## Error: User modify failed. Cannot modify user on other node: Authentication by SSH key failed!

255 Manu Chacko October 14, 2024 Common Errors & Troubleshooting 4993

## Error: failed to modify user on other node. SSH key authentication to remote node failed

**Overview:** This article addresses the error: "failed to modify user on other node. SSH key authentication to remote node failed," providing troubleshooting steps for missing public keys, SSH port settings, sshd\_config configurations, and more.

Ezeelogin			Uvelcome, Administrator Logout
😂 Servers			
■ Web Portals ►	N.	Error: User modify failed. Cannot modify user on other node: Authentication by SSH key failed!	X
±t. Users ▼		Add User	
▶ User Groups		First Name	Last Name
► LDAP	1.6	marc	m
Authentication Log	1	Username @	Email
► SSH Log		marc	marc@gmail.com
RDP Recording	6. 2		
SCP Log	20	Password	Security Code 🕑
Web Proxy Log	2.20		
Web Proxy Activity	265	Generate	Generate
Web Activity		User Group	Status
Shell Activity		Admins 🛊	Active X Suspended
<ul> <li>Server Activity</li> </ul>	14.	Expire 💿	Command Guard 🐵
Work Summary		Never 🔶	None 🔶
▶ Status	088		
Access Control	2.7	Limit IPs 🐵	Allow Disallow
		×	Virtual Shell 🐵
♥ <sub>o</sub> Settings ►	×	Allowed IPs 😡	×

Check the following on the slave/secondary node

**Step 1.** The error 'User modify failed Cannot modify user on other node: Authentication by ssh key failed' would occur when the Ezeelogin installed node has its public key missing in /root/.ssh/authorized\_keys. To add the key, execute the following command

root@gateway:~# cat /usr/local/etc/ezlogin/id_clkey.pub >> /root/.ssh/authorized_keys	
Check if the key is back in the file.	

root@gateway:~# cat /root/.ssh/authorized\_keys



**Step 2.** Also, make sure that the port sshd is listening on the servers is given as the gateway port in **Settings-> General-> Miscellaneous-> Gateway SSH port** 

Ezeelogin Welcome, Administrator Logout				
t≣ Servers ►	•	General Settings	Authentication Two Factor Authentication Security Defaults Miscellaneous	
🖬 Web Portals 🔹 🕨	×	Gateway SSH Port 💩 <	SSH Timeout	
±t Users ►		22	10	
Access Control		RDP Proxy Port 🕡	Web SSH Port 💿	
♥o Settings		22555	52222	
General	1.10	Web Proxy Port 🥹	Web Proxy Session Timeout	
► Branding		52666	300	
<ul> <li>Control Panels</li> </ul>	1	Web Proxy Request Timeout 🥯	Web Proxy Web Sockets 🥹	
<ul> <li>Data Centers</li> </ul>		120		
≻ API		Web Proxy Forwarded Header 🥪	Log Retain Duration (months) 🗑	
► LDAP	1		0	
► SAML	3			
► FIDO2		Log Space Threshold (MB) 🐵	mExec Concurrency 🥹	
► RADIUS		0	100	
► SIEM		NodeJS Command 🥥	Hide Inbuilt Backgounds 😨	
<ul> <li>Server Fields</li> </ul>		/usr/local/bin/node		
🛞 Cluster				
		Login theme 🥹	Use DNS 🐵	

**Step 3.** Also, make sure PubkeyAuthentication is set to 'YES' in your sshd\_config (sshd configuration) file. In Centos/RHEL/Fedora it would be

root@gateway:~# vi /etc/ssh/sshd\_config #set PubkeyAuthentication to yes PubkeyAuthentication yes root@gateway ~]# service sshd restart

Also, run the following command to check if you have enabled the recommended sshd settings in /etc/ssh/sshd\_config

root@gateway:~# sshd -T | grep -i 'AllowTcpForwarding|PermitRootLogin|PubkeyAuthentication|Passwo rdAuthentication|pubkeyacceptedalgorithms|Port'

port 22 permitrootlogin yes pubkeyauthentication yes passwordauthentication yes gatewayports no allowtcpforwarding yes pubkeyacceptedalgorithms ssh-ed25519-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,sk-esh-ed 25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-certv01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sh

**Step 4.** Make sure root login is permitted on the gateway server. You can check it by using the following command:

ssh root@localhost

And it should log you in; otherwise, edit /etc/ssh/sshd\_config and set PermitRootLogin yes.

root@gateway:~# vi /etc/ssh/sshd\_config

#Add the following lines to the end of /etc/ssh/sshd\_config to allow root login from localhost only

Match Address 127.0.0.1

PermitRootLogin yes

PubkeyAuthentication yes

#Replace MASTER\_NODE\_IP with your master node Ezeelogin IP ADDRESS

Match Address MASTER\_NODE\_IP

PermitRootLogin yes

PubkeyAuthentication yes

root@gateway:~# service sshd restart

After, try to authenticate with the command. Make sure you are able to login after entering the password.

ssh root@localhost

**Step 5.** Also, make sure that the web user(apache, nobody, etc) that the webserver(apache/nginx) runs as is able to read the keys in the dir /usr/local/etc/ezlogin. Make sure to grant the read privileges to

Step 6. Find out which key type is used by the server by running the below command.

root@gateway:~# ssh-keygen -l -f /usr/local/etc/ezlogin/id\_key.pub

4096 SHA256:n4lmX53/gwkKB4+nSQ30hZXxXK+DRG1LPc7N1KN/1Ag ezlogin (RSA)

Open /etc/ssh/sshd\_config file and append below line to enable RSA key type.

root@gateway:~# vim /etc/ssh/sshd\_config

PubkeyAcceptedKeyTypes +ssh-rsa

root@gateway:~# systemctl restart sshd

Step 7. Check the log file /var/log/secure

root@gateway:~# tail -f /var/log/secure

if you get this error in log file "userauth\_pubkey: signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms" refer the following article: <u>userauth\_pubkey: signature</u> algorithm ssh-rsa not in PubkeyAcceptedAlgorithms.

Step 8. Reset Ezeelogin cluster keys

Note:

If you have enabled Allow Or Deny SSH Access To A Particular User Or Group in sshd.conf, make sure that the user root is allowed

**Related Articles:** 

Error: User modify failed. Cannot modify user on other node: usermod: user luca does not exist.

Error: User modify failed. Cannot modify user on this node: Authentication by SSH key failed!

error: User modify failed Cannot modify user on this node: OS=FreeBSD: Command not found. OS: Undefined

Online URL:

https://www.ezeelogin.com/kb/article/error-user-modify-failed-cannot-modify-user-on-other-nodeauthentication-by-ssh-key-failed-255.html