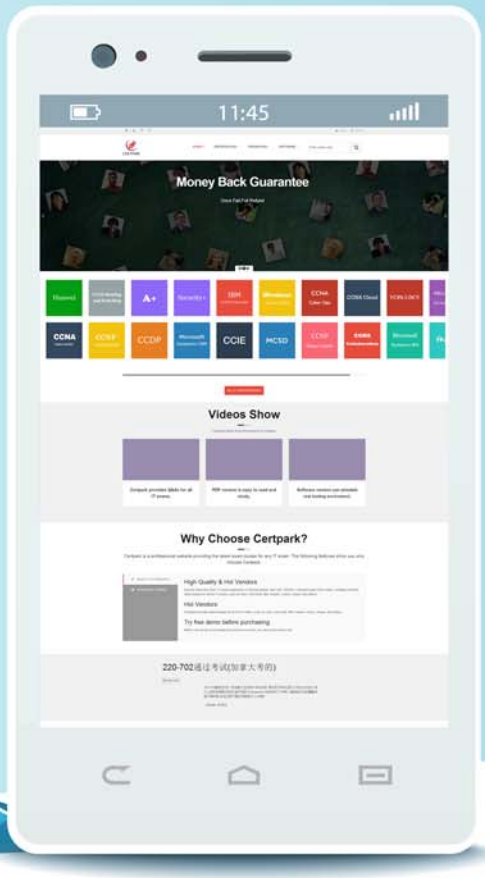
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **CPC-SEN**

Title : CyberArk Sentry - Privilege Cloud

Version : DEMO

1.You are planning to configure Multi-Factor Authentication (MFA) for your CyberArk Privilege Cloud Shared Service.
What are the available authentication methods?
A. LDAR RADIUS. SAML OpenID Connect (OIDC)
B. Windows. PKI. RADIUS. CyberArk, LDAP. SAML. OpenID Connect (OIDC)
C. Privilege Cloud Shared Services fully utilize CyberArk Identity and its MFA options.
D. Only RADIUS can be used to achieve MFA across all components, such as PSM for RDP and PSM for SSH.
Answer: B
Explanation:
In CyberArk Privilege Cloud, Multi-Factor Authentication (MFA) can be configured to enhance security by requiring multiple methods of authentication from independent categories of credentials to verify the user's identity. The available authentication methods include:
Windows Authentication: Leverages the user's Windows credentials.
PKI (Public Key Infrastructure): Utilizes certificates to authenticate.
RADIUS (Remote Authentication Dial-In User Service): A networking protocol that provides centralized Authentication, Authorization, and Accounting management.
CyberArk: Uses CyberArk's own authentication methods.
LDAP (Lightweight Directory Access Protocol): Protocol for accessing and maintaining distributed directory information services.
SAML (Security Assertion Markup Language): An open standard that allows identity providers to pass authorization credentials to service providers.
OpenID Connect (OIDC): An authentication layer on top of OAuth 2.0, an authorization framework.
Reference for this can be found in the CyberArk Privilege Cloud documentation, which details the integration and setup of MFA using these methods.

2.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
Explanation:
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.

3.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.
Reference:
CyberArk Privilege Cloud Introduction
CyberArk Privileged Access Manager
CyberArk Privilege Cloud - Manage Safe Members
CyberArk Security Fundamentals

4.After a scripted installation has successfully installed the PSM, which post-installation task is performed?
A. The screen saver for the PSM local users is disabled.
B. A new group called PSMShadowUsers is created.
C. The PSMAdminConnect user password is reset.
D. Remote desktop services are installed.
Answer: A
Explanation:
After the successful scripted installation of the Privileged Session Manager (PSM), one of the post-installation tasks is to disable the screen saver for the PSM local users. This is done to ensure that the PSMConnect and PSMAdminConnect users, which are created during the installation process, do not have a screen saver activated that could interfere with the operation of the PSM.
Reference: CyberArk documentation on PSM post-installation tasks1.
CyberArk documentation on disabling the screen saver for PSM local users

5.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.

Reference: CyberArk Privilege Cloud Introduction