The pdbedit Tool

pdbedit is a tool that can be used only by root. It is used to manage the passdb backend, as well as domain-wide account policy settings. pdbedit can be used to:

- add, remove, or modify user accounts.
- list user accounts.
- migrate user accounts.
- migrate group accounts.
- manage account policies.
- manage domain access policy settings.

The pdbedit tool is the only one that can manage the account security and policy settings. It is capable of all operations that smbpasswd can do as well as a superset of them.

One particularly important purpose of the pdbedit is to allow the import/export of account information from one passdb backend to another.

User Account Management

The pdbedit tool, like the smbpasswd tool, requires that a POSIX user account already exists in the UNIX/Linux system accounts database (backend). Neither tool will call out to the operating system to create a user account because this is considered to be the responsibility of the system administrator. When the Windows NT4 domain user manager is used to add an account, Samba will implement the add user script (as well as the other interface scripts) to ensure that user, group and machine accounts are correctly created and changed. The use of the pdbedit tool does not make use of these interface scripts.

Before attempting to use the pdbedit tool to manage user and machine accounts, make certain that a system (POSIX) account has already been created.

Listing User and Machine Accounts

The following is an example of the user account information that is stored in a tdbsam password backend. This listing was produced by running:

```
$ pdbedit -Lv met
UNIX username:        met
NT username:          met
Account Flags:        [U          ]
User SID:             S-1-5-21-1449123459-1407424037-3116680435-2004
Primary Group SID:    S-1-5-21-1449123459-1407424037-3116680435-1201
Full Name:            Melissa E Terpstra
Home Directory:       \\frodo\met\Win9Profile
HomeDir Drive:        H:
Logon Script:         scripts\logon.bat
Profile Path:         \\frodo\Profiles\met
Domain:               MIDEARTH
Account desc:
Workstations:         melbelle
Munged dial:
Logon time:           0
```

```
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 20:14:07 GMT
Password last set:    Sat, 14 Dec 2002 14:37:03 GMT
Password can change:  Sat, 14 Dec 2002 14:37:03 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
```

Accounts can also be listed in the older smbpasswd format:

```
root# pdbedit -Lw
root:0:84B0D8E14D158FF8417EAF50CFAC29C3:
     AF6DD3FD4E2EA8BDE1695A3F05EFBF52:[U          ]:LCT-42681AB8:
jht:1000:6BBC4159020A52741486235A2333E4D2:
     CC099521AD554A3C3CF2556274DBCFBC:[U          ]:LCT-40D75B5B:
rcg:1002:E95D4331A6F23AF8AAD3B435B51404EE:
     BB0F2C39B04CA6100F0E535DF8314B43:[U          ]:LCT-40D7C5A3:
afw:1003:1AAFA7F9F6DC1DEAAAD3B435B51404EE:
     CE92C2F9471594CDC4E7860CA6BC62DB:[T          ]:LCT-40DA501F:
met:1004:A2848CB7E076B435AAD3B435B51404EE:
     F25F5D3405085C555236B80B7B22C0D2:[U          ]:LCT-4244FAB8:
aurora$:1005:060DE593EA638B8ACC4A19F14D2FF2BB:
     060DE593EA638B8ACC4A19F14D2FF2BB:[W          ]:LCT-4173E5CC:
temptation$:1006:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:
     A96703C014E404E33D4049F706C45EE9:[W          ]:LCT-42BF0C57:
vaioboss$:1001:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:
     88A30A095160072784C88F811E89F98A:[W          ]:LCT-41C3878D:
frodo$:1008:15891DC6B843ECA41249940C814E316B:
     B68EADCCD18E17503D3DAD3E6B0B9A75:[W          ]:LCT-42B7979F:
marvel$:1011:BF709959C3C94E0B3958B7B84A3BB6F3:
     C610EFE9A385A3E8AA46ADFD576E6881:[W          ]:LCT-40F07A4
```

The account information that was returned by this command in order from left to right consists of the following colon separated data:

- Login ID.
- UNIX UID.
- Microsoft LanManager password hash (password converted to upper-case then hashed).
- Microsoft NT password hash (hash of the case-preserved password).
- Samba SAM Account Flags.
- The LCT data (password last change time).

The Account Flags parameters are documented in the pdbedit man page, and are briefly documented in the Account Flags Management section.

The LCT data consists of 8 hexadecimal characters representing the time since January 1, 1970, of the time when the password was last changed.

Adding User Accounts

The pdbedit can be used to add a user account to a standalone server or to a domain. In the example shown here the account for the user vlaan has been created before attempting to add the SambaSAMAccount.

```
root#  pdbedit -a vlaan
new password: secretpw
retype new password: secretpw
Unix username:        vlaan
```

```
NT username:          vlaan
Account Flags:        [U          ]
User SID:             S-1-5-21-726309263-4128913605-1168186429-3014
Primary Group SID:    S-1-5-21-726309263-4128913605-1168186429-513
Full Name:            Victor Laan
Home Directory:       \\frodo\vlaan
HomeDir Drive:        H:
Logon Script:         scripts\logon.bat
Profile Path:         \\frodo\profiles\vlaan
Domain:               MIDEARTH
Account desc:         Guest User
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 20:14:07 GMT
Password last set:    Wed, 29 Jun 2005 19:35:12 GMT
Password can change:  Wed, 29 Jun 2005 19:35:12 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Deleting Accounts

An account can be deleted from the SambaSAMAccount database

```
root#  pdbedit -x vlaan
```

The account is removed without further screen output. The account is removed only from the SambaSAMAccount (passdb backend) database, it is not removed from the UNIX account backend.

The use of the NT4 domain user manager to delete an account will trigger the delete user script, but not the pdbedit tool.

Changing User Accounts

Refer to the pdbedit man page for a full synopsis of all operations that are available with this tool.

An example of a simple change in the user account information is the change of the full name information shown here:

```
root#  pdbedit -r --fullname="Victor Aluicious Laan" vlaan
...
Primary Group SID:    S-1-5-21-726309263-4128913605-1168186429-513
Full Name:            Victor Aluicious Laan
Home Directory:       \\frodo\vlaan
...
```

Let us assume for a moment that a user's password has expired and the user is unable to change the password at this time. It may be necessary to give the user additional grace time so that it is possible to continue to work with the account and the original password. This demonstrates how the password expiration settings may be updated

```
root#  pdbedit -Lv vlaan
...
Password last set:    Sun, 09 Sep 2001 22:21:40 GMT
Password can change:  Thu, 03 Jan 2002 15:08:35 GMT
Password must change: Thu, 03 Jan 2002 15:08:35 GMT
Last bad password   : Thu, 03 Jan 2002 15:08:35 GMT
```

```
Bad password count  : 2
...
```

The user has recorded 2 bad logon attempts and the next will lock the account, but the password is also expired. Here is how this account can be reset:

```
root#  pdbedit -z vlaan
...
Password last set:    Sun, 09 Sep 2001 22:21:40 GMT
Password can change:  Thu, 03 Jan 2002 15:08:35 GMT
Password must change: Thu, 03 Jan 2002 15:08:35 GMT
Last bad password   : 0
Bad password count  : 0
...
```

The Password must change: parameter can be reset like this:

```
root#  pdbedit --pwd-must-change-time=1200000000 vlaan
...
Password last set:    Sun, 09 Sep 2001 22:21:40 GMT
Password can change:  Thu, 03 Jan 2002 15:08:35 GMT
Password must change: Thu, 10 Jan 2008 14:20:00 GMT
...
```

Another way to use this tools is to set the date like this:

```
root#  pdbedit --pwd-must-change-time="2010-01-01" \
              --time-format="%Y-%m-%d" vlaan
...
Password last set:    Sun, 09 Sep 2001 22:21:40 GMT
Password can change:  Thu, 03 Jan 2002 15:08:35 GMT
Password must change: Fri, 01 Jan 2010 00:00:00 GMT
...
```

Refer to the strptime man page for specific time format information.

Please refer to the pdbedit man page for further information relating to SambaSAMAccount management.

Account Flags Management

The Samba SAM account flags are properly called the ACB (account control block) within the Samba source code. In some parts of the Samba source code they are referred to as the account encode_bits, and also as the account control flags.

The manual adjustment of user, machine (workstation or server) or an inter-domain trust account account flgas should not be necessary under normal conditions of use of Samba. On the other hand, where this information becomes corrupted for some reason, the ability to correct the damaged data is certainly useful. The tool of choice by which such correction can be affected is the pdbedit utility.

There have been a few requests for information regarding the account flags from developers who are creating their own Samba management tools. An example of a need for information regarding the proper management of the account flags is evident when developing scripts that will be used to manage an LDAP directory.

The account flag field can contain up to 16 characters. Presently, only 11 are in use. These are listed in Samba SAM Account Control Block Flags. The order in which the flags are

specified to the pdbedit command is not important. In fact, they can be set without problem in any order in the SambaAcctFlags record in the LDAP directory.

Samba SAM Account Control Block Flags

Flag	Description
D	Account is disabled.
H	A home directory is required.
I	An inter-domain trust account.
L	Account has been auto-locked.
M	An MNS (Microsoft network service) logon account.
N	Password not required.
S	A server trust account.
T	Temporary duplicate account entry.
U	A normal user account.
W	A workstation trust account.
X	Password does not expire.

An example of use of the pdbedit utility to set the account control flags is shown here:

```
root#  pdbedit -r -c "[DLX]" jht
Unix username:        jht
NT username:          jht
Account Flags:        [DHULX      ]
User SID:             S-1-5-21-729263-4123605-1186429-3000
Primary Group SID:    S-1-5-21-729263-4123605-1186429-513
Full Name:            John H Terpstra,Utah Office
Home Directory:       \\aurora\jht
HomeDir Drive:        H:
Logon Script:         scripts\logon.bat
Profile Path:         \\aurora\profiles\jht
Domain:               MIDEARTH
Account desc:         BluntObject
Workstations:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         0
Password last set:    Sun, 03 Jul 2005 23:19:18 GMT
Password can change:  Sun, 03 Jul 2005 23:19:18 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

The flags can be reset to the default settings by executing:

```
root#  pdbedit -r -c "[]" jht
Unix username:        jht
NT username:          jht
Account Flags:        [U          ]
User SID:             S-1-5-21-729263-4123605-1186429-3000
Primary Group SID:    S-1-5-21-729263-4123605-1186429-513
Full Name:            John H Terpstra,Utah Office
Home Directory:       \\aurora\jht
```

```
HomeDir Drive:        H:
Logon Script:         scripts\logon.bat
Profile Path:         \\aurora\profiles\jht
Domain:               MIDEARTH
Account desc:         BluntObject
Workstations:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         0
Password last set:    Sun, 03 Jul 2005 23:19:18 GMT
Password can change:  Sun, 03 Jul 2005 23:19:18 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Domain Account Policy Managment

To view the domain account access policies that may be configured execute:

```
root#  pdbedit -P ?
No account policy by that name
Account policy names are :
min password length
password history
user must logon to change password
maximum password age
minimum password age
lockout duration
reset count minutes
bad lockout attempt
disconnect time
refuse machine password change
```

Policies are:

NT4 policy Name	Samba Policy Name	NT4 Range	Samba Range	Samba Default
Maximum Password Age	maximum password age	0 - 999 (days)	0 - 4294967295 (sec)	4294967295
Minimum Password Age	minimum password age	0 - 999 (days)	0 - 4294967295 (sec)	0
Minimum Password Length	min password length	1 - 14 (Chars)	0 - 4294967295 (Chars)	5
Password Uniqueness	password history	0 - 23 (#)	0 - 4294967295 (#)	0
Account Lockout - Reset count after	reset count minutes	1 - 99998 (min)	0 - 4294967295 (min)	30
Lockout after bad logon attempts	bad lockout attempt	0 - 998 (#)	0 - 4294967295 (#)	0
*** Not Known ***	disconnect time	TBA	0 - 4294967295	0
Lockout Duration	lockout duration	1 - 99998 (min)	0 - 4294967295 (min)	30
Users must log on in order to change password	user must logon to change password	0/1	0 - 4294967295	0

NT4 policy Name	Samba Policy Name	NT4 Range	Samba Range	Samba Default
*** Registry Setting ***	refuse machine password change	0/1	0 - 4294967295	0

Commands will be executed to establish controls for our domain as follows:

1. min password length = 8 characters.
2. password history = last 4 passwords.
3. maximum password age = 90 days.
4. minimum password age = 7 days.
5. bad lockout attempt = 8 bad logon attempts.
6. lockout duration = forever, account must be manually reenabled.

The following command execution will achieve these settings:

```
root#  pdbedit -P "min password length" -C 8
account policy value for min password length was 5
account policy value for min password length is now 8
root#  pdbedit -P "password history" -C 4
account policy value for password history was 0
account policy value for password history is now 4
root#  pdbedit -P "maximum password age" -C 7776000
account policy value for maximum password age was 4294967295
account policy value for maximum password age is now 7776000
root#  pdbedit -P "minimum password age" -C 604800
account policy value for minimum password age was 0
account policy value for minimum password age is now 7
root#  pdbedit -P "bad lockout attempt" -C 8
account policy value for bad lockout attempt was 0
account policy value for bad lockout attempt is now 8
root#  pdbedit -P "lockout duration" -C -1
account policy value for lockout duration was 30
account policy value for lockout duration is now 4294967295
```

Note

To set the maximum (infinite) lockout time use the value of -1.

Warning

Account policies must be set individually on each PDC and BDC. At this time (Samba 3.0.11 to Samba 3.0.14a) account policies are not replicated automatically. This may be fixed before Samba 3.0.20 ships or some time there after. Please check the WHATSNEW.txt file in the Samba-3 tarball for specific update notiations regarding this facility.