Why Key Authorization is not working?

596 Rakhi March 26, 2025 Common Errors & Troubleshooting 1991

Why key authorization is not working in a remote server through the gateway?

Overview: This article describes troubleshooting steps to resolve key authorization issues in a remote server accessed through a gateway. It covers enabling PubKeyAuthentication, verifying SSH configurations, resetting fingerprints, checking logs, and ensuring <u>SSH key</u> types are correctly configured.

Even after setting up the remote server in the gateway machine and appending the public key to /root/.ssh/authorized_keys, you may still be prompted for a password when trying to log in. Below are possible reasons and solutions.

Troubleshooting steps:

Step 1: Check whether the PubKeyAuthentication is enabled on the sshd conf of the remote server.

Ensure that public key authentication is enabled in the SSH daemon configuration on the remote server. Modify the configuration and restart the SSH service:



Step 2: Confirm that the remote server is added with the remote username "root".

Ensure that the remote server is configured with the correct username, typically "root" for administrative access.

\leftrightarrow \rightarrow C \otimes Not secure	९☆ । 🖸 🕹 🙁 🗄		
C Ezeelogin			Welcome, Administrator Logout
🗄 Servers 🗸 🗖	Edit Server		•
 Server Groups 	Hostname	IP Address(es) 🥹	
 Super Groups 	PROD_LS-02	192.168.0.108	
 Sub SSH Users 	Remote SSH / RDP Login User	SSH / PDP Password	"
 Sub SSH User Maps 	root	Son / KDF Fassword	
 mExec lists 		******	
► Import	SSH Private Key 🥹	Clear 🥹	
 Global Key 		SSH Key Passphrase 🥹	
 Kou Managamant 			

Step 3: Reset the fingerprint of the remote Server.

If there is a fingerprint mismatch, reset the fingerprint and attempt to reconnect.

← → C ONot secure https://cloudweg.com/index.php/base#servers								☆ 🙆 ᡗ 🙁	:	
C Ezeelogin							Velcome, Administrator Logou			
t≣ Servers ▼	Î								١.	
▶ Server Groups		Succ	ess: SSH fingerprint has been o	leared	and a second second second second			×	1	
► Super Groups		Serv	ers	All V domain loc	kup 💿 🖾			Rows Auto 🗸 🕥	0	
 Sub SSH Users 									1	
 Sub SSH User Maps 			<u>Name</u> ↓	IP Address	Server Group	SSH Port	Description	Actions		
 mExec lists 			+ PROD-WS01	192.168.0.106	Production servers	2222				
► Import			+ PROD_LS-02	192.168.0.108	Production servers	22			2004	
 Clobal Key 			+ cwp	192.168.0.113	Production servers	22		/ 🎭 🛄	T	
 Key Management 	6. 6	0	+ webim panel	192.168.0.106	Production servers	22		/ 📫 🔒	8	
Web Portals								©	e	
	_		+ windows_rdp_server	192.168.0.105	Win-Production servers	22		C	C	
±t Users ►								1 - 5 / 5	Û	
Access Control			A Martin Contraction	and the second second	and the second second	and the second second	-		*	
A					Non- Participation		1			

Step 4: Restart sshd service After resetting try to reset sshd and try to re-login to ezsh.

After resetting the fingerprint, restart the SSH service and attempt to log in again using the ezsh (ezeelogin shell):

root@gateway:~# systemctl restart sshd

Step 5: Check the latest SSH logs for any errors.

Examine the authentication logs for potential errors that could be causing authentication failures.

```
root@remote_server:~# tail -f /var/log/auth.log //If the remote
server is Ubuntu
root@remote_server:~# tail -f /var/log/secure //If the remote server
is CentOS
```

Step 6: Verify the enabled keys.

Run the following command to confirm the accepted key types. The output should list the supported

public key algorithms. If certain keys are missing, additional configurations may be needed.

root@gateway:~# sshd -T|grep -i key

pubkeyacceptedalgorithms ssh-ed25519-cert-v01@openssh.com,ecdsa-sha 2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openss h.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-certv01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha 2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed 25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,s k-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsasha2-512,rsa-sha2-256

Step 7: Add ssh-rsa to sshd conf in the remote server.

In Ubuntu 22, ssh-rsa is disabled by default, so you need to enter it manually.

```
root@gateway:~# echo "PubkeyAcceptedKeyTypes ssh-rsa" >>
/etc/ssh/sshd_config
```

(8) Re-run the below command and confirm that ssh-rsa has been enabled.

root@gateway:~# sshd -T | grep -i key

pubkeyacceptedalgorithms ssh-ed25519-cert-v01@openssh.com,ecdsa-sha 2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openss h.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-certv01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha 2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed 25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,s k-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsasha2-512,rsa-sha2-256,**ssh-rsa** **Related Articles:**

Add ssh pubkey for passwordless authentication in ssh.

Authentication by ssh key failed.

Error log file and config file to troubleshoot.

Online URL: https://www.ezeelogin.com/kb/article/why-key-authorization-is-not-working-596.html