CyberArk.CPC-CDE-RECERT.v2026-09-18.q34

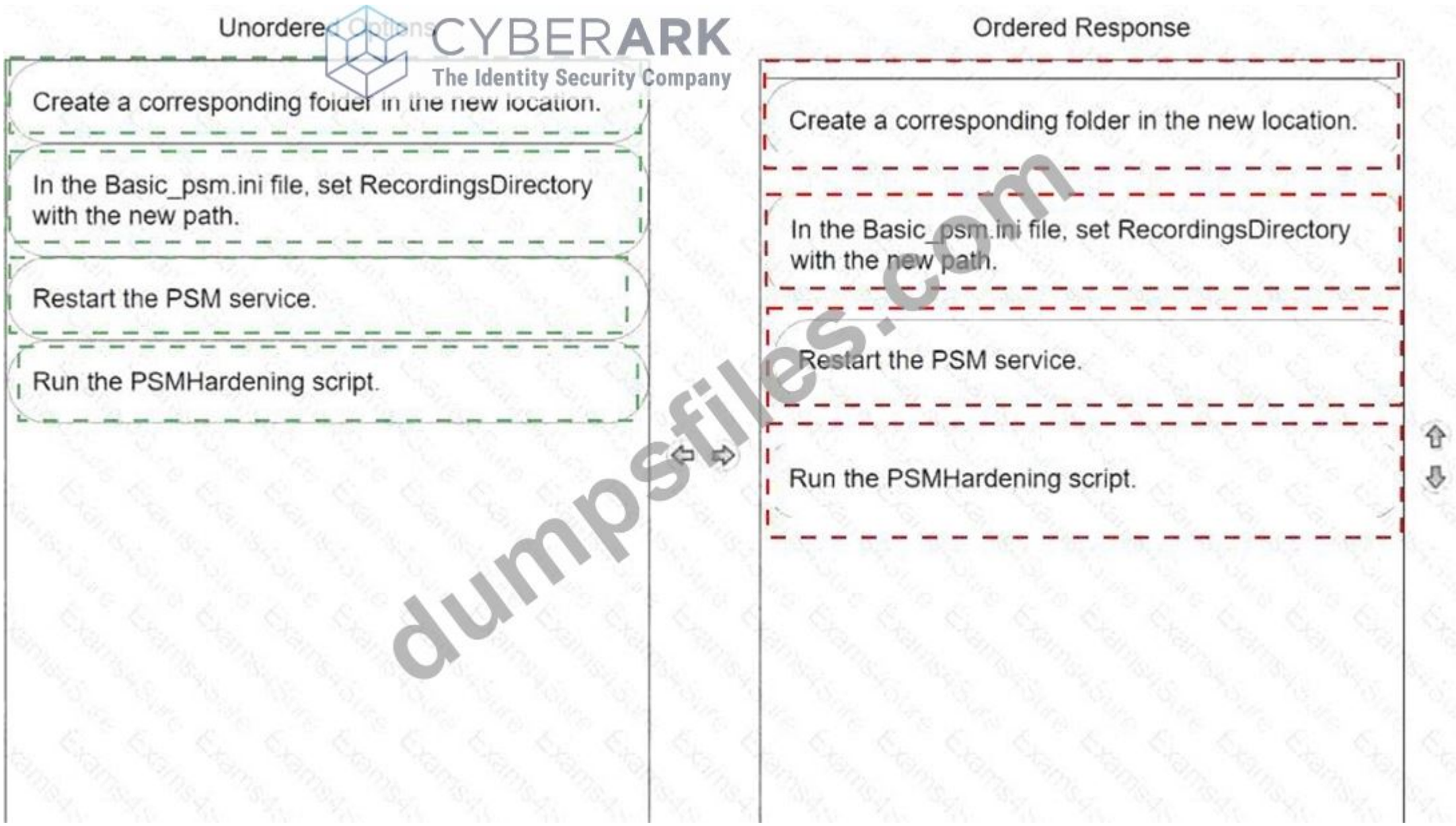
Exam Code:	CPC-CDE-RECERT
Exam Name:	CyberArk CDE-CPC Recertification
Certification Provider:	CyberArk
Free Question Number:	34
Version:	v2026-09-18
# of views:	328
# of Questions views:	455
https://www.dumpsfiles.com/files/CyberArk/CPC-CDE-RECERT/CyberArk.CPC-CDE-RECERT.v2026-09-18.q34	

NEW QUESTION: 1
You want to change the default PSM recordings folder path on the Privilege Cloud Connector Arrange the steps to accomplish this in the correct sequence.

Unordered Options

- Create a corresponding folder in the new location.
- In the Basic_psm.ini file, set RecordingsDirectory with the new path.
- Restart the PSM service.
- Run the PSMHardening script.

Answer:



Explanation:

To correctly change the default PSM recordings folder path on the Privilege Cloud Connector, the sequence of steps should be:

* Create a corresponding folder in the new location.Before making changes to configuration files, ensure the new directory for PSM recordings is created. This is where all session recordings will be stored moving forward.
* In the Basic_psm.ini file, set RecordingsDirectory with the new path.Update the Basic_psm.ini file to reflect the new path for the recordings. This step is crucial as it directs the PSM to start using the newly created directory for all future session recordings.
* Restart the PSM service.After updating the path in the configuration file, restart the PSM service to apply the changes. This ensures that all new sessions are recorded in the new specified location.
* Run the PSMHardening script.Once the service is restarted and the new settings are in place, run the PSMHardening script. This script ensures that all security measures are re-applied to the new recordings directory, maintaining the security integrity of the session recordings.

Following these steps in the given order will successfully change the recording directory for PSM sessions on the Privilege Cloud Connector, ensuring a smooth transition to the new storage location with all necessary security measures intact.

NEW QUESTION: 2

Which Safe(s) does the AllowedSafes=Win platform parameter configuration match? (Choose two.)

A. SQL-Win-SA

B. WindowsPasswords

C. win-ssh-keys

D. CXD-WIN-ADMINS

E. WiNdOwS_Accts

Answer: (SHOW ANSWER)

NEW QUESTION: 3

What is a requirement when installing the PSM on multiple Privileged Cloud Connector servers?
A. Each PSM must have the same path to the same recordings directory.
B. All PSMs in the environment must be configured to use load balancing.
C. Additional Privilege Cloud Connector servers cannot have CPM installed.
D. In-domain servers cannot be used when deploying multiple PSM servers.
Answer: (SHOW ANSWER)
When installing the Privileged Session Manager (PSM) on multiple servers, it is required that each PSM installation has the same path to the same recordings directory. This is necessary to ensure that session recordings are stored consistently across different PSM instances, which is important for high availability and load balancing implementations, as well as for maintaining a unified audit trail.
:
CyberArk documentation on installing multiple PSM servers

NEW QUESTION: 4
Before installing the Privilege Cloud Connector using Connector Management, which network rules should be in place?
A. VaultConnectivity: Privilege Cloud backend Port 1858
TunnelConnectivity: Secure Tunnel Port 443
CustomerPortalConnectivity: Port 443
B. VaultConnectivity: Privilege Cloud backend Port 1858
TunnelConnectivity: Secure Tunnel Port 5589
C. TunnelConnectivity: Secure Tunnel Port 443
CustomerPortalConnectivity: Port 5589
D. VaultConnectivity: Privilege Cloud backend Port 1858
TunnelConnectivity: Secure Tunnel Port 22
CustomerPortalConnectivity: Port 3389
Answer: A (LEAVE A REPLY)
CyberArk's Connector Management prerequisites check defines the exact network connectivity rules that must pass before installation:
* VaultConnectivity # Connect to the Privilege Cloud backend on TCP 1858
* TunnelConnectivity # Connect to the Secure Tunnel on TCP 443
* CustomerPortalConnectivity # Connect to the service backend URL on TCP 443 This matches option A exactly.

NEW QUESTION: 5
In addition to the Vault Admins and Auditors, what are the default map roles in the Privilege Cloud LDAP Directory mapping function for the Privilege Cloud Standard Services Model? (Choose two.)
A. Safe Managers
B. Safe Owners
C. Privileged Cloud Users
D. Users
Answer: (SHOW ANSWER)
In the Privilege Cloud LDAP integration workflow, CyberArk lists the default maps (built-in directory maps) as:
* Vault Admins
* Safe managers

* Auditors
* Users
Since the question asks for the default roles in addition to Vault Admins and Auditors, the remaining two default map roles are Safe managers and Users, which correspond to A and D.

NEW QUESTION: 6
A CyberArk Privileged Cloud Shared Services customer asks you how to find recent failed login events for all users. Where can you do this without generating reports?
A. Privileged Cloud Portal
B. Identity Administration Portal
C both Identity Administration and Identity User Portals
C. Identity User Portal
Answer: (SHOW ANSWER)

NEW QUESTION: 7
You plan to install Privilege Cloud Connectors on your AWS and Azure environments.
What is the maximum number of concurrent RDP/SSH sessions that each connector can handle for Large Implementations?
A. 1-10
B. 31-60
C. 100
D. 200
Answer: B (LEAVE A REPLY)
For large implementations of CyberArk Privilege Cloud Connectors in AWS and Azure environments, each connector can handle between 31-60 concurrent RDP/SSH sessions. This capacity is specified in the CyberArk documentation concerning Privilege Cloud Connectors and their scalability options. It is designed to support a higher volume of concurrent sessions to meet the needs of larger enterprise environments, ensuring that multiple users can securely access resources without significant performance degradation.

NEW QUESTION: 8
What is the purpose of the PSM Health Check hardening?
A. Remove IIS settings which can be considered security vulnerabilities.
B. Validate that the PSM is ready to be placed behind a load balancer.
C. Confirm that the Windows Services for PSM are running on the server.
D. Ensure that the AppLocker script does not have any syntax errors.
Answer: A (LEAVE A REPLY)
In CyberArk Privilege Cloud / PSM deployments, PSM Health Check is implemented as a dedicated PSM Web Service on each PSM node (typically used by a load balancer to query application-level health). (docs.
cyberark.com)
Because the Health Check relies on IIS, CyberArk includes PSM Health Check hardening activities as part of the setup. These hardening activities specifically focus on reducing IIS exposure by removing default

/unused IIS components (for example, CyberArk documents that the setup deletes IIS application pools such as "Classic .NET AppPool", ".NET v2.0", ".NET v4.5", etc.). This is a hardening action aimed at minimizing IIS attack surface / insecure defaults-i.e., removing IIS settings/configurations that could be considered security vulnerabilities. (docs.cyberark.com) Why the other options are not the "purpose":
* B: While Health Check is used for load balancer health probing, "hardening" is not about validating readiness for a load balancer; it's about tightening IIS-related configuration. (docs.cyberark.com)
* C: Service-running checks are part of health determination, but the hardening step is described in docs in terms of IIS hardening activities (like deleting app pools), not just confirming services. (docs.
cyberark.com)
* D: AppLocker is part of PSM hardening overall, but it's not the purpose of PSM Health Check hardening (which is IIS-focused). (docs.cyberark.com)

NEW QUESTION: 9
What must be done to configure the syslog server IP address(es) for SIEM integration? (Choose 2.)
A. Submit a service request to CyberArk Support.
B. Update the syslog server IP address through the Privilege Cloud Portal.
C. Update the DBPARM.ini file with the correct syslog server IP address.
D. Update the vault.ini file with the correct syslog server IP address.
E. Configure the Secure Tunnel for SIEM integration.
Answer: A,E (LEAVE A REPLY)
https://docs.cyberark.com/privilege-cloud-shared-services/Latest/en/Content/Privilege%20Cloud/privCloud- connect-siem.htm

NEW QUESTION: 10
What must be specified when authenticating to Privilege Cloud during the Secure Tunnel install?
A. Vault IP Address
B. Subdomain or Customer ID
C. Privilege Cloud URL
D. CaseID
Answer: B (LEAVE A REPLY)
During Secure Tunnel deployment, CyberArk's installation flow includes an "Authenticate to Privilege Cloud" step where you must enter Subdomain or Customer ID (plus the provided username/password). The documentation explicitly says to enter only the subdomain identifier (not the whole URL) or use the Customer ID provided by CyberArk.

NEW QUESTION: 11
Which authentication methods does PSM for SSH support? (Choose 2.)
A. OIDC
B. MFA Caching
C. SAML
D. RADIUS
E. Client Authentication Certificate
Answer: D,E (LEAVE A REPLY)
PSM for SSH supports various authentication methods, specifically focusing on secure and verified access mechanisms. The supported methods include:

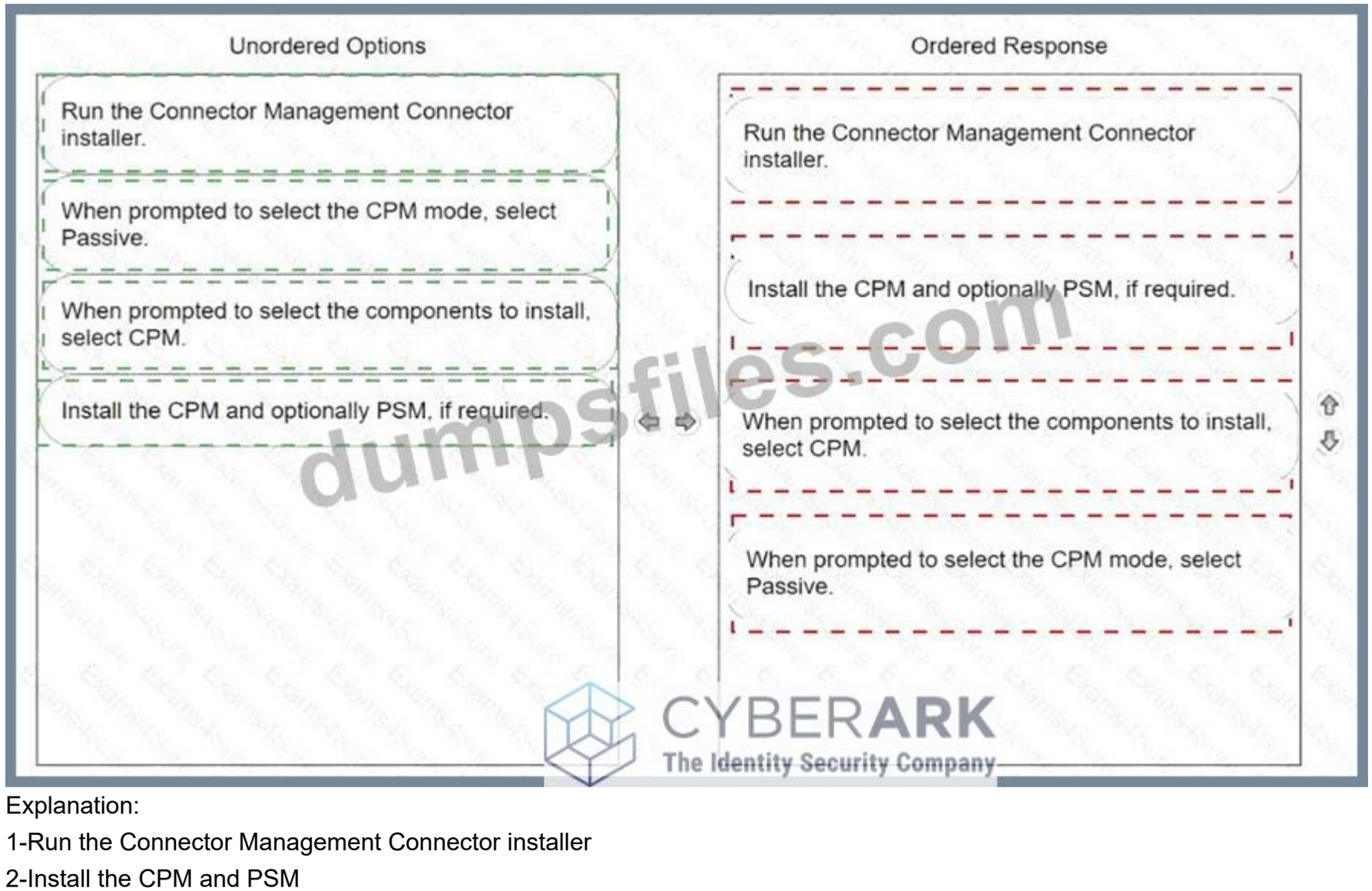
* RADIUS (D): Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service. PSM for SSH utilizes RADIUS to authenticate SSH sessions, which adds an additional layer of security by centralizing authentication requests to a RADIUS server.
* Client Authentication Certificate (E): This method uses certificates for authentication, where a client presents a certificate that the server verifies against known trusted certificates. This type of authentication is highly secure as it ensures that both parties involved in the communication are precisely who they claim to be, making it suitable for environments that require stringent security measures.
These methods provide robust security options for SSH sessions managed through CyberArk's PSM, ensuring that only authorized users can access critical systems.

NEW QUESTION: 12
In addition to CyberArk, which additional licensing implication does the PSM have?
A. RDS CALs
B. Microsoft Office
C. GCP
D. AWS
Answer: A (LEAVE A REPLY)
PSM relies on Microsoft Remote Desktop Services capabilities on Windows, and CyberArk documentation /knowledge articles call out RDS CAL considerations for PSM deployments (including guidance on CAL type implications, especially with Windows Server 2019 licensing enforcement behavior).

NEW QUESTION: 13
What is the navigation path to add account search properties?
A. Go to Administration > Configuration Options > Applications > Search Properties
B. Go to Administration > Configuration Options > Configurations > Search Properties
C. Go to Policies > Master Policy
D. Go to Administration > Configuration Options > Configurations > Accounts UI Preferences > Main > Toolbar actions
Answer: B (LEAVE A REPLY)
CyberArk's Privilege Cloud procedure for adding account search properties states:
* In the Privilege Cloud Portal, go to Administration > Configuration Options
* Under Configurations, right-click Search Properties # Add Property
That is option B.

NEW QUESTION: 14
Arrange the steps to install passive CPM using Connector Management in the correct sequence

Answer:



Explanation:

1-Run the Connector Management Connector installer

2-Install the CPM and PSM

3-When you are prompted to select the components to install, select CPM.

4-When you are prompted to select the CPM mode, select Passive.

https://docs.cyberark.com/ispss-deployment/latest/en/content/privilege%20cloud/privcloud-cpm-dr-install- config.htm

NEW QUESTION: 15

When using Connector Management, how do you configure a DR CPM in Privilege Cloud shared services?

(Choose two.)

A. Stop the CyberArk Password Manager service and set the startup type to Manual.

B. When prompted for the Vault IP address on the installation windows, leave it blank and proceed.

C. When prompted to select the CPM mode, select Passive.

D. When prompted for the Vault administrator credentials on the installation windows, leave it blank and proceed.

E. Stop the CyberArk Password Manager service and set the startup type to Automatic.

Answer: A,C (LEAVE A REPLY)

CyberArk's official DR CPM procedure for Privilege Cloud (shared services) describes two key actions in this flow:

* During installation (Connector Management): When prompted to select the CPM mode, choose Passive.

* After installation (configuration step): Stop the CyberArk Password Manager service and set its startup type to Manual.

These map directly to answers C and A.

NEW QUESTION: 16
What is a requirement for increasing the redundancy of PSMs?
A. Use a load balancer.
B. Set it by adding parameters to the basic_PSM.ini configuration file.
C. CPM must be in all data centers.
D. Install the Vault in an HA cluster.
Answer: A (LEAVE A REPLY)
CyberArk's Privilege Cloud guidance for PSM high availability explicitly ties multiple PSM instances to high availability and load balancing implementations, i.e., redundancy is achieved by deploying multiple PSMs and placing them behind a load balancer.

NEW QUESTION: 17
On the CPM, you want to verify if DEP is disabled for the required executables According to best practices, which executables should be listed? (Choose 2.)
A. Telnet.exe
B. Plink.exe
C. putty.exe
D. mstsc.exe
Answer: A,B (LEAVE A REPLY)
https://docs.cyberark.com/pam-self-hosted/11.4/en/content/pas%20inst/following-central-policy-manager- installation.htm

NEW QUESTION: 18
Which method can be used to directly authenticate users to PSM for SSH? (Choose three.)
A. CyberArk authentication
B. LDAP authentication
C. RADIUS authentication
D. Windows authentication
E. SAML authentication
F. OpenID Connect (OIDC) authentication
Answer: A,B,C (LEAVE A REPLY)
CyberArk states that users can authenticate to the Vault through PSM for SSH using:
* CyberArk password authentication (i.e., CyberArk authentication),
* LDAP, and
* RADIUS (including challenge-response).

Windows, SAML, and OIDC are not listed as direct PSM for SSH authentication methods in the PSM for SSH authentication configuration (Privilege Cloud / PSM for SSH uses the configured PSM for SSH authentication methods such as Password/LDAP/RADIUS)

NEW QUESTION: 19
What is the recommended method to enable load balancing and failover of the CyberArk Identity Connector?
A. Setup IIS based Application Request Routing on two or more CyberArk Identity Connector servers.
B. Set up a network load balancer between two or more CyberArk Identity Connector servers.
C. Set up two or more CyberArk Identity Connector servers only.
D. Set up a Microsoft Failover Cluster on two or more CyberArk Identity Connector servers.
Answer: (SHOW ANSWER)
https://docs.cyberark.com/identity/latest/en/content/coreservices/connector/connector-install.htm

NEW QUESTION: 20
Your customer recently merged with a smaller organization. The customer's connector has no network connectivity to the smaller organization's infrastructure. You need to map LDAP users from both your customer and the smaller organization. How is this achieved?
A. Create the required users in one directory and configure the Identity Connector to read that directory, as there can only be one Identity Connector.
B. Create mappings for both directories from the original Identity Connector.
C. Deploy Identity Connectors in the newly acquired infrastructure and create user mappings.
D. Switch all users to SAML authentication as there can only be one Identity Connector.
Answer: (SHOW ANSWER)
To map LDAP users from both your customer and the smaller organization they have merged with, especially when there is no network connectivity between the two infrastructures, the best approach is to:
* Deploy Identity Connectors in the newly acquired infrastructure and create user mappings (Option C). This involves setting up additional Identity Connectors within the smaller organization's network. These connectors will facilitate the integration of user directories from both organizations into the customer's Privilege Cloud environment.
Reference: CyberArk documentation on Identity Connectors often outlines the capability of deploying multiple connectors to manage different user directories, especially useful in scenarios involving mergers or acquisitions where separate infrastructures need integration.

NEW QUESTION: 21
Which statements are correct regarding enabling end users from multiple domains in the same forest to authenticate to CyberArk Privilege Cloud? (Choose two.)
A. CyberArk does not permit end users from multiple domains to authenticate to CyberArk Privilege Cloud; it only allows users from multiple directory services, such as AD, Azure AD, CyberArk Cloud Directory, etc.
B. This can be accomplished when the users' Active Directory accounts are in domains with domain controllers that have a two-way, transitive trust relationship with the domain controller to which the connector is connected.
C. Configuring authentication for users in multiple domains in the same forest is not recommended due to potential performance issues.
D. To enable authentication for users in multiple domains in the same forest, you should install separate CyberArk Identity Connectors for each independent domain.
E. CyberArk recommends consolidating users from multiple domains in the same forest into the CyberArk Cloud Directory for this specific use case.
Answer: (SHOW ANSWER)

CyberArk's official connector guidance (CyberArk Identity / Identity Administration-used with Privilege Cloud Shared Services for AD user authentication) says that for trusted domains in a single forest, you use this model when the domain controllers have a two-way, transitive trust relationship with the domain controller the connector is joined to.
It also clarifies that a single connector can be used for the entire domain tree or forest in that trusted- domain model, and authentication requests are handled according to AD trust relationships within the forest
/tree.
https://docs.cyberark.com/identity/latest/en/content/coreservices/connector/userauthmultdomain.htm

NEW QUESTION: 22
When installing the first CPM within Privilege Cloud using the Connector Management Agent, what should you set the Installation Mode to in the CPM section?
A. Active
B. Passive
C. Default
D. Primary
Answer: A (LEAVE A REPLY)
When installing the first CyberArk Privilege Management (CPM) instance in the Privilege Cloud using the Connector Management Agent, the installation mode should be set to "Active". This configuration sets the CPM to be actively involved in password management and task processing without being in a standby or passive mode. Here are the step-by-step details:
* Download the Connector Management Agent: Obtain the installer from the CyberArk Marketplace or your installation kit.
* Run the Installer: Start the setup and select the CPM component to install.
* Choose Installation Mode: When prompted, select "Active" as the installation mode. This sets up the CPM as the primary node responsible for handling password management operations.
This setup ensures that the CPM is immediately active and capable of handling requests without waiting for manual intervention or failover.
Reference: CyberArk's official documentation provides guidance on setting up the CPM, where it specifies the modes and their purposes.

NEW QUESTION: 23
When calling the PSM Health Check Webservice to assess the state of a PSM node, which response code does a healthy node return?
A. 200 (OK)
B. 404 (OK)
C. 500 (OK)
D. 503 (OK)
Answer: (SHOW ANSWER)
CyberArk documents that the health check service returns HTTP 200 (OK) when the PSM service is healthy, and returns 503 (Service unavailable) when it is not healthy (in code-based behavior).

NEW QUESTION: 24
You need to map an enterprise's Active Directory to Privilege Cloud Shared Services to enable users to log in to CyberArk through their LDAP credentials. What do you need to accomplish this? (Choose two.)
A. Read-only domain user to facilitate the LDAP mapping
B. Installation and configuration of the Identity Connector
C. Port 636 open to the Privilege Cloud back-end

D. Trusted certificate for LDAP server installed on Identity Connector
E. Configuration of a Federated Domain on the Identity Platform
Answer: B,D (LEAVE A REPLY)
CyberArk documents that to provision/authenticate users based on on-prem directory services using LDAP with Shared Services, you must first install the Identity Connector.
CyberArk also states LDAP communication to the Identity Connector is over TLS/SSL, and during the TLS handshake the LDAP server must present an X.509 certificate, meaning the connector must be able to trust the LDAP/LDAPS certificate chain (i.e., a trusted certificate on the connector side is required for LDAPS trust).
Therefore, the correct choices are B (Identity Connector) and D (trusted LDAP server certificate on the connector).
Why the other options are not correct as stated:
* C is wrong because LDAPS (636) is between the Identity Connector and the domain controllers
/LDAP server, not "opened to the Privilege Cloud back-end" directly.
* E is not required for LDAP credential login; federated domains are used for federation/SSO use cases, while LDAP mapping is handled via the connector + LDAPS trust.
* A (read-only domain user) is commonly used as the Bind DN/service account, but in the Shared Services LDAP requirement set here, the two must-have items that CyberArk calls out for enabling this path are the Identity Connector and the LDAPS certificate trust.

NEW QUESTION: 25
Which deployment criteria influences the CyberArk-provided hardening methods that need to be applied to CPM and PSM components?
A. "In Domain" and "Out of Domain"
B. "On Premises" and "On Cloud"
C. "Windows" and "Linux"
D. "Primary Privilege Cloud Connector" and "additional Privilege Cloud Connector"
Answer: A (LEAVE A REPLY)
CyberArk's hardening guidance is explicitly organized by whether the servers are In Domain or Out of Domain (for example, PSM hardening guidelines and tasks reference both deployment types, and CPM has separate "hardening in domain" guidance). Therefore, the deployment criterion that drives the hardening method/package is In Domain vs Out of Domain.

NEW QUESTION: 26
Refer to the exhibit.
You set up your LDAP Directory in CyberArk Identity, but encountered an error during the connection test.
Which scenarios could represent a valid misconfiguration? (Choose 2.)

A. TCP Port 636 could be blocked by a network firewall, preventing communication between the CyberArk Identity Connector and the LDAP Server.
B. All required CA Certificates have been installed on the CyberArk Identity Connector but the LDAP Bind credentials provided are incorrect.
C. Verify Server Certificate' is activated but the provided hostname is not listed as a Subject Alternative Name (SAN) in the LDAP server's certificate.
D. TCP Port 636 could be blocked by a network firewall, preventing communication between the Secure Tunnel and the LDAP Server.
Answer: A,C (LEAVE A REPLY)
From the error message provided, two likely scenarios could represent valid misconfigurations:
* TCP Port 636 could be blocked by a network firewall, preventing communication between the CyberArk Identity Connector and the LDAP Server (A). This is a common issue where firewall settings prevent the secure communication port (typically 636 for LDAPS) from transmitting data between the server and the connector, thus blocking the connection attempt.
* 'Verify Server Certificate' is activated but the provided hostname is not listed as a Subject Alternative Name (SAN) in the LDAP server's certificate (C). This scenario occurs when SSL/TLS security measures are stringent, requiring that the hostname used to connect to the LDAP server must match one listed in the server's SSL certificate. If the hostname does not match, the connection will fail due to SSL certificate validation errors.

NEW QUESTION: 27
Which option correctly describes the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted?
A. CyberArk Privilege Cloud only provides a username and password authentication without third-party IdP integration; CyberArk PAM Self-Hosted uses traditional on-premises methods such as Windows and LDAP. but lacks modern protocols such as SAML or OIDC.
B. CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for MFA. and supports SAML and OIDC; CyberArk PAM Self-Hosted depends on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups.
C. CyberArk Privilege Cloud requires on-premises components for all authentication and does not support other cloud-based authentication protocols; CyberArk PAM Self-Hosted offers a wide array of methods, including support for SAML. OIDC. and other modern protocols, without needing on- premises components.
D. Both use the same authentication methods.
Answer: B (LEAVE A REPLY)
The correct description of the authentication differences between CyberArk Privilege Cloud and CyberArk PAM Self-Hosted is that CyberArk Privilege Cloud uses cloud-based methods, integrating with CyberArk Identity for Multi-Factor Authentication (MFA), and supports SAML and OIDC, while CyberArk PAM Self- Hosted relies on on-premises methods such as RADIUS and LDAP, but can adopt SAML or OIDC with additional setups. CyberArk Privilege Cloud is designed to leverage modern cloud-based authentication protocols to enhance security and ease of use, particularly in distributed and diverse IT environments. In contrast, CyberArk PAM Self-Hosted offers flexibility to use traditional on-premises authentication methods but also supports modern protocols if configured to do so.

NEW QUESTION: 28
Which component supports the required communication to send audit logs from Privilege Cloud through the Syslog protocol to a SIEM application?
A. CyberArk Syslog Writer
B. Secure Tunnel
C. Privilege Cloud Connector
D. CyberArk Identity Connector
Answer: B (LEAVE A REPLY)
CyberArk's Privilege Cloud documentation for SIEM integration (Syslog) states that to connect to SIEM in Privilege Cloud, you must first deploy the Secure Tunnel.
That means the Secure Tunnel is the required component that enables the communication path for sending Privilege Cloud audit logs via Syslog (TCP/TLS) to your SIEM.
Why the other options are not correct for this Privilege Cloud Syslog requirement:
* A (CyberArk Syslog Writer) is typically referenced in CyberArk Identity / ISP logging contexts, not as the required Privilege Cloud SIEM transport component. (Privilege Cloud SIEM doc calls out Secure Tunnel explicitly.)
* C (Privilege Cloud Connector) is not what the SIEM/Syslog doc identifies as the required prerequisite; it specifically calls out Secure Tunnel.
* D (CyberArk Identity Connector) is used to integrate directory services (AD/LDAP) with CyberArk Identity/Identity Administration, not as the Privilege Cloud Syslog transport prerequisite.

NEW QUESTION: 29
You want to enforce Multi-Factor Authentication (MFA) for all Privilege Cloud Shared Services users and require them to set up an MFA factor. How should you accomplish this?
A. Only allow SAML as the authentication method, enforce MFA on the SAML Identity Provider (IdP), and ensure users set up MFA accordingly on the IdP.
B. Navigate to the Identity Administration Portal's Policies section and configure the required authentication policies for CyberArk Identity.
C. Navigate to the Identity Administration Portal's Policies section and set the user security policy for Privilege Cloud to an authentication profile that only allows Multiple Authentication Mechanisms.
D. Navigate to the Identity Administration Portal's Policies section and configure the authentication policies for CyberArk Identity, adding a new authentication rule that applies with an "identity cookie" as a filter.
Answer: B (LEAVE A REPLY)
In the Shared Services model, MFA enforcement is done in CyberArk Identity / Identity Administration using Core Services > Policies:
* To enforce MFA broadly, CyberArk documents configuring MFA for all users by enabling authentication policy controls and creating/assigning an authentication profile (the mechanisms
/challenges).
* To require users to set up MFA factors, CyberArk documents the setting under User Security Policies > User Account Settings where you specify the minimum number of authentication factors users must configure upon login.
Option B is the only choice that correctly points you to the right place and activity (Identity Administration Policies to configure authentication/MFA requirements and enrollment requirements).

NEW QUESTION: 30
You want to add an additional maintenance user on the PSM for SSH. How can you accomplish this if InstallCyberArkSSHD is set to Integrated?
A. Create a local user and add it to the PSMP_MaintenanceUsers group.

B. Create a local user called proxymaster and add it to /etc/pam.d/auth-password.
C. Create a local user and add it to the group configured for the parameter AllowGroups in the /etc/ssh /sshd_config file.
D. Create a local user called psmpmng and add it to the PSMMaintenance group in /etc/pam.d/auth- password.
Answer: C (LEAVE A REPLY)
CyberArk's PSM for SSH administration documentation explains how to create maintenance access by updating the SSH daemon configuration:
* In /etc/ssh/sshd_config, add an AllowGroups entry that includes the maintenance group(s):
AllowGroups PSMConnectUsers <MaintenanceGroupName1>..<MaintenanceGroupNameN> This matches option C exactly: you enable the additional maintenance user by placing them in the group(s) referenced by AllowGroups in sshd_config.

NEW QUESTION: 31
Which group has only View Audit and View Safe permissions?
A. Operators
B. Auditors
C. Privileged Cloud Admins
D. Backup Users
Answer: B (LEAVE A REPLY)
CyberArk's predefined groups documentation describes the Auditors group as having View audit plus Safe viewing-related authorization (documented as View Safe Members, enabling visibility into Safe contents
/activity/owners list). This matches the intent of "View Audit + View Safe" in the question better than the other options.

NEW QUESTION: 32
Which statement is correct about using the AllowedSafes platform parameter?
A. It allows users to access accounts in specific safes.
B. It prevents the CPM from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration.
C. It allows the CPM to access PSM safes to monitor platform configuration and connection component changes.
D. It prevents the CPM from processing pending items in the Discovery safes enforcing manual intervention to complete the onboarding process.
Answer: B (LEAVE A REPLY)
The correct statement about using the AllowedSafes platform parameter is that it prevents the Central Policy Manager (CPM) from scanning all safes, restricting it to scan only safes that match the AllowedSafes configuration. This parameter is crucial in large-scale deployments where efficiency and resource management are key. By specifying which safes the CPM should manage, unnecessary scanning of irrelevant safes is avoided, thus optimizing the CPM's performance and reducing the load on the CyberArk environment.
This configuration can be found in the platform management section of the CyberArk documentation.

NEW QUESTION: 33
Which Safe(s) does the AllowedSafes=Win platform parameter configuration match? (Choose two.)
A. WindowsPasswords
B. win-ssh-keys
C. CXD-WIN-ADMINS
D. SQL-Win-SA
E. WiNdOwS_Accts
Answer: A,D (LEAVE A REPLY)
AllowedSafes is a regular expression and is case sensitive.
The regex Win (with no anchors) will match any Safe name that contains the exact substring "Win" with the same case:
* WindowsPasswords # starts with Win #
* SQL-Win-SA # contains Win #
* win-ssh-keys # contains win (lowercase) # (case sensitive)
* CXD-WIN-ADMINS # contains WIN (all caps) #
* WiNdOwS_Accts # mixed case, does not contain the exact substring Win # Therefore the correct choices are A and D.

NEW QUESTION: 34
You are configuring an integration to provision users based on LDAP directory services for Privilege Cloud Shared Services. Which component must first be installed and configured in the environment to support this?
A. CyberArk Identity Connector
B. Secure Tunnel
C. Privilege Cloud Connector
D. Linux Connector Server
Answer: (SHOW ANSWER)
For Shared Services (ISPSS), CyberArk's Identity Administration documentation states: "To provision users based on on-prem directory services, you must first install the Identity Connector." This is because Privilege Cloud Shared Services leverages CyberArk Identity directory services integration (via the Identity Connector) for AD/LDAP provisioning and authentication.