

Linux

Benutzer/Gruppen/Rechte

Proseminar SS 2008

Student: Tien Duc Dinh

Betreuer: Olga Mordvinova, Julian M. Kunkel

Datum: 20-5-2008

Gliederung

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- normale Rechte
- spezielle Rechte
- chmod
- chown
- umask
- Access Control Lists

Einführung (1)

- zu den wichtigsten Eigenschaften von Linux zählt sicher die Fähigkeit zu echtem **Multitasking** und zum **Multiuser-Betrieb**
- "**Multitasking**" bedeutet dabei, dass mehrere Prozesse (englisch "tasks") parallel ablaufen, und sich dabei die vorhandenen Ressourcen teilen
- "**Multiuser**" bedeutet, dass mehrere Benutzer gleichzeitig am System arbeiten und damit die Multitasking-Fähigkeiten des Systems nutzen können
- hierbei trennt das Betriebssystem die einzelnen Benutzer, die von diesen Benutzern gestarteten Prozesse/Tasks sowie die von ihnen angelegten Dateien und Verzeichnisse voneinander und kontrolliert restriktiv den Zugriff darauf.
- in der Windows-Welt ist dieser Multiuser-Betrieb wenig bekannt. Zwar ist es auch unter Windows z. B. möglich, mehrere Benutzer auf demselben System anzulegen. Diese können im Normalfall aber nicht gleichzeitig an diesem System arbeiten.

Einführung (2)

Wie kann man alles verwalten ?

→ Benutzer-/Gruppen-/Rechteverwaltung

Benutzer/Gruppen

/etc/passwd

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- diese Datei enthält Informationen über Benutzer und die Abbildung von Benutzernamen auf die UID
- gehört root mit dem Recht rw- und ist für alle anderen Benutzer nur lesbar
- eine Zeile hat 7 Felder und sie werden durch “:” voneinander getrennt
 - Benutzername
 - Passwort
 - UID
 - GID
 - Kommentar
 - Heimatverzeichnis
 - Shell
- z.B.
 - root:x:0:0:Herr und Meister:/root:/bin/bash

UID/GID

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- jeder Benutzer und jede Gruppe im System hat eine eindeutige ID zur Verwaltung
- verschiedene IDs
 - RUID/RGID: entspricht dabei der Identität des Benutzers, der den Prozess gestartet hat
 - EUID/EGID: ist für Rechteprüfungen benötigt. Der Administrator kann diese ID bei bestimmten Programmen durch das Setzen des SetUID-Flags in der Rechtenmaske verändern
 - SUID/SGID: Diese Rechte werden auf Dateien gesetzt, die nicht mit den Rechten des ausführenden Users, sondern mit denen des Eigentümers beziehungsweise der Gruppe der Datei ausgeführt werden sollen
 - FSUID und FSGID: Unter Linux ist die FSUID die Identität für den Zugriff auf das Dateisystem und normalerweise mit der EUID identisch - so wird auch die FSUID verändert, wenn die EUID neu gesetzt wird. Jedoch hat man unter Linux über den Syscall setfsuid() die Möglichkeit, diese Identität gesondert zu verändern

shadowsuite (/etc/shadow)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- nur root hat Zugriffsrechte auf die Datei /etc/shadow
- in der Datei selbst steht nur die Kombination von Benutzernamen und Passwort
- Eine Zeile hat 9 Felder:
 - Benutzername
 - verschlüsseltes Passwort
 - letzte Änderung
 - minimale Gültigkeitsdauer
 - maximale Gültigkeitsdauer
 - Vorwarnzeit
 - Inaktivität
 - Accountende
 - Kennzeichen
- z.B.
 - jploetner:\$1\$QJgtvoES\$Ji/rS...Zrbq1:12201:0:99999:7:::

/etc/gshadow

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- nur root hat Zugriffsrechte
- ähnlich wie bei /etc/passwd und /etc/shadow werden /etc/group und /etc/gshadow für die Gruppen benutzt
- Eine Zeile hat 4Felder:
 - Gruppenname
 - Gruppenpasswort
 - Gruppenadministratoren
 - Gruppenmitglieder
- z.B.
 - test2:cO2b2WXiFGV2E::peter-dinh, kevin

SU

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- mit “su” kann man als root oder einen anderen Benutzer arbeiten
- mit “su – Benutzername” wird das Arbeitsverzeichnis auf das Homeverzeichnis des neuen Benutzers gesetzt
- z.B.
 - duc@host:/home/duc\$ su
 - Passwort: *****
 - root@vn:/home/duc# su - saigon
 - saigon@vn:~\$

sudo

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- mit sudo kann man Prozesse mit den Rechten eines anderen Benutzers (z.B. des Superusers root) starten
- ist kein Benutzer über die Option -u direkt angegeben, wird root als neue Identität genommen
- z.B.
 - peter-dinh@peter:~\$ sudo mkdir /home/test
 - peter-dinh@peter:~\$ sudo -u kevin mkdir /home/kevin/test

LDAP (1)

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- Lightweight Directory Access Protocol
- LDAP ist wie NIS ein Verzeichnisdienst (eine im Netzwerk verteilte hierarchische Datenbank), der jedoch nicht auf RPC basiert
- LDAP basiert auf dem Client/Server-Modell

LDAP (2)

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- LDAP hat im Vergleich zu einer normalen relationalen SQL-Datenbank folgende Vorteile:
 - LDAP ist für lesende Zugriffe optimiert
 - LDAP unterstützt verschiedene flexible Suchfunktionen, um lesende Zugriffe zu optimieren
 - LDAP unterstützt die Erweiterung von zugrunde liegenden Datenstrukturen
 - LDAP ist ein in verschiedenen RFCs spezifiziertes Protokoll, wodurch die Interoperabilität zwischen verschiedenen Implementierungen gewährleistet wird
 - Daten können im Netz verteilt gespeichert werden. LDAP nutzt außerdem verschiedene Replizierungstechniken, um die Daten im Netzwerk zu verteilen und vor allem konsistent zu halten
 - LDAP ist sehr gut skalierbar

LDAP (3)

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- LDAP-Eintrag (engl. “entry”) besteht aus Attributen und wird durch einen eindeutigen Namen (engl. “distinguished name”, dn) identifiziert
 - cn=Sebastian,ou=members,dc=doomed-reality,dc=org
- welche Attribute ein Eintrag haben kann, wird von dessen Objektklasse(n) bestimmt. Diese Objektklassen werden wiederum in Schemata definiert, dort ist festgelegt, wie die Attribute einer Objektklasse heißen, welche Werte zulässig sind und ob das Attribut unbedingt notwendig oder optional ist

LDAP (4)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

■ LDAP-Server konfigurieren (/etc/ldap/slapd.conf)

- **Bsp:**
- # Beispiel für die Domain doomed-reality.org
- suffix "dc=doomed-reality,dc=org"
- # Schema and objectClass definitions
- include /etc/ldap/schema/core.schema
- include /etc/ldap/schema/cosine.schema
- # Zugriffsrechte
- access to attrs=userPassword
- by dn="cn=admin,dc=doomed-reality,dc=org" write
- by anonymous auth
- by self write
- by * none
- access to *
- by dn="cn=admin,dc=doomed-reality,dc=org" write
- by * read

LDAP (5)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- LDAP gibt die Möglichkeit, Einträge hinzufügen, verändern und löschen
 - es gibt dafür momentan verschiedene Benutzerschnittstellen, z.B. die **ldap-utils** für die Kommandozeile und das Webinterface **phpldapadmin**

PAM (1)

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- Pluggable Authentication Module (PAM)
- ist eine Softwarebibliothek, die eine allgemeine Programmierschnittstelle (API) für Authentisierungsdienste zur Verfügung stellt
- alle neueren Login-Dienste setzen auf PAM als Interface zur Verifikation von Benutzerauthentifizierungen auf
- Statt die Einzelheiten der Authentisierung in jeder Applikation neu zu formulieren, bietet die PAM-API einen standardisierten Dienst in Form von Modulen an. In einer Konfigurationsdatei kann der Systemadministrator die Authentisierungsmodule einzelnen Diensten zuordnen, ohne dafür die Software, die diese Dienste realisiert, neu kompilieren zu müssen.

PAM (2)

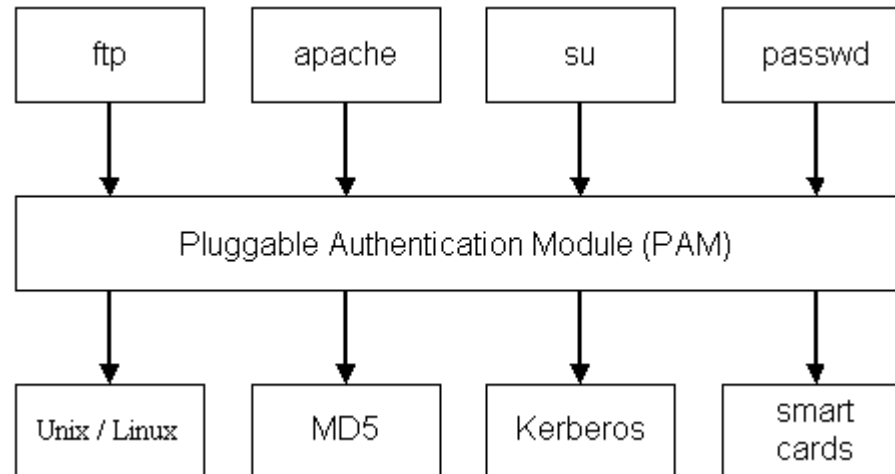
- PAM wird in der Praxis häufig dafür eingesetzt verschiedenste Serverdienste, wie SSH und FTP mit nur einem Authentisierungsdienst zu verbinden. Dies ermöglicht die zentrale Speicherung der Anmeldedaten dieser Dienste. Wird das Passwort an der zentralen Stelle geändert, kann man sich bei allen Diensten direkt mit dem neuen, zentral gespeicherten, Passwort anmelden. Getrennte Passwortdatenbanken für einzelne Dienste sind nicht notwendig

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists



Rechte

normale Rechte

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- jede Datei besitzt einen Eigentümer (u) und ist einer Gruppe (g) zu geordnet
- für diese beiden sowie für alle anderen (o) werden nun jeweils drei Rechte vergeben oder verweigert: lesen (r), schreiben (w) und ausführen (x)
- nur der Eigentümer oder root kann diese Rechte verändern
- mit “ls -l” kann man die Rechte anzeigen
 - peter-dinh@peter:~\$ ls -l
 - drwxr-xr-x 8 peter-dinh peter-dinh 4096 2008-01-04 13:15 backup
 - drwxr-xr-x 3 peter-dinh peter-dinh 4096 2008-03-22 23:47 bsp
 - -rwxr-xr-x 1 peter-dinh peter-dinh 60 2008-01-07 00:00 cc2
 - -----
 - Rights Owner Group Size Timestamp Name

SUID und SGID (1)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- SUID (Set User ID) und SGID (Set Group ID) werden durch ein s anstelle eines x bei den Eigentümer- und bei den Gruppenrechten ausgedrückt
- das s-Recht an einer ausführbaren Datei bedeutet, daß der Benutzer, der es startet, während des Programmlaufes die UID des Dateibesitzers bzw. die GID der Besitzergruppe erhält. Das hängt davon ab, ob das s beim Besitzer oder der Besitzergruppe steht. Im Falle des Programms /bin/passwd wird man z. B. während des Programmlaufs zum Superuser!
- z.B.
 - peter-dinh@peter:~\$ ls -l /etc/passwd /etc/shadow /usr/bin/passwd
 - -rw-r--r-- 1 root root 1377 2008-03-20 12:55 /etc/passwd
 - -rw-r----- 1 root shadow 911 2008-03-20 12:54 /etc/shadow
 - -rwsr-xr-x 1 root root 29104 2007-05-18 11:59 /usr/bin/passwd

SUID und SGID (2)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- wird das SGID-Recht auf ein Verzeichnis gegeben, so hat es eine andere Funktion. In diesem Fall erhalten alle Dateien, die in diesem Verzeichnis erstellt werden, automatisch die gleiche Gruppe, die auch dem Verzeichnis zugeordnet ist

■ z.B.

- peter-dinh@peter: ls -l
- drwxr-sr-x 2 peter-dinh test2 4096 2008-03-22 22:21 bsp
- peter-dinh@peter: su
- root@peter:~/bsp\$ touch a b && ls -l
- total 0
- -rw-r--r-- 1 root test2 0 2008-03-22 22:27 a
- -rw-r--r-- 1 root test2 0 2008-03-22 22:27 b

Sticky-Bit

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- das Sticky-Bit wird heutzutage meistens auf Verzeichnissen gesetzt
- nur root oder der Eigentümer können Dateien löschen oder umbenennen
- ist das Sticky-Bit nicht gesetzt, kann jeder Benutzer mit dem Schreibrechte auf das Verzeichnis Dateien löschen oder umbenennen
- auf Dateien ist dieses Bit mittlerweile unüblich und wird je nach Unix-Derivat sogar ignoriert
- mit “chmod +t” kann man das Sticky-Bit setzen

chmod

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- mit chmod kann man Rechte von Dateien verändern
- mode kann entweder eine symbolische Representation (laut man-page '[ugoa...][[+ -=][rwxXstugo...]....][, ...]'), oder eine oktale Darstellung des Rechtebitmusters sein
- eine Oktaldarstellung besteht aus 4 Ziffern, z.B. Z1, Z2, Z3, Z4.
 - Z1: setuid, setgid, sticky-bit
 - Z2, Z3, Z4: Lesen, Schreiben, Ausführen für Eigentümer, Gruppe und alle anderen
- z.B.
 - peter-dinh@peter:~/bsp\$ chmod 741 datei.file
 - peter-dinh@peter:~/bsp\$ ls -l datei.file
 - -rwxr----x 1 peter-dinh peter-dinh 0 2008-03-22 23:17 datei.file
 - peter-dinh@peter:~/bsp\$ chmod 1000 datei.file
 - peter-dinh@peter:~/bsp\$ ls -l datei.file
 - -----T 1 peter-dinh peter-dinh 0 2008-03-23 12:45 datei.file

chown

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- mit chown kann man den Eigentümer und die Gruppe verändern
- Optionen:
 - user:group
 - user:
 - group: (äquivalent zu chgrp)
- z.B.
 - peter-dinh@peter:~/bsp\$ ls -l
 - -rw-r--r-- 1 peter-dinh peter-dinh 0 2008-03-22 23:47 test
 - peter-dinh@peter:~/bsp\$ sudo chown kevin:kevin test
 - peter-dinh@peter:~/bsp\$ ls -l
 - -rw-r--r-- 1 kevin kevin 0 2008-03-22 23:47 test
 - peter-dinh@peter:~/bsp\$ sudo chgrp peter-dinh test
 - peter-dinh@peter:~/bsp\$ ls -l
 - -rw-r--r-- 1 kevin peter-dinh 0 2008-03-22 23:47 test

umask (1)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

- mit umask kann man Voreinstellungen für die Rechte neu angelegter Dateien setzen
- umask [maske]
- Die Eingabe von umask ohne Parameter gibt die aktuell eingestellte Maske wieder
- maske ist eine 3-oder 4-stellige Oktalzahl (abhängig vom System)
- umask gibt nicht an, welche Rechte gegeben werden, sondern welche entzogen werden

umask (2)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

Wert	Bedeutung
0	rw für Dateien, rwx für Verzeichnisse
1	rw für Dateien und Verzeichnisse
2	r für Dateien, rx für Verzeichnisse
3	r für Dateien und Verzeichnisse
4	w für Dateien, wx für Verzeichnisse
5	w für Dateien und Verzeichnisse
6	x für Dateien und Verzeichnisse
7	Keine Rechte für Dateien und Verzeichnisse

■ Bsp:

- duc@vn:~\$ umask
- 0022
- duc@vn:~\$ touch a && ls -l a
- -rw-r--r-- 1 duc duc 0 2008-05-03 21:52 a

Access Control Lists (1)

1. Benutzer/Gruppen

- /etc/passwd
- UID/GID
- shadowsuite
- /etc/gshadow
- su
- sudo
- LDAP
- PAM

2. Rechte

- norm. Rechte
- spez. Rechte
- chmod
- chown
- umask
- Access Control Lists

- ACLs sind im Prinzip eine mächtige Erweiterung der Standardrechte
- Im Unterschied zu einfachen Zugriffsrechten sind ACLs feiner einstellbar.
- So können etwa für eine Datei für mehrere Benutzer und Gruppen unterschiedliche Rechte vergeben werden, während reguläre Zugriffsrechte nur die Definition von einem Benutzer und einer Gruppe zulassen
- ACLs aktivieren
 - das Dateisystem muss ACLs unterstützen, z.B xfs, ext3 ...
 - das Paket acl muss nachinstalliert werden
 - man muss noch in /etc/fstab einstellen, z.B.
 - /dev/hda3 /home ext3 defaults,acl 0 2
 - nach einem Reboot oder Remount der entsprechenden Partition können ACLs genutzt werden

Access Control Lists (2)

1. Benutzer/Gruppen

- o /etc/passwd
- o UID/GID
- o shadowsuite
- o /etc/gshadow
- o su
- o sudo
- o LDAP
- o PAM

2. Rechte

- o norm. Rechte
- o spez. Rechte
- o chmod
- o chown
- o umask
- o Access Control Lists

■ ACLs setzen, z.B.

- setfacl -m u:user1:rwX a.txt
- setfacl -m g:autooren:rwX a.txt

■ ACLs abfragen, z.B.

- duc@vn:~/vortrag/ACL\$ getfacl a.txt
- # file: a.txt
- # owner: duc
- # group: duc
- user::rw-
- user:user1:rwX
- group::r--
- mask::rwX
- other::r--

Zusammenfassung

- Linux ist ein Multitasking- und Multiuser-System
- um das ganze System effizient zu verwalten benötigt man Konzepte zur Verwaltung von Benutzern, Gruppen und Rechten
- ein Verzeichnisdienst stellt in einem Netzwerk eine zentrale Sammlung an Daten bestimmter Art zur Verfügung (z.B. Personendaten) und wird von LDAP und PAM unterstützt

Quellen

<http://www.galileocomputing.de/openbook/linux/index.htm>

http://de.wikipedia.org/wiki/Pluggable_Authentication_Modules

<http://de.wikipedia.org/wiki/Pam>

<http://www.fibel.org/linux/lfo-0.6.0/node1.html>

<http://www.selflinux.org/selflinux/html/userverwaltung01.html#d61e32>

http://de.wikipedia.org/wiki/Access_Control_List

[http://de.wikipedia.org/wiki/Su_\(UNIX\)](http://de.wikipedia.org/wiki/Su_(UNIX))

<http://de.wikipedia.org/wiki/Sudo>

<http://de.wikipedia.org/wiki/LDAP>

Danke für Eure Aufmerksamkeit
!!!