CyberArk

Exam Questions CPC-SEN

CyberArk Sentry - Privilege Cloud

NEW QUESTION 1
CyberArk User Neil is trying to connect to the Target Linux server 192.168.1.164 using a domain user ACME\linuxuser01 on domain acme.corp using PSM for SSH server 192.168.65.145.
What is the correct syntax?

A. ssh neil@linuxuser01:acme.corp@192.168.1.164@192.168.65.145
B. ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145
C. sshneil@linuxuser01@192.168.1.164@192.168.65.145
D. ssh neil@linuxuser01@acme.corp@192.168.1.164@192.168.65.145

Answer: B

Explanation:
In CyberArk Privilege Cloud, when connecting to a target server using the Privileged Session Manager (PSM) for SSH, the correct syntax for the SSH command includes the following format: ssh neil@linuxuser01#acme.corp@192.168.1.164@192.168.65.145. This syntax breaks down as follows:
? neil: The CyberArk username.
? linuxuser01#acme.corp: The domain user on the target Linux server, formatted as username#domain.
? 192.168.1.164: The IP address of the target Linux server.
? 192.168.65.145: The IP address of the PSM for SSH server.
This specific format ensures that the CyberArk Privileged Access Manager correctly interprets and routes the connection through the PSM for SSH to the intended target server.
References:
? CyberArk Privilege Cloud Introduction
? CyberArk Privileged Access Manager
? CyberArk Privilege Cloud - Manage Safe Members
? CyberArk Security Fundamentals

NEW QUESTION 2
How should you configure PSM for SSH to support load balancing?

A. by using a network load balancer
B. in PVWA > Options > PSM for SSH Proxy > Servers
C. in PVWA > Options > PSM for SSH Proxy > Servers > VIP
D. by editing sshd.config on the all the PSM for SSH servers

Answer: A

Explanation:
To support load balancing for PSM for SSH, the configuration should be done by using a network load balancer. This method involves placing a network load balancer in front of multiple PSM for SSH servers to distribute incoming SSH traffic evenly among them. This setup enhances the availability and scalability of PSM for SSH by ensuring that no single server becomes a bottleneck, thereby improving performance and reliability during high usage scenarios.

NEW QUESTION 3
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: B

Explanation:
The recommended method to enable load balancing and failover of the CyberArk Identity Connector is to set up a network load balancer between two or more CyberArk Identity Connector servers. This setup allows for the distribution of requests across multiple servers, enhancing the availability and reliability of the service. Network load balancers efficiently manage traffic to ensure that no single connector server becomes a bottleneck, thereby improving overall performance and fault tolerance.

NEW QUESTION 4
How can a platform be configured to work with load-balanced PSMs?

A. Remove all entries from configured PSM Servers except for the ID of the PSMs with load balancing.
B. Create a new PSM definition that targets the load balancer IP address and assign to the platform.
C. Include details of the PSMs with load balancing in the Basic_psm.ini file on each PSM server.
D. Use the Privilege Cloud Portal to update the Session Management settings for the platform in the Master Policy.

Answer: B

Explanation:
To configure a platform to work with load-balanced Privileged Session Managers (PSMs), you should:
? Create a new PSM definition that targets the load balancer IP address and assign
it to the platform (Option B). This approach involves configuring the platform settings to direct session traffic through a load balancer that distributes the load across multiple PSM servers. This is effective in environments where high availability and fault tolerance are priorities.
Reference: CyberArk??s setup guidelines for high-availability environments typically recommend configuring platforms to utilize load balancers to ensure continuous availability and optimal distribution of session management tasks.

NEW QUESTION 5

In the directory lookup order, which directory service is always looked up first for the CyberArk Privilege Cloud solution?

A. Active Directory
B. LDAP
C. Federated Directory
D. CyberArk Cloud Directory

Answer: D

Explanation:
In the directory lookup order for the CyberArk Privilege Cloud solution, the "CyberArk Cloud
Directory" is always looked up first. This directory service is a part of the CyberArk Privilege Cloud infrastructure and is specifically designed to handle identity and access management within the cloud environment efficiently. It prioritizes the CyberArk Cloud Directory for authentication and identity resolution before consulting any external directory services.
Reference: CyberArk's architectural documentation usually emphasizes the role of the CyberArk Cloud Directory in managing and authenticating user access in cloud-based deployments, highlighting its precedence in the directory lookup process.

NEW QUESTION 6
Which tool configures the user object that will be used during the installation of the PSM for SSH component?

A. CreateUserPass
B. CreateCredFile
C. ConfigureCredFile
D. ConfigureUserPass

Answer: B

Explanation:
The tool used to configure the user object for the installation of the PSM for SSH component is CreateCredFile. This tool is responsible for creating a credentials file that stores the necessary user details required during the installation process, ensuring secure and correct authentication.
References:
? CyberArk Privilege Cloud Introduction

NEW QUESTION 7
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: AC

Explanation:
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 8
Following the installation of the PSM for SSH server, which additional tasks should be performed? (Choose 2.)

A. Delete the user.cred file used during installation.
B. Delete the vault.ini you used during installation.
C. Delete the psmpparms file you used during installation.
D. Package all installation log files for upload to CyberArk.

Answer: AC

Explanation:
Following the installation of the PSM for SSH server, certain security and cleanup tasks are crucial to secure the environment and eliminate potential vulnerabilities:
? Delete the user.cred file used during installation (A): The user.cred file contains sensitive credential information used during the installation process. Deleting this file post-installation ensures that this sensitive data is not left accessible on the system, mitigating the risk of unauthorized access.
? Delete the psmpparms file you used during installation (C): Similar to the user.cred file, the psmpparms file often contains parameters that might include sensitive configuration details. Removing this file after the installation process is completed helps in securing the server by removing potential leakage points of sensitive information.
These actions are part of best practices to secure the installation environment and reduce the risk of sensitive information exposure.

NEW QUESTION 9
'What is a default authentication profile to access CyberArk Identity?

A. Default New User Login Profile
B. Default New Device Login Profile
C. Default New Authenticator Profile
D. Default New Password Profile

Answer: B

Explanation:
The default authentication profile to access CyberArk Identity is typically the Default New Device Login Profile. This profile is used to manage the authentication settings and security measures for devices accessing CyberArk services for the first time. It includes configurations such as authentication methods, security checks, and compliance requirements, ensuring that new devices meet the organization??s security standards before gaining access.

NEW QUESTION 10
To disable the PSM default Support for Browser Sessions, which option should be set to 'No* before running Hardening?

A. SupportWebApplications
B. SupportBrowsers
C. SupportWebBrowsers
D. SupportHTML5Content

Answer: B

Explanation:
To disable the PSM default support for browser sessions, the option SupportBrowsers should be set to 'No' before running the hardening process. This configuration change is made within the PSM??s configuration files, typically found in the PSM's administrative interface or directly within specific XML configuration files like PSMHardening.xml. Setting this option to 'No' prevents the PSM from processing session requests that involve web browsers, thereby enhancing security by limiting the session types the PSM will support. This setting is particularly important in environments where web browsing sessions are deemed unnecessary or too risky.

NEW QUESTION 10
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: BC

Explanation:
On the Central Policy Manager (CPM), it is crucial to verify that Data Execution Prevention (DEP) is disabled for specific executables required for proper operation according to best practices. The relevant executables include:
? Plink.exe (Option B): This executable is commonly used for SSH communications and may require DEP to be disabled to function correctly under certain configurations.
? putty.exe (Option C): Similar to Plink.exe, Putty is another essential tool for SSH communications and might also require DEP to be disabled to prevent any execution issues.
Reference: CyberArk??s best practices for system configuration often highlight the need to adjust DEP settings for certain executables to ensure they run without interruption, particularly when these tools are crucial for secure communications and operations management.

NEW QUESTION 14
......