DSA key based authentication is not working

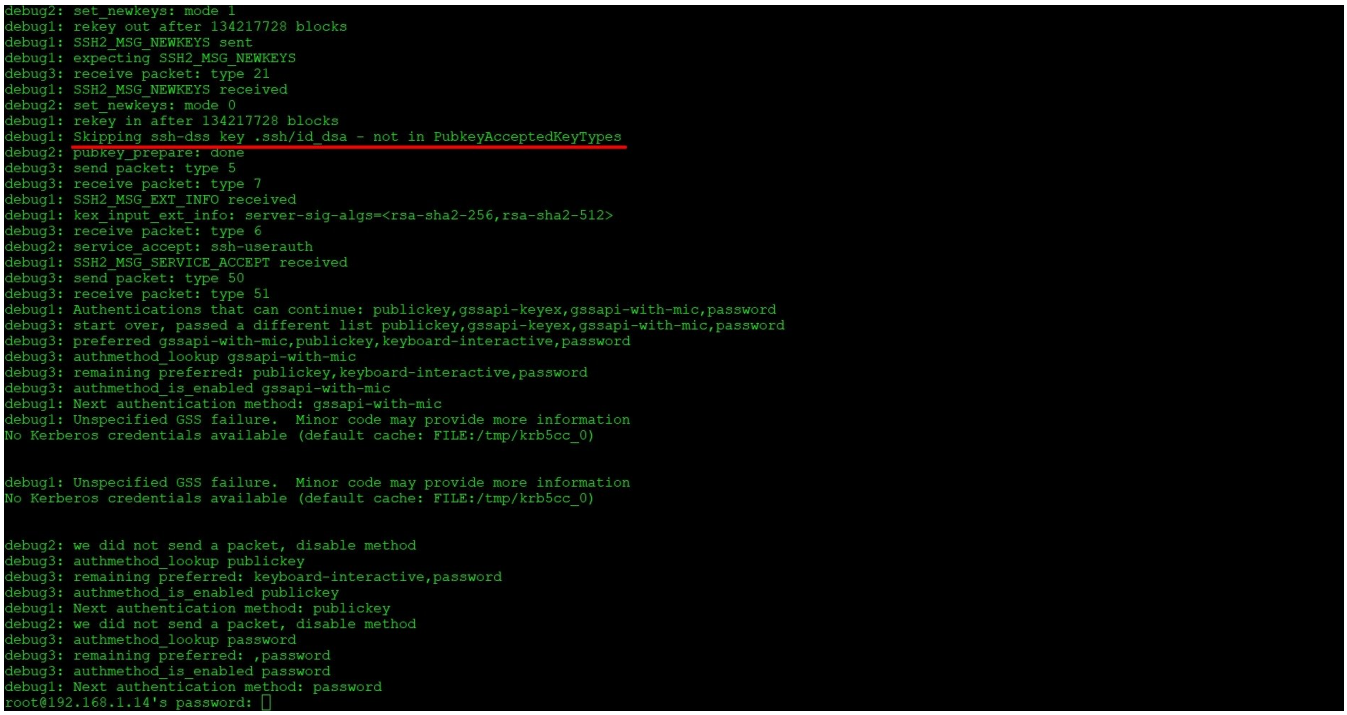
584 Nesvin KN March 3, 2023 Common Errors & Troubleshooting 1870

How to troubleshoot the DSA key-based authentication?

SSH from the client machine to the destination server with verbose and see for the messages.

```
root@client ~]# ssh -i {dsa_private_key_path} username@server_ip -vvv


debug1: Skipping ssh-dss key .ssh/id_dsa - not in
PubkeyAcceptedKeyTypes
```



Refer below steps to fix the above error.

1. Login to the client machine and append the below lines in the **ssh_config** file.

```
root@client ~]# vim /etc/ssh/ssh_config

PubkeyAcceptedKeyTypes=+ssh-dss
HostKeyAlgorithms=+ssh-dss
```

2. SSH again with below command to see if key-based authentication worked.

```
root@client ~]# ssh -i {dsa_private_key_path} username@server_ip -vvv
```

How to view the list of KEX and Keys in the Linux server?

- How to list **keys** in the Linux server?

```
root@linux ~]# ssh -Q key

ssh-ed25519
ssh-ed25519-cert-v01@openssh.com
ssh-rsa
ssh-dss
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
ssh-rsa-cert-v01@openssh.com
ssh-dss-cert-v01@openssh.com
ecdsa-sha2-nistp256-cert-v01@openssh.com
ecdsa-sha2-nistp384-cert-v01@openssh.com
ecdsa-sha2-nistp521-cert-v01@openssh.com
```

- How to list **KEX** in the Linux server?

```
root@linux ~]# ssh -Q kex

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
```

```
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
curve25519-sha256
curve25519-sha256@libssh.org
```

Related Articles

signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms

key type ssh-dss not in PubkeyAcceptedKeyTypes