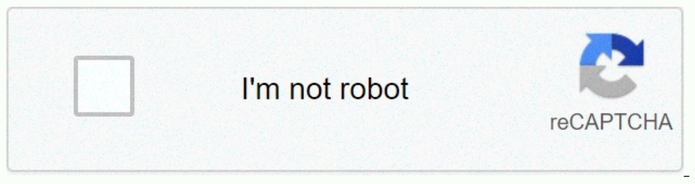

Continue

Cyberark psmp admin guide

This post is to present the installation steps of psmp. 1 Minimal installation of CentOS7 2 SSHD Service installed Installation Steps 1 Copy PSM SSH servers to the software server on which you downloaded the CyberArk Secure File Exchange (SFE) site. unzip Privileged\Session\Manager\SSH\Proxy-Rls-v11.4.1.zip 2 Create administrator-privileged users of psm ssh servers on the machine in the future administrator access. useradd proxymng passwd proxymng 3 Edit vault.ini file set your vault ip vi vault.ini 4 Create credentials file user.cred built-in administrator user to perform installation. chmod 755 CreateCredFile ./CreateCredFile user.cred 5 Edit PSMPparms file to define the installation path and accept the full installation path of the software license agreement mv psmpparms.sample /var/tmp/psmpparms or /var/tmp/psmpparms Parameter Installation Installation Folder for the full installation folder path that you previously created, and if you copied psm content for the SSH installation package. InstallCyberArkSSHD Either the PSM SSH installation installation installs the CyberArk SSHD service or is integrated with the original service. The default value is Yes. For more information, see the InstallCyberArkSSHD parameter. AcceptCyberArkEULA Whether or not you agree to all psm terms of the SSH End User License Agreement. This agreement is the installation package for the PSM installation package. Open this agreement and read it carefully, then set this parameter to Yes. You can't install PSM SSH until you agree to all terms of the license agreement whether the PSM SSH hardening settings are applied. Whether the installation creates a PSM SSH environment vault. By default, this parameter is set to Yes. The standard installation is set to Yes. Installation stages set to No 6 Install software RPM package rpm -ivh CARKpsmp-11.04.1.7.x86_64.rpm -v - Displays additional information during installation. -h – Prints the hashtags (#) as the installation progresses. PSM for SSH is installed on /etc/init.d/. The installation starts automatically and does not require an interactive response from the user. When the installation is complete, you receive the following message: The installation process has been successfully completed. If there are any problems troubleshooting, see the details of the 20INST/Installing-the-PSMP.htm 7 Test System Check System Health New PSMP Connection Components for YouTube Video: Links 1 Before installing PSM SSH 2 Install PSM SSH. Psm for SSH is installed on an automatic system service called psmpsrv. You can manage this service by using the following command: /etc/init.d/psmpsrv {start|stop|restart|status} [{psmp|psmpadb}] The Psmpsrv service allows you to manage PSM SSH and AD Bridge servers either individually or together using one of the following commands: Manage only the PSM SSH server, command: /etc/init.d/psmpsrv {start|stop|restart|status} psmp To manage only psm SSH AD Bridge server, run the following command: /etc/init.d/psmpsrv {start|stop|restart|status} psmpadb Manage both PSM SSH and PSM SSH AD Bridge server together, does not specify the server as shown below: /etc/init.d/psmpsrv {start|stop|restart|status} SSH proxy tisSi ltSi thsing device Administrators can connect to the SSH device for administrative tasks without being transmitted to the target device, using the following command: <ssh client=> <administrative user=>@ These users have high rights in the PSM of the SSH device. Therefore, they should be given access to the least respected rights principles and protected by storage and management of their credentials in the repository and by accessing their credentials for another PsM for an SSH computer. To create an administrator-privileged user, InstallCyberarkSSHD is set to Yes or no PSM SSH detects the following users for administrator users when they connect to the PSM SSH server: proxyng proxymng<number> Additional users that are assigned the PSMP_MaintenanceUsers parameter in the sshd_config configuration file. If the InstallCyberArkSSHD parameter is set to Yes or No, do the following: Create an additional administrator user in addition to the built-in root user so that the administrator user can always connect to the PSM SSH server to perform maintenance, even if remote access is disabled for the root user. You can configure more administrator user names by adding PSMP_MaintenanceUsers the sshd_config configuration file. As service users, only local users can connect. In /etc/ssh, open sshd_config file for editing. Add the following parameter to the file: PSMP_MaintenanceUsers <username>,<username> you can specify specific user names at the beginning and/or end of the user name string or use *. In this example, the following administrator users are enabled: user1, all users that end user2, all users that start with user3, and all users that contain user4. PSMP_MaintenanceUsers <user1><*user2>, , Save changes and close <user3*><*user4*> sshd_config configuration file. Restart the sshd service to take these changes to take an impact: As part of hardening the PSM SSH server and security best practices, after you install PSM SSH, the root user cannot authenticate the PSM SSH server remotely by using a password. If the administrative user is not created in advance for maintenance purposes, custody is only possible through the console or when the root user authenticates with an SSH key. Here are some administrative tasks for PSMP servers. /etc/init.d/psmpsrv {start|stop|restart|status} [{psmp|psmpadb}] By default, only the root user can log in from the console. Other users start the PSMP service to log on to a remote server using </*user4*> </user3*> </*user2> </user1> </username> </username> </proxyaddress> </administrative> </ssh> </ssh> as shown in the following screenshot. Here are the simple steps that allow the new user to log on to the PSMP server remotely to perform a management work.1 In /etc/ssh directory, open the sshd_config to edit the configuration file. 2 Add the following parameter to the file: PSMP_MaintenanceUsers <username>,<username> This example allows the following admins: user1, all users who end user2, all users that start with user3 and all users that contain user4. PSMP_MaintenanceUsers <user1>, , 3 Save changes and close the sshd_config<*user2><user3*><*user4*> configuration file. 4 Create a new user and set it to the wheel group 5 Restart the sshd service to affect these changes: /etc/init.d/sshd restart 5 After you log on to root1, Sudo -i go root account. Note: PSMPAPP_ account authentication error and PSMP disconnect [ conf]# vi /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/CAR Kpsmp/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 We need to reset the psmpappuser.cred file and vault psmpapp_psmp password. C:\CyberArk\Password Vault Web Access\Env>CreateCredFile.exe psmpappuser.cred Vault Username [mandatory] ==> PSMPAPP_psmp Vault Password (encrypted in credential file) ==> ********* Disable wait for DR synchronization before changing password (yes/no) [No] == > External Authentication Facility (LDAP/ Radius/No) [No] ==> Restrict application type [optional] ==> Restrict to executable trajectory [optional] ==> Restrict current machine IP (yes/no) [No] ==> Restrict current machine hostname (yes/no) [No] ==> Restrict OS user name [optional] ==> Show restrictions in output file (yes/no)) [Nr] ==> Use operating system protected memory credential file secret (Machine /User /No) [No] ==> Command successfully completed C:\CyberArk\Password Vault Web Access\Env>CreateCredFile.exe psmpgwuser.cred Vault Username [mandatory] ==> PSMPGW_psmp Vault Password (encrypted cred cred file) ==> Disable DR synchronization before changing the password (yes/no) [No] == > External Authentication Facility (LDAP/Radius/No) [No] ==> Restrict Application Type [optional] == > Restrict executable path [optional] == > Restrict current machine IP (yes/no) [No] = > Restrict current hostname (yes/no) [No] ==> Restrict user name to OS [optional] </user3*> </*user2> </user1> </username> </username> </username> Restrictions on the output file (yes/no) [No] ==> Use operating system protected memory credential file secret (Machine /User /No) [No] == > command ended successfully in C:\CyberArk\Password Vault Web Access\Env> WINSCP download these two files to psmp server to replace them / etc /opt/CARKpsmp / PSMP_ADB_psmp There are two related errors in the PrivateARK console Server: ITATS528E authentication error user PSMP_ADB_psmp from station ITATS433E IP address 192.168.2.27 is suspended PSMP_ADB_psmp [] conf]# cat /etc/opt/CARKpsmpadb/conf/basic_psmpadbridge.conf [Main] AppProviderParmsSafe=PSMPADBridgeConf AppProviderVaultParmsFolder=Root AppProviderVault ParmsFile=main_psmpadbridge.conf.linux.11.04 AppProviderVaultFile=/etc/opt/CARKpsmp/vault/vault.ini AppProviderCredFile=/etc/OPT/CARKpsmpadb/vault/psmpadbridgeserveruser.cred LogsFolder=var/opt/CARKpsmpadb/logs LocalParmsFileFolder=/var/opt/CARKpsmpadb TempFolder=/var/opt/CARKpsmpadb/tmp AdvancedFIPSCryptography=No PIMConfigurationSafe=PVWAConfig PIMConfigurationFolder=Root PIMPVConfigurationFileName=PVConfiguration.xml PIMPoliciesConfigurationFileName=Policies.xml Activate user PSMP_ADB_psmp and update this password. C:\CyberArk\Password Vault Web Access\Env>CreateCredFile.exe psmpadbridgeserveru ser.cred Vault Username [Mandatory] ==> PSMP_ADB_psmp Vault Password (encrypted in credential file) ==> ********* Disable wait for DR synchronization before allowing password change (yes/no) [No] ==> External Authentication Facility (LDAP/Radius/No) [No] == > Restrict application type [optional] == > Restricted run path [optional] ==> Restrict current machine IP (yes/no) [No] ==> Restrict current machine host name (yes/no) [No] ==> Restrict OS to username [optional] ==> Show restrictions in output file (yes/no) [No] ==> Use the operating system protected memory credential file secret (Machine /User /No) [No] ==> command ended successfully [ vault]# cp /home/root1/psmpadbridgeserveruser.cred . cp: write './psmpadbridgeserveruser.cred'? y [ vault]# /etc/init.d/psmpsrv restart PSM SSH proxy.... The PSM SSH proxy server was successfully stopped. Starting PSM SSH Proxy... The PSM SSH proxy server was successfully started. PSMP ADBridge has already been suspended. Starting Psmp ADBridge... PSMP ADBridge was successfully launched. [ vault]# It can also be used as a registration tool to write in a created environment in the vault: 20INST/PSMP_EnivromentManager.htm It is recommended to change the default PSMAppUser and PSMPGWUser parameter values to unique values to avoid overwriting previous installation. /opt/CARKpsmp/bin/envmanager CreateEnv -AcceptEULA Y -CredFile /tmp/user.cred -PSMPAppUser PSMPAppUser_PSMP1 -PSMPGWUser PSMPGWUser _PSMP1 _PSMP1