Cisco Policy Suite 사용자 관리

목차

소개

이 문서에서는 QPS(Quantum Policy Suite)에서 사용자(사용자 관리)를 생성, 구성 및 업데이트하는 방법에 대해 설명합니다. 이는 QPS 릴리스 5.5 이상에만 적용됩니다.사용자 관리는 QPS의 다음 3개 섹션에 대해 설명합니다.

- QPS VM에 대한 사용자 관리(모든 VM,예: PCRFClient0x, Lb0x 및 QNS0x)
- Control Center의 사용자 관리
- 정책 작성기를 위한 사용자 관리(PB-Subversion [PB-SVN] 저장소)

참고:QPS는 버전 8.0.0에서 CPS(Cisco Policy Suite)로 이름이 변경되었습니다.

QPS VM의 사용자 관리

이 섹션에서는 QPS VM(LB, PCRFClient, QNS 등)의 사용자 관리에 대해 설명합니다.

기본 그룹으로 새 로컬 사용자 생성

기본적으로 로컬 사용자 추가는 사용자 이름과 동일한 그룹 이름을 생성합니다.그룹 추가는 필수 사항이 아닙니다.

1. 사용자 ID를 **생성하려면 useradd -m -d /home/<*user id*> -c "Local User" <*user id*>** 명령을 입력합니다. 이 예에서는 'avibal'입니다
.

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

2. 새로 **생성한** 사용자**의** 비밀번호를 설정하려면 passwd <user id> 명령을 입력합니다

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

3. 새로 생성된 로컬 사용자에게 액세스 권한을 부여합니다./etc/security/access.conf 파일을 편집하고 다음 줄을 추가합니다.

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

4. **/etc/ssh/sshd_config** 파일을 편집하고 'AllowUsers' 줄 끝에 새 사용자를 추가합니다

```
[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. SSHD(**Secure** Shell Daemon) 서비스를 재시작하려면 service sshd restart 명령을 입력합니다

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

6. 새 사용자로 로그인하고 사용자 ID 및 그룹 이름을 표시하려면 **ssh localhost -l *<new_created_user id>*** 명령을 입력합니다

```
[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 ~]$
```

새 그룹을 사용하여 새 로컬 사용자 생성

1. 새 그룹을 **만들려면 groupadd *<groupname>*** 명령을 입력합니다

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

2. /etc/group 파일에서 새로 생성된 그룹 ID를 확인하려면 **cat /etc/group** 명령을 입력합니다

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

3. 새 **그룹**으로 새 로컬 사용자**를** 만들려면 **useradd -m -d /home/*<user id>* -c "Local User" *<user id>* -g*<new group name>*** 명령을 입력합니다

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

4. Create a New Local User with a Default Group 섹션에서 3단계부터 6단계까지 완료합니다.

사용자 계정 수정

비밀번호 에이징, 잠금, 잠금 해제 및 계정 만료에 대한 설정을 수정하려면 이 섹션을 완료합니다.

비밀번호 **만료 기간을** 확인하려면 **chage -l *<user id>*** 명령을 입력합니다.

```
[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
```

시스템 관리자는 필요에 따라 다음 작업을 완료할 수 있습니다.

- 모든 사용자의 비밀번호 만료일을 설정하려면 **chage -M *<number of days > <user id>*** 명령을 입력합니다.일수는 현재 시스템 날짜로부터 계산됩니다.예를 들어 25일 후 비밀번호 만료를 설정하려면 chage -**M 25 *<user ID>를 입력합니다*.**-M 옵션은 비밀번호 만료 및 비밀번호 변경 사이의 최대 기간(일)을 모두 업데이트합니다

.

```
[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]#
```

- 모든 사용자의 계정 만료일을 설정하려면 **-E "YYYY-MM-DD" *<user id>*** 명령을 입력합니다.날짜는 "YYYY-MM-DD" 형식으로 지정해야 합니다

.

```
[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]#
```

- 비밀번호 에이징을 비활성화하려면 **-m 0 -M 9999 -I -1 -E -1** ***<user id>*** 명령을 입력합니다. -m 0은 비밀번호 변경 사이의 최소 일수를 0으로 설정합니다.-M 99999는 비밀번호 변경 사이의 최대 일수를 99999로 설정합니다.-I -1(숫자 - 1)은 'Password inactive'를 never로 설정합니다.-E -1(숫자 - 1)은 '계정 만료'를 never로 설정합니다

.

```
[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 ~]#
```

- 사용자를 잠그거나 잠금을 해제하려면 다음 명령 중 하나를 입력합니다. 사용자 잠금 - **passwd -l** ***<user id>***사용자 잠금 해제 - **passwd -u** ***<user id>***
- **passwd -S** ***<user id>*** 명령을 입력하여 계정 상태가 잠겨 있는지 확인합니다.이 출력은 7개의 필드로 구성되며, 두 번째 필드는 사용자 계정에 잠긴 비밀번호(L)가 있는지, 비밀번호(NP)가 없는지 또는 사용 가능한 비밀번호(P)가 있는지 여부를 나타냅니다.**참고:**Release 5.5에서는 -S 옵션이 작동하지만 한 번에 한 명의 사용자만 사용할 수 있습니다.릴리스 6.0에서 -a 옵션을 사용할 수 있는지 확인해야 합니다. 예를 들어 passwd -**Sa** 명령을 입력합니다

.

```
[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 ~]#
```

- admin 사용자**를** 포함하여 모든 사용자 ID에 대한 비밀번호를 재설정하려면 passwd ***<user ID>*** 명령을 입력합니다.예를 들어 passwd **broadhop1과 같습니다**.
- 모든 사용자에 **대한** 실패한 로그인 시도를 확인하려면 faillog -a 명령을 입력합니다

.

```
[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
```

- 사용자를 **삭제하려면** ***<user id>*** 명령을 입력합니다.userdel **-r** ***<user ID>*** 명령은 사용자의 홈 디렉토리를 제거합니다.예를 들어, **userdel -r aravibal입니다**.

Control Center의 사용자 관리

CC(Control Center)는 이전 버전의 QPS에서 사용할 수 없으며, CC는 QPS 릴리스 2.5.7에서 사용할 수 없습니다. CC GUI는 QPS 릴리스 5.3 이상에서만 사용할 수 있습니다.

PCRFClient01, '***/etc/broadhop/authentication-provider.xml***'에서 이 XML 파일을 편집하여 새 사용자 ID를 추가하거나 CC에서 암호를 변경합니다.CC, 읽기 전용 및 관리자를 위한 두 가지 권한이 있습니다.

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

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

사용자를 삭제하려면 이 XML 파일에서 적절한 행을 제거합니다.

```
<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"/>
```

정책 작성기의 사용자 관리

이 섹션에서는 PB의 사용자 관리에 대해 설명합니다.

사용자 생성

1. SVN **사용자를 추가하려면 pcrfclient01에서 htpasswd -b /var/www/svn/password** ***<username> <password>*** 명령을 입력합니다.**참고:**경우에 따라 비밀번호 파일이 .htpasswd로 숨겨집니다.**htpasswd -b /var/www/svn/.htpasswd** ***<username> <password>를*** 입력해야 합니다
   .

```
[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. 사용자에게 읽기/쓰기 액세스 권한을 제공하려면 */var/www/svn/users-access-file* 파일에서 line admins = broadhop, *<username>*을 편집합니다

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

사용자 수정

1. PB(SVN 저장소)에서 현재 사용자의 비밀번호를 재설정하려면 htpasswd /var/www/svn/password *<username>* 명령을 입력합니다. 예를 들어 **htpasswd /var/www/svn/password broadhop2입니다.참고:**경우에 따라 비밀번호 파일이 .htpasswd로 숨겨집니다.**htpasswd -b /var/www/svn/.htpasswd *<username> <password>*를** 입력해야 합니다

```
[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. PB(PB-**SVN** 저장소)의 사용자를 삭제하려면 htpasswd -D password *<user id>* 명령을 입력합니다. 예를 들어 **htpasswd -D password broadhop1입니다**

```
[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. PB에서 최근에 변경 사항을 커밋한 사용자와 변경 사항을 커밋한 모든 사용자를 확인하려면

다음 명령을 입력합니다. **#svn 로그 http://pcrfclient01/repos/configuration/ | 기타#svn 로그 http://pcrfclient01/repos/configuration/ | grep '^r[0-9]' | awk '{print $3}' | 정렬 | uniq**

유용한 정보

- 시스템 기본 사용자 'qns'에 암호가 없습니다.
- /etc/passwd, /etc/shadow 및 /etc/group의 무결성을 확인하려면 'pwck' 및 'grpck'를 사용합니다.
- PB의 여러 사용자는 QPS 릴리스 6.0 이상에서 사용할 수 있습니다.이전 버전에서는 PB에 로그인하여 변경할 수 있는 사용자가 여러 명 있을 수 있지만, 이 경우 재정의가 이루어집니다.
- 유휴 세션 시간을 유지하려면 export **TMOUT=120** 명령**을** 입력합니다.(사용자가 2분 동안 비활성 상태인 경우 로그아웃됩니다= 120초).
- 사용자가 PB(SVN 저장소)에 연결할 때 */var/log/httpd/access_log*를 체크 인할 수 있습니다.
- PB와 관련된 모든 사용자 인증 오류는 */etc/httpd/logs/error_log*에서 확인할 수 있습니다.
- 인증 및 권한 부여 권한과 관련된 정보는 */var/log/secure*에서 찾을 수 있습니다. 예를 들어 SSHD는 실패한 로그인을 포함하는 모든 메시지를 기록합니다.