Allowing SSH access to VMware vSphere ESXi/ESX hosts with public/private key authentication

Archived: 2026-04-05 13:22:09 UTC

Allowing SSH access to VMware vSphere ESXi/ESX hosts with public/private key authentication

calendar_today

Updated On: 10-05-2025

Products

VMware vSphere ESXi

Issue/Introduction

This article provides steps to allow SSH access to VMware vSphere ESXi/ESX hosts with public/private key authentication rather than with username/password authentication.

Environment

VMware vSphere ESXi 8.0
VMware vSphere ESXi 7.0

Resolution

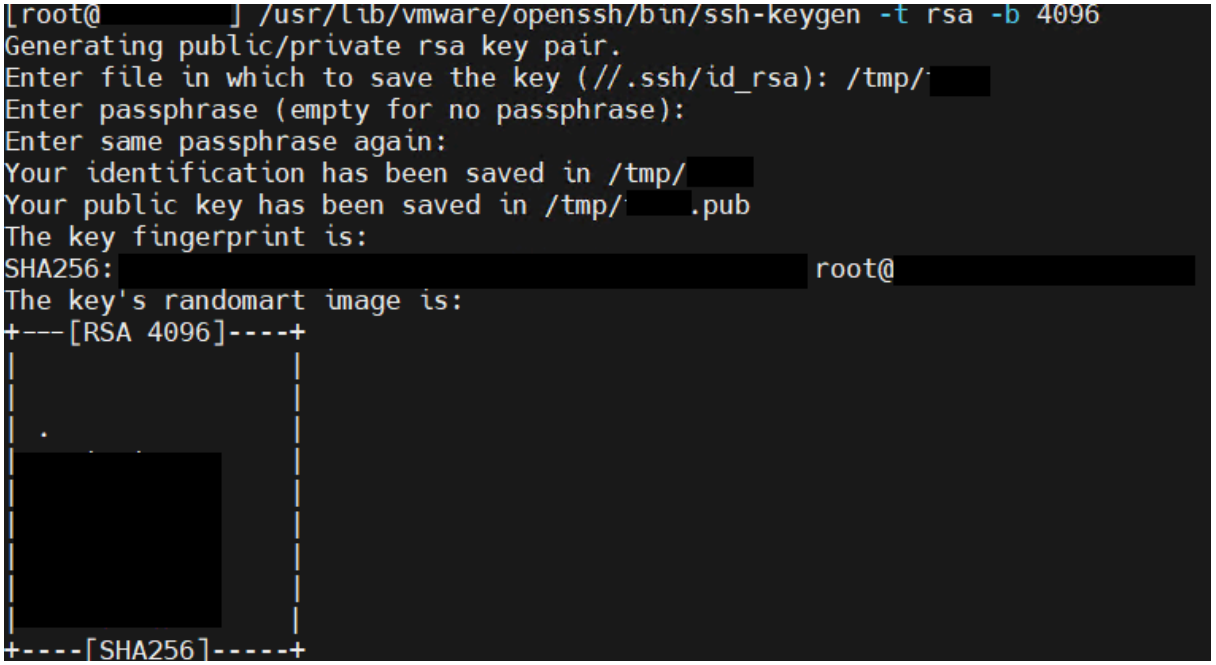
Note: VMware vSphere ESXi does not support preserving SSH-Keys for Active Directory users.

To allow SSH access to ESXi or ESX hosts with public/private key authentication:

1. Generate public/private keys on ESXi by running the below command:

   `/usr/lib/vmware/openssh/bin/ssh-keygen -t rsa -b 4096`

   Example:



For more information, see the OpenBSD Reference Manual section in the [OpenBSD]

2. The above command will generate two files, private and a public key in the specified location. Example:

   Private Key `:` key_file_name

   `Public Key: key_file_name.pub`

3. On the ESXi host, store the public key content in /etc/ssh/keys-root/authorized_keys.

   (e.g. `cat` key_file_name `.` pub >> authorized_keys)

   Notes:

   - The above step will store the public key for the root user.
   - More than one key can be stored in this file.

4. Ensure the PermitRootLogin parameter is set to `yes` in /etc/ssh/sshd_config.

   Note: (optional) To disable password logins via SSH to ESXi host, change ChallengeResponseAuthentication and PasswordAuthentication to no in `/etc/ssh/sshd_config.`

   In ESXi version 8.0.1 and later, the PasswordAuthentication option is no longer configurable. To achieve equivalent functionality, set the ChallengeResponseAuthentication parameters to yes

   esxcli system ssh server config set -k challengeresponseauthentication -v yes

   Note: No need to restart the SSH service for the above esxcli command.

5. Reload the SSH service:

- For ESXi, run the command:

  `/etc/init.d/SSH restart`

To login from a linux machine(could be ESXi or vCenter appliance):

1. Copy the private key to the linux machine.
2. Browse to the path where the private key resides.
3. Change the permission on the private key file using the command: `chmod 600 <private_key_file>`
4. Run the below command:

   `ssh -i <private_key_file> -l root <esxi_hostname>`

Additional Information

Feedback

Was this article helpful?

thumb_up Yes

thumb_down No
