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

346 Manu Chacko July 25, 2024 Features & Functionalities, Technical

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 usir

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
AAAAB3NzaC1yc2EAAAADAQABAAACAQCzCOoNRS9t6Eg86XMmnH9V8irlmDQn+G1x+d41aIEwrgllgrfCHe1QwJeTUhME7SnarbjmVLQfYuSVLpb0BtFoqdHQXY/Kp6yuyuJWsRntiPzH5Yu
```

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.