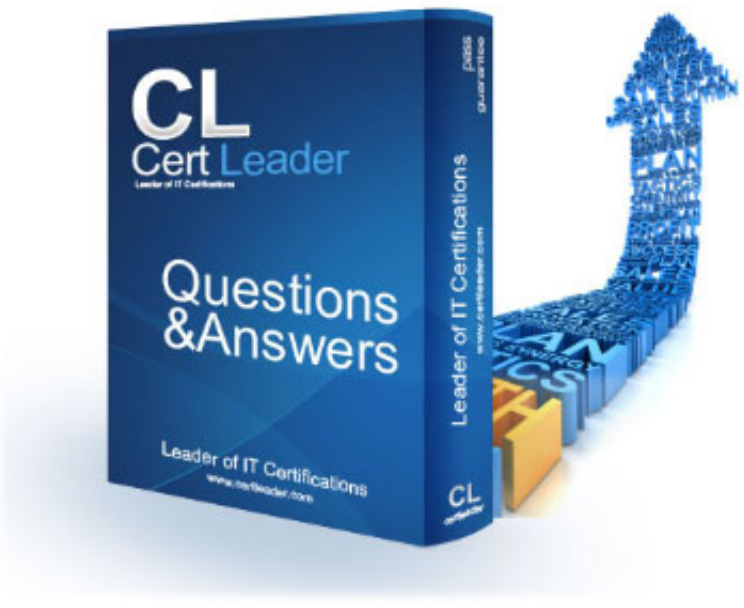
PAM-DEF Dumps

CyberArk Defender - PAM

https://www.certleader.com/PAM-DEF-dumps.html



NEW QUESTION 1
Which of the Following can be configured in the Master Poky? Choose all that apply.

A. Dual Control
B. One Time Passwords
C. Exclusive Passwords
D. Password Reconciliation
E. Ticketing Integration
F. Required Properties
G. Custom Connection Components
H. Password Aging Rules

Answer: ABCH

Explanation:
The Master Policy is a centralized overview of the security and compliance policy of privileged accounts in the organization. It allows the administrator to configure compliance driven rules that are defined as the baseline for the enterprise. The Master Policy includes the following main concepts1:
? Basic policy rules: These rules allow the administrator to define specific aspects of privileged account management, such as privileged access workflows, password management, session monitoring and auditing.
? Advanced policy rules: Some basic policy rules have related advanced settings that provide more granular control over the policy enforcement.
? Exceptions: These are policy rules that differ from the overall Master Policy for a specific scope of accounts, such as accounts associated with a specific platform.
The Master Policy rules are divided into four sections2:
? Privileged Access Workflows: These rules define how the organization manages access to privileged accounts, such as requiring dual control, one-time passwords, exclusive passwords, transparent connections, reason for access, etc.
? Password Management: These rules determine how passwords are managed, such as requiring password change, password verification, password reconciliation, ticketing integration, required properties, custom connection components, etc.
? Session Management: These rules determine whether or not privileged sessions are recorded and how they are monitored, such as requiring session isolation, session recording, session audit, etc.
? Audit: This rule determines how Safe audits are retained, such as specifying the audit retention period.
Based on the above information, the following options can be configured in the Master Policy:
? A. Dual Control: This is a basic policy rule in the Privileged Access Workflows
section that determines whether users need to get approval from authorized users before accessing a privileged account2.
? B. One Time Passwords: This is a basic policy rule in the Privileged Access
Workflows section that determines whether users can only use a password once before it is changed2.
? C. Exclusive Passwords: This is a basic policy rule in the Privileged Access
Workflows section that determines whether users need to check out a password and prevent other users from accessing it until it is checked in2.
? H. Password Aging Rules: This is a basic policy rule in the Password Management
section that determines how often passwords need to be changed2. The following options cannot be configured in the Master Policy:
? D. Password Reconciliation: This is not a policy rule, but a process that restores
the password of a privileged account to the value that is stored in the Vault, in case it is changed or out of sync3.
? E. Ticketing Integration: This is not a policy rule, but a feature that enables the
integration of the Vault with external ticketing systems, such as ServiceNow, Jira, etc.
? F. Required Properties: This is not a policy rule, but a platform setting that determines which properties are mandatory for adding accounts to a platform.
? G. Custom Connection Components: This is not a policy rule, but a platform setting that determines which connection components are used to connect to target systems, such as PVWA, PSM, PSMP, etc.
References:
? 1: The Master Policy
? 2: Master Policy Rules
? 3: Password Reconciliation
? : Ticketing Integration
? : Required Properties
? : Custom Connection Components

NEW QUESTION 2
Which keys are required to be present in order to start the PrivateArk Server service?

A. Recovery public key
B. Recovery private key
C. Server key
D. Safe key

Answer: AC

Explanation:
The server key and the public recovery key are required to be present in order to start the PrivateArk Server service. The server key opens the Vault, much like the key of a physical Vault. The public recovery key is part of the asymmetric recovery key that enables the Master User to log on to the Vault in case of a disaster. The server key and the public recovery key are usually stored on a removable media, such as a disk or CD, so that they can be safely secured in a physical safe. The recovery private key and the safe key are not needed to start the PrivateArk Server service. The recovery private key is only used for recovery purposes and the safe key is only used to access a specific safe that is defined with an external key. References: Server keys, Server Components

NEW QUESTION 3
Which option in the Private Ark client is used to update users' Vault group memberships?

A. Update > General tab
B. Update > Authorizations tab
C. Update > Member Of tab
D. Update > Group tab

Answer: C

Explanation:
In the Private Ark client, to update users' Vault group memberships, you use the Update > Member Of tab. This tab allows administrators to manage which groups a user is a member of. By adding or removing groups in this tab, you can effectively update the user's group memberships and, consequently, their access permissions within the Vault1.
References:
? CyberArk's official documentation on managing users in the Private Ark client, which includes instructions on how to update users' group memberships

NEW QUESTION 4
A new HTML5 Gateway has been deployed in your organization. Where do you configure the PSM to use the HTML5 Gateway?

A. Administration > Options > Privileged Session Management > Configured PSM Servers> Connection Details > Add PSM Gateway
B. Administration > Options > Privileged Session Management > Add Configured PSMGateway Servers
C. Administration > Options > Privileged Session Management > Configured PSM Servers> Add PSM Gateway
D. Administration > Options > Privileged Session Management > Configured PSM Servers> Connection Details

Answer: C

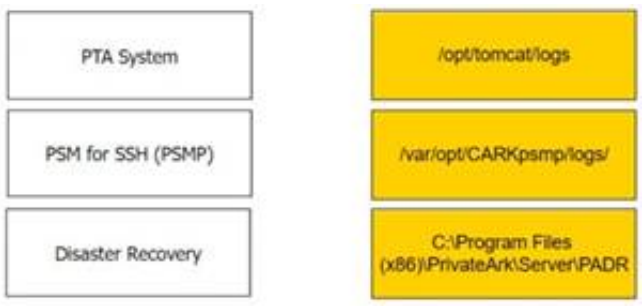
Explanation:
After deploying a new HTML5 Gateway in your organization, you configure the PSM to use the HTML5 Gateway by navigating to the Administration section in the PVWA. From there, you go to Options, then Privileged Session Management, and under Configured PSM Servers, you will find the option to Add PSM Gateway1. This is where you can specify the details of the newly deployed HTML5 Gateway to ensure that the PSM can utilize it for secure remote access to target machines through an HTML5-based session. References:
? CyberArk's official documentation provides a step-by-step guide on how to install and configure the PSM HTML5 Gateway, including the process of adding the gateway to the PSM configuration1.
? For more detailed instructions and best practices on configuring the PSM with an HTML5 Gateway, refer to the CyberArk Defender PAM course materials and study guides

NEW QUESTION 5
DRAG DROP
Match each component to its respective Log File location.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Comprehensive explanation: The log file locations for each component in CyberArk's Privileged Access Management (PAM) are specific to the function and operation of that component. The PTA System logs are typically found in the PrivateArk Server directory, specifically in the PADR folder. The PSM for SSH, which is the Privileged Session Manager for SSH, stores its logs in the tomcat logs directory. Lastly, the logs for Disaster Recovery operations are located in the CARKsymop logs directory on a Linux-based system. References: The information is based on the CyberArk documentation and best practices for managing and maintaining log files for different components within the PAM solution123. The log file locations are essential for troubleshooting and auditing purposes, ensuring that all activities and changes are properly recorded and can be reviewed when necessary.

NEW QUESTION 6
What is the purpose of the PrivateArk Database service?

A. Communicates with components
B. Sends email alerts from the Vault
C. Executes password changes
D. Maintains Vault metadata

Answer: D

Explanation:
The purpose of the PrivateArk Database service is to maintain the Vault metadata, which includes the information about the Safes, accounts, policies, users, groups, and audit records that are stored in the Vault. The PrivateArk Database service is a Windows service that manages the database files that contain the Vault data. The PrivateArk Database service is responsible for creating, updating, deleting, and backing up the database files, as well as performing encryption and compression operations on the data1. The PrivateArk Database service is installed automatically as part of the Vault server installation and can be configured using the DBParm.ini file2.
The other options are not the purpose of the PrivateArk Database service, although they may be related to other services or components of the Vault. The

PrivateArk Server service is the service that communicates with the components, such as the PVWA, the CPM, the PSM, and the PTA, and handles the requests from the clients and components3. The Event Notification Engine service is the service that sends email alerts from the Vault, based on predefined events and recipients4. The Central Policy Manager component is the component that executes password changes, verifications, and reconciliations for the accounts that are managed by the Vault. References:
? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
? DBParm.ini - CyberArk, section “Main parameters”
? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
? Event Notification Engine - CyberArk, section “Event Notification Engine”
? [Change Passwords - CyberArk], section “Change Passwords”

NEW QUESTION 7
As long as you are a member of the Vault Admins group you can grant any permission on any safe.

A. TRUE
B. FALSE

Answer: B

Explanation:
The Vault Admins group is a predefined group that is automatically created during the installation or upgrade of the Vault. This group has all possible permissions in the Vault, and can create and manage other users, groups, platforms, policies, safes, and accounts. However, this group is not automatically added to every safe in the Vault, but only to some system safes that are used for administrative purposes. Therefore, being a member of the Vault Admins group does not guarantee that you can grant any permission on any safe, unless you are also a member or an owner of that safe. To grant permissions on a safe, you need to have the Authorize safe members authorization on that safe, which allows you to add or remove users or groups as safe members, and assign or revoke their authorizations. Alternatively, you can use the Administrator user, which is a predefined user that is a member of the Vault Admins group, and has all possible permissions on any safe in the Vault. References:
? Predefined users and groups
? Safe member authorizations

NEW QUESTION 8
You want to give a newly-created group rights to review security events under the Security pane. You also want to be able to update the status of these events. Where must you update the group to allow this?

A. in the PTAAuthorizationGroups parameter, found in Administration > Options > PTA
B. in the PTAAuthorizationGroups parameter, found in Administration > Options > General
C. in the SecurityEventsAuthorizationGroups parameter, found in Administration > Security> Options
D. in the SecurityEventsFeedAuthorizationGroups parameter, found in Administration > Options > General

Answer: D

Explanation:
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security- Events.htm?TocPath=End%20User%7CSecurity%20Events%7C2#Permissions

NEW QUESTION 9
Which usage can be added as a service account platform?

A. Kerberos Tokens
B. IIS Application Pools
C. PowerShell Libraries
D. Loosely Connected Devices

Answer: B

Explanation:
A service account platform is a type of platform that defines how CyberArk manages passwords for service accounts, which are accounts that run applications or services on remote machines. A usage is a configuration that allows CyberArk to manage passwords for files, such as XML or INI files, that are stored on remote machines. A usage is associated with a parent account, which is the account that has access to the file. A usage can be added as a service account platform if the file contains the password of a service account. For example, IIS Application Pools is a usage that can be added as a service account platform, because it manages the passwords of the application pools that run on IIS servers. The other options, Kerberos Tokens, PowerShell Libraries, and Loosely Connected Devices, are not usages that can be added as service account platforms, because they do not manage passwords for service accounts. References: Usages, Service Account Platforms

NEW QUESTION 10
When are external vault users and groups synchronized by default?

A. They are synchronized once every 24 hours between 1 AM and 5 A
B. Most Voted
C. They are synchronized once every 24 hours between 7 PM and 12 AM.
D. They are synchronized every 2 hours.
E. They are not synchronized according to a specific schedule.

Answer: A

Explanation:
By default, external vault users and groups are synchronized once every 24 hours between 1 AM and 5 AM. This synchronization schedule is determined by the AutoSyncExternalObjects parameter in the DBParm.ini file, which specifies that the Vault’s external users and groups will be synchronized with the External Directory during this time frame1.
References:

? CyberArk Docs - Synchronize External Users and Groups in the Vault with the External Directory

NEW QUESTION 10
Target account platforms can be restricted to accounts that are stored m specific Safes using the Allowed Safes property.

A. TRUE
B. FALSE

Answer: A

Explanation:
Target account platforms can be restricted to accounts that are stored in specific Safes using the Allowed Safes property. This property is a parameter that can be configured in the Platform Management settings for each platform. The Allowed Safes property specifies the name or names of the Safes where the platform can be applied. The default value is .*, which means that the platform can be used in any Safe. However, if you want to limit the platform to certain Safes, you can enter the name or names of the Safes, separated by a pipe (|) character. For example, if you want to restrict the platform to Safes called WindowsPasswords and LinuxPasswords, you can enter AllowedSafes=(WindowsPasswords)|(LinuxPasswords). This feature is useful for preventing unauthorized users from accessing passwords, especially if you implement the reconciliation functionality. It also helps the CPM to focus its search operations on specific Safes, instead of scanning all Safes it can see in the Vault1. References:
? 1: Limit Platforms to Specific Safes

NEW QUESTION 14
DRAG DROP
Match each key to its recommended storage location.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? The recommended storage locations for each key are as follows:
? Recovery Private Key: It is recommended to store the Recovery Private Key on the Vault Server Disk Drive. This is because the Recovery Private Key is used to decrypt the data stored in the Vault.
? Recovery Public Key: It is recommended to store the Recovery Public Key in a Hardware Security Module. This is because the Recovery Public Key is used to encrypt the data stored in the Vault.
? Server Key: It is recommended to store the Server Key in a Physical Safe. This is because the Server Key is used to open the Vault, much like the key of a physical Vault. The key is required to start the Vault, after which the Server Key can be removed until the Server is restarted. When the Vault is stopped, the information stored in the Vault is completely inaccessible without that key.
? SSH Keys: It is recommended to store the SSH Keys in the Vault. This is because the SSH Keys are used to connect to remote machines using the SSH protocol. The Vault can manage the passwords and sessions for the SSH Keys and provide secure access to the target systems.
References: Server keys - CyberArk, Cyberark Key Storage Plugin (Enterprise) - Rundeck

NEW QUESTION 15
It is possible to restrict the time of day, or day of week that a [b]verify[/b] process can occur

A. TRUE
B. FALSE

Answer: A

Explanation:
It is possible to restrict the time of day, or day of week that a verify process can occur by using the Verify Time Window parameter in thePlatform Management page. This parameter allows the administrator to define a time window for each platform, during which the verify process can be performed. The verify process will not run outside of this time window, unless it is manually initiated by the administrator. This feature can help reduce the load on the target systems and the network during peak hours. References:
? [Defender PAM Course], Module 4: Managing Accounts, Lesson 2: Account Verification, Slide 8: Verify Time Window
? [Defender PAM Documentation], Version 12.3, Administration Guide, Chapter 4: Managing Platforms, Section: Verify Time Window

NEW QUESTION 20
When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.

A. True; this is the default behavior
B. False, the Vault administrator must manually set the DR Vault to DR mode by setting “FailoverMode=no” in the padr.ini file
C. True, if the AllowFailback setting is set to “yes” in the padr.ini file
D. False, the Vault administrator must manually set the DR Vault to DR mode by setting “FailoverMode=no” in the dbparm.ini file

Answer: B

Explanation:
According to the web search results, when a DR Vault Server becomes an active vault, it will not automatically revert back to DR mode once the Primary Vault comes back online. The Vault administrator must manually set the DR Vault to DR mode by setting “FailoverMode=no” in the padr.ini file1. This file is located in the /opt/CARKaim/conf directory on the DR Vault machine2. The Vault administrator must also stop the replication process on the DR Vault and restart the PrivateArk Server service1. This procedure is known as a DR failback, which restores the original roles of the Primary Vault and the DR Vault after a failover1. The AllowFailback setting in the padr.ini file does not affect the DR failback process, as it only determines whether the DR Vault can be used as a backup for another DR Vault in a cascading DR scenario3. The dbparm.ini file is not relevant for the DR failback process, as it contains the database parameters for the Vault server.
References:
? Initiate a DR failback to the Production Vault - CyberArk
? Install the Disaster Recovery application - CyberArk
? Cascading DR - CyberArk
? [dbparm.ini file - CyberArk]

NEW QUESTION 22
CyberArk implements license limits by controlling the number and types of users that can be provisioned in the vault.

A. TRUE
B. FALSE

Answer: B

Explanation:
CyberArk does not implement license limits by controlling the number and types of users that can be provisioned in the vault. CyberArk implements license limits by controlling the number and types of users that can authenticate to the vault and use its features. The license limits are based on the user types and objects that are defined in the vault, such as Vault Users, LDAP Users, LDAP Groups, Safes, Accounts, etc. The license limits are enforced by the License Manager, which is a service that runs on the Vault server and monitors the license usage. The License Manager can send notifications and alerts when the license usage reaches certain thresholds, and can also block or allow access to the vault based on the license status1.
References:
? 1: Manage the CyberArk License

NEW QUESTION 24
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 two.)

A. Recordings safe
B. Safe the account is in
C. System safe
D. PVWAConfiguration safe
E. VaultInternal safe

Answer: AB

Explanation:
To view recorded sessions through the PVWA without having auditor access, a user needs access to two specific safes: the Recordings safe and thesafe the account is in. The Recordings safe is where the PSM session recordings are stored, and users need permission to access this safe to view the recordings. Additionally, users need access to the safe where the account associated with the recorded session is stored, as this is where the session details and permissions are managed12.
References:
? CyberArk Docs - Configure video and text recordings3
? CyberArk Community - Viewing PSM recorded sessions1

NEW QUESTION 29
An auditor needs to login to the PSM in order to live monitor an active session. Which user ID is used to establish the RDP connection to the PSM server?

A. PSMConnect
B. PSMMaster
C. PSMGwUser
D. PSMAdminConnect

Answer: A

Explanation:
The PSMConnect user is a local user on the PSM server that is used to establish RDP connections to the PSM server. The PSMConnect user has the following permissions: Log on locally, Log on as a batch job, and Allow log on through Remote Desktop Services. The PSMConnect user is also a member of the local group PSMUsers, which has access to the PSM web console. The other user IDs are not used for RDP connections to the PSM server. The PSMMaster user is a local user on the PSM server that is used to run the PSM services. The PSMGwUser user is a local user on the PSM server that is used to run the PSM Gateway service. The PSMAdminConnect user is a local user on the PSM server that is used to connect to the PSM web console as an administrator. References: Privileged Session Manager, Defender - PAM, PSM for Web Console, Connect through PSM for SSH

NEW QUESTION 30
Before failing back to the production infrastructure after a DR exercise, what must you do to maintain audit history during the DR event?

A. Ensure that the Production Instance replicates changes that occurred from the Disaster Recovery Instance.
B. Briefly stop and start the Disaster Recovery Instance before attempting to fail components back to the Production Instance.
C. Stop the CPM services before starting the production server.
D. Perform an IIS Reset on all PVWA servers.

Answer: A

Explanation:
Before failing back to the production infrastructure after a Disaster Recovery (DR) exercise, it is crucial to ensure that the Production Instance replicates all changes that occurred from the Disaster Recovery Instance. This includes all audit history and any other changes made during the DR event. The replication process ensures that no data is lost and that the audit history is maintained consistently across both the DR and Production environments1.
References:
? CyberArk Docs - Reports and Audits1
? CyberArk Docs - Vault Audit Action Codes2
? CyberArk Blog - Failover and Failback Process

NEW QUESTION 34
A Logon Account can be specified in the Master Policy.

A. TRUE
B. FALSE

Answer: B

Explanation:
A Logon Account cannot be specified in the Master Policy. The Master Policy is a set of rules that define the security and compliance policy of privileged accounts in the organization, such as access workflows, password management, session monitoring, and auditing1. The Master Policy does not include any technical settings that determine how the system manages accounts on various platforms1. A Logon Account is a technical setting that defines the account that the CPM uses to log on to a target system and perform password management tasks, such as changing, verifying, or reconciling passwords2. A Logon Account can be specified in the Platform Management settings, which are configured by the IT administrator for each platform2. The Platform Management settings are independent of the Master Policy and can be customized according to the organization's environment and security policies1. References:
? The Master Policy
? [Platform Management]

NEW QUESTION 39
What is the maximum number of levels of authorization you can set up in Dual Control?

A. 1
B. 2
C. 3
D. 4

Answer: B

Explanation:
Dual Control is a feature that allows you to set up a workflow for approving access requests to sensitive accounts. You can configure up to two levels of authorization for each account, meaning that you need up to two different authorizers to approve the request before the user can access the account. The authorizers can be either users or groups, and they can have different approval methods, such as email, SMS, or CyberArk interface. References:
? [Defender PAM] course, Module 5: Privileged Session Management, Lesson 5.2:
Dual Control
? [Defender PAM Sample Items Study Guide], Question 31
? [CyberArk Documentation], Dual Control

NEW QUESTION 43
A Vault administrator have associated a logon account to one of their Unix root accounts in
the vault. When attempting to verify the root account's password the Central Policy Manager (CPM) will:

A. ignore the logon account and attempt to log in as root
B. prompt the end user with a dialog box asking for the login account to use
C. log in first with the logon account, then run the SU command to log in as root using the password in the Vault
D. none of these

Answer: C

Explanation:
According to the web search results, when a Vault administrator has associated a logon account to one of their Unix root accounts in the vault, the CPM will log in first with the logon account, then run the SU command to log in as root using the password in the Vault1. This is a common use case for using a logon account, as the best practice for Unix systems is to disallow the root user from logging in using SSH, which is what the CPM uses to sign in to a system to manage the password2. The logon account can be defined on the target account level or on the platform level, making it available to all
accounts associated with the platform2. The CPM can also use the logon account to initiate PSM sessions to the target machine3.

NEW QUESTION 48
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 PVWA, 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 PVWA, 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.

Answer: B

Explanation:
The easiest way to duplicate an existing platform is to use the PVWA, which is the web interface that allows users to access and manage the CyberArk Defender PAM system. The PVWA has a platforms page that displays all the platforms that are available in the system, categorized by platform types. Users can duplicate

an existing platform by selecting it, clicking the ellipsis button next to it, and then clicking Duplicate. This will create a copy of the platform with the same settings and properties, which can be customized according to the user's needs. Users can name the new platform and save it in the system.
References: Manage platforms - CyberArk

NEW QUESTION 50
What is the configuration file used by the CPM scanner when scanning UNIX/Linux devices?

A. UnixPrompts.ini
B. plink.exe
C. dbparm.ini
D. PVConfig.xml

Answer: A

Explanation:
The configuration file used by the CPM scanner when scanning UNIX/Linux devices is UnixPrompts.ini. This file is located in the CPM scanner installation folder and can be customized according to the UNIX/Linux machine's specific configuration. The file contains parameters that define the prompts and paths for various commands and files used by the CPM scanner, such as login password, sudo password, sudo error, passwd file, group file, shadow file, and sudoers file.
References: Configure the CPM
Scanner, CPM Scanner parameters file (CACPMScanner.exe.config)

NEW QUESTION 53
For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure a group of users to access a password without approval.

A. Create an exception to the Master Policy to exclude the group from the workflow process.
B. Edith the master policy rule and modify the advanced' Access safe without approval' rule to include the group.
C. On the safe in which the account is stored grant the group the' Access safe without audit' authorization.
D. On the safe in which the account is stored grant the group the' Access safe without confirmation' authorization.

Answer: D

Explanation:
Dual Control is a feature that requires the approval of another user before accessing a password. It is based on a Master Policy rule that applies to all accounts attached to platforms that have this rule enabled. However, there may be situations where a group of users needs to access a password without approval, such as in an emergency or for troubleshooting purposes. In this case, an exception can be made by granting the group the 'Access safe without confirmation' authorization on the safe in which the account is stored. This authorization bypasses the Dual Control workflow and allows the group to retrieve the password without waiting for approval. However, the password retrieval will still be audited and recorded in the Vault.

NEW QUESTION 58
Which CyberArk utility allows you to create lists of Master Policy Settings, owners and safes for output to text files or MSSQL databases?

A. Export Vault Data
B. Export Vault Information
C. PrivateArk Client
D. Privileged Threat Analytics

Answer: B

Explanation:
The Export Vault Information utility is a CyberArk tool that allows you to create lists of Master Policy settings, owners and safes for output to text files or MSSQL databases. This utility can be used to export various types of information from the Vault, such as accounts, safes, platforms, policies, users, groups, and audit records. The utility can also generate reports based on predefined templates or custom queries. The utility can be run from the command line or the graphical user interface. References: Export Vault Information, Export Vault Information Utility

NEW QUESTION 60
It is possible to restrict the time of day, or day of week that a [b]reconcile[/b] process can occur

A. TRUE
B. FALSE

Answer: A

Explanation:
It is possible to restrict the time of day, or day of week that a reconcile process can occur by using the Reconcile Safe option in thePlatform Management section of thePrivateArk Client. This option allows the administrator to define the reconcile schedule for each platform, which specifies when the reconcile process can run and how often it should be performed. The reconcile schedule can be set to run daily, weekly, monthly, or on specific days and times. By restricting the reconcile process, the administrator can reduce the risk of unauthorized access to the accounts and improve the performance of the system. References:
? [Defender PAM Course], Module 5: Reconcile and Rotate, Lesson 1: Reconcile and Rotate Overview, Slide 9: Reconcile Safe
? [Defender PAM Study Guide], Section 5.1: Reconcile and Rotate Overview, Page 24: Reconcile Safe
? [CyberArk Documentation], Privileged Access Security Implementation Guide, Chapter 5: Configure the Vault, Section 5.4: Configure Platforms, Subsection 5.4.2: Reconcile Safe

NEW QUESTION 63
In order to connect to a target device through PSM, the account credentials used for the connection must be stored in the vault?

A. True.
B. Fals

C. Because the user can also enter credentials manually using Secure Connect.
D. Fals
E. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect.
F. Fals
G. Because if credentials are not stored in the vault, the PSM will prompt forcredentials.

Answer: B

Explanation:
In order to connect to a target device through PSM, the account credentials used for the connection do not necessarily have to be stored in the vault. The user can also enter credentials manually using Secure Connect, which is a feature that enables users to connect to target systems through PSM without storing the account credentials in the vault. Secure Connect allows users to provide their own credentials at the time of connection, and these credentials are not saved or managed by CyberArk. Secure Connect can be used with any connection component that supports PSM, such as RDP, SSH, WinSCP, etc. To use Secure Connect, the user needs to specify the target system address and the connection component ID in the URL, and then enter the credentials in the PSM login screen1.
The other options are not correct, because:
? A. True. This is not correct, because as explained above, the user can also enter credentials manually using Secure Connect.
? C. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect. This is not correct, because PSM Connect is a predefined user that is created on the PSM server during the installation. This user is used to establish the connection between the PSM server and the target server, and to run the PSM processes. The PSM Connect user is not used to log into the target device as the end user2.
? D. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials. This is not correct, because this option is essentially the same as Secure Connect, which is the correct answer.
References:
? 1: Secure Connect
? 2: PSMConnect and PSMAdminConnect

NEW QUESTION 66
Where can you check that the LDAP binding is using TCP/636?

A. in Active Directory under "Users OU" => "User Properties" => "External Bindings" => "Port"
B. in PVWA, under "LDAP Integration" => "LDAP" => "Directories" => "" => "Hosts" => "Host"
C. in PrivateArk Client, under "Tools" => "Administrative Tools" => "Directory Mapping" => ""
D. From the PVWA, connect to the domain controller using Test-NetConnection on Port 636.

Answer: D

Explanation:
To check that the LDAP binding is using TCP/636, you can use the Test- NetConnection cmdlet from the PVWA to connect to the domain controller on Port 636. This method allows you to verify that the LDAP service is listening on the secure port and that the connection can be established using SSL/TLS, which is typically associated with port 6361.
References:
? CyberArk Docs - LDAP Integration2
? CyberArk Knowledge Article - How to test outgoing LDAP external directory connectivity to the vault

NEW QUESTION 70
Which permissions are needed for the Active Directory user required by the Windows Discovery process?

A. Domain Admin
B. LDAP Admin
C. Read/Write
D. Read

Answer: D

Explanation:
The Active Directory user required by the Windows Discovery process needs to have Read permissions in the OU to scan and all sub-OUs1. This allows the Discovery process to scan predefined machines for new and modified accounts and their dependencies without requiring elevated privileges such as Domain Admin or LDAP Admin rights. The Read permission is sufficient for the Discovery process to retrieve the necessary information about the accounts that should be onboarded into the Vault. References:
? CyberArk's official documentation on managing discovery processes outlines the permissions required for the Discovery process, including the need for Read permissions for the Active Directory user performing the discovery1.
? Additional details on the required credentials for scanning and the Discovery process can be found in the supported target machines section of CyberArk's documentation2.

NEW QUESTION 74
Which change could CyberArk make to the REST API that could cause existing scripts to fail?

A. adding optional parameters in the request
B. adding additional REST methods
C. removing parameters
D. returning additional values in the response

Answer: C

Explanation:
Changes to the REST API that could cause existing scripts to fail include removing parameters. When parameters are removed from an API, scripts that rely on those parameters being present may no longer function correctly because they expect certain data to be available. This can lead to errors or unexpected behavior in the scripts that use the API1.
References:
? CyberArk Docs: REST APIs1

NEW QUESTION 77
Refer to the exhibit.

Why is user "EMEALevel2Support" unable to change the password for user "Operator"?

A. EMEALevel2Support's hierarchy level is not the same or higher than Operator.
B. EMEALevel2Support does not have the "Manage Directory Mapping" role.
C. Operator can only be reset by the Master user.
D. EMEALevel2Support does not have rights to reset passwords for other users.

Answer: D

Explanation:
The image description indicates that "EMEALevel2Support" has the following rights: Add/Update Users, Manage Server File Categories, Manage Directory Mapping, Backup All Files, Restore All Files. Since there is no mention of the right to reset passwords for other users, this suggests that "EMEALevel2Support" lacks the necessary permission to change the password for "Operator".

NEW QUESTION 82
A recently-hired colleague onboarded five new Local Accounts that are used for five 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 two.)

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

Answer: ABE

Explanation:
? Verify Server Address: Ensure that the address field is populated with the correct IP or FQDN for each server (Option A).
? Check PSM Settings: Confirm that the correct PSM connection component is specified within the account platform settings (Option B).
? Automatic Management: Check if the "Disable automatic management for this account" setting is not enabled (Option E).
These steps should help in troubleshooting the connection issue in the CyberArk Privileged Access Management (PAM) solution.

NEW QUESTION 85
Which file must be edited on the Vault to configure it to send data to PTA?

A. dbparm.ini
B. PARAgent.ini
C. my.ini
D. padr.ini

Answer: A

Explanation:
To configure the CyberArk Vault to send data to Privileged Threat Analytics (PTA), you must edit the dbparm.ini file on the Vault. This file contains parameters that specify how the Vault should forward syslog events to PTA, ensuring that the Vault can send secured syslog data to PTA for analysis and threat detection1.
References:
? CyberArk Docs: Configure Vault Trusted Connection to PTA2
? Netenrich: CyberArk Vault via Syslog1

NEW QUESTION 89
When managing SSH keys, the CPM stored the Private Key

A. In the Vault
B. On the target server
C. A & B
D. Nowhere because the private key can always be generated from the public key.

Answer: A

Explanation:
When managing SSH keys, the CPM stores the private key in the Vault. The CPM generates a new random SSH key pair and updates the public SSH key on the target server. The new private SSH key is then stored in the Digital Vault where it benefits from all the accessibility and security features of the Vault. The private SSH key is never stored on the target server, as this would expose it to unauthorized access or theft. The private SSH key cannot be generated from the public key, as this would defeat the purpose of
asymmetric encryption. References:
? Manage SSH Keys
? SSH Key Manager
? Use SSH Keys

NEW QUESTION 94
To manage automated onboarding rules, a CyberArk user must be a member of which group?

A. Vault Admins
B. CPM User
C. Auditors
D. Administrators

Answer: A

Explanation:
To manage automated onboarding rules in CyberArk, a user must be a member of the Vault Admins group. This group has the necessary permissions to create and manage predefined rules that automatically onboard newly discovered accounts, which helps minimize the time it takes to onboard and securely manage accounts, reduces the time spent on reviewing pending accounts, and prevents human errors that may occur during manual onboarding1.
References:
? CyberArk's official documentation on onboarding rules provides detailed information on the groups required to manage these rules, including the Vault Admins group1.

NEW QUESTION 95
According to CyberArk, which issues most commonly cause installed components to display as disconnected in the System Health Dashboard? (Choose two.)

A. network instabilities/outages
B. vault license expiry
C. credential de-sync
D. browser compatibility issues
E. installed location file corruption

Answer: AC

Explanation:
The System Health Dashboard in CyberArk provides a visual representation of the health status of different CyberArk components. When components are displayed as disconnected, the most common issues are network instabilities/outages and credential de- sync. Network issues can disrupt the connectivity between components and the Vault, while credential de-sync indicates that a component is no longer able to authenticate to the Vault due to synchronization problems with the credentials12. References:
? CyberArk Docs: Monitor system health1
? CyberArk Docs: System Health Dashboard details

NEW QUESTION 96
Which utilities could you use to change debugging levels on the vault without having to restart the vault. Select all that apply.

A. PAR Agent
B. PrivateArk Server Central Administration
C. Edit DBParm.ini in a text editor.
D. Setup.exe

Answer: AB

Explanation:
To change debugging levels on the vault without having to restart the vault, you can use the following utilities:
? PAR Agent: This is a utility that runs on the vault server and allows you to change the debug level of the vault by editing the PARAgent.ini file. You can set the EnableTrace parameter to yes and specify the debug level in the DebugLevel parameter. The changes will take effect immediately without restarting the vault. The log file is located in the PARAgent.log file1.
? PrivateArk Server Central Administration: This is a graphical user interface that runs on the vault server and allows you to change the debug level of the vault by selecting the vault server and clicking the Debug button. You can choose the debug level from a list of predefined options or enter a custom value. The changes will take effect immediately without restarting the vault. The log files are located in the Trace.dX files, where X is a number from 0 to 42.
You cannot use the following utilities to change debugging levels on the vault without having to restart the vault:
? Edit DBParm.ini in a text editor: This is a configuration file that stores the vault parameters, such as the database name, port, and password. Editing this file does not affect the debug level of the vault, and requires restarting the vault for the changes to take effect3.
? Setup.exe: This is an installation program that runs on the vault server and allows you to install, upgrade, or uninstall the vault. It does not allow you to change

the debug level of the vault, and requires restarting the vault for any changes to take effect4. References:
? 1: Configure Debug Levels, Vault section, PARAgent subsection
? 2: Configure Debug Levels, Vault section, PrivateArk Server Central Administration subsection
? 3: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section: Configuring the Vault, Subsection: DBParm.ini
? 4: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section: Installing the Vault

NEW QUESTION 101
Which of the following options is not set in the Master Policy?

A. Password Expiration Time
B. Enabling and Disabling of the Connection Through the PSM
C. Password Complexity
D. The use of “One-Time-Passwords”

Answer: C

Explanation:
Password Complexity is not set in the Master Policy, but in the Platform Management settings for each platform. The Master Policy is a set of rules that define the security and compliance policy of privileged accounts in the organization, such as access workflows, password management, session monitoring, and auditing1. The Master Policy does not include any technical settings that determine how the system manages accounts on various platforms1. Password Complexity is a technical setting that defines the minimum requirements for the length and composition of the passwords that are generated by the CPM for the accounts associated with the platform2. Password Complexity can be configured in the Platform Management settings, which are independent of the Master Policy and can be customized according to the organization’s environment and security policies1.
The other options are set in the Master Policy, as follows:
? A. Password Expiration Time: This is a policy rule that determines how often passwords are changed. It can be set in the Master Policy under the Password Management section1.
? B. Enabling and Disabling of the Connection Through the PSM: This is a policy rule that determines whether users can connect to target systems through the PSM. It can be set in the Master Policy under the Session Management section1.
? D. The use of “One-Time-Passwords”: This is a policy rule that determines whether passwords are changed every time they are retrieved by a user. It can be set in the Master Policy under the Password Management section1. References:
? 1: The Master Policy
? 2: Platform Management, Password Complexity subsection

NEW QUESTION 105
What is the chief benefit of PSM?

A. Privileged session isolation
B. Automatic password management
C. Privileged session recording
D. ‘Privileged session isolation’ and ‘Privileged session recording’

Answer: D

Explanation:
According to the web search results, the chief benefit of PSM is to provide both privileged session isolation and privileged session recording. Privileged session isolation means that the PSM server acts as a proxy between the user and the target machine, preventing the user from directly accessing the target machine or exposing the privileged account credentials. Privileged session recording means that the PSM server captures and stores a video and a transcript of the user’s activity on the target machine, enabling auditing and monitoring of the privileged session. These benefits help to enhance the security and compliance of the privileged access management solution, as they prevent credential exposure, restrict unauthorized access, detect malicious activity, and provide evidence for forensic analysis

NEW QUESTION 107
You want to generate a license capacity report. Which tool accomplishes this?

A. Password Vault Web Access
B. PrivateArk Client
C. DiagnoseDB Report
D. RestAPI

Answer: B

Explanation:
The license capacity report is a tool that provides information about the licensed user types and objects in the Vault. It enables users to see the maximum number of licenses for each user type or object, and the number of used licenses for each one. Only user types and objects that are limited by the license are displayed in this report. To generate a license capacity report, users need to use the PrivateArk Client, which is a graphical user interface that allows users to manage safes and their properties. Users can access the report from the Tools menu in the PrivateArk Client. References: Reporting License Usage, Manage the CyberArk License

NEW QUESTION 112
By default, members of which built-in groups will be able to view and configure Automatic Remediation and Session Analysis and Response in the PVWA?

A. Vault Admins
B. Security Admins
C. Security Operators
D. Auditors

Answer: B

Explanation:

Security Admins are the built-in group that can view and configure Automatic Remediation and Session Analysis and Response in the PVWA. These features are part of the Privileged Threat Analytics (PTA) module, which is designed to detect and respond to anomalous activities and risky behaviors in the privileged environment. Security Admins have the permissions to access the PTA settings and configure the policies and actions for Automatic Remediation and Session Analysis and Response. References:
? Defender PAM Sample Items Study Guide, page 18, question 49
? Privileged Threat Analytics Implementation Guide, page 9, section “Security Admins”

NEW QUESTION 115
SAFE Authorizations may be granted to . Select all that apply.

A. Vault Users
B. Vault Group
C. LDAP Users
D. LDAP Groups

Answer: ABCD

Explanation:
SAFE Authorizations may be granted to Vault Users, Vault Groups, LDAP Users, and LDAP Groups. These are the four types of users that can be defined in the Vault and assigned permissions to access Safes and manage passwords. Vault Users and Vault Groups are created and managed within the Vault, while LDAP Users and LDAP Groups are imported from an external directory service such as Active Directory. References:
? Defender PAM Course, Module 4: Managing Safes, Lesson 4.2: Safe Authorizations, slide 4
? Defender PAM Sample Items Study Guide, Question 39, page 15
? CyberArk Privileged Access Security Documentation, Vault Administration Guide, Chapter 4: Managing Safes, Section: Safe Authorizations, page 4-12

NEW QUESTION 118
You received a notification from one of your CyberArk auditors that they are missing Vault level audit permissions. You confirmed that all auditors are missing the Audit Users Vault permission.
Where do you update this permission for all auditors?

A. Private Ark Client > Tools > Administrative Tools > Directory Mapping > Vault Authorizations
B. Private Ark Client > Tools > Administrative Tools > Users and Groups > Auditors > Authorizations tab
C. PVWA User Provisioning > LDAP integration > Vault Auditors Mapping > Vault Authorizations
D. PVWA> Administration > Configuration Options > LDAP integration > Vault Auditors Mapping > Vault Authorizations

Answer: B

Explanation:
To update the Vault level audit permissions for all auditors, you would use the Private Ark Client. Specifically, you would navigate to the Tools menu, select Administrative Tools, then Users and Groups. Within the Users and Groups section, you would select the Auditors group and go to theAuthorizations tab. Here, you can manage and update the permissions for the Auditor group, including the Audit Users Vault permission. This ensures that all members of the Auditors group have the necessary permissions to perform their audit functions within the Vault1.
References:
? CyberArk’s official documentation on predefined users and groups, which includes information on the Auditor user and the permissions associated with this role1.
? Information on the administrative tools available in the Private Ark Client, which are used for managing users and groups, including auditors2.

NEW QUESTION 121
dbparm.ini is the main configuration file for the Vault.

A. True
B. False

Answer: B

Explanation:
dbparm.ini is not the main configuration file for the Vault. It is one of the several configuration files that control the initial settings and method of operation of the Server. The main configuration file for the Vault is DBParm.ini, which contains the general parameters of the database, such as the Vault name, the Vault IP address, the Vault port, the encryption algorithm, the log retention, and the debug mode1. References:
? DBParm.ini - CyberArk, section “Main parameters”

NEW QUESTION 125
What is the purpose of the Interval setting in a CPM policy?

A. To control how often the CPM looks for System Initiated CPM work.
B. To control how often the CPM looks for User Initiated CPM work.
C. To control how long the CPM rests between password changes.
D. To control the maximum amount of time the CPM will wait for a password change to complete.

Answer: A

Explanation:
The Interval setting in a CPM policy is used to control how often the CPM looks for System Initiated CPM work, such as password changes, verifications, and reconciliations. The Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the required actions. For example, if the Interval is set to 60, the CPM will check the accounts every hour and change, verify, or reconcile the passwords according to the policy settings. The Interval setting does not affect User Initiated CPM work, such as manual password changes or retrievals, which are performed immediately upon request. The Interval setting also does not control how long the CPM rests between password changes or the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe. References:
? [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide 9: CPM Policy Settings

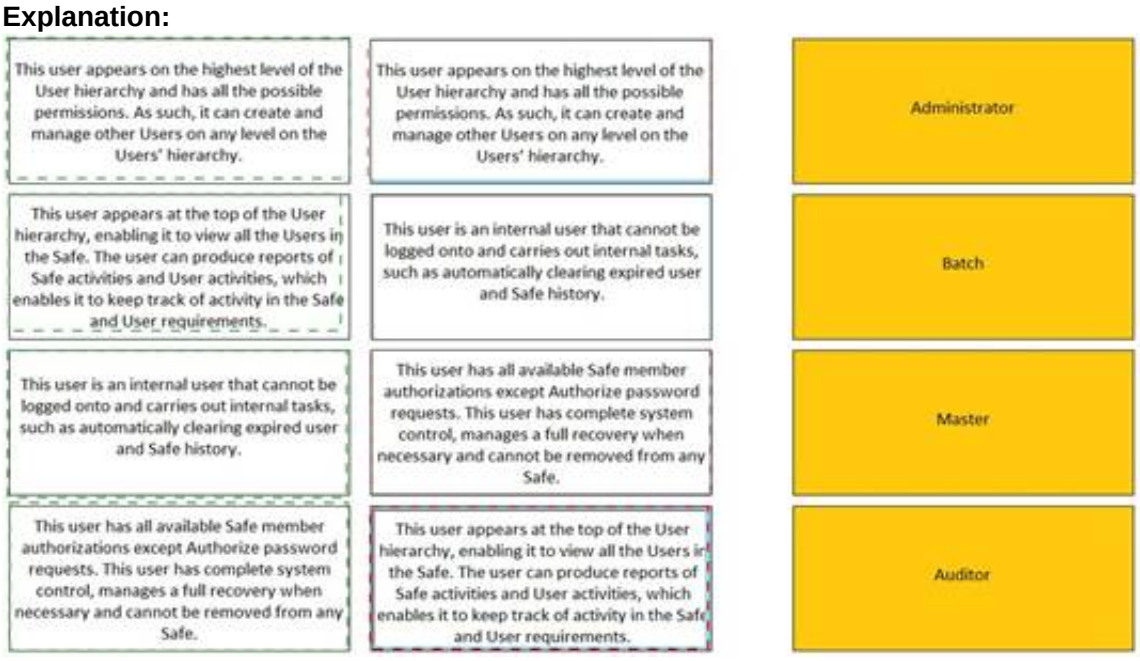
? [Defender PAM Sample Items Study Guide], Question 4: CPM Policy Settings
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Interval

NEW QUESTION 129
DRAG DROP
Match the built-in Vault User with the correct definition.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 132
Which command generates a full backup of the Vault?

A. PAReplicate.exe Vault.ini /LogonFromFile user.ini /FullBackup
B. PAPreBackup.exe C:\PrivateArk\Server\Conf\Vault.ini Backup/Asdf1234 /full
C. PARestore.exe PADR ini /LogonFromFile vault.ini /FullBackup
D. CAVaultManager.exe RecoverBackupFiles /BackupPoolName BkpSvr1

Answer: A

Explanation:
The command PAReplicate.exe with the /FullBackup option is used to generate a full backup of the CyberArk Vault. This command requires the Vault configuration file (typically Vault.ini) and a credential file (specified with /LogonFromFile) that contains the user's encrypted logon credentials. The /FullBackup option indicates that a full backup of the Vault is to be performed, as opposed to an incremental backup1. References:
? CyberArk Docs: Install the Vault Backup Utility2
? CyberArk Knowledge Article: PAReplicate Configuration and Usage

NEW QUESTION 133
Time of day or day of week restrictions on when password verifications can occur configured in .

A. The Master Policy
B. The Platform settings
C. The Safe settings
D. The Account Details

Answer: C

Explanation:
Time of day or day of week restrictions on when password verifications can occur are configured in the Safe settings. This is a security feature that prevents Safes from being opened except at certain times (e.g., 8 a.m. to 5 p.m.). If a user tries to enter at a time that has not been designated for access, they will receive a message that informs them that the Safe is unavailable. References: Advanced Safe Management

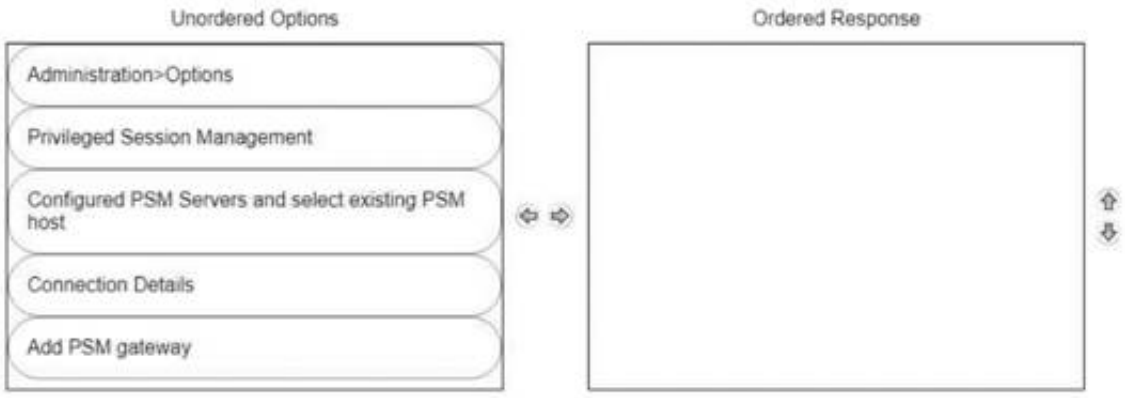
NEW QUESTION 137
A user requested access to view a password secured by dual-control and is unsure who to contact to expedite the approval process. The Vault Admin has been asked to look at the account and identify who can approve their request.
What is the correct location to identify users or groups who can approve?

A. PVWA> Administration > Platform Configuration > Edit Platform > UI & Workflow > Dual Control> Approvers
B. PVWA> Policies > Access Control (Safes) > Safe Members > Workflow > Authorize Password Requests
C. PVWA> Account List > Edit > Show Advanced Settings > Dual Control > Direct Managers
D. PrivateArk > Admin Tools > Users and Groups > Auditors (Group Membership)

Answer: B

Explanation:
In CyberArk's Privileged Access Management (PAM), the correct location to identify users or groups who can approve a dual-control request is within the Password Vault Web Access (PVWA). Specifically, you would navigate to the 'Policies' section, then to 'Access Control (Safes)', and within a safe, you would go to 'Safe Members'. Here, under the 'Workflow' tab, there is an option to 'Authorize Password Requests'. This is where the Vault Admin can identify which users or groups are authorized to approve requests for viewing passwords secured by dual-control.
References: The information is based on the best practices and guidelines provided in the CyberArk Defender PAM course and learning resources, which include the official CyberArk documentation and study guides.

NEW QUESTION 139
DRAG DROP
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To configure a PSM host to use the HTML5 Gateway from the PVWA, you would typically follow these steps:
? Log into the PVWA with an administrative user.
? Navigate to Administration > Options.
? Right-click on Privileged Session Management and select Add Configured PSM Gateway Servers.
? Right-click Configured PSM Gateway Servers, then Add PSM Gateway Server.
? Select the newly added gateway server and enter a unique ID for the PSM HTML5 Gateway.
? Expand the newly created gateway server and enter the necessary configuration details.
Please note that these steps are based on general procedures for configuring a PSM host with an HTML5 Gateway and should be verified against the official CyberArk documentation or by a qualified CyberArk professional. For detailed instructions and best practices, refer to the CyberArk documentation123.

NEW QUESTION 141
Which processes reduce the risk of credential theft? (Choose two.)

A. require dual control password access approval
B. require password change every X days
C. enforce check-in/check-out exclusive access
D. enforce one-time password access

Answer: BD

NEW QUESTION 144
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PAM-DEF Exam with Our Prep Materials Via below:

https://www.certleader.com/PAM-DEF-dumps.html