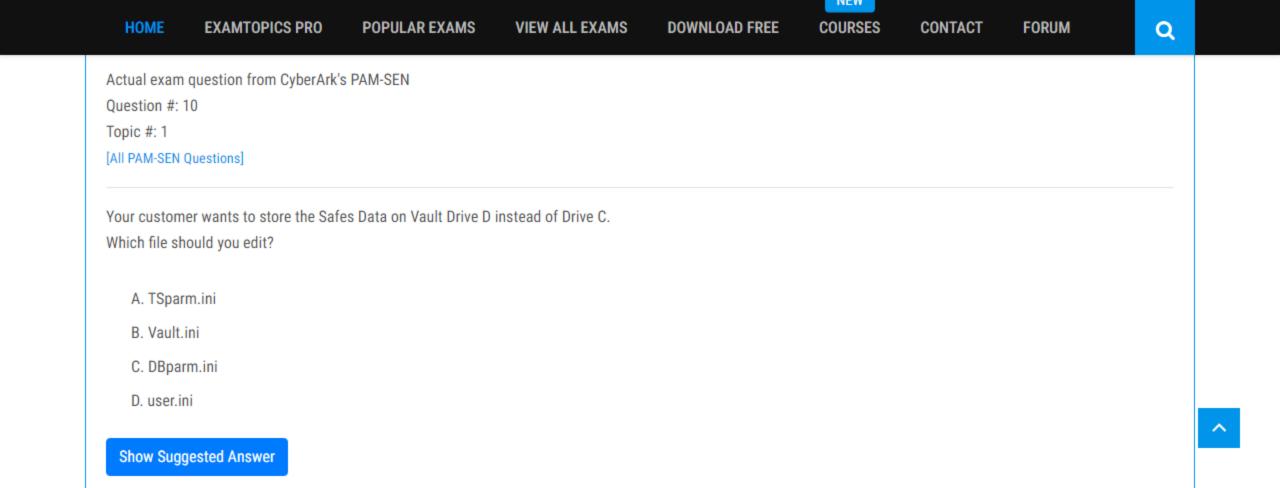
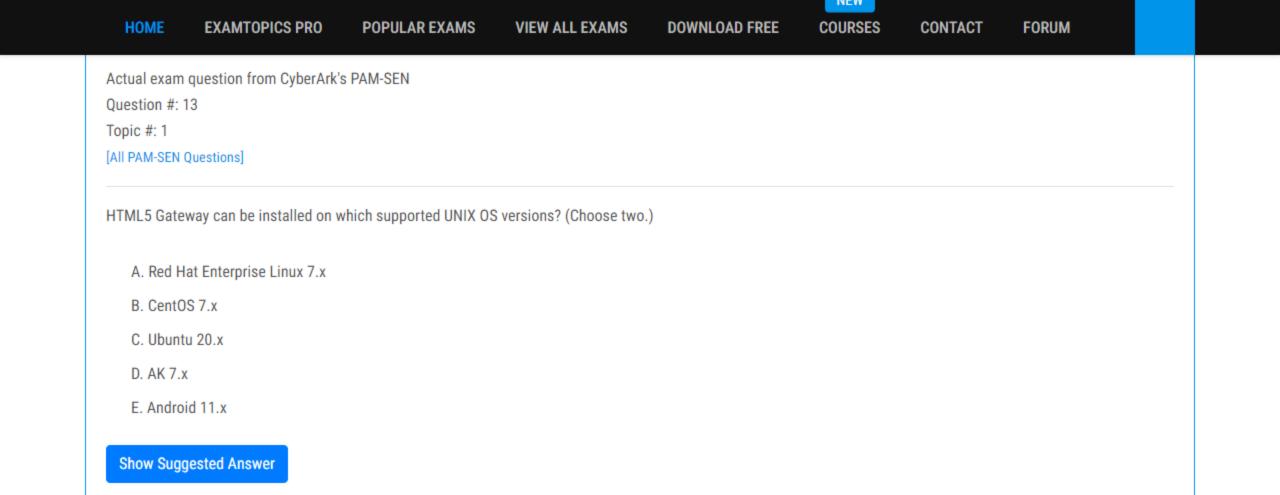
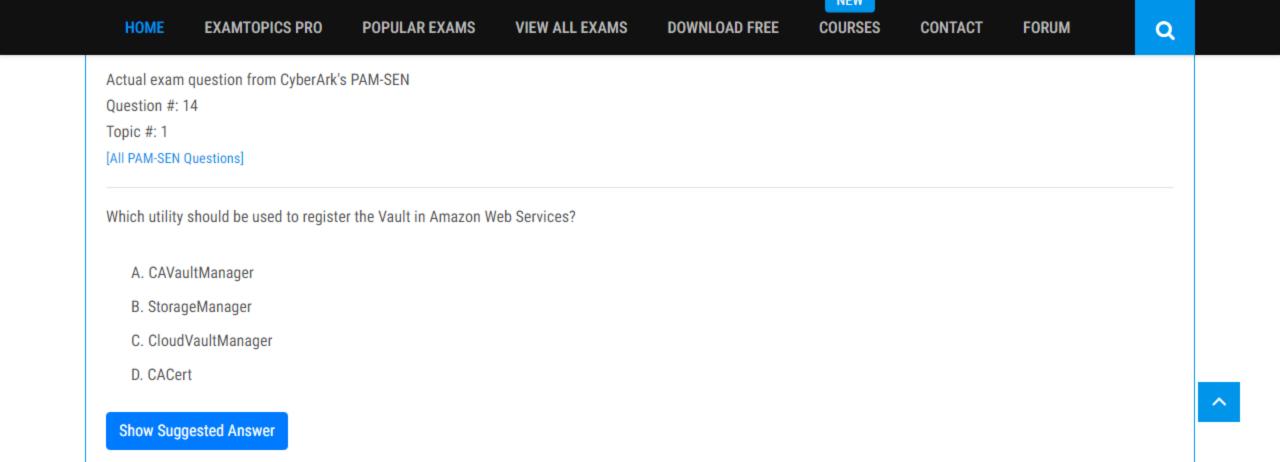


- C. TSParm.ini
- D. CyberArkv2 MIB file







Question #: 15 Topic #: 1

[All PAM-SEN Questions]

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

HOME **EXAMTOPICS PRO POPULAR EXAMS VIEW ALL EXAMS COURSES** CONTACT **FORUM** Q **DOWNLOAD FREE** Actual exam question from CyberArk's PAM-SEN Question #: 17 Topic #: 1 [All PAM-SEN Questions] DRAG DROP -

Answer Area

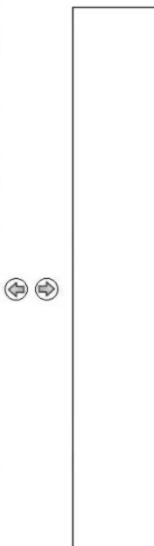
Open Powershell as Administrator and run the script.

Unordered Options

Review these script logs: HardeningScript.log and CYBRHardeningsecedit.log.

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

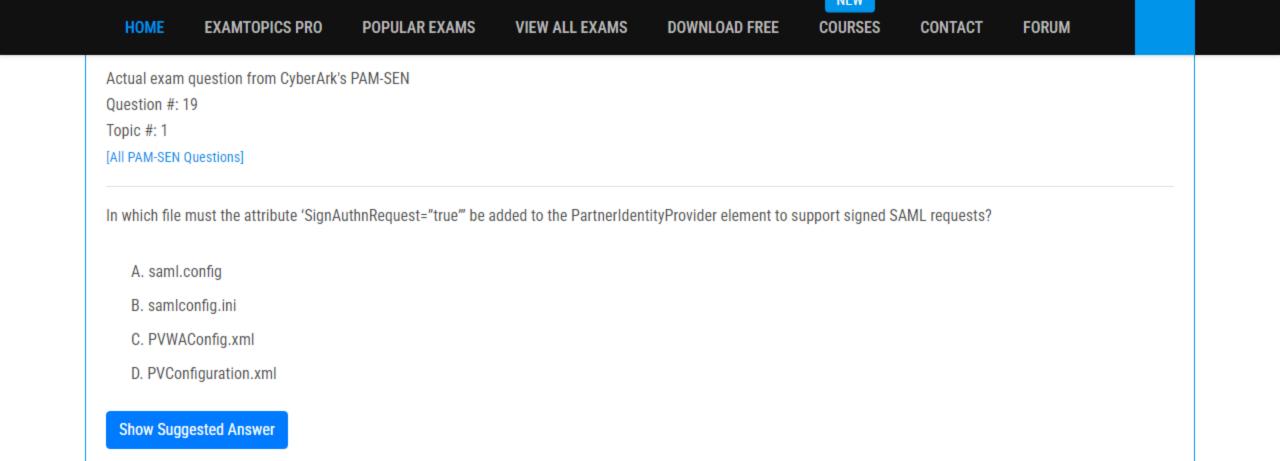
Locate the CPM_Hardening.ps1 script in the installation media.





Ordered Response





Q

Actual exam question from CyberArk's PAM-SEN

Question #: 21

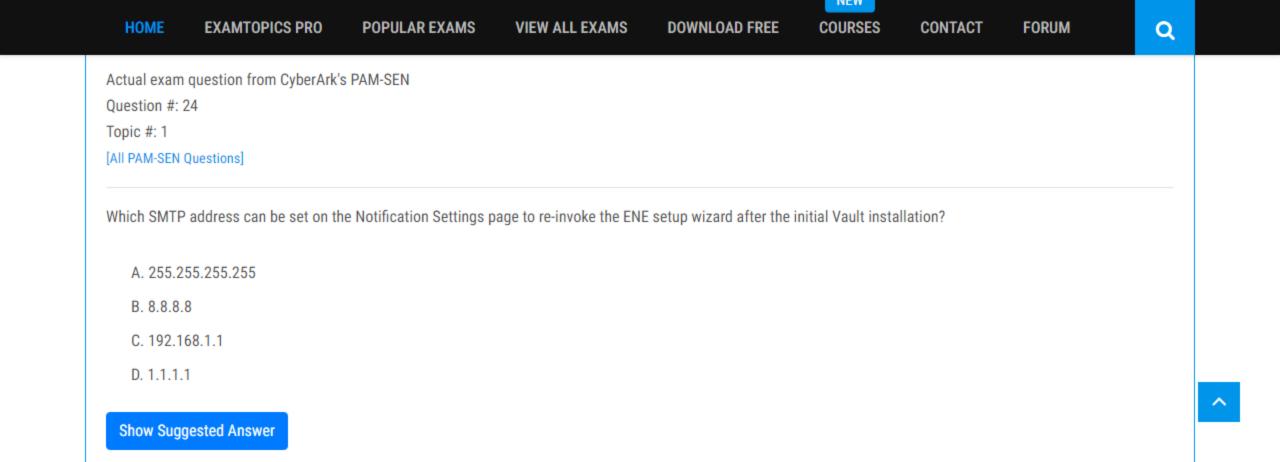
Topic #: 1

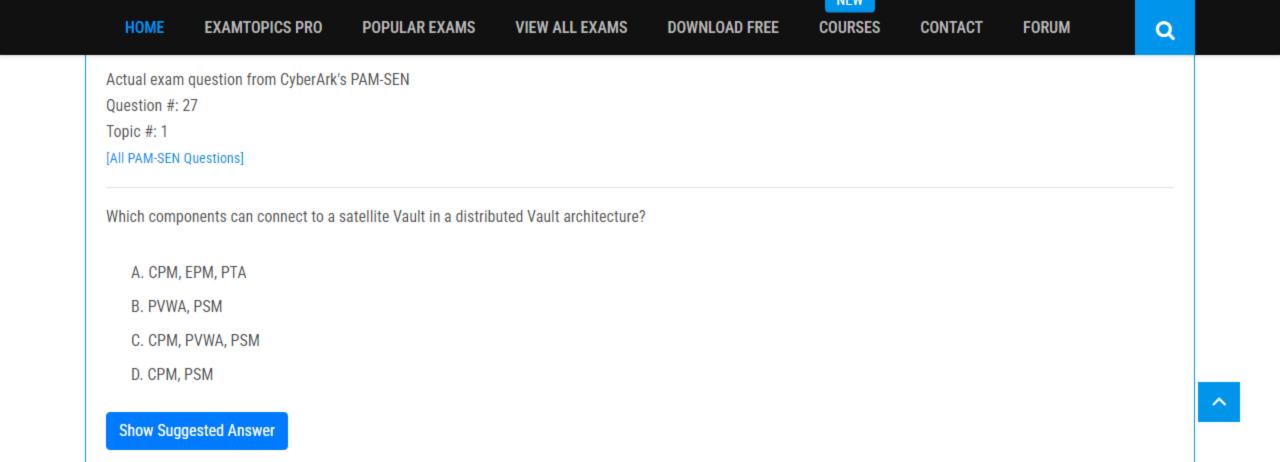
[All PAM-SEN Questions]

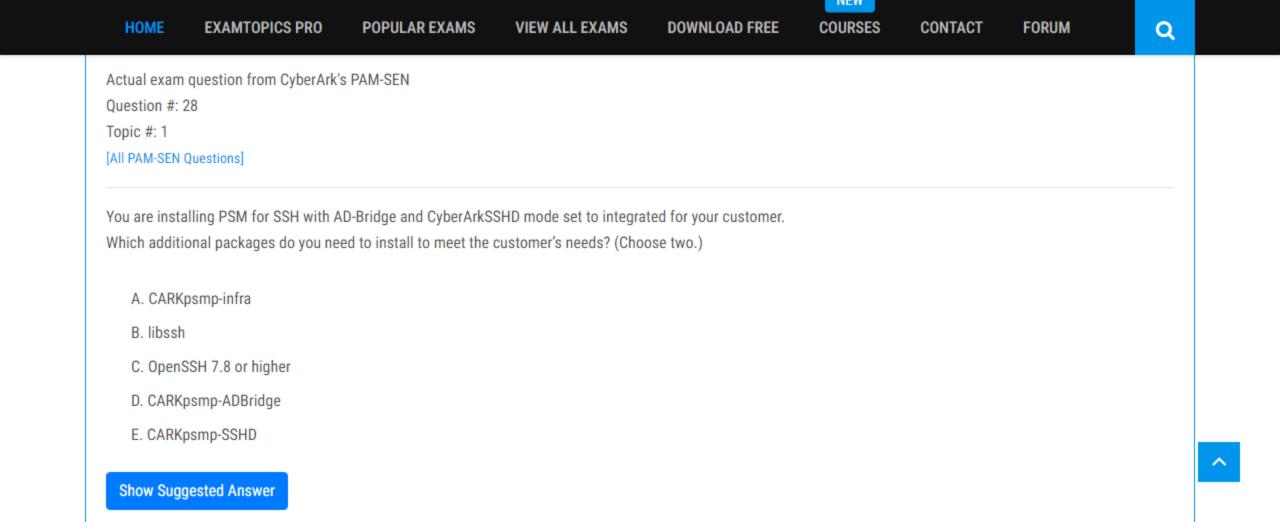
Your customer upgraded recently to version 12.2 to allow the Linux team to use the new MFA caching feature. The PSM for SSH was installed with default configuration settings. After setting the Authentication to SSH key and enabling MFA Caching from the PVWA interface, the Linux Team cannot connect successfully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

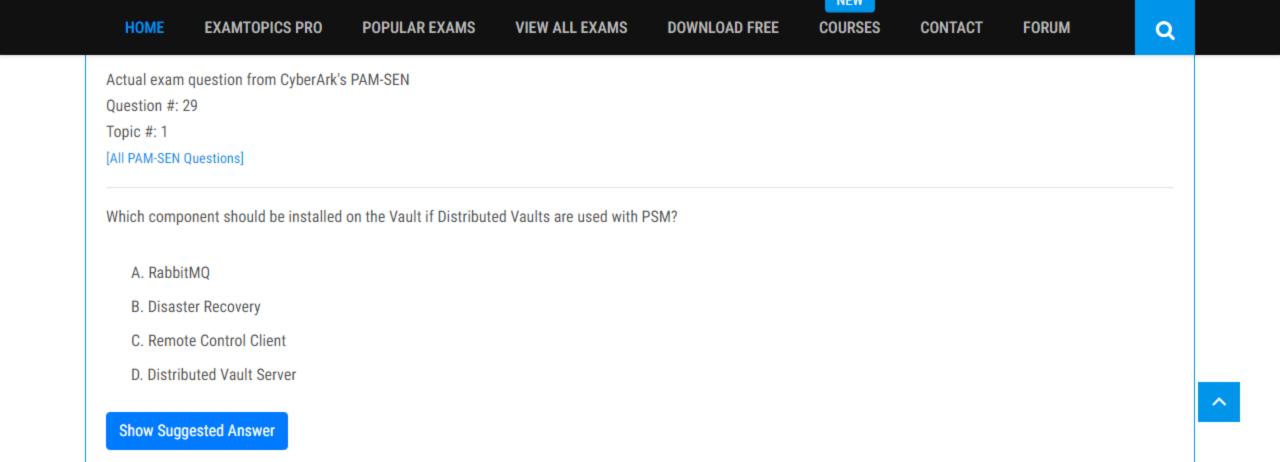
What is the most probable cause?

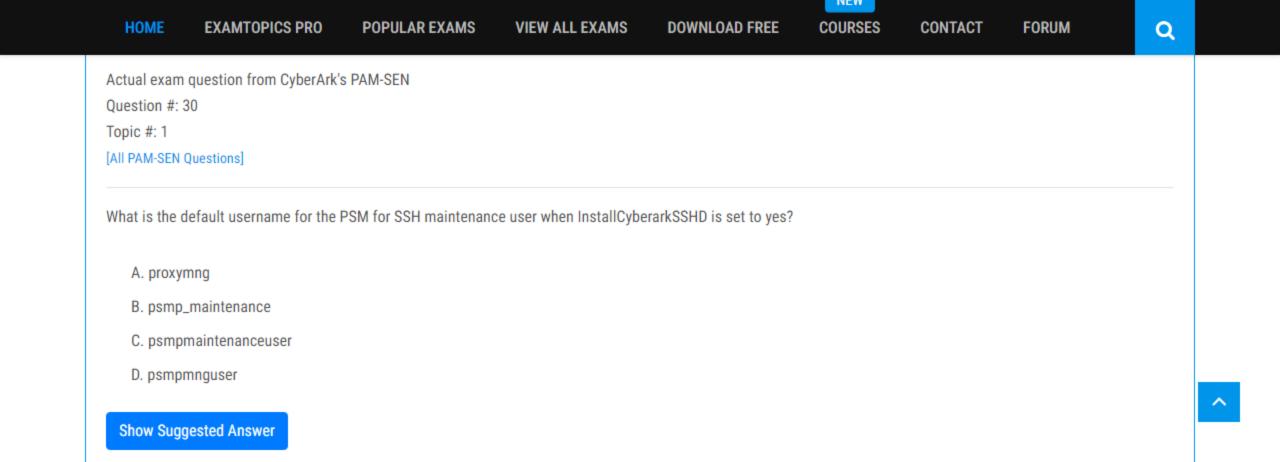
- A. OpenSSH 7.8 or above is not installed.
- B. The MFACaching parameter in the psmpparms file is not set to True.
- C. A passphrase policy must be added.
- D. MFA caching is not supported when the PSM for SSH is deployed with default settings.

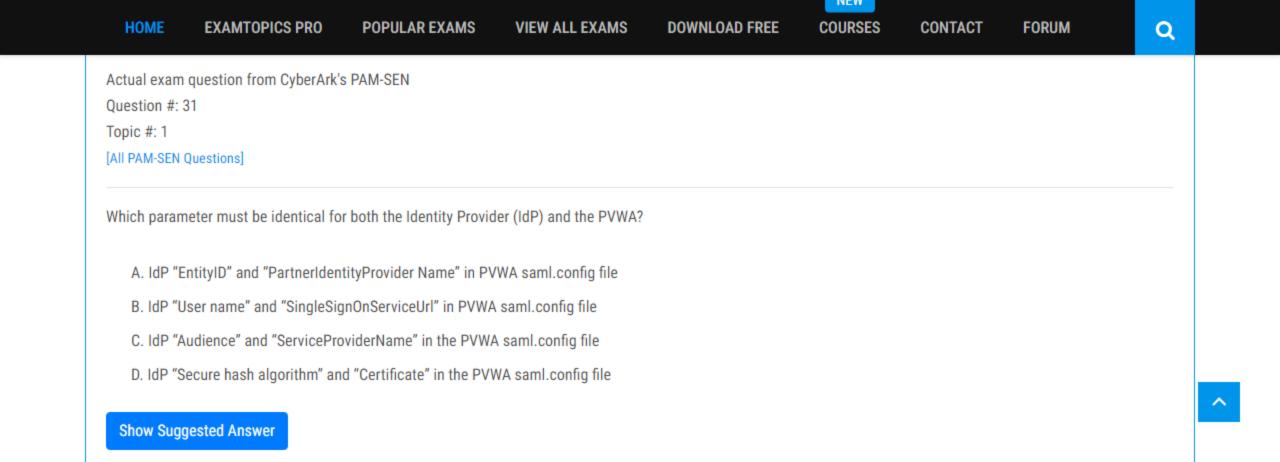












Actual exam question from CyberArk's PAM-SEN

Question #: 32

Topic #: 1

[All PAM-SEN Questions]

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.

COURSES

CONTACT

FORUM

Actual exam question from CyberArk's PAM-SEN

Question #: 33

Topic #: 1

[All PAM-SEN Questions]

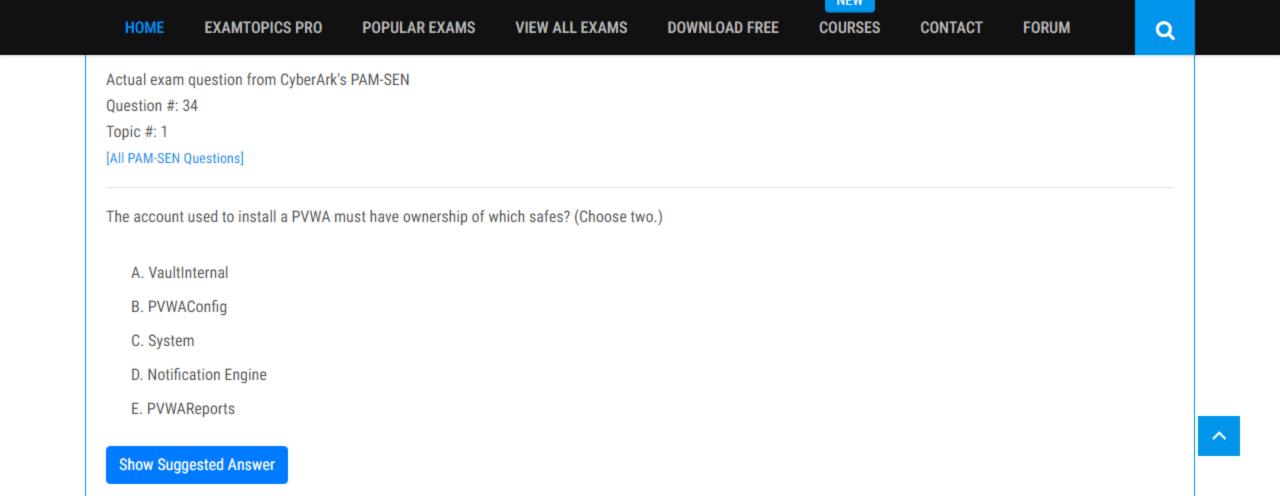
You have been asked to limit a platform called "Windows_Servers" to safes called "WindowsDC1" and "WindowsDC2". The platform must not be assigned to any other safe.

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".

Show Suggested Answer

 $^{\sim}$



HOME EXAMTOPICS PRO POPULAR EXAMS VIEW ALL EXAMS DOWNLOAD FREE COURSES CONTACT FORUM

Actual exam question from CyberArk's PAM-SEN

Question #: 35

Topic #: 1

[All PAM-SEN Questions]

DRAG DROP -

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

Answer Area

Unordered Options

Run the PVWAInstallation.ps1 script in PowerShell as Administrator.

Run the PVWA_Prerequisites.ps1 script in Powershell as Administrator.

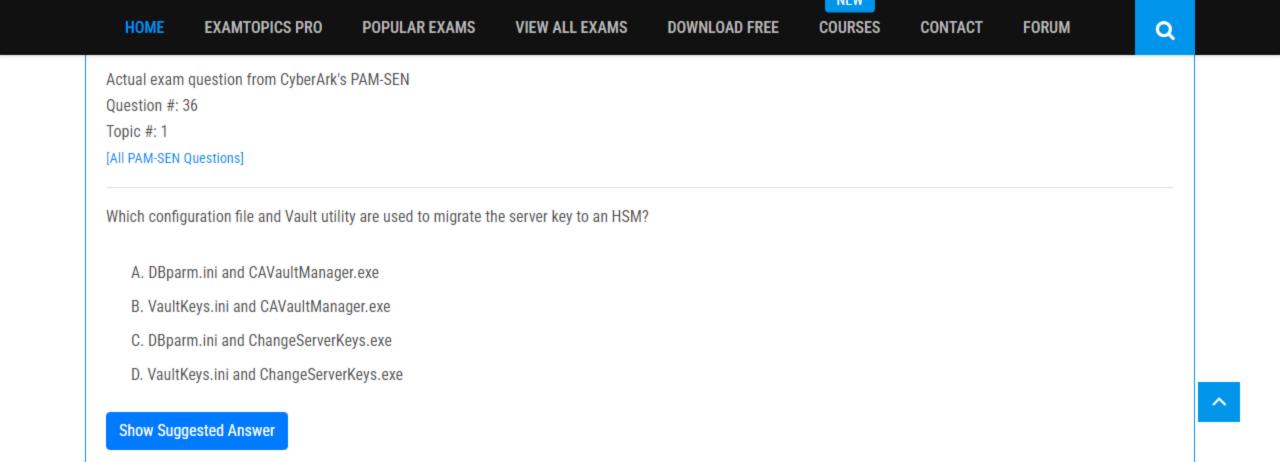
Run the PVWARegisterComponent.ps1 script with the Vault password and run the PVWA_Hardening.ps1 script in PowerShell as Administrator.

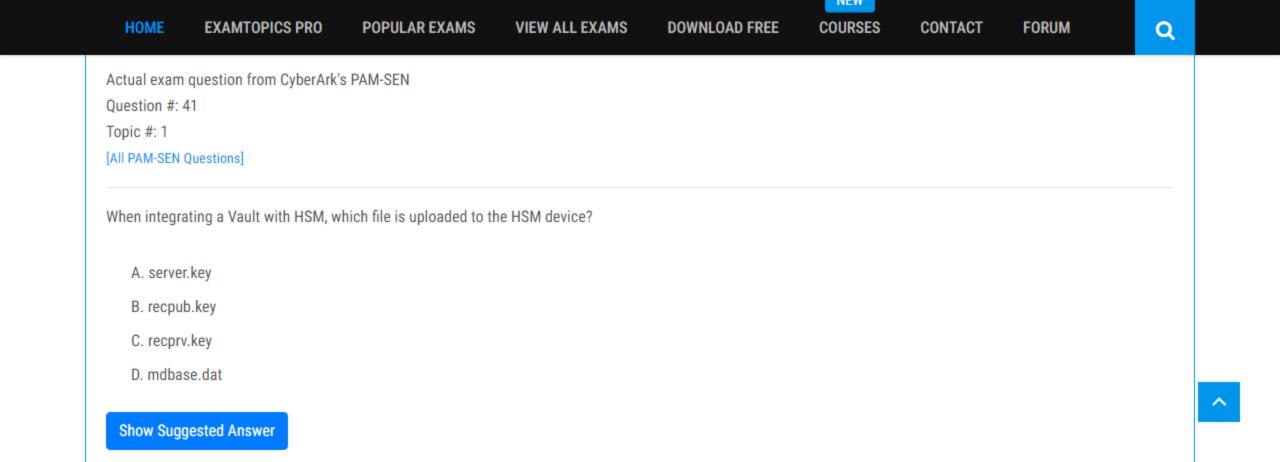


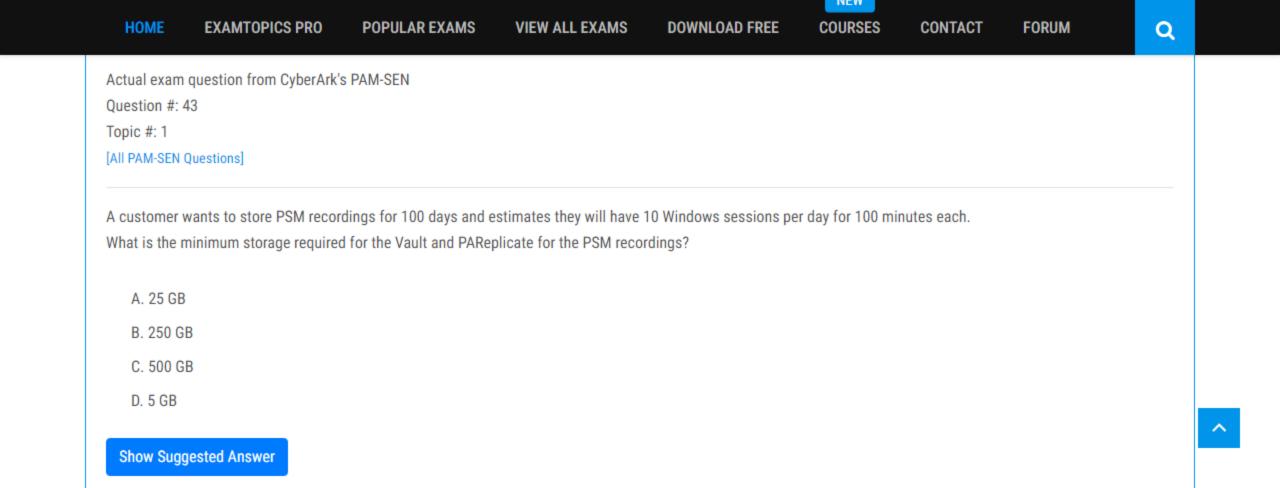
Ordered Response











INEVV

FORUM

Question #: 44

Topic #: 1

[All PAM-SEN Questions]

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

INEVV

FORUM

Question #: 45

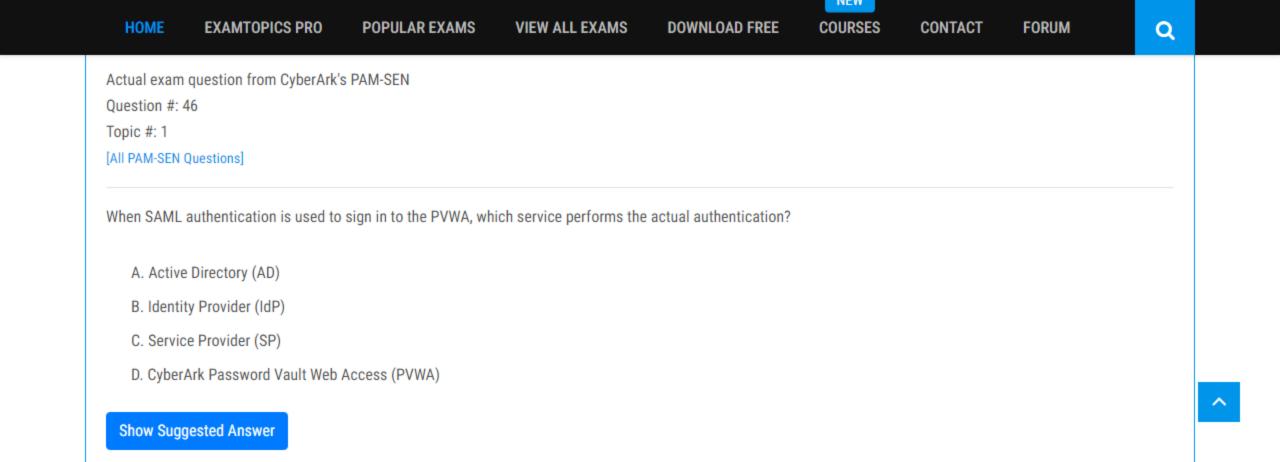
Topic #: 1

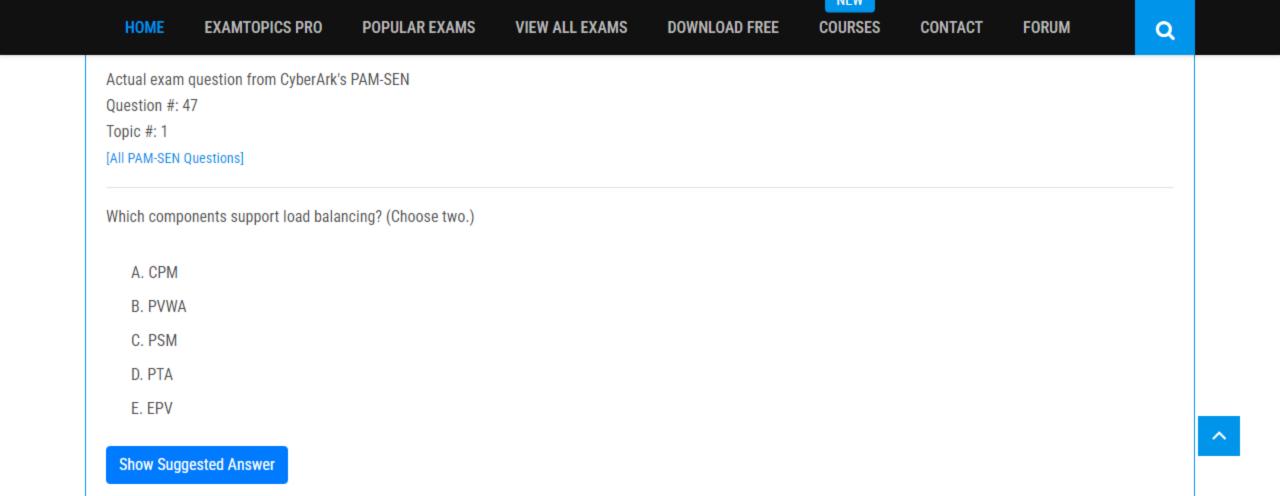
[All PAM-SEN Questions]

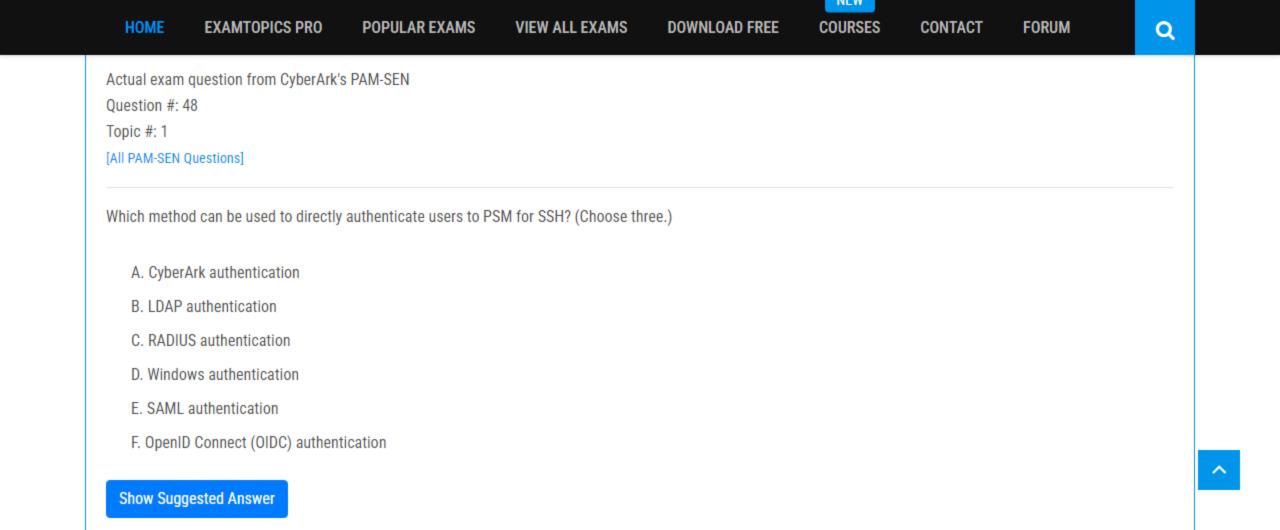
In addition to disabling Windows services or features not needed for PVWA operations, which tasks does PVWA_Hardening.ps1 perform when run? (Choose two.)

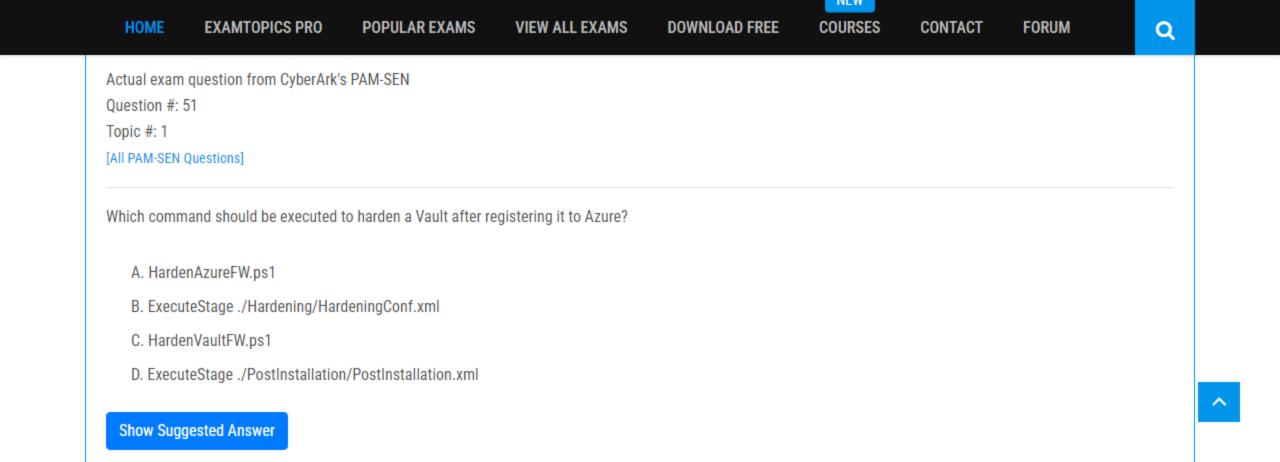
- A. performs IIS hardening
- B. configures all group policy settings
- C. renames the local Administrator Account
- D. configures Windows Firewall
- E. imports the CyberArk INF configuration

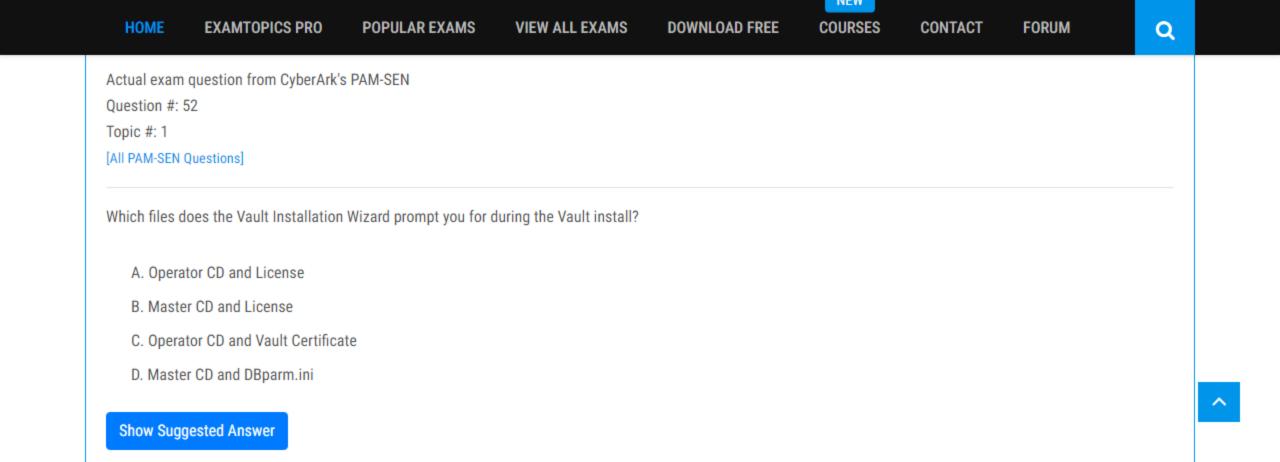












DOWNLOAD FREE COURSES CONTACT

INEW

FORUM

Q

Actual exam question from CyberArk's PAM-SEN

Question #: 54

Topic #: 1

[All PAM-SEN Questions]

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.

HOME	EXAMTOPICS PRO	POPULAR EXAMS	VIEW ALL EXAMS	DOWNLOAD FREE	COURSES	CONTACT	FORUM	
Actual exam	question from CyberArk's	s PAM-SEN						
Question #:	55							
Topic #: 1								
[All PAM-SEN	Questions]							
Vou are inst	alling the HTML5 gateway	on a Linux host using th	ho DDM provided					
	ng the Tomcat webapp, w							
Alter Ilistalli	пу те топісат мерарр, м	mat is the next step in th	le ilistaliation process?					
A. Deplo	y the HTML5 service (gua	acd).						
B. Secur	e the connection betweer	n the guacd and the web	арр.					
C. Secur	e the webapp and JWT va	alidation endpoint.						
D. Config	jure ASLR.							
Show Sug	gested Answer							
								I

INLAA

	question from CyberArk'	s PAM-SEN			
Question #:	56				
Topic #: 1					
[All PAM-SEN	Questions]				
	ired before the first CPM nvironment must have at		PVWA installed.		
B. The V	ault environment must ha	ve at least one account	stored in a safe.		
C. Custo	m platforms must be dov	vnloaded from the Cyber	Ark Marketplace.		
		nstalled and proper func	tionality validated		

INLAA

