output-till30 testdraft

IMG-20231015-WA0001.jpg

Which accounts can be selected for use in the Windows discovery process? (Choose 2)

an account stored in the Vault  
an account specified by the user  
the Vault Administrator  
any user with Auditor membership  
the PasswordManager user

IMG-20231015-WA0002.jpg

Your organization requires all passwords be rotated every 90 days. Where can you set this requirement?

Master Policy  
Safe Templates  
PVWAConfigxml  
Platform Configuration

IMG-20231015-WA0003.jpg  
You created a new platform by duplicating the out-of-box Linux through the SSH platform. Without any change, which Text Recorder Type(s) will the new platform support? (Choose 2.)

SSH Text Recorder  
Universal Keystrokes Text Recorder  
Events Text Recorder  
SQL Text Recorder  
Telnet Commands Text Recorder

IMG-20231015-WA0004.jpg

What is required to Manage loosely connected devices?

PSM for SSH  
EPM  
PSM  
PTA

IMG-20231015-WA0005.jpg  
Where can reconcile and/or logon accounts be linked to an account? (Choose 2)

account settings  
platform settings  
master policy  
safe settings  
service account settings

IMG-20231015-WA0006.jpg

Which dependent accounts does the CPM support out-of-the-box? (Chaos

Solaris Configuration file  
Windows Services  
Windows Scheduled Tasks  
Windows DCOM Applications  
Windows Registry  
Key Tab file

IMG-20231015-WA0007.jpg  
CyberArk Defender - PAM - Dattatraya B Ingale

In addition to add accounts and update account contents, which additional permission on the safe is required to add a Single account?

Upload Accounts Properties  
Rename Accounts  
Update Account Properties  
Manage Safe

IMG-20231015-WA0008.jpg

Which parameters can be used to harden the Credential Files (CredFiles) while using CreateCredFile Utility? (Choose 3 )

OS Username  
Current machine IP  
Current machine hostname  
Operating System Type (Linux/Windows/HP-UX)  
Vault IP Address  
Time Frame

IMG-20231015-WA0009.jpg  
Yvoe

Where can a user with the appropriate permissions generate a report? (Choose 2)

PWVA > Reports  
PrivateArk Client  
Cluster Vault Manager  
PrivateArk Server Monitor  
PARClient

IMG-20231015-WA0010.jpg

When should vault keys be rotated?

when it is copied to file systems outside the vault  
annually  
whenever a CyberArk user leaves the organization  
when migrating to a new data center

IMG-20231015-WA0011.jpg

Which statement is true about setting the reconcile account at the platform level?

This is the only way to enable automatic reconciliation of account passwords.  
CPM performance will be improved when the reconcile account is set at the platform level.  
A rule can be used to specify the reconcile account dynamically or a specific reconcile account can be selected.  
This configuration prevents the association from becoming broken if the reconcile account is moved to a different safe.

IMG-20231015-WA0012.jpg

You have been asked to turn off the time access restrictions for a safe.Where is this setting found?

PrivateArkClient  
RestAPl  
PVWA  
Vault

IMG-20231015-WA0013.jpg

What are valid ways to invite vendors using the Remote Access portal? (Choose 2.)

Use the vendor invitation form.  
Call the vendor users and have them scan a QR code  
Use the self-service invitation URL.  
Add the vendors in PVWA and send them their password.  
Contact CyberArk support to help invite the vendors,

IMG-20231015-WA0014.jpg  
PSM-SSH

Match the connection component to the corresponding OS/Function.

| **OS** | **Function** |
| --- | --- |
| PSM-SSH | UNIX |
| PSM-RDP | Windows |
| PSM-WinSCP | NIX File Transfer |
| PSM-SQLPlus | Database |
| PSM-OS390 | Mainframe |

IMG-20231015-WA0015.jpg

The Privileged Access Management solution provides an out-of-the-box target platform to manage SSH keys, called UNIX Via SSH Keys. How are these keys managed?

CyberArk stores Private keys in the Vault and updates Public keys on target systems  
CyberArk stores Public keys in the Vault and updates Private keys on target systems  
CyberArk does not store Public or Private keys and instead uses a reconcile account to create keys on demand  
CyberArk stores both Private and Public keys and can update target systems with either key

IMG-20231015-WA0017.jpg

Your organization has a requirement to allow only one user to "check out passwords" and connect through the PSM securely. What needs to be configured in the Master policy to ensure this will happen?

Enforce check-in/check-out exclusive access = active; Require privileged session monitoring and isolation = active  
Enforce check-in/check-out exclusive access = inactive- Require privileged session monitoring and isolation = inactive  
Enforce check-in/check-out exclusive access = inactive; Record and save session activity = active  
Enforce check-in/check-out exclusive access = active; Record and save session activity = inactive

IMG-20231015-WA0018.jpg

What can you do to ensure each component server is operational?

Logon to PVWA with v10 UI, navigate to Healthcheck and validate each component server is connected to the Vault.  
Ping each component server to ensure connectivity  
Use the PrivateArk client to connect to the Vault server and validate all the services are running  
Install the Vault Server Interface on a remote machine to avoid Interactive logon to the Vault OS and review the ITALog.log through the Vault Server interface.

IMG-20231015-WA0019.jpg

To use PSM connections while in the PVVVA, what are the minimum safe permissions a user or group will need?

List Accounts, Use Accounts  
List Accounts, Use Accounts, Retrieve Accounts  
Use Accounts  
List Accounts, Use Accounts, Retrieve Accounts, Access Safe without confirmation

IMG-20231015-WA0020.jpg

What must you specify when configuring a discovery scan for UNIX? (Choose 2)

Vault Administrator  
CPM Scanner  
root password for each machine  
list of machines to scan  
safe for discovered accounts

IMG-20231015-WA0021.jpg

According to CyberArk, which Issues most commonly cause installed components to display as disconnected in the System Health Dashboard? (Choose 2)

network instabilities!outages  
vault license expiry  
credential de-sync  
browser compatibility issues  
installed location file corruption

IMG-20231015-WA0022.jpg

What does the minvalidity parameter on a platform policy determine?

time between a password retrieval and the account becoming eligible for a password change  
timeout for users signed into the PVWA as configured in the global settings  
minimum amount of time that Just In Time access is valid  
time in minutes before an empty safe ill be automatically deleted

IMG-20231015-WA0023.jpg

Which tools can you use to identify the machines and accounts that create the highest risk and are exposed to lateral movement? (Choose 2)

Accounts Discovery Feed  
CyberArk DNA Report  
REST API scripts  
CyberArk DNA Map  
Get-LocalUser Powershell cmdlet

IMG-20231015-WA0024.jpg

In your organization the "click to connect" button is not active by default. How can this feature be activated?

Policies > Master Policy > Allow EPV transparent connections > Inactive  
Policies > Master Policy— Session Management > Require privileged session monitoring and isolation > Add Exception  
Policies > Master Policy > Allow EPV transparent connections > Active  
Policies > Master Policy > Password Management

IMG-20231015-WA0025.jpg

You are adding a new application in the Remote Access portal. Which authentication methods can you use to authenticate users to the PW/AQ (Choose 2)

Password `  
OpenID  
Certificate  
SAML  
OTP

IMG-20231015-WA0026.jpg

Due to corporate storage constraints, you have been asked to disable session monitoring and recording for 500 testing accounts used for your lab environment. How do you accomplish this?

Master Policy>select Session Management>add Exceptions to the platform(s)>disable Session Monitoring and Recording policies  
Administration>Platform Management>select the platform(s)>disable Session Monitoring and Recording  
Polices>Access Control (Safes)>select the safe(s)>disable Session Monitoring and Recording policies  
Administration>Configuration Options>Optjon9select Privilege Session Management>disable Session Monitoring and Recording policies

IMG-20231015-WA0027.jpg

A password compliance audit found

1. One-time password access of 20 domain accounts that are members of Domain Admins group In Active Directory are not being enforced
2. All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM  
   What should you do to address these findings?

Edit the Master Policy and add two policy exceptions. enable "Enforce one-time password access', enable "Record and save session activity"  
Edit safe properties and add two policy exceptions. enable •Enforce one-time password access", enable "Record and save session activity'  
Edit CPM Settings and add two policy exceptions enable "Enforce one-time password access", enable "Record and save session activity"  
Contact the Windows Administrators and request them to add two policy exceptions at Active Directory Level. enable "Enforce one-time password access", enable "Record and save session activity"

IMG-20231015-WA0028.jpg

A company has multiple business units that have their own set of vendors. Each business unit has a distinct role to manage vendor access. The business units want to have full control over the Invitation process for their set of vendors. After inviting the user to the Remote Access portal, which permissions should be delegated?

Administrator  
Vendor Manager  
Viewer  
User

IMG-20231015-WA0029.jpg

You are running a "Privileged Accounts Inventory" Report through the Reports page in PVWA on a specific safe, To show complete account inventory information, which permission/s are needed on that safe?

List Accounts, View Safe Members  
Manage Safe Owners  
List Accounts, Access Safe without confirmation  
Manage Safe, View Audit

IMG-20231015-WA0030.jpg

Which master policy settings ensure non-repudiation?

Require password verification every X days and enforce one-time password access.  
Enforce check-in/check-out exclusive access and enforce one-time password access.  
Allow EPV transparent connections ('Click to connect') and enforce check-in/check-out exclusive access.  
Allow EPV transparent connections ('Click to connect') and enforce one-time password access.