

Пользовательское администрирование комплекта политики Cisco

Содержание

[Введение](#)

[Управление пользователями для VM QPS](#)

[Создайте нового локального пользователя с группой по умолчанию](#)

[Создайте нового локального пользователя с New Group](#)

[Модифицируйте учетную запись пользователя](#)

[Управление пользователями для центра управления](#)

[Управление пользователями для разработчика политики](#)

[Создайте пользователя](#)

[Модифицируйте пользователя](#)

[Полезная информация](#)

Введение

Этот документ описывает, как создать, настроить, и обновить пользователей (пользовательское администрирование) в Комплекте политики Quantum (QPS). Это является более определенным для Выпуска 5.5 QPS и позже. Управление пользователями описано для этих трех разделов в QPS:

- Управление пользователями для VM QPS (все VM; такой как PCRFCClient0x, Lb0x и QNS0x)
- Управление пользователями для центра управления
- Управление пользователями для разработчика политики (подрывная деятельность петабайта [SVN петабайта] репозиторий)

Примечание: QPS был переименован к Комплекту политики Cisco (CPS) в Версии 8.0.0.

Управление пользователями для VM QPS

Этот раздел объясняет об управлении пользователями в VM QPS (LB, PCRFCClient, QNS, и так далее).

Создайте нового локального пользователя с группой по умолчанию

По умолчанию добавление локального пользователя создает имя группы то же как имя пользователя. Добавление группы не является обязательным.

1. Введите `useradd -m -d /домой / <идентификатор пользователя>-с` команда `<user id>` "Локального пользователя" для создания идентификатора пользователя. В данном примере это -
'aravibal'.

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

2. Введите команду `<user id> passwd` для установки пароля для недавно созданного

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

пользователя.

3. Предоставьте доступ недавно созданному локальному пользователю.
Отредактируйте `/etc/security/access.conf` файл и добавьте эту линию: `"+:<User ID>:ALL`
4. Отредактируйте `/etc/ssh/sshd_config` файл и добавьте нового пользователя до конца линии
'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. Введите команду `service sshd restart` для перезапуска Демона Secure Shell (SSHD) сервис.

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

6. Войдите как новый пользователь и введите **локальный узел** `ssh-l` команда `<newly_created_user id>` для показа идентификатора пользователя и имени группы.

```
[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 ~]$
```

Создайте нового локального пользователя с New Group

1. Введите `groupadd` команду `<groupname>` для создания новой

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

2. Введите `кошки/etc/group` команда для проверки недавно созданного идентификатора группы в файле `/etc/group`.

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

3. Введите `useradd -m -d /домой / <идентификатор пользователя>-с` "Локальный

пользователь" <идентификатор пользователя> -g команда <new group name> для создания нового локального пользователя с новой группой.

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

4. Завершенные шаги 3 - 6 в [Создание Нового Локального пользователя с разделом Группы по умолчанию](#).

Модифицируйте учетную запись пользователя

Завершите этот раздел, чтобы модифицировать параметры настройки для устаревания пароля, заблокировать, разблокируйте, и истечение учетной записи.

Введите **chage-l** команда <user id> для проверки возраста истечения срока действия пароля.

```
[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
```

Системный администратор может завершить эти действия по мере необходимости:

- Введите **chage-M** <число дней> команда <user id> для установки даты окончания срока действия пароля для любого пользователя. Число дней вычислено с текущей системной даты. Например, если требуется установить истечение срока действия пароля после того, как 25 дней входят <идентификатор пользователя> **chage-M 25**. Опция-M обновляет и пароль, истекает и максимальное число дней между изменением пароля.

```
[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]#
```

- Введите **chage-E** "YYYY-MM-DD" команда <user id> для установки даты окончания срока действия учетной записи для любого пользователя. Дата должна быть дана в формате "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]# 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]# █

```

- Введите команду `chage-m 0-M 99999-l-1-E-1 <user id>` для отключения устаревания пароля. - m 0 наборов минимальный номер дней между изменением пароля к 0- M 99999 устанавливает максимальное число дней между изменениями пароля к 99999- Я- 1 (номер минус один) устанавливаю 'Пароль, неактивный' в никогда- E-1 (номер минус один) наборы 'Учетная запись истекает' к никогда

```

[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 ~]# █

```

- Введите одну из этих команд, чтобы блокировать или разблокировать пользователя: блокируйте пользователя - `passwd-l <идентификатор пользователя>` разблокируйте пользователя - `passwd-u <идентификатор пользователя>`
- Введите `passwd-S` команда `<user id>`, чтобы проверить, блокирован ли статус учетной записи. Эти выходные данные состоят из семи полей, второе поле указывает, имеет ли учетная запись пользователя блокированный пароль (L), имеет никакой пароль (NP) или имеет применимый пароль (P). **Примечание:** В Выпуске 5.5-S опция работает, но только с одним пользователем за один раз. Необходимо будет проверить, имеете ли вы-а опцию в наличии в Выпуске 6.0. Например, введите `passwd-Sa` команда.

```

[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 ~]# █

```

- Введите команду `<user ID> passwd` для изменения паролей для всех идентификаторов

пользователя, включительно пользователя с правами администратора. Например, `passwd broadhop1`.

- Введите `faillog -a` команда, чтобы проверить, что отказавшие входят в попытки для всех пользователей.

```
[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
```

- Введите `userdel` команду `<user id>` для удаления пользователя. `userdel-r` команда `<user ID>` удаляет главный каталог пользователя. Например, `userdel-r aravibal`.

Управление пользователями для центра управления

Центр управления (CC) не доступен в более ранних версиях QPS, который является CC, не доступно в Выпуске 2.5.7 QPS. GUI CC доступен только в Выпуске 5.3 QPS и позже.

Отредактируйте этот XML-файл в `PCRFCClient01`, `/etc/broadhop/authentication-provider.xml`, чтобы добавить идентификатор нового пользователя или изменить пароль в CC. Существует два полномочий для CC, только для чтения и `admin`.

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

Удалите соответствующую линию из этого XML-файла для удаления пользователя.

```
<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"/>
```

Управление пользователями для разработчика политики

Этот раздел объясняет о пользовательском администрировании в петабайте.

Создайте пользователя

1. Введите `htpasswd-b/var/www/svn/password` команда `<password> <username>` на `pcrfclient01` для добавления пользователя SVN. **Примечание:** В некоторых случаях файл с паролями скрыт как `.htpasswd`. Вы, возможно, должны были бы ввести `htpasswd-b/var/www/svn/.htpasswd <password>`

<username>.

```
[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:jW4yE2tHU5EUk  
[root@AIO-POD1 /]#
```

2. Отредактируйте **admin** линии = **broadhop**, **<username>** в **/var/www/svn/users-access-file** файл для обеспечения доступа для чтения-записи к пользователю.

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

Модифицируйте пользователя

1. Введите **htpasswd/var/www/svn/password** команда **<username>** для изменения пароля для текущего пользователя в петабайте (репозиторий SVN). Например, **htpasswd/var/www/svn/password broadhop2**. **Примечание:** В некоторых случаях файл с паролями скрыт как **.htpasswd**. Вы, возможно, должны были бы ввести **htpasswd-b/var/www/svn/.htpasswd <password>**

<username>.

```
[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. Введите **htpasswd -D** команда **<user id>** пароля для удаления пользователей в петабайте (РЕПОЗИТОРИЙ SVN ПЕТАБАЙТА). Например, **htpasswd-D пароль broadhop1**.

```
[root@AIO-POD1 svn]#  
[root@AIO-POD1 svn]# cat password  
broadhop:1O.kr2yt8IEZQ  
broadhop1:XyCYz3uCYMJLk  
broadhop2:AnIGmvtW4ydmk  
broadhop3:jW4yE2tHU5EUK  
[root@AIO-POD1 svn]# htpasswd -D password broadhop1  
Deleting password for user broadhop1
```

3. Введите эти команды для определения, какой пользователь недавно передал изменение в петабайте и кто все пользователи, которые передали изменения. **#svn** регистрируют <http://pcrfclient01/repos/configuration/> | больше**#svn** регистрируют <http://pcrfclient01/repos/configuration/> `grep, '^r [0-9]' | awk '{распечатывают 3$}' | вид | uniq`

Полезная информация

- У пользователя системного параметра по умолчанию 'qns' нет пароля.
- Используйте 'pwck' и 'grpck' для проверки целостности/etc/passwd,/etc/shadow, и/etc/group.
- Несколько пользователей в петабайте доступны в Выпуске 6.0 QPS и позже. В более ранних версиях петабайт может иметь несколько пользователей, чтобы войти и внести изменения, но это приводит к замене.
- Если требуется поддержать время пустого сеанса, введите команду **TMOUТ=120 экспорта**. (Пользователи выйдутся из системы, если они будут неактивны в течение двух минут = 120 секунд.)
- Когда пользователь соединяется с петабайтом (репозиторий SVN), можно зарегистрироваться **в/var/log/httpd/access_log**.
- Во всех ошибках аутентификации пользователя, отнесенных к петабайту, можно зарегистрироваться**/etc/httpd/logs/error_log**.
- Информация, отнесенная к привилегиям проверки подлинности и авторизация, может быть найдена в**/var/log/secure**. Например, SSHD регистрирует все сообщения, которые включают неуспешный журнал ins.