Benutzerhandbuch

LDAP-Server

Benutzerhandbuch für den LDAP-Server: hamster.panzer

Serverinformationen:

- **Domain Name**: hamster.panzer
- **IP-Adresse**: 192.168.56.100
- **Betriebssystem**: Ubuntu Biotic

LDAP-Benutzer und Gruppenverwaltung

Hinzufügen eines Benutzers:

1. Erstellen einer LDIF-Datei mit folgendem Inhalt:

dn: uid=<Benutzername>,ou=people,dc=hamster,dc=panzer

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: top

cn: <Benutzername>

sn: <Nachname>

uid: <Benutzername>

uidNumber: <UID>

gidNumber: <GID>

homeDirectory: /home/<Benutzername>

loginShell: /bin/bash

userPassword: {SSHA}<Passwort>

2. Hinzufügen eines Benutzers mit folgendem Befehl:

l***dapadd -x -D cn=admin,dc=hamster,dc=panzer -W -f <Dateiname.ldif>***

Entfernen eines Benutzers:

Löschen eines Benutzers mit folgendem Befehl

```
ldapdelete -x -D cn=admin,dc=hamster,dc=panzer -W
"uid=<Benutzername>,ou=people,dc=hamster,dc=panzer"
```

Hinzufügen einer Gruppe:

1. Erstellen einer LDIF-Datei für die Gruppe:

```
dn: cn=<Gruppenname>,ou=groups,dc=hamster,dc=panzer
objectClass: posixGroup
cn: <Gruppenname>
gidNumber: <GID>
```

Hinzufügen der Gruppe mit folgendem Befehl:

```
ldapadd -x -D cn=admin,dc=hamster,dc=panzer -W -f <Dateiname.ldif>
```

Modifizieren eines Benutzers oder einer Gruppe:

1. Erstellen einer LDIF-Datei für die gewünschten Änderungen, z.B.

```
dn: uid=<Benutzername>,ou=people,dc=hamster,dc=panzer
changetype: modify
replace: loginShell
loginShell: /bin/zsh
```

Anwenden der Änderungen:

```
ldapmodify -x -D cn=admin,dc=hamster,dc=panzer -W -f
<Dateiname.ldif>
```

Betrieb und Wartung

LDAP-Server Status anzeigen:

sudo systemctl status slapd

LDAP-Server neu starten:

sudo systemctl restart slapd

LDAP-Logs einsehen:

tail -f /var/log/syslog | grep slapd

LDAP-Datenbank sichern:

sudo slapcat -v -l /backup/ldap-$(date +%F).ldif

LDAP-Datenbank wiederherstellen:

1. LDAP-Server stoppen:

   sudo systemctl stop slapd

2. Datenbank importieren:

   sudo slapadd -v -l /backup/ldap-<Datum>.ldif

3. LDAP-Server starten:

   sudo systemctl start slapd

Aktualisierung und Upgrade des Systems:

sudo apt update && sudo apt upgrade -y

Sicherheit und zusätzliche Software

ClamAV:

- **Status des Daemons überprüfen**:

  sudo systemctl status clamav-daemon

- **Manueller Virenscan:**

  sudo clamscan -r /pfad/zum/verzeichnis

- **Aktualisierung der Virendatenbank:**

  sudo freshclam

Fail2Ban:

- **Status überprüfen:**

  sudo systemctl status fail2ban

- **Logs anzeigen:**

  sudo fail2ban-client status sshd

- **Konfiguration neu laden:**

  sudo systemctl reload fail2ban

RKHunter:

- **System auf Rootkits überprüfen:**

  sudo rkhunter --checkall

- **Datenbank aktualisieren:**

  sudo rkhunter --update

UFW:

- **Firewall-Status anzeigen:**

  sudo ufw status

- **Regeln hinzufügen:**

  sudo ufw allow <port/service>

AppArmor:

- **AppArmor Status anzeigen:**

  sudo aa-status

- **Profile aktivieren**

  sudo aa-enforce /etc/apparmor.d/<profile>

Snort:

- **Snort-Dienst Status anzeigen:**

  sudo systemctl status snort

- **Logs anzeigen:**

  sudo tail -f /var/log/snort/alert

Suricata:

- **Suricata-Dienst Status anzeigen:**

  sudo systemctl status suricata

- **Suricata-Konfiguration testen:**

  sudo suricata -T -c /etc/suricata/suricata.yaml

SSH

SSH-Dienst Status anzeigen:

sudo systemctl status ssh

SSH-Dienst neu starten:

sudo systemctl restart ssh

Konfigurationsdatei ändern:

- Datei bearbeiten:

  sudo nano /etc/ssh/sshd_config

- Änderungen anwenden:

  sudo systemctl restart ssh

SSH-Troubleshooting:

- **Logs anzeigen:**

  sudo journalctl -u ssh
