
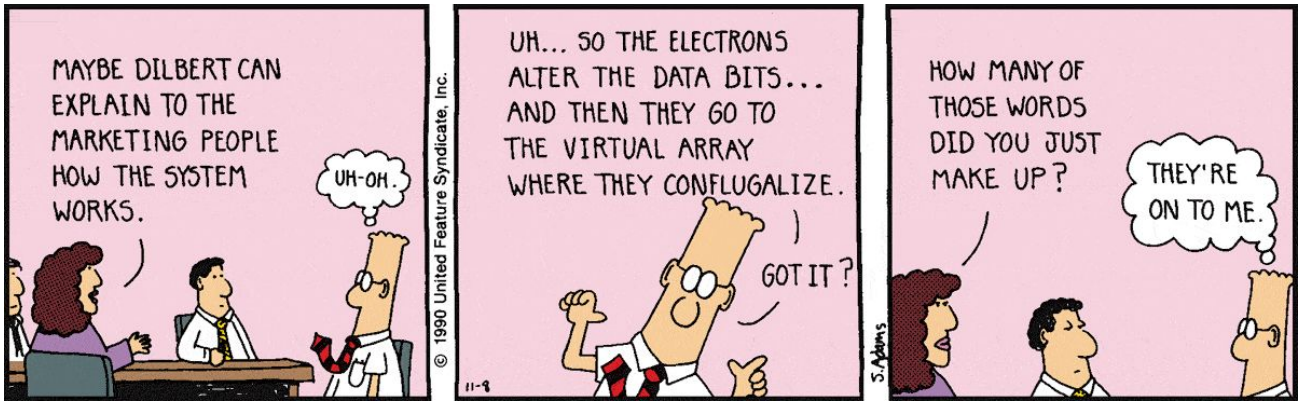


Waiting Room

# Role and Responsibilities

## Linux System Administrator

Source: opensource.com #redhat

Asst. Prof. Ashwini Mathur

**System administrators are critical to the reliable and successful operation of an organization and its network operations center and data center**

A sysadmin must have expertise with the system's underlying platform (i.e., Windows, Linux) as well as be familiar with multiple areas including networking, backup, data restoration, IT security, database operations, middleware basics, load balancing, and more.

Sysadmin tasks are not limited to server management, maintenance, and repair, but also any functions that support a smoothly running production environment with minimal (or no) complaints from customers and end users.

If you work in a sysadmin role (or hope to one day), make sure you are ready to follow these best practices.

# Documentation

Documentation is how sysadmins keep records of assets, including hardware and software types, counts, and licenses. Should there be any issues in the production environment, documentation helps identify the hardware, virtual machine, appliance, software, etc., that may be involved.

## Hardware inventory

Maintain lists of all your physical and virtual servers with the following details:

- **OS:** Linux or Windows, hypervisor with versions
- **RAM:** DIMM slots in physical servers
- **CPU:** Logical and virtual CPUs
- **HDD:** Type and size of hard disks
- **External storage (SAN/NAS):** Make and model of storage with management IP address and interface IP address
- **Open ports:** Ports opened at the server end for incoming traffic
- **IP address:** Management and interface IP address with VLANs
- **Engineering appliances:** e.g., Exalogic, PureApp, etc.

## Software inventory

- **Configured applications:** e.g., Oracle WebLogic, IBM WebSphere Application Server, Apache Tomcat, Red Hat JBoss, etc.
- **Third-party software:** Any software not shipped with the installed OS

## License details

Maintain license counts and details for physical servers and virtual servers (VMs), including licenses for Windows, subscriptions for Linux OS, and the license limit of hypervisor host.

# Server health check up

- **Running processes:** Check for processes that are consuming more resources than expected, and take action to fine-tune the applications (with the help of the application team).
- **CPU utilization:** Consistently monitor and check the CPU utilization of the critical process like "java", "http", "mysql" etc. to ensure that these are not consuming the CPU resources more than expected. If it is so, then coordinate with the application team to check it at application level  and fine tune the same. Parallely analyse the OS parameters like "Ulimits".
- **Memory utilization:** Check memory utilization and clear the cache, if required.
- **Zombie processes:** Check for processes where the PID still exists in the process table after it is terminated. Zombie processes degrade server performance, so find and kill any that exist.
- **Load average:** If you're having performance issues, check the load average and tune the server for performance.
- **Disk/SAN/NAS utilization:** Check the I/O reports for externally attached storage to track and check the speed of read/write operations. If you find any issues, coordinate with the storage and network teams immediately to correct them.

# Backup and disaster recovery planning

Communicate with the backup team and provide them the data and client priorities for backup. The recommended backup criteria for production servers is:

- **Incremental backups:** Daily, Monday to Friday
- **Full backup:** Saturday and Sunday
- **Disaster recovery drills:** Perform restoration mock drills once a month (preferably, or quarterly if necessary) with the backup team to ensure the data can be restored in case of an issue.

# Patching

Operating system patches for known vulnerabilities must be implemented promptly. There are many types and levels of patches, including:

- Security
- Critical
- Moderate

When a patch is released, check the bug or vulnerability details to see how it applies to your system (e.g., does the vulnerability affect the hardware in your system?), and take any necessary actions to apply the patches when required. Make sure to cross-verify applications' compatibility with patches or upgrades.

# Server hardening

**Linux:**

- **Set a BIOS password:** This prevents users from altering BIOS settings.
- **Set a GRUB password:** This stops users from altering the GRUB bootloader.
- **Deny root access:** Rejecting root access minimizes the probability of intrusions.
- **Sudo users:** Make sudo users and assign limited privileges to invoke commands.
- **TCP wrappers:** This is the weapon to protect a server from hackers. Apply a rule for the SSH daemon to allow only trusted hosts to access the server, and deny all others. Apply similar rules for other services like FTP, SSH File Transfer Protocol, etc.
- **Firewalld/iptables:** Configure firewalld and iptables rules for incoming traffic to the server. Include the particular port, source IP, and destination IP and allow, reject, deny ICMP requests, etc. for the public zone and private zone.
- **Antivirus:** Install antivirus software and update virus definitions regularly.
- **Secure and audit logs:** Check the logs regularly and when required.
- **Rotate the logs:** Keep the logs for limited period of time like "for 7 days", to keep the sufficient disk space for flawless operation.

# Use a syslog server

By configuring a syslog server in the environment to keep records of system and application logs, in the event of an intrusion or issue, the sysadmin can check previous and real-time logs to diagnose and resolve the problem.

# Automation

Many sysadmin tasks (such as server health checkups, resource utilization, backup triggers, transfer files and logs, etc.) must be done at specific times. Therefore, the sysadmin must write scripts or use external tools and configure them as cron jobs to do the tasks automatically at the proper time.

# Monitoring tools

Install and configure live monitoring tools like Nagios, HP, etc., to monitor your IT infrastructure and issue alerts about potential problems.