Cisco ポリシー スイート ユーザ管理

目次

概要

このドキュメントでは Quantum Policy Suite（QPS）内でユーザを作成、変更、更新する方法（ユーザ管理）について説明します。 これは QPS リリース 5.5 以降に特に該当します。 以下に示す QPS 内の 3 つのセクションに分けてユーザ管理を説明します。

- QPS VM（すべての VM、つまり PCRFClient0x、Lb0x、QNS0x など）でのユーザ管理
- Control Center でのユーザ管理
- Policy Builder（PB-Subversion [PB-SVN] リポジトリ）でのユーザ管理

注: バージョン 8.0.0 で QPS は Cisco Policy Suite（CPS）に名前が変更されました。

QPS VM でのユーザ管理

この項では、QPS VM（LB、PCRFClient、QNS など）でのユーザ管理について説明します。

デフォルト グループで新しいローカル ユーザを作成する

デフォルトでは、ローカル ユーザの追加によりユーザ名と同じグループ名が作成されます。 グループの追加は必須ではありません。

1. ユーザ ID の作成には、**useradd -m -d /home/<*user id*> -c "Local User" <*user id*>** コマンドを入力します。 次の例では「aravibal」です。
2. 新しく作成したユーザのパスワード設定には、**passwd <*user id*>** コマンドを入力します。
3. 新しく作成されたローカル ユーザにアクセス権を付与します。 **/etc/security/access.conf** フ

ァイルを編集して、次の行を追加します。
"+:<User ID>:ALL
4. **/etc/ssh/sshd_config** ファイルを編集し、「AllowUsers」の行の最後に新しいユーザを追加します。
5. セキュア シェル デーモン（SSHD）サービスを再起動するために **service sshd restart** コマンドを入力します。
6. 新しいユーザとしてログインして **ssh localhost -l <*newly_created_user id*>** コマンドを入力し、ユーザ ID およびグループ名を表示します。

新しいグループと新しいローカル ユーザを作成する

1. 新しいグループを作成するには、**groupadd <*groupname*>** コマンドを入力します。
2. **cat /etc/group** コマンドを入力し、ファイル /etc/group に新しく作成したグループ ID があるかを確認します。
3. **useradd -m -d /home/<*user id*> -c "Local User" <*user id*> -g<*new group name*>** コマンドを使い、新しく作成したグループに新たなローカル ユーザを追加します。
4. 「デフォルト グループで新しいローカル ユーザを作成する」のステップ 3 ~ 6 を実行します。

ユーザ アカウントの変更

パスワード エイジング、ロック、ロック解除、アカウント期限切れの設定を変更するには、この項の説明に従います。

パスワード期限をチェックするには、**chage -l <*user id*>** コマンドを入力します。

システム管理者は必要に応じて以下の操作を実行できます。

- **chage -M <*number of days* > <*user id*>** コマンドでユーザのパスワード有効期限を設定します。日数は現在のシステム日付から計算されます。 たとえば、25 日後にパスワード有効期限を設定するには、**chage -M 25 <*user ID*>** と入力します。 オプション -M はパスワード変更間隔の最大日数とパスワード有効期限の両方を更新します。
- **chage -E "YYYY-MM-DD" <*user id*>** コマンドでユーザ アカウントの有効期限を設定します。日付は YYYY-MM-DD 形式で指定します。
- **chage -m 0 -M 99999 -I -1 -E -1 <*user id*>** コマンドでパスワードエイジングを無効にします。 -m 0 で、パスワード変更間隔の最小日数を 0 に設定します。-M 99999 でパスワード変更間隔の最大日数を 99999 に設定します。-I -1（マイナス 1）で、「パスワード非アクティブ」が起きないように設定します。-E -1（マイナス 1）で、「アカウント期限切れ」が起きないように設定します。
- ユーザをロックまたはロック解除するには、次のコマンドを入力します。 ユーザのロック：**passwd -l <*user id*>**ユーザのロック解除：**passwd -u <*user id*>**
- **passwd -S <*user id*>** コマンドでアカウントがロックされているかどうかを確認します。この出力には 7 つのフィールドがあり、2 番目のフィールドが、ユーザ アカウントに、ロックされたパスワードがある（L）、パスワードがなし（NP）、使用可能なパスワードがある（P）のどれであるかを示します。**注:** リリース 5.5 でも -S オプションは動作しますが、一度に 1 ユーザしか表示しません。 リリース 6.0 では -a オプションが利用可能かどうかを確認してください。 たとえば、**passwd -Sa** コマンドを入力します。
- 管理者ユーザを含むすべてのユーザでパスワードをリセットするには、**passwd <*user ID*>** コ

マンドを入力します。 例：**passwd broadhop1**
- すべてのユーザについて失敗したログイン試行をチェックするには、**faillog -a** コマンドを入力します。
- ユーザを削除するには、**userdel *<user id>*** コマンドを入力します。 **userdel -r *<user ID>*** コマンドはユーザのホームディレクトリを削除します。 例：**userdel -r aravibal**

Control Center でのユーザ管理

Control Center（CC）は以前のバージョンの QPS では使用できません。つまり QPS リリース 2.5.7 で CC は使用できません。 CC GUI は QPS リリース 5.3 以降でのみ使用可能です。

CC で新しいユーザ ID の追加またはパスワードの変更を行うには、pcrfclient01 の XML ファイル「*/etc/broadhop/authentication-provider.xml*」を編集します。 CC には、読み取り専用と管理者という 2 種類の権限があります。

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

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

ユーザを削除するには、この XML ファイルから該当する行を削除します。

Policy Builder でのユーザ管理

ここでは、PB でのユーザ管理について説明します。

ユーザの作成

1. SVN ユーザを追加するには、pcrfclient01 で **htpasswd -b /var/www/svn/password *<username>* *<password>*** コマンドを入力します。**注:** パスワード ファイルは .htpasswd という隠しファイルの場合があります。 その場合は、**htpasswd -b /var/www/svn/.htpasswd *<username>* *<password>*** と入力する必要があります。
2. ユーザに読み取り/書き込み権限を与えるには、***/var/www/svn/users-access-file*** ファイルの **admins = broadhop, *<username>*** という行を編集します。

ユーザの変更

1. 現在の PB（SVN リポジトリ）ユーザのパスワードをリセットするには **htpasswd /var/www/svn/password *<username>*** コマンドを入力します。 例：**htpasswd /var/www/svn/password broadhop2注:** パスワード ファイルは .htpasswd という隠しファイルの場合があります。 その場合は、**htpasswd -b /var/www/svn/.htpasswd *<username>* *<password>*** と入力する必要があります。
2. PB（SVN リポジトリ）ユーザを削除するには **htpasswd -D password *<user id>*** コマンドを入力します。 例：**htpasswd -D password broadhop1**
3. 最近 PB に変更をコミットしたユーザ、または変更をコミットしたユーザの一覧を確認するには、次のコマンドを入力します。 **##svn log http://pcrfclient01/repos/configuration/ | more##svn log http://pcrfclient01/repos/configuration/ | grep '^r[0-9]' | awk '{print $3}' | sort |**

uniq

有用な情報

- システム既定のユーザ「qns」にパスワードはありません。
- /etc/passwd、/etc/shadow、/etc/group の整合性をチェックするには、pwck および grpck を使用します。
- QPS リリース 6.0 以降では複数のユーザが PB で使用できます。 以前のバージョンの PB でも複数のユーザがログインして変更を行えますが、変更は上書きされます。
- アイドル セッション時間を維持するには、**export TMOUT=120** コマンドを入力します（非アクティブなユーザは 120 秒つまり 2 分でログアウトされます）。
- ユーザが PB（SVN リポジトリ）に接続された時間は */var/log/httpd/access_log* で確認できます。
- PB に関連するすべてのユーザ認証の障害は */etc/httpd/logs/error_log* で確認できます。
- 認証および認証権限に関する情報は */var/log/secure* で確認できます。 たとえば、SSHD にはログインの不成功を含むすべてのメッセージが記録されます。