

REPUBLIQUE DU CAMEROUN

\*\*\*\*\*

Paix-Travail-Patrie

\*\*\*\*\*

MINISTERE DE L'ENSEIGNEMENT

SUPERIEUR

\*\*\*\*\*

Université de Yaoundé 1

\*\*\*\*\*

Institut Saint Jean

REPUBLIC OF CAMEROON

\*\*\*\*\*

Peace-Work-Fatherland

\*\*\*\*\*

MINISTRY OF HIGHER

EDUCATION

\*\*\*\*\*

University of Yaoundé 1

\*\*\*\*\*

Institute Saint Jean



## **TRAVAUX PRATIQUES DE ADMINISTRATION**

### **SYSTEME**

# **Les étapes pour modifier ou supprimer un mot de passe d'une machine Windows avec un système linux et observation des disques windows**

Rédigé par l'étudiant

BAKOA BAYANA Joseph Corneille

**Sous l'encadrement académique de :**

**M. MAHAMAT MASSOUD**

**Année Académique  
2024-2025**

---

---

## Sommaire

### Table des matières

Introduction.....	3
Étapes pour modifier ou supprimer le mot de passe d'un utilisateur Windows depuis Ubuntu	
:.....	4
ETAPE 1 :.....	4
ETAPE 2: .....	5
ETAPE 3: .....	5
ETAPE 4 : .....	5
Conclusion .....	9

---

---

# Introduction

Dans certains cas, il peut être nécessaire de modifier ou de supprimer les mots de passe d'un compte utilisateur sur une machine Windows. Cela peut être utile si vous avez oublié votre mot de passe ou si vous avez besoin de gérer l'accès à un système Windows sans pouvoir vous connecter avec les identifiants appropriés. Bien que Windows propose des outils internes pour la gestion des mots de passe, il existe des méthodes alternatives, notamment en utilisant un autre système d'exploitation comme **Ubuntu**. Ubuntu, un système d'exploitation basé sur Linux, offre plusieurs outils puissants pour interagir avec des systèmes de fichiers Windows, ce qui permet de manipuler les fichiers système nécessaires à la gestion des mots de passe. Ce processus, souvent utilisé par les administrateurs système ou les utilisateurs avancés, repose sur l'utilisation d'outils comme `chntpw`, qui permettent de modifier ou de supprimer les mots de passe des comptes Windows directement depuis Ubuntu, en accédant aux fichiers de configuration des utilisateurs dans les partitions Windows. Dans ce guide, nous allons explorer les étapes nécessaires pour modifier ou supprimer un mot de passe sur une machine Windows en utilisant Ubuntu, sans avoir besoin de vous connecter directement à Windows.

---

---

Pour modifier ou supprimer les mots de passe d'un utilisateur Windows à l'aide d'Ubuntu, vous devez utiliser des outils spécifiques qui permettent d'accéder au système de fichiers Windows. Voici les étapes détaillées pour y parvenir :

### Prérequis :

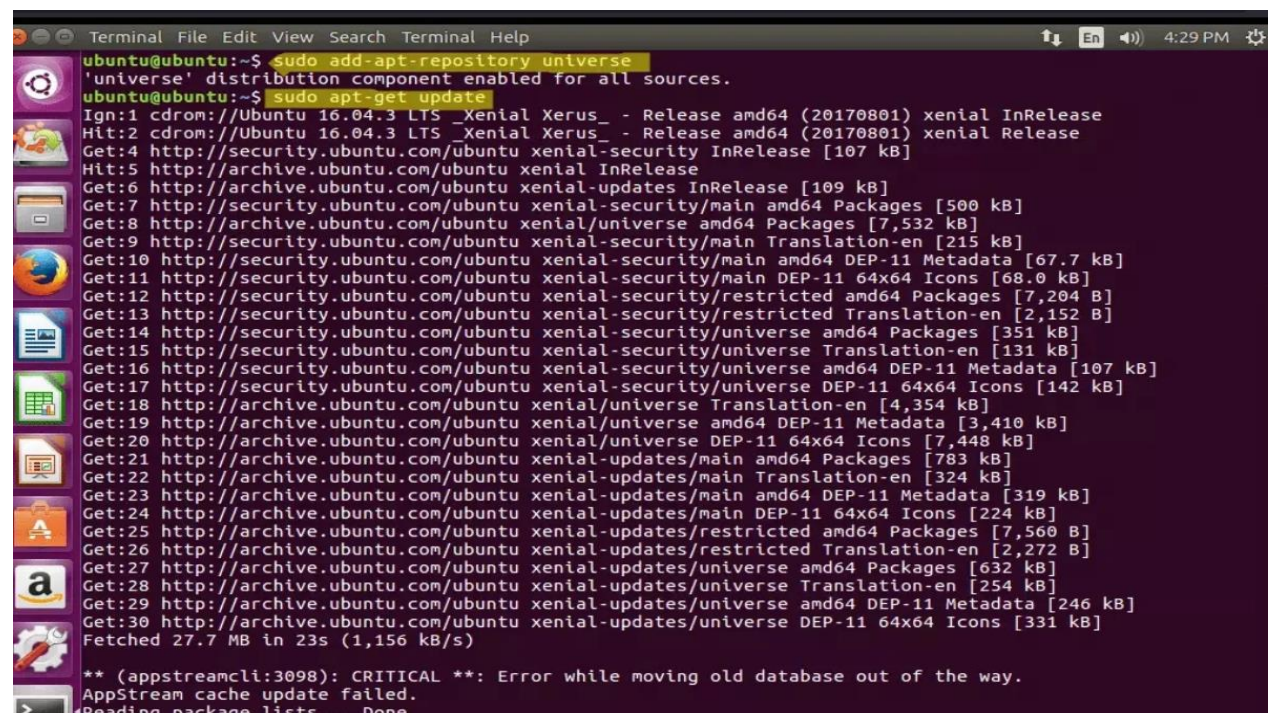
- Vous devez avoir un accès physique à la machine Windows ou au moins un accès à un disque dur externe qui contient la partition Windows.
- Vous devez démarrer Ubuntu sur la machine, soit en l'installant sur la machine, soit en utilisant un Live CD/USB.

## Étapes pour modifier ou supprimer le mot de passe d'un utilisateur Windows depuis Ubuntu :

### ETAPE 1 :

`sudo add-apt-repository universe`

`sudo apt-get update`



```
Terminal File Edit View Search Terminal Help
ubuntu@ubuntu:~$ sudo add-apt-repository universe
'universe' distribution component enabled for all sources.
ubuntu@ubuntu:~$ sudo apt-get update
Ign:1 cdrom://Ubuntu 16.04.3 LTS _Xenial Xerus_ - Release amd64 (20170801) xenial InRelease
Hit:2 cdrom://Ubuntu 16.04.3 LTS _Xenial Xerus_ - Release amd64 (20170801) xenial Release
Get:4 http://security.ubuntu.com/ubuntu xenial-security InRelease [107 kB]
Hit:5 http://archive.ubuntu.com/ubuntu xenial InRelease
Get:6 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [500 kB]
Get:8 http://archive.ubuntu.com/ubuntu xenial/universe amd64 Packages [7,532 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [215 kB]
Get:10 http://security.ubuntu.com/ubuntu xenial-security/main amd64 DEP-11 Metadata [67.7 kB]
Get:11 http://security.ubuntu.com/ubuntu xenial-security/main DEP-11 64x64 Icons [68.0 kB]
Get:12 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [7,204 B]
Get:13 http://security.ubuntu.com/ubuntu xenial-security/restricted Translation-en [2,152 B]
Get:14 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [351 kB]
Get:15 http://security.ubuntu.com/ubuntu xenial-security/universe Translation-en [131 kB]
Get:16 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 DEP-11 Metadata [107 kB]
Get:17 http://security.ubuntu.com/ubuntu xenial-security/universe DEP-11 64x64 Icons [142 kB]
Get:18 http://archive.ubuntu.com/ubuntu xenial/universe Translation-en [4,354 kB]
Get:19 http://archive.ubuntu.com/ubuntu xenial/universe amd64 DEP-11 Metadata [3,410 kB]
Get:20 http://archive.ubuntu.com/ubuntu xenial/universe DEP-11 64x64 Icons [7,448 kB]
Get:21 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [783 kB]
Get:22 http://archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [324 kB]
Get:23 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 DEP-11 Metadata [319 kB]
Get:24 http://archive.ubuntu.com/ubuntu xenial-updates/main DEP-11 64x64 Icons [224 kB]
Get:25 http://archive.ubuntu.com/ubuntu xenial-updates/restricted amd64 Packages [7,560 B]
Get:26 http://archive.ubuntu.com/ubuntu xenial-updates/restricted Translation-en [2,272 B]
Get:27 http://archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [632 kB]
Get:28 http://archive.ubuntu.com/ubuntu xenial-updates/universe Translation-en [254 kB]
Get:29 http://archive.ubuntu.com/ubuntu xenial-updates/universe amd64 DEP-11 Metadata [246 kB]
Get:30 http://archive.ubuntu.com/ubuntu xenial-updates/universe DEP-11 64x64 Icons [331 kB]
Fetched 27.7 MB in 23s (1,156 kB/s)

** (appstreamcli:3098): CRITICAL **: Error while moving old database out of the way.
AppStream cache update failed.
Reading package lists... Done
```

---

---

## ETAPE 2:

`sudo apt-get install chnptw`

```
** (appstreamcli:3098): CRITICAL **: Error while moving old database out of the way.
AppStream cache update failed.
Reading package lists... Done
ubuntu@ubuntu:~$ sudo apt-get install chnptw
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  chnptw
```

## ETAPE 3:

Après avoir accédé au disque dur, vous pouvez aussi utiliser la commande **mount** afin de localiser le point de montage du disque dur.

## ETAPE 4 :

Une fois dedans, on peut utiliser la commande `chnptw` pour lister les utilisateurs :

`sudo chnptw -l SAM`

enfin pour travailler sur un utilisateur en particulier :

`sudo chnptw -u <nom de l'utilisateur> SAM`

```
Terminal File Edit View Search Terminal Help
ubuntu@ubuntu:~$ cd /media/ubuntu/B63A60393A5FF4B9/Windows/System32/config/
ubuntu@ubuntu:/media/ubuntu/B63A60393A5FF4B9/Windows/System32/config$ sudo chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 287/57472 blocks/bytes, unused: 2/3744 blocks/bytes.

| RID | ----- Username ----- | Admin? | Lock? |
| 01f4 | Administrateur             | ADMIN  | dis/lock |
| 01f7 | DefaultAccount             |         | dis/lock |
| 03e8 | defaultuser0               |         | dis/lock |
| 03ea | Demo                       |         | dis/lock |
| 01f5 | Invit                      |         | dis/lock |
| 03e9 | mail                       | ADMIN  | dis/lock |
| 01f8 | WDAGUtilityAccount         |         | dis/lock |

ubuntu@ubuntu:/media/ubuntu/B63A60393A5FF4B9/Windows/System32/config$ sudo chntpw -u Demo SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 287/57472 blocks/bytes, unused: 2/3744 blocks/bytes.

===== USER EDIT =====

RID      : 1002 [03ea]
Username: Demo
fullname: demo
comment  :
homedir  :

00000221 = Utilisateurs (which has 4 members)

Account bits: 0x0210 =
[ ] Disabled      | [ ] Homedir req.   | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout   | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20) | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total login count: 1
```

En clair donc, vous aurez probablement besoin d'utiliser l'option 1 dans le cas où le mot de passe de l'utilisateur est perdu ou L'option 3 pour passer un utilisateur administrateur, si vous avez perdu l'accès administrateur.



```
//www.malekal.com/wp-content/uploads/reinitialiser-mot-passe-utilisateur-linux-ubuntu-4.jpg
Terminal File Edit View Search Terminal Help 4:57 PM

| 03ea | Demo | | | |
| 01f5 | Invite | | | |
| 03e9 | mail | ADMIN | dis/lock |
| 01f8 | WDAGUtilityAccount | | dis/lock |

ubuntu@ubuntu:/media/ubuntu/B63A60393A5FF4B9/Windows/System32/config$ sudo chntpw -u Demo SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 287/57472 blocks/bytes, unused: 2/3744 blocks/bytes.

===== USER EDIT =====

RID      : 1002 [03ea]
Username: Demo
fullname: demo
comment  :
homedir  :

00000221 = Utilisateurs (which has 4 Members)

Account bits: 0x0210 =
[ ] Disabled | [ ] Homedir req. | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account |
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act |
[X] Pwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08) |
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40) |

Failed login count: 0, while max tries is: 0
Total login count: 1

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

===== USER EDIT =====

RID      : 1002 [03ea]
```

L'option 3 passe l'utilisateur administrateur, il faut confirmer avec la touche y pour yes.  
Le message Promotion Done indique que l'opération s'est bien déroulée.

```
no ADMIN user found. Please try login with no password.

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 3

=== PROMOTE USER

Will add the user to the administrator group (0x220)
and to the users group (0x221). That should usually be
what is needed to log in and get administrator rights.
Also, remove the user from the guest group (0x222), since
it may forbid logins.

(To add or remove user from other groups, please other menu selections)

Note: You may get some errors if the user is already member of some
of these groups, but that is no problem.

Do it? (y/n) [n] : y
* Adding to 0x220 (Administrators) ...
sam_put_user_grpids: success exit
* Adding to 0x221 (Users) ...
sam_put_user_grpids: success exit
* Removing from 0x222 (Guests) ...
remove_user_from_grp: NOTE: group not in users list of groups, may mean user not member at all. Safe. Con
tinuing.
remove_user_from_grp: NOTE: user not in groups list of users, may mean user was not member at all. Does n
ot matter, continuing.
sam_put_user_grpids: success exit

Promotion DONE!

===== USER EDIT =====

RID      : 1002 [03ea]
Username: Demo
fullname: demo
comment  :
```

Enfin, on quit avec la touche q et surtout on écrit les modifications dans le SAM à la fin.

```
Terminal File Edit View Search Terminal Help
remove_user_from_grp: NOTE: user not in groups list of users, may mean user was not member at all. Does n
ot matter, continuing.
sam_put_user_grpids: success exit

Promotion DONE!
===== USER EDIT =====

RID      : 1002 [03ea]
Username: Demo
fullname: demo
comment  :
homedir  :

00000221 = Utilisateurs (which has 4 members)
00000220 = Administrateurs (which has 3 members)

Account bits: 0x0210 =
[ ] Disabled           | [ ] Homedir req.       | [ ] Passwd not req. |
[ ] Temp. duplicate    | [X] Normal account    | [ ] NMS account     |
[ ] Domain trust ac    | [ ] Wks trust act.    | [ ] Srv trust act   |
[X] Pwd don't expir    | [ ] Auto lockout      | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)     | [ ] (unknown 0x20)    | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total login count: 1
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > q

Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
ubuntu@ubuntu:/media/ubuntu/B63A60393A5FF4B9/Windows/System32/config$
```

Il ne reste plus qu'à redémarrer Windows. L'utilisateur n'aura plus de mot de passe et vous pourrez vous identifier avec sans problème.



---

---

# Conclusion

Modifier ou supprimer un mot de passe d'un compte utilisateur Windows à l'aide d'Ubuntu est une solution efficace lorsque l'accès à Windows est verrouillé ou lorsque le mot de passe est oublié. En utilisant des outils comme chntpw et en accédant aux fichiers système de Windows via la partition montée sous Ubuntu, il devient possible de réinitialiser un mot de passe sans avoir besoin de démarrer Windows. Cependant, il est essentiel de procéder avec prudence, car toute manipulation incorrecte des fichiers système pourrait entraîner des conséquences inattendues, notamment la perte de données ou des problèmes de fonctionnement de Windows. Cette méthode, bien que puissante, doit donc être utilisée par des utilisateurs expérimentés ou sous la supervision d'un professionnel, afin de garantir que le système reste stable et sécurisé après la modification des mots de passe. Ces étapes peuvent aussi être utilisées pour récupérer un simple fichier sur windows.