CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
Which accounts can be selected for use in the Windows discovery process? (Choose two.)

A. an account stored in the Vault
B. an account specified by the user
C. the Vault Administrator
D. any user with Auditor membership
E. the PasswordManager user

Answer: AB

Explanation:
During the Windows discovery process in CyberArk Defender PAM, accounts that can be selected for use include an account that is already stored in the Vault and an account that is specified by the user. The discovery process scans predefined machines for new and modified accounts and their dependencies. After the scan, accounts that should be onboarded into the Vault for secure and automatic management are identified12. References: The information provided is based on general knowledge of CyberArk PAM best practices and the account discovery process as outlined in CyberArk's official documentation1

NEW QUESTION 2
The primary purpose of exclusive accounts is to ensure non-repudiation (Individual accountability).

A. TRUE
B. FALSE

Answer: A

Explanation:
The primary purpose of exclusive accounts is to ensure non-repudiation (individual accountability). Exclusive accounts are accounts that can only be used by one user at a time, and are locked during usage. This means that no other user can access the same account until the current user releases it or the session expires. By using exclusive accounts, the organization can enforce individual accountability and traceability for the actions performed on the target systems. Exclusive accounts also reduce the risk of credential theft and unauthorized access, as the passwords are changed every time they
are retrieved by a user1. Exclusive accounts can be configured in the Master Policy under the Password Management section, by enabling the Exclusive Access rule2. References:
? 1: The Master Policy, One Time Password subsection
? 2: The Master Policy, Exclusive Access subsection

NEW QUESTION 3
Which Automatic Remediation is configurable for a PTA detection of a "Suspected Credential Theft"?

A. Add to Pending
B. Rotate Credentials
C. Reconcile Credentials
D. Disable Account

Answer: B

Explanation:
For a Privileged Threat Analytics (PTA) detection of a "Suspected Credential Theft," the automatic remediation that can be configured is Rotate Credentials. This remediation action is designed to automatically initiate password changes when PTA identifies a suspected credential threat, such as a credential theft event. By rotating the credentials, CyberArk ensures that the potentially compromised credentials are changed, thus mitigating the risk of unauthorized access1.
References:
? CyberArk's official documentation on configuring PTA remediations, which includes information on automatic password rotation for suspected credential threats2.
? Additional details on the remediation actions that can be configured for different types of PTA detections, including Suspected Credential Theft1.

NEW QUESTION 4
The vault supports Role Based Access Control.

A. TRUE
B. FALSE

Answer: A

Explanation:
The vault supports Role Based Access Control (RBAC), which is a method of granting access to resources based on the roles of users or groups. RBAC enables the administrator to define roles that represent different functions or responsibilities in the organization, and assign permissions to those roles according to the principle of least privilege. Users or groups can then be assigned to one or more roles, and inherit the permissions of those roles. RBAC simplifies the management of access control by reducing the complexity and redundancy of assigning permissions to individual users or groups. RBAC also enhances security and compliance by ensuring that users or groups only have the minimum level of access required to perform their tasks1.
References:
? 1: Role Based Access Control

NEW QUESTION 5
A new domain controller has been added to your domain. You need to ensure the CyberArk infrastructure can use the new domain controller for authentication. Which locations must you update?

A. on the Vault server in Windows\System32\Etc\Hosts and in the PVWA Application under Administration > LDAP Integration > Directories > Hosts
B. on the Vault server in Windows\System32\Etc\Hosts and on the PVWA server in Windows\System32\Etc\Hosts

C. in the Private Ark client under Tools > Administrative Tools > Directory Mapping
D. on the Vault server in the certificate store and on the PVWA server in the certificate store

Answer: A

Explanation:
When a new domain controller is added to a domain, it is necessary to update the CyberArk infrastructure to ensure it can use the new domain controller for authentication. This involves updating the hosts file on theVault server located
at Windows\System32\Etc\Hosts to include the new domain controller's details. Additionally, within the PVWA Application, you need to navigate to Administration > LDAP Integration > Directories > Hosts and update the information there as well. This ensures that both the Vault server and the PVWA Application are aware of the new domain controller and can authenticate against it1.
References:
? CyberArk's official documentation on configuring Active Directory integration, which includes details on setting up domain controllers for authentication2.
? Information on adding Active Directory as a directory service in CyberArk Identity, which discusses the integration of domain controllers3.

NEW QUESTION 6
All of your Unix root passwords are stored in the safe UnixRoot. Dual control is enabled for some of the accounts in that safe. The members of the AD group UnixAdmins need to be able to use the show, copy, and connect buttons on those passwords at any time without confirmation. The members of the AD group Operations Staff need to be able to use the show, copy and connect buttons on those passwords on an emergency basis, but only with the approval of a member of Operations Managers never need to be able to use the show, copy or connect buttons themselves.
Which safe permission do you need to grant Operations Staff? Check all that apply.

A. Use Accounts
B. Retrieve Accounts
C. Authorize Password Requests
D. Access Safe without Authorization

Answer: AB

Explanation:
To use the show, copy, and connect buttons on the accounts in the safe UnixRoot, the Operations Staff need to have the Use Accounts permission, which allows them to request access to the accounts and perform actions on them. However, since dual control is enabled for some of the accounts, they also need to have the Retrieve Accounts permission, which allows them to view the password of the account after it is authorized by another user. The Authorize Password Requests permission is not needed, as it is only required for the users who can approve the requests, not the ones who make them. The Access Safe without Authorization permission is not needed, as it would bypass the dual control mechanism and allow the Operations Staff to access the accounts without approval. References:
? [Defender PAM Sample Items Study Guide], page 10, question 5
? [CyberArk Privileged Access Security Implementation Guide], page 30, table 2-1
? [CyberArk Privileged Access Security Administration Guide], page 43, section 3.2.2.1

NEW QUESTION 7
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 8
What is the purpose of a linked account?

A. To ensure that a particular collection of accounts all have the same password.
B. To ensure a particular set of accounts all change at the same time.
C. To connect the CPNI to a target system.
D. To allow more than one account to work together as part of a password management process.

Answer: D

Explanation:
A linked account is an account that is associated with another account to enable the password management process. A linked account can be used for various purposes, such as logging on to a target system, changing the password of another account, or enabling privileged commands. A linked account can be defined either on the platform level or on the account level, depending on the type and scope of the linked account. The types of linked accounts that are supported by CyberArk are1:
? Logon account: An account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the CPM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the CPM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account.
? Reconcile account: An account that contains the password used in reconciliation processes. Reconciliation is 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 sync. A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the target account, the CPM can use the reconcile account to restore the password of the target account, in case it is changed or out of sync.
? Other additional accounts: Additional accounts can be used in various cases. For example:

The other options are not the purpose of a linked account, because:
? A. To ensure that a particular collection of accounts all have the same password.
This is not the purpose of a linked account, but of a group account. A group account is an account that is associated with multiple target systems that share the same credentials. A group account allows the CPM to manage the password of multiple systems with a single password object in the Vault2.
? B. To ensure a particular set of accounts all change at the same time. This is not the purpose of a linked account, but of a password change schedule. A password change schedule is a feature that allows the administrator to define a time frame for changing the passwords of a set of accounts. A password change schedule can be configured either in the Master Policy or in the Platform settings3.
? C. To connect the CPNI to a target system. This is not the purpose of a linked account, but of a service account. A service account is an account that is used by a service or an application to connect to a target system. A service account can be managed by the Central Credential Provider (CCP), which is a component that provides applications and services with the credentials they need to access target systems4.
References:
? 1: Linked Accounts
? 2: Group Accounts
? 3: Password Change Schedule
? 4: Service Accounts

NEW QUESTION 9
Which of the following logs contains information about errors related to PTA?

A. ITAlog.log
B. diamond.log
C. pm_error.log
D. WebApplication.log

Answer: B

Explanation:
According to the web search results, the diamond.log is the main log file that records the PTA system activities, such as receiving and processing events, generating alerts, and sending notifications1. The diamond.log also contains information about errors related to PTA, such as connection failures, configuration issues, parsing problems, or internal exceptions2. The diamond.log can be found in the /opt/tomcat/logs directory on the PTA machine1. The debug level of the diamond.log can be changed using the changeLogLevel.sh utility or manually editing the log4j.properties file1. The diamond.log can be used for troubleshooting PTA issues and viewing statistics

NEW QUESTION 10
What is required to enable access over SSH to a Unix account through both PSM and PSMP?

A. The platform must contain connection components for PSM-SSH and PSMP-SSH.
B. PSM and PSMP must already have stored the SSH Fingerprint for the Unix host.
C. The 'Enable PSMP' setting in the Unix platform must be set to Yes.
D. A duplicate platform (Called) with the PSMP settings must be created.

Answer: A

Explanation:
To enable access over SSH to a Unix account through both Privileged Session Manager (PSM) and Privileged Session Manager Proxy (PSMP), the platform must contain the necessary connection components for both PSM-SSH and PSMP-
SSH. This ensures that the system can handle SSH connections through PSM for a native user experience and through PSMP for secure, transparent connections to remote systems12. References:
? CyberArk Docs: Connect through PSM for SSH1
? CyberArk Docs: Connect to Unix machines (using PSM for SSH)2

NEW QUESTION 10
As long as you are a member of the Vault Admins group, you can grant any permission on any safe that you have access to.

A. TRUE
B. FALSE

Answer: B

Explanation:
Being a member of the Vault Admins group does not automatically grant you any permission on any safe that you have access to. The Vault Admins group is a predefined group that is created during the installation or upgrade of the vault. This group has the Vault Admin authorization, which allows its members to perform administrative tasks on the vault, such as managing users, groups, platforms, policies, and safes1. However, this authorization does not include any safe member authorizations, such as View, Retrieve, Use, or Manage Safe2. Therefore, to grant any permission on a safe, you need to be added as a safe member with the appropriate authorizations, either directly or through another group. The Vault Admins group can be added to safes with all safe member authorizations, but this is not done automatically for all safes. By default, this group is only added to a number of system safes, such as the Password Manager Safe, the PVWAConfig Safe, and the Notification Methods Safe3. For other safes, the Vault Admins group can be added manually by the safe owner or another user with the Manage Safe authorization4. References:
? 1: Predefined users and groups, Predefined groups subsection
? 2: [CyberArk Privileged Access Security Implementation Guide], Chapter 3: Managing Safes, Section: Safe Authorizations, Table 2-1: Safe Authorizations
? 3: What default groups can be automatically added to Safes when they are created?
? 4: [CyberArk Privileged Access Security Administration Guide], Chapter 3: Managing Safes, Section: Adding Safe Members

NEW QUESTION 15
DRAG DROP
Match each automatic remediation to the correct PTA security event.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
In CyberArk's Privileged Threat Analytics (PTA), automatic remediations are actions that can be configured to respond to specific security events. For the event of an unmanaged privileged account, the remediation "Add To Pending" is used to add the account to the pending accounts queue. When there is a suspected credential theft, "Rotate Credentials" is the remediation that initiates a password change. Lastly, for a suspicious password change event, "Reconcile Credentials" is the remediation that ensures the credentials are correct and valid1.
References:
? CyberArk Docs: Configure security events

NEW QUESTION 19
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?

A. Set the parameter RCAllowManualReconciliation to Yes.
B. Set the parameter ChangePasswordinResetMade to Yes.
C. Set the parameter IgnoreReconcileOnMissingAccount to No.
D. Set the UnlockUserOnReconcile to Yes.

Answer: C

Explanation:
In CyberArk's Privileged Access Management (PAM), when an account cannot change its own password, setting the parameter IgnoreReconcileOnMissingAccount to No ensures that the reconcile account is used for password reset. This is because the reconcile account has the necessary permissions to reset the password when the primary account cannot do so. References: The information provided is based on general knowledge of CyberArk PAM best practices and is not taken from any specific CyberArk Defender PAM course or learning resources.

NEW QUESTION 24
Which of the following statements are NOT true when enabling PSM recording for a target Windows server? (Choose all that apply)

A. The PSM software must be instated on the target server
B. PSM must be enabled in the Master Policy (either directly, or through exception)
C. PSMConnect must be added as a local user on the target server
D. RDP must be enabled on the target server

Answer: AC

Explanation:
The following statements are not true when enabling PSM recording for a target Windows server:
? A. The PSM software must be instated on the target server. This is not true, because the PSM software is installed on a dedicated server that acts as a proxy between the user and the target server. The PSM server intercepts the user's connection request, initiates the connection to the target server, and records the privileged session. The target server does not need to have the PSM software installed on it1.
? C. PSMConnect must be added as a local user on the target server. This is not true, because PSMConnect 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 target server does not need to have a local user named PSMConnect on it2.
The following statements are true when enabling PSM recording for a target Windows server:
? B. PSM must be enabled in the Master Policy (either directly, or through exception). This is true, because 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. One of the rules in the Master Policy is the Session Isolation rule, which determines whether or not privileged sessions are isolated and recorded by PSM. This rule can be enabled either directly in the Master Policy, or through an exception for a specific scope of accounts3.
? D. RDP must be enabled on the target server. This is true, because RDP is the protocol that is used by PSM to connect to Windows servers. The target server must have RDP enabled and configured properly to allow the PSM server to access it. The PSM server must also have the RDP client installed on it4.
References:
? 1: Privileged Session Manager
? 2: PSMConnect and PSMAdminConnect
? 3: Session Isolation
? 4: Configure RDP for PSM

NEW QUESTION 27
Where can you assign a Reconcile account? (Choose two.)

A. in PVWA at the account level
B. in PVWA in the platform configuration
C. in the Master policy of the PVWA

D. at the Safe level
E. in the CPM settings

Answer: AB

Explanation:
A Reconcile account can be assigned in the Privileged Vault Web Access (PVWA) at both the account level and within the platform configuration. At the account level, a Reconcile account password can be defined which will override the account specified in the platform1. In the platform configuration, you can navigate to Platform Management, select the platform, edit it, and then expand Automatic Password Management to enter the values in the 'ReconcileAccountSafe' and 'ReconcileAccountName' fields, which will apply to all accounts attached to that specific platform2.
References:
? CyberArk Docs - Reconcile Password1
? CyberArk Community - Associate reconcile account with a specific platform

NEW QUESTION 30
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 accoun
B. After an account on a one-time password platform is used, the account is deleted from the safe automatically.
C. Exclusive access locks the account indefinitel
D. One-time password can be used replace invalid account passwords.
E. Exclusive access is enabled by default in the Master Polic
F. One-time password should only be enabled for emergencies.
G. Exclusive access allows only one person to check-out an account at a tim
H. One-time password schedules an account for a password change after the MinValidityPeriod period expires.

Answer: D

Explanation:
The Master Policy in CyberArk defines the behavior of one-time passwords and exclusive accessExclusive access ensures that only one user can check out an account at any given time, effectively locking the account during its use to prevent simultaneous access1. On the other hand, one-time password functionality is designed to change the account's password after it is used, based on a timer set by the MinValidityPeriod parameter in the policy file. This means that once the password is checked out and the timer expires, the Central Policy Manager (CPM) will change the password2. These settings are often used together to maintain accountability and security for the usage of shared privileged accounts. References:
? CyberArk Docs: One-time passwords and exclusive accounts1
? CyberArk Knowledge Article: CPM: What is the difference between "One Time" and "Exclusive" passwords?2

NEW QUESTION 34
Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?

A. They are added to the Pending Accounts list and can be reviewed and manually uploaded.
B. They cannot be onboarded to the Password Vault.
C. They must be uploaded using third party tools.
D. They are not part of the Discovery Process.

Answer: A

Explanation:
When accounts are discovered by CyberArk but do not match any automated onboarding rule, they are added to the Pending Accounts list. This allows administrators to review these accounts and decide whether to onboard them manually into the Vault. The Pending Accounts list serves as a holding area for accounts that require further review or do not meet the criteria set by existing onboarding rules1.
References:
? CyberArk's official documentation on Onboarding Rules, which explains the process of managing accounts that are discovered but not automatically onboarded1.

NEW QUESTION 38
You are concerned about the Windows Domain password changes occurring during business hours.
Which settings must be updated to ensure passwords are only rotated outside of business hours?

A. In the platform policy - Automatic Password Management > Password Change > ToHour & FromHour
B. in the Master Policy Account Change Window > ToHour & From Hour
C. Administration Settings - CPM Settings > ToHour & FromHour
D. On each individual account - Edit > Advanced > ToHour & FromHour

Answer: B

Explanation:
To ensure that Windows Domain password changes occur outside of business hours, the settings that must be updated are found in the Master Policy under the Account Change Window section. Here, you can specify the ToHour and FromHour to define the time frame outside of which the passwords should be rotated. This setting allows you to control when password changes can occur, ensuring
that they do not interfere with business operations by taking place during non-business hours1.
References:
? CyberArk Docs - Set password policies

NEW QUESTION 42
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 45
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?

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

Answer: A

Explanation:
SSH keys are a way to authenticate to a target machine with a privileged account, and are subject to the same risks and challenges as privileged passwords. CyberArk provides an out-of-the-box target platform to manage SSH keys, called UNIX Via SSH Keys, which simplifies and automates SSH keys lifecycle management. This platform works as follows:
? CyberArk stores the private keys in the Vault, where they benefit from all the security and accessibility features of the Vault, such as encryption, auditing, and backup.
? CyberArk updates the public keys on the target systems, using a parent account that has access to the file that contains the public key, such as ~/.ssh/authorized_keys. CyberArk can generate new random SSH key pairs and update the public keys on the target systems according to the organizational policy, such as after a single use, after a predefined period, or manually.
? CyberArk can also verify that the private and public keys are synchronized, and reconcile them if they are not, using a reconcile account that can reset the SSH key pairs on the target systems.
References: Manage SSH Keys, Use SSH Keys

NEW QUESTION 46
Which master policy settings ensure non-repudiation?

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

Answer: B

Explanation:
Non-repudiation in the context of CyberArk Master Policy settings refers to the assurance that a user cannot deny the validity of their actions. The settings that ensure non-repudiation are those that enforce accountability and traceability of actions. Enforcing check-in/check-out exclusive access ensures that only one user can access an account at a time, and their actions can be traced back to themEnforcing one-time password access means that passwords are used only once and then changed, which prevents the reuse of credentials and ties actions to specific instances of access12.
References:
? CyberArk Docs: Master Policy Rules2
? CyberArk Docs: The Master Policy1

NEW QUESTION 50
Which of these accounts onboarding methods is considered proactive?

A. Accounts Discovery
B. Detecting accounts with PTA
C. A Rest API integration with account provisioning software
D. A DNA scan

Answer: C

Explanation:
A Rest API integration with account provisioning software is considered a proactive account onboarding method, because it enables the automatic creation and management of accounts in the Vault as soon as they are provisioned in the target systems. This way, the accounts are secured from the start and do not need to be discovered or onboarded manually later. A Rest API integration with account provisioning software can be achieved by using the CyberArk Accounts Feed REST API, which allows external applications to send account information to the Vault1.
The other options are not proactive account onboarding methods, because they rely on the discovery of existing accounts that may have been exposed or compromised before being onboarded to the Vault. Accounts Discovery is a feature that enables the Vault to scan target systems and identify privileged accounts that are not managed by the Vault2. Detecting accounts with PTA is a feature that enables the Privileged Threat Analytics (PTA) component to detect and alert on suspicious account activities and credential thefts3. A DNA scan is a feature that enables the Discovery and Audit (DNA) tool to scan Windows and Unix machines and generate a report on the privileged accounts and vulnerabilities found4.
References:
? CyberArk Accounts Feed REST API - CyberArk, section “CyberArk Accounts Feed REST API”
? Accounts Discovery - CyberArk, section “Accounts Discovery”
? Detect and Respond to Privileged Account Threats - CyberArk, section “Detect and Respond to Privileged Account Threats”
? CyberArk DNA - CyberArk, section “CyberArk DNA”

NEW QUESTION 54
To ensure all sessions are being recorded, a CyberArk administrator goes to the master policy and makes configuration changes.
Which configuration is correct?

A. Require privileged session monitoring and isolation = inactive; Record and save session activity = active.
B. Require privileged session monitoring and isolation = inactive; Record and save session activity = inactive.
C. Require privileged session monitoring and isolation = active; Record and save session activity = active.
D. Require privileged session monitoring and isolation = active; Record and save session activity = inactive.

Answer: C

Explanation:
This configuration ensures that privileged sessions are monitored and isolated, and all session activities are recorded and saved for future reference 1.

NEW QUESTION 57
If a password is changed manually on a server, bypassing the CPM, how would you configure the account so that the CPM could resume management automatically?

A. Configure the Provider to change the password to match the Vault's Password
B. Associate a reconcile account and configure the platform to reconcile automatically
C. Associate a logon account and configure the platform to reconcile automatically
D. Run the correct auto detection process to rediscover the password

Answer: B

Explanation:
A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the account that has been changed manually, the CPM can use the reconcile account to restore the password of the account to the value that is stored in the Vault, in case it is changed or out of sync. This process is called password reconciliation and it ensures that the passwords are synchronized and available for use. To configure the account so that the CPM can resume management automatically, the platform that the account belongs to must have the following parameters set1:
? RCAutomaticReconcileWhenUnsynched: This parameter determines whether passwords will be reconciled automatically after the CPM detects a password on a remote machine that is not synchronized with its corresponding password in the Vault. The acceptable values are Yes or No.
? RCReconcileReasons: This parameter determines the codes that represent the CPM plugin errors that will launch a reconciliation process. The acceptable values are plug-in return codes separated by a comma.
? RCFromHour, RCToHour: These parameters determine the time frame in hours during which the CPM can reconcile passwords, either manually or automatically. The acceptable values are 0-23 or -1 for none.
? RCExecutionDays: This parameter determines the days of the week when the CPM will reconcile passwords. The acceptable values are days of the week, separated by commas.
References:
? 1: Password Reconciliation

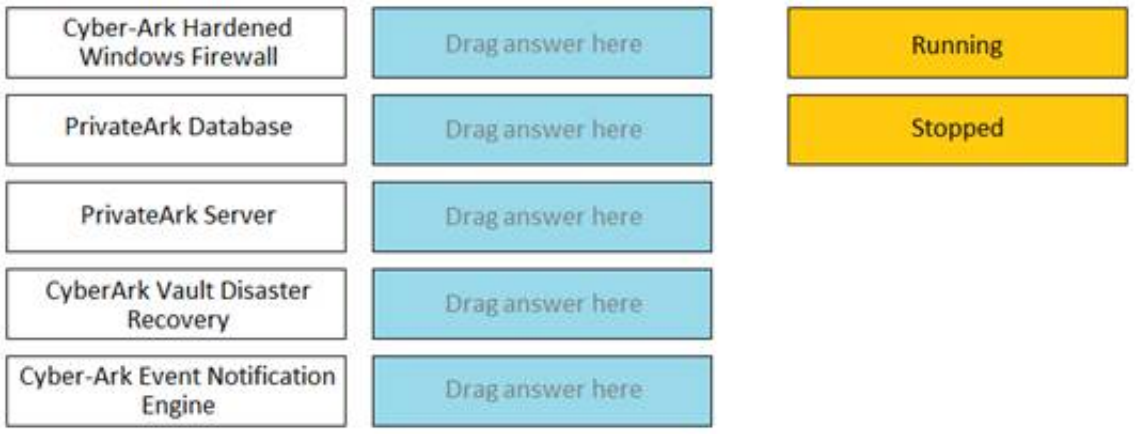
NEW QUESTION 58
How much disk space do you need on a server to run a full replication with PAReplicate?

A. 500 GB
B. 1 TB
C. same as disk size on Satellite Vault
D. at least the same disk size as the Primary Vault

Answer: D

Explanation:
When running a full replication with PAReplicate, it is essential to have at least the same amount of disk space on the server as the disk size of the Primary Vault. This ensures that there is sufficient space to replicate all the data from the Primary Vault without any issues. The disk space should be equal to or larger than the total size of the data being replicated to accommodate the full backup1.
References:
? CyberArk Docs: Install the Vault Backup Utility

NEW QUESTION 59
DRAG DROP
Match the Status of Service on a DR Vault to what is displayed when it is operating normally in Replication mode.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
CyberArk Hardened Windows Firewall -> Running PrivateArk Database -> Running
PrivateArk Server -> Stopped
CyberArk Vault Disaster Recovery -> Running CyberArk Event Notification Engine -> Stopped
? Comprehensive Explanation: A DR Vault is a Vault that acts as a standby replica of the Primary Vault and is ready to take its place when the Primary Vault is unavailable. The DR Vault operates in Replication mode, which means it continuously replicates the data and metadata from the Primary Vault. In Replication mode, the following services have the following status on the DR Vault:
? Cyber-Ark Hardened Windows Firewall: This service provides firewall protection for the Vault server. It should be running on the DR Vault to ensure security.
? PrivateArk Database: This service manages the database that stores the metadata of the Vault. It should be stopped on the DR Vault, because the database is not active in Replication mode. The database is only activated when the DR Vault switches to Production mode.
? PrivateArk Server: This service manages the Vault server and its communication with other components. It should be stopped on the DR Vault, because the Vault server is not active in Replication mode. The Vault server is only activated when the DR Vault switches to Production mode.
? CyberArk Vault Disaster Recovery: This service manages the replication process between the Primary Vault and the DR Vault. It should be running on the DR Vault to ensure data synchronization and readiness for failover.
? Cyber-Ark Event Notification Engine: This service manages the event notifications and alerts for the Vault. It should be stopped on the DR Vault, because the event notifications are not relevant in Replication mode. The event notifications are only activated when the DR Vault switches to Production mode.
References: Primary-DR environment - CyberArk, Replicate the Primary Vault to the Satellite Vaults - CyberArk

NEW QUESTION 62
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 67
Which user is automatically added to all Safes and cannot be removed?

A. Auditor
B. Administrator
C. Master
D. Operator

Answer: C

Explanation:
The user that is automatically added to all Safes and cannot be removed is the Master user. The Master user is a predefined user that is created during the Vault installation and has full permissions on all Safes and accounts. The Master user is the only user that can perform certain tasks, such as creating other predefined users, managing the Vault configuration, and restoring the Vault from a backup. The Master user cannot be deleted or modified by any other user, and is always a member of every Safe12. References:
? Predefined users and groups - CyberArk, section “Master”
? Safes and Safe members - CyberArk, section “Safe members overview”

NEW QUESTION 69
Users can be resulted to using certain CyberArk interfaces (e.g.PVWA or PACLI).

A. TRUE
B. FALSE

Answer: A

Explanation:
Users can be restricted to using certain CyberArk interfaces (e.g. PVWA or PACLI) by using the User Type property. The User Type property is a parameter that can be configured in the User Management settings for each user. The User Type property defines which interfaces the user can access the Vault through, such as PVWA, PrivateArk Client, PACLI, PSM, etc. The User Type property is determined by the CyberArk license and can be assigned to users when they are added to the Vault or when their properties are updated. For example, if a user is assigned the User Type of EPVUser, they can access the Vault through PVWA, PrivateArk Client, PrivateArk Webclient, PACLI, and
PIMSU. However, if a user is assigned the User Type of BizUser, they can only access the Vault through PVWA1. Therefore, by using the User Type property, administrators can control and restrict which CyberArk interfaces the users can use. References:
? 1: Manage users, Types of users subsection

NEW QUESTION 70
Which certificate type do you need to configure the vault for LDAP over SSL?

A. the CA Certificate that signed the certificate used by the External Directory
B. a CA signed Certificate for the Vault server
C. a CA signed Certificate for the PVWA server
D. a self-signed Certificate for the Vault

Answer: A

Explanation:
To enable SSL-based encryption for LDAP integration, the Vault machine and the PVWA machine need to trust the certificate used by the External Directory. This can be achieved by importing the CA Certificate that signed the certificate used by the External Directory into the Windows certificate store on both the Vault and PVWA machines. This will facilitate an SSL connection between the Vault and the External Directory. References: Configure the Vault for LDAP, Configure LDAPS in CyberArk. What certificate I need to use?

NEW QUESTION 74
The Vault administrator can change the Vault license by uploading the new license to the system Safe.

A. True
B. False

Answer: A

Explanation:
According to the web search results, the Vault administrator can change the Vault license by uploading the new license to the system Safe123. This can be done either from the Vault machine or from a remote machine using the PrivateArk client. The new license file should be named license.xml and replace the current one in the system Safe. This can be done without having to reinstall the Vault or restart the service.

NEW QUESTION 76
To change the safe where recordings are kept for a specific platform, which setting must you update in the platform configuration?

A. SessionRecorderSafe Most Voted
B. SessionSafe
C. RecordingsPath
D. RecordingLocation

Answer: A

Explanation:
To change the safe where recordings are kept for a specific platform, you must update the SessionRecorderSafe setting in the platform configuration. This setting specifies the name of the safe where the Privileged Session Manager (PSM) recordings will be stored. After updating the SessionRecorderSafe setting, you need to restart the PSM service or wait for the new settings to be applied, which typically takes about 10 minutes. Once the new settings are in effect, any new PSM sessions initiated will have their recordings stored in the newly specified safe1.
References:
? CyberArk Docs - How to Create/Change/Configure PSM Recording Safes

NEW QUESTION 79
Which methods can you use to add a user directly to the Vault Admin Group? (Choose three.)

A. REST API
B. PrivateArk Client
C. PACLI
D. PVWA
E. Active Directory
F. Sailpoint

Answer: ABC

Explanation:
To add a user directly to the Vault Admin Group in CyberArk, you can use the following methods:
? REST API: The REST API allows for programmatic management of users and groups within the Vault, including adding users to the Vault Admin Group1.
? PrivateArk Client: The PrivateArk Client provides a graphical interface for managing users and groups, and it can be used to add users directly to the Vault Admin Group2.
? PACLI: The PACLI (Privileged Access Command Line Interface) is a command- line tool that enables administrators to manage the Vault, including adding users to groups2.
These methods provide different ways to manage users and their group memberships within the CyberArk Vault, offering flexibility for administrators to choose the most suitable approach for their needs.
References:
? CyberArk's official documentation on using the REST API to manage users and groups1.
? Information on managing users and groups through the PrivateArk Client and PACLI2.

NEW QUESTION 82
What do you need on the Vault to support LDAP over SSL?

A. CA Certificate(s) used to sign the External Directory certificate Most Voted
B. RECPRV.key
C. a private key for the external directory
D. self-signed Certificate(s) for the Vault

Answer: A

Explanation:
To support LDAP over SSL, the Vault requires the CA Certificate(s) that were used to sign the certificate of the External Directory. This is necessary to establish a trusted SSL connection between the Vault and the External Directory. The CA Certificate(s) must be imported into the Windows certificate store on the Vault machine to facilitate this SSL connection1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the requirements for configuring LDAP over SSL as outlined in CyberArk's official documentation1.

NEW QUESTION 85
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection.

A. TRUE
B. FALSE

Answer: A

Explanation:
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection. Auto-detection is a feature that enables the CPM to automatically discover and onboard accounts on target systems that are associated with a specific platform. Auto-detection can be configured in the Platform Management settings for each platform that supports this functionality. However, auto-detection has some limitations, such as requiring the CPM to have access to the target system, not supporting all platforms, and not providing comprehensive information about the accounts and their security risks1. DNA, on the other hand, is a standalone scanning tool that can discover and audit privileged accounts across the network, regardless of the platform or the CPM access. DNA can provide additional discovery functions, such as identifying machines vulnerable to Pass-the-Hash attacks, collecting reliable and comprehensive audit information, and generating reports and visual maps that evaluate the privileged account security status in the organization2. DNA can also be used before or independently of the CyberArk PAM solution, as it does not require agents to be installed on target systems2. References:
? 1: Auto-detection
? 2: CyberArk DNA Overview

NEW QUESTION 90
If a user is a member of more than one group that has authorizations on a safe, by default that user is granted .

A. the vault will not allow this situation to occur.
B. only those permissions that exist on the group added to the safe first.
C. only those permissions that exist in all groups to which the user belongs.
D. the cumulative permissions of all groups to which that user belongs.

Answer: D

Explanation:
When a user is a member of more than one group that has authorizations on a safe, by default that user is granted the cumulative permissions of all groups to which that user belongs. This means that the user will have the highest level of access that any of the groups have on the safe. For example, if one group has View and Retrieve permissions, and another group has Add and Delete permissions, the user will have View, Retrieve, Add, and Delete permissions on the safe. This is the default behavior of the vault, unless the Exclusive option is enabled on the safe. The Exclusive option restricts the user's permissions to only those of the group added to the safe first. References:
? [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.2:
Safe Permissions, Slide 8: Cumulative Permissions
? [Defender PAM Sample Items Study Guide], Question 1: Safe Permissions
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Properties, Subsection: Exclusive

NEW QUESTION 93
What is the name of the Platform parameters that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?

A. Min Validity Period
B. Interval
C. Immediate Interval
D. Timeout

Answer: A

Explanation:
The name of the Platform parameter that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy is Min Validity Period. This parameter defines the number of minutes to wait from the last retrieval of the account until it is replaced. This gives the user a minimum period to be able to use the password before it is changed by the CPM. The Min Validity Period parameter can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 60 minutes, but it can be modified according to the organization's security policy1. The Min Validity Period parameter is also used to release exclusive accounts automatically1. References:
? 1: Privileged Account Management, Min Validity Period subsection

NEW QUESTION 95
A password compliance audit found:
1) One-time password access of 20 domain accounts that are members of Domain Admins group in Active Directory are not being enforced.
2) All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM.
What should you do to address these findings?

A. Edit the Master Policy and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
B. Edit safe properties and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
C. Edit CPM Settings and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
D. 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".

Answer: A

Explanation:
To address the findings of the password compliance audit, you should edit the Master Policy in CyberArk Privileged Access Manager. The Master Policy is where you can enforce one-time password access and record session activity. One-time password access ensures that each password is used only once and then changed, which is a security measure to prevent unauthorized reuse of passwords1. Recording session activity is a feature of the Privileged Session Manager (PSM) that allows all activities during a session to be recorded for auditing purposes2. By enabling these settings in the Master Policy, you ensure that the domain accounts have one-time password access enforced and that all sessions connecting to domain controllers are recorded by CyberArk PSM. References:
? CyberArk Docs: One-time passwords and exclusive accounts1

NEW QUESTION 97
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 98
You have been asked to create an account group and assign three accounts which belong to a cluster. When you try to create a new group, you receive an unauthorized error; however, you are able to edit other aspects of the account properties.
Which safe permission do you need to manage account groups?

A. create folders
B. specify next account content
C. rename accounts
D. manage safe

Answer: D

Explanation:
To manage account groups, you need the manage safe permission, which allows you to create, update, and delete account groups in a safe. The other permissions are not related to account groups. The create folders permission allows you to create folders in a safe. The specify next account content permission allows you to specify the next password or SSH key for an account. The rename accounts permission allows you to rename accounts in a safe. References: Manage account groups, Safe member permissions

NEW QUESTION 99
What are the mandatory fields when onboarding from Pending Accounts? (Choose two.)

A. Address
B. Safe
C. Account Description
D. Platform
E. CPM

Answer: BD

Explanation:
When onboarding accounts from the Pending Accounts list, the mandatory fields that must be specified are the Safe where the account will be stored and the Platform that the account will be associated with. The Safe is crucial as it determines the secure location within the CyberArk Vault where the account's credentials will be kept. The Platform is essential because it defines the set of policies and behaviors that will be applied to the account, such as password rotation and session monitoring12.
References:
? CyberArk Docs - Pending accounts1
? CyberArk Docs - Onboarding rules

NEW QUESTION 101
When running a "Privileged Accounts Inventory" Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to show complete account inventory information?

A. List Accounts, View Safe Members
B. Manage Safe Owners
C. List Accounts, Access Safe without confirmation
D. Manage Safe, View Audit

Answer: A

Explanation:

The Privileged Accounts Inventory Report provides information about all the privileged accounts in the system, based on different filters, such as safe, platform, policy, and owner. To run this report through the Reports page in PVWA on a specific safe, the user needs to have the following permissions on that safe:
? List Accounts: This permission allows the user to view the accounts in the safe and their properties, such as name, address, platform, and policy.
? View Safe Members: This permission allows the user to view the members of the safe and their authorizations, such as owners, users, and groups.
These permissions are required to show complete account inventory information for the specific safe. Other permissions, such as Manage Safe Owners, Access Safe without confirmation, Manage Safe, and View Audit, are not relevant for this report. References: Reports and Audits - CyberArk, Safe Member Authorizations

NEW QUESTION 104
For a safe with Object Level Access enabled you can turn off Object Level Access Control when it no longer needed on the safe.

A. TRUE
B. FALSE

Answer: B

Explanation:
According to the CyberArk documentation1, once Object Level Access Control is enabled for a Safe, it cannot be disabled. This feature allows granular control over user access to passwords and files in the Safe, regardless of their Safe level member authorizations2. To enable Object Level Access Control, users need to have the Manage Safe authorization in the Vault1.

NEW QUESTION 107
In your organization the “click to connect” button is not active by default. How can this feature be activated?

A. Policies > Master Policy > Allow EPV transparent connections > Inactive
B. Policies > Master Policy > Session Management > Require privileged session monitoring and isolation > Add Exception
C. Policies > Master Policy > Allow EPV transparent connections > Active
D. Policies > Master Policy > Password Management

Answer: C

Explanation:
The “click to connect” button is a feature that allows users to connect to target systems without entering their credentials manually. It is also known as EPV transparent connections or PSM transparent connections. To activate this feature, you need to enable the Allow EPV transparent connections parameter in the Master Policy. This parameter determines whether users can use the “click to connect” button to initiate a privileged session from the PVWA. If the parameter is set to Active, the button is enabled and users can connect to target systems with one click. If the parameter is set to Inactive, the button is disabled and users need to copy the credentials and paste them in the target system login screen. References: Connect and configure - CyberArk, How to enable/disable Connect button in PVWA console - force.com

NEW QUESTION 111
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 112
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 116
The Active Directory User configured for Windows Discovery needs which permission(s) or membership?

A. Member of Domain Admin Group
B. Member of LDAP Admin Group
C. Read and Write Permissions
D. Read Only Permissions

Answer: D

Explanation:
The Active Directory User configured for Windows Discovery requiresRead Only Permissions. This level of permission allows the user to query and discover objects within the Active Directory without the ability to modify any objects or settings. Having read- only access is sufficient for discovery purposes, as it enables the user to retrieve necessary information without posing a risk of unintended changes to the directory1.
References:
? Microsoft Learn: Configure discovery methods1

NEW QUESTION 121
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 126
Ad-Hoc Access (formerly Secure Connect) provides the following features. Choose all that apply.

A. PSM connections to target devices that are not managed by CyberArk.
B. Session Recording.
C. Real-time live session monitoring.
D. PSM connections from a terminal without the need to login to the PVWA.

Answer: ABC

Explanation:
Ad-Hoc Access (formerly Secure Connect) is a feature that allows users to connect to target devices that are not managed by CyberArk through the PSM. Users can specify the address, username, and password of the target device, and select a client to launch the connection. Ad-Hoc Access sessions benefit from the standard PSM features, such as session recording, detailed auditing, and real-time live session monitoring. However, Ad- Hoc Access does not allow users to connect from a terminal without logging in to the PVWA, as this would bypass the authentication and authorization mechanisms of CyberArk. References:
? Configure ad hoc connections
? Ad Hoc Connections
? Privileged Remote Access Management – PAM Remote Access

NEW QUESTION 128
Where can PTA be configured to send alerts? (Choose two.)

A. SIEM
B. Email
C. Google Analytics
D. EVD
E. PAReplicate

Answer: AB

Explanation:
CyberArk's Privileged Threat Analytics (PTA) can be configured to send alerts to a Security Information and Event Management (SIEM) system and via Email. SIEM systems are used for real-time analysis of security alerts generated by applications and network hardware, while email alerts can be sent to individual or group email addresses for immediate notification1.
References:
? CyberArk Docs: Send PTA Alerts to Email1

NEW QUESTION 132
Secure Connect provides the following. Choose all that apply.

A. PSM connections to target devices that are not managed by CyberArk.
B. Session Recording
C. Real-time live session monitoring.
D. PSM connections from a terminal without the need to login to the PVWA

Answer: ABC

Explanation:

Secure Connect provides the following features:
? A. PSM connections to target devices that are not managed by CyberArk. This is true, because Secure Connect 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, etc1.
? B. Session Recording. This is true, because Secure Connect sessions are recorded by PSM and stored in the Vault, just like regular PSM sessions. The recorded sessions can be viewed and audited by authorized users through the PVWA or the PSM web interface2.
? C. Real-time live session monitoring. This is true, because Secure Connect sessions can be monitored in real-time by authorized users through the PSM web interface. The PSM web interface allows users to view the live session screen, send messages to the session user, pause or terminate the session, and take control of the session if needed3.
The following feature is not provided by Secure Connect:
? D. PSM connections from a terminal without the need to login to the PVWA. This is false, because Secure Connect requires users to login to the PVWA and initiate the connection from there. The PVWA provides the URL for the Secure Connect session, which contains the target system address and the connection component ID. The user then needs to copy and paste the URL into a browser or a remote connection manager to launch the session1.
References:
? 1: Secure Connect
? 2: Recorded Sessions
? 3: PSM Web Interface

NEW QUESTION 135
Which report shows the accounts that are accessible to each user?

A. Activity report
B. Entitlement report
C. Privileged Accounts Compliance Status report
D. Applications Inventory report

Answer: B

Explanation:
The report that shows the accounts that are accessible to each user is the Entitlement report. According to the web page in the edge browser, the Entitlement report provides information about users' entitlement rights in PAM - Self-Hosted regarding user, Safe, active platform, target machine, target account, etc. This report includes each user's effective access control and authorization level on each account that the user has access to in PAM - Self-Hosted. The Entitlement report can be generated in PVWA or PrivateArk1.

NEW QUESTION 139
Which of the following are secure options for storing the contents of the Operator CD, while still allowing the contents to be accessible upon a planned Vault restart? (Choose three.)

A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed
B. Copy the entire contents of the CD to the system Safe on the Vault
C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions
D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS permissions

Answer: ABD

Explanation:
? A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed. This option ensures that the CD is kept in a secure location when not in use, and that the keys are available when needed. This is the default option suggested by CyberArk1.
? B. Copy the entire contents of the CD to the system Safe on the Vault. This option allows the Vault to access the keys from the system Safe, which is a special Safe that stores the Vault configuration files and keys. The system Safe is encrypted and protected by the Vault, and can only be accessed by authorized users2.
? D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS permissions. This option provides an additional layer of security for the server key, which is the most critical key for the Vault. An HSM is a physical device that stores and manages cryptographic keys in a tamper-resistant and isolated environment. The Vault can integrate with an HSM to store and retrieve the server key3. The rest of the keys can be stored in a folder on the Vault Server and secured with NTFS permissions, which restrict access to authorized users and groups.
The following option is not secure and should be avoided:
? C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions. This option exposes the keys to potential risks, such as unauthorized access, data corruption, or deletion. NTFS permissions are not sufficient to protect the keys from malicious or accidental actions. Moreover, this option does not comply with the CyberArk best practices, which recommend to store the keys on a removable media or an HSM

NEW QUESTION 140
When creating an onboarding rule, it will be executed upon .

A. All accounts in the pending accounts list
B. Any future accounts discovered by a discovery process
C. Both "All accounts in the pending accounts list" and "Any future accounts discovered by a discovery process"

Answer: C

Explanation:
According to the CyberArk Defender PAM documentation1, when creating an onboarding rule, it will be executed upon both all accounts in the pending accounts list and any future accounts discovered by a discovery process. This means that the rule will automatically onboard and provision the accounts that match the rule criteria, regardless of when they were discovered. The rule will also apply to any new accounts that are discovered by subsequent discovery processes. This way, the onboarding rule can minimize the time and effort required to securely manage the accounts in the vault.

NEW QUESTION 141
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 143
VAULT authorizations may be granted to .

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

Answer: AC

Explanation:
Vault Authorizations
• Can be assigned only to users (not groups).
• Cannot be inherited via group membership.
• Defined only via the Private Ark Client. Safe Auth
• Assigned to users and/or groups.
• Can be inherited via group membership.
• Can be defined in the Private Ark Client or PVWA

NEW QUESTION 146
According to the DEFAULT Web Options settings, which group grants access to the REPORTS page?

A. PVWAUsers
B. Vault Admins
C. Auditors
D. PVWAMonitor

Answer: C

Explanation:
According to the CyberArk Defender-PAM study guide, the REPORTS page is used to generate reports on various aspects of the CyberArk Privileged Access Management Solution, such as user activity, password usage, and compliance status. The default group that grants access to the REPORTS page is the Auditors group, which is a built-in group in the Vault that has the AuditUsers authorization. Members of the Auditors group can view and generate reports, but cannot modify them. References:
? CyberArk Defender-PAM study guide, page 17, section 3.2.1
? CyberArk Privileged Access Security Documentation, page 48, section 2.3.2.1

NEW QUESTION 151
What does the Export Vault Data (EVD) utility do?

A. exports data from the Vault to TXT or CSV files, or to MSSQL databases
B. generates a backup file that can be used as a cold backup
C. exports all passwords and imports them into another instance of CyberArk
D. keeps two active vaults in sync

Answer: A

Explanation:
The Export Vault Data (EVD) utility is used to export data from the CyberArk Vault to TXT or CSV files, or to MSSQL databases. This utility enables the creation of reports such as a list of Safes or incoming requests by exporting data from the Vault. Each report is saved in a separate file, which can then be imported into third-party applications or databases for further analysis or reporting purposes12.
References:
? CyberArk Docs - Export Vault Data (EVD) utility1
? CyberArk Docs - Export data to files

NEW QUESTION 152
The vault supports Subnet Based Access Control.

A. TRUE
B. FALSE

Answer: A

Explanation:
According to the web page in the edge browser, the vault supports Subnet Based Access Control. This is a feature that allows you to restrict access to a key vault

to a specified virtual network and subnet. You can also use firewall settings to deny internet traffic and allow only specific IP addresses. This way, you can enhance the security and privacy of your key vault data12

NEW QUESTION 155
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 159
A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.

A. True
B. False

Answer: A

Explanation:
According to the web search results, a Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control. SMTP is a protocol that enables the sending and receiving of email messages. By integrating SMTP with CyberArk Defender PAM, the Event Notification Engine (ENE) can automatically send email notifications about PAM activities to predefined users1. For example, the ENE can notify users about password requests, password confirmations, password changes, password verifications, password reconciliations, password access, password usage, password expiration, and password violations1. The ENE can also notify users about system events, such as Vault backup, Vault restore, Vault shutdown, Vault startup, and Vault license expiration1. These notifications help to monitor the Vault activity and ensure compliance with the security policies.
SMTP integration is also essential for facilitating workflow processes, such as Dual Control. Dual Control is a feature that enables authorized Safe owners to either grant or deny requests to access accounts. This feature adds an additional measure of protection, in that it enables you to see who wants to access the information in the Safe, when, and for what purpose. The Master Policy enables organizations to ensure that passwords can only be retrieved after permission or 'confirmation' has been granted from an authorized Safe Owner(s). This is known as Dual Control2. SMTP integration enables the ENE to send email notifications to the requesters and the confirmers about the status of the password requests. The ENE can also send reminders to the confirmers if they have not responded to the requests within a specified time period2. These notifications help to streamline the workflow process and ensure timely and secure access to the accounts.
References:
? Email notifications - CyberArk
? Dual Control - CyberArk

NEW QUESTION 162
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 166
DRAG DROP
Match each permission to where it can be found.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Add Accounts: This permission is associated with the ability to add new accounts to the CyberArk Vault. It is typically found in the Vault's administrative settings where account management is handled.
? Initiate CPM account management operations: This permission allows users to initiate operations related to the Central Policy Manager (CPM) for account management within a Safe. It is found in the Safe's permissions settings.
? Add/Update Users: This permission enables the addition or updating of user information in the Vault. It is found in the Vault's user management settings.
? Add Safes: This permission is related to the creation of new Safes in the Vault. It is found in the Vault's administrative settings where Safe management is conducted.
References:
? The permissions and their locations can be referenced in the CyberArk Defender PAM course materials and official documentation, which provide detailed information on the management of permissions within the CyberArk solution.

NEW QUESTION 170
When onboarding multiple accounts from the Pending Accounts list, which associated setting must be the same across the selected accounts?

A. Platform
B. Connection Component
C. CPM
D. Vault

Answer: A

Explanation:
When onboarding multiple accounts from the Pending Accounts list, all the selected accounts must be associated with the same platform. This is necessary because the platform setting determines how the accounts will be managed within CyberArk, including the policies and behaviors that apply to those accounts. If an account contains dependencies, those dependencies are automatically onboarded with the account. This ensures that all accounts and their dependencies are managed consistently and according to the correct policies1.
References:
? CyberArk's official documentation on Onboarding Accounts and SSH Keys1.

NEW QUESTION 175
What can you do to ensure each component server is operational?

A. Logon to PVWA with v10 UI, navigate to Healthcheck, and validate each component server is connected to the Vault.
B. Ping each component server to ensure connectivity.
C. Use the PrivateArk client to connect to the Vault server and validate all the services are running.
D. 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.

Answer: A

Explanation:
To ensure that each component server is operational, you can log on to the Privileged Vault Web Access (PVWA) with the version 10 user interface, navigate to the Healthcheck section, and validate that each component server is connected to the Vault. The System Health dashboard in PVWA provides a high-level visual representation of the health status of the different CyberArk components, including whether the Vault service is up and whether the component servers are connected1.
References:
? CyberArk Docs - Monitor system health

NEW QUESTION 179
It is possible to control the hours of the day during which a user may log into the vault.

A. TRUE
B. FALSE

Answer: A

Explanation:
It is possible to control the hours of the day during which a user may log into the vault by using the Time Restrictions feature. This feature allows administrators to define the days and times that users can access the vault. Users who try to log in outside the permitted hours will be denied access and receive a message informing them of the restriction. Time restrictions can be applied to individual users or groups of users. References:
? [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.3:
User Management, Slide 7: Time Restrictions
? [Defender PAM Sample Items Study Guide], Question 2: Time Restrictions

? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 4: Managing Users and Groups, Section: Time Restrictions

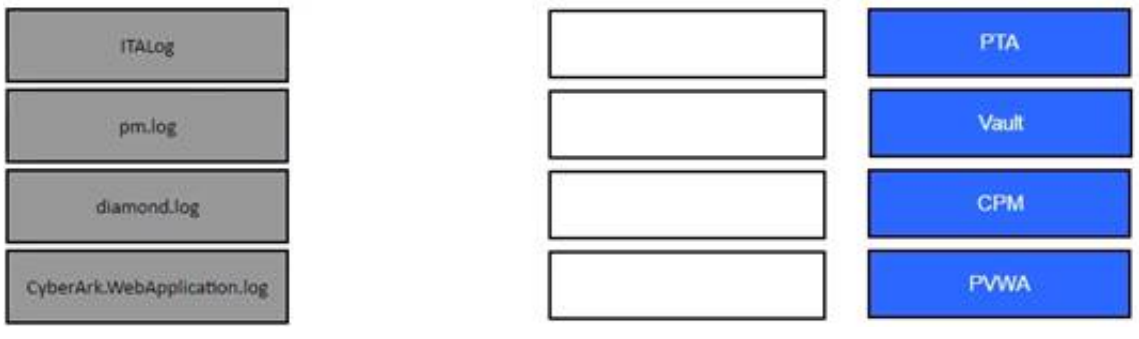
NEW QUESTION 184
Can the 'Connect' button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?

A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction.
B. Yes, only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component.
C. Yes, if a logon account is associated with the root account.
D. No, it is not possible.

Answer: B

Explanation:
The 'Connect' button is a feature of the PVWA that allows users to initiate a privileged session to a target system through PSM without revealing the account credentials. The 'Connect' button can be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, but only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component. A logon account is a linked account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the PSM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the PSM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account. The PSM-SSH connection component is a predefined connection component that enables users to connect to Unix systems through PSM using SSH. The PSM-SSH connection component supports the use of logon accounts to access root accounts on Unix systems1.
The other options are not correct, because:
? A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction. This is not correct, because PMTerminal.exe is a process that is used by the PSM-RDP connection component, not the PSM-SSH connection component. PMTerminal.exe is a terminal emulator that enables users to connect to Windows systems through PSM using RDP. PMTerminal.exe does not bypass the root SSH restriction, but rather uses the credentials stored in the Vault to authenticate to the target system2.
? C. Yes, if a logon account is associated with the root account. This is not correct, because a logon account alone is not sufficient to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied. The user also needs to connect through the PSM-SSH connection component, which supports the use of logon accounts to access root accounts on Unix systems1.
? D. No, it is not possible. This is not correct, because it is possible to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, as explained in option B.
References:
? 1: Logon Accounts for SSH and Telnet Connections
? 2: Connect through PSM for SSH

NEW QUESTION 186
DRAG DROP
Match the log file name with the CyberArk Component that generates the log.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
? Log Files
? [Defender PAM Sample Items Study Guide], Question 46, page 16

NEW QUESTION 190
In addition to add accounts and update account contents, which additional permission on the safe is required to add a single account?

A. Upload Accounts Properties
B. Rename Accounts
C. Update Account Properties
D. Manage Safe

Answer: C

Explanation:
In addition to the permissions to add accounts and update account contents, the permission to Update Account Properties is required to add a single account to a safe in CyberArk. This permission allows the user to modify the properties of an account, which is a necessary step when adding a new account to ensure that all relevant details and configurations are correctly set1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the permissions required for account management as outlined in CyberArk's official documentation

NEW QUESTION 192

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

A. Master Policy
B. Safe Templates
C. PVWAConfig.xml
D. Platform Configuration

Answer: D

Explanation:
The platform configuration defines the password management settings for each type of account, such as the password complexity, rotation frequency, verification method, and reconciliation options. You can set the regulatory requirement for password rotation in the platform configuration by specifying the number of days in the Password Change Interval parameter. This parameter determines how often the CPM will change the passwords of the accounts that are associated with the platform. For example, if you set the Password Change Interval to 90, the CPM will change the passwords every 90 days. References: Credentials Rotation - CyberArk, How do I manage or change passwords stored in CyberArk?

NEW QUESTION 194
A newly created platform allows users to access a Linux endpoint. When users click to connect, nothing happens.
Which piece of the platform is missing?

A. PSM-SSH Connection Component
B. UnixPrompts.ini
C. UnixProcess.ini
D. PSM-RDP Connection Component

Answer: A

Explanation:
A platform is a set of parameters that defines how CyberArk manages passwords and sessions for a specific type of account or system. To allow users to access a Linux endpoint, the platform needs to have a PSM-SSH connection component, which enables transparent connections to Linux machines using the SSH protocol. The PSM-SSH connection component is configured in the Master Policy and defines the settings for the PSM connection, such as the port, the authentication method, and the terminal type. If the platform is missing the PSM-SSH connection component, the users will not be able to click to connect to the Linux endpoint. References: Connection Components, PSM-SSH Connection Component

NEW QUESTION 195
Where can reconcile and/or logon accounts be linked to an account? (Choose two.)

A. account settings
B. platform settings
C. master policy
D. safe settings
E. service account settings

Answer: BD

Explanation:
Reconcile and logon accounts can be linked to an account within the platform settings and safe settings. The platform settings define the parameters for its linked accounts in either the Target Account or Service Account that requires them. When linked accounts are specified in the Target Account platform, they appear in the CPM pane of the Account Details page. Similarly, when they are specified in the Service Account platform, they appear in the CPM pane of the Service Account Details page1. Safe settings are also involved in the process of linking accounts, as they determine where the accounts are stored and managed within the CyberArk Vault.
References:
? CyberArk Docs - Linked Accounts1
? CyberArk REST API documentation on adding Reconcile and Login Accounts to an Account

NEW QUESTION 199
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 200
Which item is an option for PSM recording customization?

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

Answer: C

Explanation:
For PSM recording customization, one of the options is to use the Universal keystrokes text recorder with theWindows events text recorder disabled. This configuration allows for the recording of all keystrokes that are typed during privileged sessions on all supported connections. However, it is important to note that Universal keystroke recording andWindows events recordings cannot be configured for the same PSM-RDP connection. By default, Windows events text recording is enabled for PSM-RDP connections, so to enable universal keystrokes text recording, the Windows events text recording must first be disabled1.
References:
? CyberArk's official documentation on configuring recordings and audits in PSM, which includes details on how to customize text recorders and the limitations of configuring multiple recorders for the same connection1

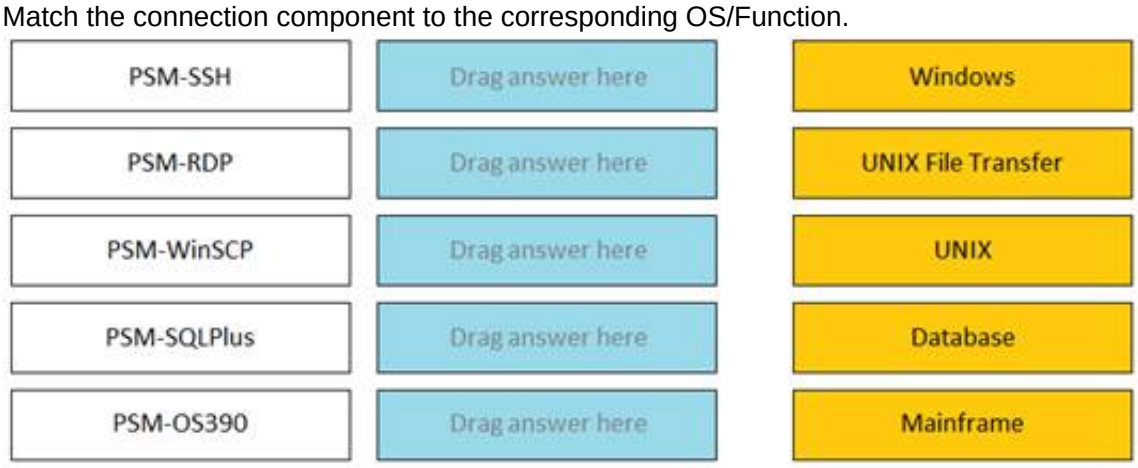
NEW QUESTION 202
tsparm.ini is the main configuration file for the Vault.

A. True
B. False

Answer: B

Explanation:
tsparm.ini isnot 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 mode. References:
? Defender PAM Sample Items Study Guide, page 9, question 92
? CyberArk Privileged Access Security Implementation Guide, page 75, section "DBParm.ini"
? CyberArk Vault Server Parameter Files, page 1, section "TSParm.ini"

NEW QUESTION 204
DRAG DROP
Match the connection component to the corresponding OS/Function.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? A connection component is a set of parameters that defines how PSM connects to a target system using a specific protocol or application. Different connection components are suitable for different types of systems or functions. The correct matches are as follows:
? PSM-SSH: This connection component enables transparent connections to UNIX machines using the SSH protocol. It supports various UNIX flavors, such as Linux, Solaris, AIX, and HP-UX.
? PSM-RDP: This connection component enables transparent connections to Windows machines using the RDP protocol. It supports various Windows versions, such as Windows Server, Windows 10, and Windows 7.
? PSM-WinSCP: This connection component enables transparent connections to UNIX machines using the WinSCP application. It supports file transfer operations, such as upload, download, delete, and rename, between the local and remote machines.
? PSM-SQLPlus: This connection component enables transparent connections to Oracle databases using the SQL*Plus application. It supports various Oracle versions, such as Oracle 12c, Oracle 11g, and Oracle 10g.
? PSM-OS390: This connection component enables transparent connections to IBM mainframes using the OS/390 protocol. It supports various mainframe applications, such as TSO, CICS, and IMS.
References: Connection Components, Connection Component Parameters

NEW QUESTION 205
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 207
Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.

A. TRUE
B. FALSE

Answer: B

Explanation:
Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The 'Access Safe without confirmation' safe permission is a special permission that allows a user to bypass the Dual control mechanism and access the accounts in the safe without requiring confirmation from other authorized users. This permission can be useful for emergency situations or trusted users who need immediate access to the accounts. However, this permission also increases the risk of unauthorized or malicious access, so it should be granted with caution and monitored closely1.
References:
? 1: Access without confirmation

NEW QUESTION 208
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 212
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 217
Which is the primary purpose of exclusive accounts?

A. Reduced risk of credential theft
B. More frequent password changes
C. Non-repudiation (individual accountability)
D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization

Answer: D

Explanation:
According to the web search results, exclusive accounts are a feature of CyberArk Defender PAM that enables organizations to permit users to check out a 'one-time' password and lock it so that no other users can retrieve it at the same time1. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account1.
The primary purpose of exclusive accounts is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges. By requiring a check-out and check-in process, exclusive accounts ensure that there is a 'collusion to commit' fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. One user must check out the password and use it, while another user must approve the check-in and verify the password change. This way, exclusive accounts add an additional measure of protection and accountability for accessing sensitive accounts.

NEW QUESTION 218
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"

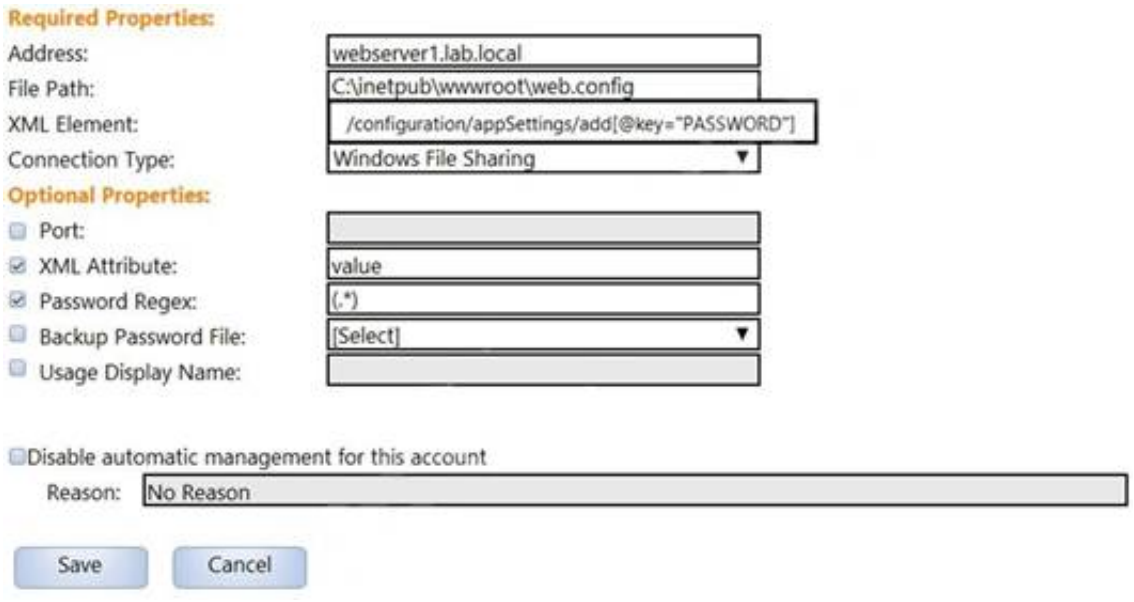
NEW QUESTION 219
In the Private Ark client, how do you add an LDAP group to a CyberArk group?

A. Select Update on the CyberArk group, and then click Add > LDAP Group
B. Select Update on the LDAP Group, and then click Add > LDAP Group
C. Select Member Of on the CyberArk group, and then click Add > LDAP Group
D. Select Member Of on the LDAP group, and then click Add > LDAP Group

Answer: C

Explanation:
To add an LDAP group to a CyberArk group, you need to use the Private Ark client and follow these steps1:
? In the Users and Groups tree, select the CyberArk group that you want to add the
LDAP group to.
? In the Properties pane, click Member Of.
? Click Add > LDAP Group.
? In the LDAP Group dialog box, enter the name of the LDAP group and click OK. References: Add an LDAP group to a Vault group

NEW QUESTION 220
In the screenshot displayed, you just configured the usage in CyberArk and want to update its password.
What is the least intrusive way to accomplish this?



A. Use the “change” button on the usage’s details page.
B. Use the “change” button on the parent account’s details page.
C. Use the “sync” button on the usage’s details page.
D. Use the “reconcile” button on the parent account’s details page.

Answer: C

Explanation:
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. To update the password of a usage, the least intrusive way is to use the “sync” button on the usage’s details page. This will synchronize the password value between the Vault and the file, without changing the actual password. The “change” button will initiate a password change process by the CPM, which will generate a new random password for the usage and the file. The “reconcile” button will initiate a password reconcile process by the CPM, which will use a reconcile account to reset the password of the usage and the file to the value stored in the Vault. References: Usages, Manage passwords for usages

NEW QUESTION 223
The password upload utility must run from the CPM server

A. TRUE
B. FALSE

Answer: A

Explanation:
According to the CyberArk documentation1, the Password Upload utility must run from the Central Policy Manager (CPM) server. This utility works by uploading passwords and their properties into the Password Vault from a pre-prepared file, creating the required environment, when necessary. It is run from a command line whenever a password upload is required1.

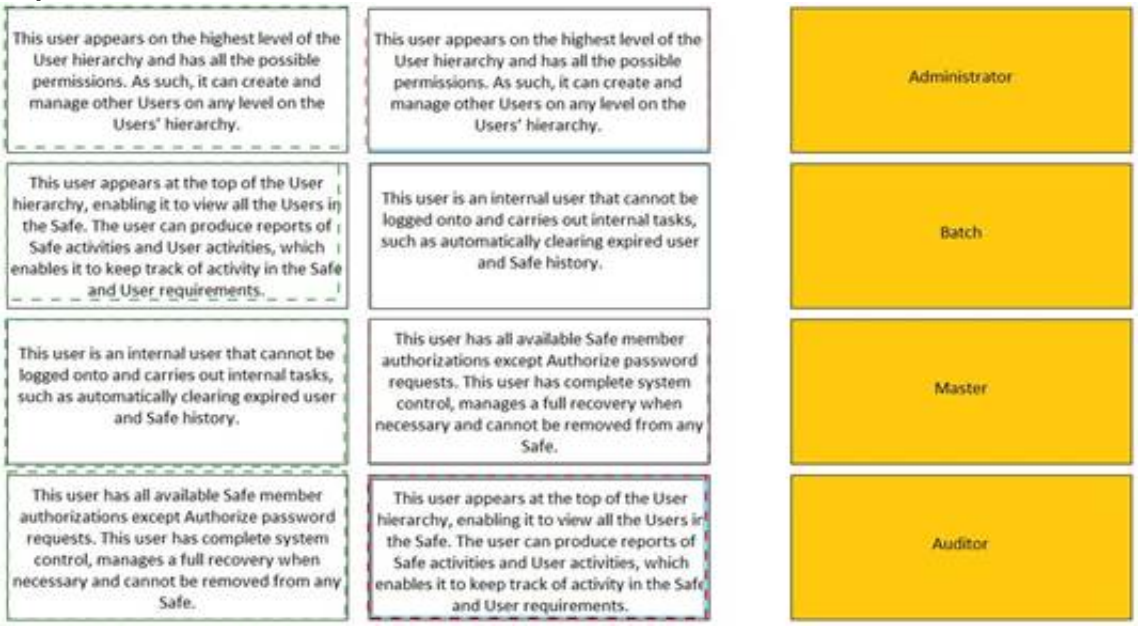
NEW QUESTION 226
You received a notification from one of your CyberArk auditors that they are missing Vault level audit permissions. You confirmed that all auditors are missing the Audit Users Vault permission.
Where do you update this permission for all auditors?

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 231
DRAG DROP
Match the built-in Vault User with the correct definition.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 236
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.
B. Search common community portals like stackoverflow, reddit, github for an existing platform.
C. From the platforms page, uncheck the “Hide non-supported platforms” checkbox and see if a platform meeting your needs appears.
D. Visit the CyberArk marketplace and search for a platform that meets your needs.

Answer: D

Explanation:
The CyberArk marketplace is a platform that simplifies delivery of privileged access security solutions, such as CyberArk Privileged Account Security Solution. It features the industry’s broadest and deepest portfolio of technology integrations, including platforms for various types of accounts. Customers can find and deploy integrations with CyberArk Marketplace in as little as four clicks. If there is no platform that meets the customer’s needs, they can request a custom platform from CyberArk or create their own using the Platform Development Kit (PDK). References: CyberArk Marketplace, Platform Development Kit

NEW QUESTION 241
Which onboarding method would you use to integrate CyberArk with your accounts provisioning process?

A. Accounts Discovery
B. Auto Detection
C. Onboarding RestAPI functions
D. PTA Rules

Answer: C

Explanation:
The Onboarding RestAPI functions are a set of web services that allow you to integrate CyberArk with your accounts provisioning process. You can use the Onboarding RestAPI functions to create, update, delete, or verify accounts in the CyberArk Vault, as well as to retrieve information about accounts, platforms, and safes. The Onboarding RestAPI functions are part of the Central Credential Provider component, which is installed on a dedicated server that communicates with the Vault. References:
? [Defender PAM Course], Module 4: Onboarding Accounts, Lesson: Onboarding
RestAPI Functions
? [Onboarding RestAPI Functions Guide], Introduction

NEW QUESTION 243
To enable the Automatic response “Add to Pending” within PTA when unmanaged credentials are found, what are the minimum permissions required by PTAUser for the PasswordManager_pending safe?

A. List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties
B. List Accounts, Add accounts (includes update properties), Delete Accounts, Manage Safe
C. Add accounts (includes update properties), Update Account content, Update Account properties, View Audit
D. View Accounts, Update Account content, Update Account properties, Access Safe without confirmation, Manage Safe, View Audit

Answer: A

Explanation:
To enable the automatic response “Add to Pending” within PTA when unmanaged credentials are found, the PTAUser needs to have the minimum permissions for the PasswordManager_pending safe as follows:
? List Accounts: This permission allows the PTAUser to view the accounts in the safe and their properties.
? View Safe members: This permission allows the PTAUser to view the members of the safe and their authorizations.
? Add accounts (includes update properties): This permission allows the PTAUser to add new accounts to the safe and update their properties, such as name, address, platform, and policy.
? Update Account content: This permission allows the PTAUser to update the password of the accounts in the safe.
? Update Account properties: This permission allows the PTAUser to update the properties of the existing accounts in the safe, such as name, address, platform, and policy.
These permissions are required for the PTAUser to be able to detect unmanaged privileged accounts and add them to the pending accounts queue in the PasswordManager_pending safe. The PTAUser also needs to have the same permissions for the PasswordManager_reconcile safe to enable the automatic response “Reconcile credentials” for suspicious password change events. References: Configure PTA Remediations, Safe Member Authorizations

NEW QUESTION 247
Which values are acceptable in the address field of an Account?

A. It must be a Fully Qualified Domain Name (FQDN)
B. It must be an IP address
C. It must be NetBIOS name
D. Any name that is resolvable on the Central Policy Manager (CPM) server is acceptable

Answer: D

Explanation:
The address field of an Account is used to identify the target system where the Account is located. The CPM uses this address to connect to the target system and perform password management operations. Therefore, the address field can be any name that is resolvable on the CPM server, such as a FQDN, an IP address, a NetBIOS name, or a custom name defined in the hosts file of the CPM server. References:
? Defender PAM Sample Items Study Guide, page 9, question 91
? CyberArk Privileged Access Security Implementation Guide, page 75, section “Address”

NEW QUESTION 248
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 251
How much disk space do you need on the server for a PAReplicate?

A. 500 GB
B. 1 TB
C. same as disk size on Satellite Vault
D. same as disk size on Primary Vault

Answer: D

Explanation:
The PAReplicate utility exports the Safe files from the CyberArk Vault to a computer on the local network where the Backup utility has been installed. The Safes are copied in a similar format and structure to the one in the Server. Therefore, the disk space required on the server for a PAReplicate is the same as the disk size on the Primary Vault1. References: Use the CyberArk Backup Process

NEW QUESTION 256
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?

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.

Answer: C

Explanation:
One-time passwords and exclusive access are security features that can be configured for a platform in the Master Policy. These features enhance the security and accountability of shared accounts by ensuring that each password is used only once and by only one user at a time. One-time passwords generate a new password for each check- out and check-in of an account, preventing password reuse and exposure. Exclusive access prevents multiple users from accessing the same account simultaneously, avoiding conflicts and confusion. By configuring both one-time passwords and exclusive access for the appropriate platform, the account owner can track who was using an account at any given moment and ensure that the passwords are always secure and unique. References
: One-Time Passwords, Exclusive Access, Master Policy

NEW QUESTION 261
Users are unable to launch Web Type Connection components from the PSM server. Your manager asked you to open the case with CyberArk Support.
Which logs will help the CyberArk Support Team debug the issue? (Choose three.)

A. PSMConsole.log
B. PSMDebug.log
C. PSMTrace.log
D. <Session_ID>.Component.log
E. PMconsole.log
F. ITAlog.log

Answer: ACD

Explanation:
When users are unable to launch Web Type Connection components from the PSM server, the CyberArk Support Team will require specific logs to debug the issue. The logs that are typically helpful in such cases include:
? PSMConsole.log: This log file contains informational messages and errors related to the PSM function, which can help identify issues with the PSM server's operation1.
? PSMTrace.log: This log file includes errors and trace messages, which can provide detailed insights into the issues occurring during the PSM server's processes1.
? <Session_ID>.Component.log: This log file contains errors and trace messages related to the connection component, which can be crucial for troubleshooting issues with launching Web Type Connection components1.
These logs can provide the necessary information to understand the problem and assist the support team in resolving the issue effectively.
References:
? CyberArk's official documentation on PSM for Web Troubleshooting, which outlines the types of logs available and their purposes in the troubleshooting process1.
? Additional resources on managing and interpreting PSM logs, which provide guidance on using logs for diagnosing and resolving issues with the PSM server2

NEW QUESTION 265
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 266
You have been asked to identify the up or down status of Vault services. Which CyberArk utility can you use to accomplish this task?

A. Vault Replicator
B. PAS Reporter
C. Remote Control Agent
D. Syslog

Answer: C

Explanation:
The Remote Control Agent (PARAgent) is a CyberArk utility that can be used to monitor the status of Vault services remotely. It can also perform other tasks, such as starting and stopping the Vault, backing up and restoring the Vault, and running other utilities. The PARAgent communicates with the Remote Control Client (PARClient), which is a graphical user interface that displays the Vault status and allows the user to execute commands on the Vault. The PARAgent can also send SNMP traps to a remote terminal if the Vault service is down. References: How do I monitor the Vault status remotely?, Monitor system health

NEW QUESTION 267
What must you specify when configuring a discovery scan for UNIX? (Choose two.)

A. Vault Administrator
B. CPM Scanner
C. root password for each machine
D. list of machines to scan
E. safe for discovered accounts

Answer: BD

Explanation:

When configuring a discovery scan for UNIX, you must specify theCPM Scanner and thelist of machines to scan. The CPM Scanner is the component responsible for executing the discovery process, and it requires a list of target machines to scan for new and modified accounts and their dependencies. This list can be provided in the form of a CSV file for UNIX machines1. The discovery process will then scan the predefined machines to identify privileged accounts that should be onboarded into the Vault for secure and automated management according to enterprise compliance policies2. References:
? CyberArk Docs - Manage discovery processes1
? CyberArk Docs - Scan for accounts using Account Discovery

NEW QUESTION 270
What is the purpose of the password change process?

A. To test that CyberArk is storing accurate credentials for accounts
B. To change the password of an account according to organizationally defined password rules
C. To allow CyberArk to manage unknown or lost credentials
D. To generate a new complex password

Answer: B

Explanation:
The purpose of the password change process is to change the password of an account according to organizationally defined password rules. The password change process is a feature of CyberArk that enables the Central Policy Manager (CPM) to manage the passwords of privileged accounts that are stored in the Vault. The CPM can change the passwords automatically or manually, based on predefined policies, schedules, or user requests. The password change process ensures that the passwords are secure, compliant, and synchronized with the target systems and the Vault. The password change process also supports different types of accounts, such as one-time passwords, exclusive accounts, and dual accounts1.
The other options are not the main purpose of the password change process, although they may be related to some aspects of it. The password change process does not test that CyberArk is storing accurate credentials for accounts, although it may verify the password validity before changing it. The password change process does not allow CyberArk to manage unknown or lost credentials, although it may reconcile the passwords if they are out of sync with the target systems. The password change process does not generate a new complex password, although it may use a random password generation mechanism to create a new password that meets the password policy requirements. References:
? Change Passwords - CyberArk, section “Change Passwords”

NEW QUESTION 275
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PAM-DEF Practice Exam Features:

* PAM-DEF Questions and Answers Updated Frequently

* PAM-DEF Practice Questions Verified by Expert Senior Certified Staff

* PAM-DEF Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PAM-DEF Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year