CyberArk Sentry Certification

Study Guide

How to use this study guide

We recommend that you thoroughly review each topic listed within the Exam Topics section of this study guide. Make sure you understand each topic using the suggested resources or by searching the CyberArk online documentation and the Technical Community. Hands-on experience with the CyberArk solution will be very helpful.

Exam Objectives

The CyberArk Sentry-PAM Certification tests for the necessary expertise and technical skills to deploy, install, and configure the CyberArk Privileged Access Management solution. It is intended to certify an candidate's competence to fill one of the following roles within a Privileged Access Managment Program.

CyberArk Subject Matter Expert

The CyberArk SME designs controls which will be implemented with CyberArk and acts as a liaison to user groups.

CyberArk Engineer

The CyberArk Engineer installs and manages CyberArk PAM environments, tests new features and creates internal documentation.

Exam Format

Number questions: 60 Multiple-Choice items

Time allotted: 90 minutes

Exam Fee: 200 USD

Preparing for the Exam

We recommend a combination training, self-study, and on-the-job experience to get yourself ready to take this exam.

Training

The CyberArk Privileged Access Management (PAM) Install & Configure Course can help you learn for this certification exam. While taking the training can be an important part of your preparation, it does not guarantee success on the exam. Self-study and on-the-job experience are also important determinants of success.

Study Resources

Sample Question – Sentry – PAM Sample Items

Free eLearning

HTML5 Based Remote Access

External Storage of PSM Recordings

Documentation

CyberArk Privileged Access Security Online Documentation

Exam Topics

The CyberArk Sentry Certification tests examanees ability to form the following tasks in eight knowledge domains. Only functions of the Core PAM solution are included.

Deploy the Vault

Identify and describe the steps to migrate the server key to an HSM Identify and describe the steps to complete a post-install hardening Identify and describe the components and steps to complete a Vault installation Describe how to prepare a Windows server for Vault installation Describe how to register a primary vault in AWS using AMIs Describe how to register a primary vault in Azure using the CyberArk image	Preparation resources: PAM – System Requirements PAM – Before You Install PAM – CyberArk Digital Vault Installation PAM – Install PAS in a Cloud Environment Privileged Access Management (PAM) Install & Configure

Deploy the Password Vault Web Access (PVWA)

Identify and describe the steps to install the first and additional PVWAs Evaluate and scope a customer environment todetermine the appropriate number of PVWAs and their placement within the network Describe the process to correctly harden a PVWA server Describe various PVWA load balancing options	Preparation resources: PAM – System Requirements PAM – Before You Install PAM – Install PVWA Privileged Access Management (PAM) Install & Configure

Prepare a Windows server for PVWA installation	

Deploy the Central Policy Manager (CPM)

Identify and describe the steps to correctly harden a CPM server Identify and describe the steps required to prepare a Windows server for CPM installation Identify and describe the steps to install the first and additional CPMs Identify and describe the steps to rename a CPM Evaluate and scope a customer environment to determine the number of CPMs required and their placement within the network Identify and describe Fault Tolerant Architecture components Determine the quantities and locations of components needed to provide a fault tolerant architecture to meet customer needs Identify and describe distributed architecture components Determine the quantities and locations of components needed to provide a distributed architecture to meet customer needs	Preparation resources: PAM – System Requirements PAM – Before You Install PAM – Install CPM Privileged Access Management (PAM) Install & Configure

Deploy the Privileged Session Manager (PSM)

Identify and describe the steps to install the first and additional PSMs Identify and describe preparation considerations for PSM deployment Evaluate and scope a customer environment to calculate the amount of	Preparation resources: PAM – System Requirements PAM – Before You Install PAM – Install PSM

storage that should be available to the PSMs for PSM recordings Evaluate and scope a customer environment to calculate the amount of storage that should be available to the Vault and PAReplicate for PSM recordings Evaluate and scope a customer environment to determine the appropriate number of PSMs and their placement withi the network Identify and describe the steps to prepare a Windows server for PSM installation Describe post-installation processes Identify and describe the steps to complete an HTML5 Gateway installation Identify and describe the steps to prepare a UNIX server for HTML5 Gateway installation Describe various PSM load-balancing options Describe how to correctly harden a PSM server	Privileged Access Management (PAM) Install & Configure

Deploy the PSM For SSH

Identify and describe the steps to install the first and additional PSMs for SSH Describe how to configure usrmng accounts Describe the process to correctly harden a PSM for SSH server Describe how to prepare a UNIX server for PSM for SSH installation	Preparation resources: PAM – System Requirements PAM – Before You Install PAM – Install PSM for SSH Privileged Access Management (PAM) Install & Configure

Configure Integrations

Configure authentication methods Describe the steps required to combine a Vault and a PVWA authentication method to create two-factor authentication Describe how to configure PKI authentication Describe how to configure RADIUS authentication Describe how to configure SAML authentication Identify and describe the components that work with each authentication method Describe how to generate a custom connection component using the PGU Perform integration tasks, including integrating with NTP, SMTP, SNMP, LDAP, and Syslog/SIEM	Preparation resources: PAM – Configure Authentication Methods PAM – Plugin Generator Utility PAM – Email Notifications PAM – SIEM Applications PAM – Monitor the Vault Privileged Access Management (PAM) Install & Configure

Performance tune the solution

Identify and describe the steps to convert a platform from PMTerminal to TPC Identify and describe how to correctly configure Interval and concurrent settings Identify and describe how to correctly configure the Allowed Safes parameter Evaluate and scope a customer environment to correctly size the servers to meet customer needs	Preparation resources: PAM – Create Extensions Privileged Access Management (PAM) Install & Configure CPM Plugin & PSM Connector Development

Install and deploy on a public cloud

Identify best practices agnostic to public cloud deployments Identify and describe different cloud architectures	Preparation resources: PAM – Install PAS in a Cloud Environment

Describe key management considerations in a public cloud Identify and describe various cost reduction strategies when deploying into a public cloud	