How To Copy Files With Rsync Over SSH

Authored by: ***ASPHostServer Administrator*** *[asphostserver@gmail.com]*
Saved From: *http://faq.asphosthelpdesk.com/article.php?id=210*

Step 1 - Setup public SSH keys

On our origin server, we will generate public SSH keys with no password:

```
ssh-keygen -f ~/.ssh/id_rsa -q -P ""
cat ~/.ssh/id_rsa.pub
```

This is our public SSH key that can be placed on other hosts to give us access:

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAABAQDLVDBIpdpfePg/a6h8au1HTKPPrg8wuTrjdh0QFVPpTI4KHctf6/FGg1
root@cloudads
```

Copy this key to your clipboard and login to your destination server.

Place this SSH key into your ~/.ssh/authorized_keys file:

If your SSH folder does not exist, create it manually:

```
mkdir ~/.ssh
chmod 0700 ~/.ssh
touch ~/.ssh/authorized_keys
chmod 0644 ~/.ssh/authorized_keys
```

Step 3 - Rsync files over

Rsync is a great utility, as it allows you, among many other things, to copy files recursively with compression, and over an encrypted channel.

We will copy a file from our origin server (198.211.117.101) in /root/bigfile.txt over to our destination server (IP: 198.211.117.129) and save it in /root/bigfile.txt as well.

Login on 198.211.117.101 and rsync the file over to 198.211.117.129:

```
rsync -avz -e "ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null"
--progress /root/bigfile.txt 198.211.117.129:/root/
```

If you are using a different user, for example "username" then you would have to append it in front of destination server. Make sure to have your public key in that user's ~/.ssh/authorized_keys file:

```
rsync -avz -e "ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null"
--progress /root/bigfile.txt username@198.211.117.129:/
```

The SSH options are useful to keep Rsync quiet and not prompting everytime you connect to a new server.

Verify that you have received the file on destination server (198.211.117.129):

```
ls -la /root/bigfile.txt
```

And you are all done!