# Assignment for Week 3: Puppet setup

**Assignment for Week 3: Puppet setup**

## Execution after "Remove the sshd package"

I am assuming "sshd package" here means the "openssh-server" package.

```
root@ip-10-0-6-235:/etc/puppet# apt remove openssh-server -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  openssh-server
0 upgraded, 0 newly installed, 1 to remove and 20 not upgraded.
After this operation, 898 kB disk space will be freed.
(Reading database ... 87555 files and directories currently installed.)
Removing openssh-server (1:7.6p1-4ubuntu0.3) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
root@ip-10-0-6-235:/etc/puppet# service sshd status
Unit sshd.service could not be found.
root@ip-10-0-6-235:/etc/puppet# puppet apply /etc/puppet/manifests/site.pp
Notice: Compiled catalog for ip-10-0-6-235.us-west-2.compute.internal in
environment production in 0.47 seconds
Notice: /Stage[main]/Sshd::Prelude/Package[openssh-server]/ensure: created
Notice: Applied catalog in 5.03 seconds
root@ip-10-0-6-235:/etc/puppet# service sshd status
• ssh.service - OpenBSD Secure Shell server
```

```
    Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:
enabled)
    Active: active (running) since Fri 2019-07-12 20:03:55 UTC; 4s ago
 Main PID: 21779 (sshd)
    Tasks: 1 (limit: 547)
    CGroup: /system.slice/ssh.service
            └─21779 /usr/sbin/sshd -D


Jul 12 20:03:55 ip-10-0-6-235 systemd[1]: Starting OpenBSD Secure Shell
server...
Jul 12 20:03:55 ip-10-0-6-235 sshd[21779]: Server listening on 0.0.0.0 port
22.
Jul 12 20:03:55 ip-10-0-6-235 sshd[21779]: Server listening on :: port 22.
Jul 12 20:03:55 ip-10-0-6-235 systemd[1]: Started OpenBSD Secure Shell server.
```

## Execution after "Stop sshd"

```
root@ip-10-0-6-235:/etc/puppet# service sshd stop
root@ip-10-0-6-235:/etc/puppet# service sshd status
● ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:
enabled)
    Active: inactive (dead) since Fri 2019-07-12 20:04:20 UTC; 2s ago
  Process: 21779 ExecStart=/usr/sbin/sshd -D $SSHD_OPTS (code=exited,
status=0/SUCCESS)
 Main PID: 21779 (code=exited, status=0/SUCCESS)


Jul 12 20:03:55 ip-10-0-6-235 systemd[1]: Starting OpenBSD Secure Shell
server...
Jul 12 20:03:55 ip-10-0-6-235 sshd[21779]: Server listening on 0.0.0.0 port
22.
Jul 12 20:03:55 ip-10-0-6-235 sshd[21779]: Server listening on :: port 22.
Jul 12 20:03:55 ip-10-0-6-235 systemd[1]: Started OpenBSD Secure Shell server.
Jul 12 20:04:20 ip-10-0-6-235 sshd[21779]: Received signal 15; terminating.
Jul 12 20:04:20 ip-10-0-6-235 systemd[1]: Stopping OpenBSD Secure Shell
server...
Jul 12 20:04:20 ip-10-0-6-235 systemd[1]: Stopped OpenBSD Secure Shell server.
root@ip-10-0-6-235:/etc/puppet# puppet apply /etc/puppet/manifests/site.pp
Notice: Compiled catalog for ip-10-0-6-235.us-west-2.compute.internal in
environment production in 0.51 seconds
```

```
Notice: /Stage[main]/Sshd::Prelude/Service[sshd]/ensure: ensure changed
'stopped' to 'running'
Notice: Applied catalog in 0.35 seconds
root@ip-10-0-6-235:/etc/puppet# service sshd status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:
enabled)
   Active: active (running) since Fri 2019-07-12 20:04:29 UTC; 1s ago
  Process: 21998 ExecStartPre=/usr/sbin/sshd -t (code=exited,
status=0/SUCCESS)
 Main PID: 22002 (sshd)
    Tasks: 1 (limit: 547)
   CGroup: /system.slice/ssh.service
           └─22002 /usr/sbin/sshd -D

Jul 12 20:04:29 ip-10-0-6-235 systemd[1]: Starting OpenBSD Secure Shell
server...
Jul 12 20:04:29 ip-10-0-6-235 sshd[22002]: Server listening on 0.0.0.0 port
22.
Jul 12 20:04:29 ip-10-0-6-235 sshd[22002]: Server listening on :: port 22.
Jul 12 20:04:29 ip-10-0-6-235 systemd[1]: Started OpenBSD Secure Shell server.
```

# Execution after "Modify or delete /etc/ssh/sshd_config."

### After modification

```
root@ip-10-0-6-235:/etc/puppet# echo "# Appending" >> /etc/ssh/sshd_config
root@ip-10-0-6-235:/etc/puppet# cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port 22
```

```
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
```

```
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
```

```
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp  /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
# X11Forwarding no
# AllowTcpForwarding no
# PermitTTY no
# ForceCommand cvs server# Appending
root@ip-10-0-6-235:/etc/puppet# puppet apply /etc/puppet/manifests/site.pp
Notice: Compiled catalog for ip-10-0-6-235.us-west-2.compute.internal in
environment production in 0.46 seconds
Notice: /Stage[main]/Sshd::Prelude/File[/etc/ssh/sshd_config]/content: content
changed '{md5}89f3d2400a7d4c5c909a6185773642c9' to
'{md5}52c2e9c45a8778e02ea5bb05fa7188e8'
Notice: /Stage[main]/Sshd::Prelude/Service[sshd]: Triggered 'refresh' from 2
events
Notice: Applied catalog in 0.18 seconds
root@ip-10-0-6-235:/etc/puppet# cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
```

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
```

```
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
```

```
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp  /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
# X11Forwarding no
# AllowTcpForwarding no
# PermitTTY no
# ForceCommand cvs server
```

**After deletion**

```
root@ip-10-0-6-235:/etc/puppet# rm /etc/ssh/sshd_config
root@ip-10-0-6-235:/etc/puppet# puppet apply /etc/puppet/manifests/site.pp
Notice: Compiled catalog for ip-10-0-6-235.us-west-2.compute.internal in
environment production in 0.46 seconds
Notice: /Stage[main]/Sshd::Prelude/File[/etc/ssh/sshd_config]/ensure: defined
content as '{md5}52c2e9c45a8778e02ea5bb05fa7188e8'
Notice: /Stage[main]/Sshd::Prelude/Service[sshd]: Triggered 'refresh' from 2
events
Notice: Applied catalog in 0.16 seconds
root@ip-10-0-6-235:/etc/puppet# ls /etc/ssh/sshd_config
/etc/ssh/sshd_config
```

# Execution after "Modify or delete .ssh/authorized_keys in an instance's user account."

## After modification

```
root@ip-10-0-6-235:/etc/puppet# echo "tempering" >>
/home/ubuntu/.ssh/authorized_keys
root@ip-10-0-6-235:/etc/puppet# puppet apply /etc/puppet/manifests/site.pp
Notice: Compiled catalog for ip-10-0-6-235.us-west-2.compute.internal in
environment production in 0.47 seconds
Notice:
/Stage[main]/Sshd::Prelude/File[/home/ubuntu/.ssh/authorized_keys]/content:
content changed '{md5}0a5545701823df52b9bd95b307de16e9' to
'{md5}d41d8cd98f00b204e9800998ecf8427e'
Notice: /Stage[main]/Sshd::Prelude/Service[sshd]: Triggered 'refresh' from 2
events
Notice:
/Stage[main]/Sshd::Action/Ssh_authorized_key[xzpjerry@gmail.com]/ensure:
created
Notice: /Stage[main]/Sshd::Action/Ssh_authorized_key[mapu_pub_key]/ensure:
created
Notice: Applied catalog in 0.21 seconds
```

## After Deletion

```
root@ip-10-0-6-235:/etc/puppet# rm /home/ubuntu/.ssh/authorized_keys
root@ip-10-0-6-235:/etc/puppet# puppet apply /etc/puppet/manifests/site.pp
Notice: Compiled catalog for ip-10-0-6-235.us-west-2.compute.internal in
environment production in 0.44 seconds
Notice:
/Stage[main]/Sshd::Prelude/File[/home/ubuntu/.ssh/authorized_keys]/ensure:
defined content as '{md5}d41d8cd98f00b204e9800998ecf8427e'
Notice: /Stage[main]/Sshd::Prelude/Service[sshd]: Triggered 'refresh' from 2
events
Notice:
/Stage[main]/Sshd::Action/Ssh_authorized_key[xzpjerry@gmail.com]/ensure:
created
Notice: /Stage[main]/Sshd::Action/Ssh_authorized_key[mapu_pub_key]/ensure:
created
Notice: Applied catalog in 0.19 seconds
```