Knowledge Base Article #ETM57718

Upgrading OpenSSH on PolicyGuru® Solution v3.x Systems

Synopsis

This document describes the procedure to upgrade OpenSSH to OpenSSH_9.3p1. These instructions and RPMs are intended for use on CentOS 7.9.2009 systems running PolicyGuru® Solution v3.x..

Versions Affected

PolicyGuru® Solution v3.x

OpenSSH_9.3p1 Installation Instructions

Before you begin

Contact SecureLogix Technical Support to obtain a copy of the tarball containing the required OpenSSH_9.3p1 RPMs.

To upgrade OpenSSH on each PolicyGuru® System v3.x component

1. Backup the **/etc/pam.d/sshd file**:

   ```
   cp /etc/pam.d/sshd /root/pam.sshd.pre
   ```

2. Copy the **OpenSSH_9.3p1** tarball to the computer where the RPMs will be installed.

3. Un-tar the tarball.

4. Install the RPMs:

   ```
   yum localupdate *.rpm
   ```

   There are three RPMS that are added as dependencies:

   - **libICE**
   - **libSM**
   - **LibXt**

5. Edit the **/etc/ssh/sshd_config** file to include the following changes:

   a. Add the following content:

   ```
   hostkeyalgorithms 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-ssh-ed25519-cert-v01@openssh.com,sk-
   ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-
   v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-
   nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-
   ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-
   sha2-256,ssh-rsa,ssh-dss
   ```

   b. Ensure that this line is uncommented:

   ```
   UsePAM yes
   ```

   c. Ensure that this line is uncommented:

```
PermitRootLogin yes
```

d. Comment out the following lines:
```
#Ciphers aes256-ctr,aes192-ctr,aes128-ctr

#MACs hmac-sha2-512,hmac-sha2-256 124

#KexAlgorithms diffie-hellman-group-exchange-sha256
```

6. Edit the **/etc/pam.d/sshd** file to look like the following:
```
#%PAM-1.0
auth required pam_sepermit.so
auth include password-auth

# Used with polkit to reauthorize users in remote sessions

account required pam_nologin.so
account include password-auth
password include password-auth

# pam_selinus.so close should be the first session rule

session required pam_selinux.so close
session required pam_loginuid.so

# pam_selinus.so open should only be followed by session to be executed in
the user context

session required pam_selinux.so open env_params
#session required pam_namespace.so
session optional pam_keyinit.so force revoke
session include password-auth
#session include postlogin

# Used with polkit to reauthorized users in remote sessions

session optional pam_reauthorize.so prepare
```

7. Change the permissions on the **/etc/pam.d/sshd** file:
```
chmod 644 /etc/pam.d/sshd
```

8. Generate a **ssh_host_dsa_key:**
```
ssh-keygen -f /etc/ssh/ssh_host_dsa_key -N '' -t dsa
```

9. Ensure that the key files in the **/etc/ssh** directory have permissions set to 600:
```
chmod 600 *key
chmod 600 *.pub

chgrp ssh_keys /etc/ssh/*key
```

10. Start and stop the **sshd.service**
```
systemctl stop sshd.service

systemctl start sshd.service
```

11. Repeat this procedure on each PolicyGuru Solution v3.x host platform in the deployment.

Last Update: 5/30/2023

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232
(210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • support.securelogix.com