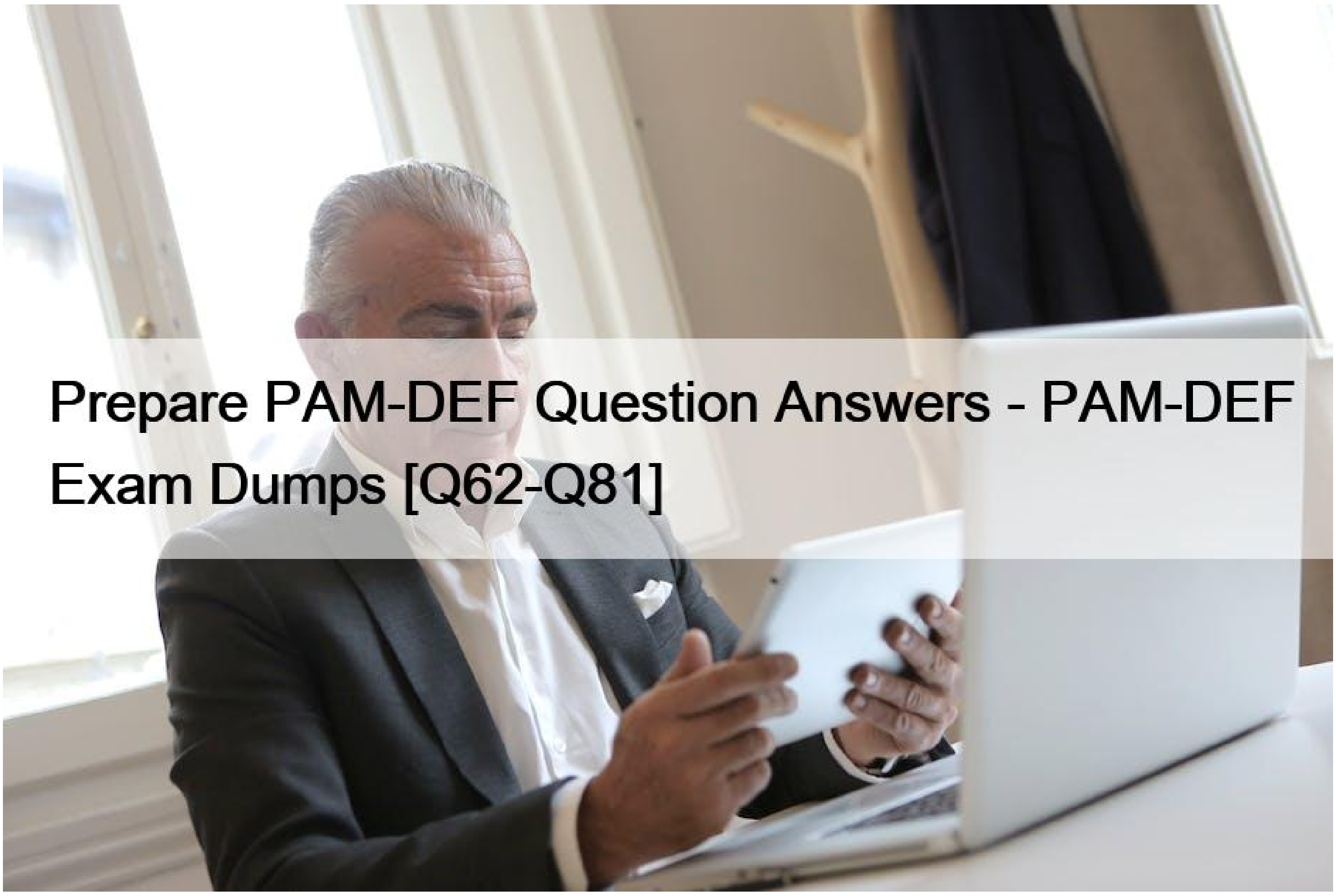
Prepare PAM-DEF Question Answers - PAM-DEF Exam Dumps [Q62-Q81



Prepare PAM-DEF Question Answers - PAM-DEF Exam Dumps
Real CyberArk PAM-DEF Exam Questions [Updated 2025]

NO.62 In accordance with best practice, SSH access is denied for root accounts on UNIX/LINUX system. What is the BEST way to allow CPM to manage root accounts.
* Create a privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Reconcile account of the target server&#8217;s root account.
* Create a non-privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Logon account of the target server&#8217;s root account.
* Configure the Unix system to allow SSH logins.
* Configure the CPM to allow SSH logins.

NO.63 You need to enable the PSM for all platforms.

Where do you perform this task?
* Platform Management > (Platform) > UI & Workflows
* Master Policy > Session Management
* Master Policy > Privileged Access Workflows

* Administration > Options > Connection Components
Explanation

To enable PSM for specific platforms, you need to go to Platform Management, select the platform you want to configure, click Edit, expand UI & Workflows, and select Privileged Session Management. There you can customize the PSM settings for that platform, such as the PSM server ID, the connection components, the PSM connection method, and the PSM recording options. You can also disable dual control for PSM connections if needed. References: Configure PSM for Specific Platforms

NO.64 Where can a user with the appropriate permissions generate a report? (Choose two.)
* PVWA > Reports
* PrivateArk Client
* Cluster Vault Manager
* PrivateArk Server Monitor
* PARClient

NO.65 The Vault administrator can change the Vault license by uploading the new license to the system Safe.
* True
* False
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.

NO.66 What is the purpose of the Immediate Interval setting in a CPM policy?
* To control how often the CPM looks for System Initiated CPM work.
* To control how often the CPM looks for User Initiated CPM work.
* To control how often the CPM rests between password changes.
* To Control the maximum amount of time the CPM will wait for a password change to complete.

NO.67 Which one the following reports is NOT generated by using the PVWA?
* Accounts Inventory
* Application Inventory
* Sales List
* Convince Status

NO.68 You are onboarding 5,000 UNIX root accounts for rotation by the CPM. You discover that the CPM is unable to log in directly with the root account and will need to use a secondary account.

How should this be configured to allow for password management using least privilege?
* Configure each CPM to use the correct logon account.
* Configure each CPM to use the correct reconcile account.
* Configure the UNIX platform to use the correct logon account.
* Configure the UNIX platform to use the correct reconcile account.

NO.69 Customers who have the &#8216;Access Safe without confirmation&#8217; safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.
* TRUE
* FALSE

NO.70 When should vault keys be rotated?

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

NO.71 A user needs to view recorded sessions through the PVWA.

Without giving auditor access, which safes does a user need access to view PSM recordings? (Choose two.)
* Recordings safe
* Safe the account is in
* System safe
* PVWAConfiguration safe
* VaultInternal safe
Explanation

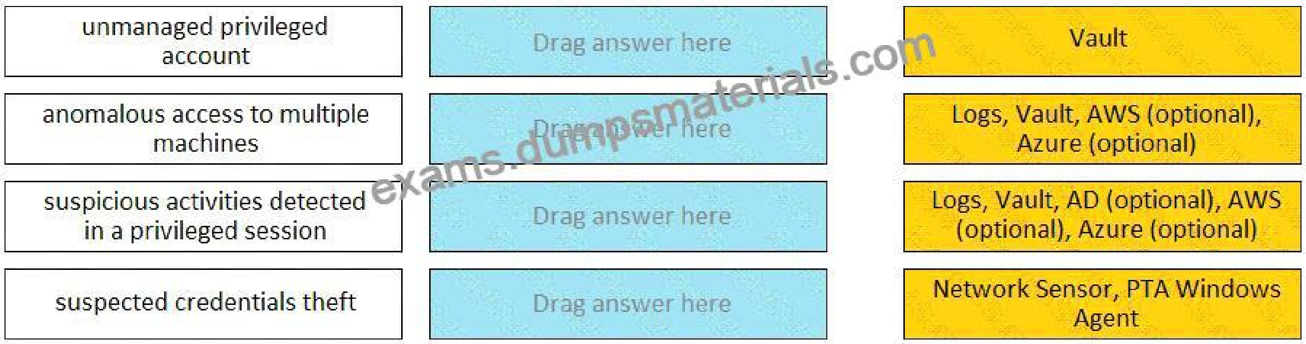
To view recorded sessions through the PVWA without having auditor access, a user needs access to two specific safes: the Recordings safe and the safe the account is in. The Recordings safe is where the PSM session recordings are stored, and users need permission to access this safe to view the recordings. Additionally, users need access to the safe where the account associated with the recorded session is stored, as this is where the session details and permissions are managed12.

References:

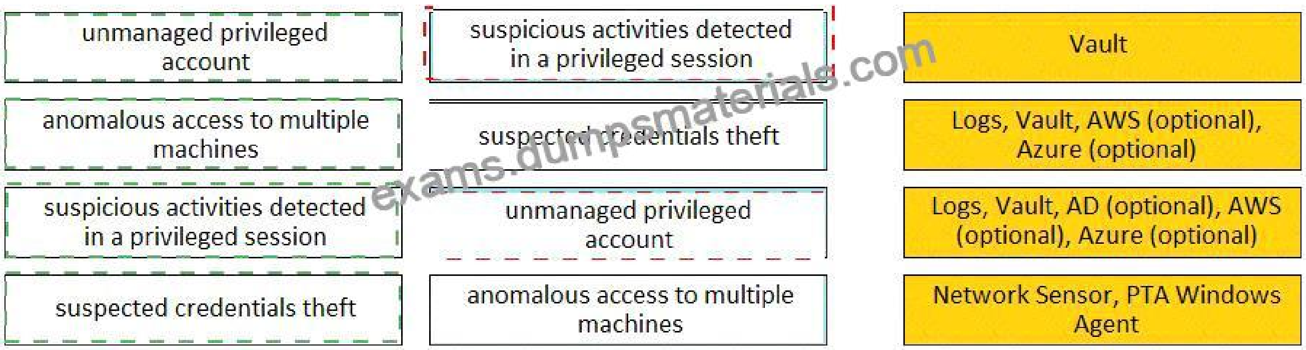
* CyberArk Docs &#8211; Configure video and text recordings3

* CyberArk Community &#8211; Viewing PSM recorded sessions1

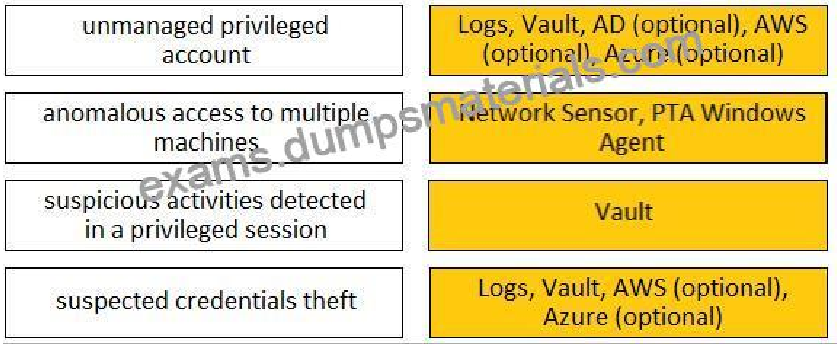
NO.72 Match each PTA alert category with the PTA sensors that collect the data for it.



unmanaged privileged account	Drag answer here	Vault
anomalous access to multiple machines	Drag answer here	Logs, Vault, AWS (optional), Azure (optional)
suspicious activities detected in a privileged session	Drag answer here	Logs, Vault, AD (optional), AWS (optional), Azure (optional)
suspected credentials theft	Drag answer here	Network Sensor, PTA Windows Agent



unmanaged privileged account	suspicious activities detected in a privileged session	Vault
anomalous access to multiple machines	suspected credentials theft	Logs, Vault, AWS (optional), Azure (optional)
suspicious activities detected in a privileged session	unmanaged privileged account	Logs, Vault, AD (optional), AWS (optional), Azure (optional)
suspected credentials theft	anomalous access to multiple machines	Network Sensor, PTA Windows Agent



unmanaged privileged account	Logs, Vault, AD (optional), AWS (optional), Azure (optional)
anomalous access to multiple machines	Network Sensor, PTA Windows Agent
suspicious activities detected in a privileged session	Vault
suspected credentials theft	Logs, Vault, AWS (optional), Azure (optional)

NO.73 You need to enable the PSM for all platforms.

Where do you perform this task?
* Platform Management > (Platform) > UI & Workflows
* Master Policy > Session Management
* Master Policy > Privileged Access Workflows
* Administration > Options > Connection Components

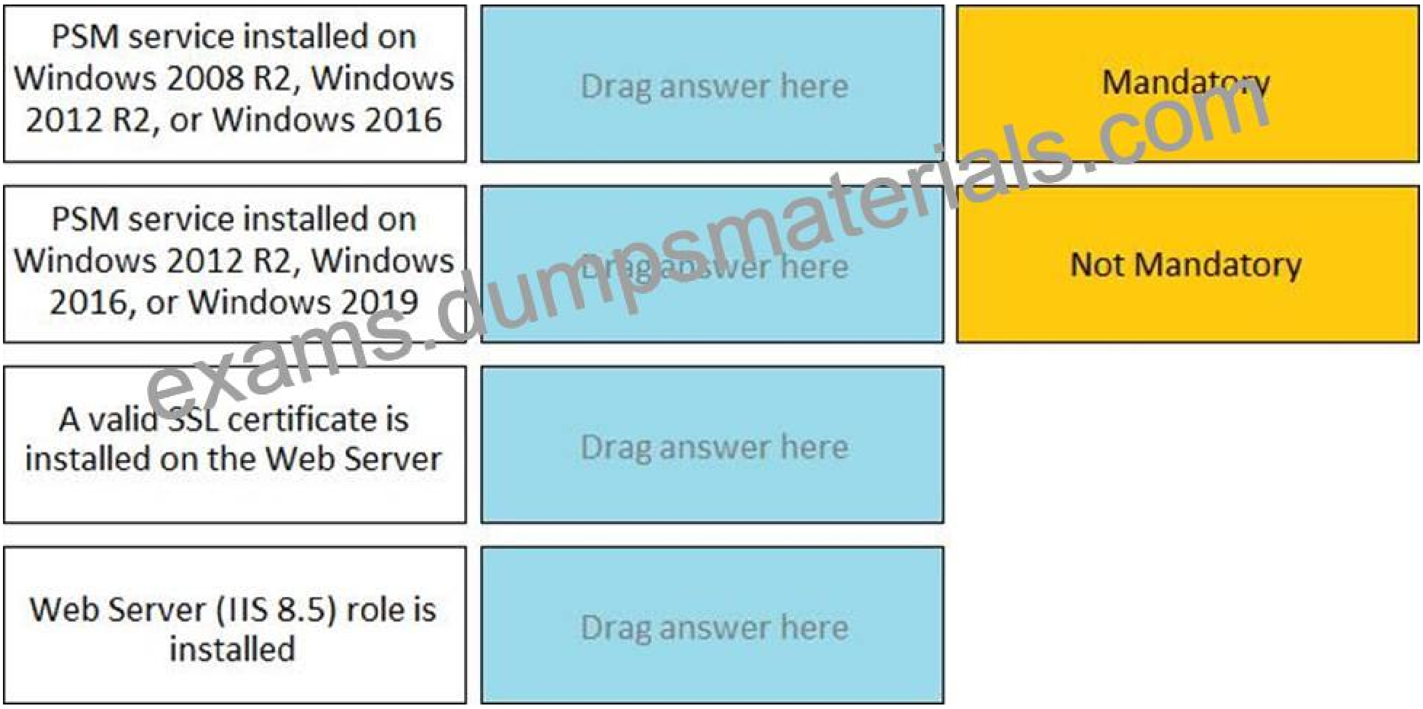
NO.74 One can create exceptions to the Master Policy based on ____________________.
* Safes
* Platforms
* Policies
* Accounts

NO.75 You are creating a Dual Control workflow for a team&#8217;s safe.

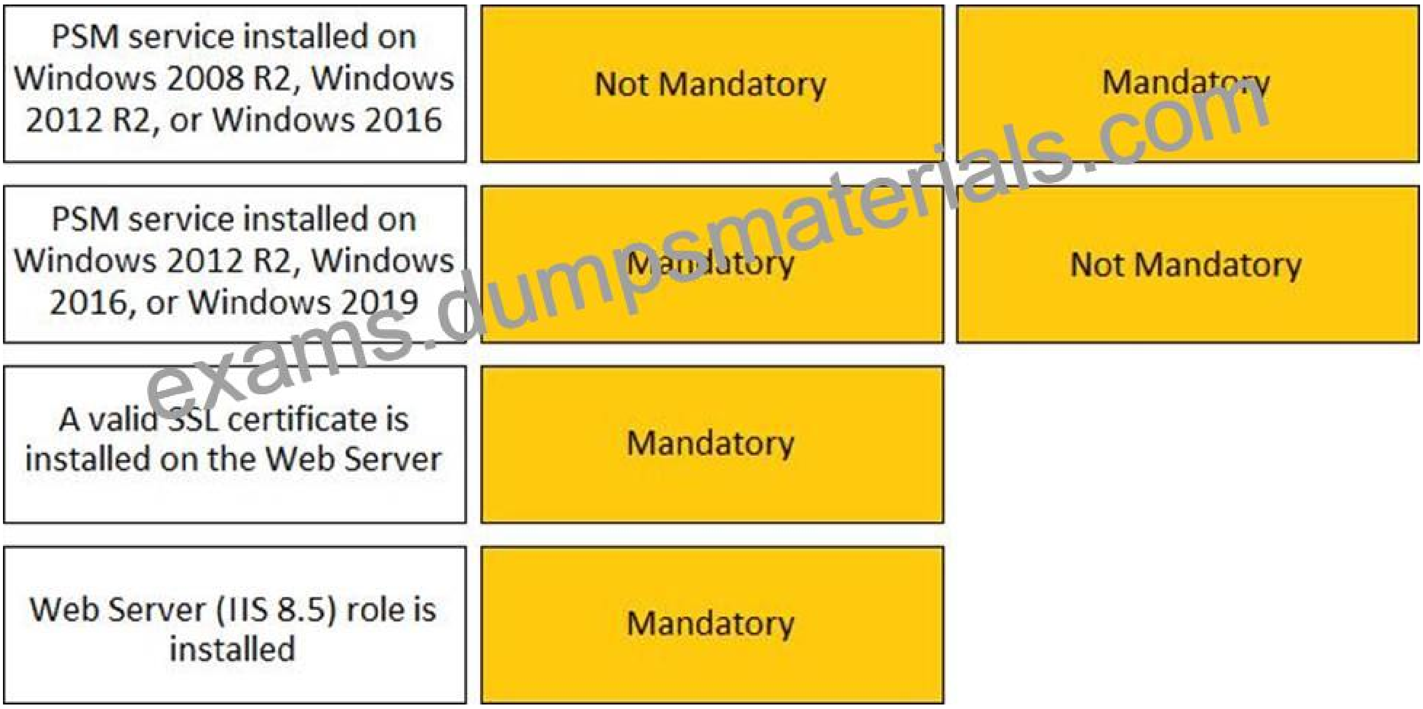
Which safe permissions must you grant to the Approvers group?
* List accounts, Authorize account request
* Retrieve accounts, Access Safe without confirmation
* Retrieve accounts, Authorize account request
* List accounts, Unlock accounts

NO.76 DRAG DROP

For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.



PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016	Drag answer here	Mandatory
PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019	Drag answer here	Not Mandatory
A valid SSL certificate is installed on the Web Server	Drag answer here	
Web Server (IIS 8.5) role is installed	Drag answer here	



PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016	Not Mandatory	Mandatory
PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019	Mandatory	Not Mandatory
A valid SSL certificate is installed on the Web Server	Mandatory	
Web Server (IIS 8.5) role is installed	Mandatory	

NO.77 You notice an authentication failure entry for the DR user in the ITALog.

What is the correct process to fix this error? (Choose two.)
* PrivateArk Client > Tools > Administrative Tools > Users and Groups > DR User > Update > Authentication > Update Password.
* Create a new credential file, on the DR Vault, using the CreateCredFile utility and the newly set password.

. Create a new credential file, on the Primary Vault, using the CreateCredFile utility and the newly set password.
* PVWA > User Provisioning > Users and Groups > DR User > Update Password.

* PrivateArk Client > Tools > Administrative Tools > Users and Groups > PAReplicate User > Update > Authentication > Update Password.

NO.78 VAULT authorizations may be granted to_____.
* Vault Users
* Vault Groups
* LDAP Users
* LDAP Groups
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

NO.79 Your organization requires all passwords be rotated every 90 days.

Where can you set this regulatory requirement?
* Master Policy
* Safe Templates
* PVWAConfig.xml
* Platform Configuration
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 &#8211; CyberArk, How do I manage or change passwords stored in CyberArk?

NO.80 When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.
* True; this is the default behavior
* False, the Vault administrator must manually set the DR Vault to DR mode by setting &#8220;FailoverMode=no&#8221; in the padr.ini file
* True, if the AllowFailback setting is set to &#8220;yes&#8221; in the padr.ini file
* False, the Vault administrator must manually set the DR Vault to DR mode by setting &#8220;FailoverMode=no&#8221; in the dbparm.ini file

NO.81 As long as you are a member of the Vault Admins group you can grant any permission on any safe.
* TRUE
* FALSE
Explanation

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

* Predefined users and groups

* Safe member authorizations