A administração do usuário da série da política de Cisco

Índice

[Introdução](#)
[Gerenciamento de usuário para QPS VM](#)
[Crie um usuário local novo com um grupo padrão](#)
[Crie um usuário local novo com um grupo novo](#)
[Altere a conta de usuário](#)
[Gerenciamento de usuário para Control Center](#)
[Gerenciamento de usuário para o construtor da política](#)
[Crie um usuário](#)
[Altere um usuário](#)
[Informações úteis](#)

Introdução

Este documento descreve como criar, configurar-lo, e usuários de atualização (a administração do usuário) na série da política do quantum (QPS). Isto é mais específico à liberação 5.5 QPS e mais atrasado. O gerenciamento de usuário é descrito para estas três seções dentro de QPS:

- Gerenciamento de usuário para QPS VM (todos os VM; como PCRFClient0x, Lb0x, e QNS0x)
- Gerenciamento de usuário para Control Center
- Gerenciamento de usuário para o construtor da política (repositório do [PB-SVN] da PB-subversão)

Note: QPS foi rebatizado à série da política de Cisco (CP) na versão 8.0.0.

Gerenciamento de usuário para QPS VM

Esta seção explica sobre o gerenciamento de usuário em QPS VM (LB, PCRFClient, QNS, e assim por diante).

Crie um usuário local novo com um grupo padrão

Àrevelia, uma adição do usuário local cria o nome do grupo o mesmos que o nome de usuário. A adição do grupo não é imperativa.

1. Incorpore o **useradd - m - usuário local" < *usuário* d /home/ < *usuário* -** comando

identificação identificação > - c “- > a fim criar o usuário - identificação a este exemplo que é “aravibal”.
2. Incorpore o comando *identificação da senha < usuário - >* a fim ajustar a senha para o usuário recém-criado.
3. Acesso de Grant ao usuário local recém-criado. Edite o arquivo de **/etc/security/access.conf** e adicionar esta linha:
   `"+:<User ID>:ALL`
4. Edite o arquivo de **/etc/ssh/sshd_config** e adicionar o novo usuário à extremidade da linha “AllowUsers”.
5. Inscreva o **comando service sshd restart** a fim reiniciar o serviço do demônio do Secure Shell (SSHD).
6. Entre como o novo usuário e entre o no **host local do ssh - l <newly_created_user** *identificação >* comando a fim mostrar o usuário - identificação e nome do grupo.

Crie um usuário local novo com um grupo novo

1. Incorpore o comando do *<groupname> do groupadd* a fim criar um grupo novo.
2. Incorpore o comando de **/etc/group do gato** a fim verificar seu ID de grupo recém-criado no arquivo /etc/group.
3. Incorpore o **useradd - m - d /home/ <** *usuário* **- usuário local” <** *usuário identificação* **> - c “-** *identificação* **> -** *nome do grupo* **>** comando do **g<new** a fim criar o usuário local novo com o grupo novo.
4. Termine etapas 3 com 6 na criação um usuário local novo com uma seção do grupo padrão.

Altere a conta de usuário

Termine esta seção a fim alterar ajustes para o envelhecimento de senha, trave-a, destrave-a, e explique-a expiração.

Entre no **chage - l <** *usuário* **-** comando *identificação >* a fim verificar a idade da expiração de senha.

O administrador de sistema pode terminar estas ações como necessárias:

- Entre no **chage -** *<number* **M dos** *dias > < usuário -* comando *identificação >* a fim ajustar a data de expiração da senha para algum usuário.O número de dias é calculado da data do sistema atual. Por exemplo, se você gostaria de ajustar a expiração de senha após 25 dias entre no **chage - M25** *< usuário - identificação >*. A opção - M atualiza a senha expira e número máximo de dias entre a mudança da senha.
- Entre no **chage -** Comando *identificação E “YYYY-MM-DD” < usuário - >* a fim ajustar a data de expiração da conta para algum usuário. A data deve ser dada no formato “YYYY-MM-DD”.
- Entre no **chage - m 0 -** comando *identificação E-1 M 99999 - I-1 - < usuário - >* a fim desabilitar o envelhecimento de senha. - m 0 ajusta o número mínimo de dias entre a mudança da senha a 0- M 99999 ajusta o número máximo de dias entre mudanças da senha a 99999- O I-1 (número menos um) ajusta a “senha inativa” a nunca- O E-1 (número menos um) ajusta a “conta expira” a nunca
- Incorpore um destes comandos a fim travar ou destravar um usuário: trave o usuário - **senha - l** *< usuário - identificação >*destrave o usuário - **senha - u** *< usuário - identificação >*

- Entre na **senha -** Comando ***identificação S < usuário - >*** a fim verificar se o estado de conta esteja travado.Esta saída consiste em sete campos, o segundo campo indica se a conta de usuário tem uma senha fechado (L), não tem nenhuma senha (NP), ou tem uma senha útil (P).**Note**: Na liberação 5.5 - Trabalhos da opção S, mas somente com um usuário de cada vez. Você terá que verificar se você tem - a opção disponível na liberação 6.0. Por exemplo, entre na **senha -** Comando **Sa**.
- Entre na **senha *< usuário - identificação >*** comando a fim restaurar as senhas para todo o usuário - os ids, inclusivos do usuário admin. Por exemplo, **senha broadhop1**.
- Incorpore o **faillog - um** comando a fim verificar as falhas de tentativa de login para ver se há todos os usuários.
- Incorpore o comando ***identificação do userdel < usuário - >*** a fim suprimir do usuário. **O userdel -** comando ***identificação r < usuário - >*** remove o diretório home do usuário. Por exemplo, **userdel - r aravibal**.

Gerenciamento de usuário para Control Center

Control Center (CC) não está disponível nas versões anterior de QPS, isso é CC não está disponível na liberação 2.5.7 QPS. O CC GUI está disponível somente na liberação 5.3 QPS e mais atrasado.

Edite este arquivo XML em PCRFClient01, "***/etc/broadhop/authentication-provider.xml***", a fim adicionar um novo usuário - identificação ou mudar a senha no CC. Há duas autoridades para o CC, de leitura apenas e o admin.

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

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

Remova a linha apropriada deste arquivo XML a fim suprimir de um usuário.

Gerenciamento de usuário para o construtor da política

Esta seção explica sobre a administração do usuário no PB.

Crie um usuário

1. Incorpore o **htpasswd -** ***comando <password> do <username>*** **b /var/www/svn/password em** pcrfclient01 a fim adicionar um usuário SVN.**Note**: Em alguns casos o arquivo de senha é hidden como .htpasswd. Você pôde precisar de incorporar o **htpasswd -** ***<password> do <username>*** **b /var/www/svn/.htpasswd**.
2. Edite a linha **admins = broadhop,** ***<username> no*** arquivo de ***/var/www/svn/users-access-file*** a fim fornecer o acesso de leitura/gravação ao usuário.

Altere um usuário

1. Incorpore o comando do ***<username> de /var/www/svn/password do htpasswd*** a fim

restaurar a senha para um usuário atual em PB (repositório SVN). Por exemplo, **htpasswd /var/www/svn/password broadhop2**.**Note**: Em alguns casos o arquivo de senha é hidden como .htpasswd. Você pôde precisar de incorporar o **htpasswd -** ***<password> do <username>*** **b /var/www/svn/.htpasswd**.

2. Incorpore o **htpasswd -** Comando ***identificação da senha D < usuário - >*** a fim suprimir de usuários em PB (repositório PB-SVN). Por exemplo, **htpasswd - Senha broadhop1 D**.
3. Incorpore estes comandos a fim determinar que usuário comprometeu recentemente uma mudança no PB e quem são todos os usuários que comprometeram mudanças. **log http://pcrfclient01/repos/configuration/ do #svn | maislog http://pcrfclient01/repos/configuration/ do #svn | grep '^r[0-9] | awk '{cópia $3}' | tipo | uniq**

Informações úteis

- O usuário “qns” do padrão de sistema não tem uma senha.
- Use o “pwck” e o “grpck” a fim verificar a integridade de /etc/passwd, de /etc/shadow, e de /etc/group.
- Os usuários múltiplos no PB estão disponíveis na liberação 6.0 QPS e mais atrasado. Nas versões anterior o PB pode ter os usuários múltiplos para entrar e fazer mudanças, mas este conduz a uma ultrapassagem.
- Se você gostaria de manter o tempo da sessão ociosa, incorpore o comando da **exportação TMOUT=120**. (Os usuários estarão registrados para fora se são inativos para o minutes= dois 120 segundos.)
- Você pode verificar dentro ***/var/log/httpd/access_log*** quando o usuário conecta a PB (repositório SVN).
- Todas as falhas da autenticação de usuário relativas ao PB podem ser ***/etc/httpd/logs/error_log*** dentro verificado.
- Relativo à informação aos privilégios da authentication e autorização pode ser encontrado em ***/var/log/secure***. Por exemplo, o SSHD registra todas as mensagens que incluem o ins mal sucedido do log.