output-process

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

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

1. PrivateArkClient
2. RestAPl
3. PVWA
4. 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

Q : To use PSM connections while in the PVVVA, what are the minimum safe permissions a user or group will need?  
A: (1) List Accounts, Use Accounts

1. List Accounts, Use Accounts
2. List Accounts, Use Accounts, Retrieve Accounts
3. Use Accounts
4. 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)  
answer : CPM Scanner  
list of machines to scan

Options

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

Q : What does the minvalidity parameter on a platform policy determine?  
A : time between a password retrieval and the account becoming eligible for a password change

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

**Question** : A password compliance audit found

* One-time password access of 20 domain accounts that are members of Domain Admins group In Active Directory are not being enforced
* All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM  
  What should you do to address these findings?  
  **Answer** : (1) Edit the Master Policy and add two policy exceptions. enable "Enforce one-time password access', enable "Record and save session activity"

1. Edit the Master Policy and add two policy exceptions. enable "Enforce one-time password access', enable "Record and save session activity"
2. Edit safe properties and add two policy exceptions. enable •Enforce one-time password access", enable "Record and save session activity'
3. Edit CPM Settings and add two policy exceptions enable "Enforce one-time password access", enable "Record and save session activity"
4. 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.`

IMG-20231015-WA0031.jpg  
You need to identity the most powerful accounts in your organization to prepare for the initial PAM onboarding process. Which tools or features can be used to locate and onboard these accounts? (Choose 2.)

Discovery and Audit (DNA)  
CyberArk's Command Line Interface (PACLI)  
Onboarding and Secure Account Feed  
Accounts Discovery  
Privilege Account Matrix (PAM) XML-based

IMG-20231015-WA0032.jpg  
CyberArk Defender - PAM -

Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?  
Ans : They are added to the Pending Accounts list.

They are added to the Pending Accounts list.  
They cannot be onboarded to the Password Vault.  
They must be uploaded using third party tools.  
They are not part of the Discovery Process.

IMG-20231015-WA0033.jpg  
Q : You are onboarding an account that is not supported out of the box. What should you do first to obtain a platform to import?  
A : Create a service ticket in the customer portal explaining the requirements of the custom platform.

Create a service ticket in the customer portal explaining the requirements of the custom platform.  
Search common community portals like stackoverflow, reddit, github for an existing platform.  
From the platforms page, uncheck the "Hide non-supported platforms" checkbox and see if a platform meeting your needs appears.  
Visit the CyberArk marketplace and search for a platform that meets your needs.

IMG-20231015-WA0034.jpg  
Which item is an option for PSM recording customization?

Windows events text recorder with automatic play-back  
Windows events text recorder and universal keystrokes recording simultaneously  
Universal keystrokes text recorder with windows events text recorder disabled  
Custom audio recording for windows events

IMG-20231015-WA0035.jpg

What are the mandatory fields when onboarding from Pending Accounts? (Choose 2.)

Address  
Safe  
Account Description  
Platform  
CPM

IMG-20231015-WA0036.jpg

Q: Which Vault authorization does a user need to have assigned to able to generate the "Entitlement Report" from the reports page in PVWA? (Choose 2)  
A : (1,2) Manage Users,Audit Users  
Manage Users  
Audit Users  
Read Activity  
View Entitlements  
List Accounts

IMG-20231015-WA0037.jpg

What are the minimum permissions to add multiple accounts from a file when using PWIA bulk-uploadQ (Choose 3.)

add accounts  
rename accounts  
update account content  
update account properties  
view safe members  
add safes

IMG-20231015-WA0038.jpg

A user needs to view recorded sessions through the PVWA. Without giving auditor access, which safes does a user need access to view PSM recordings? (Choose 2)

Recordings safe  
Safe the account is in  
System safe  
PYWAConfiguratjon safe  
Vaultlnternal safe

IMG-20231015-WA0039.jpg  
A user requested access to view a password secured by dual control and IS unsure who to contact to expedite the approval process The Vault Admin has been asked to look at the account and identify who can approve their request. What is the correct location to Identify users or groups who can approve?

PWVA > Administration > Platform Configuration Edit Platform > Ul & Workflow > Dual Control > Approvers  
PVWA Policies > Access Control (Safes) Select the safe > Safe Members > Workflow > Authonze Password Requests  
PVWA> Account List > Edit > Show Advanced Settings Dual Control > Direct Managers  
PrivateArk > Adrntn Tools > Users and Groups Auditors (Group Membership)

IMG-20231015-WA0040.jpg

In PVWA you are attempting to play a recording made of a session by user jsmith. but there is no option to "Fast Forward" within the video, It plays and only allows you to skip between commands instead. You are also unable to download the Video What could be the cause?

Recording is of a PSM for SSH sesston.  
The browser you are using ts out of date and needs an update to be supported  
You do not have the iView Audit" permtsslon on the sate where the account stored.  
You need to update the recorder settings in the platform to enable screen capture every ms or lessons

IMG-20231015-WA0041.jpg  
CyberArk Defender - PAM - Dattatraya B Ingale

You are configuring CyberArk to use TML5 gateways exclusively for PSM connections. In the PVWA, where do you set DefaultConnectionMethod to HTML5?

Options > Privileged Session Management Ul  
Options > Privileged Session Management  
Options > Privileged Session Management Defaults  
Options > Privileged Session Management Interface

IMG-20231015-WA0042.jpg

Match each key to its recommended storage location.

| Key | Storage Location |
| --- | --- |
| Recovery Private Key | Store in a Physical Safe |
| Recovery Public Key | Store in a Hardware Security Module |
| Server Key | Store on the Vault Server Disk Drive |
| SSH Keys | Store in the Vault |

IMG-20231015-WA0043.jpg

Which processes reduce the risk of credential theft? (Choose 2.)

require dual control password access approval  
require password change every X days  
enforce check-in/check-out exclusive access  
enforce one-time password access

IMG-20231015-WA0045.jpg

What are common ways that organizations leverage the CyberArk Blueprint for Identity Security Success? (Choose 3.)

to understand the identity attack chain  
to discover all digital Identities  
to describe the explicit order of operations for Identity Security  
to assess an organization's security posture  
to build an Identity Security roadmap  
to secure their human identities

IMG-20231015-WA0046.jpg

You are creating a shared safe for the help desk. What must be considered regarding the naming convention?

Ensure the naming convention does not exceed 28 characters.  
Combine environments, owners and platforms to minimize the total number of safes created.  
Safe owners should determine the safe name to enable them to easily remember it.  
The word "Safe" cannot be used

IMG-20231015-WA0048.jpg  
You are onboarding 5000 UNIX root accounts for rotation by the CPM. You discover that the CPM is unable to login directly with the root account and will need to use a secondary account. How can this be configured to allow for password management using least privilege?

Configure each CPM to the correct logon account  
Configure each CPM to use the correct reconcile account  
Configure the UNIX platform to use the correct logon account  
Configure the UNIX platform to use the correct reconcile account

IMG-20231015-WA0049.jpg  
Where can you find resources to learn more about the CyberArk Blueprint? (Choose 2)  
CyberArk Blueprint Webpage  
References within the Identity Security Platform  
Product Webinars  
CyberArk University Course

IMG-20231015-WA0050.jpg  
A recently-hired colleague onboarded five new Local Accounts that are used for standalone Windows Servers. After attempting to connect to the servers from PVWA, the colleague noticed that the "Connect" button was greyed out for all five new accounts. What can you do to help your colleague resolve this issue? (Choose 2.)  
ans : - Verify that the address field is populated with an IP or FQDN of each server.

* Verify that the correct PSM connection component appears within account platform settings.

Options

* Verify that the address field is populated with an IP or FQDN of each server.
* Verify that the correct PSM connection component appears within account platform settings.
* Verify that the address field is blank and that the correct PSM connection component appears within account platform settings.
* Notify the Windows Team that created the new accounts that the CyberArk PAM solution is not designed to manage local accounts on Windows Servers.
* Verify that the "Disable automatic management for this account" setting for each account is not enabled.

IMG-20231015-WA0051.jpg  
You receive this error:  
"Error in changepass to user domainuser on domain server[domain].(winRc=5) Access is denied."  
Which could be the cause?

* **A.** The account does not have sufficient permissions to change its own password.
* **B.** The domain controller is unreachable.
* **C.** The password has been changed recently and minimum password age is preventing the change.
* **D.** The CPM service is disabled and will need to be restarted.

IMG-20231015-WA0052.jpg

Which configuration file is used by the CPM scanner when scanning UNIX/Linux devices?

UnixPrompts-ini  
plink-exe  
dbparm-ini  
UnixScannerini

IMG-20231015-WA0053.jpg

Which built-in report from the reports page in PVWA displays the number of days until a password is due to expire?

Privileged Accounts Inventory  
Pnvileged Accounts Compliance Status  
Activity Log  
Privileged Accounts CPM Status

IMG-20231015-WA0054.jpg  
What is the easiest way to duplicate an existing platform?

* **A.** From PrivateArk, copy/paste the appropriate Policy.ini file, then rename it.
* **B.** From the PWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform and then click Duplicate, name the new platform.
* **C.** From PrivateArk, copy/paste the appropriate settings in PVConfiguration.xml, then update the policyName variable.
* **D.** From the PWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform, manually update the platform settings and click "Save as" INSTEAD of save to duplicate and rename the platform.

IMG-20231015-WA0055.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-WA0056.jpg  
What are common ways that organizations leverage the CyberArk Blueprint tor identity Security Success? (choose 3)

to understand the identity attack chain  
to discover all digital identities  
to describe the explicit order of operations for Identity Security  
to assess an organization's security posture  
to build an Identity Security roadmap  
to secure their human identities

IMG-20231015-WA0057.jpg

Which CyberArk utility allows you to create lists of Master Policy Settings, owners and safes for output to .txt files or MSSQL databases?

Export Vault Data  
Export Vault Information  
PrivateArk Client  
Privileged Threat Analytics

IMG-20231015-WA0058.jpg

**In PWA, you are attempting to play a recording made of a session by user jsmith, but there is no option to fast forward within the video. It plays and only allows you to skip between commands instead. You are also unable to download the video. What could be the cause?**

* **A.** Recording is of a PSM for SSH session.
* **B.** The browser you are using is out of date and needs an update to be supported.
* **C.** You do not have the "View Audit" permission on the safe where the account is stored.
* **D.** You need to update the recorder settings in the platform to enable screen capture every 10000 ms or less.

IMG-20231015-WA0059.jpg  
You need to enable the PSM for all platforms. Where do you perform this task?

Platform Management > (Platform) > Ul & Workflows  
Master Policy > Session Management  
Master Policy > Privileged Access  
Administration > Options > Connection Components

IMG-20231015-WA0060.jpg  
Q: When the CPM connects to a database, which interface is most commonly used?  
A : (2) ODBC

1. Kerberos
2. ODBC
3. VBScript
4. Sybase

IMG-20231015-WA0061.jpg

question : What is the correct process to install a custom platform from the CyberArk Marketplace?  
ans : Download the platform from the Marketplace and import it using fhe PVWA

Locate the custom platform in the Marketplace and click Import  
Download the platform from the Marketplace and import it using fhe PVWA  
Contact CyberArk Suppart for guidance on how to import the platform  
Duplicate an existing platform and align the setting to match the platform from the Marketplace

IMG-20231015-WA0062.jpg

How do you create a cold storage backup?

On the DR Vault, install PAReplicate.exe according to the Installation guide, configure the logon Ini file, and define the Schedule tasks for full and Incremental backups.  
Install the Vault Backup utility on a different machine from the Enterprise Password Vault server and tngger the full backup  
Configure the backup options in the PVWA  
On the DR Vault, configure the cold storage backup path In TSParm.ini file,

IMG-20231015-WA0063.jpg  
Q : To manage automated onboarding rules, a CyberArk user must be a member ot which groups?  
Ans : Vault Admins

Vault Admins  
PasswordManagers  
Auditors  
Administrators

IMG-20231015-WA0064.jpg

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

Logon to PWVA with 10th v1O Ul, navigate to Healthcheck, and validate each component server IS connected to the Vault  
Ping each component server to ensure connectivity.  
Use the PnvateArk 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 renew the ITALOG.log through the vault server interface.

IMG-20231015-WA0065.jpg  
You want to create a new onboarding rule. Where do you accomplish this?

In PVWA, click Reports > Unmanaged Accounts > Rules  
In PVWA, click Options > Platform Management > Onboarding Rules  
In PrivateArk, click Tools > Onboarding Rules  
In PVWA7 click Accounts > Onboarding Rules

IMG-20231015-WA0066.jpg  
Q: When onboarding multiple accounts from the Pending Accounts list, which associated setting must be the same across the selected accounts?  
A : Platform

Platform  
Connection Component  
CPM  
Vault

IMG-20231015-WA0067.jpg  
Which tools can you use to identify the machines and accounts that create the highest risk and are exposed to lateral movement?

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

IMG-20231015-WA0068.jpg

**You have been asked to secure a set of shared accounts in CyberArk whose passwords will need to be used by end users. The account owner wants to be able to track who was using an account at any given moment. Which security configuration should you recommend?**  
Ans : Configure both one-time passwords and exclusive access for the appropriate platform in Master Policy.

* **A.** Configure one-time passwords for the appropriate platform in Master Policy.
* **B.** Configure shared account mode on the appropriate safe.
* **C.** Configure both one-time passwords and exclusive access for the appropriate platform in Master Policy.
* **D.** Configure object level access control on the appropriate safe.

IMG-20231015-WA0069.jpg

Which processes reduce the risk of credential theft (Choose 2)

require dual control password access approval  
require password change every X days  
enforce check-in/checkout exclusive access  
enforce one-time password access

IMG-20231015-WA0070.jpg

Which setting in the Master Policy controls whether PSM is enabled and sessions will be recorded?

Require privileged session monitoring and isolation = inactive; Record and save session activity = active  
Require privileged session monitoring and isolation = inactive; Record and save session activity = inactive  
Require privileged session monitoring and isolation = active; Record and save session activity = active  
Require privileged session monitoring and isolation = active; Record and save session activity = inactive

IMG-20231015-WA0071.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 Tme access is valid  
time in minutes before an empty safe will be automatically deleted

IMG-20231015-WA0072.jpg

To change the safe where recordings are kept for a specific platform, which setting must you update in the platform configuration?

SessionRecorderSafe  
SessionSafe  
RecordingsPath  
RecordingLocatjon

IMG-20231015-WA0073.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?**

* **A.** Administrator
* **B.** User
* **C.** Vendor Manager
* **D.** Viewer

IMG-20231015-WA0074.jpg  
Q : Which usage can be added as a service account platform?  
A : IISApplication Pools  
KerberosTokens  
IISApplication Pools  
PowerShell Libraries  
LooselyConnected Devices

IMG-20231015-WA0075.jpg  
When an account is unable to change its own password, how can you ensure that password reset with the reconcile account is performed each time instead of a change?

Set the parameter RCAllowManualReconciliaüon to Yes.  
Set the parameter ChangePasswordlnResetMode to Yes.  
Set the parameter IgnoreReconcileOnMissingAccount to No.  
Set the UnlockUserOnReconcile to Yes.

IMG-20231015-WA0076.jpg  
You are adding a new application in the Remote Access portal. Which authentication methods can you use to authenticate users to the PWIAQ (Choose 2)

Password  
OpenID  
Certificate  
SAML  
OTP

IMG-20231015-WA0077.jpg

You need to identity the most powerful accounts in your organization to prepare for the Initial PAM onboarding process. Which tools or features can be used to locate and onboard these accounts? (Choose 2)

Discovery and Audit (DNA)  
CyberArk's Command Line Interface (PACLI)  
Onboarding and Secure Account Feed  
Accounts Discovery  
Pnvllege Account Matnx (PAM) XLS

IMG-20231015-WA0078.jpg

Which Vault authorizatlon does a user need to have assigned to able to generate the "Entitlement Report". from the reports page in PVWA? (choose 2)

Manage Users  
Audit Users  
Read Activity  
View Entitlements  
List Accounts

IMG-20231015-WA0079.jpg  
You have been given the requirement that certain accounts cannot have their passwords updated during business hours. How can you set up a configuration to meet this requirement?

Change settings on the CPM configuration safe so that access is permitted after business hours only.  
Update the password change parameters of the platform to match the permitted time frame.  
Disable automatic CPM management for all accounts that are assigned to this plafform.  
Add an exception to the Master Policy to allow the action for this platform during the permitted time.

IMG-20231015-WA0080.jpg

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-WA0081.jpg

When should vault keys be rotated?  
ans : when it is copied to file systems outside the vault

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

IMG-20231015-WA0082.jpg

**Which statement about the Master Policy best describes the differences between one-time password and exclusive access functionality?**

* **A.** Exclusive access means that only a specific group of users may use the account. After an account on a one-time password platform is used, the account is deleted from the safe automatically.
* **B.** Exclusive access locks the account indefinitely. One-time password can be used replace invalid account passwords.
* **C.** Exclusive access is enabled by default in the Master Policy. One-time password should only be enabled for emergencies.
* **D.** Exclusive access allows only one person to check-out an account at a time. One-time password schedules an account for a password change after the MinValidityPeriod period expires.

IMG-20231015-WA0084.jpg

The Active Directory User configured for Windows Discovery needs which permission(s) or membership?

Member of Domain Admin Group  
Member of LDAP Admin Group  
Read and Write Permissions  
Read Only Permissions

IMG-20231015-WA0085.jpg

**Which authorizations are required in a recording safe to allow a group to view recordings?**

| **Authorizations** | **Status** (select the right option) |
| --- | --- |
| Retrieve accounts/files | Required/Not Required |
| List accounts/files | Required/Not Required |
| View audit | Required/Not Required |
| Access Safe without confirmation | Required/Not Required |
| Create Folders | Required/Not Required |

IMG-20231015-WA0086.jpg

A new HTML5 Gateway has been deployed in your organization.  
From the PVWA, arrange the steps to configure a PSM host to use the HTML5 Gateway in the correct sequence.

**Unordered Options**

Administration>Options  
Privileged Session Management  
Configured PSM Servers and select existing PSM  
host  
Connection Details  
Add PSM gateway

IMG-20231015-WA0087.jpg

Which item is an option for PSM recording customization?

Windows events text recorder with automatic play-back  
Windows events text recorder and universal keystrokes recording simultaneous  
Universal keystrokes text recorder with windows events text recorder disabled  
Custom audio recording for windows events

IMG-20231015-WA0088.jpg  
F

Shdepoa  
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-WA0089.jpg

Where can you assign a Reconcile account? (Choose 2 }

in PVWA at the account level  
in PVWA in the platform configuration  
in the Master policy of the PVVVA  
at the Safe level  
in the CPM settings

IMG-20231015-WA0090.jpg

What are the minimum permissions to add multiple accounts from a file when using PVWA bulk-upload?

add accounts  
rename accounts  
update account content  
update account properties  
view safe members  
add safes

IMG-20231015-WA0091.jpg  
Where can you find resources to learn more about the CyberArk blueprint? (choose 2)  
CyberArk blueprint webpage  
references with the identity security platform  
product webinars  
CyberArk university course

IMG-20231015-WA0092.jpg

In a default CyberArk installation, which group must a user be a member of to view the "reports" page in PVWA?

PVWAMonitor  
ReportUsers  
PVWAReports  
Operators

IMG-20231015-WA0093.jpg

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

OS Usemame  
Current machine IP  
Current machine hostname  
Operating System Type (LinuxIWindows/HP-UX)  
Vault IP Address  
Time Frame

IMG-20231015-WA0094.jpg

You are concerned about the Windows Domain password changes occur Q during business hours. Which settings must be updated to ensure passwords are only rotated outside of business hours?

In the platform policy > Automatic Password Management > Password Change > ToHour & FromHour  
In the Master Policy > Account Change Window > ToHour & From Hour  
Administration Settings > CPM Settings > ToHour & FromHour  
On each individual account > Edit > Advanced > ToHour & FromHour

#todo #later  
WhatsApp Image 2023-10-15 at 11.01.27\_14ffa2af.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?

OA Enforce check-in'check-out exclusive access = active, Require privileged session monitor ng and isolation = active

0B. Enforce check-in‘check-out exclusive access =

mactive: Require privileged session monitoring and isolation = inactive

OC. Enforce check-inicheck-out exclusive access = inactive, Record and save session activity = active

oD. Enforce check-in/check-out exclusive access = active, Record and save session activity = active

WhatsApp Image 2023-10-15 at 11.01.27\_5bf82ef3.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

WhatsApp Image 2023-10-15 at 11.01.27\_ea51b6cf.jpg  
Privileged Access Management solution provides an out4Df-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