CYBERARK®

CYBERARK UNIVERSITY

PSM for SSH Servers

CyberArk Training

OBJECTIVES

By the end of this lesson, you will be able to:

- Describe the functionality of the PSM for SSH server
- Install the PSM for SSH server
- Configure the system to work with the PSM for SSH server
- Connect to a target machine through the PSM for SSH server

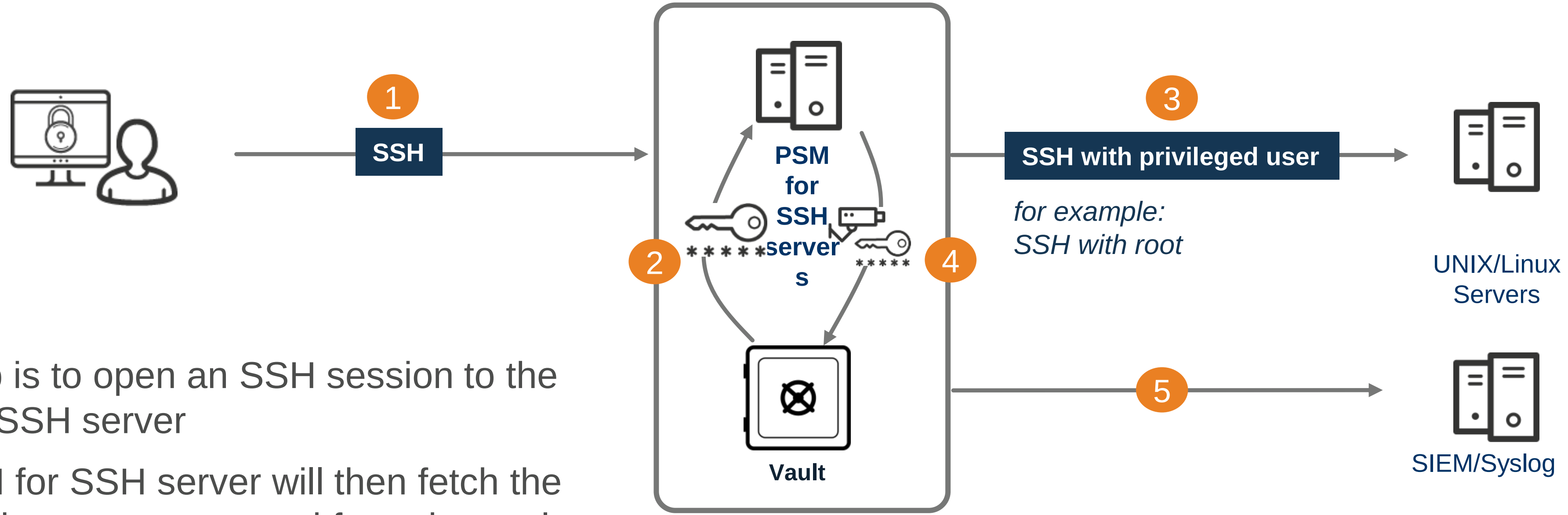
CYBERARK

OVERVIEW AND FUNCTIONALITY

THE PROBLEM

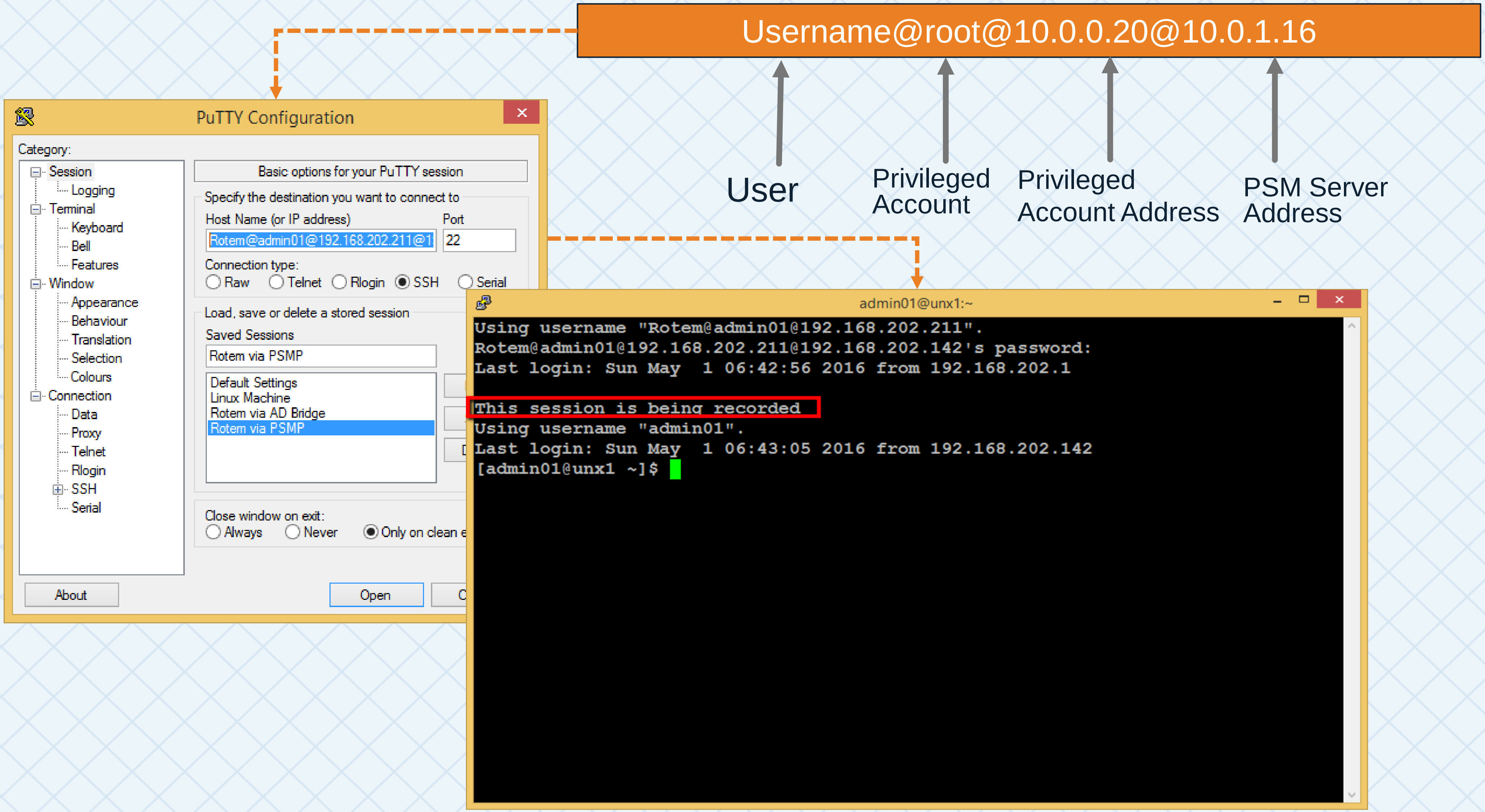
- The average enterprise manages hundreds of Unix servers and Network devices
- Unix, Linux systems are usually critical and are not centrally managed
- Unix Administrators understandably, will be reluctant to change their existing workflow and tool set to accommodate a new security layer
- The goal should be to integrate seamlessly with the existing business process using PSM for SSH servers

PSM FOR SSH SERVERS - OVERVIEW



1. First step is to open an SSH session to the PSM for SSH server
2. The PSM for SSH server will then fetch the privileged account password from the vault (using GW user)
3. The PSM for SSH servers will then establish an SSH session to the target system using the privileged account credentials
4. The session recording is uploaded to the vault
5. Logs are forwarded to the SIEM

CONNECTING VIA PSM FOR SSH SERVERS



Username@root@10.0.0.20@10.0.1.16

Specify the destination you want to connect to

Host Name (or IP address): Rotem@admin01@192.168.202.211@1

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Rotem via PSMP

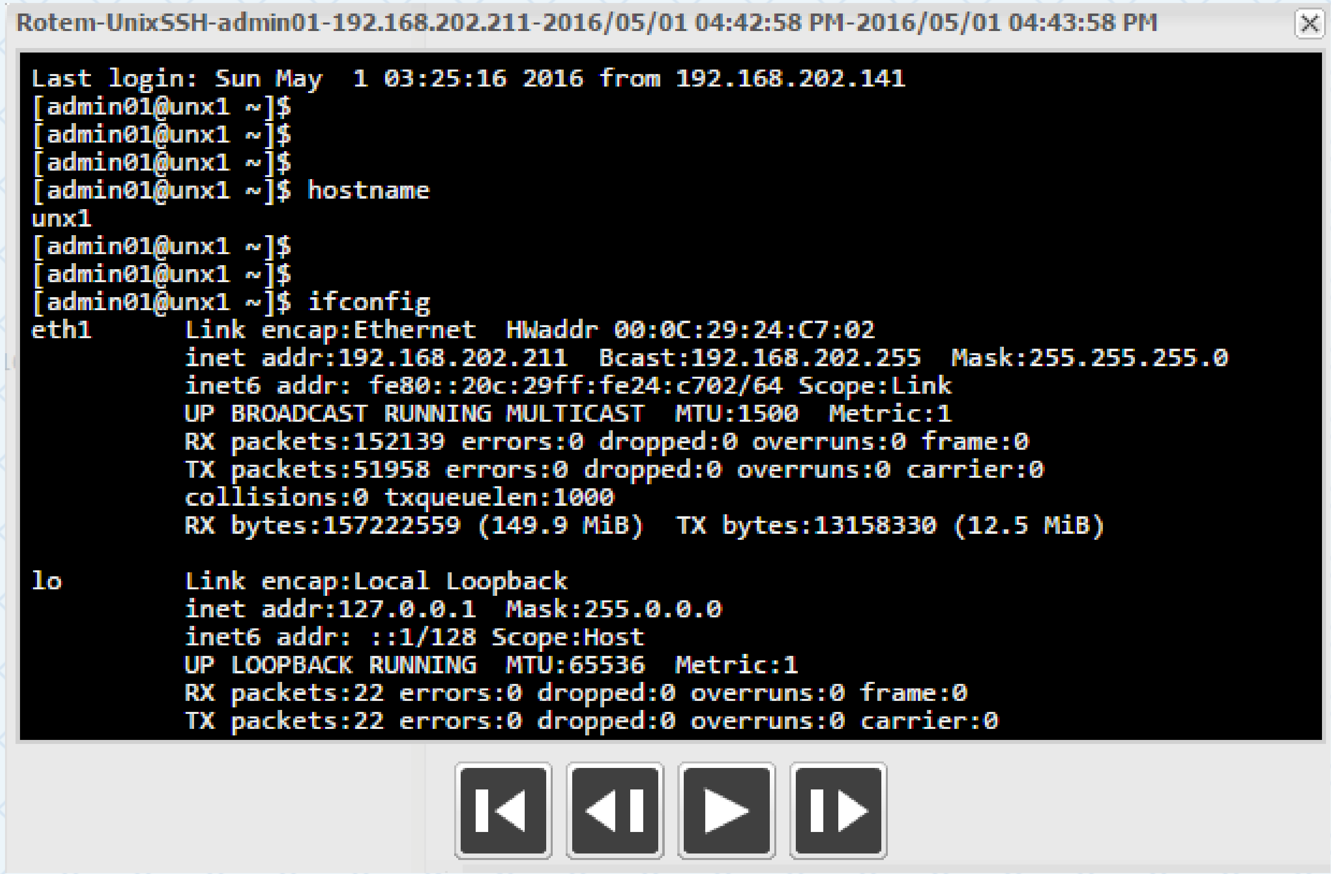
- Default Settings
- Linux Machine
- Rotem via AD Bridge
- Rotem via PSMP

Close window on exit: ○ Always ○ Never ● Only on clean e

```
Using username "Rotem@admin01@192.168.202.211".
Rotem@admin01@192.168.202.211@192.168.202.142's password:
Last login: Sun May  1 06:42:56 2016 from 192.168.202.1

This session is being recorded
Using username "admin01".
Last login: Sun May  1 06:43:05 2016 from 192.168.202.142
[admin01@unx1 ~]$
```

PSM SSH PROXY (PSM FOR SSH SERVERS) - AUDITING

Just like with PSM, members of the Auditors group can view PSM for SSH server video and text-based recordings



Rotem-UnixSSH-admin01-192.168.202.211-2016/05/01 04:42:58 PM-2016/05/01 04:43:58 PM

```
Last login: Sun May  1 03:25:16 2016 from 192.168.202.141
[admin01@unx1 ~]$
[admin01@unx1 ~]$
[admin01@unx1 ~]$
[admin01@unx1 ~]$ hostname
unx1
[admin01@unx1 ~]$
[admin01@unx1 ~]$
[admin01@unx1 ~]$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0C:29:24:C7:02
          inet addr:192.168.202.211  Bcast:192.168.202.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe24:c702/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:152139 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51958 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:157222559 (149.9 MiB)  TX bytes:13158330 (12.5 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
```

FEATURES

Protocols Support

- SSH, SSH Tunneling, SCP

PSSO

- Privileged Single Sign On (PSSO)
- Secure Connect
- AD Bridge

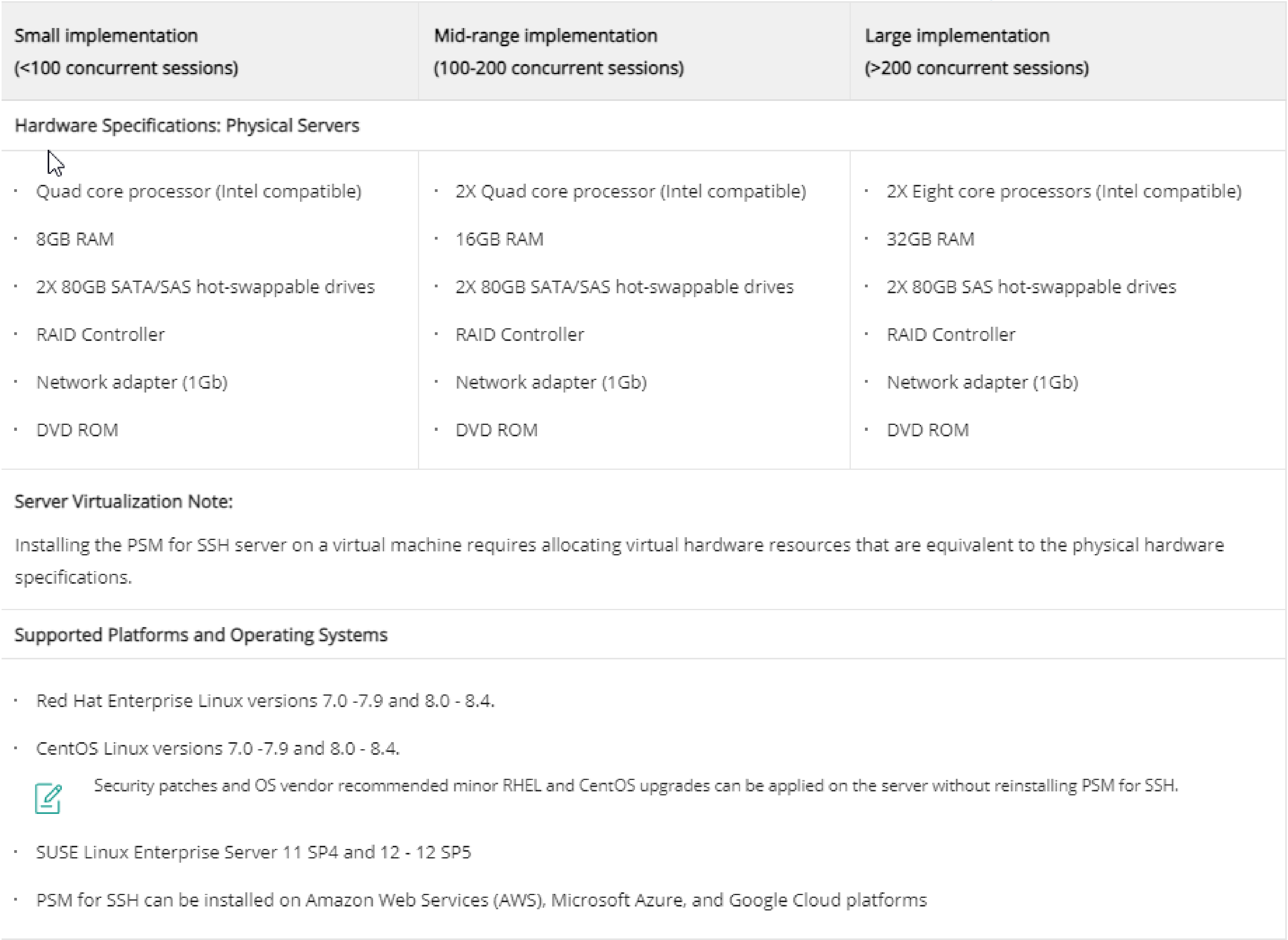
Access Control

- PSM for SSH servers manages access to privileged accounts at a centralized point and facilitates a control point to initiate privileged sessions

Session Recording

- The PSM for SSH servers record all activities that occur in the privileged session in a compact format
- Recordings are stored and protected in the Vault server and are accessible to authorized users

SYSTEM REQUIREMENTS



Small implementation (<100 concurrent sessions)	Mid-range implementation (100-200 concurrent sessions)	Large implementation (>200 concurrent sessions)
Hardware Specifications: Physical Servers		
· Quad core processor (Intel compatible) · 8GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Quad core processor (Intel compatible) · 16GB RAM · 2X 80GB SATA/SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM	· 2X Eight core processors (Intel compatible) · 32GB RAM · 2X 80GB SAS hot-swappable drives · RAID Controller · Network adapter (1Gb) · DVD ROM
Server Virtualization Note: Installing the PSM for SSH server on a virtual machine requires allocating virtual hardware resources that are equivalent to the physical hardware specifications.		
Supported Platforms and Operating Systems		
· Red Hat Enterprise Linux versions 7.0 -7.9 and 8.0 - 8.4. · CentOS Linux versions 7.0 -7.9 and 8.0 - 8.4. Security patches and OS vendor recommended minor RHEL and CentOS upgrades can be applied on the server without reinstalling PSM for SSH. · SUSE Linux Enterprise Server 11 SP4 and 12 - 12 SP5 · PSM for SSH can be installed on Amazon Web Services (AWS), Microsoft Azure, and Google Cloud platforms		

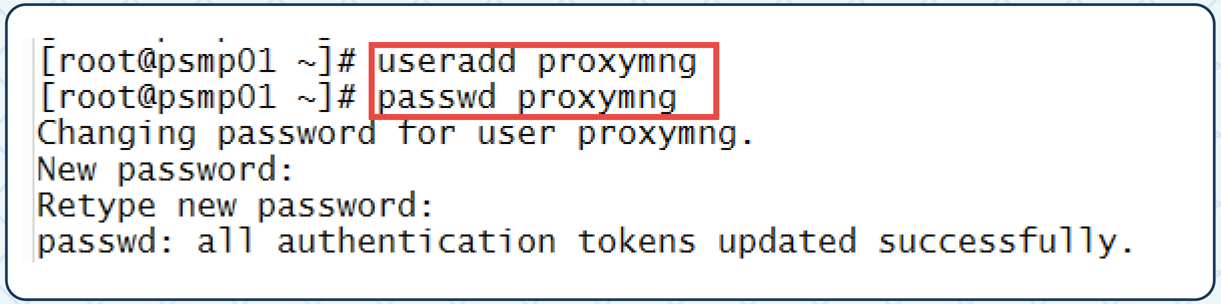
INSTALLATION

INSTALLATION STEPS

1. Copy the PSM for SSH server's software to the server. *This is done for you in your lab!*
2. Create administrative users
3. Edit the vault.ini
4. Create a credential file for the built-in Administrator user
5. Edit the PSMPparms file
6. Install PSM for SSH software

CREATE AN ADMINISTRATIVE USER

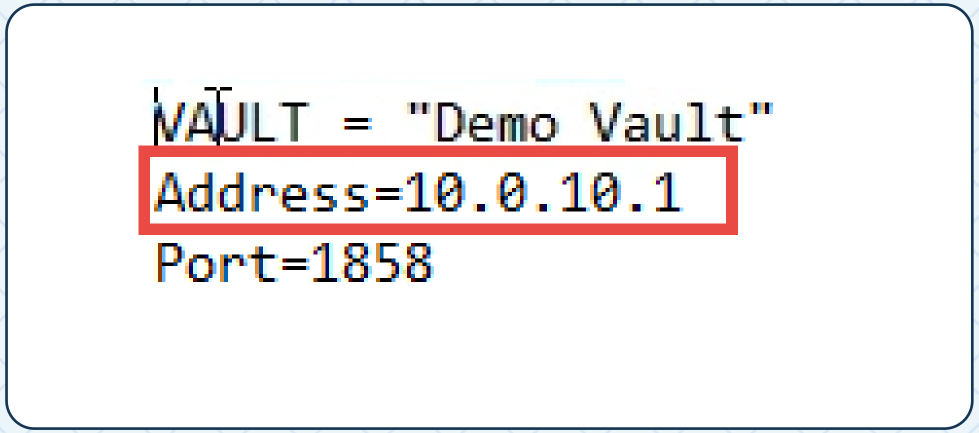
- Administrative users can connect to the PSM for SSH servers to perform management tasks without being forwarded to a target machine
- In addition to the built-in root users, the PSM for SSH servers identifies the following users as administrative users when they connect to the PSM for SSH servers server:
  - proxymng
  - proxymng<number>
  - Additional users that are specified in the **PSMP_MaintenanceUsers** parameter in the **sshd_config** configuration file



```
[root@psmp01 ~]# useradd proxymng
[root@psmp01 ~]# passwd proxymng
Changing password for user proxymng.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

EDIT VAULT.INI

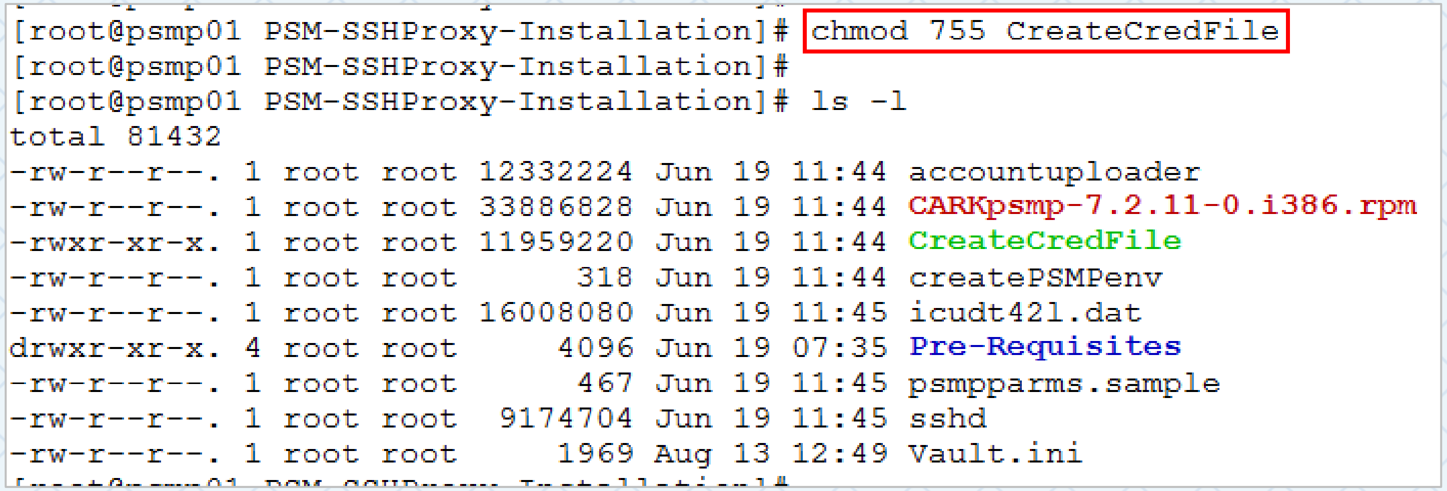
- Editing the vault.ini file to specify the Vault IP address



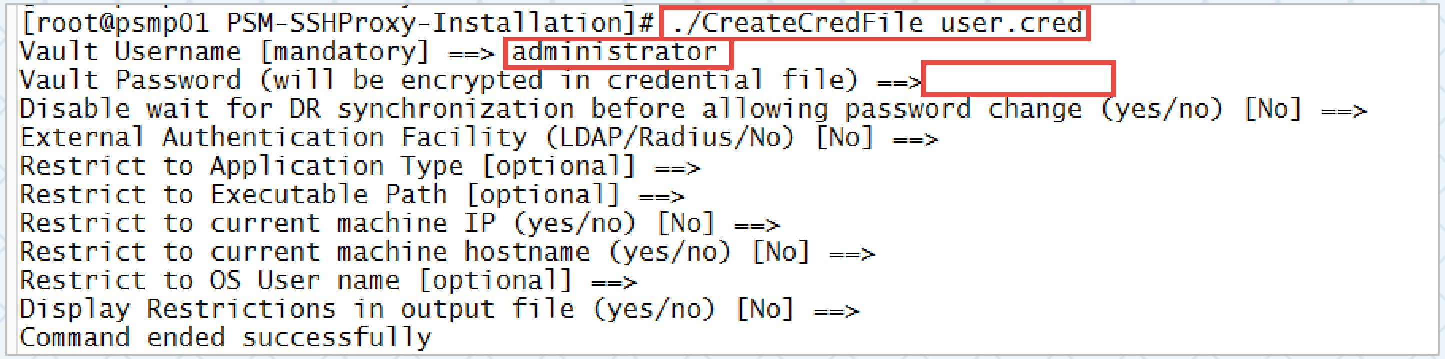
```
VAULT = "Demo Vault"
Address=10.0.10.1
Port=1858
```

CREATE CREDENTIAL FILE

- Create a credential file for the administrator user who will create the Vault environment during installation
- Add execute permissions on the CreateCredFile utility by running “chmod 755 CreateCredFile”



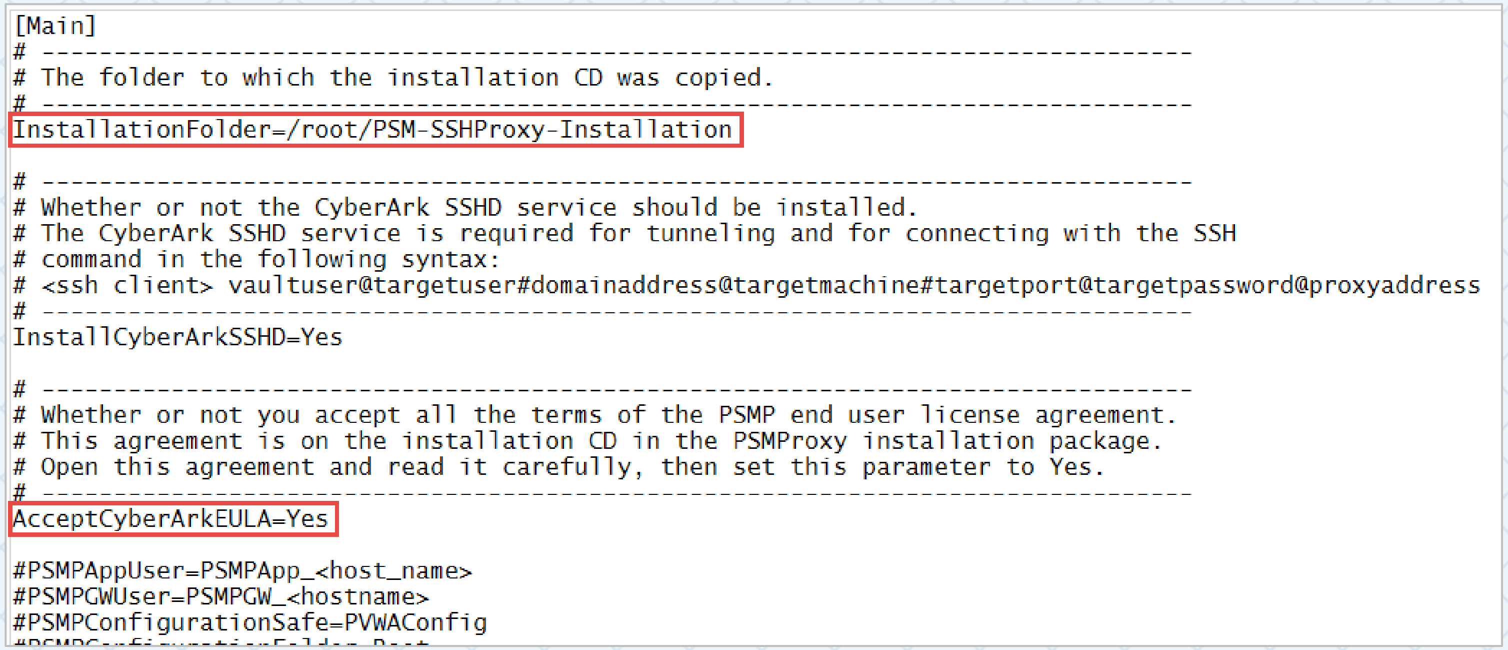
```
[root@psmp01 PSM-SSHProxy-Installation]# chmod 755 CreateCredFile
[root@psmp01 PSM-SSHProxy-Installation]#
[root@psmp01 PSM-SSHProxy-Installation]# ls -l
total 81432
-rw-r--r--. 1 root root 12332224 Jun 19 11:44 accountuploader
-rw-r--r--. 1 root root 33886828 Jun 19 11:44 CARKpsmp-7.2.11-0.i386.rpm
-rwxr-xr-x. 1 root root 11959220 Jun 19 11:44 CreateCredFile
-rw-r--r--. 1 root root      318 Jun 19 11:44 createPSMPenv
-rw-r--r--. 1 root root 16008080 Jun 19 11:45 icudt421.dat
drwxr-xr-x. 4 root root     4096 Jun 19 07:35 Pre-Requisites
-rw-r--r--. 1 root root      467 Jun 19 11:45 psmpparms.sample
-rw-r--r--. 1 root root  9174704 Jun 19 11:45 sshd
-rw-r--r--. 1 root root     1969 Aug 13 12:49 Vault.ini
```



```
[root@psmp01 PSM-SSHProxy-Installation]# ./CreateCredFile user.cred
Vault Username [mandatory] ==> administrator
Vault Password (will be encrypted in credential file) ==>
Disable wait for DR synchronization before allowing password change (yes/no) [No] ==>
External Authentication Facility (LDAP/Radius/No) [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to current machine IP (yes/no) [No] ==>
Restrict to current machine hostname (yes/no) [No] ==>
Restrict to OS User name [optional] ==>
Display Restrictions in output file (yes/no) [No] ==>
Command ended successfully
```

CREATE THE PSM FOR SSH SERVERS PARAMETERS FILE

- Move **PSMPparms.sample** to the ***/var/tmp*** directory and rename it to **PSMPparms**
- Edit the file and specify the following mandatory parameters:
  - InstallationFolder
  - AcceptCyberArkEULA

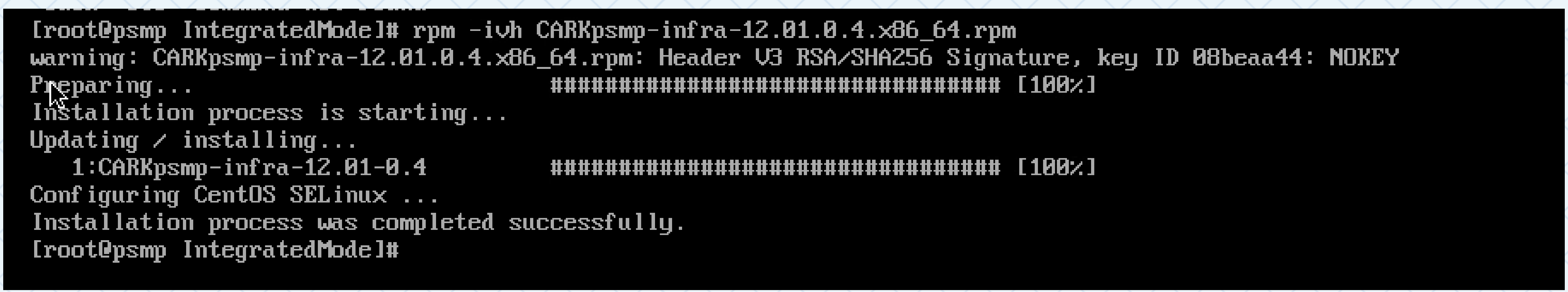


```
[Main]
# ---------------------------------------------------------------------------------
# The folder to which the installation CD was copied.
# ---------------------------------------------------------------------------------
InstallationFolder=/root/PSM-SSHProxy-Installation

# ---------------------------------------------------------------------------------
# Whether or not the CyberArk SSHD service should be installed.
# The CyberArk SSHD service is required for tunneling and for connecting with the SSH
# command in the following syntax:
# <ssh client> vaultuser@targetuser#domainaddress@targetmachine#targetport@targetpassword@proxyaddress
# ---------------------------------------------------------------------------------
InstallCyberArkSSHD=Yes

# ---------------------------------------------------------------------------------
# Whether or not you accept all the terms of the PSMP end user license agreement.
# This agreement is on the installation CD in the PSMProxy installation package.
# Open this agreement and read it carefully, then set this parameter to Yes.
# ---------------------------------------------------------------------------------
AcceptCyberArkEULA=Yes

#PSMPAppUser=PSMPApp_<host_name>
#PSMPGWUser=PSMPGW_<hostname>
#PSMPConfigurationSafe=PVWAConfig
#PSMPConfigurationFolder=Root
```

INSTALL THE PSM FOR SSH INFRASTRUCTURE PACKAGE

The PSM for SSH Infrastructure package is an important pre-requisite to running the PSM for SSH installation

Launch the PSMP Infrastructure package

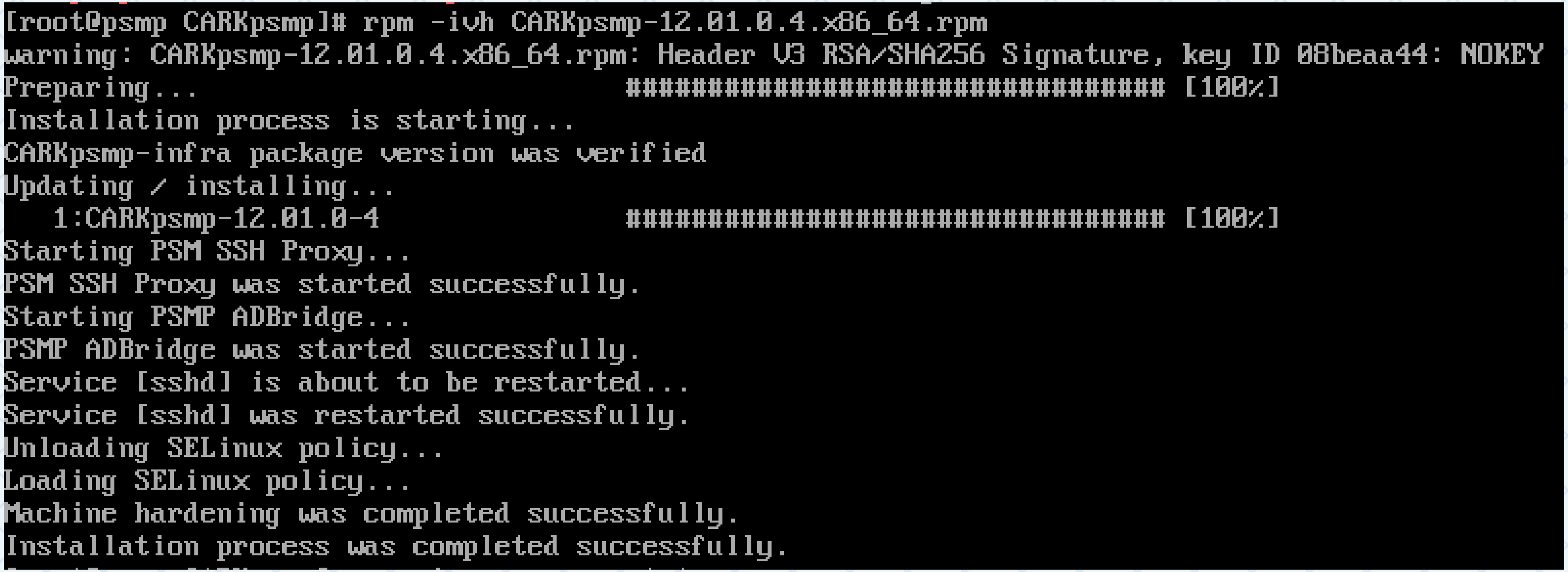


```
[root@psmp IntegratedMode]# rpm -ivh CARKpsmp-infra-12.01.0.4.x86_64.rpm
warning: CARKpsmp-infra-12.01.0.4.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID 08beaa44: NOKEY
Preparing...                          ################################# [100%]
Installation process is starting...
Updating / installing...
   1:CARKpsmp-infra-12.01-0.4         ################################# [100%]
Configuring CentOS SELinux ...
Installation process was completed successfully.
[root@psmp IntegratedMode]#
```

RUN THE INSTALLATION

- Run the following **rpm** command to begin the installation:
  - rpm –i <rpm-file-name>

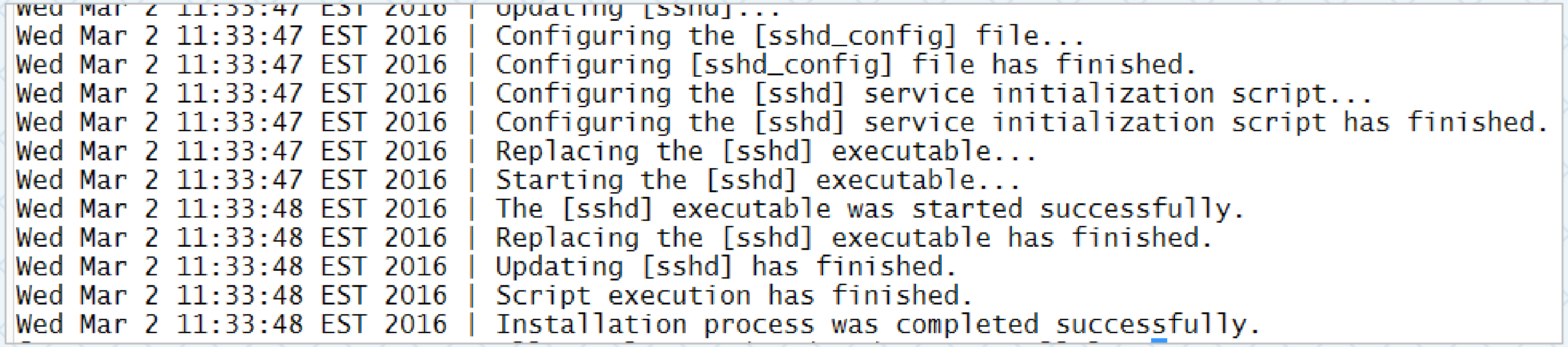
- Optionally, use the following switches for the rpm command:
  - **-v** – Displays additional information while installing
  - **-h** – Prints pound symbols (#) as installation progresses



```
[root@psmp CARKpsmp]# rpm -ivh CARKpsmp-12.01.0.4.x86_64.rpm
warning: CARKpsmp-12.01.0.4.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID 08beaa44: NOKEY
Preparing...                          ################################# [100%]
Installation process is starting...
CARKpsmp-infra package version was verified
Updating / installing...
   1:CARKpsmp-12.01.0-4               ################################# [100%]
Starting PSM SSH Proxy...
PSM SSH Proxy was started successfully.
Starting PSMP ADBridge...
PSMP ADBridge was started successfully.
Service [sshd] is about to be restarted...
Service [sshd] was restarted successfully.
Unloading SELinux policy...
Loading SELinux policy...
Machine hardening was completed successfully.
Installation process was completed successfully.
```

VERIFY THE INSTALLATION

- Review the following installation log files to ensure the installation completed successfully or find errors that occurred:
  - **/var/tmp/PSMP_install.log** – This log file describes the activities that occurred during the installation process
  - **/var/opt/CARKPSMP/temp/CreateEnv.log** – This log file describes the activities that occurred when the Vault environment for PSM for SSH servers was created

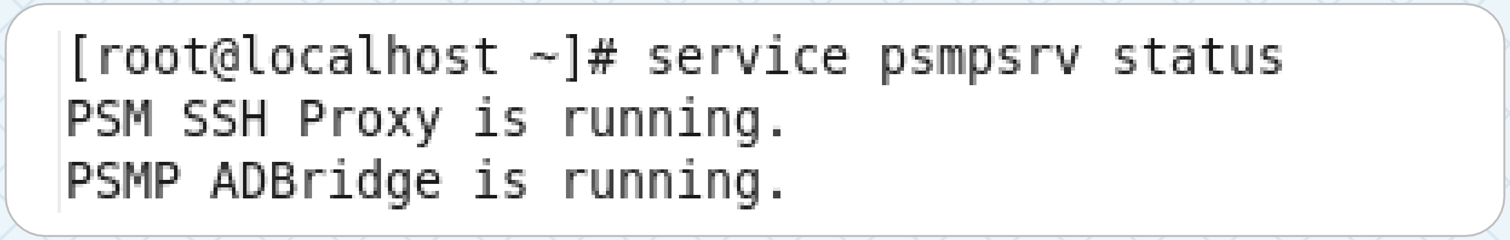


```
Wed Mar 2 11:33:47 EST 2016 | Updating [sshd]...
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd_config] file...
Wed Mar 2 11:33:47 EST 2016 | Configuring [sshd_config] file has finished.
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd] service initialization script...
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd] service initialization script has finished.
Wed Mar 2 11:33:47 EST 2016 | Replacing the [sshd] executable...
Wed Mar 2 11:33:47 EST 2016 | Starting the [sshd] executable...
Wed Mar 2 11:33:48 EST 2016 | The [sshd] executable was started successfully.
Wed Mar 2 11:33:48 EST 2016 | Replacing the [sshd] executable has finished.
Wed Mar 2 11:33:48 EST 2016 | Updating [sshd] has finished.
Wed Mar 2 11:33:48 EST 2016 | Script execution has finished.
Wed Mar 2 11:33:48 EST 2016 | Installation process was completed successfully.
```

THE PSM FOR SSH SERVERS SERVICE

Monitoring the PSM for SSH servers Service

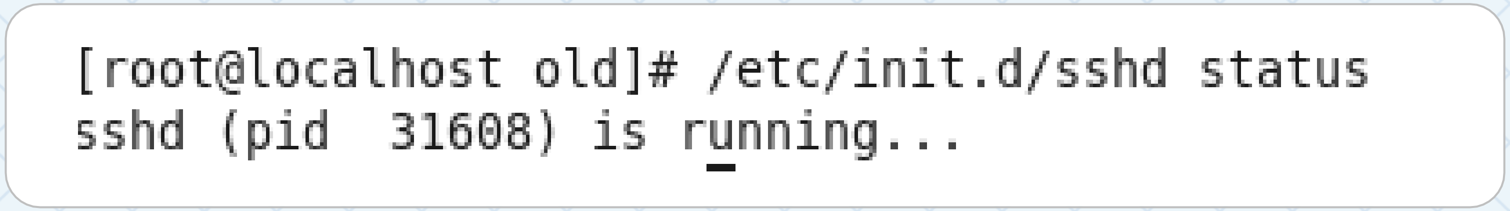
- /etc/init.d/psmpsrv stop | start | status
- psmpsrvstop | start | status



```
[root@localhost ~]# service psmpsrv status
PSM SSH Proxy is running.
PSMP ADBridge is running.
```

Monitoring the ‘sshd’ daemon service

- SSH Daemon:
- service sshd [status | stop | start]



```
[root@localhost old]# /etc/init.d/sshd status
sshd (pid  31608) is running...
```

VERIFY ENVIRONMENT

INSTALLATION FOLDER

/opt/CARKPSMP/bin/

- PSM for SSH serversserver
- createenv
- createcredfile

/var/opt/CARKPSMP/

- logs
- recordings

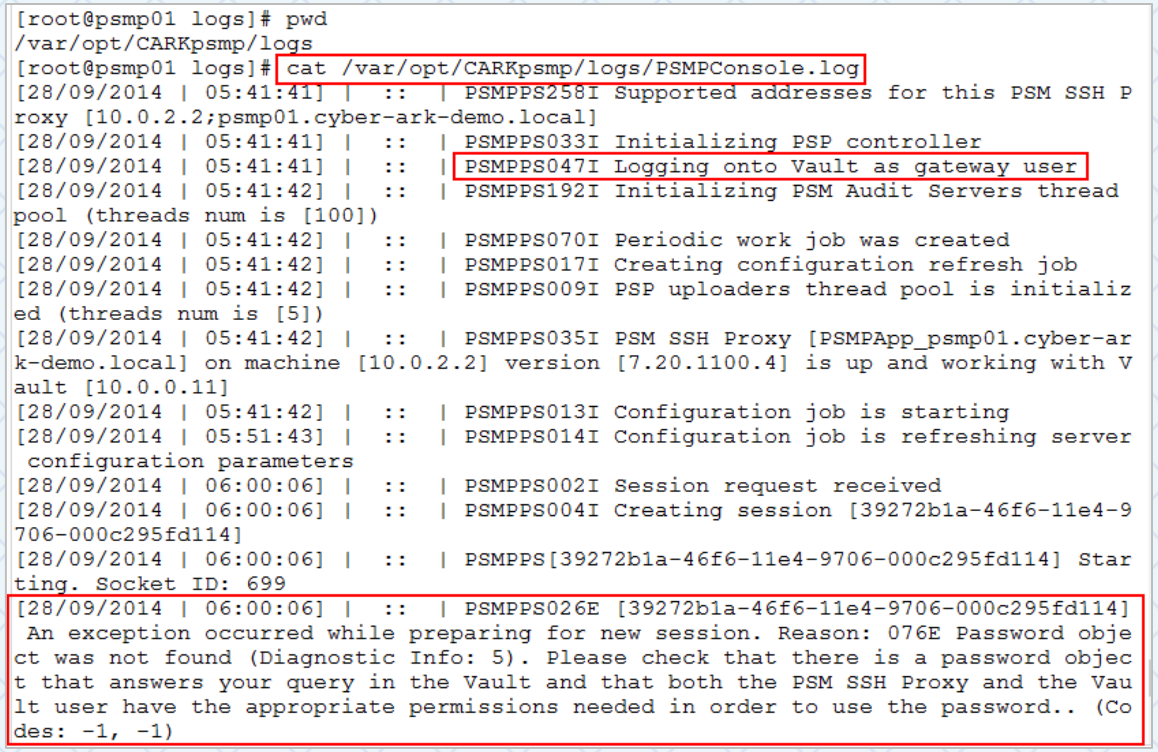
/etc/opt/CARKPSMP/

- conf – basic configuration file
- vault – vault.ini and cred files

PSM FOR SSH SERVERS LOGS

- **PSMPConsole.log** – contains informational messages and errors that refer to PSM function. This log is meant for the system administrator who needs to monitor the status of the PSM for SSH servers
- **PSMPTrace.log** – contains errors and trace messages. The types of messages that are included depend on the debug levels specified in the main configuration file

**Log Location:
/var/opt/CARKPSMP/logs/**



```
[root@psmp01 logs]# pwd
/var/opt/CARKpsmp/logs
[root@psmp01 logs]# cat /var/opt/CARKpsmp/logs/PSMPConsole.log
[28/09/2014 | 05:41:41] |  ::  | PSMPPS258I Supported addresses for this PSM SSH P
roxy [10.0.2.2;psmp01.cyber-ark-demo.local]
[28/09/2014 | 05:41:41] |  ::  | PSMPPS033I Initializing PSP controller
[28/09/2014 | 05:41:41] |  ::  | PSMPPS047I Logging onto Vault as gateway user
[28/09/2014 | 05:41:42] |  ::  | PSMPPS192I Initializing PSM Audit Servers thread
pool (threads num is [100])
[28/09/2014 | 05:41:42] |  ::  | PSMPPS070I Periodic work job was created
[28/09/2014 | 05:41:42] |  ::  | PSMPPS017I Creating configuration refresh job
[28/09/2014 | 05:41:42] |  ::  | PSMPPS009I PSP uploaders thread pool is initializ
ed (threads num is [5])
[28/09/2014 | 05:41:42] |  ::  | PSMPPS035I PSM SSH Proxy [PSMPApp_psmp01.cyber-ar
k-demo.local] on machine [10.0.2.2] version [7.20.1100.4] is up and working with V
ault [10.0.0.11]
[28/09/2014 | 05:41:42] |  ::  | PSMPPS013I Configuration job is starting
[28/09/2014 | 05:51:43] |  ::  | PSMPPS014I Configuration job is refreshing server
 configuration parameters
[28/09/2014 | 06:00:06] |  ::  | PSMPPS002I Session request received
[28/09/2014 | 06:00:06] |  ::  | PSMPPS004I Creating session [39272b1a-46f6-11e4-9
706-000c295fd114]
[28/09/2014 | 06:00:06] |  ::  | PSMPPS[39272b1a-46f6-11e4-9706-000c295fd114] Star
ting. Socket ID: 699
[28/09/2014 | 06:00:06] |  ::  | PSMPPS026E [39272b1a-46f6-11e4-9706-000c295fd114]
 An exception occurred while preparing for new session. Reason: 076E Password obje
ct was not found (Diagnostic Info: 5). Please check that there is a password objec
t that answers your query in the Vault and that both the PSM SSH Proxy and the Vau
lt user have the appropriate permissions needed in order to use the password.. (Co
des: -1, -1)
```

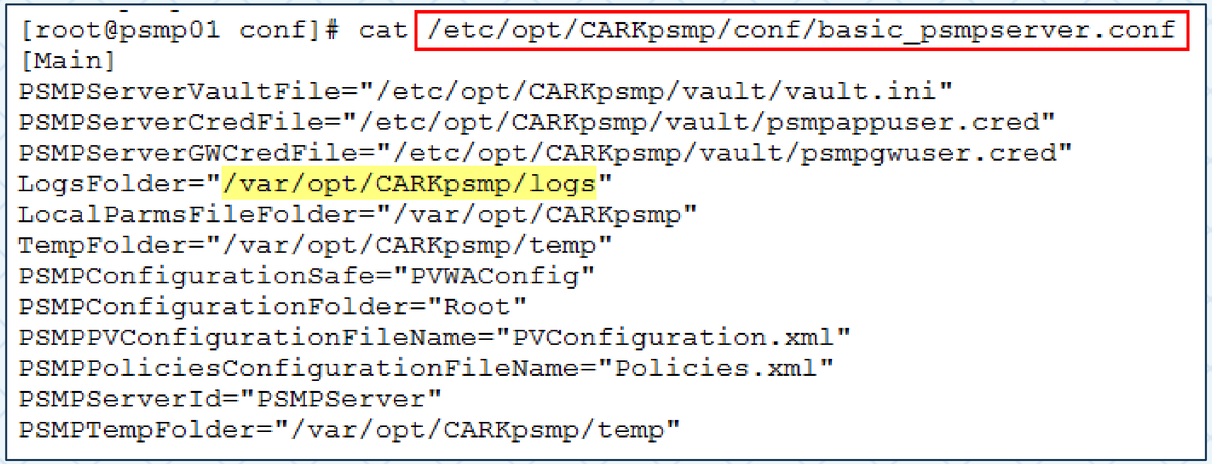
PSM FOR SSH SERVERS BASIC CONFIGURATION FILE

The PSM for SSH server configuration file is located here:

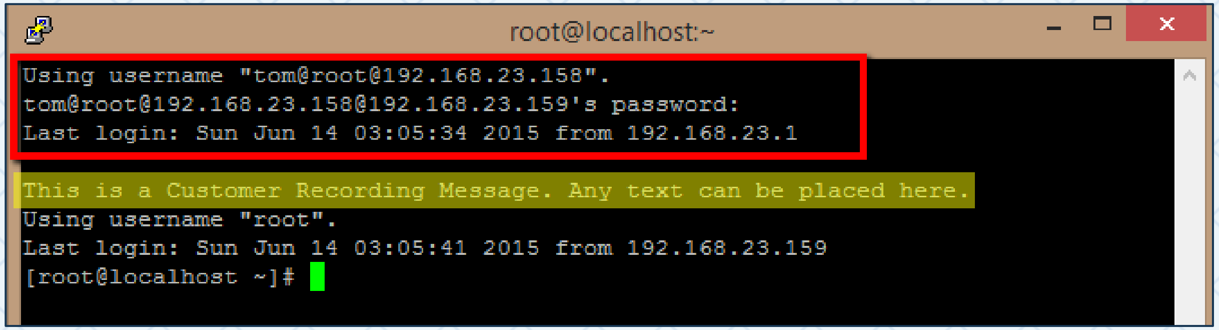
/etc/opt/CARKPSMP/conf/basic_PSMPserver.conf

Optional: Add the following parameter in the basic_PSMPserver.conf file to customize the message that is displayed to the end users:

PSMPRecordingNotificationMessage=“Your Message”



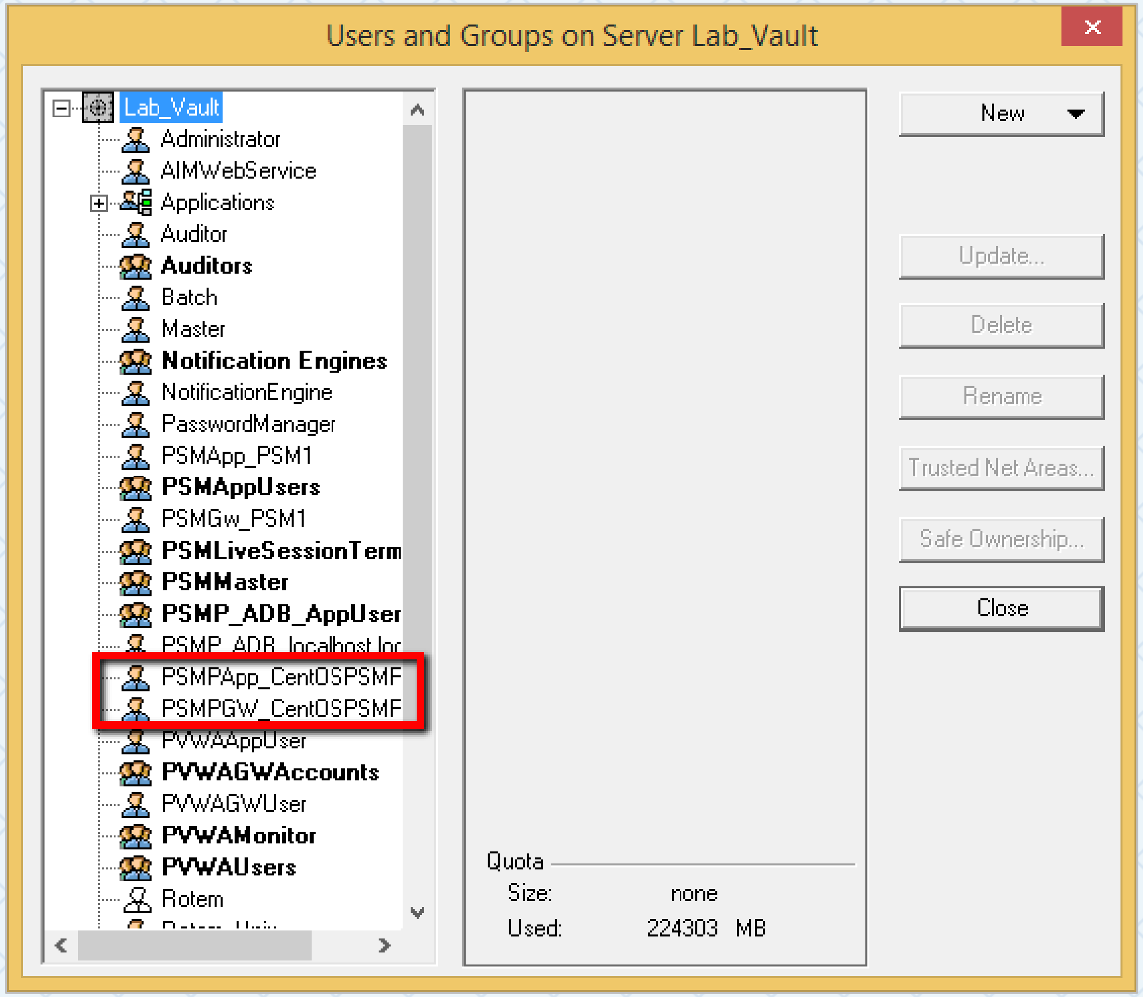
```
[root@psmp01 conf]# cat /etc/opt/CARKpsmp/conf/basic_psmpserver.conf
[Main]
PSMPServerVaultFile="/etc/opt/CARKpsmp/vault/vault.ini"
PSMPServerCredFile="/etc/opt/CARKpsmp/vault/psmpappuser.cred"
PSMPServerGWCredFile="/etc/opt/CARKpsmp/vault/psmpgwuser.cred"
LogsFolder="/var/opt/CARKpsmp/logs"
LocalParmsFileFolder="/var/opt/CARKpsmp"
TempFolder="/var/opt/CARKpsmp/temp"
PSMPConfigurationSafe="PVWAConfig"
PSMPConfigurationFolder="Root"
PSMPPVConfigurationFileName="PVConfiguration.xml"
PSMPPoliciesConfigurationFileName="Policies.xml"
PSMPServerId="PSMPServer"
PSMPTempFolder="/var/opt/CARKpsmp/temp"
```



```
Using username "tom@root@192.168.23.158".
tom@root@192.168.23.158@192.168.23.159's password:
Last login: Sun Jun 14 03:05:34 2015 from 192.168.23.1

This is a Customer Recording Message. Any text can be placed here.
Using username "root".
Last login: Sun Jun 14 03:05:41 2015 from 192.168.23.159
[root@localhost ~]#
```

PSM FOR SSH SERVERS ENVIRONMENT (VAULT)

- PSMPApp_<ServerName> is used by the PSM for SSH servers for internal processing
- PSMPGW_<ServerName> is the Gateway user through which the PSM for SSH servers will access the Vault to retrieve the privileged account



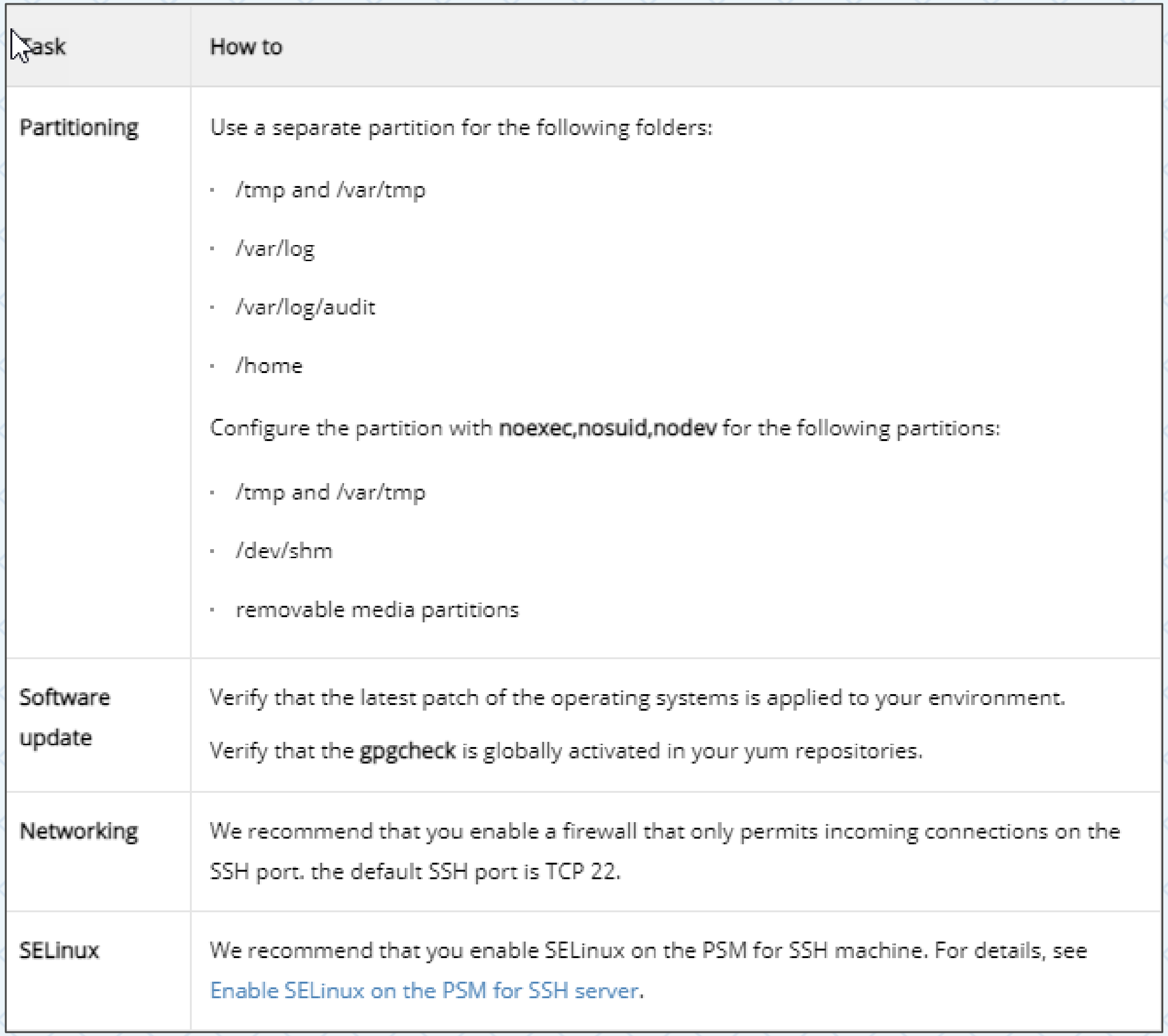
Lab_Vault
- Administrator
- AIMWebService
- Applications
- Auditor
- **Auditors**
- Batch
- Master
- **Notification Engines**
- NotificationEngine
- PasswordManager
- PSMApp_PSM1
- **PSMAppUsers**
- PSMGw_PSM1
- **PSMLiveSessionTerm**
- **PSMMaster**
- **PSMP_ADB_AppUser**
- PSMP_ADB_localhost_loc
- PSMPApp_CentOSPSMF
- PSMPGW_CentOSPSMF
- PVWAAppUser
- **PVWAGWAccounts**
- PVWAGWUser
- **PVWAMonitor**
- **PVWAUsers**
- Rotem

Quota
Size: none
Used: 224303 MB

HARDENING AND SECURITY

PSM FOR SSH SERVER HARDENING AND SECURITY

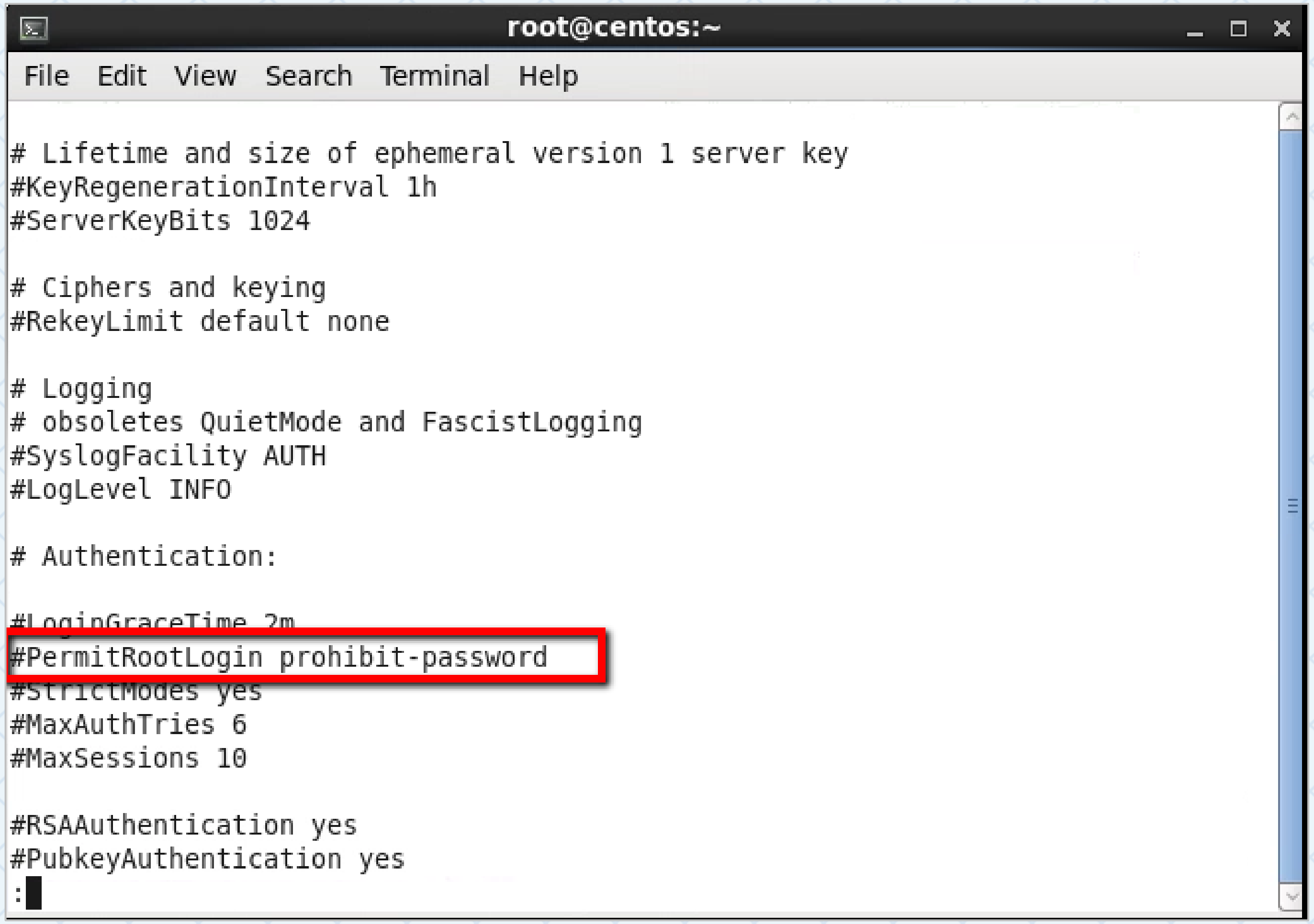
- The PSM for SSH server is automatically hardened during installation on supported platforms
- Hardening enforces security best practices recommended for these platforms
- The table on the right describes the additional manual steps you need to do to harden the PSM for SSH server after installation



Task	How to
Partitioning	Use a separate partition for the following folders: · /tmp and /var/tmp · /var/log · /var/log/audit · /home Configure the partition with **noexec,nosuid,nodev** for the following partitions: · /tmp and /var/tmp · /dev/shm · removable media partitions
Software update	Verify that the latest patch of the operating systems is applied to your environment. Verify that the **gpgcheck** is globally activated in your yum repositories.
Networking	We recommend that you enable a firewall that only permits incoming connections on the SSH port. the default SSH port is TCP 22.
SELinux	We recommend that you enable SELinux on the PSM for SSH machine. For details, see Enable SELinux on the PSM for SSH server.

DISABLING ROOT ACCESS

- The root user will not be able to authenticate to the PSM for SSH server remotely using a password, after hardening
- If an **administrative user** is not created **in advance**, access will only be possible either by console access or by authenticating the root user with an SSH key

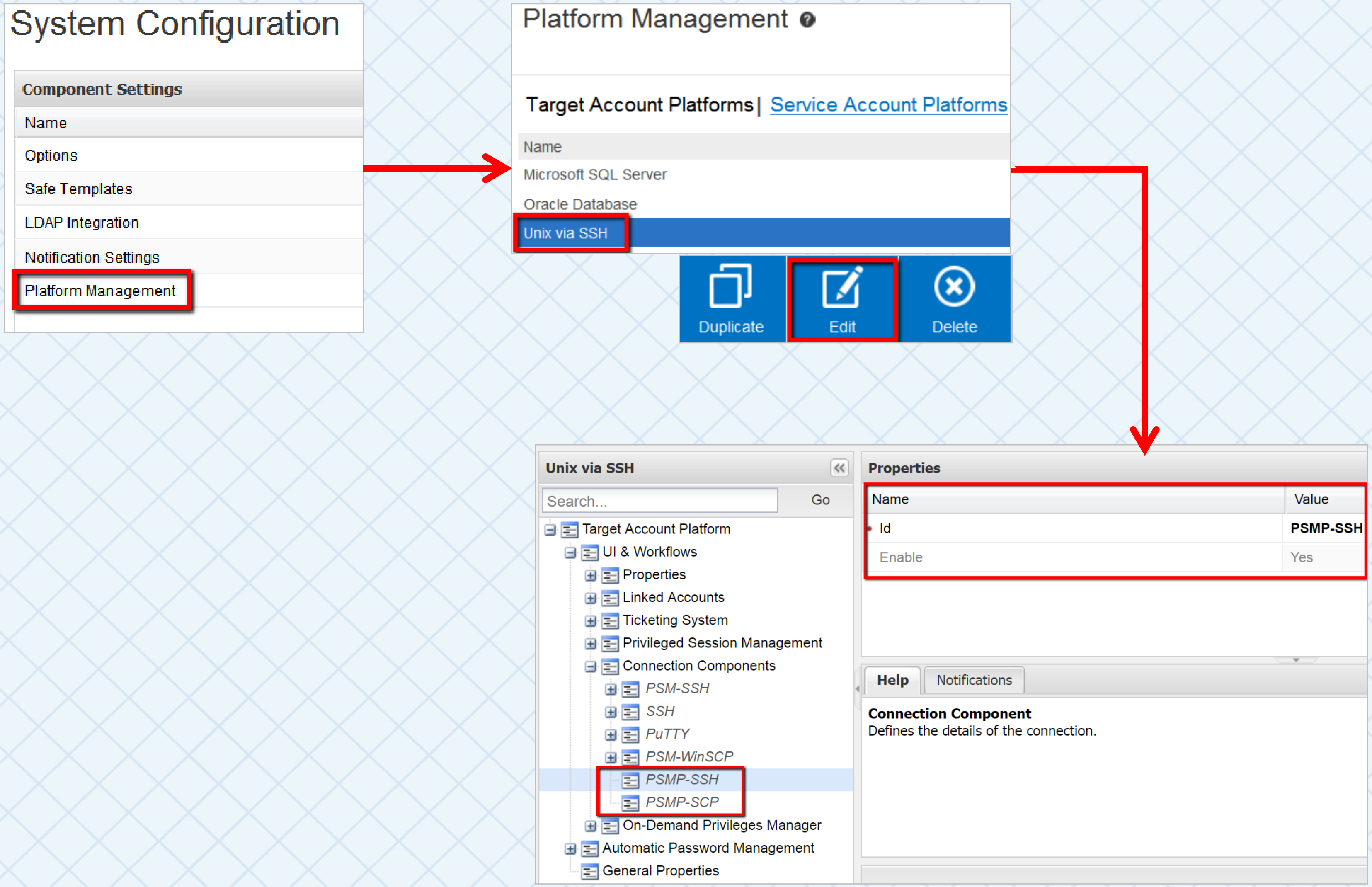


```
# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#RSAAuthentication yes
#PubkeyAuthentication yes
:
```

ENABLE PSM FOR SSH SERVERS

ADD CONNECTION COMPONENT TO PLATFORM

- In the Master Policy, Privileged Session Management must be enabled for Target Platforms
- Enabling PSM for SSH server is as simple as adding the PSM for SSH servers-SSH connection component link to a Target Account Platform, as shown in the slide
- PSMP-SSH and PSMP-SCP are only automatically added to the default Unix via SSH Target Account Platform

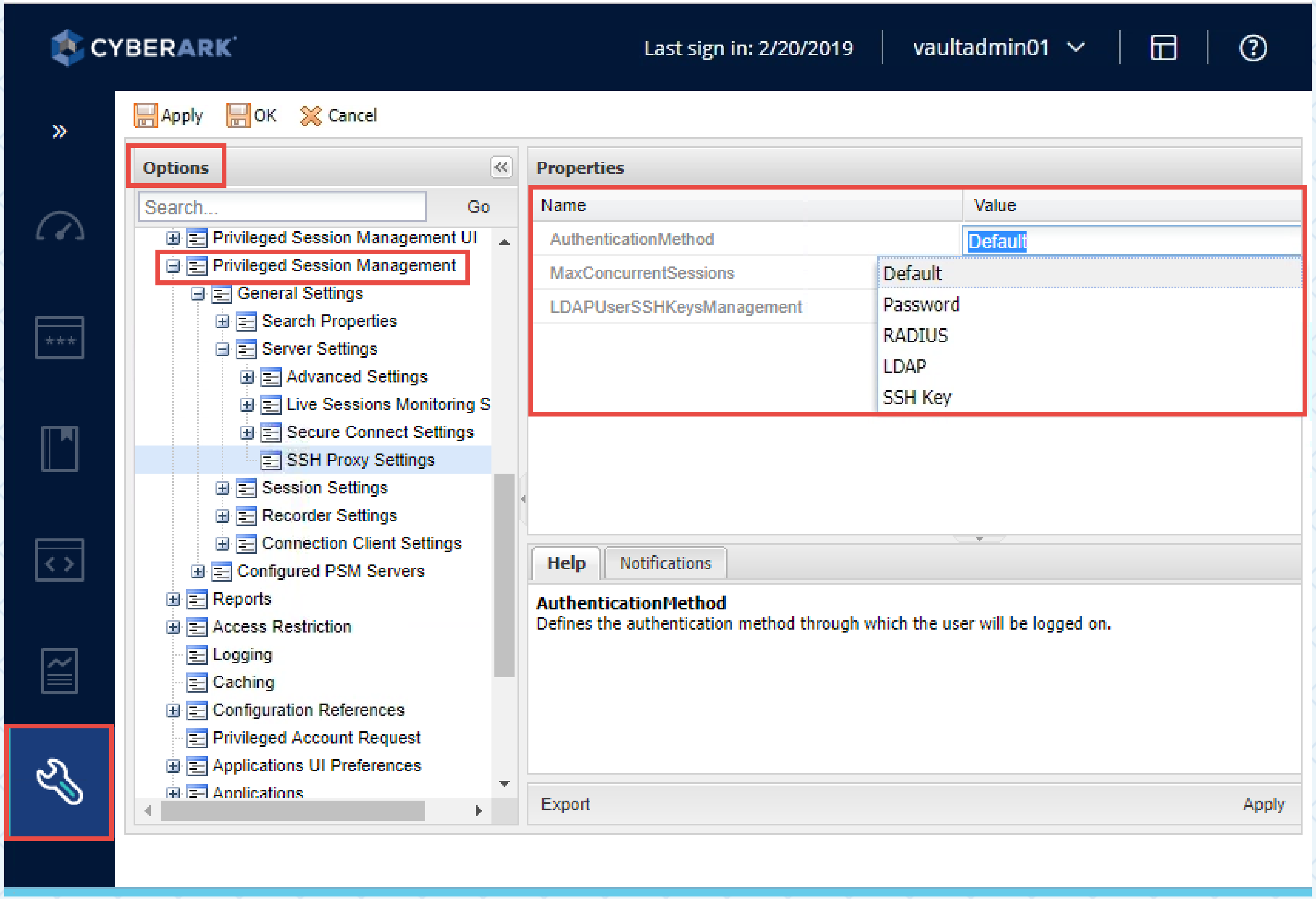


Name	Value
Id	PSMP-SSH
Enable	Yes

Connection Component
Defines the details of the connection.

CONFIGURING AUTHENTICATION METHODS

- Supported authentication methods include;
  - CyberArk authentication
  - RADIUS
  - LDAP
  - SSH Key
- MFA Caching is now supported in v12.1 allowing the same authentication methods used at the PVWA
- See “MFA Caching” on docs.cyberark.com

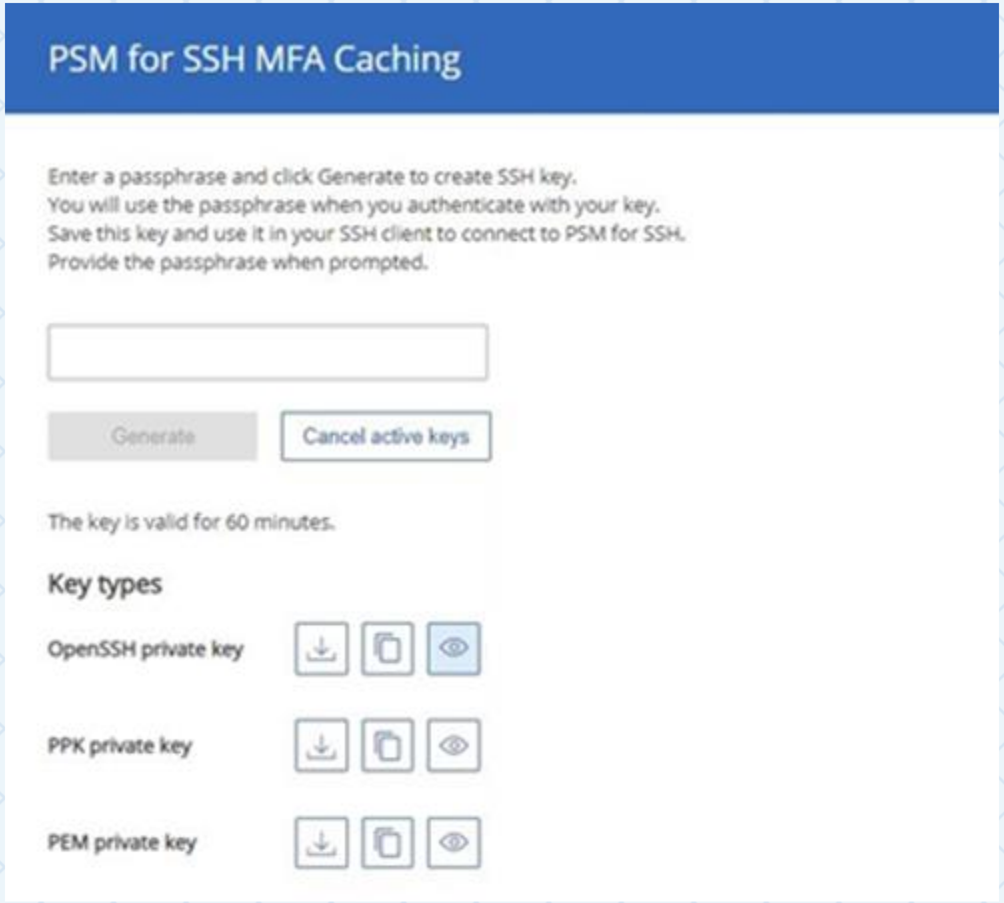


Name	Value
AuthenticationMethod	Default
MaxConcurrentSessions	
LDAPUserSSHKeysManagement	

AuthenticationMethod
Defines the authentication method through which the user will be logged on.

MFA CACHING

- Any method supported for authentication to the PVWA, can now use the same authentication method in PSM for SSH
- Administrators must first access the PVWA and select the required authentication method
- Then navigate to the PSM for SSH MFA caching page and generate an SSH Key with a preconfigured validity period allowing users to connect to any target server



PSM for SSH MFA Caching

Enter a passphrase and click Generate to create SSH key.
You will use the passphrase when you authenticate with your key.
Save this key and use it in your SSH client to connect to PSM for SSH.
Provide the passphrase when prompted.

The key is valid for 60 minutes.

Key types

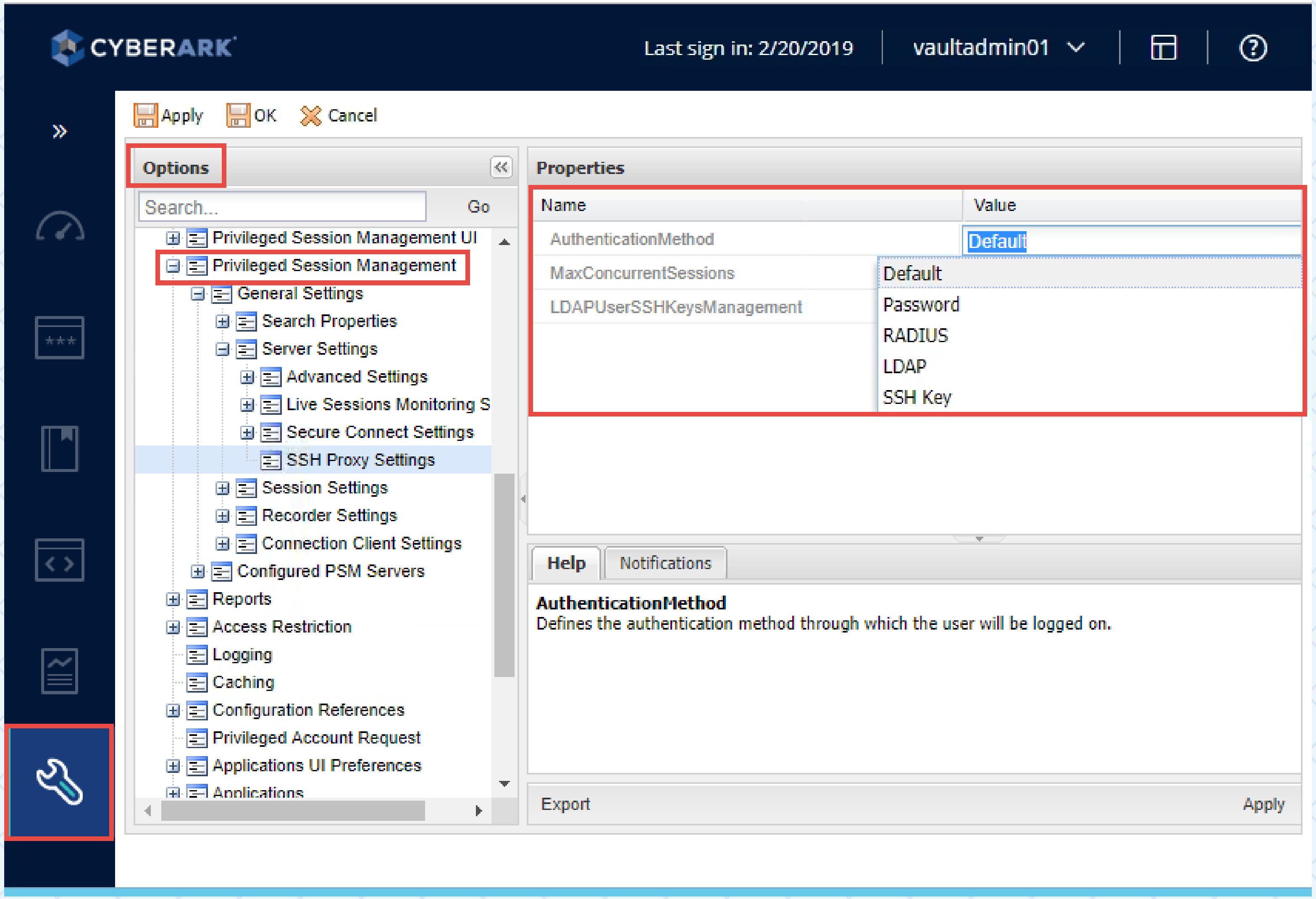
OpenSSH private key

PPK private key

PEM private key

CONFIGURING AUTHENTICATION METHODS

- CyberArk recommends using Change Management procedures when implementing policy changes
- Changes to policies are propagated automatically and do not require a restart of the service
- In the case of an emergency where the change must be implemented immediately, restart the services manually on the PSM for SSH server



Name	Value
AuthenticationMethod	Default
MaxConcurrentSessions	
LDAPUserSSHKeysManagement	

Default
Password
RADIUS
LDAP
SSH Key

AuthenticationMethod
Defines the authentication method through which the user will be logged on.

SUMMARY

OBJECTIVES

In this session we covered:

- The functionality of the PSM for SSH server
- Installing the PSM for SSH server
- Configuring the system to work with the PSM for SSH server
- Connecting to a target machine through the PSM for SSH server

CYBERARK

THANK YOU