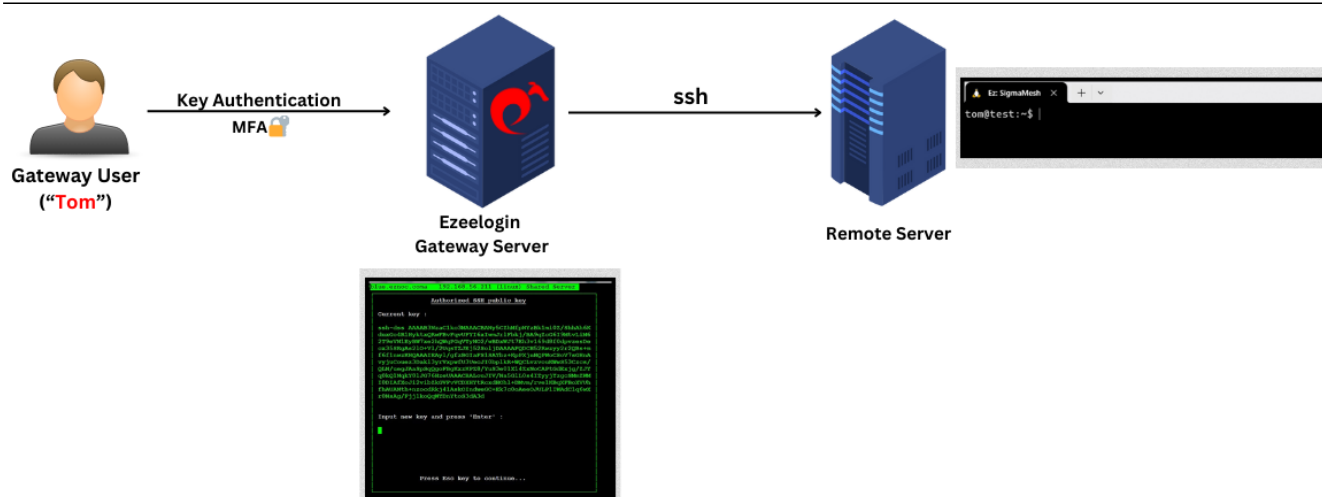


How to add ssh public key for passwordless authentication in ssh

137 admin November 24, 2024 [Tweaks & Configuration](#) 9375

Enabling passwordless SSH Login from gateway to remote servers using public keys

Overview: This article offers a step-by-step guide to configure passwordless SSH authentication for gateway users accessing the Ezeelogin backend shell (ezsh). It details the process of adding SSH public keys to the gateway server, allowing users to log in seamlessly without being prompted for passwords.

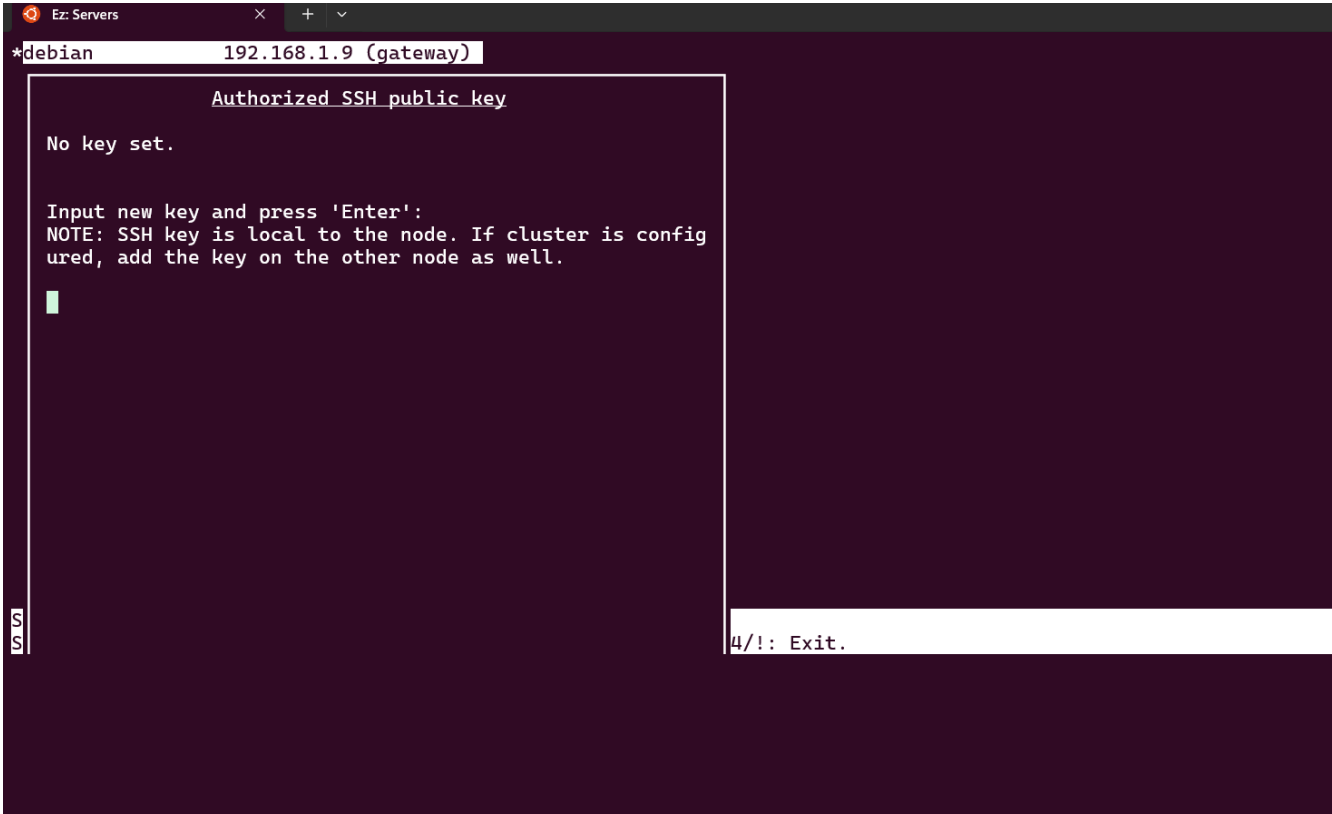


SSH Gateway users can add their public keys for passwordless authentication to log in from the ezsh shell (ezeelogin backend shell). Press the F2 key in the ezeelogin shell to enter the public keys for SSH-authorized keys-based authentication so that the user's password will not

be prompted again. Follow the steps below:

Step 1: Log into the Ezeelogin backend interface (known as the ezsh shell). Start by entering your password. If two-factor authentication (2FA) is enabled, you'll need to complete that step as well. This will give you access to the necessary configuration options.

Step 2: Once you're in the ezsh shell, press "F2" or "#" on your keyboard. This will take you to the section where you can manage SSH public keys.

A screenshot of a terminal window titled "Ez: Servers". The terminal shows a shell prompt for a user named "debian" on the host "192.168.1.9 (gateway)". The terminal displays the "Authorized SSH public key" section, which currently shows "No key set." and prompts the user to "Input new key and press 'Enter':". A note below the prompt states: "NOTE: SSH key is local to the node. If cluster is configured, add the key on the other node as well." A cursor is visible on the line following the prompt. At the bottom of the terminal, there is a partial prompt "4/!: Exit." and a vertical "SS" indicator on the left side of the terminal window.

```
Ez: Servers
*debian 192.168.1.9 (gateway)
Authorized SSH public key
No key set.
Input new key and press 'Enter':
NOTE: SSH key is local to the node. If cluster is configured, add the key on the other node as well.
4/!: Exit.
```

Step 3: In this section, you'll find a prompt where you can add SSH public keys. Paste the SSH public key you want to use into the provided space and press Enter to confirm and save it. This key will now be used for authentication.

```
Ez: Servers
x + v
*debian 192.168.1.9 (gateway)

Authorized SSH public key

Current key :

expiry-time="20240710" ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBA
AABgQDbAgGFRAHkLRPT8eLC+CNBBVDQH/ZeLPy5JDwshNhUvYQcDZ0IA
X/oAwboVFm833eXvfaI0bI4XzjULzMIrfIYqLKndd+VPQ0/2Kx66i63H
viholx2yr3RgS6UGEnnSAjNPYmu6YhMRZDlBBjexLE6qgeeIYg6U01UX
h0jjfXu54JyDAsdv3AdDcVtS1eFKBy++gju0ncRnMMSXsLRa8vkmjqF
zmjuqy2I3T1nMeg4/tvuvNuqIykcw3l3eNt8MhDoJLWJZow+JaHSFBDH
9IZz0sZW74DZ5SsTwaAD4h59qyIsA6e9JFupqaUsidPyTIUNhPYBjpw
Ec5I9nUEbXBGXqP0lya9ZPuzH6q7Ry1T9Nm7GSIFdoHYw1d5jrooia63
6nnJ7eSrFXTowG0hiDRDnfzov/N+vTaogSLqtHIt9j0ER2RFLVbUqgLB
JAndg6RpC6K3ifLHpitC8znkbo0ZjERJGDwGsy1evdvv/JntKR2H30Wz
W7xfts8I/m327U= root@debian

Input new key and press 'Enter':
NOTE: SSH key is local to the node. If cluster is config
ured, add the key on the other node as well.

4/!: Exit.
```

If you need to add multiple SSH public keys, you can also do so by editing the file located at `/home/tom/.ssh/authorized_keys`. Simply append the new keys to this file, ensuring each key is on a new line.

Note:

The public key you are adding to the ezeelgin master node will not be synced/copied to the slave/secondary node.

Copy the public key from the master node to the slave node and vice versa.

As an alternative way,

Step 1: Create an `authorized_keys` file and paste your public key inside it.

```
root@gw: ~
GNU nano 6.2 authorized_keys *
AAAhfhkWEybiuop;nkmnvygcrsxqsdfgnhm,wertyuiolsxcvbnjkitredsdfguikmSWTDFXCZFEAURDxcbnkLopoi98trewq|wsgFDGVBNMsdF>

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Step 2: After transferring the public keys into the authorized_keys file, Follow the below steps;-

```
root@gateway:~# sftp tom@gateway_ip
```

Step 3: Enter the password of the gateway user when prompted.

```
sftp> cd .ssh/
sftp> put authorized_keys
```

Related Articles:

[Different types of SSH authentication keys](#)

[Set SSH Key Expiry for the gateway users](#)

[Enable/Disable password or key-based authentication](#)

[How can I add more than one public key to ezeelogin users?](#)

Online URL:

<https://www.ezeelogin.com/kb/article/how-to-add-ssh-public-key-for-passwordless-authentication-in-ssh-137.html>