

Date de remise : 30 novembre 2022

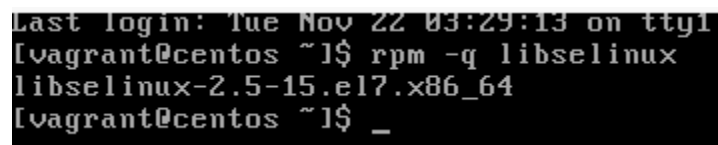
Partie 1 : Linux

Démarrer une nouvelle VM (Linux CentOS/7) en utilisant le Vagrantfile (fourni). N'oubliez pas de mettre à jour la VM avant de commencer le travail.

En utilisant le guide CIS du durcissement de CentOS/7 (document fourni), réalisez les tâches suivantes :

1. **Vérifier si SELinux est installé (contrôle : 1.6.2). Fournir une capture d'écran qui montre si SELinux est installé ou non.**

Linux est bel et bien installé sur ma machine CentOS/7. La commande `rpm -q libselinux` a été utilisée. Voir Image 1.



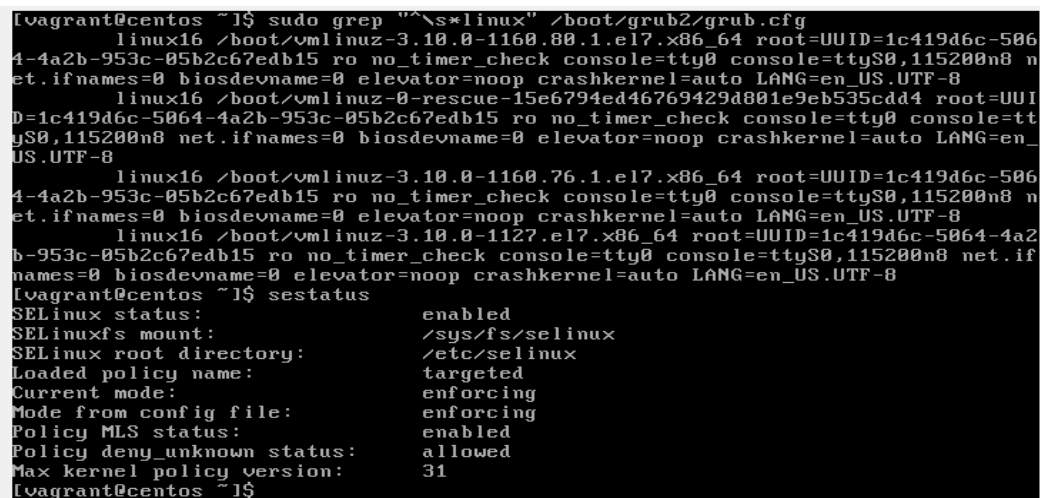
```
Last login: Tue Nov 22 03:29:13 on tty1
[vagrant@centos ~]$ rpm -q libselinux
libselinux-2.5-15.el7.x86_64
[vagrant@centos ~]$ _
```

Image 1

2. **Vérifier si SELinux n'est pas désactivé au niveau du bootloader (contrôle 1.6.1.1).**

SELinux n'est pas désactivé au niveau du bootloader. Les commandes `sudo grep "^s*linux" /boot/grub2/grub.cfg` et `sestatus` ont été utilisées. Voir Image 2.

- a) **Fournir une capture d'écran qui montre si SELinux est désactivé au niveau bootloader.**



```
[vagrant@centos ~]$ sudo grep "^s*linux" /boot/grub2/grub.cfg
linux16 /boot/vmlinuz-3.10.0-1160.80.1.el7.x86_64 root=UUID=1c419d6c-5064-4a2b-953c-05b2c67edb15 ro no_timer_check console=tty0 console=ttyS0,115200n8 net.ifnames=0 biosdevname=0 elevator=noop crashkernel=auto LANG=en_US.UTF-8
linux16 /boot/vmlinuz-0-rescue-15e6794ed46769429d801e9eb535cdd4 root=UUID=1c419d6c-5064-4a2b-953c-05b2c67edb15 ro no_timer_check console=tty0 console=ttyS0,115200n8 net.ifnames=0 biosdevname=0 elevator=noop crashkernel=auto LANG=en_US.UTF-8
linux16 /boot/vmlinuz-3.10.0-1160.76.1.el7.x86_64 root=UUID=1c419d6c-5064-4a2b-953c-05b2c67edb15 ro no_timer_check console=tty0 console=ttyS0,115200n8 net.ifnames=0 biosdevname=0 elevator=noop crashkernel=auto LANG=en_US.UTF-8
linux16 /boot/vmlinuz-3.10.0-1127.el7.x86_64 root=UUID=1c419d6c-5064-4a2b-953c-05b2c67edb15 ro no_timer_check console=tty0 console=ttyS0,115200n8 net.ifnames=0 biosdevname=0 elevator=noop crashkernel=auto LANG=en_US.UTF-8
[vagrant@centos ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            targeted
Current mode:                  enforcing
Mode from config file:         enforcing
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Max kernel policy version:     31
[vagrant@centos ~]$
```

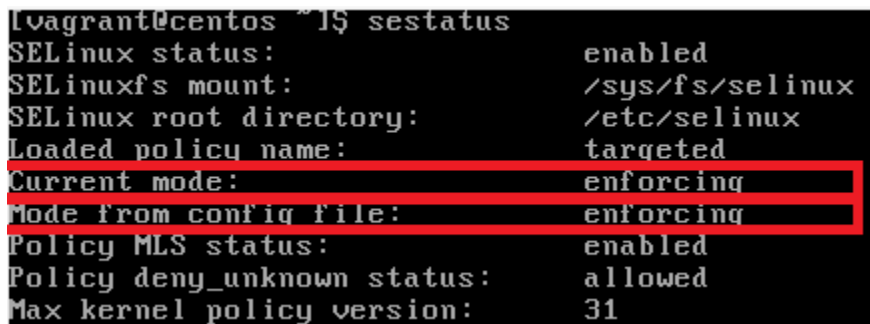
Image 2

b) Quelle est votre conclusion ? Est-ce que SELinux est désactivé au niveau du bootloader?

Linux n'est pas désactivé au niveau du Bootloader comme nous avons pu constater dans la capture d'écran ci-dessus.

3. Vérifier l'état de SELinux (*Disabled, Permissive, Enforcing*) (1.6.1.2). Fournir une capture d'écran qui montre l'état actuel de SELinux.

L'état de SELinux est configuré à *Enforcing*. La même commande `sestatus` a été utilisée. Voir Image 3.

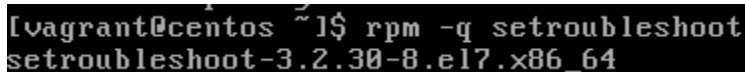


```
[vagrant@centos ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                  enforcing
Mode from config file:        enforcing
Policy MLS status:            enabled
Policy deny_unknown status:    allowed
Max kernel policy version:    31
```

Image 3

4. Vérifier si l'outil de débogage SELinux est installé. (contrôle : 1.6.1.4). Fournir une capture d'écran qui montre si l'outil de débogage SELinux est installé ou non.

L'outil de débogage est activé et la version est démontrée. La commande `rpm -q setroubleshoot` a été utilisée. Voir Image 4.



```
[vagrant@centos ~]$ rpm -q setroubleshoot
setroubleshoot-3.2.30-8.el7.x86_64
```

Image 4

5. Vérifier quelle politique est activée (*targeted, minimum, mls*) et changez-la. (contrôle : 1.6.1.3).

La politique *targeted* est activée. Elle a été changée à *mls*. Voir Image 5 et Image 6.

a) Fournir une capture d'écran qui montre la politique activée dans SELinux.

```

[vagrant@centos ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                 enforcing
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Max kernel policy version:    31

```

Image 5

b) Fournir une capture d'écran de SELinux après avoir changé la politique.

Pour changer la politique de *targeted* à *mls*, il a fallu tout d'abord installer le package *mls* en utilisant la commande `sudo yum install selinux-policy-mls`. Ensuite, entrer dans le text editor *vi* en utilisant la commande suivante : `vi /etc/selinux/config`. Arrivé dans le text editor, nous sommes maintenant en mesure de changer la politique à *mls*. Voir Image 6 pour voir la politique à *mls*.

```

"config" 12L, 536C written
[vagrant@centos selinux]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           mls
Current mode:                 enforcing
Mode from config file:       permissive
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Max kernel policy version:    31

```

Image 6

Partie 2 : Windows

Démarrer une nouvelle VM (Windows server 2012-R2) en utilisant le Vagrantfile (fourni). Vous pouvez utiliser la même VM que celle du cours. Créez une stratégie de groupe (GPO) et nommez-la GPO_TS. Associez cette GPO au domaine que vous avez déjà créé (ex : CR345_domain.net).

En utilisant le guide CIS du durcissement de Windows 2012-R2 (document fourni), réalisez les tâches suivantes sur la GPO créée:

1. Vérifier la politique relative à l'historique des mots de passe (1.1.1 (L1) *Ensure 'Enforce password history'*).

- a) Fournir une capture écran qui montre la valeur actuelle de la politique relative à l'historique des mots de passe.

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

- b) Modifier l'historique des mots de passe à « 5 ». Fournir une capture écran qui montre la nouvelle valeur.

Policy	Policy Setting
Enforce password history	5 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

2. Vérifier la politique relative à l'âge maximal des mots de passe (1.1.2 (L1) *Ensure 'Maximum password age'*).

L'âge maximale est présentement set a 42 jours

- a) Fournir une capture écran qui montre l'âge maximal actuel des mots de passe.

Maximum password age	42 days
----------------------	---------

- b) Modifier l'âge maximal des mots de passe à 30 jours. Fournir une capture écran qui montre la nouvelle valeur.

Maximum password age	30 days
----------------------	---------

3. Vérifier la politique relative à la longueur des mots de passe (1.1.4 (L1) *Ensure 'Minimum password length'*).

Elle est par default set a 7 caractères

- a) Fournir une capture écran qui montre la longueur actuelle des mots de passe.

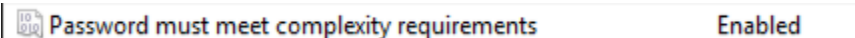


- b) Modifier la longueur des mots de passe à 8 caractères. Fournir une capture écran qui montre la nouvelle valeur.

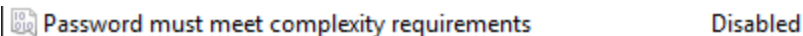


4. Vérifier la politique relative à la complexité des mots de passe (1.1.5 (L1) *Ensure 'Password must meet complexity requirements'*)

- a) Fournir une capture écran qui montre le statut de la politique relative à la complexité des mots de passe.

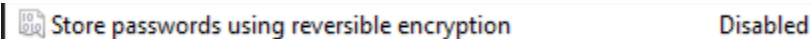


- b) Modifier le statut de la politique. Fournir une capture écran qui montre la nouvelle valeur.

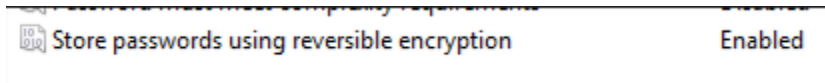


5. Vérifier la politique relative à la sauvegarde des mots de passe (1.1.6 (L1) *Ensure 'Store passwords using reversible encryption'*).

- a) Fournir une capture écran qui montre le statut de la politique relative à la sauvegarde des mots de passe.



- b) **Modifier le statut de la politique. Fournir une capture écran qui montre la nouvelle valeur.**



Références :

[-https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/using-multi-level-security-mls_using-selinux#switching-the-selinux-policy-to-mls_using-multi-level-security-mls](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/using-multi-level-security-mls_using-selinux#switching-the-selinux-policy-to-mls_using-multi-level-security-mls)

-https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/enabling-mls-in-selinux

-Windows et CentOS CIS benchmark guides (fournis en classe par le professeur)

Livrable : Il faut préparer un document PDF et y inclure les 10 questions demandées.

Évaluation : Chaque réponse compte pour 1 point, pour un total de 17 points. Bonne chance!