Kommandos und Dateien/Verzeichnisse LPI 202

Netzwerk

Allgemeine Netzwerk-Konfiguration
/sbin/ifconfig - konfiguriert Netzwerkinterface
/sbin/arp - manipuliert System-ARP-Cache
/usr/sbin/arpwatch - ARP-Überwachung
/sbin/route - manipuliert IP-Routingtabelle
mgetty - Login via Modem
setserial - Einstellen der seriellen Schnittstelle
/etc/ppp/pap-secrets - Authentifizierugsdaten
/etc/ppp/chap-secrets - Authentifizierugsdaten
/etc/ppp/options.server – pppd-Optionen (IP-Adressen)
Fortgeschrittene Netzwerk-Konfiguration und Problemlösungen
/bin/netstat - listet Verbindungen und Routen
/bin/ping - sendet Echoanforderungen
/usr/sbin/tcpdump - snifft Netzwerkverkehr
/usr/sbin/lsof - listet geöffnete Dateien
/usr/bin/nc -

Mail & News

Konfiguration von Mailing-Listen
wrapper - Parser für Majordomo
/etc/aliases - Weiterleitung einer Mail an Majord.
/var/lib/majordomo/lists - Hauptverzeichnis
listenname - Datei mit Mitgliederliste
listenname.info - Beschreibung der Mailingliste
listenname.config - Konfigurationsdatei
info listenname - Listenbeschreibung abfragen
who listenname - Mitgliederliste abfragen
subscribe listenname - abbonieren
unsubscribe listenname - abbestellen
help - generelle Hilfe
lists - Abfrage aller Majordomo-Listen
Verwendung von Sendmail
/usr/sbin/sendmail- Binärprogramm des Servers
/etc/aliases - Adress-Alias auf existierende User
newaliases - Umwandeln in Binär-DB-Format
makemap hash - allg. Umwandeln ins Binärformat
sendmail.cw - Aliasnamen für localhost
local-host-names - neuer Name der sendmail.cw
virtusertable - übersetzt eingehende Adressen (Adressaten)
genericstable - übersetzt ausgehende Adressen (Absender)
mailertable - Mailrouting für externe Mails
Verwaltung von Mail-Verkehr
procmail - Mail-Delivery-Agent
~/.procmailrc - Konfigurationsdatei
Bereitstellen von News
innd - Hauptdaemon, direkte Verteilung der News
/etc/news/inn.conf - Hauptkonfigurationsdatei
ctlinnd - Anlegen und Löschen von Newsgroups
Weiterverteilung:
innfeed - Senden von News (real time)
innxmit - ausgehende News an Server senden (batch)
nntpsend - w. o.
nnrpd - beantwortet Anfragen von Newsreadern
Abholen:
nntpget - Abholen von News-Artikeln
rnews - Abholen per UUCP

DNS

Allgemeine BIND 8 Konfiguration
/etc/named.boot - Konfigurationsdatei bis bind7
/etc/named.conf - Konfigurationsdatei ab bind8
named-bootconf - konvertiert Konfig V4 nach V8/9
kill - Beeinflussung des DNS-Daemons
ndc - wie kill, Batch oder interaktiv
/var/run/ndc - Socket zur Kommunikation mit ndc
Anlegen und Verwalten von DNS-Zonen
/var/named - Ablage der Zonendateien
dig - stellt NS-Anfragen
nslookup - stellt NS-Anfragen
host - stellt NS-Anfragen
Absichern eines DNS-Servers
/etc/passwd - andere UID für named
chroot - erzeugt virtuelles Wurzelverzeichnis
dnskeygen - generiert Schlüsselpaar für DNS
dnssigner - signiert DNS-Antworten mit priv. key

Webdienste

Implementierung eines Webservers
httpd.conf - Haupt-Konfigurationsdatei
apxs - Einbinden von externen Modulen
access.log - definierte Zugriffs-Logdatei
.htaccess - Rechtevergabe durch Anwender
mod_auth - für Benutzerauthentifizierung (DAC)
mod_access - für Host- und Netz-Access (MAC)
htpasswd - Erzeugen von Passwörtern
htgroup - Verwaltung der Gruppendatei
NameVirtualHosts -Einleitung virtueller Hosts
openssl genrsa - erzeugt Schlüsselpaar für SSL (.key)
openssl req - Zertifikatsantrag (.csr)
openssl x509 - Zertifikat selbst unterzeichnen (.crt)
Verwaltung eines Webservers
httpd.conf - w. o.
Implementierung eines Proxy-Servers
squid.conf - Hauptkonfigurationsdatei
acl name type element - Syntax ACLs
directive all/den aclname - Syntax Direktive
http_access - zwingende Direktive für HTTP

Verwaltung von Netwerk-Clients

DHCP Konfiguration
dhcpd.conf - Hauptkonfigurationsdatei
dhcpd.leases - Adressdatenbank (zwingend)
Konfiguration von NIS
domainname - setzt Namen der NIS-Domäne
/etc/defaultdomain - ordnet Client einer Dom. zu
nisupdate - Skript der Webmin-Suite?
ypbind - findet zuständigen NIS-Server
ypcat - Ausgabe beliebiger Map-Dateien
ypmatch - liefert Werte eines Keys einer Map
ypserv - Binary des NIS-Daemons
ypswitch -
yppasswd - ändert NIS-Passwort (nicht lokal)
ypchsh - ändert NIS-Benutzershell
ypchfn - ändert NIS-Benutzerkommentar
ypinit –m - Skript zum aut. Erzeugen der Maps

yppoll - Zeitst. und Masterserver einer Map
yppush - geänderte Maps an Slave senden
rpc.ypxfrd - beschleunigt Maptransfer vom Master
ypwhich - Name des Masters einer Map
ypset NIS-Server - fordert neuen NIS-Server an
rpcinfo - Kontrolle des Portmappers
nis.conf -
nsswitch.conf - verwaltet Systemdatenbanken
ypserv.conf - NIS-Server-Konfigurationsdatei
/etc/netgroup - fasst Netzwerkbenutzer zusammen
/etc/nis/nicknames- Zweitnamen der Maps
/etc/nis/securenets - erlaubt Zugriff aus diesen Netzen
/var/yp/Makefile - Infos zum Erstellen der Maps

Konfiguration von LDAP

slapd - Server-Binary
slapd.conf - Server-Konfigurationsdatei
ldap.conf - Client-Konfigurationsdatei
*.ldif - Dateiformat der LDAP-Datenpflege
ldapadd - Hinzufügen von Datensätzen
ldapmodify - Ändern von Datensätzen
ldapmodrdn - Umbenennen kompletter Objekte
ldapsearch - Suchen und Auslesen von Daten
ldapdelete - Löschen von Datensätzen
ldappasswd - setzt Passwort in LDAP-Datenbank
slurpd - Replikationsdienst

Authentisierung mittels PAM

/etc/pam.d/ - Verzeichnis zur PAM-Konfiguration
/etc/pam.d/other - konfiguriert alle Dienste ohne K.datei
pam.conf - alternative Konfigurationsdatei
/etc/security/ - Konfiguration komplexerer Module
/lib/security - Speicherort der PAM-Module

Systemsicherheit

Konfiguration eines Routers

/proc/sys/net/ipv4 - Kernelparameter für IP
…/ipv4/conf/eth0/ - Kernelparameter für Interfaces
/etc/services - Zuordnung Portnummer zu Dienst
ipfwadm - Firewall-Konfiguration Kernel 2.0
ipchains - Firewall-Konfiguration Kernel 2.2
ipmasqadm - Portforwarding bei Kernel 2.2
iptables - Firewall-Konfiguration Kernel 2.4
iptables-save - Sichern der Einstellungen in Kdoform
iptables-restore - Einspielen der Konig.sicherung
PortSentry - verhindert Portscans (IDS)
routed - dynamisches Routing

Absichern eines FTP-Servers

/etc/ftpaccess - Zugriffsverwaltung wuFTP
/etc/ftpusers - Benutzer mit FTP-Verbot
/etc/ftphosts - Benutzerzugriff von einem Host
/etc/ftpgroups - zusätzliche Gruppenrechte
/etc/ftpchroot - diese Benutzer landen im chroot
/etc/passwd - enthält anonymous-Konto
ftpmsg.dead - Textdatei für ftpaccess-Direktiven
chroot - neue Dateisystemwurzel

Secure Shell (OpenSSH)

ssh - Client-Binary
sshd - Server-Binary
ssh-keygen - Erzeugen von User-Schlüsseln
ssh-agent - Verwalten der Passphrasen
ssh-add - Verwalten der Passphrasen
/etc/ssh/sshd_config -Hauptkonfigurationsdatei Server
~/.ssh/identity[.pub] - User-Schlüsselpaar Version 1
~/.ssh/id_dsa[.pub] - User-Schlüsselpaar DSA Ver. 2
~/.ssh/authorized_keys –Benutzerschlüssel der Clients
.shosts - Benutzeräquivalenzen nur für SSH
.rhosts - Benutzeräquivalenzen r-Utilities
/etc/ssh/host_key[.pub] - Hostkey V1
/etc/ssh/host_r(s|d)a_key[.pub] - Hostkey V2

TCP_wrappers

inetd.conf - Konfigurationsdatei für inetd
tcpd - Zugriffskotrolle für Internetdienste
hosts.allow - Zugriffsregeln für tcpd
hosts.deny - Zugriffsregeln für tcpd
xinetd - extended inetd
tcpdchk - tcpd Konfigurations-Checker
tcpdmatch - simuliert Client-Zugriff auf Server

Security-Tätigkeiten

kerberos - verteilter Authentifizierungsdienet
/etc/krb5.conf - Kerberos-Konfigurationsdatei
kadmin addprinc - Hinzufügen eines Prinzipals
telnet - checkt Funktion von Protokollen
Tripwire - checkt Dateisystem-Integrität
aide - checkt Dateisystem-Integrität
md5sum - checkt Dateisystem-Integrität
snort - Intrusion Detection System
LIDS - Linux Intrusion Detection System
Bugtraq - Mailingliste für Sicherheitsprobleme
CERT - Center of internet security expertise
CIAC - Computer Incident Advisory Capabil.

Lösen von Netzwerkproblemen

Lösen von Netzwerkproblemen

/sbin/ifconfig - konfiguriert Netzwerkinterface
/sbin/route - listet und managet Routingtabelle
/bin/netstat - listet Verbindungen und Routen
/etc/network - Netzwerknamen in Netzwerk-IDs
/etc/sysconfig/network-scripts/
/var/log/syslog - Konfigdatei syslog
/var/log/messages - Haupt-Konfigurationsdatei
/bin/ping - sendet Echoanforderungen
/etc/resolv.conf - legt Nameserver und Suchdomain fest
/etc/hosts - Rechnernamen in IPs
/etc/hosts.allow - erlaubt Rechnerzugriffe
/etc/hosts.deny - verbietet Rechnerzugriffe
/etc/hostname -
/etc/HOSTNAME- enthält FQDN des Rechners
/etc/netgroup - Netzgruppen für NFS, NIS, r-utilities
/sbin/hostname - listet Rechnernamen ohne Domain
/usr/sbin/traceroute - listet die Router zum Zielrechner
/usr/bin/nslookup- interaktive Nameserverabfrage
/usr/bin/dig - DNS lookup Utility
/bin/dmesg - listet Kernel-Ringbuffer
host - DNS lookup Utility