# Hardening de accesos. Configuración para AIX y Linux

Administración AIX/ Hugo Messina / última revisión: 17-07-2012

## Objetivos

1. **REQUISITOS DEL PROYECTO:**
2. Implementar sistemas de control de acceso en todos los componentes del sistema.
3. Configuración de accesos, a los efectos de hacer cumplir los privilegios asignados a los individuos sobre la base de la clasificación de la tarea y la función.
4. Asignación única de ID con acceso a componentes del sistema o titulares de tarjetas. Empleando al menos uno de los métodos siguientes para autenticar a todos los usuarios: Algo que el usuario sepa, como una contraseña o frase de seguridad. Garantizando que no se
5. Garantizar que no se utilice cuentas ni contraseñas de grupos, compartidas o genéricas, ni ningún otro método de autenticación.
6. Inhabilitación o eliminación de ID de usuario y cuentas genéricas.
7. No existen ID de usuario compartidas para realizar actividades de administración del sistema y demás funciones críticas. Las ID de usuario compartidas y genéricas no se utilizan para administrar componentes del sistema.
8. Configuración de contraseña:
   1. [Longitud mínima de siete caracteres](#_AIX:).
   2. [Conteniendo tanto caracteres numéricos como alfabéticos](#_AIX:_1)
   3. [No permitiendo la utilización de cualquiera de las últimas cuatro contraseñas manipuladas](#_AIX:_2).
   4. [Limitando los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos](#_AIX:_3)
   5. [Confirmación de bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario](#_AIX:_4)
   6. [Reingreso de contraseña luego de una inactividad mayor a 15 minutos](#_AIX:_5)
9. Revisión de aplicaciones de la base de datos y las ID de aplicaciones relacionadas para verificar que las ID de aplicación las puedan utilizar sólo las aplicaciones (y no los usuarios u otros procesos).

* [ANEXO](#_ANEXO_–_Vencimiento): Vencimiento de contraseñas
* [ANEXO 2](#_ANEXO_2_–): Referencias en la web

***Referencias:***

|  |  |
| --- | --- |
| Parámetro: Parámetro(s) más relevante(s) utilizado(s) | *<- Hacerlo por c/user* : Acaración en el código |
| NOTA: Aclaración importante | **TODO**: Pendiente de documentar |
| adm01:/home/root>: Código AIX | suc250:/etc/pam.d>: Código Linux |

## *Implementación de controles y corrección*

## 7 - Configuración de contraseña:

A - Longitud mínima de siete caracteres.

## *AIX:*

Parámetro

**minlen**

Control (individual):

Verificar que minlen tenga un valor de 7

adm01:/home/root>lsuser -a minlen hmessina

hmessina minlen=7

Corrección (global):

adm01:/home/root>chuser minlen= hmessina *<- Hacerlo por c/user*

adm01:/home/root>chsec -f /etc/security/user -s default -a minlen=7

Usuarios con excepción (individual):

adm01:/home/root>chuser minlen=0 root

NOTA: root puede fijar el password de cualquier usuario, pero se le solicitará cambio en el login. Esto vale de acá en más para AIX

#### LINUX:

Parámetros

**minlen  
PASS\_MIN\_LEN**

Control y corrección (global):

Verificar que exista en el archivo /etc/pam.d/system-auth el parámetro minlen=7 en el la línea del módulo **pam\_cracklib.so** del stack de PAM en la sección password. Si no fuera así editar el archivo y agregarlo.  
En el archivo /etc/login.defs debe figurar PASS\_MIN\_LEN 7. Si no fuera así editar el archivo y agregarlo.

suc250:/etc/pam.d>grep minlen system-auth

password requisite /lib/security/$ISA/pam\_cracklib.so retry=3 minlen=7 dcredit=-2 ocredit=-2 difok=2 maxrepeat=2

suc250:/etc/pam.d>grep PASS\_MIN\_LEN /etc/login.defs | grep -v "#"

PASS\_MIN\_LEN 7

Usuarios con excepción (Válido para todos los parámetros de PAM de ahora en adelante):

Solo root queda exceptuado de estas reglas con esta configuración, root puede además fijar el password de cualquier usuario y solo será advertido. Para obligar a cambiar el password en el próximo login debe ejecutarse:

suc250:/root>chage -d 0 hmessina

B- Conteniendo tanto caracteres numéricos como alfabéticos

#### AIX:

Parámetros

|  |
| --- |
| **minalpha**: Mínimo de caracteres alfabéticos |
| **minother**: Mínimo de caracteres no alfabéticos |
| **mindiff**: Mínimo de caracteres que estuvieron presentes en el password previo y que no pueden ser usados en el nuevo |
| **maxrepeats**: Mínimo de caracteres que no pueden estar repetidos |

Control (individual):

Verificar los siguientes valores: minalpha=4 minother=2 mindiff=3 maxrepeats=2

adm01:/home/root>lsuser -a minalpha minother mindiff maxrepeats hmessina

hmessina minalpha=4 minother=2 mindiff=3 maxrepeats=2

Corrección (global):

adm01:/home/root>chuser minalpha= minother= mindiff= maxrepeats= hmessina *<- Hacerlo por c/user*

adm01:/home/root>chsec -f /etc/security/user -s default -a minalpha=4 -a minother=2 -a mindiff=3 -a maxrepeats=2

Usuarios con excepción (individual):

adm01:/home/root>chuser minalpha=0 minother=0 mindiff=0 maxrepeats=0 root

#### LINUX:

Parámetros

**lcredit** (valor negativo): Mínimo de caracteres en minúsculas

**ucredit** (valor negativo): Mínimo de caracteres en mayúsculas

**dcredit** (valor negativo): Mínimo de caracteres con dígitos numéricos

**ocredit** (valor negativo): Mínimo de caracteres no alfabéticos

**difok** (menor o igual **minlen**): Mínimo de caracteres diferentes al password previo

**maxrepeat**: Máximo de caracteres consecutivos que pueden estar repetidos

Control y corrección (global):

Verificar que existan en el archivo /etc/pam.d/system-auth los parámetros dcredit=-2, ocredit=-2, difok=2 y maxrepeat=2 en el la línea del módulo **pam\_cracklib.so** del stack de PAM en la sección password. Si no fuera así editar el archivo y agregarlos

suc250:/etc/pam.d>grep cracklib system-auth

password requisite /lib/security/$ISA/pam\_cracklib.so retry=3 minlen=7 dcredit=-2 ocredit=-2 difok=2 maxrepeat=2

NOTA: Linux rechazará el nuevo password si no cumple con estos requisitos informarando alguno de los siguientes:

BAD PASSWORD: it is WAY too short

BAD PASSWORD: it does not contain enough DIFFERENT characters

BAD PASSWORD: is too simple

BAD PASSWORD: it is too simplistic/systematic

1. No permitiendo la utilización de cualquiera de las últimas cuatro contraseñas manipuladas

#### AIX:

Parámetro

**histsize**

Control (individual):

Verificar que histsize tenga un valor de 4

adm01:/home/root>lsuser -a histsize hmessina

hmessina histsize=4

Corrección (global):

adm01:/home/root>chuser histsize= hmessina *<- Hacerlo por c/user*

adm01:/home/root>chsec -f /etc/security/user -s default -a histsize=4

Usuarios con excepción (individual):

adm01:/home/root>chuser histsize=0 root

#### LINUX:

Parámetro

**remember**

Control y corrección (global):

Verificar que exista en el archivo /etc/pam.d/system-auth el parámetro remember=4 en el la línea del módulo **pam\_unix2.so** del stack de PAM en la sección password. Si no fuera así editar el archivo y agregarlo

Verificar además que exista el archivo /etc/security/opasswd, si no estuvise crearlo con permisos 0600 y owner root

suc250:/etc/pam.d>grep remember system-auth

password sufficient /lib/security/$ISA/pam\_unix.so nullok use\_authtok md5 shadow remember=4

suc250:/etc/pam.d>touch /etc/security/opasswd

suc250:/etc/pam.d>chown root:root /etc/security/opasswd

suc250:/etc/pam.d>chmod 600 /etc/security/opasswd

suc250:/etc/pam.d>ls -l /etc/security/opasswd

-rw------- 1 root root 0 Jul 23 2007 /etc/security/opasswd

1. Limitando los intentos de acceso repetidos mediante el bloqueo de la ID de usuario después de más de seis intentos

## *AIX:*

Parámetro

**loginretries**

Control (individual):

Verificar que loginretries tenga un valor de 6

adm01/home/hmessina>lsuser -a loginretries hmessina

hmessina loginretries=6

Corrección (global):

adm01:/home/root>chuser loginretries= hmessina *<- Hacerlo por c/user*

adm01:/home/root>chsec -f /etc/security/user -s default -a loginretries=6

Usuarios con excepción (individual):

adm01:/home/root>chuser loginretries=0 root

#### LINUX:

Parámetro

**deny**

Control y corrección (global):

Verificar que exista en el archivo /etc/pam.d/system-auth el parámetro deny=6 y no\_magic\_root en el la línea del módulo **pam\_tally2.so** del stack de PAM en las secciones auth y account. Si no fuera así editar el archivo y agregarlo

suc250:/etc/pam.d>grep tally system-auth

auth required /lib/security/$ISA/pam\_tally2.so deny=6 no\_magic\_root unlock\_time=1800

Se puede agregar el parámetro retry=3 en cracklib para que desconecte la sesión a los 3 intentos fallidos

suc250:/etc/pam.d>grep retry system-auth  
password requisite /lib/security/$ISA/pam\_cracklib.so retry=3 minlen=7 dcredit=-2 ocredit=-2 difok=2 maxrepeat=2

Usuarios con excepción (Válido para todos los parámetros de PAM de ahora en adelante):

E l parámetro no\_magic\_root evita que el usuario **root** se bloquee por intentos fallidos de password

suc250:/etc/pam.d>grep no\_magic\_root system-auth  
auth required /lib/security/$ISA/pam\_tally2.so deny=6 no\_magic\_root unlock\_time=1800

1. Confirmación de bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite la ID del usuario

## *AIX:*

Parámetro

**TODO**

Control (individual):

Verificar que TODO tenga un valor de TODO

adm01/home/hmessina>

Corrección (global):

adm01:/home/root>

Usuarios con excepción (individual):

adm01:/home/root>TODO root

#### LINUX:

Parámetro

**unlock\_time**

Control y corrección (global):

Verificar que exista en el archivo /etc/pam.d/system-auth el parámetro unlock\_time=1800 en el la línea del módulo **pam\_tally2.so** del stack de PAM en la sección account. Si no fuera así editar el archivo y agregarlo

suc250:/etc/pam.d>grep no\_magic\_root system-auth  
auth required /lib/security/$ISA/pam\_tally2.so deny=6 no\_magic\_root unlock\_time=1800

1. Reingreso de contraseña luego de una inactividad mayor a 15 minutos

## *AIX:*

Parámetro

**logintimeout**

Control (global):

Verificar que logintimeout tenga un valor de 900

adm01/home/hmessina>lssec -f /etc/security/login.cfg -s usw -a logintimeout

usw logintimeout=900

Corrección (global):

adm01:/home/root>chsec -f /etc/security/login.cfg -s usw -a logintimeout=900

Usuarios con excepción (individual):

Este valor no debería tener una excepción

#### LINUX:

Parámetro

**TMOUT**: Variable de entorno

Control (global):

Verficar que la variable TMOUT esté definida con un valor de 900 y sea read only

suc02:/root>echo $TMOUT

900

suc02:/root>export TMOUT=900

ksh: TMOUT: is read only

suc02:/root>

Corrección (global):

Agregar al final del archivo /etc/profile las siguientes lineas:

suc02:/etc>grep TMOUT profile

TMOUT=900

readonly TMOUT

export TMOUT

## ANEXO – Vencimiento de contraseñas:

El vencimiento de las contraseñas no aparece como requisito en el documento original, por lo que se toma el siguiente criterio:

Vencimiento = 60 días a partir del cambio

Permitir cambio = 7 días luego del cambio

Advertencia = 5 días antes del vencimiento

Bloqueo de cuenta = 14 días de inactividad desde el vencimiento

## *AIX:*

Parámetros

**maxage**: Expiración de contraseña en semanas **minage**: Permitir cambio de contraseña como mínimo cada tantas semanas **pwdwarntime**: Advertencia de vencimiento de contraseña en días

**maxexpired**: Indica cuántas semanas desde el vencimento del password, se puede cambiar la contraseña antes de bloquear la cuenta.

Control (individual):

Verificar que los parámetros tengan los siguientes valores: maxage=8, minage=1, pwdwarntime=5 y maxexpired=2

adm01/home/hmessina>lsuser -a maxage minage pwdwarntime maxepxired hmessina

hmessina maxage=8 minage=1 pwdwarntime=5

Corrección (global):

adm01:/home/root>chuser maxage= minage= pwdwarntime= maxexpired= hmessina *<- Hacerlo por c/user*

adm01:/home/root>chsec -f /etc/security/user -s default -a maxage=8 minage=1 pwdwarntime=5

Usuarios con excepción (individual):

adm01:/home/root>chuser maxage=0 minage=0 maxexpired=0 root

Script para aplicar todas las correcciones en un server:

for i in $(lsuser ALL | awk '{ print $1 }') ; do chuser minage= maxage= maxexpired= minalpha= minother= minlen= mindiff= maxrepeats= loginretries= histsize= $i ; done

chuser loginretries=0 minlen=0 maxage=0 minage=0 maxexpired=0 root

chsec -f /etc/security/user -s default -a minage=1 -a maxage=8 -a maxexpired=2 -a minalpha=4 -a minother=2 -a minlen=7 -a mindiff=3 -a maxrepeats=2 -a loginretries=6 -a histsize=4

chsec -f /etc/security/login.cfg -s usw -a logintimeout=900

#### LINUX:

Parámetros

**PASS\_MAX\_DAYS**

**PASS\_MIN\_DAYS**

**PASS\_WARN\_AGE**

Control (individual):

Verificar los valores de mínimo (m), máximo (M), warning (W) e inactive (I), establecidos para cada usuario:

slnxapp2:/etc>chage -l hmessina

Last password change : Jul 05, 2012 <- fecha base

Password expires : Sep 03, 2012

Password inactive : Sep 17, 2012

Account expires : never

Minimum number of days between password change : 7

Maximum number of days between password change : 60

Number of days of warning before password expires : 5

Verificar además que estén configurados estos valores en el archivo /etc/login.defs: PASS\_MAX\_DAYS 60, PASS\_MIN\_DAYS 7 y PASS\_WARN\_AGE 5

slnxapp2:/etc>grep PASS login.defs | grep -v "#"

PASS\_MAX\_DAYS 60

PASS\_MIN\_DAYS 7

PASS\_MIN\_LEN 7

PASS\_WARN\_AGE 5

Corrección (individual):

slnxapp2:/etc>chage -d today -m 7 -M 60 -W 5 -I 14 hmessina

Usuarios con excepción (individual):

slnxapp2:/etc>chage -d today -m -1 -M -1 -W 5 -I -1 root

Script para aplicar todas las correcciones en un server, contemplando los usuarios conocidos con excepción:

for i in $(cat /etc/passwd | awk -F : '$3 >= 500 { print $1 }'| egrep -v 'oracle|sfctrl|vprctrl|ctmsrv|ctmagt|pchecker|sts')

do

echo "usuario $i"

chage -d today -m 7 -M 60 -W 5 –I 14 $i

done

for i in root oracle sfctrl vprctrl ctmsrv ctmagt pchecker sts

do

echo "usuario $i"

chage -d today -m -1 -M -1 -W 5 -I -1 $i

done

Script perl para modificar el archivo /etc/login.defs a los valores requeridos:  
  
my $anterior = "/etc/login.defs.bak"; <- Ejecutar antes: mv /etc/login.defs /etc/login.defs.bak

my $nuevo = "/etc/login.defs";

my $linea;

open ($ENTRADA, "<", "$anterior") or die ("No se puede abrir $anterior");

open ($SALIDA, ">", "$nuevo") or die ("No se puede abrir $nuevo");

print "Escribiendo $nuevo";

while (<$ENTRADA>) {

chomp();

$linea = $\_;

if ( m/PASS\_MAX\_DAYS/ and (substr ($linea, 0, 1) ne "#")) {

$linea = "PASS\_MAX\_DAYS\t60";

}

if ( m/PASS\_MIN\_DAYS/ and (substr ($linea, 0, 1) ne "#")) {

$linea = "PASS\_MIN\_DAYS\t7";

}

if ( m/PASS\_MIN\_LEN/ and (substr ($linea, 0, 1) ne "#")) {

$linea = "PASS\_MIN\_LEN\t7";

}

if ( m/PASS\_WARN\_AGE/ and (substr ($linea, 0, 1) ne "#")) {

$linea = "PASS\_WARN\_AGE\t5";

}

print $SALIDA "$linea\n";

}

print "\n";

close $ENTRADA;

close $SALIDA;

Configuración del archivo /etc/pam.d/system-auth:  
  
# PAM modificado para estar en cumplimiento con PCI-DSS - no alterar

auth required /lib/security/$ISA/pam\_env.so

auth required /lib/security/$ISA/pam\_tally2.so deny=6 no\_magic\_root unlock\_time=1800

auth sufficient /lib/security/$ISA/pam\_unix.so likeauth nullok

auth required /lib/security/$ISA/pam\_deny.so

account required /lib/security/$ISA/pam\_unix.so

account sufficient /lib/security/$ISA/pam\_succeed\_if.so uid < 100 quiet

account required /lib/security/$ISA/pam\_permit.so

password requisite /lib/security/$ISA/pam\_cracklib.so retry=3 minlen=7 dcredit=-2 ocredit=-2 difok=2 maxrepeat=2

password sufficient /lib/security/$ISA/pam\_unix.so nullok use\_authtok md5 shadow remember=4

password required /lib/security/$ISA/pam\_deny.so

session required /lib/security/$ISA/pam\_limits.so

session required /lib/security/$ISA/pam\_unix.so

## ANEXO 2 – Referencias en la web:

<http://en.wikipedia.org/wiki/PCI_DSS>

<http://www.ibm.com/developerworks/aix/library/au-password_expiry/index.html>

<http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html>

<http://linux.die.net/man/8/pam_cracklib>

<http://linux.die.net/man/8/pam_tally>