PAM-SEN

[Total Questions: 136]

Question #:1

What authentication methods can be implemented to enforce Two-Factor Authentication (2FA) for users authenticating to CyberArk using both the PVWA (through the browser) and the PrivateArk Client?

A. LDAP and RADIUS Most Voted

B. CyberArk and RADIUS

C. SAML and Cyber Ark

D. SAML and RADIUS

Answer: A

Question #:2

The connect button requires PSM to work.

A. TRUE

B. FALSE

Answer: B

https://community.cyberark.com/s/article/00003654

Question #:3

There is a requirement for a password to change between 01:00 and 03:00 on Saturdays and Sundays; however, this does not work consistently.

Which platform setting may be the cause?

Interval è il numero di minuti che il CPM attende prima di cambiare la password

A. The Interval setting for the platform is incorrect and must be less than 120.

B. The ImmediateInterval setting for the platform is incorrect and must be greater than or equal to 1.

C. The DaysToRun setting for the platform is incorrect and must be set to Sat,Sun.

HeadStartInterval è il numero di giorni che il CPM aspetta prima di iniziare il cambio password

D. The HeadStartInterval setting for the platform is incorrect and must be set to 0.

Answer: A D

https://docs.cyberark.com/pam-self-hosted/13.2/en/Content/PASREF/Automatic%20Password%20Management%20-%20General.htm?tocpath=Administrator%7CReferences%7CConfigure%20the%20system%20through%20PVWA%7CPlatform%20properties%7CAutomatic%20Password%20Management%7C_____1#:~:text=value%3A%205-,Interval,-The%20number%20of

https://community.cyberark.com/s/question/0D52J00006wrplgSAA/what-is-the-reasoning-behind-the-headstartinterval

Question #:4

By default, the vault secure protocol uses which IP port and protocol.

A. TCP/1858 Protocollo utilizzato per sicurezza il tcp, cyberark è proprietario della porta 1858

B. TCP/443

C. UDP/1858

D. TCP/80

Answer: A

Question #:5

You are installing multiple PVWAs behind a load balancer.

Which statement is correct?

A. Port 1858 must be opened between the load balancer and the PVWAs.

B. The load balancer must be configured in DNS round robin.

C. The load balancer must support "sticky sessions". Le sticky sessions (o session stickiness) in un load balancer si riferiscono a una tecnica in cui le richieste successive provenienti dallo stesso client vengono sempre indirizzate allo stesso server, anziché essere distribuite a un qualsiasi server disponib

D. The LoadBalancerClientAddressHeader parameter in the PVWA.ini file must be set.

Answer: C https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PAS%20INST/PVWA-install-multiple-PVWA-env.htm?TocPath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C_____8

Question #:6

A vault admin received an email notification that a password verification process has failed Which service sent the message?

A. The PrivateArk Server Service on the Vault.

B. The CyberArk Password Manager service on the Components Server.

C. The CyberArk Event Notification Engine Service on the Vault

D. The CyberArk Privileged Session Manager service on the Vault.

Answer: C https://www.reddit.com/r/CyberARk/comments/67mzwo/ene_notifications/

Question #:7

A customer's environment has three data centers consisting of 5,000 servers in Germany, 10,000 servers in Canada, and 1,500 servers in Singapore. You want to manage target servers and avoid complex firewall rules. How many CPMs should you deploy?

A. 1

B. 3 total, 1 per data center

C. 15

D. 6 total, 2 per data center

Answer: B

Question #:8

What is a prerequisite step before CyberArk can be configured to support RADIUS authentication?

A. Log on to the PrivateArk Client, display the User properties of the user to configure, run the Authentication method drop-down list, and select RADIUS authentication.

B. In the RADIUS server, define the CyberArk Vault as a RADIUS client/agent. Most Voted

C. In the Vault installation folder, run CAVaultManager as administrator with the SecureSecretFiles command.

D. Navigate to /Server/Conf and open DBParm.ini and set the RadiusServersInfo parameter.

Answer: B https://docs.cyberark.com/PAS/13.2/en/Content/PAS%20INST/RADIUS-Authentication.htm?tocpath=Administrator%7CUser%20Management%7CAuthenticate%20to%20Privileged%20Access%20Manager%20-%20Self-Hosted%7CConfigure%20authentication%20methods%7C_____4#:~:text=to%20255%20characters.-,Configure%20RADIUS%20Authentication,-To%20configure%20the

Question #:9

When performing “In Domain” hardening of a PSM server, which steps must be performed? (Choose two.)

A. Import CyberArk policy settings from the provided file into a new GPO. Most Voted

B. Apply advanced audit on the PSM server.

C. Link GPO to a dedicated OU containing CyberArk PSM servers. Most Voted

D. Import an INF file to the local machine.

E. Configure AppLocker rules to block running unknown executables.

Answer: A C

Question #:10

Does CyberArk need service accounts on each server to change passwords?

A. Yes. it requires a domain administrator account to change any password on any server.

B. Yes. it requires a local administrator account on any Windows server and a root level account on any Unix server.

C. No. passwords are changed by the Password Provider Agent.

D. No. the CPM uses the account information stored in the vault to login and change the account's password using its own credentials

Answer: B

Question #:11

What is a valid combination of primary and secondary layers of authentication to a company's two-factor authentication policy?

A. RSA SecurID Authentication (in PVWA) and LDAP Authentication

B. CyberArk Authentication and RADIUS Authentication

C. Oracle SSO (in PVWA) and SAML Authentication

D. LDAP Authentication and RADIUS Authentication

Answer: A https://docs.cyberark.com/pam-self-hosted/12.1/en/Content/PAS%20INST/Authenticating-to-the-Privileged-Account-Security-Solution.htm#Secondaryauthentication

Question #:12

In addition to bit rate and estimated total duration of recordings per day, what is needed to determine the amount of storage required for PSM recordings?

A. retention period

B. number of PSMs

C. number of users

D. number of targets

Answer: A

Question #:13

Which browser is supported for PSM Web Connectors developed using the CyberArk Plugin Generator Utility (PGU)?

A. Internet Explorer

B. Google Chrome

C. Opera

D. Firefox

Answer: B https://docs.cyberark.com/pam-self-hosted/14.2/en/Content/PASIMP/psm_WebApplication.htm

Question #:14

The PrivateArk clients allows a user to view the contents of the vault like a filesystem.

A. TRUE

B. FALSE

Answer: A

Question #:15

A customer has three data centers distributed globally and wants highly-available PSM connections in each segmented zone. In addition, the customer needs a highly-available PSM connection for the CyberArk Admins.

What will best satisfy this customer's needs?

A. one PSM per zone with a load balancer and two PSMs for Admins with a load balancer

B. six PSMs in the mam data center with a load balancer and one PSM for Admins

C. two PSMs per zone with a load balancer and two PSMs for Admins with a dedicated load balancer

D. three PSMs per zone with CyberArk built-in load balancing

Answer: C

Question #:16

Which file would you modify to configure the vault to send SNMP traps to your monitoring solution?

A. dbparm ini

B. paragent.ini

C. ENEConf.ini I

D. padr ini

Answer: B https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASREF/Remote%20Control%20Agent%20Parameter%20File.htm#:~:text=Remote%20Control%20Agent%20Parameter%20File.%20The%20Remote%20Control

Question #:17

Which file would you modify to configure your Vault Server to forward Activity Logs to a SIEM or SYSLOG server?

A. dbparm.ini

B. PARagent.ini

C. ENEConf.ini

D. padr.ini

Answer: C

Question #:18

What are the basic network requirements to deploy a CPM server?

A. Port 1858 to Vault and Port 443 to PVWA

B. Port 1858 only

C. all ports to the Vault

D. Port UDP/1858 to Vault and all required ports to targets and Port 389 to the PSM

Answer: A

Question #:19

The primary purpose of the CPM is Password Management.

A. TRUE

B. FALSE

Answer: A

Question #:20

After installing the Vault, you need to allow Firewall Access for Windows Time service to sync with NTP servers 10.1.1.1 and 10.2.2.2.

What should you do?

A. Edit DBParm.ini to add: AllowNonStandardFWAddresses=[10.1.1.1,10.2.2.2],Yes,123:outbound/udp. Most Voted

B. Edit DBParm.ini to add: NTPServer=[10.1.1.1:123/UDP,10.2.2.2:123/UDP].

C. Edit DBParm.ini to add: AllowNonStandardFWAddresses=[10.1.1.1,10.2.2.2],Yes,123:outbound/udp,123:inbound/udp.

D. Edit the Windows Firewall configuration to add a rule for Port 123/udp outbound to 10.1.1.1 and 10.2.2.2.

Answer: D https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/following-vault-Installation.htm#ConfiguretimesynchronizationontheVaultServerusingNTP

Question #:21

When a DR vault server becomes an active vault, it will automatically fail back to the original state once the primary vault comes back online.

A. True, this is the default behavior

B. False, this is not possible

C. True, if the 'AllowFailback' setting is set to yes in the PADR.ini file.

D. True if the 'AllowFailback' setting is set to yes in the dbparm mi file

Answer: C

Question #:22

What is a requirement for setting fault tolerance for PSMs?

A. Use a load balancer

B. Use a backup solution

C. CPM must be in all data centers

D. Install the Vault in an HA cluster

Answer: C https://cyberark-customers.force.com/s/question/0D52J00007R7zixSAB/how-fault-tolerant-is-cyberark-if-tdc-blew-up-for-example

Question #:23

You are installing a CPM.

In addition to Add Safes, Add/Update Users, Reset Users' Passwords and Manage Server File Categories,

which Vault authorization(s) does a CyberArk user need to install the CPM?

A. Manage Directory Mapping

B. Activate Users

C. Backup All Safes, Restore All Safes

D. Audit Users, Add Network Areas

Answer: B https://docs.cyberark.com/pam-self-hosted/14.2/en/Content/PAS%20INST/CPM-install-requirements.htm

Question #:24

To enable LDAP over SSL for a Vault when DNS lookups are blocked, which step must be completed?

A. Add the FQDN & IP details for each LDAP host into the local hosts file of the Vault server. Most Voted

B. Configure an AllowNonStandardFWAddresses rule in DBParm.ini on the Vault to allow outbound TCP 53 to the organization's DNS servers.

C. Ensure LDAP hosts added to the directory mapping configuration are defined using only IP addresses.

D. Set the ReferralsDNSLookup parameter value to "No" in the directory configuration.

Answer: A

Question #:25

Which parameter must be provided when registering a primary Vault in Azure, but not in Amazon Web Services?

A. /RecPub

B. /AdminPass

C. /MasterPass

D. /RDPGateway

Answer: D https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PAS%20Cloud/Azure-Manual-PrimaryVault.htm

Question #:26

Which of the following protocols need to be installed on a standalone vault server? Check all that apply.

A. Client for Microsoft Networks

B. QoS Packet Scheduler

C. File and Printer Sharing for Microsoft Networks

D. Internet Protocol version 4 (TCP/IPv4)

E. NIC Teaming Driver, if applicable

Answer: A B C D

Question #:27

Which components can connect to a satellite Vault in a distributed Vault architecture?

A. CPM, EPM, PTA

B. PVWA, PSM

C. CPM, PVWA, PSM

D. CPM, PSM

Answer: B

Question #:28

Which component must be installed before the first CPM installation?

A. PTA vault->PVWA->CPM->psm->Ptm

B. PSM

C. PVWA

D. EPM

Answer: A

Question #:29

What would be a good use case for the Replicate module?

A. Recovery Time Objectives or Recovery Point Objectives are at or near zero

B. Integration with an Enterprise Backup Solution is required.

C. Off site replication is required.

D. PSM is used

Answer: C

Question #:30

Which CyberArk component changes passwords on Target Devices?

A. Vault

B. CPM

C. PVWA

D. PSM

E. PrivateArk

F. OPM

G. AIM

Answer: B C D

Question #:31

HTML5 Gateway can be installed on which supported UNIX OS versions? (Choose two.)

A. Red Hat Enterprise Linux 7.x

B. CentOS 7.x

C. Ubuntu 20.x

D. AK 7.x

E. Android 11.x

Answer: A B

Question #:32

Which is the correct order of installation for PAS components?

A. Vault, CPM. PVWA, PSM

B. CPM, Vault. PSM, PVWA

C. Vault, CPM. PSM, PVWA

D. PVWA, Vault, CPM, PSM

Answer: A

Question #:33

You are installing the HTML5 gateway on a Linux host using the RPM provided.

After installing the Tomcat webapp, what is the next step in the installation process?

A. Deploy the HTML5 service (guacd). Most Voted

B. Secure the connection between the guacd and the webapp.

C. Secure the webapp and JWT validation endpoint.

D. Configure ASLR.

Answer: B https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Install_PSM_HTML5_RPM.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PSM%7CAdvanced%20PSM%20Implementations%7CInstall%20PSM%20HTML5%20Gateway%7C_____2#:~:text=java%2Ddevel%20openssl-,Install%20the%20HTML5%20Gateway,-This%20section%20describes

Question #:34

In which configuration file do you add LoadBalancerClientAddressHeader when you enable x-forwarding on the PVWA loadbalancer?

A. PVconfiguration.xml

B. web.config

C. apigw.ini

D. CyberArkScheduledTasks.exe.config

Answer: B https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PAS%20INST/PVWA-install-multiple-PVWA-env.htm?tocpath=Installation%7CInstall%20PAM%20-%20Self-Hosted%7CInstall%20PVWA%7C_____8#ConfigurethePVWAtoworkwiththeloadbalancer

Question #:35

Your customer wants to store the Safes Data on Vault Drive D instead of Drive C.

Which file should you edit?

A. TSparm.ini Most Voted

B. Vault.ini

C. DBparm.ini

D. user.ini

Answer: A

Question #:36

What is a prerequisite step before installing the Vault on Windows 2019?

A. Configure the Kerberos authentication method on the default IIS Application pool

B. Check that the server IP address is correctly configured and that it is static

C. In the Network Connection properties, configure Preferred DNS Servers

D. Install Microsoft Windows patch KB4014998

Answer: B

Question #:37

After a PSM session is complete, the PSM server uploads the recording to the Vault for long-term storage.

A. TRUE

B. FALSE

Answer: A

Question #:38

In a SIEM integration it is possible to use the fully-qualified domain name (FQDN) when specifying the SIEM server address(es)

A. TRUE Possibile ma non raccomandabile

B. FALSE

Answer: A

Question #:39

CyberArk User Neil is trying to connect to the Target Linux server 192.168.1.164 using a domain account ACME/linuxuser01 on domain acme.corp using PSM for SSH server 192.168.65.145.

What is the correct syntax?

A. ssh neil@linuxuser01:acme.corp@192.168.1.164@192.168.65.145

B. ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145 Most Voted

C. ssh neil@linuxuser01@192.168.1.164@192.168.65.145

D. ssh neil@linuxuser01@acme.corp@192.168.1.164@192.168.65.145

Answer: B

Question #:40

What would be a good use case for a High Availability vault?

A. Recovery Time Objectives or Recovery Point Objectives are at or near zero.

B. Integration with an Enterprise Backup Solution is required.

C. Off site replication is required

D. PSM is used.

Answer: A

Question #:41

During the PSM installation process, Safes and a User are created.

In addition to Add Safes, Add/Update Users, Reset Users' Passwords, and Activate Users, which authorization(s) does the Vault user installing the PSM need to enable them to be successfully created?

A. Manage Vault File Categories Most Voted

B. Manage Server File Categories

C. Manage Directory Mapping, Manage Server File Categories

D. Manage Directory Mapping, Manage Vault File Categories

Answer: A https://docs.cyberark.com/PAS/Latest/en/Content/PAS%20INST/Before-Installing-PSM.htm

Question #:42

Which keys are required to be present in order to start the PrivateArk Server Service? Select all that apply.

A. Server Key

B. Recovery Public Key

C. Recovery Private Key

D. Safe Key

Answer: A

Question #:43

The account used to install a PVWA must have ownership of which safes? (Choose two.)

A. VaultInternal

B. PVWAConfig

C. System

D. Notification Engine

E. PVWAReports

Answer: A D

Question #:44

Which step is required to register a Vault manually in Amazon Web Services using CAVaultManager?

A. Specify Amazon as the cloud vendor using the /CloudVendor Flag

B. After running the postinstall utility, restart the "PrivateArk Server" service

C. Specify the Cloud region using the /CloudRegion flag

D. Specify whether the Vault is distributed or stand alone

Answer: C

Question #:45

A customer wants to store PSM recordings for 100 days and estimates they will have 10 Windows sessions per day for 100 minutes each.

What is the minimum storage required for the Vault and PAReplicate for the PSM recordings?

A. 25 GB Most Voted

B. 250 GB

C. 500 GB

D. 5 GB

Recording 250KB/Min
And exp
1Day -> 10*100= 1000Min/Day
100Days - > 1000*100= 100000 Min
1MB = 1000KB
1GB = 1000MB= 1000*1000KB= 1000000KB
1KB = 1/1000000 GB
Total GB = 100000*250/1000000= 25GB

Answer: B

Question #:46

The RemoteApp feature of PSM allows seamless Application windows (i e the Desktop of the PSM server will not be visible)

A. TRUE

B. FALSE

Answer: A

Question #:47

For redundancy, you want to add a secondary RADIUS server.

What must you do to accomplish this?

A. Add to the application settings of the PVWA web.config file.

B. In the PVWA vault.ini file, list each RADIUS server host address in the "Addresses" attribute separated by commas.

C. Open the DBParm.ini on the Vault server. Add the second RADIUS server configuration settings after the first one, separated by a comma. Most Voted

D. In the PVWA web.config file, add the location element at the end of the config file. Set the path value to "Default Web Site/PasswordVault/api/auth/pkipn/logon".

Answer: C

Question #:48

You have been asked to limit a platform called “Windows_Servers” to safes called “WindowsDC1” and “WindowsDC2”. The platform must not be assigned to any other safe.

What is the correct way to accomplish this?

A. Edit the "Windows_Servers" platform, expand "Automatic Password Management", then select General and modify "AllowedSafes" to be (WindowsDC1)|(WindowsDC2).

B. Edit the "Windows_Servers" platform, expand "Automatic Password Management", then select Options and modify "AllowedSafes" to be (Win*).

C. Edit the "WindowsDC1" and "WindowsDC2" safes through Safe Management, Add "Windows_Servers" to the "AllowedPlatforms".

D. Log in to PrivateArk using an Administrative user, Select File, Server File Categories, Locate the category "WindowsServersAllowedSafes" and specify "WindowsDC1,WindowsDC2".

Answer: A

Question #:49

A stand alone Vault server requires DNS services to operate properly.

A. TRUE

B. FALSE

Answer: B

Question #:50

Which SMTP address can be set on the Notification Settings page to re-invoke the ENE setup wizard after the initial Vault installation?

A. 255.255.255.255

B. 8.8.8.8

C. 192.168.1.1

D. 1.1.1.1

Answer: D

Question #:51

As a member of a PAM Level-2 support team, you are troubleshooting an issue related to load balancing four PVWA servers at two data centers. You received a note from your Level-1 support team stating "When testing PVWA website from a workstation, we noticed that the "Source IP of last sign-in" was shown as the VIP (Virtual IP address) assigned to the four PVWA servers instead of the workstation IP where the PVWA site was launched from."

Which step should you take?

A. Verify the "LoadBalancerClientAddressHeader" parameter setting in PVWA configuration file Web.config is set to "X-Forwarded-For".

B. Add the VIP (Virtual IP address) assigned to the four PVWA servers to the certificates issued for all four PVWA servers, if missing.

C. Add a firewall rule to allow the testing workstation to connect to the VIP (Virtual IP address) assigned to the four PVWA servers on Port TCP 443.

D. Edit the dbparm.ini file on the Vault server and add the IP or subnet of the workstation to the whitelist.

Answer: A

Question #:52

Which statement is correct about CPM behavior in a distributed Vault environment?

A. CPMs should only access the primary Vault. When it is unavailable, CPM cannot access any Vault until another Vault is promoted as the new primary Vault.

B. CPMs should access only the satellite Vaults.

C. CPMs should only access the primary Vault. When it is unavailable, CPM cannot access any Vault until the original primary Vault is operational again.

D. CPM should access all Vaults - primary and the satellite.

Answer: A

Question #:53

A customer has five main data centers with one PVWA in each center under different URLs.

How can you make this setup fault tolerant?

A. This setup is already fault tolerant.

B. Install more PVWAs in each data center.

C. Continuously monitor PVWA status and send users the link to another PVWA if issues are encountered.

D. Load balance all PVWAs under same URL.

Answer: D

Question #:54

You are configuring SNMP remote monitoring for your organization's Vault servers.

In the PARAgent.ini, which parameter specifies the destination of the Vault SNMP traps?

A. SNMPHostIP Most Voted

B. SNMPTrapPort

C. SNMPCommunity

D. SNMPVersion

Answer: A

Question #:55

In an SMTP integration it is possible to use the fully-qualified domain name (FQDN) when specifying the SMTP server address(es)

A. TRUE

B. FALSE

Answer: B

Question #:56

You are beginning the post-install process after a manual PSM installation is completed.

What must you do?

A. Disable screen saver for the PSM local users.

B. Create a new group called PSMShadowUsers.

C. Reset the PSMAdminConnect user password.

D. Enable load balancing on the PSM server.

Answer: A

Question #:57

What is the default username for the PSM for SSH maintenance user when InstallCyberarkSSHD is set to yes?

A. proxymng

B. psmp_maintenance

C. psmpmaintenanceuser

D. psmpmnguser

Answer: A

Question #:58

How should you configure PSM for SSH to support load balancing?

A. by using a network load balancer Most Voted

B. in PVWA > Options > PSM for SSH Proxy > Servers

C. in PVWA > Options > PSM for SSH Proxy > Servers > VIP

D. by editing sshd.config on the all the PSM for SSH servers

Answer: C

Question #:59

Before the hardening process, your customer identified a PSM Universal Connector executable that will be required to run on the PSM.

Which file should you update to allow this to run?

A. PSMConfigureAppLocker.xml

B. PSMHardening.xml

C. PSMAppConfig.xml

D. PSMConfigureHardening.xml

Answer: A

Question #:60

In order to avoid conflicts with the hardening process, third party applications like Antivirus and Backup Agents should be installed on the Vault server before installing the Vault.

A. TRUE

B. FALSE

Answer: B

Question #:61

What is the purpose of the PSM health check hardening?

A. Remove IIS settings which can be considered security vulnerabilities.

B. Validate that the PSM is ready to be placed behind a load balancer.

C. Confirm that the Windows Services for PSM are running on the server.

D. Ensure that the AppLocker script does not have any syntax errors.

Answer: A

Question #:62

As Vault Admin, you have been asked to enable your organization's CyberArk users to authenticate using LDAP.

In addition to Audit Users, which permission do you need to complete this task?

A. Add Network Areas

B. Manage Directory Mapping

C. Add/Update Users

D. Activate Users

Answer: B

Question #:63

What is the name of the account used to establish the initial RDP session from the end user client machine to the PSM server?

A. PSMConnect

B. PSMAdminConnect

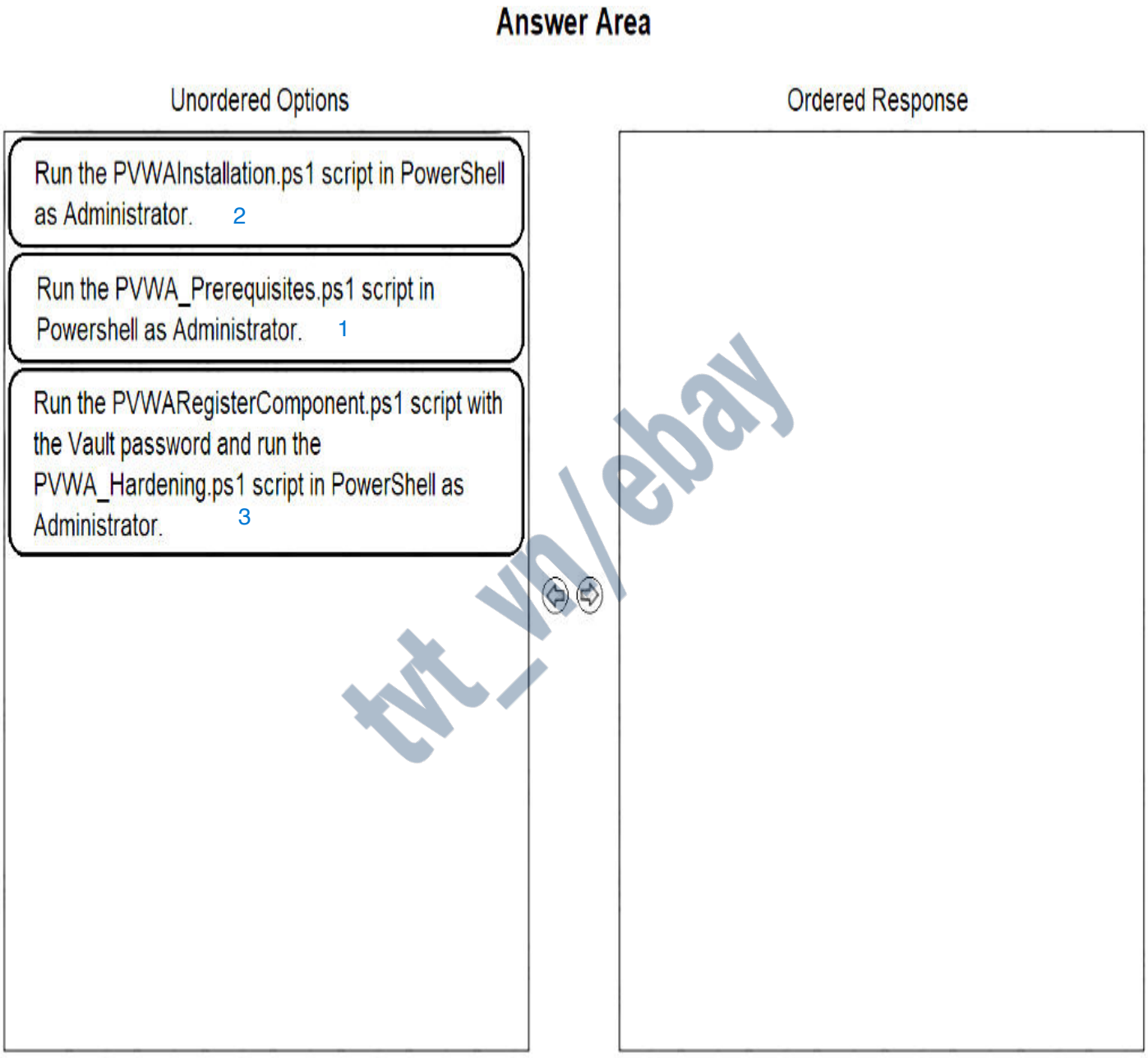
C. PSM

D. The credentials the end user retrieved from the vault

Answer: A

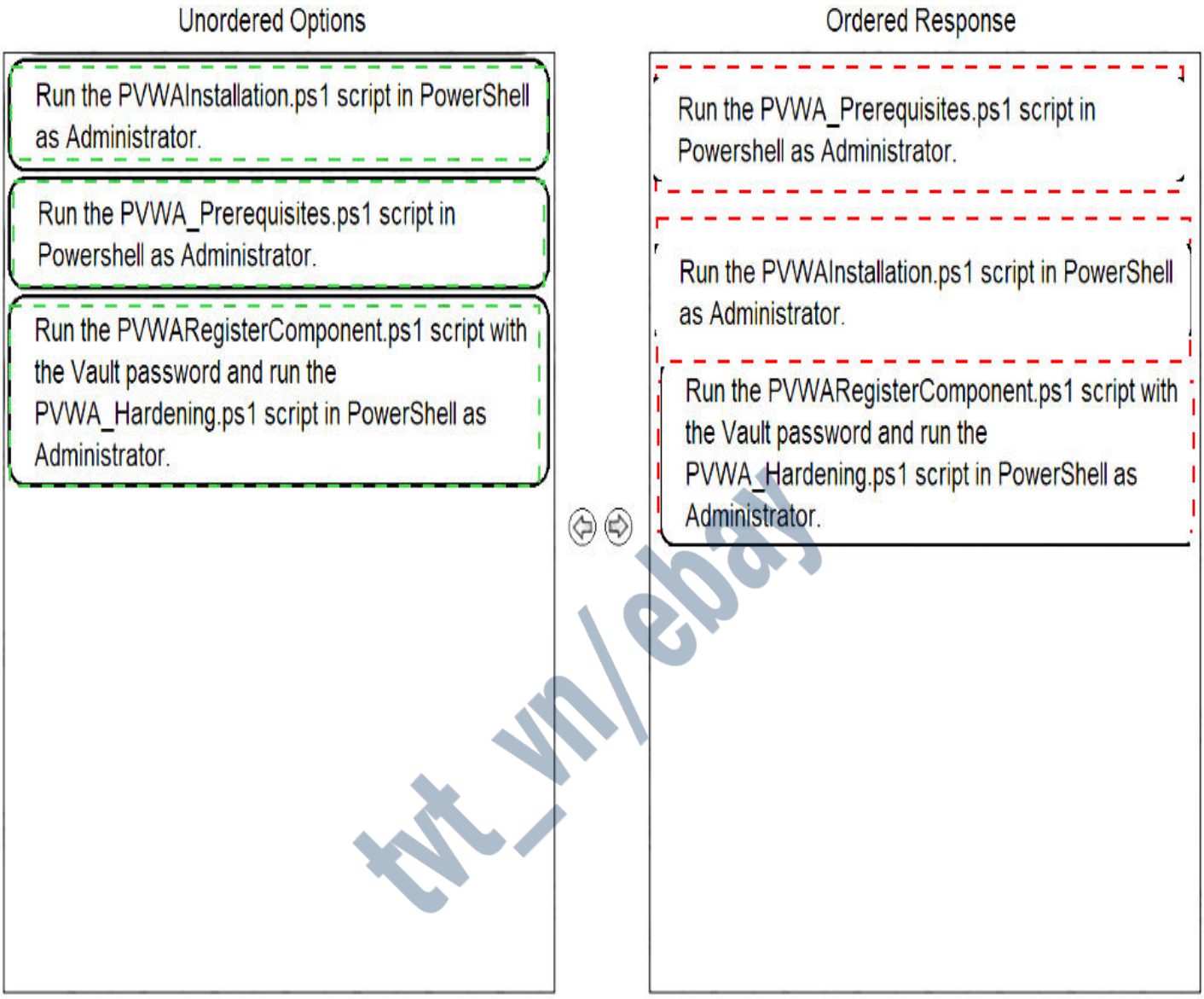
Question #:64

Arrange the steps to install the Password Vault Web Access (PVWA) in the correct sequence.



Answer:

Answer Area



Ordered Response

Run the PVWA_Prerequisites.ps1 script in Powershell as Administrator.
Run the PVWAInstallation.ps1 script in PowerShell as Administrator.
Run the PVWARegisterComponent.ps1 script with the Vault password and run the PVWA_Hardening.ps1 script in PowerShell as Administrator.

Suggested Answer: The steps needed to install the Password Vault Web Access (PVWA) should be completed in the following order: PVWA_Prerequisites.ps1, PVWAInstallation.ps1, and PVWARegisterComponent.ps1 with the Vault password followed by PVWA_Hardening.ps1. This will ensure that all prerequisites are met before attempting to install and configure PVWA properly. By ensuring these steps are taken in this specific order, it allows for a successful installation of the software on the desired machine or server. After taking these necessary steps in sequence, users can then enjoy their newly installed Password Vault Web Access.

Question #:65

Which statements are correct about the PSM HTML5 gateway? (Choose two.)

A. Smart card redirection is supported
B. It does not support connections to target system where NLA is enabled on the PSM server
C. SSH sessions cannot be established
D. Printer redirection cannot be enabled
E. It does not support session recording capabilities for applications that run outside a web browser

Answer: B D

Question #:66

A customer asked you to help scope the company's PSM deployment.

What should be included in the scoping conversation?

A. Recordings file path
B. Recordings codec
C. Recordings retention period

D. Recordings file type

Answer: C

Question #:67

What is required before the first CPM can be installed?

A. The environment must have at least one Vault and one PVWA installed.

B. The Vault environment must have at least one account stored in a safe.

C. Custom platforms must be downloaded from the CyberArk Marketplace.

D. The PSM component must be installed and proper functionality validated.

Answer: A

Question #:68

What must you do to prepare a Windows server for PVWA installation?

A. In the InstallationAutomation folder, run the PVWA_Prerequisites.ps1 file as an administrator in Powershell. Most Voted

B. Install the PrivateArk client.

C. Verify the user performing the installation is Domain Administrator and has logon access to the Vault server.

D. Enable IPv6.

Answer: A

Question #:69

Which command should be executed to harden a Vault after registering it to Azure?

A. HardenAzureFW.ps1 Most Voted

B. ExecuteStage ./Hardening/HardeningConf.xml

C. HardenVaultFW.ps1

D. ExecuteStage ./PostInstallation/PostInstallation.xml

Answer: C

Question #:70

When creating a distributed Vault environment architecture, what is the maximum number of Vault servers that can be deployed?

A. 5 - number of primary and satellite Vaults can be specified during installation

B. 3 - all primary

C. 6 - 1 primary and 5 satellite

D. 10 - 2 primary and 8 satellite

Answer: C

Question #:71

Which components support load balancing? (Choose two.)

A. CPM

B. PVWA

C. PSM

D. PTA

E. EPV

Answer: B C

Question #:72

You are setting up a Linux host to act as an HTML 5 gateway for PSM sessions.

Which servers need to be trusted by the Linux host to secure communications through the gateway?

A. PSM and PVWA

B. PSM and CPM

C. PVWA and Vault

D. Vault and PSM

Answer: A

Question #:73

In large-scale environments, it is important to enable the CPM to focus its search operations on specific Safes instead of scanning all Safes it sees in the Vault.

How is this accomplished?

A. Administration Options > CPM Settings

B. AllowedSafe Parameter on each platform policy

C. MaxConcurrentConnection parameter on each platform policy

D. Administration > Options > CPM Scanner

Answer: B

Question #:74

What is the purpose of the CPM_Preinstallation.ps1 script included with the CPM installation package?

A. It prompts for input parameters that will be used to pre-populate form fields in the installation wizard.

B. It automatically installs the CPM, requiring no additional user input.

C. It allows you to install the CPM using a command line approach rather than using the installation wizard.

D. It verifies the NET version installed on the server and sets the IIS SSL TLS server configuration.

Answer: D

Question #:75

Which user is enabled when replicating data between active and stand-by Vaults?

A. DR

B. Backup

C. Operator

D. Auditor

Answer: A

Question #:76

What is the purpose of the password Reconcile process?

A. To test that CyberArk is storing accurate credentials for accounts.

B. To change the password of an account according to organizationally defined password rules

C. To allow CyberArk to manage unknown or lost credentials.

D. To generate a new complex password.

Answer: B

Question #:77

What is the recommended method to determine if a PVWA is unavailable and should be disabled in a load balancing pool?

A. Monitor Port 443 on the PVWA server

B. Monitor Port 1858 on the PVWA server

C. Ping the PVWA server

D. Monitor Port 3389 on the PVWA server

Answer: B

Question #:78

Which of the following are prerequisites for installing PVWA Check all that Apply.

A. Web Services Role

B. NET 4.5.1 Framework Feature

C. Remote Desktop Services Role

D. Windows BitLocker

Answer: A

Question #:79

Which component should be installed on the Vault if Distributed Vaults are used with PSM?

A. RabbitMQ

B. Disaster Recovery

C. Remote Control Client

D. Distributed Vault Server

Answer: A

Question #:80

At what point is a transparent user provisioned in the vault?

A. When a directory mapping matching that user id is created.

B. When a vault admin runs LDAP configuration wizard.

C. The first time the user logs in.

D. During the vault's nightly LDI^P refresh

Answer: A

Question #:81

You are designing the number of PVWAs a customer must deploy. The customer has three data centers with a distributed Vault in each, requires high availability, and wants to use all Vaults at all times.

How many PVWAs does the customer need?

A. six or more

B. four

C. two or less

D. three

Answer: A

Question #:82

Which method can be used to directly authenticate users to PSM for SSH? (Choose three.)

A. CyberArk authentication Most Voted

B. LDAP authentication Most Voted

C. RADIUS authentication Most Voted

D. Windows authentication

E. SAML authentication

F. OpenID Connect (OIDC) authentication

Answer: A B C

Question #:83

A customer has two data centers and requires a single PVWA url.

Which deployment provides the fastest time to reach the PVWA and the most redundancy?

A. Deploy two PVWAs behind a global traffic manager.

B. Deploy one PVWA only.

C. Deploy two PVWAs in an active/standby mode.

D. Deploy two PVWAs using DNS round robin.

Answer: A

Question #:84

After installing the first PSM server and before installing additional PSM servers, you must ensure the user performing the installation is not a direct owner of which safe?

A. PSMUnmanagedSessionAccounts Safe

B. PSMRecordingsSessionAccounts Safe

C. PSMUnmanagedApplicationAccounts Safe

D. PSMSessionBackupAccounts Safe

Answer: A

Question #:85

To apply a new license file you must:

A. Upload the license.xml file to the System Safe

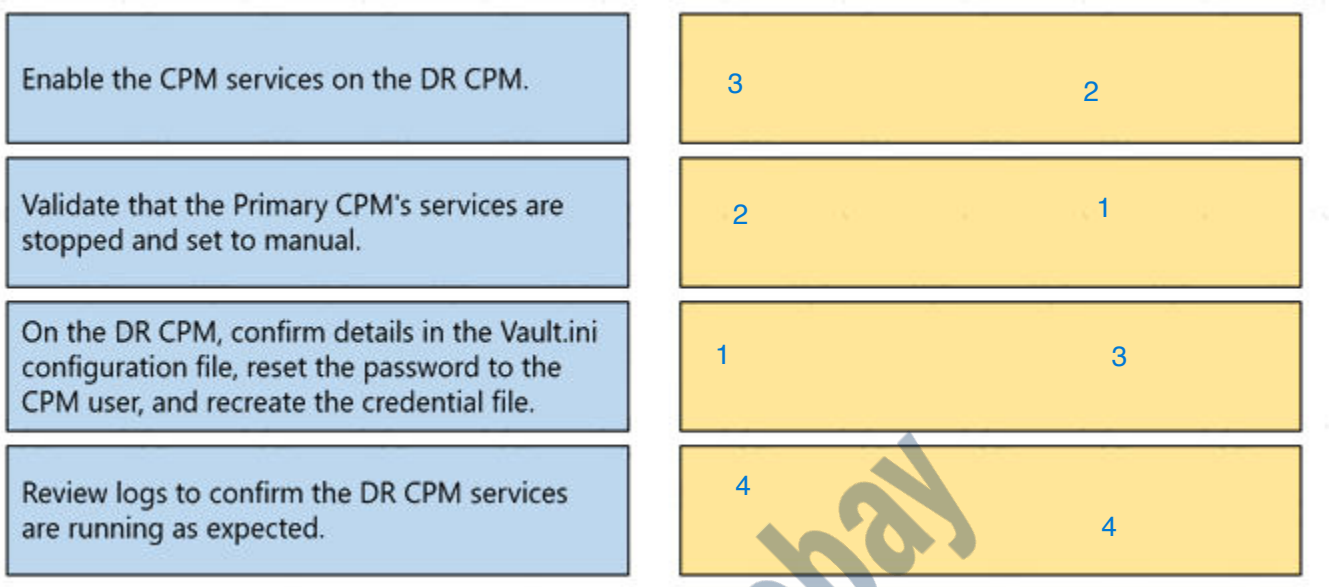
B. Upload the license.xml file to the VaultInternal Safe.

C. Upload the license.xml file to the System Safe and restart the PrivateArk Server service.

D. Upload the license.xml file to the VaultInternal Safe and restart the PrivateArk Server service.

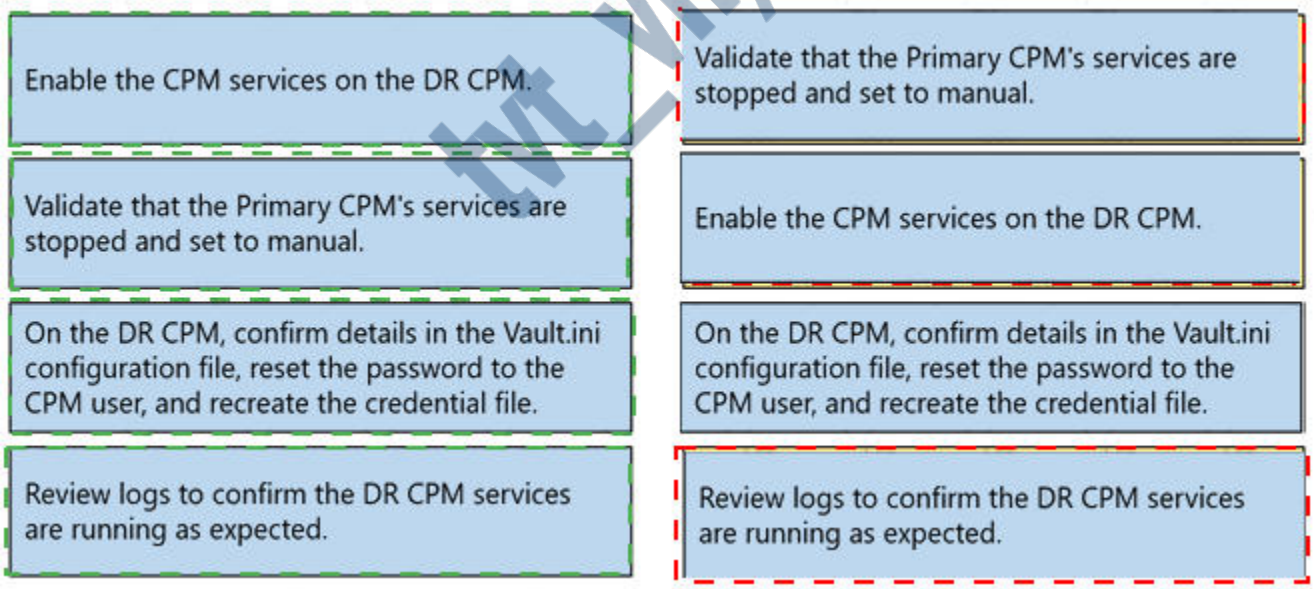
Answer: A

Question #:86

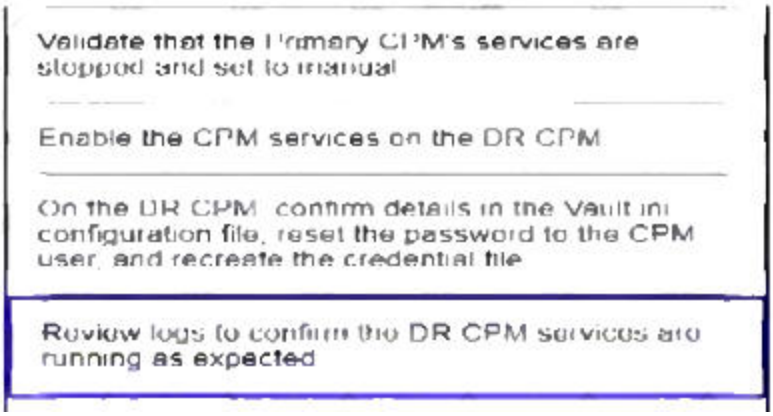


Arrange the steps to failover to the DR CPM in the correct sequence.

Answer:



Suggested Answer:



Question #:87

You need to add a new PSM server to an existing CyberArk environment.

What is the best way to determine the sizing of this server?

A. Review the "Recommended Server Specifications" for PSMs in the CyberArk Documents website. Most Voted

B. Use the specifications of any existing PSM and request a server of the same size.

C. Use the CyberArk Support Knowledgebase, search for "PSM Sizing" and locate the Knowledgebase article related to sizing.

D. Refer to the Microsoft Windows website, determine the minimum specifications required for the Operating System you are installing, and then add 4 Gb of RAM and 20 GB of disk.

Answer: C

Question #:88

The Remote Desktop Services role must be property licensed by Microsoft.

A. TRUE

B. FALSE

Answer: A

Question #:89

What utility is used to create or update a credential file?

A. CreateCredFile exe

B. CAVaultManager.exe

C. Central Policy Manager

D. Password Vault Web Access

Answer: A

Question #:90

Which of the following are secure options for storing the contents of the Operator CD, while still allowing the contents to be accessible upon a planned Vault restart? Choose all that apply

A. Store the CD in a physical safe and mount the CD every time vault maintenance is performed.

B. Copy the contents of the CD to the System Safe on the vault

C. Copy the contents of the CD to a folder on the vault server and secure it with NTFS permissions.

D. Store the server key in a Hardware Security Module.

E. Store the server key in the Provider cache

Answer: C D

Question #:91

Which pre-requisite step must be completed before installing a Vault?

A. Join the server to a domain.

B. Install a clean operating system.

C. Install antivirus software.

D. Copy the master CD to a folder on the Vault server.

Answer: B

Question #:92

Which utility should be used to register the Vault in Amazon Web Services?

A. CAVaultManager Most Voted

B. StorageManager

C. CloudVaultManager

D. CACert

Answer: A

Question #:93

In which file must the attribute 'SignAuthnRequest="true"' be added to the PartnerIdentityProvider element to support signed SAML requests?

A. saml.config

B. samlconfig.ini

C. PVWAConfig.xml

D. PVConfiguration.xml

Answer: C

Question #:94

In addition to disabling Windows services or features not needed for PVWA operations, which tasks does PVWA_Hardening.ps1 perform when run? (Choose two.)

A. performs IIS hardening

B. configures all group policy settings

C. renames the local Administrator Account

D. configures Windows Firewall

E. imports the CyberArk INF configuration

Answer: A D

Question #:95

Which statement is correct about a post-install hardening?

A. The Vault must be hardened during the Vault installation process. Most Voted

B. After the Vault server is installed, you must join the server to the Enterprise Domain and reboot the host.

C. It is executed after Vault installation by running CAVaultHarden.exe and hardening options can be edited by changing the Hardening.ini file. Most Voted

D. If it is mandated by an organization's IT governance, you do not have to execute Vault hardening;

however, server hardening cannot be reversed.

Answer: C

Question #:96

When SAML authentication is used to sign in to the PVWA, which service performs the actual authentication?

A. Active Directory (AD)

B. Identity Provider (IdP) Most Voted

C. Service Provider (SP)

D. CyberArk Password Vault Web Access (PVWA)

Answer: B

Question #:97

Which files does the Vault Installation Wizard prompt you for during the Vault install?

A. Operator CD and License Most Voted

B. Master CD and License

C. Operator CD and Vault Certificate

D. Master CD and DBparm.ini

Answer: A

Question #:98

Which configuration file and Vault utility are used to migrate the server key to an HSM?

A. DBparm.ini and CAVaultManager.exe

B. VaultKeys.ini and CAVaultManager.exe

C. DBparm.ini and ChangeServerKeys.exe

D. VaultKeys.ini and ChangeServerKeys.exe

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASREF/DBParm.ini.htm?tocpath=Administrator%7CReferences%7CConfiguration%20Files%7CCyberArk%20Vault%20Server%20Parameter%20Files%7C_____1

Answer: D

Question #:99

When integrating a Vault with HSM, which file is uploaded to the HSM device?

A. server.key

B. recpub.key

C. recprv.key

D. mdbase.dat

Answer: A

Question #:100

You want to improve performance on the CPM by restricting accounts for the CYBRWINDAD platform to only the WINDEMEA and WINDEMEA_Admin safes.

How do you set this in CyberArk?

A. In the CYBRWINDAD platform, under Automatic Password Management/General, configure AllowedSafes and set to (WINDEMEA)|(WINDEMEA_ADMIN). Most Voted

B. In the settings for Configuration/CPM assigned to the WINDEMEA and WINDEMEAADMIN safes, configure AllowedSafes and set to (WINDEMEA)|(WINDEMEAADMIN).

C. In the CYBRWINDAD platform, under UI&Workflows/Properties/Optional, configure AllowedSafes and set to (WINDEMEA)|(WINDEMEA_ADMIN).

D. Modify cpm.ini on the relevant CPM/s and add the setting AllowedSafesCYBRWINDAD and set to (WINDEMEA)|(WINDEMEAADMIN).

Answer: A

Question #:101

You want to change the name of the PVWAappuser of the second PVWA server.

Which steps are part of the process? (Choose two.)

A. Update PVWA.ini with new user name

B. Update Vault.ini with new user name

C. Create new user in PrivateArk

D. Rename user in PrivateArk

E. Create new cred file for user

Answer: D E

Question #:102

Which service must be set to Automatic (delayed start) after the Vault is installed and configured?

A. Windows Time service

B. PrivateArk Database

C. Windows Update service

D. PrivateArk Server

Answer: A

Question #:103

Your customer upgraded recently to version 12.2 to allow the Linux team to use the new MFA caching feature. The PSM for SSH was installed with default configuration settings. After setting the Authentication to SSH key and enabling MFA Caching from the PVWA interface, the Linux Team cannot connect successfully using the new MFA caching feature.

What is the most probable cause?

A. OpenSSH 7.8 or above is not installed.

B. The MFACaching parameter in the psmpparms file is not set to True.

C. A passphrase policy must be added.

D. MFA caching is not supported when the PSM for SSH is deployed with default settings.

Answer: D

Question #:104

What are the operating system prerequisites for installing CPM? Select all that apply.

A. NET 3.51 Framework Feature

B. Web Services Role

C. Remote Desktop Services Role

D. Windows 2008 R2 or higher.

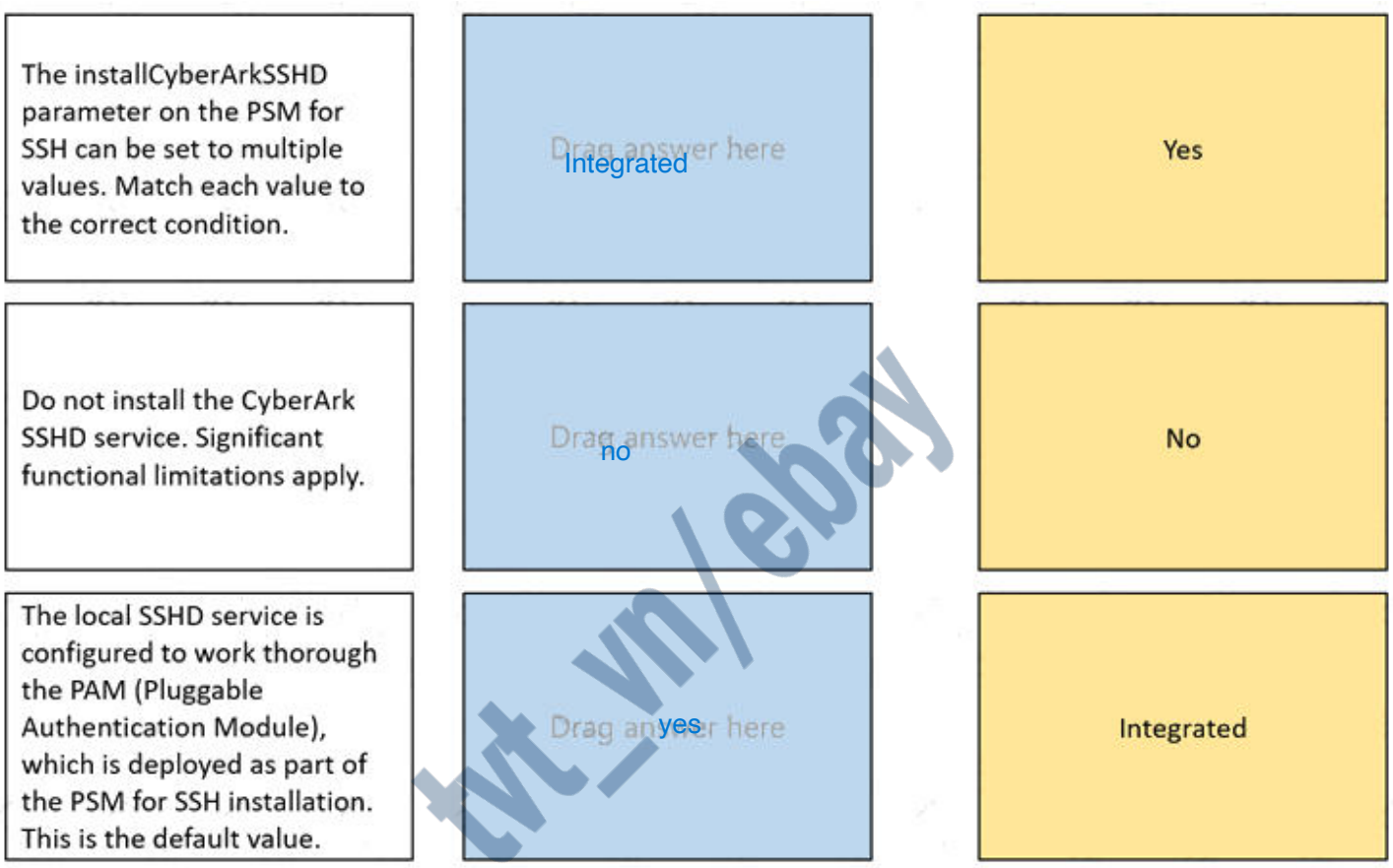
Answer: A

Question #:105

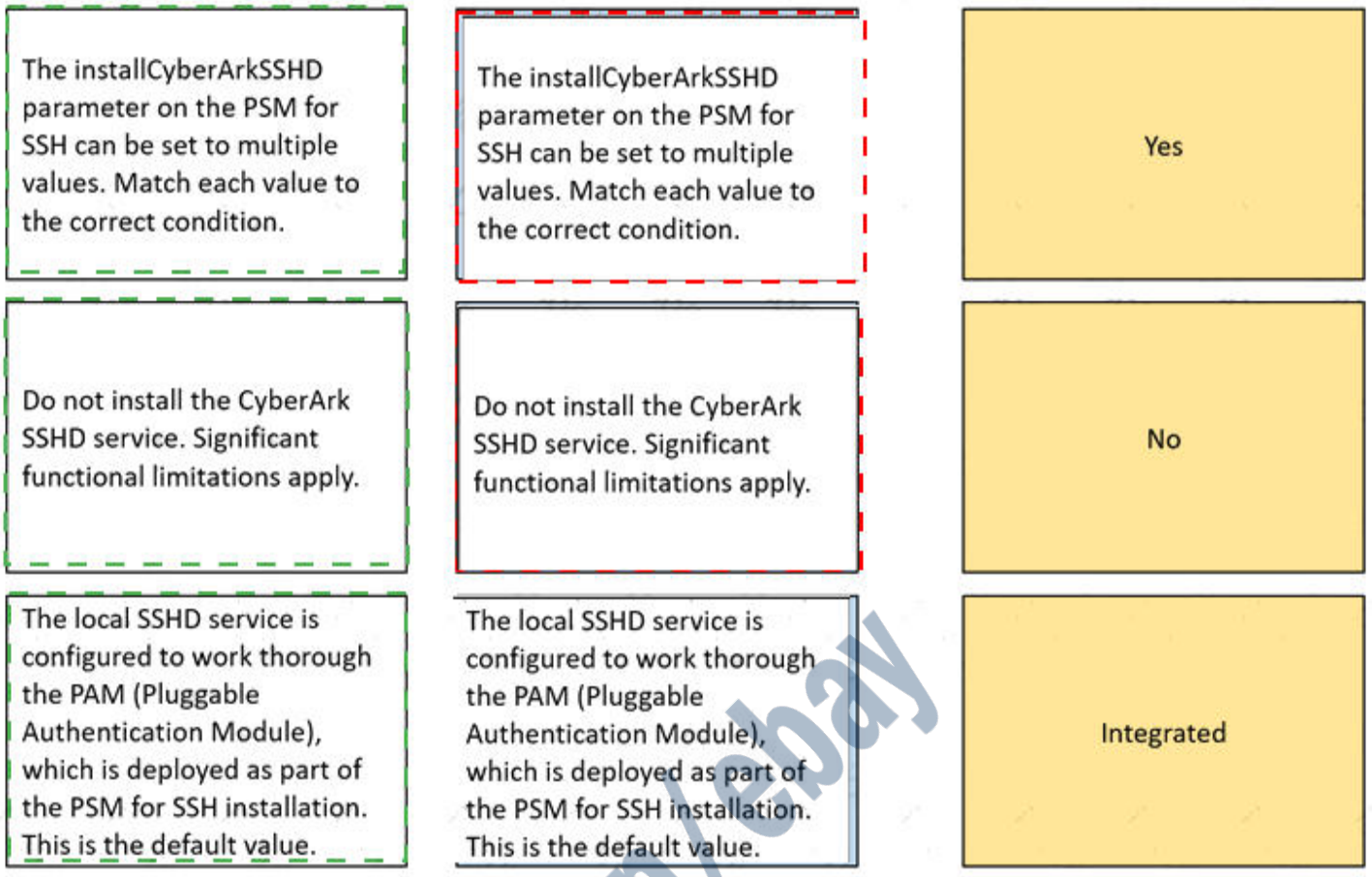
-

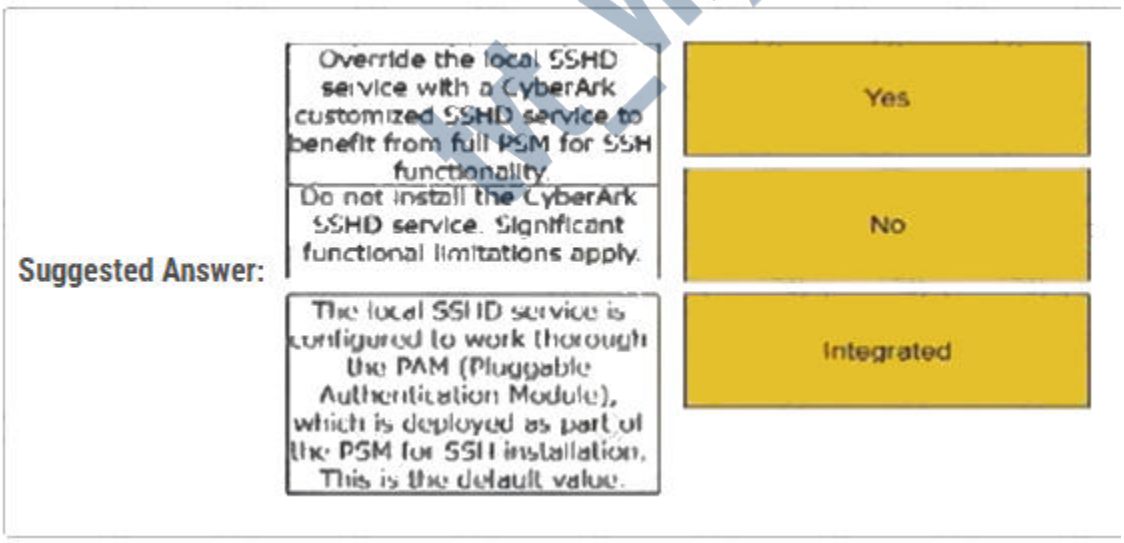
The installCyberArkSSHD parameter on the PSM for SSH can be set to multiple values.

Match each value to the correct condition.



Answer:





Question #:106

You are successfully managing passwords in the alpha cyberark com domain; however, when you attempt to manage a password in the beta cyberark com domain, you receive the 'network path not found' error. What should you check first?

A. That the username and password are correct

B. That the CPM can successfully resolve addresses in the beta cyberark com domain

C. That the end user has the correct permissions on the safe.

D. That an appropriate trust relationship exists between alpha.cyberark com and beta cyberark.com

Answer: B

Question #:107

Which statement about REST API is correct? (Choose two.)

A. When a user successfully authenticates to the Vault, an authentication token is returned. Most Voted

B. REST API Windows authentication method allows skipping the logon API by using the Windows default credentials with a Kerberos ticket.

C. To allow High Availability, REST API can be configured to support Session Load Balancing by editing the PVConfiguration.xml and setting the AllowPVWASessionRedandancy=Yes.

D. Each REST API call requires that a valid authentication token be provided. Most Voted

E. REST calls are directly sent to the currently active Vault using Port 1858.

Answer: A D

Question #:108

When configuring RADIUS authentication, which utility is used to create a file containing an encrypted version of the RADIUS secret?

A. CAVaultManager

B. CACert

C. CreateAuthFile

D. CreateCredFile

Answer: C

Question #:109

What is determined by the "MaxConcurrentConnections" setting within a platform?

A. maximum number of concurrent connections that can be opened between the CPM and the remote

machines for the platform

B. maximum number of concurrent connections that can be between the PSM and the remote machines for the platform

C. maximum number of concurrent connections allowed for a specific account on the platform through the PSM

D. maximum number of concurrent connections to the Vault allowed for sending audit activities relating to the platform

Answer: A

Question #:110

Which authentication methods does PSM for SSH support?

A. CyberArk password LDAP, RADIUS, SAML

B. LDAP, Windows Authentication, SSH keys

C. RADIUS, Oracle SSO, CyberArk Password

D. CyberArk Password, LDAP, RADIUS

Answer: D

Question #:111

A new domain controller has been added to your domain. You need to ensure the CyberArk infrastructure can use the new domain controller for authentication.

Which locations must you update?

A. on the Vault server in C:\Windows\System32\drivers\etc\hosts and in the PVWAApplication under Administration > LDAP Integration > Directories > Hosts

B. on both the Vault and the PVWA servers in C:\Windows\System32\drivers\etc\hosts

C. in the Private Ark client under Tools > Administrative Tools > Directory Mapping

D. on the Vault server in the certificate store and on the PVWA server in the certificate store

Answer: A

Question #:112

Name two ways of viewing the ITAlog

A. Log into the vault locally and navigate to the Server folder under the PrivateArk install location.

B. Log into the PVWA and go to the Reports tab.

C. Access the System Safe from the PrivateArk client.

D. Go to the Thirdpary log directory on the CPM

Answer: A C

Question #:113

What is the PRIMARY reason for installing more than 1 active CPM?

A. Installing CPMs in multiple sites prevents complex firewall rules to manage devices at remote sites.

B. Multiple instances create fault tolerance.

C. Multiple instances increase response time.

D. Having additional CPMs increases the maximum number of devices CyberArk can manage

Answer: D

Question #:114

If a transparent user matches two different directory mappings, how does the system determine which user template to use?

A. The system will use the template for the mapping listed first.

B. The system will use the template for the mapping listed last.

C. The system will grant all of the vault authorizations from the two templates.

D. The system will grant only the vault authorizations that are listed in both templates

Answer: A

Question #:115

You are installing PSM for SSH with AD-Bridge and CyberArkSSHD mode set to integrated for your customer.

Which additional packages do you need to install to meet the customer's needs? (Choose two.)

A. CARKpsmp-infra

B. libssh

C. OpenSSH 7.8 or higher

D. CARKpsmp-ADBridge

E. CARKpsmp-SSHD

Answer: A B

Question #:116

Which file must you edit to ensure the PSM for SSH server is not hardened automatically after installation?

A. vault.ini

B. user.cred

C. psmpparms

D. psmgw.config

Answer: C

Question #:117

What is the best practice for storing the Master CD?

A. Copy the files to the Vault server and discard the CD.

B. Copy the contents of the CD to a Hardware Security Module and discard the CD.

C. Store the CD in a secure location, such as a physical safe.

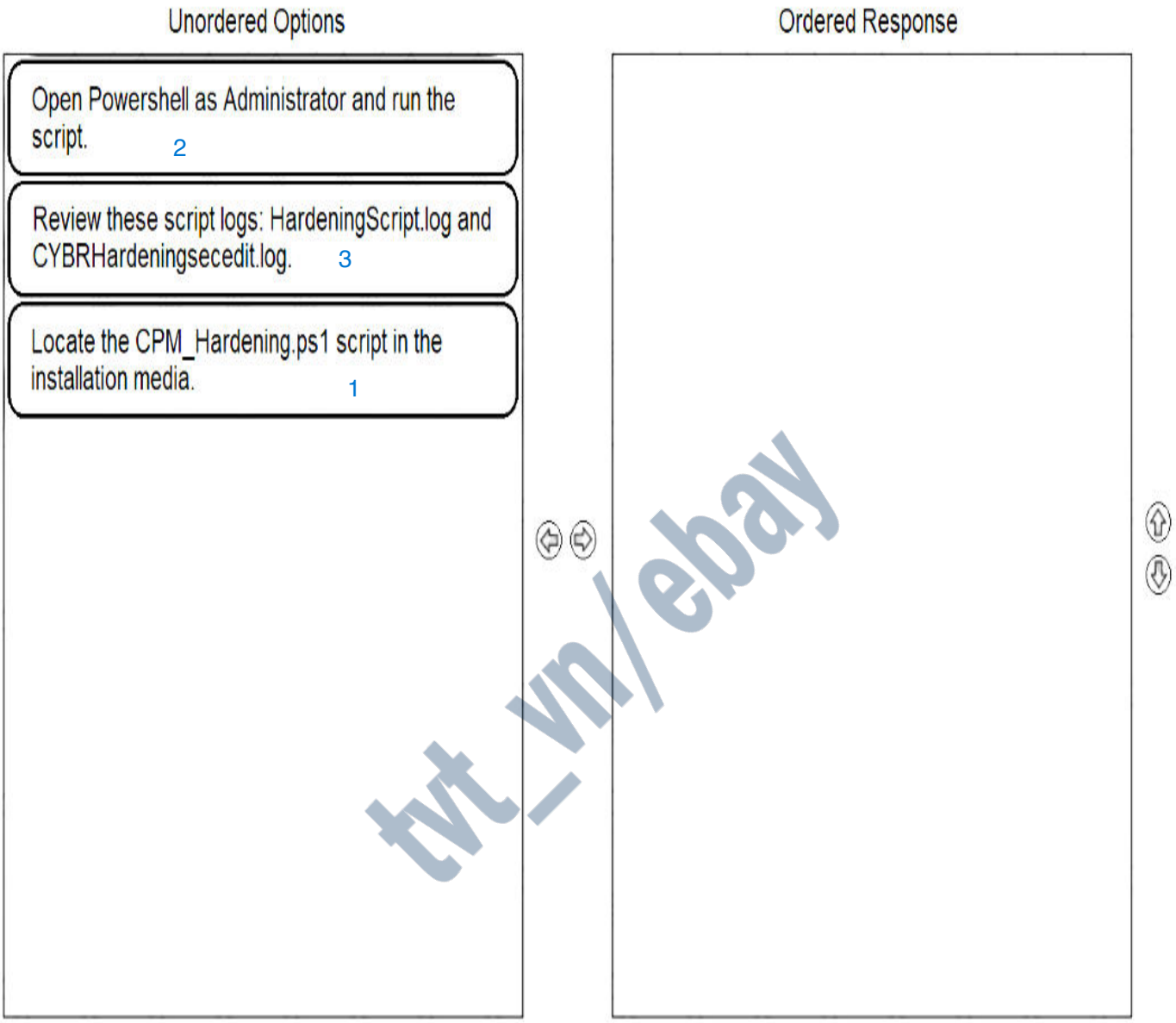
D. Store the CD in a secure location, such as a physical safe, and copy the contents of the CD to a folder (secured with NTFS permissions} on the vault.

Answer: D

Question #:118

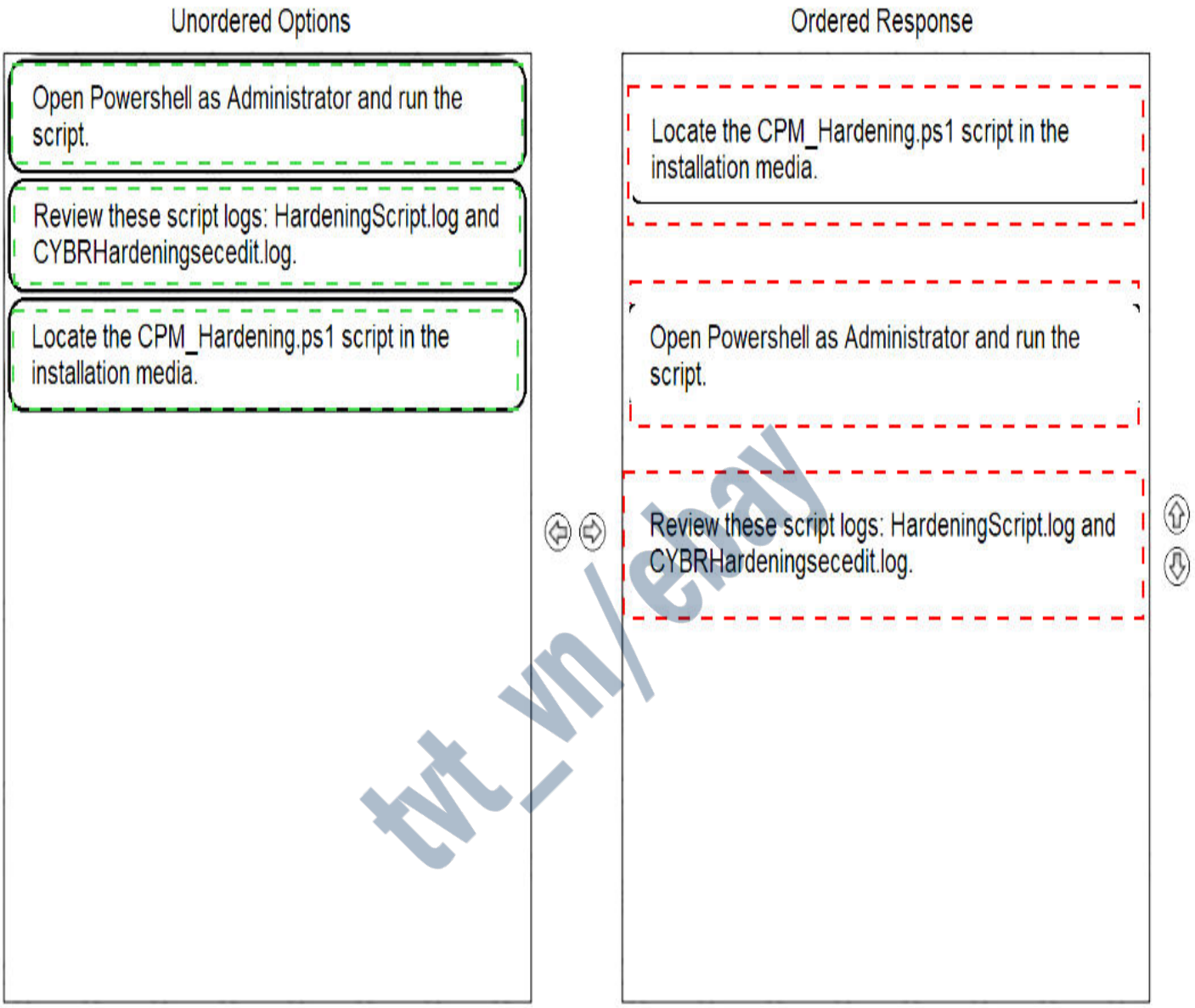
Arrange the steps to complete CPM Hardening for Out-of-Domain Deployment in the correct sequence.

Answer Area



Answer:

Answer Area



Ordered Response

1) Locate the CPM_Hardening.ps1 script in the installation media.
2) Open Powershell as Administrator and run the script.
3) Review these script logs: HardeningScript.log and CYBRHardeningsecedit.log.

Suggested Answer:

The correct sequence for completing CPM Hardening for Out-of-Domain Deployment is to first locate the CPM_Hardening.ps1 script in the installation media, then open Powershell as Administrator and run the script, followed by reviewing the HardeningScript.log and CYBRHardeningsecedit.log script logs. This ensures that all the necessary steps are taken in order to properly secure an out-of-domain deployment of CPM.

Question #:119

You want to add an additional maintenance user on the PSM for SSH.

How can you accomplish this if InstallCyberarkSSHD is set to Integrated?

A. Create a local user and add it to the PSMMaintenance Group.

B. Create a local user called proxymng.

C. Create a local user and add it to group configured for the parameter AllowGroups in the /etc/sshd_config file

D. Create a local user, called psmpmng.

Answer: C

Question #:120

If a customer has one data center and requires fault tolerance, how many PVWAs should be deployed?

A. two or more

B. one PVWA cluster

C. one

D. two PVWA clusters

Answer: A

Question #:121

What must you do to synchronize a new Vault server with an organization's NTP server?

A. Configure an AllowNonStandardFWAddresses rule for the organization's NTP server in DBParm.ini on the Vault server.

B. Use the Windows Firewall console to configure a rule on the Vault server which allows communication with the organization's NTP server.

C. Ensure the organization's NTP server is installed in the same location as the Vault server requiring synchronization.

D. Update the AutoSyncExternalObjects configuration in DBParm.ini on the Vault server to schedule regular synchronization.

Answer: A

Question #:122

A first PSM server has been installed.

What should you confirm before installing any additional PSM servers?

A. The PSM ID of the first installed PSM server was changed and the additional PSM server can use the same PSM ID.

B. The user performing the installation is a direct owner in the PSMUnmanagedSessionAccounts Safe, PSM safe and member of PVWAMonitor group.

C. The user performing the installation is not a direct owner in the PSMUnmanagedSessionAccounts Safe. Most Voted

D. The path of the Recordings Folder must be different on all PSM installations.

Answer: C

Question #:123

A customer has five PVWA servers. Three are located at the primary data center and the remaining two are at a satellite data center.

What is important to consider about the load balancer? (Choose two.)

A. It must not alter page content, or should include a mechanism to prevent pages from being altered. Most Voted

B. It must support "sticky sessions". Most Voted

C. It must be able to digitally sign and issue certificates for PVWA servers.

D. It must be able to connect to all Vault and PVWA servers through Port TCP 443.

E. It must be configured with high-availability (HA) enabled.

Answer: A B

Question #:124

Which parameter must be identical for both the Identity Provider (IdP) and the PVWA?

A. IdP "EntityID" and "PartnerIdentityProvider Name" in PVWA saml.config file

B. IdP "User name" and "SingleSignOnServiceUrl" in PVWA saml.config file

C. IdP "Audience" and "ServiceProviderName" in the PVWA saml.config file

D. IdP "Secure hash algorithm" and "Certificate" in the PVWA saml.config file

Answer: C

Question #:125

You are configuring the Vault to send syslog audit data to your organization's SIEM solution.

What is a valid value for the SyslogServerProtocol parameter in DBPARM.INI file?

A. TLS

B. SSH

C. SMTP

D. SNMP

Answer: A

Question #:126

The vault server uses a modified version of the Microsoft Windows firewall.

A. TRUE

B. FALSE

Answer: B

Question #:127

Which tools are used during a CPM renaming process? (Choose two.)

A. APIKeyManager Utility Most Voted

B. CreateCredFile Utility Most Voted

C. CPMInDomain_Hardening.ps1

D. PMTerminal.exe

E. Data Execution Prevention

Answer: A D

Question #:128

All 80 employees from your satellite Tokyo office are complaining that browsing the PVWA site is very slow; however, your New York headquarters users are not experiencing this. The current PAM solution is:

2 distributed Vaults, the primary one in New York and a satellite in Tokyo

2 PVWA servers, both in New York with load balancing configured

2 PSM servers, both in New York without load balancing configured

1 CPM server in New York

All PVWA, PSM, and CPM servers are connected to the primary Vault

Which proposal optimally resolves the performance issue while minimizing the impact to production?

A. Install two new PVWA servers in Tokyo data center, configure load balancing, connect to the local satellite Vault and provide the URL of new PVWA servers to the local employees.

B. Install two new PVWA servers in New York data center, configure load balancing and have them connect to the satellite Vault in Tokyo.

C. Install two new PSM servers in the Tokyo data center, configure load balancing, connect to the local satellite vault, and inform the local employees to browse using the same PVWA URL.

D. Change the current distributed Vaults architecture, migrate back to a Primary-DR architecture, install two new PVWA servers in the Tokyo data center and configure load balancing. Connect to the local DR Vault and provide the URL of new PVWA servers to the local employees.

Answer: A

Question #:129

In which configuration file on the Vault can filters be configured to either include or exclude log messages that are sent through SNMP?

A. PARAgent.ini

B. DBParm.ini

C. TSParm.ini

D. CyberArkv2 MIB file

Answer: A

Question #:130

What is a step to enable NTP synchronization on a stand-alone Vault?

A. Run Powershell and add the NTP module.

B. Restart the organization's NTP servers.

C. Edit dbparm.ini and add a Firewall rule for the NTP address.

D. Restart the Vault Event Notification Engine service.

Answer: C

Question #:131

The security of the Vault Server is entirely dependent on the security of the network.

A. TRUE

B. FALSE

Answer: B

Question #:132

This value needs to be added to the PVWA configuration file:

Assuming all CyberArk PVWA servers were installed using default paths/folders, which configuration file should you locate and edit to accomplish this?

A. c:\inetpub\wwwroot\passwordvault\web.config

B. c:\inetpub\wwwroot\passwordvault\services\web.config

C. c:\cyberark\password vault web access\env\web.config

D. c:\program files\cyberark\password vault web access\web.config

Answer: A

Question #:133

What would be a good use case for the Disaster Recovery module?

A. Recovery Time Objectives or Recovery Point Objectives are at or near zero.

B. Integration with an Enterprise Backup Solution is required.

C. Off site replication is required.

D. PSM is used.

Answer: C

Question #:134

Which of the following are supported authentication methods for CyberArk? Check all that apply

A. CyberArk Password (SRP)

B. LDAP

C. SAML

D. PKI

E. RADIUS

F. OracleSSO

G. Biometric

Answer: B D E

Question #:135

In order to retrieve data from the vault a user MUST use an interface provided by CyberArk.

A. TRUE

B. FALSE

Answer: A

Question #:136

A customer is moving from an on-premises to a public cloud deployment.

What is the best and most cost-effective option to secure the server key?

A. Install the Vault in the cloud the same way you would in an on-premises environment. Place the server key in a password protected folder on the operating system.

B. Install the Vault in the cloud the same way you would in an on-premises environment. Purchase a Hardware Security Module to secure the server key.

C. Install the Vault using the native cloud images and secure the server key using native cloud Key Management Systems.

D. Install the Vault using the native cloud images and secure the server key with a Hardware Security Module.

Answer: C