

008 Linux-Server-Administration und Wartung

Administration Aufgabe
Anforderungsniveau: Mittel

1 Ziel der Aufgabe

Diese Aufgabe beschreibt die Einrichtung, den Betrieb und die Wartung eines Linux-Servers für ein kleines Team (bis zu 15 Mitarbeitende). Schwerpunkte sind:

- Regelmäßige Paket- und Sicherheitsupdates.
- Umsetzung einer Backup- und Wiederherstellungsstrategie.
- Benutzer- und Rechtemanagement nach dem Least-Privilege-Prinzip.
- Absicherung des Systems (SSH-Härtung, Firewall, Eindringungserkennung).
- Monitoring der Systemressourcen und zentralisiertes Logging.
- Dokumentation aller Schritte und Konfigurationen.

2 Aufgabenbeschreibung

1. Basisinstallation und Erstkonfiguration

- *Betriebssystemwahl und Updates:*
 - Nutzen Sie eine virtuelle Maschine (z. B. in einer Cloud-Umgebung) mit Debian 12 oder Ubuntu 22.04 LTS.
 - Führen Sie nach der Installation zunächst ein vollständiges Update aller Pakete und Sicherheits-Patches durch.
- *Systembenutzer und SSH-Sicherheit:*
 - Legen Sie einen separaten Administrationsbenutzer an, der über sudo-Rechte verfügt, und deaktivieren Sie den direkten Root-Login.
 - Schränken Sie die SSH-Anmeldung auf Schlüsselbasierte Authentifizierung ein und wählen Sie einen alternativen Port.

- *Firewall-Konfiguration:*
 - Installieren und aktivieren Sie eine einfache Firewall (z. B. ufw). Blockieren Sie standardmäßig alle eingehenden Verbindungen und erlauben nur notwendige Dienste (SSH, Web-Ports).
 - Begrenzen Sie SSH-Zugriffe auf das interne Büro-Subnetz.

2. Benutzer- und Rechtemanagement

- *Gruppen und Nutzer:*
 - Richten Sie zwei Hauptgruppen („admins“ und „developers“) ein. Weisen Sie dem Administrationsbenutzer die Gruppe „admins“ zu.
 - Erstellen Sie für jeden Mitarbeitenden einen eigenen Benutzer und ordnen Sie sie der Gruppe „developers“ zu.
- *Verzeichnisrechte:*
 - Legen Sie ein zentrales Verzeichnis für Projekte an und setzen Sie die Eigentümergruppe auf „admins“ sowie restriktive Zugriffsrechte (z. B. rwxrwx—).
 - Stellen Sie sicher, dass nur Mitglieder der jeweiligen Gruppe Schreibzugriff haben.
- *Sudo-Konfiguration:*
 - Erlauben Sie Mitgliedern der Gruppe „admins“ die Nutzung von sudo ohne Passwortabfrage für notwendige Administrative Aktionen.
 - Dokumentieren Sie die erlaubten sudo-Befehle, um das Least-Privilege-Prinzip zu wahren.

3. Paketverwaltung und Systemaktualisierung

- *Unattended-Upgrades (optional):*
 - Installieren Sie das Paket für automatische Sicherheitsupdates und konfigurieren Sie es so, dass kritische Sicherheits-Patches automatisch eingespielt werden.
- *Geplanter Wartungs-Task:*
 - Erstellen Sie ein Skript oder eine Anweisung, die wöchentlich alle Pakete aktualisiert und veraltete Pakete entfernt.
 - Richten Sie einen Cron-Job ein, der dieses Skript regelmäßig ausführt und die Ausgabe in eine Log-Datei schreibt.

4. Backup-Strategie

- *Backup-Skript:*
 - Entwickeln Sie ein einfaches Skript, das wichtige Verzeichnisse und Konfigurationsdateien (z. B. /etc, /home, /srv/projects) in komprimierte Archive sichert.
 - Fügen Sie optional einen MySQL/MariaDB-Dump hinzu, falls eine Datenbank im Einsatz ist.
 - Stellen Sie sicher, dass alte Backups (älter als 7 Tage) automatisch gelöscht werden.
- *Cron-Job für Backups:*
 - Planen Sie das Backup-Skript so, dass es einmal täglich in den frühen Morgenstunden ausgeführt wird.
 - Leiten Sie die Protokollausgabe in eine Log-Datei um, um den Ablauf nachvollziehen zu können.
- *Remote-Sicherung (optional):*
 - Richten Sie eine SSH-Verbindung zu einem externen Backup-Server ein und übertragen Sie die erstellten Archive per rsync.
 - Planen Sie gegebenenfalls einen separaten Cron-Job für die Synchronisation.
- *Wiederherstellungstests:*
 - Spiegeln Sie mindestens einmal monatlich ein Backup auf einer Testinstanz und verifizieren Sie, dass alle Daten und Dienste korrekt wiederhergestellt werden können.
 - Dokumentieren Sie jeden Schritt im Wiederherstellungsvorgang in einem Testprotokoll.

5. Sicherheit und Systemhärtung

- *SSH-Härtung:*
 - Deaktivieren Sie Passwort-Authentifizierung, erlauben Sie ausschließlich Schlüssel-basierte Logins und begrenzen Sie Login-Versuche durch Fail2Ban oder ein ähnliches Werkzeug.
 - Schalten Sie ungenutzte SSH-Optionen (z. B. TCP-Weiterleitungen) ab.
- *Firewall-Feinabstimmung:*
 - Schließen Sie alle Ports, die nicht aktiv benötigt werden. Überprüfen Sie laufend offene Dienste und Ports.

- *Dateisystem-Berechtigungen:*
 - Setzen Sie restriktive Rechte für sensible Konfigurationsverzeichnisse (z. B. SSL-Schlüssel, /root).
 - Stellen Sie sicher, dass nur berechtigte Benutzer Lese- und Schreibzugriff haben.

6. Monitoring und Logging

- *Monitoring-Agent:*
 - Installieren Sie einen Agenten wie den Prometheus Node Exporter oder den Zabbix-Agenten, um Metriken (CPU, RAM, Festplattenplatz) zu sammeln.
 - Konfigurieren Sie den Dienst als Systemd-Unit und starten Sie ihn automatisch mit dem System.
- *Logrotate:*
 - Legen Sie für eigene Log-Dateien (z. B. Backup- oder Update-Logs) eine eigene Logrotate-Konfiguration an, um wöchentliche Drehung, Komprimierung und begrenzte Aufbewahrung festzulegen.
- *Zentrales Logging:*
 - Richten Sie rsyslog oder einen vergleichbaren Dienst so ein, dass wichtige Log-Einträge an einen zentralen Log-Server weitergeleitet werden.
 - Testen Sie die Weiterleitung und prüfen Sie, ob alle relevanten Log-Kategorien (Auth, Syslog, Anwendungslogs) erfasst werden.
- *Alarmierung:*
 - Definieren Sie in Ihrem Monitoring-System (z. B. Prometheus Alertmanager oder Zabbix) Benachrichtigungen, die bei kritischen Zuständen (z. B. CPU-Auslastung über 80 %, Festplattenspeicher unter 10 %) eine E-Mail an das Administrations-Team senden.
 - Dokumentieren Sie, wie ein Alarm ausgelöst und wie auf ihn reagiert wird.

7. Dokumentation und Übergabe

- *Administrationshandbuch:*

- Erstellen Sie ein Handbuch (z. B. als Markdown- oder PDF-Dokument), das alle Konfigurationsdateien (SSH, Firewall, Backup-Skript, Monitoring-Unit) enthält.
- Erklären Sie in jedem Abschnitt klar die einzelnen Schritte – etwa „So legen Sie einen neuen Benutzer an“ oder „So konfigurieren Sie automatische Updates“.
- *Serverübersicht:*
 - Legen Sie eine Übersicht an, in der Hostname, IP-Adresse, Betriebssystem-Version, SSH-Port, installierte Dienste und FQDN vermerkt sind.
- *Notfall-Übergabeprozess:*
 - Definieren Sie, wie bei einem Ausfall des Hauptadministrators ein zweiter Administrator schnell eingreifen kann:
 - * Ort der Zugangsdaten (z. B. in einem verschlüsselten Passwort-Manager).
 - * Pfad zum Administrationshandbuch auf dem Server.
 - * Kontaktinformationen für Eskalationen (Telefon, E-Mail).

3 Anforderungen

- **Automatisierung:** Verwenden Sie Skripte und Cron-Jobs, um wiederkehrende Aufgaben zu minimieren. Optional können Sie Ansible-Playbooks verwenden.
- **Sicherheit:** Halten Sie das Least-Privilege-Prinzip ein (keine unnötigen Root-Aktionen, restriktive Dateirechte, Schlüssel-basierte SSH-Logins, Fail2Ban).
- **Dokumentation:** Dokumentieren Sie alle Konfigurationsschritte und Abläufe in einem klar strukturierten Handbuch.
- **Testumgebung:** Testen Sie Backup- und Wiederherstellungsprozesse auf einer separaten Instanz und protokollieren Sie die Ergebnisse.
- **Skalierbarkeit:** Geben Sie Hinweise, wie bei steigendem Nutzeraufkommen (z. B. Load Balancer, Cluster, zusätzliche Backup-Knoten) vorgegangen werden kann.

Viel Erfolg bei der Umsetzung!

Stand: 31. Mai 2025