DSA key based authentication is not working

584 Nesvin KN March 23, 2025 Common Errors & Troubleshooting 5848

How to troubleshoot the DSA key-based authentication?

Overview: This article explains how to resolve the ssh-dss key error in SSH by updating the ssh_config file and how to list available KEX and key types on a Linux server.

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
```

```
debug2: set_newkeys: mode 1
debug1: rekey out after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug3: receive packet: type 21
debug1: SSH2_MSG_NEWKEYS received
debug2: set_newkeys: mode 0
debug1: rekey in after 134217728 blocks
debug1: Skipping ssh-dss key .ssh/id_dsa - not in PubkeyAcceptedKeyTypes
debug2: pubkey_prepare: done
debug3: send packet: type 5
debug3: receive packet: type 7
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<rsa-sha2-256,rsa-sha2-512>
debug3: receive packet: type 6
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug3: send packet: type 50
debug3: receive packet: type 51
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug3: start over, passed a different list publickey,gssapi-keyex,gssapi-with-mic,password
debug3: preferred gssapi-with-mic,publickey,keyboard-interactive,password
debug3: authmethod_lookup gssapi-with-mic
debug3: remaining preferred: publickey,keyboard-interactive,password
debug3: authmethod_is_enabled gssapi-with-mic
debug1: Next authentication method: gssapi-with-mic
debug1: Unspecified GSS failure.  Minor code may provide more information
No Kerberos credentials available (default cache: FILE:/tmp/krb5cc_0)


debug1: Unspecified GSS failure.  Minor code may provide more information
No Kerberos credentials available (default cache: FILE:/tmp/krb5cc_0)


debug2: we did not send a packet, disable method
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug2: we did not send a packet, disable method
debug3: authmethod_lookup password
debug3: remaining preferred: ,password
debug3: authmethod_is_enabled password
debug1: Next authentication method: password
root@192.168.1.14's password:
```

Refer below steps to fix the above error.

Step 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
```

Step 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

Online URL: https://www.ezeelogin.com/kb/article/dsa-key-based-authentication-is-not-working-584.html