

How to transfer Ezeelogin SSH session logs recorded to a remote server ?

346 Manu Chacko July 25, 2024 [Features & Functionalities](#), [Technical](#) 2851

Transfer Ezeelogin SSH session logs recorded to a remote server

Overview: This article describes steps to create a Linux system user on a remote server, set up SSH-key-based authentication, and transfer [SSH session logs](#) from an Ezeelogin Jumpserver using rsync.

Step 1: Create a Linux System User

- If not already existing, create a Linux system user on the remote server where SSH session [logs](#) will be transferred.

You can skip this step if a Linux system user already exists on the remote machine.

- Add the user with the following command. You can replace the username "backup-user" with a username of your choice.

```
root@remote-server:~#useradd backup-user
```

Step 2. Setup SSH-KEY-based authentication for passwordless authentication.

- 2.a.) Create an ssh key pair on the server using the following command on the Jumpserver.

```
root@jumpserver:~# ssh-keygen -m PEM -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:eUKBEDUlDVzQgCKT3QHBVwHHCH0IjWa8cDdNkRBrvZM root@jumpserver
The key's randomart image is:
```

```

----[RSA 2048]-----
|      =B#B/@%o      |
|      = @ @=B.o     |
|      B = o.        |
|      .o . o        |
|      S E           |
|      o .           |
|-----[SHA256]-----|

```

- Now, the public key has been saved in the file `/root/.ssh/id_rsa.pub`, and the private key in `/root/.ssh/id_rsa`

2. b) Paste the public key in the remote server user's "backup-user" authorized key file.

```

root@remote-server:~# vi /home/backup-user/.ssh/authorized_keys

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACzCOoNRS9t6Eg86XMmnH9V8irlmDQn+
Glx+d41aIEwrgllgrfCHelQwJeTUhME7SnarbjmVLQfYuSVLpb0BtFoqdHQXY/Kp6yuyu
JWsRntiPzH5YuVhN0zaITdmmALTLip9A9hi+pbMy51tDAwJCJPJjvf51VW313ddG9lxm
WbzHTHbIQHwV0TPFP81j2BDDCSL5nw+2QiQ+R36GI8YVpn0aB1RqRMCPyE+lWJOsvfRs+
SvUawkbUgTCg9nhEBPb/Xj1INTZnU6A0J2T6mk5tsMb70pEvDWbd6QPpwhOo/3UT5vk5Q
t4Q+RBKyheS6jP7lhlpfG9cwtqYRmZ3n74f8qnmwiRCVppiRmSW6YepM0/KoL1byk7RVb
aiYWxQZJwdiH/Xfda/nGji6cb0mrsBxKV7QXpF/kstlMQ7zT5HoEGXRYRN4rll+ekCFnp
FkCjZ75ss+hOwrmdliw9luiGdHiV3aQaGTMxWqD48OXXZuoAeC6NVE5LEiqRbOn4W3KPD
ky4b490UedMhpRdhVXm+Ow3GQJgCPOGqbPP2Huftxn5ZIm3XGfW85J4SsChQ+b3jrxeZF
5h/e+nrYWqoTbPxH7DCWVRoI1lu174eBkdUR5oJc4C5v5qTbyzqNE6WK3jsgcazfK32ea
bCyKfH2AeKAGZM1o4Zn3MozmGFKfNrw

```

- So that you can SSH to a remote server from the Jumpserver without a password.

Step 3. **Copy/sync logs** from the Ezeelogin Jumpserver to the remote server using the `rsync` command.

```

root@jumpserver:~# rsync -av /var/log/ezlogin backup-
user@10.10.10.1:/home/backup-user/

```

- If you want to copy a ssh user log file to the remote server, use the following command:

```
root@jumpserver:~# rsync -av  
/var/log/ezlogin/full/ezadm622/acer~test.centos2.com backup-  
user@10.10.10.1:/home/logs/
```

Related Articles:

[View logs of all users.](#)

[Decrypt the encrypted SSH logs.](#)

Online URL:

<https://www.ezeelogin.com/kb/article/how-to-transfer-ezeelogin-ssh-session-logs-recorded-to-a-remote-server-346.html>