VIRTUAL DESKTOPS AND REMOTE WORK

PHASE 2: DESIGN A SOLUTION BLUEPRINT

College Name: Shree Devi Institute of Technology, Mangalore

Group Members:

- **Name:** Abdulla Shafaz K U
  CAN ID: CAN_34027192
  Contribution: Service Integration

- **Name:** Abhishek Kulal
  CAN ID: CAN_34029363
  Contribution: Implementation Plan

- **Name:** Dhanya Ashok Kamat
  CAN ID: CAN_34030860
  Contribution: Architecture Overview

- **Name:** Shrutika Shetty
  CAN ID: CAN_34030246
  Contribution: Data Flow Diagram

Architecture Overview

1. Core Components

The architecture for this project consists of the following key components:

- Apache Guacamole: Acts as the clientless remote desktop gateway, enabling users to access remote desktops via a web browser.
- VNC Server: Provides remote desktop sessions that Guacamole connects to using the VNC protocol.
- MariaDB: Serves as the database backend for Guacamole, storing user accounts, connections, and configurations.
- Tomcat9: Functions as the servlet container running the Guacamole web application.
- Oracle Virtual Instance: Hosts the entire deployment, providing the necessary compute and storage resources.

2. Data Flow

- User Access: Users access the Guacamole web interface via a browser.
- Authentication: Guacamole authenticates users against the MariaDB database.
- Remote Desktop Connection: Guacamole connects to the VNC Server using the VNC protocol to provide remote desktop access.
- Database Management: MariaDB stores and manages all user and connection data securely.

Service Integration

1. Guacamole and VNC Server Integration

- Guacamole connects to the VNC Server using the VNC protocol to provide remote desktop sessions.
- The VNC Server is configured to run on the Oracle Virtual Instance, providing remote desktop access to users.

2. Database Integration

- MariaDB is integrated with Guacamole to store user accounts, connection details, and configurations.
- The database is secured with strong passwords and access controls to ensure data protection.

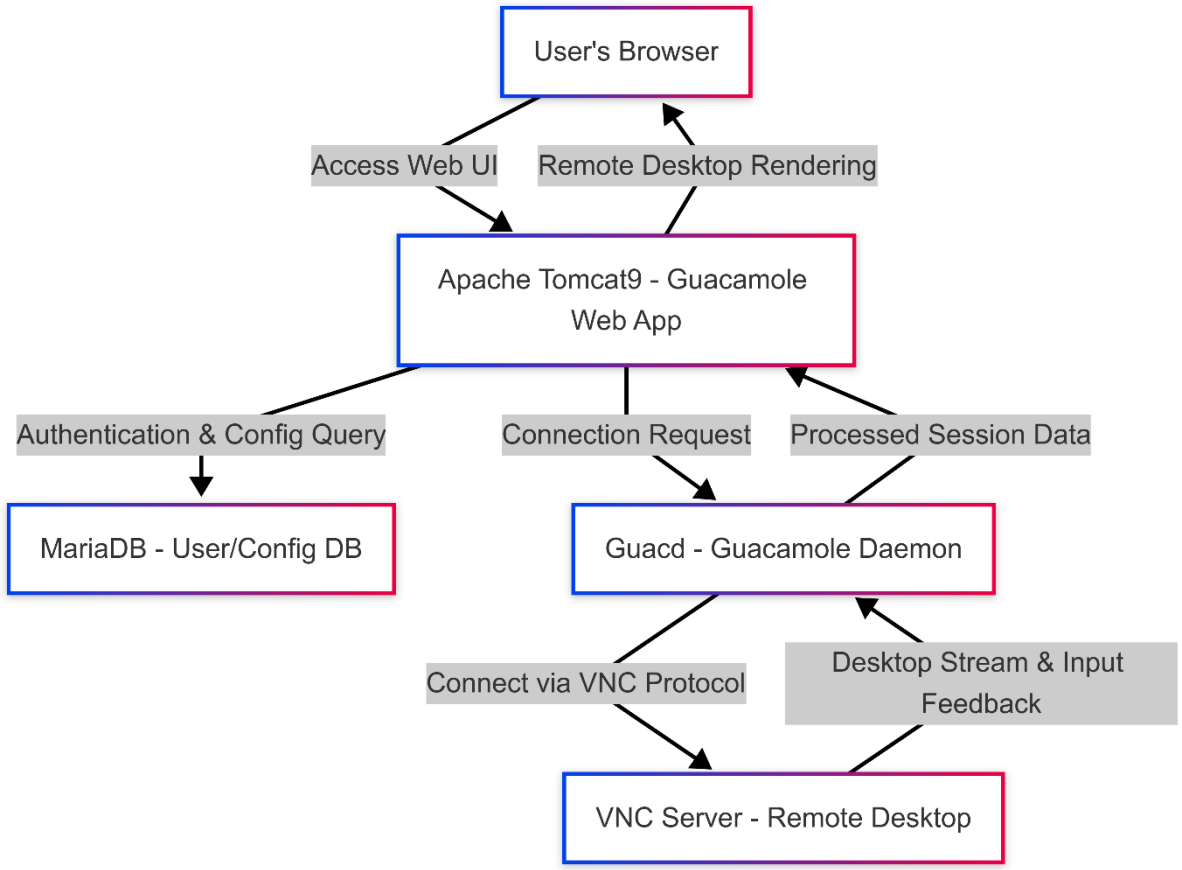
3. Tomcat9 Integration

- Tomcat9 serves as the servlet container for the Guacamole web application.
- The Guacamole WAR file is deployed to Tomcat9, making the web application accessible via a browser.

4. Security Integration

- Firewall Configuration: Restrict access to necessary ports (e.g., 8080 for Tomcat9, 5901 for VNC Server).
- Database Security: Implement strong passwords and access controls for MariaDB.

Data Flow Diagram



Implementation Plan

Step 1: Set Up Oracle Virtual Instance

- Provision an Oracle Virtual Instance with Ubuntu 20.04 or later.
- Ensure the instance has sufficient resources (e.g., 2 vCPUs, 4 GB RAM, 20 GB storage).
- Configure network settings to allow access to ports 8080 (Tomcat9), 3306 (MariaDB), and 5901 (VNC Server).

Step 2: Install and Configure MariaDB

- Install MariaDB on the Oracle Virtual Instance.
- Secure the installation by setting a strong root password and running the secure installation script.
- Create a database and user for Guacamole with appropriate permissions.

Step 3: Install and Configure Tomcat9

- Install Tomcat9 and its admin tools on the Oracle Virtual Instance.
- Deploy the Guacamole WAR file to Tomcat9.
- Restart Tomcat9 to apply changes.

Step 4: Install and Configure Apache Guacamole

- Install Guacamole Server and its dependencies.
- Configure Guacamole to use MariaDB as the database backend by editing the Guacamole properties file.

Step 5: Install and Configure VNC Server

- Install a VNC Server (e.g., TigerVNC) on the Oracle Virtual Instance.
- Configure the VNC Server to start automatically and set a secure password.
- Edit the VNC startup script to launch the desktop environment (e.g., Xfce).
- Restart the VNC Server to apply changes

.

Step 6: Test the Deployment

- Access the Guacamole web interface using the instance's IP address and port 8080.
- Log in using the credentials configured in MariaDB.
- Test the VNC connection by connecting to the remote desktop session.