How to decrypt the encrypted SSH logs in Ezeelogin?

429 Riya Francis April 1, 2025 Technical 4334

Converting encrypted SSH logs in ezeelogin to CSV files

Overview: This article demonstrates how to decrypt encrypted SSH logs in Ezeelogin and convert them into CSV files using specific command-line tools.

Run the following command to decrypt the logs. Replace the log file name with your log file path.

```
root@gateway:~# /usr/local/ezlogin/eztool.php -show_log /var/log/ezlogin/full/username/log_name
```

The following scripts show an example for decrypting logs accessed by the admin user.

```
root@gateway:~# /usr/local/ezlogin/eztool.php -show_log
/var/log/ezlogin/full/admin/root~server.cent.test~Thu_Jul_15_09\:56\:02_2021

############################
# Ezeelogin Tool       #
############################

Checking environment... The memory limit is less than 4 GB. If the script crashes abruptly without any errors, try increasing the PHP memory limit.
done (1722)
Checking license... done (1956)

Enter the Ezeelogin administrator password: Admin!2345

Log Info:
ID: 3
Server: server.cent.test
User: admin
SSH User: root
Log Type: full
Status: end
Encryption: 1
Created: 2021-07-15 09:56:02
File: /var/log/ezlogin/full/admin/root~server.cent.test~Thu_Jul_15_09:56:02_2021
File Size: 8207
Data Size: 60334
Decrypt Command: /usr/local/ezlogin/ezlogsearch '3' '05ca04c241f735cb0a045d341968a2767c07a7d5' 0 2>&1
(0)
Contents:

Last login: Thu Jul 15 09:55:47 2021 from 192.168.1.7
[root@localhost ~]# ls
1 anaconda-ks.cfg
[root@localhost ~]

#host ~]# exit
logout
Read count: 0
<===[END]===>
```

Run the following command to decrypt the SSH logs and save them to a CSV file.

```
root@gateway:~# /usr/local/ezlogin/eztool.php -show_log /var/log/ezlogin/full/username/filename -out file_name.csv
```

Refer the following script as an example for decrypting ssh logs into a CSV file.

```
root@gateway:~# /usr/local/ezlogin/eztool.php -show_log /var/log/ezlogin/full/admin/root~server.cent.test~Thu_Jul_15_09\:56\:02_2021 -out log_admin.csv

############################
# Ezeelogin Tool       #
############################

Checking environment... The memory limit is less than 4 GB. If the script crashes abruptly without any errors, try increasing the PHP memory limit.
done (1722)
Checking license... done (1956)

Enter the Ezeelogin administrator password: Admin!2345

Log Info:
ID: 3
Server: server.cent.test
User: admin
SSH User: root
Log Type: full
Status: end
Encryption: 1
Created: 2021-07-15 09:56:02
File: /var/log/ezlogin/full/admin/root~server.cent.test~Thu_Jul_15_09:56:02_2021
File Size: 8207
Data Size: 60334
Decrypt Command: /usr/local/ezlogin/ezlogsearch '3' '05ca04c241f735cb0a045d341968a2767c07a7d5' 0 2>&1
(0)
```

Related Articles:

View SSH logs of all users

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

how do i access the ssh logs history that was recorded for the ssh user ?

Online URL: https://www.ezeelogin.com/kb/article/how-to-decrypt-the-encrypted-ssh-logs-in-ezeelogin-429.html