Gestion d'utilisateur de suite de stratégie de Cisco

Contenu

Introduction

Ce document décrit comment créer, configure, et des utilisateurs en mise à jour (gestion d'utilisateur) dans la suite de stratégie de Quantum (QPS). C'est plus spécifique à la version 5.5 et ultérieures QPS. La gestion des utilisateurs est décrite pour ces trois sections dans QPS :

- Gestion des utilisateurs pour la VM QPS (toutes les VMs ; comme PCRFClient0x, Lb0x, et QNS0x)
- Gestion des utilisateurs pour le Control Center
- Gestion des utilisateurs pour le builder de stratégie (référentiel de Pb-subversion [PB-SVN])

Remarque: QPS a été renommé à la suite de stratégie de Cisco (CPS) dans la version 8.0.0.

Gestion des utilisateurs pour la VM QPS

Cette section explique au sujet de la gestion des utilisateurs dans la VM QPS (livre, PCRFClient, QNS, et ainsi de suite).

Créez un nouvel utilisateur local avec un groupe par défaut

Par défaut, un ajout d'utilisateur local crée le nom de groupe les mêmes que le nom d'utilisateur. L'ajout de groupe n'est pas obligatoire.

1. Écrivez l'**useradd - m - d /home/** commande de **< *user-id* > de « utilisateur local » du < *user-***

id **> - c** afin de créer l'user-id. Dans cet exemple il est « aravibal ».

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

2. Sélectionnez la commande de **< *user-id* > de passwd** afin de placer le mot de passe pour l'utilisateur de création récente.

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

3. Accès de Grant à l'utilisateur local de création récente. Éditez le fichier de **/etc/security/access.conf** et ajoutez cette ligne :`"+:<User ID>:ALL`
4. Éditez le fichier de **/etc/ssh/sshd_config** et ajoutez le nouvel utilisateur à l'extrémité de la ligne « 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. Sélectionnez la commande de **reprise de sshd de service** afin de redémarrer le service sécurisé du démon de shell (SSHD).

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

6. Ouvrez une session en tant que nouvel utilisateur et écrivez le le **localhost de ssh - l *id* >** commande de **<newly_created_user** afin d'afficher le nom d'user-id et de groupe.

```
[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 ~]$
```

Créez un nouvel utilisateur local avec un nouveau groupe

1. Sélectionnez la commande de ***<groupname> de* groupadd** afin de créer un nouveau groupe.

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

2. Sélectionnez la commande de **/etc/group de cat** afin de vérifier votre identification groupe de création récente dans le fichier /etc/group.

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

3. Écrivez l'**useradd - m - d /home/ *nom* >** commande de ***groupe de* g<new de < *user-id* > -**

user-id > de « utilisateur local » c < - afin de créer le nouvel utilisateur local avec le nouveau groupe.

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

4. Étapes complètes 3 à 6 dans la [création un nouvel utilisateur local avec une] section de [groupe par défaut].

Modifiez le compte utilisateur

Remplissez cette section afin de modifier des configurations pour le vieillissement de mot de passe, verrouillez, la déverrouillez, et rendez compte échéance.

Entrez dans le **chage - l** commande de ***< user-id >*** afin de vérifier l'âge d'expiration du mot de passe.

```
[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
```

L'administrateur système peut se terminer ces actions comme nécessaires :

- Entrez dans le **chage - *<number* M des *jours >*** commande de ***< user-id >*** afin de placer l'expiration date de mot de passe pour tout utilisateur.Le nombre de jours est calculé à partir de la date du système en cours. Par exemple, si vous voudriez placer l'expiration du mot de passe après 25 jours entrez dans le **chage - M 25 *< user-id >***. L'option - M met à jour le mot de passe expire et nombre maximal de jours entre la modification de mot de passe.

```
[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]#
```

- Entrez dans le **chage -** Commande de ***< user-id >*** **E « YYYY-MM-DD »** afin de placer l'expiration date de compte pour tout utilisateur. La date devrait être donnée dans le format « YYYY-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]#
```

- Entrez dans le **chage - m 0 -** commande de ***< user-id >*** **M 99999 - I -1 - E -1** afin de désactiver le vieillissement de mot de passe. - m 0 place le nombre minimal de jours entre la modification de mot de passe à 0- M 99999 place le nombre maximal de jours entre les modifications de mot de passe à 99999- I -1 (nombre sans un) place le « mot de passe inactif » à jamais- E -1 (nombre sans un) place le « compte expire » à
jamais

```
[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 ~]#
```

- Sélectionnez une des ces commandes afin de verrouiller ou déverrouiller un utilisateur : verrouillez l'utilisateur - **passwd - l *< user-id >***déverrouillez l'utilisateur - **passwd - u *< user-id >***
- Entrez dans le **passwd -** Commande de ***< user-id >*** **S** afin de vérifier si la position de compte est verrouillée.Cette sortie se compose de sept champs, le deuxième champ indique si le compte utilisateur a un mot de passe verrouillé (l), n'a aucun mot de passe (NP), ou a un mot de passe utilisable (p).Remarque: Dans la version 5.5 - Travaux d'option S, mais seulement avec un utilisateur à la fois. Vous devrez vérifier si vous avez - de l'option disponible dans la version 6.0. Par exemple, entrez dans le **passwd -** Commande
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 ~]#
```

- Sélectionnez la commande de ***< user-id > de*** **passwd** afin de remettre à l'état initial les mots de passe pour tous les user-id, y compris l'utilisateur d'admin. Par exemple, **passwd**

broadhop1.

- Écrivez le **faillog - une** commande afin de vérifier les échecs de tentative de connexion pour tous les
utilisateurs.

```
[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
```

- Sélectionnez la commande de ***< user-id > d'*****userdel** afin de supprimer l'utilisateur. **L'userdel - la** commande de ***< user-id >*** **r** enlève le répertoire home de l'utilisateur. Par exemple, **userdel - r aravibal**.

Gestion des utilisateurs pour le Control Center

Le Control Center (cc) n'est pas disponible dans les versions antérieures de QPS, cela est cc n'est pas disponible dans la version 2.5.7 QPS. Le GUI cc est disponible seulement dans la version 5.3 et ultérieures QPS.

Éditez ce fichier XML dans PCRFClient01, « ***/etc/broadhop/authentication-provider.xml*** », afin d'ajouter un nouvel user-id ou changer le mot de passe dans le cc. Il y a deux autorités pour le cc, en lecture seule et l'admin.

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

Retirez la ligne correspondante à partir de ce fichier XML afin de supprimer un utilisateur.

```
<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"/>
```

Gestion des utilisateurs pour le builder de stratégie

Cette section explique au sujet de la gestion d'utilisateur en PB.

Créez un utilisateur

1. Écrivez le **htpasswd -** commande de ***<password> de <username>*** **b /var/www/svn/password** sur pcrfclient01 afin d'ajouter un utilisateur SVN.Remarque: Dans certains cas le fichier de

mot de passe est masqué comme .htpasswd. Vous pourriez devoir écrire le **htpasswd - *<password> de <username>* b /var/www/svn/.htpasswd**.

```
[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. Éditez la ligne **admins = broadhop, *<username>*** dans le fichier de ***/var/www/svn/users-access-file*** afin de fournir l'accès lecture/écriture à l'utilisateur.

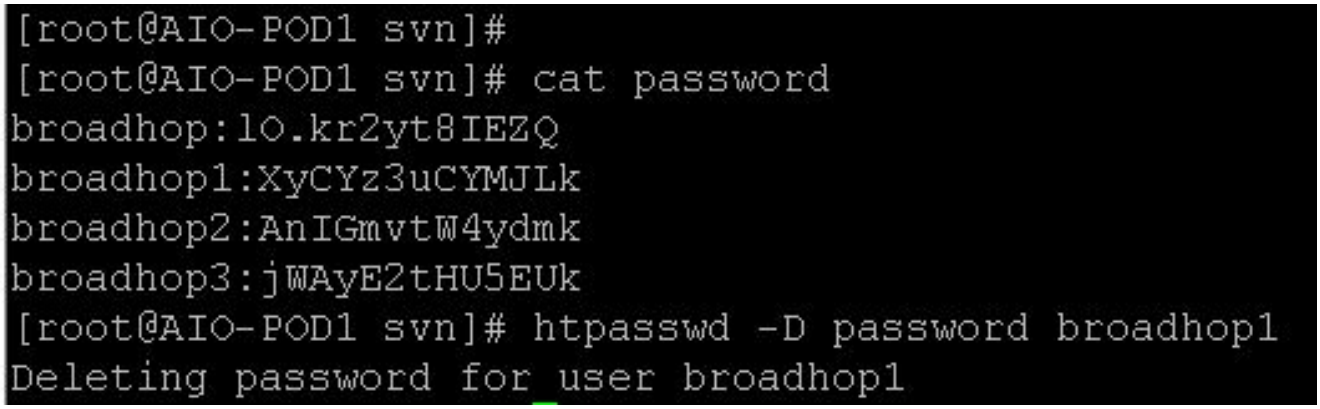
```
[root@AIO-POD1 svn]# cat users-access-file
[groups]
admins = broadhop, broadhop1
nonadmins = read-only
[/]
@admins = rw
@nonadmins = r
[root@AIO-POD1 svn]#
```

Modifiez un utilisateur

1. Sélectionnez la commande de ***<username> de*** **/var/www/svn/password de htpasswd** afin de remettre à l'état initial le mot de passe pour un utilisateur courant en PB (référentiel SVN). Par exemple, **htpasswd /var/www/svn/password broadhop2**.Remarque: Dans certains cas le fichier de mot de passe est masqué comme .htpasswd. Vous pourriez devoir écrire le **htpasswd - *<password> de <username>* b /var/www/svn/.htpasswd**.

```
[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. Écrivez le **htpasswd -** Commande de ***< user-id > de*** **mot de passe D** afin de supprimer des utilisateurs en PB (référentiel PB-SVN). Par exemple, **htpasswd - Mot de passe broadhop1 D**.



3. Sélectionnez ces commandes afin de déterminer quel utilisateur a récemment commis un changement de PB et qui sont tous les utilisateurs qui ont commis des modifications. **log http://pcrfclient01/repos/configuration/ de #svn | pluslog http://pcrfclient01/repos/configuration/ de #svn | grep '^r[0-9] | awk '{copie $3}' | tri | uniq**

Les informations utiles

- L'utilisateur « qns » de paramètres systèmes par défaut n'a pas un mot de passe.
- Employez le « pwck » et le « grpck » afin de vérifier l'intégrité de /etc/passwd, de /etc/shadow, et de /etc/group.
- Les plusieurs utilisateurs en PB sont disponibles dans la version 6.0 et ultérieures QPS. Dans les versions antérieures le PB peut avoir des plusieurs utilisateurs à ouvrir une session et apporter des modifications, mais ceci a comme conséquence un dépassement.
- Si vous voudriez garder le temps de veille de session, sélectionnez la commande de l'**exportation TMOUT=120**. (Les utilisateurs veulent sont enregistré s'ils sont inactifs pour le minutes= deux 120 secondes.)
- Vous pouvez signer */var/log/httpd/access_log* quand l'utilisateur se connecte au PB (référentiel SVN).
- Toutes les pannes d'authentification de l'utilisateur liées au PB peuvent être signé */etc/httpd/logs/error_log*.
- Relatif à l'information aux privilèges d'authentification et d'autorisation peut être trouvé dans */var/log/secure*. Par exemple, SSHD se connecte tous les messages qui incluent l'Institut central des statistiques infructueux de log.