Installation Guide for LS-AUSS

1. Introduction

This guide provides a **step-by-step procedure** for installing, configuring, and executing the **Linux System Automation project** (/system_automation). The scripts automate critical tasks such as **disk monitoring, backups, process management, user provisioning, system health checks, and security auditing,** ensuring a more reliable and secure Linux environment.

2. Prerequisites

Supported Operating Systems

- Ubuntu 20.04+ (recommended)
- Debian 10+
- CentOS 7+ / RHEL 8+
- Fedora 34+

Required Packages & Dependencies

Ensure the following utilities are installed:

- sudo apt install mailutils net-tools tar cron procps gawk sed -y

- **mail** → Sends notifications
- **tar** → Creates and extracts backups
- **df** → Monitors disk space
- **pgrep** → Checks active processes
- **awk/sed** → Log parsing
- **cron** → Job scheduling
- **netstat** → Network monitoring
- **journalctl** → Security audit logs

Permissions

- Root (sudo) privileges required for user management, backup, and system auditing.
- Scripts must have executable permissions (chmod +x script.sh).

3. Installation Steps

Step 1: Clone or Copy the Project

- sudo mkdir -p /opt/system_automation
- sudo cp -r <project_source>/* /opt/system_automation/
- cd /opt/system_automation/scripts

Step 2: Set Permissions

- sudo chmod +x *.sh

Step 3: Configure Environment Variables (Optional)

Add the scripts directory to your PATH:

- echo 'export PATH=$PATH:/opt/system_automation/scripts' >> ~/.bashrc
- source ~/.bashrc

Step 4: Setup Cron Jobs

Schedule automated execution:

- crontab -e

Example entries:

- 0 8 * * * /opt/system_automation/scripts/master_script.sh # Run daily at 8 AM
- */30 * * * * /opt/system_automation/scripts/disk_monitor.sh # Run every 30 minutes

4. Execution Examples

Run Scripts Individually

./disk_monitor.sh # Check disk space

./user_management.sh # Add/Delete users

./backup.sh # Run backup

./process_monitor.sh # Restart failed services

./system_health.sh # Display CPU & memory usage

./security_audit.sh # Check failed SSH logins

./network_monitor.sh # Show open ports

./performance_logger.sh # Log performance metrics

Run All Scripts Together

./master_script.sh

5. Troubleshooting Tips

Issue	Possible Cause	Solution
Permission denied	Missing execution rights	Run chmod +x script.sh
Command not found	Utility not installed	Install via apt or yum
Cron job not running	Cron service disabled	sudo systemctl enable --now cron
Backup fails	Missing directory path	Edit backup.sh and verify source path
No mail alerts	Mail not configured	Install & configure mailutils

6. Best Practices

- Always test scripts in a staging environment before production.
- Store backups on a separate partition or external server.
- Monitor cron jobs with:
  - grep CRON /var/log/syslog