Administración del usuario de Cisco Policy Suite

Contenido

[Introducción](#)
[Administración de usuarios para VM QPS](#)
[Crear un nuevo usuario local con un grupo predeterminado](#)
[Crear un nuevo usuario local con un nuevo grupo](#)
[Modificar la cuenta de usuario](#)
[Administración de usuarios para Control Center](#)
[Administración de usuarios para creador de políticas](#)
[Crear un usuario](#)
[Modificar un usuario](#)
[Información útil](#)

Introducción

Este documento describe cómo crear, configurar y actualizar usuarios (administración de usuarios) en Quantum Policy Suite (QPS). Esto es más específico de QPS Release 5.5 y posteriores. Se describe la administración de usuarios para estas tres secciones dentro de QPS:

- Administración de usuarios para VM QPS (todas las VM; como PCRFClient0x, Lb0x y QNS0x)
- Administración de usuarios para Control Center
- Administración de usuarios para el repositorio de Policy Builder (PB-Subversion [PB-SVN])

Nota: Se cambió el nombre de QPS a Cisco Policy Suite (CPS) en la versión 8.0.0.

Administración de usuarios para VM QPS

En esta sección se explica la gestión de usuarios en QPS VM (LB, PCRFClient, QNS, etc.).

Crear un nuevo usuario local con un grupo predeterminado

De forma predeterminada, una adición de usuario local crea el nombre de grupo igual que el nombre de usuario. La adición de grupo no es obligatoria.

1. Ingrese el comando **useradd -m -d /home/<*user id*> -c "Local User" <*user id*>** para crear el id de usuario. En este ejemplo es 'aravibal'.

```
[root@AIO-POD1 ~]# useradd -m -d /home/aravibal -c "Local User" aravibal
[root@AIO-POD1 ~]#
```

2. Ingrese el comando **passwd <*user id*>** para establecer la contraseña para el usuario recién creado.

```
[root@AIO-POD1 ~]# passwd aravibal
Changing password for user aravibal.
New UNIX password:
```

3. Otorgue acceso al usuario local recién creado. Edite el archivo **/etc/security/access.conf** y agregue esta línea:

```
"+:<User ID>:ALL
```

4. Edite el archivo **/etc/ssh/sshd_config** y agregue el nuevo usuario al final de la línea 'AllowUsers'.

```
[root@AIO-POD1 ~]# vi /etc/ssh/sshd_config
[root@AIO-POD1 ~]# grep AllowUsers /etc/ssh/sshd_config
AllowUsers nx remote qns root aravibal
[root@AIO-POD1 ~]#
```

5. Ingrese el comando **service sshd restart** para reiniciar el servicio Secure Shell Daemon (SSHD).

```
[root@AIO-POD1 ~]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@AIO-POD1 ~]#
[root@AIO-POD1 ~]#
```

6. Inicie sesión como el nuevo usuario e ingrese el comando **ssh localhost -l <*new_create_user id*>** para mostrar la ID de usuario y el nombre de grupo.

```
[root@AIO-POD1 ~]# ssh localhost -l aravibal
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
aravibal@localhost's password:
[aravibal@AIO-POD1 ~]$ id
uid=505(aravibal) gid=505(aravibal) groups=505(aravibal)
[aravibal@AIO-POD1 ~]$
```

Crear un nuevo usuario local con un nuevo grupo

1. Ingrese el comando **groupadd *<groupname>*** para crear un nuevo grupo.

```
[root@AIO-POD1 ~]# groupadd ciscoQPS
```

2. Ingrese el comando **cat /etc/group** para verificar su ID de grupo recién creado en el archivo /etc/group.

```
[root@AIO-POD1 ~]# useradd -m -d /home/grouptestuser -c "Local User" grouptestuser -g ciscoQPS
[root@AIO-POD1 ~]#
[root@AIO-POD1 ~]#
```

3. Ingrese el comando **useradd -m -d /home/<*user id*> -c "Local User" <*user id*> -g<**new group name**> para crear el nuevo usuario local con el nuevo grupo.

```
grouptestuser@localhost's password:
[grouptestuser@AIO-POD1 ~]$ id
uid=506(grouptestuser) gid=506(ciscoQPS) groups=506(ciscoQPS)
[grouptestuser@AIO-POD1 ~]$
```

4. Complete los pasos 3 a 6 en la sección [Creación de un nuevo usuario local con un grupo predeterminado](#).

Modificar la cuenta de usuario

Complete esta sección para modificar la configuración para el envejecimiento de la contraseña, bloqueo, desbloqueo y vencimiento de la cuenta.

Ingrese el comando **change -l** ***<user id>*** para verificar la antigüedad de vencimiento de la contraseña.

```
[root@AIO-POD1 svn]# chage -l test1
Last password change                                    : May 02, 2014
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
```

El administrador del sistema puede completar estas acciones según sea necesario:

- Ingrese el comando **change -M** ***<number of days > <user id>*** para establecer la fecha de vencimiento de la contraseña para cualquier usuario.El número de días se calcula a partir de la fecha actual del sistema. Por ejemplo, si desea establecer la caducidad de la contraseña después de 25 días, introduzca **cambio -M 25** ***<ID de usuario>***. La opción -M actualiza tanto la contraseña caduca como el número máximo de días entre el cambio de contraseña.

```
[root@AIO-POD1 svn]# chage -M 25 test1
[root@AIO-POD1 svn]# chage -l test1
Last password change                                    : May 02, 2014
Password expires                                        : May 27, 2014
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 25
Number of days of warning before password expires       : 7
[root@AIO-POD1 svn]# date
Wed May  7 02:20:01 MDT 2014
[root@AIO-POD1 svn]#
```

- Ingrese el **comando de cambio -E "AAAA-MM-DD"** ***<id de usuario>*** para establecer la fecha de vencimiento de la cuenta para cualquier usuario. La fecha debe indicarse en el formato "AAAA-MM-
DD".

```
[root@AIO-POD1 svn]#
[root@AIO-POD1 svn]#
[root@AIO-POD1 svn]# chage -E "2015-05-07" test1
[root@AIO-POD1 svn]#
[root@AIO-POD1 svn]#
[root@AIO-POD1 svn]# chage -l test1
Last password change                                    : May 02, 2014
Password expires                                        : May 27, 2014
Password inactive                                       : never
Account expires                                         : May 07, 2015
Minimum number of days between password change          : 0
Maximum number of days between password change          : 25
Number of days of warning before password expires       : 7
[root@AIO-POD1 svn]#
```

- Ingrese el **comando chage -m 0 -M 9999 -I -1 -E -1** ***<user id>*** para inhabilitar el envejecimiento de la contraseña. -m 0 establece el número mínimo de días entre el cambio de contraseña en 0-M 99999 establece el número máximo de días entre los cambios de contraseña en 99999-I -1 (número menos uno) establece la 'Contraseña inactiva' como Nunca-E -1 (número menos uno) establece 'La cuenta vence' en Nunca

```
[root@AIO-POD1 ~]# chage -m 0 -M 999999 -I -1 -E -1 aravibal
[root@AIO-POD1 ~]# chage -l aravibal
Last password change                                    : May 07, 2014
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 999999
Number of days of warning before password expires       : 7
[root@AIO-POD1 ~]#
```

- Ingrese uno de estos comandos para bloquear o desbloquear un usuario: bloquear el usuario - **passwd -l** ***<user id>***desbloquear el usuario - **passwd -u** ***<user id>***
- Ingrese el comando **passwd -S** ***<user id>*** para verificar si el estado de la cuenta está bloqueado.Este resultado consta de siete campos, el segundo campo indica si la cuenta de usuario tiene una contraseña bloqueada (L), no tiene ninguna contraseña (NP) o tiene una contraseña utilizable (P).**Nota:** En la versión 5.5, la opción -S funciona, pero sólo con un usuario a la vez. Deberá comprobar si tiene la opción -a disponible en la versión 6.0. Por ejemplo, ingrese el comando **passwd -Sa**.

```
[root@AIO-POD1 ~]# passwd -l aravibal
Locking password for user aravibal.
passwd: Success
[root@AIO-POD1 ~]# passwd -S aravibal
aravibal LK 2014-05-09 0 999999 7 -1 (Password locked.)
[root@AIO-POD1 ~]# passwd -u aravibal
Unlocking password for user aravibal.
passwd: Success.
[root@AIO-POD1 ~]# passwd -S aravibal
aravibal PS 2014-05-09 0 999999 7 -1 (Password set, MD5 crypt.)
[root@AIO-POD1 ~]#
```

- Ingrese el comando **passwd** ***<user ID>*** para restablecer las contraseñas para todos los ID de usuario, incluido el usuario administrador. Por ejemplo, **passwd broadcast1**.

- Ingrese el comando **faillog -a** para verificar los intentos de inicio de sesión fallidos para todos los
usuarios.

```
[root@AIO-POD1 log]# faillog -a
Login       Failures Maximum Latest                  On

root            0        0   12/31/69 17:00:00 -0700
bin             0        0   12/31/69 17:00:00 -0700
daemon          0        0   12/31/69 17:00:00 -0700
adm             0        0   12/31/69 17:00:00 -0700
lp              0        0   12/31/69 17:00:00 -0700
sync            0        0   12/31/69 17:00:00 -0700
```

- Ingrese el comando **userdel** ***<user id>*** para eliminar el usuario. El comando **userdel -r** ***<user ID>*** quita el directorio principal del usuario. Por ejemplo, **userdel -r aravibal**.

Administración de usuarios para Control Center

Control Center (CC) no está disponible en versiones anteriores de QPS, es decir, CC no está disponible en la versión 2.5.7 de QPS. La GUI de CC sólo está disponible en la versión 5.3 y posteriores de QPS.

Edite este archivo XML en PCRFClient01, '***/etc/broadhop/authentication-provider.xml***', para agregar un nuevo ID de usuario o cambiar la contraseña en CC. Hay dos autoridades para CC, de sólo lectura y admin.

```
<user name="userid" password="password" authorities="ROLE_READONLY"/>

<user name="userid" password="password" authorities="ROLE_SUMADMIN"/>
```

Quite la línea adecuada de este archivo XML para eliminar un usuario.

```
<authentication-provider>
  <user-service>
    <user name="sum-admin" password="broadhop" authorities="ROLE_SUMADMIN"/>
    <user name="admin" password="broadhop" authorities="ROLE_SUMADMIN"/>
    <user name="readonly" password="broadhop" authorities="ROLE_READONLY"/>
    <user name="view " password="broadhop" authorities="ROLE_READONLY"/>
```

Administración de usuarios para creador de políticas

Esta sección explica la administración del usuario en PB.

Crear un usuario

1. Ingrese el comando **htpasswd -b /var/www/svn/password** ***<username> <password>*** en pcrfclient01 para agregar un usuario SVN.**Nota:** En algunos casos, el archivo de contraseña se oculta como .htpasswd. Es posible que deba ingresar **htpasswd -b**

/var/www/svn/.htpasswd *<username>*
<password>.

```
[root@AIO-POD1 /]#
[root@AIO-POD1 /]#
[root@AIO-POD1 /]# htpasswd -b /var/www/svn/password broadhop3 password3
Adding password for user broadhop3
[root@AIO-POD1 /]# cat /var/www/svn/password
broadhop:lO.kr2yt8IEZQ
broadhop1:XyCYz3uCYMJLk
broadhop2:1abtv8E0hkEd6
broadhop3:jWAyE2tHU5EUk
[root@AIO-POD1 /]#
```

2. Edite la línea **admins = broadcast,** *<username>* en el *archivo /var/www/svn/users-access-file* para proporcionar acceso de lectura/escritura al usuario.

```
[root@AIO-POD1 svn]# cat users-access-file
[groups]
admins = broadhop, broadhop1
nonadmins = read-only
[/]
@admins = rw
@nonadmins = r
[root@AIO-POD1 svn]#
```

Modificar un usuario

1. Ingrese el comando **htpasswd /var/www/svn/password** *<username>* para restablecer la contraseña para un usuario actual en PB (repositorio SVN). Por ejemplo, **htpasswd /var/www/svn/password bandhop2**.**Nota:** En algunos casos, el archivo de contraseña se oculta como .htpasswd. Es posible que deba ingresar **htpasswd -b /var/www/svn/.htpasswd** *<username>*
<password>.

```
[root@AIO-POD1 svn]# htpasswd /var/www/svn/password broadhop2
New password:
Re-type new password:
Updating password for user broadhop2
[root@AIO-POD1 svn]#
```

2. Ingrese el comando **htpasswd -D password** *<user id>* para eliminar usuarios en PB (repositorio PB-SVN). Por ejemplo, **htpasswd -D password bandhop1**.

```
[root@AIO-POD1 svn]#
[root@AIO-POD1 svn]# cat password
broadhop:lO.kr2yt8IEZQ
broadhop1:XyCYz3uCYMJLk
broadhop2:AnIGmvtW4ydmk
broadhop3:jWAyE2tHU5EUk
[root@AIO-POD1 svn]# htpasswd -D password broadhop1
Deleting password for user broadhop1
```

3. Ingrese estos comandos para determinar qué usuario ha confirmado recientemente un cambio en PB y quiénes son todos los usuarios que han realizado cambios. **#svn log http://pcrfclient01/repos/configuration/ | más#svn log http://pcrfclient01/repos/configuration/ | grep '^r[0-9]' | awk '{print $3}' | ordenar | uniq**

Información útil

- El usuario predeterminado del sistema 'qns' no tiene una contraseña.
- Utilice 'pwck' y 'grpck' para verificar la integridad de /etc/passwd, /etc/shadow y /etc/group.
- Varios usuarios en PB están disponibles en QPS Release 6.0 y posteriores. En las versiones anteriores, PB puede tener varios usuarios para iniciar sesión y realizar cambios, pero esto da como resultado una invalidación.
- Si desea mantener el tiempo de sesión inactivo, ingrese el comando **export TMOUT=120**. (Los usuarios se desconectarán si están inactivos durante dos minutos = 120 segundos.)
- Puede proteger ***/var/log/httpd/access_log*** cuando el usuario se conecta a PB (repositorio SVN).
- Todas las fallas de autenticación de usuario relacionadas con PB se pueden proteger ***/etc/httpd/logs/error_log***.
- La información relacionada con los privilegios de autenticación y autorización se puede encontrar en ***/var/log/secure***. Por ejemplo, SSHD registra todos los mensajes que incluyen los inicios de sesión fallidos.