

# Samba som PDC



Udarbejdet af Kenneth Dalbjerg

**Titelblad:**

Samba som PDC, er udviklet af Kenneth Dalbjerg. Rapporten er skrevet på Erhvervsakademi Midtjylland, under IT & Elektronik teknolog.  
Rapport er afleveret d. 19/3 2003.

**Resumé:**

Denne rapport omhandler opsætning af samba som en PDC server. (Primary Domain Controller), under debian, men med teknisk snilde kan du sagtens ændre dette til nogen af de andre distributioner. Derud over finder du også oplysninger omkring file level security.

## Indholdsfortegnelse:

Forord .....	5
Indledning: .....	6
Samba 2.2.3a-6 som PDC .....	7
Oprettelse af bruger: .....	8
Oprettelse af grupper: .....	8
Windows 9x klienter: .....	9
Windows 2000 / XP klienter: .....	10
Deling af mapper: .....	12
Logon script:.....	13
Ressourcer: .....	14
Share level security: .....	14
User level security: .....	14
File level security:.....	15
Ekstra Tools: .....	16
Hjælp share: .....	16
Time Server: .....	16
Bilag 1: Smb.conf filen. ....	19
Bilag 2: Oversigt over rettigheder på mapper. ....	21
Bilag 3: Bruger & Grupper.....	22

## Forord

Jeg har hentede meget informationer fra bogen Using Samba, som du finder på denne adresse: [http://sunsite.dk/samba/oreilly/using\\_samba/index.html](http://sunsite.dk/samba/oreilly/using_samba/index.html), hvor du også kan finde mange flere informationer omkring de enkle ting.

Derud over har jeg søgt på [www.google.com](http://www.google.com) efter div. Informationer og hjælp.

## Indledning:

Opgaven lyder på, opsætning af Samba som en PDC, med følgende:

- Lav 3 grupper: SALG, LAGER, BOGH, bestående af 2 bruger hver.
- Hver bruger skal have en privat share.
- Der skal laves følgende mapper & shares:  
APPS med:  
share-level-permission  
Administrators: Full  
Alle: Read  
og file-level-permission:  
Alle: Full
- Alle med:  
share-level-permission  
Administrators: Full  
Everyone: Full  
og file-level-permission:  
Alle: Full
- På Alle skal der derudover laves følgende mapper med file-level-permission efter følgende:

Mapper	File-level-permission
SALG	Administrators: Full Alle: Read SALG: Full
LAGER	Administrators: Full Alle: Read Lager: Full
BOGH	Administrators: Full Alle: Read BOGH: Full

- Lav en rapport som beskriver arbejdsgangen for brugeradministrationen. F.eks. Hvordan oprettes bruger, hvordan gør man en bruger medlem af en gruppe, hvordan laves shares og permission til dem etc.

## Samba 2.2.3a-6 som PDC

Jeg benytter debian, men med lidt teknisk snilde, kan du også bruge denne guide, til dit system.

Allerførst skal du have installeret samba, i debian gøres det nemmest således "apt-get install samba".

Få at for samba op og kører som PDC server, skal du ændre nogen ting i din konfigurations fil, de vigtigste ting er:

```
#Hvilket domæne, ønsker du at samba skal kontrollere
workgroup = dalbjerg
#Hvilket maskine navn skal samba have
netbios name = dalserver
#Hvilket måde skal samba tjekke for adgang.
security = user
#Skal samba være domæne controller
domain logons = yes
#Siger vist sig selv
encrypt passwords = yes
#Dette OS level svare til at samba, har samme status som en NT Server
os level = 33
domain master = yes
preferred master = yes
local master = yes
#Login script, skal ligge i den mappe som du vælger at dele som netlogon
logon script = login.bat
#Hvilket gruppe skal være administrators, her er det adm.
domain admin group = @adm
```

**Husk at workgroup & netbios name ikke må være det samme.**

Se mere i den medfølgende konfigurations fil. Omkring hvilket andre ting, som er nødvendigt for at få det til at køre.

Herefter skal du have genstartede samba. I debian gøres det nemmest således "/etc/init.d/samba restart".

Jeg gør opmærksom på at det jeg har skrevet herinde, ikke er nok til at sætte det samba op, som PDC server, du skal ind og redigere i den medfølgende konfigurations fil.

### ***Oprettelse af bruger:***

At oprette en bruger i samba, er ikke meget svære end at oprette en bruger i Linux selv. Du skal først have oprettet en bruger, i Linux. Dette gøres med kommandoen adduser.

Eks:

```
adduser foo
```

herefter spørg den efter password til brugeren, her vælger du så et password, du ønsker at bruge.

Med fordel kan man skrive:

```
Adduser foo --shell /bin/false, der brugeren så ikke kan logge ind på serveren via eks, ssh.
```

Nå du har oprette dem i Linux, skal de oprettes i samba, dette gøres med smbpasswd. Her skriver du:

```
Smbpasswd -a foo, hvorefter den spørger om passwordet. Herefter er brugeren oprettet i samba, og kan nu logge ind.
```

### ***Oprettelse af grupper:***

Hvis du ønsker at oprette grupper, som jo er meget smart, nå man skal sætte sikkerhed op, således man ikke skal ind og gøre det for hver enkel bruger. For at oprette en gruppe skriver du:

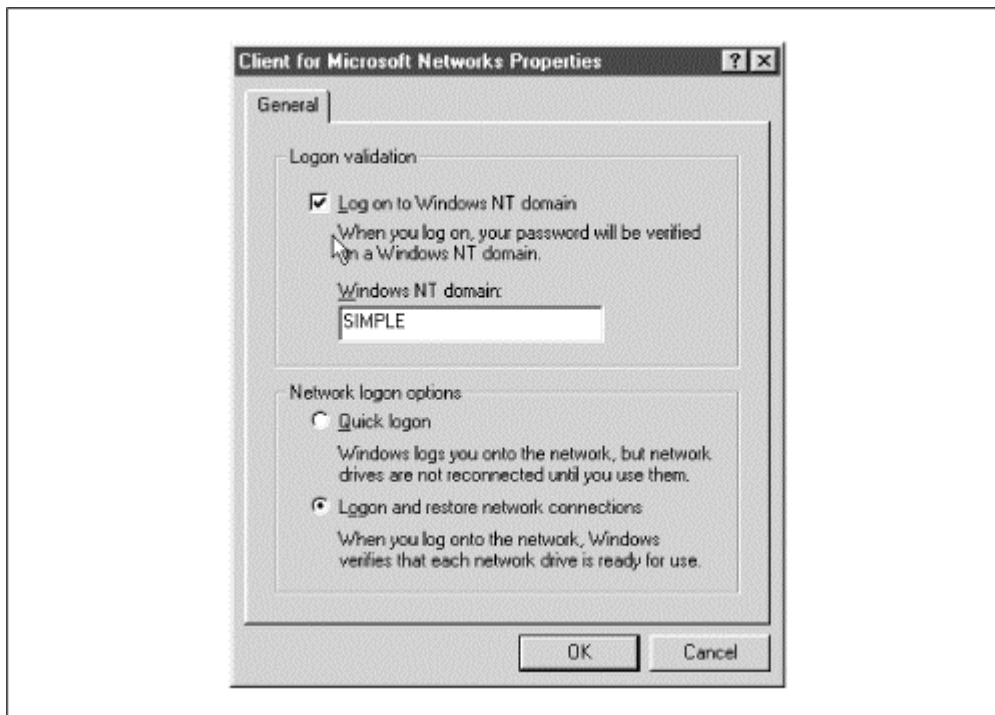
```
Groupadd foo, så oprette du en gruppe ved navn foo.
```

Hvis du derimod ønsker at melde en bruger ind i en gruppe skriver du adduser brugernavn gruppenavn.



### **Windows 9x klienter:**

Det er nemmest at få sat Windows 9x klienter, til at connecte til en Samba PDC, det er i hvert fald mine erfaringer. Du går ind i netværksopsætning, og vælger properties ved "Client for Microsoft Networks", så skulle du gerne for en skærm frem som det herunder. Der hvor der her står SIMPLE, dette skal du erstatte med det du har skrevet som workgroup i din konfigurations fil.



Herefter skal du bare logge af og logge på igen, så skulle det virke.

### **Windows 2000 / XP klienter:**

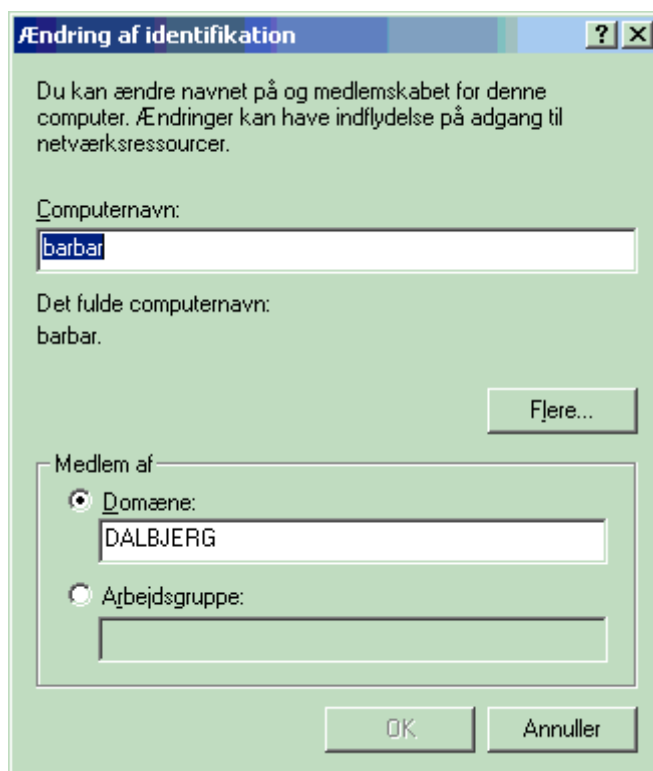
For at få Windows 2000 / XP klienter, til at koble sig op mod en samba PDC, skal du have oprette en "trust account" på Linux maskinen og i samba. Dette gør du ved at skrive `useradd maskinenavn$ -s /bin/false`. Bemærk at \$ skal være der. Eks, hvis dit maskinenavn er barbar, skal du altså skrive `barbar$`.

Du kan se dit maskinenavn ved at skrive `ipconfig /all`, ude i command. I første linie, står der

Værtsnavn . . . . . : barbar, det er her du kan se din maskinenavn, dette er i dette eks, barbar.

Herefter skriver du `smbpasswd -a barbar`, bemærk at det her er uden \$.

Herefter skal du have sat din windows 2000 klient, op til at kører mod et domæne, dette vises, lettes ved hjælp af billeder. Du gå ind i kontrol panel, og trykker på system, netværksidentifikation, herefter vælger netværksidentifikation, egenskaber. Herefter kommer denne frem:



Her kan du også se computernavnet. Normalt står den under arbejdsgruppe ud for "Medlem af", den skal du så sætte til Domæne. Og så skal du skrive Domæne, det er det

domæne, du satte op i smb.conf. Herefter trykker du på OK, den spørger så efter et brugernavn & adgangskode, her skal du bruge root og den tilhørende adgangskode. Du skal huske at lave root brugeren i samba, dette gør man med smbpasswd -a root. (Du skal så huske at der i din smb.conf fil, ikke må står invalid user = root.

## ***Deling af mapper:***

Deling af mapper, foregå via smb.conf filen. For at del en mappe, skal man f. eks: skrive følgende i bunden af sin smb.conf fil:

```
[alle]
path = /home/samba/alle
writeable = yes
browseable = yes
comment = Her har alle mulighed for at ligge filer.
create mode = 0740
directory mode = 0740
valid user = @alle
```

Path, er der hvor du ønsker at det skal ligge på serveren, eks, her ligger vi det i /home/samba/alle.

Writeable: skal man kunne skrive til denne mappe, dog skal du bemærke, at brugeren som er logget ind, også skal kunne skrive til mappen, hvis han var logget ind via eks ssh. Så han skal altså også havde skrive adgang på "filelevel security".

Browseable: Skal drevet være synlig nå en Windows maskine browser serveren, altså skal den være synlig.

Comment: En beskrivelse/kommentar til den delte mappe.

Create mode: Nå der oprettes filer, hvordan skal disse så oprettes, altså med hvilket rettigheder skal de filerne havde.

Directory mode: Dette er så bare biblioteks rettigheder

Valid user: De gyldige bruger, nå man en @ foran, betyder det at alle som er i gruppen som står bagved få adgang.

## **Logon script:**

Med login script, kan man gøre således at når man logger ind, på en computer så mapper den automatisk de forskellige sharing på en server. Man kan lave en masse i disse scripts, eks, hente klokken fra serveren således at alle computer kører med samme tid, som kan være smart, hvis man skal søge efter en error i en log, på både en client & en server, så skal man kigge efter samme tid.

Man kan også starte div. Services op, eks, således at en mappe kun er delt, når en bruger er logget ind, og sådan noget.

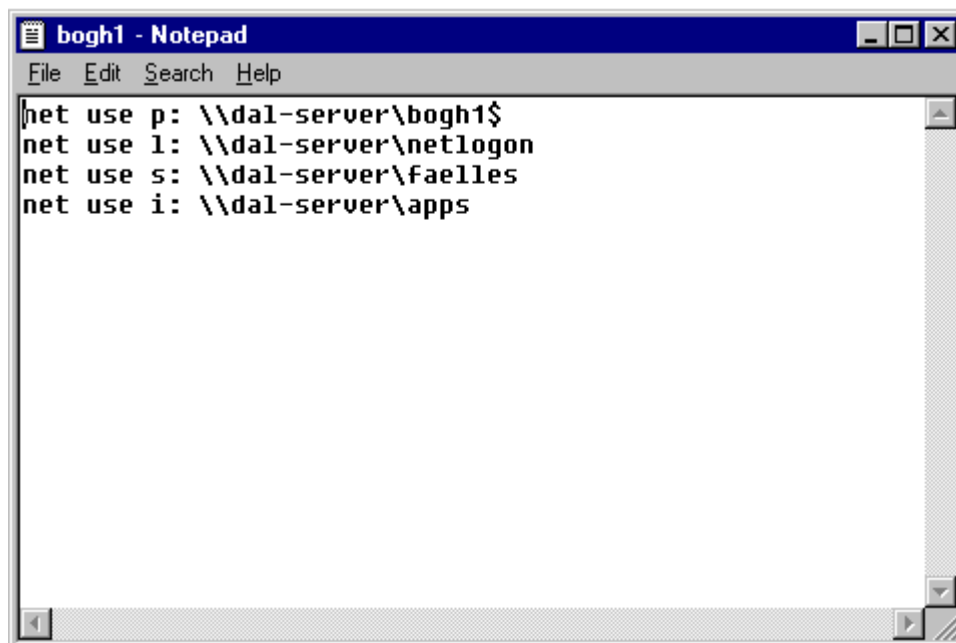
Glem filen som en windows bat fil, i en mappe, på serveren, som du deler under navnet netlogon. I din smb.conf fil, skal dette evt. se således ud:

```
[netlogon]
path = /home/samba/netlogon
writable = yes
browseable = no
comment = PDC netlogon share
```

Under [global] skal der står dette :

```
logon script = login.bat
```

Hvor login.bat, selvfølgelig er den fil du ønsker kørt. Du kan i denne også skrive %u.bat, så vil den kører filen som hedder "brugernavn som logger ind".bat.



```
File Edit Search Help
[net use p: \\dal-server\bogh1$
net use l: \\dal-server\netlogon
net use s: \\dal-server\faelles
net use i: \\dal-server\apps
```

*Her er et eks. på et logon script, dette script mapper automatisk 4 mapper på serveren dal-server.*

*Da jeg brugte windows 95 klienter, som ikke understøtter %username% er man nød til at gøre det på denne måde.*

## **Ressourcer:**

En ressource er noget andre bruger kan for adgang, til. Dette kan eks. være en Web Server, en deling eller andet.

Deling: Bruges f.eks. på en PDC, til at lave et fælles sted data glemmes, således at der bliver taget backup af det. Da det ikke er smart for administratoren, at skulle rundt til hver enkel pc, og tage backup. Man kan også dele en printer, således at anden computer kan printe ud på printeren som eks. er sat til serveren, det er ikke en nødvendigt at den sidder på serveren.

### ***Share level security:***

Hvis man deler på share level, så kan man ikke bestemme hvem som må se filer og hvem som må skrive af forskellige bruger. Man kan kun sætte 2 password på, et til at må læse og et til at skrive. Bruges af blandt andet Windows 95, 98, ME.

### ***User level security:***

Hvis man der i mod, deler på User level, så definere man hver enkel bruger eller gruppe, som må havde adgang, til delingen / printeren. Bruges blandt andet af Windows NT, 2K, XP.

### **File level security:**

Nå man logger på en Linux maskine, via samba. Henter samba rettighederne for Linux systemet, og man skal således både have rettigheder i Linux og igennem samba, for at kunne benytte sig af den delte ressource.

Hvis vi f.eks. siger vi har delt mappen /home/samba/alle, så for at brugerne kan for læse rettigheder til denne mappe skal man sætte mappen op til dette. Dette kan man bruge 2 forskellige komponenter til, disse 2 er chown & chmod.

Jeg har lavet en gruppe ved navn alle, hvor jeg har smidt alle mine samba bruger ind i. så har jeg givet gruppen adgang til denne mappe med, chown root.alle -R /home/samba/alle Dette bevirker, at alle filer, mapper og andet under denne mappe, vil blive tildelt brugeren root & gruppen alle som owner.

Herefter skrev jeg med chmod, chmod 770 -R /home/samba/alle. Hvad betyder de nummer som er tastede ind.

For at finde ud af dette, skal man dele talende op i 3 grupper, den først er owner af filen, den næste er group owner & den sidste er alle andre.

Herefter skal man ind og se lidt bit mønster:

Oktal talsystem	Bit for at opnår det oktale tal.
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Hernæst skal man tag de 3 grupper og opdele dem i 3 grupper, således at hver gruppe for en R, W, & en E gruppe. Altså således:

Bruger	Gruppe	Andre
R W E	R W E	R W E

Hvis vi så kun tager udkast i bruger gruppen, så vil det blive, således:

Bruger
R W E

Hvis man så tager R, W & E inddelinger, og omdøbe disse til 0, så det se sådan ud:

Bruger
0 0 0

Så står disse 0, for nummer for de 3 bit. Dette vil altså sige at hvis vi gerne vil havde at en gruppe kun må læse en fil, så skal man skrive 4. Dette skal du fordi, at tog man R W E, skal man altså finde et sted, hvor der kun er 1 i den første, og det er der ud for 4 oppe i tabellen over oktal tal.

### **Ekstra Tools:**

#### **Hjælp share:**

Med samba, kan man også lave således at hvis en bruger skriver

[\\servernavn\etellerandet](#), og etellerandet ikke findes, så for man en help share, hvor der for eksempel kunne ligge en hjælp fil, til hvad brugeren kan gøre.

Dette gør du med parameteren

```
Default service = help
```

Du skal så bare lave et share her der hedde help.

#### **Time Server:**

Samba, kan også kører time server, således at maskinerne, i netværket har samme tid, dette er smart nå man skal finde frem til en fejl i div. Log filer på forskellige maskiner, at det så er samme tidspunkt man skal kigge efter.

Man kan så evt. lade sin server hente tiden fra en af Internet. Eks på dette kunne være ntp, hvor man kan bruge en klient ved navn ntpdate. De fleste danske udbyder har en tidsserver, i hvert fald de største.



Men tilbage til samba, som Time Server, dette gør du med parameteret:

```
Time server = yes
```

## Konklusion:

Folkene bag samba, har virkelig lavet et program, som kan bruges til mange ting. Folkene har helt sikkert brugt meget tid, på at lave dette, og at de så til og med har gjort dette gratis, det er jo kanon. Jeg er dybt fascineret af dette stykke værktøj, hvad man kan med det. Dog er der nogen få mangler i form af hvad en Windows kan. Der er lidt problemer med at give rettigheder fra en windows maskine, nå man er logget ind som administrator og sådan noget.

Men Samba er i hvert fald et godt altandativ til windows, som dækker rigtig mange behov hos virksomhederne, da systemet ikke koster noget kan de således også spare rigtig mange penge, dog vil jeg mene at man godt kunne give nogen af de penge, man har sparet, til Open Sourcen, således at det kan blive endnu bedre.

Ligeledes ligger kilde koden til samba frit fremme, således man selv kan redigere i den.

Alt i alt er samba et kanon værktøj.

Kenneth Dalbjerg

---

## Bilag 1: Smb.conf filen.

```
[global]
workgroup = dalbjerg
netbios name = dumdidum
server string = Samba %v on %L

#Hvad skal folk logges ind med hvis de vælger at være gæster
guest ok = yes
guest account = ftp

status = yes

log level = 1

security = user
domain logons = yes
encrypt passwords = yes

os level = 65
domain master = yes
preferred master = yes
local master = yes

wins support = yes
time server = yes

logon script = login.bat
#logon drive = U:
#logon home = \\%L\%U
#logon path = \\%L\profile\%U

domain admin group = @adm

#Hvis man forbinder til en share som ikke er der, skal der vises
default service = help

#hosts allow = 192.168.1. 127.0.0.1

[homes]
```

```
writable = yes  
browseable = no  
comment = Users' home directories
```

```
[netlogon]  
path = /home/samba/netlogon  
writable = yes  
browseable = no  
comment = PDC netlogon share
```

```
[Alle]  
path = /home/samba/alle  
writeable = yes  
browseable = yes  
comment = Her har alle mulighed for at ligge filer.  
create mode = 0770  
directory mode = 0770  
valid user = @alle
```

```
[Apps]  
path = /home/samba/apps  
writeable = yes  
browseable = yes  
comment = Her har alle mulighed for at ligge filer.  
create mode = 0740  
directory mode = 0740  
valid user = @alle
```

```
[Help]  
path = /home/samba/help  
writeable = yes  
guest ok = yes  
browseable = yes  
comment = Hjælp.  
volume = Help  
create mode = 0744  
directory mode = 0744
```

## Bilag 2: Oversigt over rettigheder på mapper.

For at få denne liste frem, skrive du ls -l

dalserver:/home# ls -l

```
drwxr-xr-x  2 bogh1  salg      4096 Mar 19 11:18  bogh1
drwxr-xr-x  2 bogh2  bogh      4096 Mar 19 11:19  bogh2
drwxr-xr-x  9 dalbjerg dalbjerg  4096 Mar 17 12:09  dalbjerg
drwxr-xr-x  2 lager1  lager     4096 Mar 19 11:19  lager1
drwxr-xr-x  2 lager2  lager     4096 Mar 19 11:20  lager2
drwxr-xr-x  2 salg2   lager     4096 Mar 19 11:16  salg1
drwxr-xr-x  2 salg2   salg      4096 Mar 19 11:18  salg2
```

dalserver:/home/samba# ls -l

```
drwxrws--- 2 root    alle      4096 Mar  6 16:09  alle
drwxr-sr-x 2 root    staff     4096 Mar  6 14:41  apps
drwxr-sr-x 2 dalbjerg dalbjerg  4096 Mar  6 15:06  help
drwxr-sr-x 2 dalbjerg dalbjerg  4096 Mar  6 16:03  netlogon
```

dalserver:/home/samba/alle# ls -l

```
drwxrwxr-x 2 root  bogh      4096 Mar 19 12:30 bogh
drwxrwxr-x 2 root  lager     4096 Mar 19 12:30 lager
drwxrwxr-x 2 root  salg      4096 Mar 19 12:30 salg
```

## Bilag 3: Brugere & Grupper.

```
dalserver:/home/dalbjerger# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
games:x:5:100:games:/usr/games:/bin/sh
man:x:6:100:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
postgres:x:31:32:postgres:/var/lib/postgres:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/home:/bin/sh
dalbjerg:x:1000:1000:Kenneth Dalbjerg,,,:/home/dalbjerger:/bin/bash
sshd:x:100:65534:./var/run/sshd:/bin/false
barbar$:x:1001:1001:Trust Account:/dev/null:/dev/null
pc0002$:x:1003:1003:.,.,./dev/null:/dev/null
Barbaren$:x:1004:1004:.,.,./dev/null:/dev/null
maskinenavn$:x:1006:100:./home/maskinenavn$:/bin/false
ftp:x:1007:1007:.,.,./home/ftp:/bin/bash
pc0006$:x:1008:100:./home/pc0006$:
salg1:x:1002:1003:.,.,./home/salg1:/bin/bash
salg2:x:1005:1003:.,.,./home/salg2:/bin/bash
```

```
bogh1:x:1009:1004:,,,:/home/bogh1:/bin/bash
```

```
bogh2:x:1010:1004:,,,:/home/bogh2:/bin/bash
```

```
lager1:x:1011:1005:,,,:/home/lager1:/bin/bash
```

```
lager2:x:1012:1005:,,,:/home/lager2:/bin/bash
```

```
dalserver:/home/dalbjerg# cat /etc/group
```

```
root:x:0:
```

```
daemon:x:1:bin:x:2:
```

```
sys:x:3:
```

```
adm:x:4:dalbjerg
```

```
tty:x:5:
```

```
disk:x:6:
```

```
lp:x:7:lp
```

```
mail:x:8:
```

```
news:x:9:
```

```
uucp:x:10:
```

```
proxy:x:13:
```

```
kmem:x:15:
```

```
dialout:x:20:
```

```
fax:x:21:
```

```
voice:x:22:
```

```
cdrom:x:24:
```

```
floppy:x:25:
```

```
tape:x:26:
```

```
sudo:x:27:
```

```
audio:x:29:
```

```
dip:x:30:
```

```
postgres:x:32:
```

```
www-data:x:33:
```

```
backup:x:34:
```

```
operator:x:37:
```

```
list:x:38:
```

```
irc:x:39:
```

src:x:40:

gnats:x:41:

shadow:x:42:

utmp:x:43:

video:x:44:

staff:x:50:

games:x:60:

users:x:100:

nogroup:x:65534:

dalbjerg:x:1000:

sasl\*:x:45:

ssh:x:101:

alle:x:1001:dalbjerg,salg1,salg2,bogh1,bogh2,lager1,lager2

jan:x:1002:

ftp:x:1007:

salg:x:1003:

bogh:x:1004:

lager:x:1005: