🔧 Configuring System-to-System Log Forwarding Using rsyslog on Ubuntu 🐧

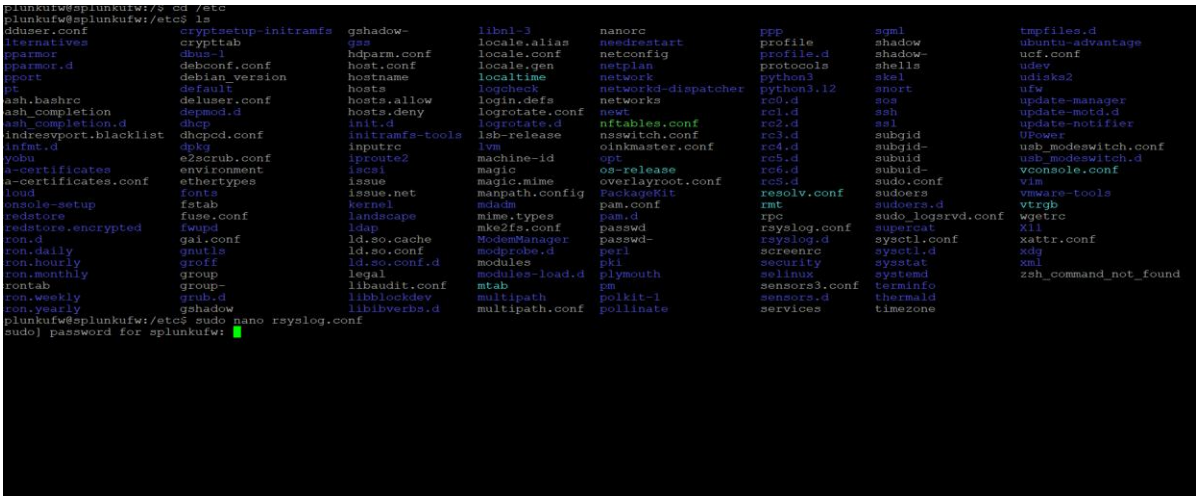
🖥️ To begin the configuration process, **launch the terminal** on your Ubuntu system.

📂 Once the terminal is open, **navigate to the system configuration directory** by executing the command to enter the /etc path.

🗂️ This directory contains important **configuration files**, including those necessary for managing rsyslog services used for log forwarding.

📁 **Next**, use the ls command within the /etc directory to **list and locate the rsyslog configuration files**.

🔍 This step helps **verify the presence** of rsyslog-related files such as rsyslog.conf

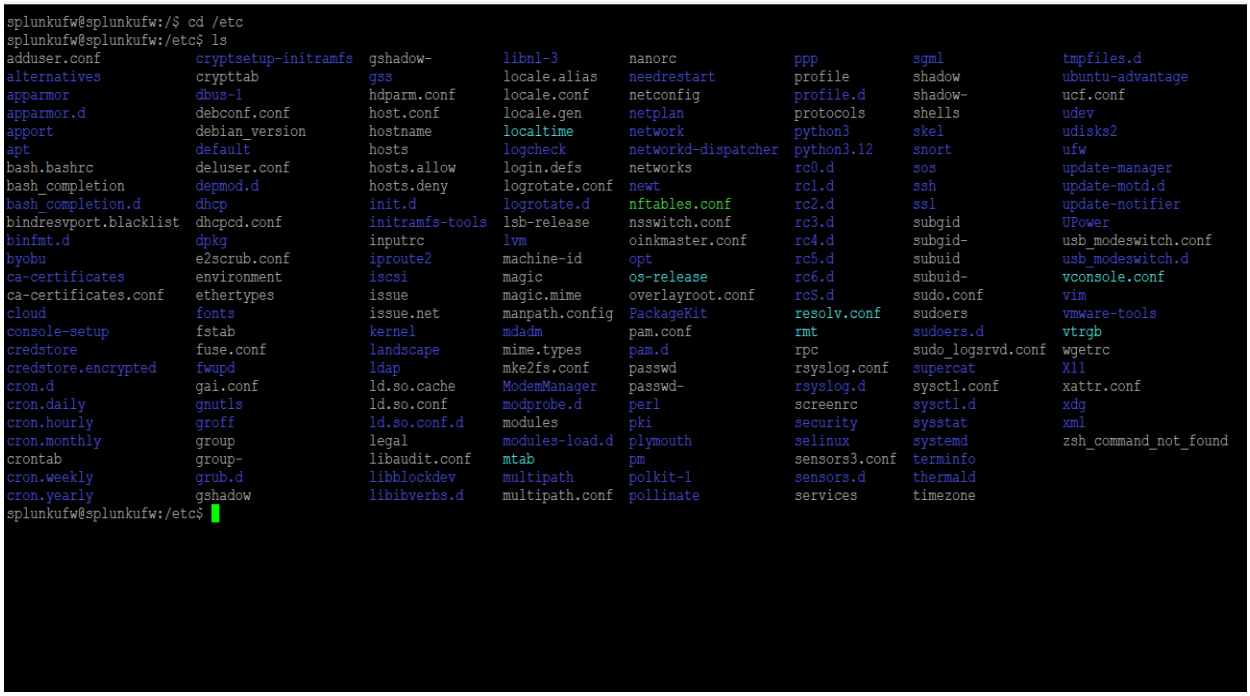


or the rsyslog.d directory, which are essential for configuring log forwarding and centralized logging.

🔐 At this stage, we need to **access the rsyslog configuration file or directory with elevated privileges**.

🛡️ Since the /etc directory and its contents are protected system files, you will be **prompted to enter the Ubuntu user password** when executing commands with sudo.

✅ This ensures **secure access** to modify rsyslog settings necessary for



system-to-system log forwarding.

📝 Once the rsyslog.conf file is opened in the **Nano text editor**, you will be able to **view and edit its contents**.

🛠️ At this point, specific **configuration lines** need to be added or

modified to define the **destination IP address** of the second system to which logs will be forwarded.

🔁 This second system acts as an **intermediary**, receiving logs from the source machine and subsequently forwarding them to a centralized **enterprise log server** or **SIEM platform** 📊 for further analysis and storage.

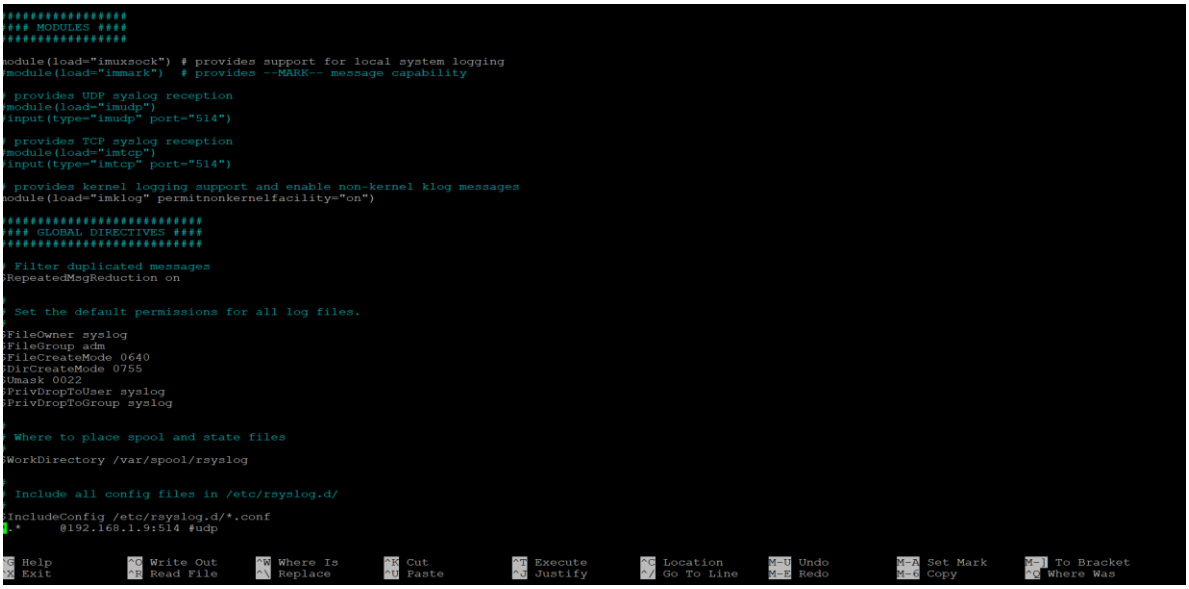
💡 At this point, you will need to **insert a specific configuration directive** into the rsyslog.conf file.

📜 An example of such a directive is:

. @192.168.1.9:514

📤 This line instructs rsyslog to **forward all log messages**—across all facilities and severity levels—to the **remote system** identified by the IP address 192.168.1.9 using **UDP on port 514** 🔁.

🚀 This setup is essential for enabling **real-time log transmission** from the local system to a remote **log collector or server** 📡.



⚙️ In the configuration syntax, the @ symbol signifies that the log messages should be forwarded using **UDP (User Datagram Protocol)** 📡.

🔁 If **TCP** is preferred for more reliable transmission, the @@ symbol should be used instead.

💾 After entering or modifying the required configuration line, **save the changes** in the Nano editor by:

- Pressing Ctrl + X to exit
- Pressing Y to confirm saving the changes
- Hitting Enter to finalize and return to the terminal ⌨️.