Denne guide er oprindeligt
udgivet på Eksperten.dk

COMPUTERWORLD

Gør Administrator-brugeren til almindelig bruger

Guide til at fjerne den indbyggede administrator fra administratorgruppen. Det kræver et rimeligt godt kendskab til registreringsdatabasen.

Skrevet den **03. Feb 2009** af **squashguy** I kategorien **Styresystemer / Generelt** | ⭐⭐⭐☆☆

Her er en lille dirty guide til, at lave den indbyggede administratorkonto i Windows om til en begrænset konto (vi melder den simpelthen ud af administratorgruppen).

ADVARSEL inden du går i gang: guiden omhandler ændringer i registry/sam. Uden korrekt backup, kan du hurtigt stå med skægget i postkassen, hvis noget skulle gå galt.

Jeg fralægger mig ethvert ansvar for hvad der kan/måtte ske, hvis du følger denne guide.

:: Hvad du skal vide inden du læser videre

SID
Hver konto på systemet har en unik værdi, på 16 bytes, kaldet SID = Security Identifer. Denne benyttes alle steder hvor der tildeles rettigheder til kontoen. SID ændrer sig aldrig. Derfor kan du også omdøbe en konto uden at skulle ændre permissions andre steder i systemet.

RID
Relative Identifer. RID er den værdi som adskiller hver brugerkonto fra computerens konto. Brugerens SID = Computerens SID + Brugerens RID

:: SAM

Security Accounts Manager

I SAM-filen gemmes oplysninger om alle lokale brugere og grupper. I sin fysiske form, ligger den som filen 'sam' i \system32\config biblioteket. Under 2k/xp, kan filen ikke læses mens du står i Windows.

Filen indgår som en del af registry, og kan findes her:
HKEY_LOCAL_MACHINE\SAM\SAM\Domains

For at læse denne del af registry skal du først give dig selv adgang. Administratorer har nemlig ikke som standard adgang hertil. Under 2k skal du bruge regedt32.exe for at sætte permissions.

Hvis du ikke ønsker at ændre permissions, kan du starte regedit under 'LocalSystem Account', som er computerens systemkonto (den har adgang til alle dele af systemet). Her benytter vi at:

at <tid> /interactive regedit

Nu startes regedit under LocalSystem. Forudsat at servicen task scheduler/opgavestyring er startet, er sat til at logge på med LocalSystem, og givet tilladelse til at fungere interaktivt med skrivebord (standard-konfiguration).

(Tid: Hvis klokken lige nu er 10:10, sætter du den til at starte 10:11)

:: Opbygning af SAM i registry

```
HKEY_LOCAL_MACHINE\SAM\SAM\
  Domains
    Account
    Builtin
```

Account: alle brugere og ikke-indbyggede-grupper
Builtin: alle indbyggede grupper

Grupper oprettes i undermapper med navnet 'Aliases'
Brugere oprettes i undermapper med navnet 'Users'

:: Brugerkonti i SAM

```
SAM\Domains\Account\Users
000001F4 (500)
000001F5 (501)
...
Names
   Administrator (default værdi: 0x1F4, henviser til den overliggende 000001F4-
mappe)
   Guest (default værdi: 0x1F5)
   ...
```

Under 'Names' ligger navnene på alle brugerkonti. Hvert navn har tilknyttet en defaultværdi, som henviser til den mappe (med samme navn), der ligger lige under 'Users'.

Den indbyggede Administrator har altid værdien 0x1F4
Den indbyggede Gæst har altid værdien 0x1F5

Disse værdier er brugernes RID

Hver konto har to værdier (binær). Her ses den indbyggede Administrator:

```
SAM\Domains\Account\Users\000001F4
F
V
```

F indeholder oplysninger om kontoens tilstand. F.eks. om den er aktiv eller deaktiveret.
V indeholder alle oplysninger om selve kontoen. F.eks. SID, navn og password-hash.

Jeg vil senere vise hvordan du fra V-værdien henter kontoens SID ud.

:: Grupper i SAM

```
SAM\Domains\Builtin\Aliases
00000220
00000222
...
Names
   Administrators (default værdi: 0x220 - altid den samme for administrators)
   Guests (default værdi: 0x222 - altid den samme for guests)
   ...
```

Vi kigger nærmere på gruppen 'Administrators':

```
SAM\Domains\Builtin\Aliases\00000220
  C
```

Denne C-værdi indholder oplysninger om gruppen. Den indeholder faktisk hvad vi leder efter: Gruppens medlemmer (deres SID).

Hvert medlem optager 28 bytes (16 bytes til SID, og 12 bytes til start-signatur). Brugerne ligger til sidst i C-værdien. Hvert medlem har følgende form:

```
Medlem 1:
01 05 00 00 00 00 00 05 15 00 00 00             [12 bytes med start-signatur]
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx [16 bytes med SID]

Medlem 2:
01 05 00 00 00 00 00 05 15 00 00 00             [12 bytes med start-signatur]
yy yy yy yy yy yy yy yy yy yy yy yy yy yy yy yy [16 bytes med SID]

...
```

Det vi så gør er, at vi manuelt går ind og fjerner SID for den indbyggede administrator fra denne C-værdi. Og voilá: kontoen er ikke længere medlem af administratorgruppen.

Ud over at fjerne SID, skal vi ændre to andre steder i C-værdien, da gruppen nu har et medlem mindre.

For overblikkets skyld, er her et udsnit af C-værdien fra min administratorgruppe:

```
0000: 20 02 00 00 00 00 00 00
0008: 98 00 00 00 02 00 01 00
0010: 98 00 00 00 1e 00 00 00
0018: 00 00 00 00 b8 00 00 00
0020: 8a 00 00 00 00 00 00 00
0028: xx xx xx xx[70 00 00 00 offset 002C: antallet af medlemmer
0030: 04 00 00 00]xx xx xx xx (dette offset ligger altid fast)
...
0178: 01 05 00 00 00 00 00 05 på offset 0178 ligger første start-signatur for første medlem
0180: 15 00 00 00 15 25 af 47 (kan godt ligge andetsteds på din maskine)
0188: 20 38 bb 24 82 8b a6 28
0190: f4 01 00 00 01 05 00 00 på offset 0194 starter en ny signatur
...
```

Fra offset 0002C har vi to 32-bit værdier:
70 00 00 00 ** længde af afsnittet med SIDs

04 00 00 00 ** antal SIDs

Disse to værdier ligger i reversed hex. Dvs for at få den korrekte værdi, vendes rækkefølgen af bytes:
00 00 00 70 (0x70 = 112 decimalt)
00 00 00 04

Da hvert medlem optager 28 bytes, skal følgende regnskab gerne gå op:
antallet af medlemmer * 28 = længde af afsnit

I mit tilfælde:
4 * 28 = 112 (korrekt)

(Kigger jeg i administratorgruppen ligger her rigtig nok også fire medlemmer)

Når vi har fjernet SID for administratoren, skal vi korrigere disse to værdier.

Ny længde: 3 * 28 = 84 (0x54)

Vi skal derfor ændre værdierne til:
54 00 00 00
03 00 00 00

For at fjerne administratoren, skal du først kende hans SID. Den finder du ved at kigge i V-værdien for kontoen (RID er altid den samme, så du kan også nøjes med at lede efter denne):

`HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4`
V

Her følger samme struktur som ved gruppen:
01 05 00 00 00 00 00 05 15 00 00 00 [12 bytes med start-signatur]
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx [16 bytes med SID]

Du finder denne omkring offset 0140-0150. Denne klippes så ud af C-værdien for gruppen.

Opsumering

1)
Find SID for brugeren. Fjern SID + start-signatur fra gruppens C-værdi.

Fjernes: 01 05 00 00 00 00 00 05 15 00 00 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx

2)
Korriger de to værdier i gruppens C-værdi, som angiver antallet af SIDs.

:: Alternativ måde at finde SID

Som nævnt i starten, findes brugerens SID ved at tage computerens SID og lægge RID til.

Computerens SID finder du her:

```
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account
  V
```

De sidste 12 bytes af V-værdien er computerens SID (De sidste 4 bytes tilføjer du selv)

RID for administrator:
000001F4 [00 00 01 F4]

SID for administrator:
yy yy yy yy yy yy yy yy yy yy yy yy F4 01 00 00

Bemærk: brugerens RID ligger reversed.

:: Links

Detaljeret beskrivelse af SAM
<a
href="http://neworder.box.sk/files/nullak_ntsecurity/">http://neworder.box.sk/files/nullak_ntsecurity/

Pointen med guiden? Tja, at lære noget nyt.. :-)

Kommentar af the_email d. 26. Nov 2004 | 1

Fin nok artikel. Men jeg kan ligesom morteewart ikke helt se pointen i den

Kommentar af hub d. 02. Nov 2004 | 2

Fint arbejde på et højt niveau, tak for det..

Kommentar af serverservice d. 12. Jun 2005 | 3

Har set dette lille trick efterspurgt, men kan slet ikke selv se hvad folk skal bruge det til i praksis. Hvis man mister admin kontoen hvordan skal man fortryde og hvordan skal man administrere sin pc - rettigheder , netværk, drivere , opdateringer osv. Men fuld valuta da artiklen er så gennemført.

Kommentar af sorenbs d. 04. Nov 2004 | 4

Kommentar af morteeart d. 03. Nov 2004 | 5

fin, godt forklaret.. dog mangler pointen med at slette den konto. (Og man kan da godt dissable admin konto'en i win2k så vidt jeg har oplevet.)

Kommentar af visualdeveloper d. 22. Apr 2005 | 6

fed artikel...