may be used to enhance backup, and how much less human interaction is needed.

Relevant Studies: Look for publications that discuss automated backup options and their success and failure rates.

4. Backup for Specific Server Types: Important Points: Web, database, and mail server backups need special attention. Consider what kinds of information and configurations need to be protected and why.

Studies that are pertinent: Do research on the benefits and issues associated with mirroring different kinds of servers. An example of this would be the backup of non-structured data on a web server vs data from traditional or structured databases.

5. Backup System Security

Important Ideas: Examine several approaches to safeguarding backup data against loss, corruption, and hacking.

Studies that are pertinent: Look into topics like data encryption, storage security management, and safe methods for accessing data backups.

6. Instances and Situations

Important Ideas: Conduct research on the actual use of automated backup systems and provide an overview of the main problems, solutions, and outcomes.

Relevant Studies: Case studies of audits from many industries, particularly those involving any company that processes vital data.

7. We go over the present trends in knowledge management that are good predictors of future trends in the subject in the section that follows.

Key Concepts: Learn about the latest advancements in automation and backup technologies, such as cloud connectivity, AI backups, and analytical backup projections.

Relevant Studies: Papers and articles discussing upcoming developments and innovations in data recovery and backup.

# System Development and Design

* 1. **Proposed System:**

The proposed system for a backup server in a Linux environment involves a comprehensive setup that ensures data integrity, availability, and security across multiple servers. This configuration includes three dedicated Linux machines serving as a web server, database server, and mail server, along with a remote backup server and monitoring tools. Below is a detailed outline of the proposed system:

1. **System Architecture**

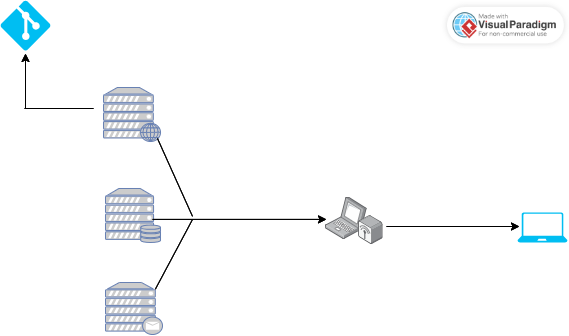
* **Primary Servers**:
  + **Web Server**: Hosts the organization's website and web applications.
  + **Database Server**: Manages databases and handles data transactions.
  + **Mail Server**: Facilitates email communications for the organization.
* **Backup Server**: A dedicated Linux machine configured to perform regular backups of the primary servers. This server will utilize tools such as rsync  for efficient data backup and restoration.
* **Remote Backup Storage**: A separate remote machine configured on VMware, for redundancy and fault tolerance. This setup ensures that data remains secure and accessible even in the event of hardware failure.
* **Monitoring and Security**: A fifth machine running **Nagios** for monitoring server health and performance, and **Snort** for intrusion detection and prevention, ensuring that the entire system is secure and operational.

2. **Backup Process**

* **Automated Backups**: The backup server will be configured to perform automated backups at scheduled intervals (e.g., daily incremental backups and weekly full backups).
* **Data Encryption**: Backups will be encrypted during transmission to the remote storage to protect sensitive information from unauthorized access.
* **Backup Types**:
  + **Full Backups**: Comprehensive backups of all data at regular intervals.
  + **Incremental Backups**: Backups that capture only the changes made since the last backup, optimizing storage and time.

3. **Monitoring and Reporting**

* **Nagios Configuration**: Nagios will monitor the status of all servers, ensuring that any issues are promptly reported to the IT team.
* **Snort Configuration**: Snort will monitor network traffic for potential threats, providing alerts for suspicious activity.
* **Backup Status Reports**: Regular reports will be generated to summarize backup success, failures, and storage utilization.
  1. **Flow chart**

****



* 1. **Technology used:**

**1. Web Server**

Apache HTTP Server is one of the most widely used open-source web servers, known for its reliability and flexibility in serving web content.

**Key Features**:

* + **Modular Architecture**: Supports a wide range of modules for functionality such as URL rewriting, authentication, and security.
  + **Cross-Platform Compatibility**: Runs on various operating systems, including Linux, Windows, and macOS.
  + **Customizable Configuration**: Allows for extensive configuration through .htaccess files and main configuration files.
  + **Support for Multiple Protocols**: Primarily serves content over HTTP/HTTPS, with support for FTP and other protocols.

**2. Database Server**

MySQL is a popular open-source relational database management system that uses SQL for querying and managing data.

**Key Features**:

* + **ACID Compliance**: Ensures reliable transactions and data integrity.
  + **Scalability**: Capable of handling large databases and high-traffic applications.
  + **Replication Support**: Facilitates data redundancy and load balancing through master-slave replication.
  + **User Management**: Provides robust user access controls and security features.

**3.Mail Server**

Postfix is an open-source mail transfer agent (MTA) that routes and delivers electronic mail.

**Key Features**:

* + **Performance and Security**: Designed to be fast and secure, with built-in anti-spam and anti-virus features.
  + **Easy Configuration**: Offers a straightforward configuration process, making it accessible for administrators.
  + **Support for Multiple Protocols**: Works with SMTP for sending emails and can be configured to support IMAP and POP3 for receiving emails.
  + **Virtual Domain Support**: Allows hosting of multiple domains on a single server.

**4. rsync Command**

rsync is a command-line utility for efficiently transferring and synchronizing files between local and remote systems.

**Key Features**:

* + **Incremental Backups**: Transfers only the changed portions of files, reducing bandwidth and time.
  + **Preservation of File Attributes**: Maintains permissions, timestamps, and symbolic links during transfer.
  + **Local and Remote Synchronization**: Can be used to synchronize files across different machines over SSH or on the same machine.
  + **Compression Options**: Supports compression during transfer to save bandwidth.

**5. Git**

Git is a distributed version control system designed for tracking changes in source code during software development.

**Key Features**:

* + **Branching and Merging**: Allows developers to create branches for new features and merge them back into the main codebase efficiently.
  + **Distributed Architecture**: Each developer has a complete copy of the repository, enabling offline work and collaboration.
  + **Commit History**: Maintains a detailed history of changes, making it easy to revert to previous versions.
  + **Collaboration Tools**: Supports pull requests and code reviews, facilitating team collaboration.

**6. Snort**

Snort is an open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS) developed by Cisco. It is designed to monitor network traffic in real-time and detect malicious activities.

**Key Features**:

* + **Traffic Analysis**: Snort performs real-time traffic analysis and packet logging on IP networks, allowing it to detect various types of attacks and probes.
  + **Rule-Based Detection**: Utilizes a flexible rule-based language to define malicious network activity, enabling it to identify known threats and anomalies.
  + **Multiple Operating Modes**: Can operate in different modes:
    - **Sniffer Mode**: Captures and displays packets in real-time.
    - **Packet Logger Mode**: Logs packets to disk for later analysis.
    - **Intrusion Detection Mode**: Monitors traffic against a set of user-defined rules and generates alerts when suspicious activity is detected.
  + **Community and Subscriber Rulesets**: Offers both community-driven and subscription-based rulesets for detecting threats, with updates provided by Cisco's Talos team.

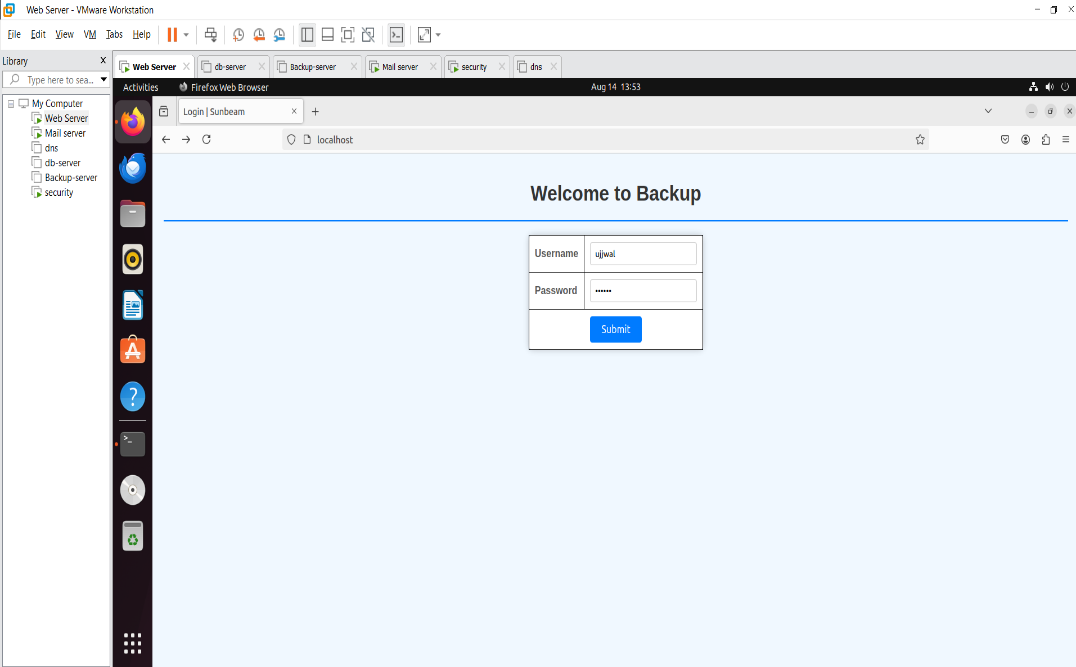
**7. Nagios**

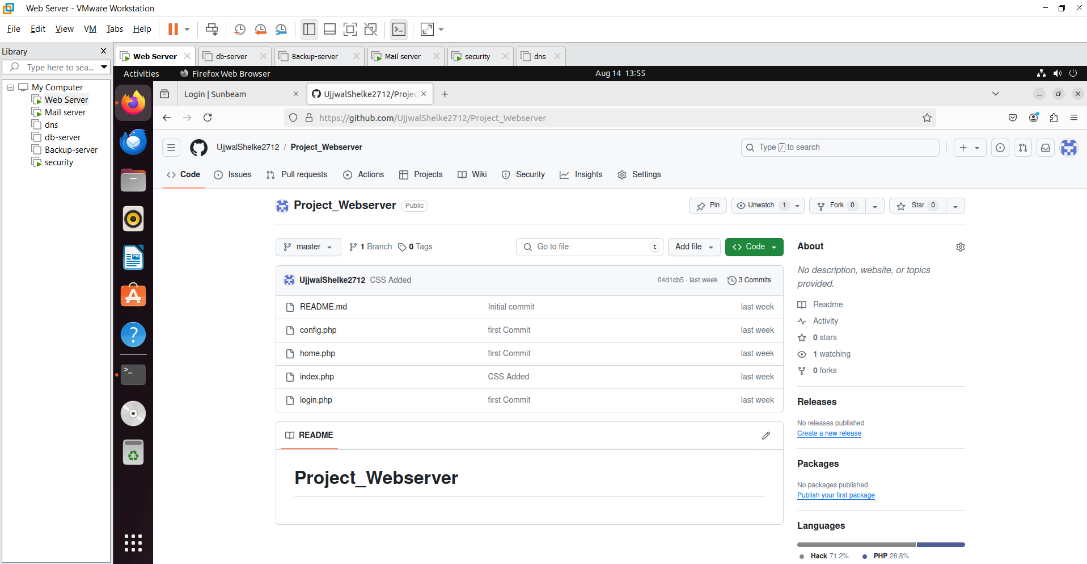
Nagios is an open-source monitoring system that provides monitoring and alerting services for servers, switches, applications, and services. It is widely used for network monitoring and infrastructure management.

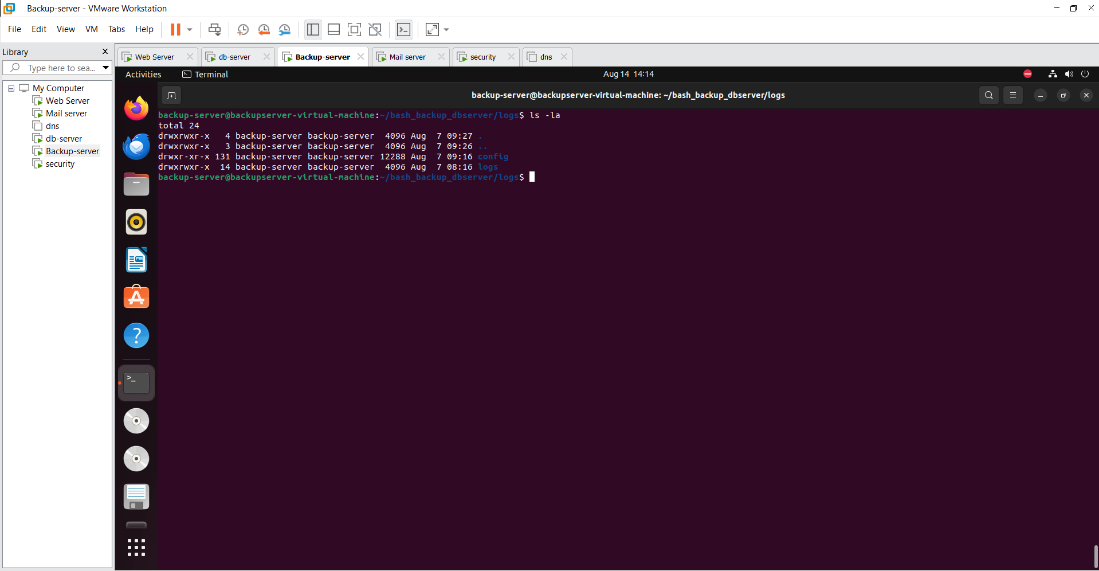
**Key Features**:

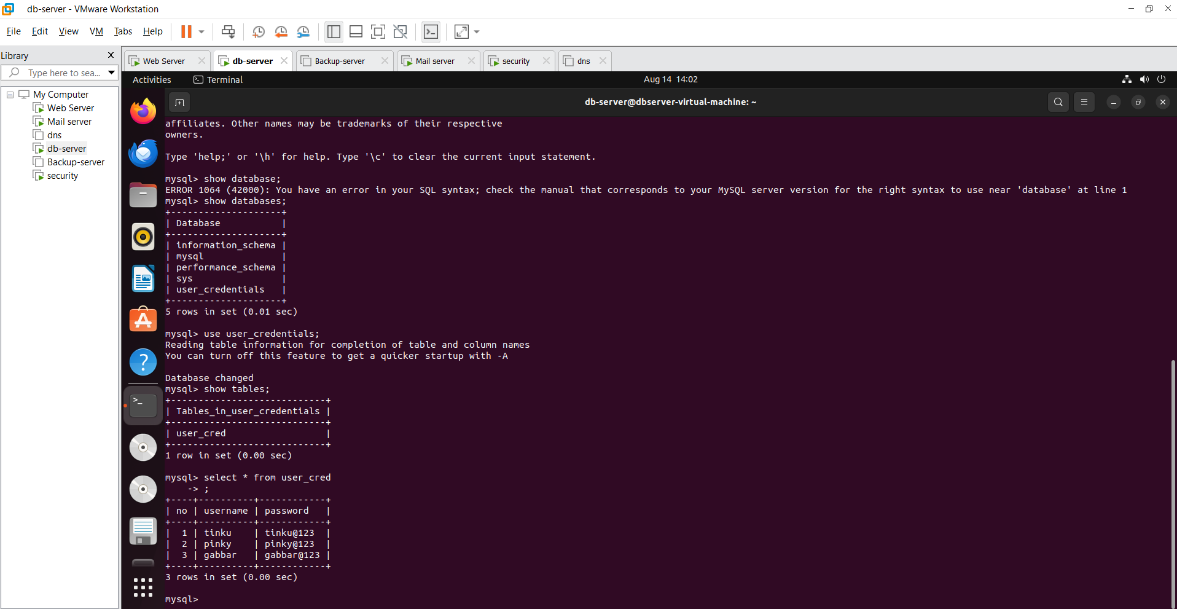
* + **Comprehensive Monitoring**: Monitors the availability and performance of various network services, including HTTP, SMTP, and more.
  + **Alerting System**: Sends alerts via email or SMS when issues are detected, allowing for proactive response to potential problems.
  + **Extensibility**: Supports plugins that extend its functionality, enabling users to customize monitoring capabilities for specific needs.
  + **Web Interface**: Provides a user-friendly web interface for viewing system status, performance metrics, and alerts.

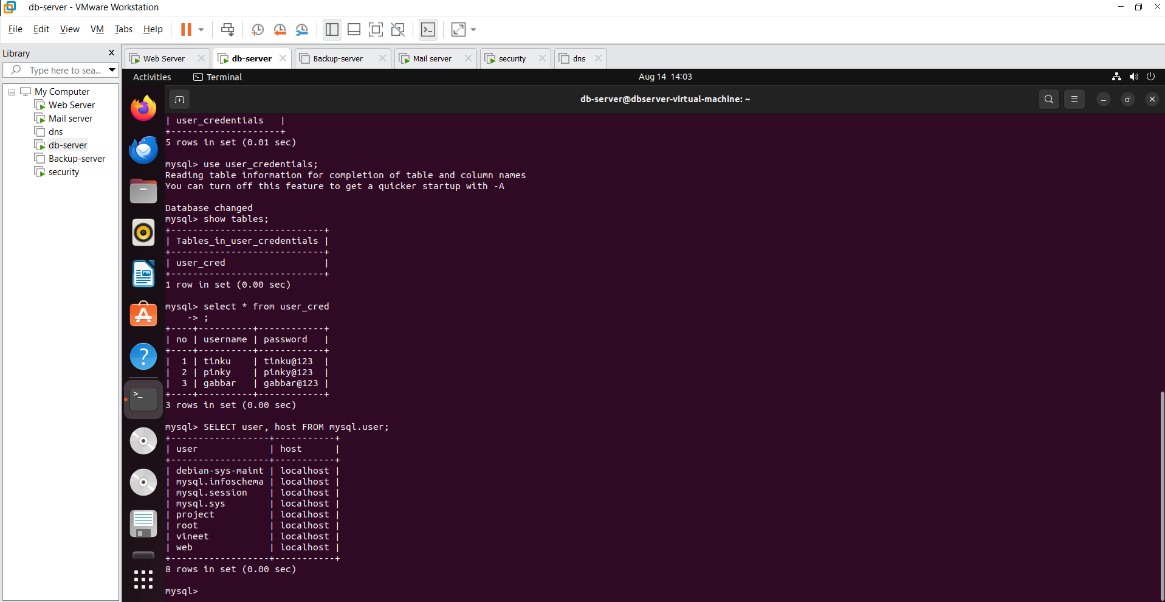
1. **Project Output**

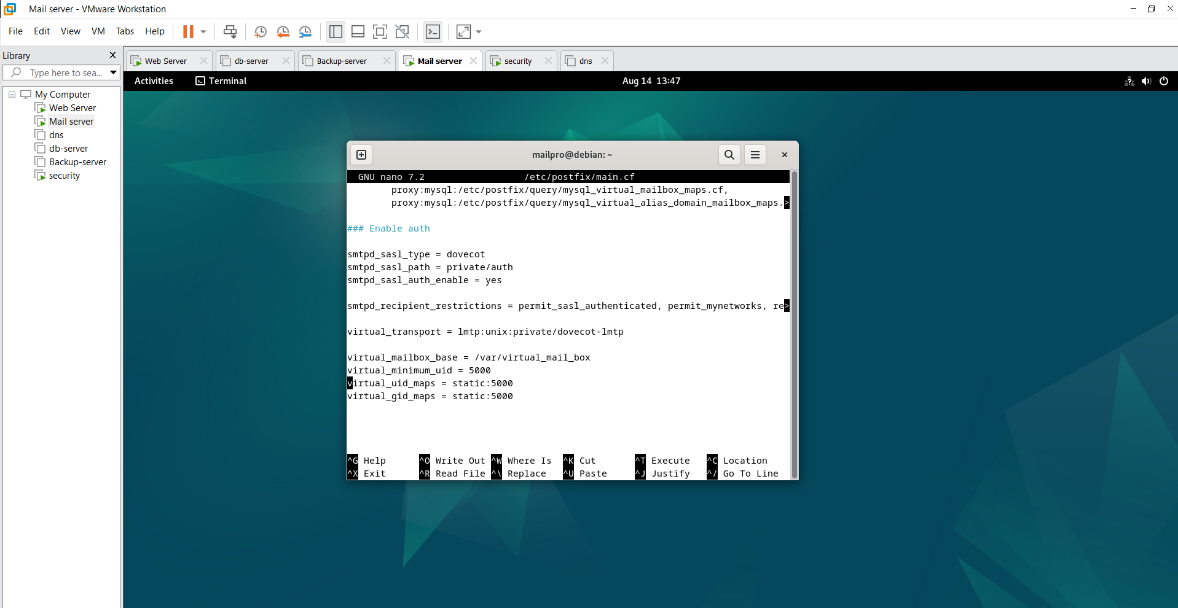
****

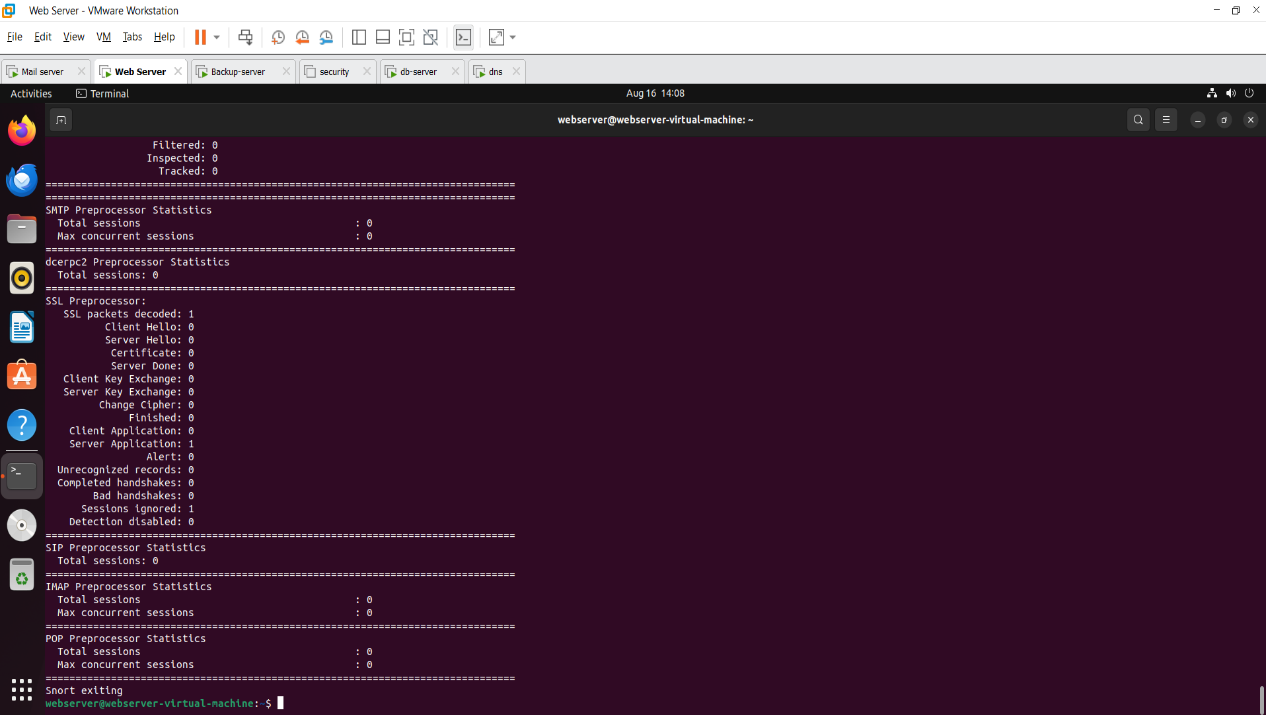
****

****

****

****

****

****

**5. CONCLUSION**

**5.1 Conclusion:**

Backup servers are essential for organizations seeking to ensure availability. They provide several advantages, including rapid data recovery, enhanced control over data security, and reduced dependency on internet connectivity. However, they also present challenges such as vulnerability to physical disasters and limited scalability.

**5.2 Future Scope:**

Backup servers is likely to be characterized by a blended approach that emphasizes the strengths of both local and cloud-based solutions. As businesses seek to protect their data more effectively, local backup servers will remain an integral part of comprehensive data management strategies, adapting to meet the challenges of scalability, security, and compliance in an increasingly digital world.

**REFERENCES**

<https://www.shellscript.sh/>

<https://geeksforgeeks.org/linux-tutorial/>

<https://www.youtube.com/>

<https://stackoverflow.com/>

<https://mariadb.com/>

<https://www.linux.org/>