User can only rsync files with no shell access

Ein lokaler User, soll ausschlisslich mit rsync Daten vom Server kopieren können. **(Er darf sich nicht auf einer Shell anmelden können!)**

Möglichkeit 1 - Konfiguration / Umsetzung mit Skript

Achtung: Es wird dringend empfohlen, die Möglichkeit 2 umzusetzen, da Möglichkeit 1 nicht zu 100% sicher ist.

1. Create a new user (pfrsync) as future rsync User:

```
# useradd pfrsync
```

2. Add a new group (pfrsynconly) and add the user to that group:

```
# groupadd pfrsynconly
# usermod -g pfrsynconly pfrsync
```

3. Set password for the pfrsync user.

```
 # passwd pfrsync
```

4. Create check_command Skript and set correct permissions as follows:

```
# touch /home/pfrsync/check_command.sh
# chmod +x /home/pfrsync/check_command.sh
# chown pfrsync:pfrsynconly /home/pfrsync/check_command.sh

# vim /home/pfrsync/check_command.sh
```

```
#!/bin/bash
case $SSH_ORIGINAL_COMMAND in
 'rsync'*)
    $SSH_ORIGINAL_COMMAND
    ;;
 *)
    echo "Access Denied"
    ;;
esac
```

5. Modify /etc/ssh/sshd_config as following:

```
 # vim /etc/ssh/sshd_config
```

```
#
# sshd_config managed by puppet, do not edit by hand!
```

```
#

Port 22
ListenAddress 172.31.130.28
Protocol 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
LoginGraceTime 2m

PermitRootLogin no
StrictModes yes
DSAAuthentication yes
AuthorizedKeysFile /etc/ssh/authorized_keys/%u
HostbasedAuthentication no
IgnoreRhosts yes
PasswordAuthentication no
PermitEmptyPasswords no

ChallengeResponseAuthentication no
UsePAM yes

X11Forwarding yes
UsePrivilegeSeparation yes

Subsystem       sftp    /usr/libexec/openssh/sftp-server
ClientAliveInterval 60
ClientAliveCountMax 5
AllowTcpForwarding yes

LogLevel INFO
MaxAuthTries 4
PermitUserEnvironment no
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group-
exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521
MACs hmac-sha2-256,hmac-sha2-512
PubkeyAuthentication yes
AllowAgentForwarding yes

Match group pfrsynconly
       #ChrootDirectory /var/lib/pulp
       X11Forwarding no
       AllowTcpForwarding no
       AllowAgentForwarding no
       PasswordAuthentication yes
       ForceCommand /home/pfrsync/check_command.sh
```

- **Keep in mind:** There is no need, to create an Group, if just one user should be able to have Access. In this case replace “Match group pfrsynconly” with “Match user pfrsync”

After all changes, restart sshd!

```
# systemctl restart sshd
```

Möglichkeit 2 - Konfiguration / Umsetzung mit Lshell

Sichere und unumgehbare Varante durch Restrictet Shell!

1. Create a new user (pfrsync) as future rsync User:

```
# useradd pfrsync
```

2. Install lshell Package and add the user to it's group:

```
# yum install lshell
# usermod -aG lshell pfrsync
```

3. Set password for the pfrsync user.

```
 # passwd pfrsync
```

4. Replace default Shell for User “pfrsync” and make nessesary configuration changes:

```
# chsh -s /usr/bin/lshell pfrsync

# vim /etc/lshell.conf
```

```
# lshell.py configuration file
#
# $Id: lshell.conf,v 1.27 2010-10-18 19:05:17 ghantoos Exp $

[global]
logpath         : /var/log/lshell/
loglevel        : 2
#syslogname      : myapp

[default]
allowed         : ['ls','cd','ll']
forbidden       : [';', '&', '|','`','>','<', '$(', '${']
##  number of warnings when user enters a forbidden value before
getting
##  exited from lshell, set to -1 to disable.
warning_counter : 2
aliases         : {'ll':'ls -l', 'vim':'rvim'}
```

```
##  list of command allowed to execute over ssh (e.g. rsync, rdiff-
backup, etc.)
#overssh         : ['ls', 'rsync']

##  logging strictness. If set to 1, any unknown command is considered
as
##  forbidden, and user's warning counter is decreased. If set to 0,
command is
##  considered as unknown, and user is only warned (i.e. *** unknown
synthax)
strict          : 0

##  force files sent through scp to a specific directory
#scpforce        : '/home/bla/uploads/'

##  history file maximum size
#history_size     : 100

##  set history file name (default is /home/%u/.lhistory)
#history_file     : "/home/%u/.lshell_history"

[pfrsync]
path            : ['/var/lib/pulp', '/home/pfrsync']
home_path       : '/var/lib/pulp'
overssh         : ['ls', 'rsync']
##  define the script to run at user login
#login_script     : "/path/to/myscript.sh"
```

5. Modify /etc/ssh/sshd_config as following:

```
 # vim /etc/ssh/sshd_config
```

```
#
# sshd_config managed by puppet, do not edit by hand!
#

Port 22
ListenAddress 172.31.130.28
Protocol 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
LoginGraceTime 2m

PermitRootLogin no
StrictModes yes
DSAAuthentication yes
AuthorizedKeysFile /etc/ssh/authorized_keys/%u
HostbasedAuthentication no
IgnoreRhosts yes
PasswordAuthentication no
```

```
PermitEmptyPasswords no

ChallengeResponseAuthentication no
UsePAM yes

X11Forwarding yes
UsePrivilegeSeparation yes

Subsystem       sftp    /usr/libexec/openssh/sftp-server
ClientAliveInterval 60
ClientAliveCountMax 5
AllowTcpForwarding yes

LogLevel INFO
MaxAuthTries 4
PermitUserEnvironment no
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group-
exchange-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521
MACs hmac-sha2-256,hmac-sha2-512
PubkeyAuthentication yes
AllowAgentForwarding yes

Match group pfrsync
       X11Forwarding no
       AllowTcpForwarding no
       AllowAgentForwarding no
       PasswordAuthentication yes
```

- **Keep in mind:** There is no need, to create an Group, if just one user should be able to have Access. In this case replace “Match group pfrsynconly” with “Match user pfrsync”

After all changes, restart sshd!

```
# systemctl restart sshd
```

Weiteres:

- **Restrict SSH Access for User with LShell (Limited Shell)**

Last update: **2017/11/08 10:26**