EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

A Helpdesk technician needs to provide remote assistance to a user whose laptop cannot connect to the Internet to pull EPM policies. What CyberArk EPM feature should the Helpdesk technician use to allow the user elevation capabilities?

A. Offline Policy Authorization Generator

B. Elevate Trusted Application If Necessary

C. Just In Time Access and Elevation

D. Loosely Connected Devices Credential Management

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

A (100%)

**Shizukya** Highly Voted 2 years, 10 months ago

It's A obviously, offline generator

upvoted 7 times

**Eeeek** Most Recent 1 year, 2 months ago

Whole EPM exam has changed since beginning of 2025, need to update all with the new questions

upvoted 2 times

**JuCyberArk** 1 year, 7 months ago

I agree totally dvikas´comments

upvoted 2 times

**Takumi** 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/One-time%20Run%20Authorization%20Tool.htm

upvoted 1 times

**dvikas** 2 years, 2 months ago

If the machine is not connected to internet then how the JIT policies will work on the machine. OPAG is the feature used in this type of scenarios.

upvoted 2 times

**TonyC73** 2 years, 4 months ago

According to a similar question from the actual CyberArk practice exam the correct answer should be "A".

upvoted 2 times

**Porongos** 2 years, 5 months ago

It's A

upvoted 3 times

Question #2 *Topic 1*

Which user or group will not be removed as part of CyberArk EPM's Remove Local Administrators feature?

A. Built-in Local Administrator

B. Domain Users

C. Admin Users

D. Power Users

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/epm/24.2.1/en/Content/EPM/Server%20User%20Guide/ManageLocalAdministrators.htm

upvoted 3 times

**gatoblack** 2 years, 3 months ago

A it´s correct

upvoted 2 times

**Porongos** 2 years, 5 months ago

https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/ManageLocalAdministrators.htm

upvoted 2 times

Question #3 *Topic 1*

An end user is reporting that an application that needs administrative rights is crashing when selecting a certain option menu item. The Application is part of an advanced elevate policy and is working correctly except when using that menu item.
What could be the EPM cause of the error?

A. The Users defined in the advanced policy do not include the end user running the application.

B. The Advanced: Time options are not set correctly to include the time that the user is running the application at.

C. The Elevate Child Processes option is not enabled.

D. The Specify permissions to be set for selected Services on End-user Computers is set to Allow Start/Stop

**Suggested Answer:** *C*
Official Answer: C

*Community vote distribution*
C (100%)

**Takumi** Most Recent 1 year, 11 months ago
The answer is C. https://docs.cyberark.com/epm/24.2.1/en/Content/Policies/PoliciesIntro-NewUI.htm#Childprocesses
upvoted 3 times

**omardw** 2 years, 2 months ago
correct C
upvoted 2 times

**pathomas1971** 2 years, 5 months ago
A. The Users defined in the advanced policy do not include the end user running the application. The error could be caused by the fact that the end user's account is not included in the list of users defined within the advanced elevate policy. This means that the application is elevated for the specified users in the policy, but not for the specific end user who is experiencing the issue. As a result, when the end user tries to access the certain menu item that requires administrative rights, the application crashes since the necessary elevation is not being applied to their account. To resolve this issue, the end user's account should be added to the list of users defined in the advanced elevate policy to ensure that the application functions properly when that user interacts with the menu item.
upvoted 1 times

Question #4 *Topic 1*

Which setting in the agent configuration controls how often the agent sends events to the EPM Server?

A. Event Queue Flush Period

B. Heartbeat Timeout

C. Condition Timeout

D. Policy Update Rate

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/AgentConfiguration.htm

upvoted 2 times

**omardw** 2 years, 2 months ago

A is correct

upvoted 2 times

Question #5 *Topic 1*

Which of the following application options can be used when defining trusted sources?

A. Publisher, Product, Size, URL

B. Publisher, Name, Size, URI

C. Product, URL, Machine, Package

D. Product, Publisher, User/Group, Installation Package

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

D (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is D. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/TrustPolicies-NewUI.htm#Createapolicy

upvoted 2 times

**omardw** 2 years, 2 months ago

D is correct https://docs.cyberark.com/EPM/22.8.0/en/Content/EPM/Server%20User%20Guide/TrustedSources-Windows.htm

upvoted 2 times

Question #6 *Topic 1*

What EPM component is responsible for communicating password changes in credential rotation?

A. EPM Agent

B. EPM Server

C. EPM API

D. EPM Discovery

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**ihristov99** Highly Voted 2 years, 8 months ago

its A for sure

upvoted 7 times

**nadeeeemm** Highly Voted 2 years, 10 months ago

probably A EPM Agent

upvoted 6 times

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/Installation/Windows-InstallAgents.htm

upvoted 2 times

**pathomas1971** 2 years, 5 months ago

A. EPM Agent In CyberArk's Endpoint Privilege Manager (EPM) solution, the component responsible for communicating password changes in credential rotation is typically the EPM Agent.

upvoted 3 times

**Shizukya** 2 years, 10 months ago

EPM agent manage the credential rotations

upvoted 4 times

Question #7 *Topic 1*

An EPM Administrator would like to notify end users whenever the Elevate policy is granting users elevation for their applications. Where should the EPM Administrator go to enable the end-user dialog?

A. End-user UI in the left panel of the console

B. Advanced, Agent Configurations

C. Default Policies

D. End-User UI within the policy

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*




**Takumi** Most Recent 1 year, 11 months ago

The answer is D. https://docs.cyberark.com/epm/24.3.0/en/Content/Policies/PoliciesIntro-NewUI.htm

upvoted 3 times

**Souvik0730** 2 years, 2 months ago

D is Correct.

upvoted 2 times

**Phenomx64L** 2 years, 5 months ago

D https://docs.cyberark.com/EPM-onprem/10.10/en/Content/EPM/Server%20User%20Guide/End-User%20UI.htm

upvoted 3 times

**CurryMuncher** 2 years, 10 months ago

I am pretty sure the answer is C https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/23.3.1/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-ElevateUnhandledApps-NewUI.htm#Activatethedefaultpolicy

upvoted 2 times

Question #8 *Topic 1*

Which of the following is CyberArk's Recommended FIRST roll out strategy?

A. Implement Application Control

B. Implement Privilege Management

C. Implement Threat Detection

D. Implement Ransomware Protection

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is B. https://docs.cyberark.com/EPM/Latest/en/Content/Intro/Implement%20Privilege%20Management.htm

upvoted 3 times

**Souvik0730** 2 years, 2 months ago

B is the correct answer according to CyberArk's recommendation.

upvoted 4 times

**dvikas** 2 years, 2 months ago

The Answer should be A, because if we don't have the data of application which requires the elevation rights, and we remove the privileges from the users then it will create a chaos in the organization.

upvoted 2 times

Question #9 *Topic 1*

An EPM Administrator would like to include a particular file extension to be monitored and protected under Ransomware Protection. What setting should the EPM Administrator configure to add the extension?

A. Authorized Applications (Ransomware Protection)

B. Files to be Ignored Always

C. Anti-tampering Protection

D. Default Policies

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

D (100%)

**rayjohn28** Highly Voted 2 years, 2 months ago

D is correct. File extensions to be protected can only be added on default policies>ransomware.

upvoted 6 times

**Takumi** Most Recent 1 year, 11 months ago

The answer is D. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/DefaultPolicies-NewUI.htm

upvoted 2 times

**DaBulls** 2 years, 1 month ago

It is more as tricky questions as we have the following guidance: https://cyberark.my.site.com/s/article/EPM-Protect-against-ransomware
https://docs.cyberark.com/EPM/23.11.0/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm

upvoted 1 times

**Souvik0730** 2 years, 2 months ago

D is correct

upvoted 3 times

**Hyper** 2 years, 5 months ago

D is correct

upvoted 4 times

Question #10 *Topic 1*

When deploying EPM and in the Privilege Management phase what is the purpose of Discovery?

A. To identify all non-administrative events B. To identify all administrative level events

B. To identify both administrative and non-administrative level events

C. To identify non-administrative threats

**Suggested Answer:** *B*

Official Answer: C

*Community vote distribution*

C (100%)

**Sathesh** Most Recent 1 year, 10 months ago

Answer is B

upvoted 2 times

**dru0pa** 2 years, 3 months ago

It needs to know if non-admin or admin task

upvoted 1 times

**Takumi** 2 years, 5 months ago

The answer is B. https://docs.cyberark.com/EPM/Latest/en/Content/Intro/Implement%20Privilege%20Management.htm

upvoted 2 times

**Hyper** 2 years, 11 months ago

B is correct https://docs.cyberark.com/EPM/23.9.0/en/Content/Intro/Implement%20Privilege%20Management.htm A list of applications discovered by EPM which require administrative rights.

upvoted 4 times

Question #11 *Topic 1*

What are Trusted sources for Windows endpoints used for?

A. Creating policies that contain trusted sources of applications.

B. Defining applications that can be used by the developers.

C. Listing all the approved application to the end users.

D. Managing groups added by recommendation.

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

A (100%)

**Phenomx64L** Highly Voted 2 years, 5 months ago

A: https://docs.cyberark.com/EPM/Latest/en/Content/Intro/Implementing%20Application%20Control.htm

upvoted 6 times

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/TrustPolicies-NewUI.htm

upvoted 2 times

**Souvik0730** 2 years, 2 months ago

A is the correct Answer.

upvoted 3 times

Question #12 *Topic 1*

CyberArk's Privilege Threat Protection policies are available for which Operating Systems? (Choose two.)

A. Windows Workstations

B. Windows Servers

C. MacOS

D. Linux

**Suggested Answer:** *A, B*

Official Answer: AB

*Community vote distribution*

AB (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer are A and B. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/DefaultPolicies-NewUI.htm

upvoted 3 times

**omardw** 2 years, 2 months ago

A & B is correct

upvoted 2 times

Question #13 *Topic 1*

Which threat intelligence source requires the suspect file to be sent externally?

A. NSRL

B. Palo Alto Wildfire

C. VirusTotal

D. CyberArk Application Risk Analysis Service (ARA)

**Suggested Answer:** *B*
Official Answer: B

*Community vote distribution*
B (100%)

**9cf186a** Most Recent 1 year, 10 months ago
not sure but I'll say D: According to documenntation, wildfire needs the file to execute and analyze it. plus is the only integration with an "upload timeout value" https://docs.cyberark.com/EPM-onprem/10.10/en/Content/EPM/Server%20User%20Guide/FireEye%20AX%20Series.htm
upvoted 1 times

**Takumi** 2 years, 4 months ago
The answer must be B or D. On other hand VirusTotal and NSRL only analyze the checksum so they don't send files externally. Probably Palo Alto is the best answer.
upvoted 1 times

**Hyper** 2 years, 11 months ago
The correct answer is Virus total, because epm sents files to virus total to be analyzed. You must have internet access to enable automatic upload to VirusTotal. https://docs.cyberark.com/EPM-onprem/11.5.1/en/Content/EPM/Server%20User%20Guide/Virus%20Total.htm
upvoted 2 times

**Hyper** 2 years, 11 months ago
Is B. Palo alto, fireeyes & check point needs interchange a file. https://docs.cyberark.com/EPM-onprem/11.5.1/en/Content/EPM/Server%20User%20Guide/Configuring%20Integration%20Settings.htm
upvoted 2 times

**pathomas1971** 2 years, 11 months ago
B. Palo Alto Wildfire Palo Alto Wildfire is a threat intelligence source that requires the suspect file to be sent externally for analysis. Wildfire is a cloud-based service provided by Palo Alto Networks that analyzes unknown files to determine if they are malicious. When a file is suspected of being malicious, it can be sent to the Wildfire service for evaluation. The service examines the file in a controlled environment to determine its behavior and potential threat level. The other options mentioned, such as NSRL (National Software Reference Library), VirusTotal, and CyberArk Application Risk Analysis Service (ARA), do not necessarily require the suspect file to be sent externally for analysis in the same way as Palo Alto Wildfire.
upvoted 2 times

**CurryMuncher** 3 years, 3 months ago
Not convinced D is the answer. I think its C https://docs.cyberark.com/Product-Doc/OnlineHelp/EPM/21.9/en/Content/EPM/Server%20User%20Guide/Virus%20Total.htm Says "You must have internet access to enable automatic upload to VirusTotal" I would go for C,
upvoted 3 times

**buczy** 3 years, 4 months ago
D is correct
upvoted 3 times

Question #14 *Topic 1*

What feature is designed to exclude applications from CyberArk EPM's Ransomware Protection, without whitelisting the application launch?

A. Trusted Sources

B. Authorized Applications (Ransomware Protection)

C. Threat Intelligence

D. Policy Recommendations

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**Hyper** Highly Voted 2 years, 5 months ago

is the option B. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm Authorized Applications (Ransomware protection) A group of applications that is automatically excluded from the Protect against Ransomware policy.

upvoted 5 times

**Takumi** Most Recent 1 year, 11 months ago

The answer is B. https://docs.cyberark.com/epm/24.3.0/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm

upvoted 3 times

**CurryMuncher** 2 years, 9 months ago

The correct answer is A. Trusted Sources. The Trusted Sources feature in CyberArk EPM (Endpoint Privilege Manager) is designed to exclude applications from the ransomware protection feature without requiring the application to be whitelisted for launch. This feature enables organizations to define trusted sources of software and exclude applications from the ransomware protection policy if they originate from those trusted sources. Authorized Applications is a feature in CyberArk EPM that allows organizations to create policies for specific applications and grant privileges to those applications based on the policies. Threat Intelligence is a feature in CyberArk EPM that provides real-time threat intelligence feeds to help organizations detect and respond to cyber threats. Policy Recommendations is a feature in CyberArk EPM that suggests policies based on best practices and industry standards to help organizations improve their security posture.

upvoted 3 times

Question #15 *Topic 1*

An EPM Administrator would like to exclude an application from all Threat Protection modules. Where should the EPM Administrator make this change?

A. Privilege Threat Protection under Policies.

B. Authorized Applications under Application Groups.

C. Protect Against Ransomware under Default Policies.

D. Threat Protection under Agent Configurations.

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

D (100%)

**Shizukya** Highly Voted 2 years, 10 months ago

I would say "D" for global excluded applications, go to Agent Configuration > Threat Protection > Excluded Applications

upvoted 7 times

**rayjohn28** Highly Voted 2 years, 2 months ago

D is correct for global configuration. You can also exempt via A answer however, the questions require ALL protection modules. It will be tedious if you do it one by one.

upvoted 5 times

**Takumi** Most Recent 1 year, 11 months ago

The asnwer is D. https://docs.cyberark.com/epm/24.3.0/en/Content/Policies/DefaultPolicies-NewUI.htm

upvoted 1 times

**Souvik0730** 2 years, 2 months ago

D is the correct answer

upvoted 3 times

**Hyper** 2 years, 5 months ago

A. https://docs.cyberark.com/EPM-onprem/Latest/en/Content/EPM/Server%20User%20Guide/Threat%20Detection%20Events.htm

upvoted 2 times

**CurryMuncher** 2 years, 9 months ago

Correct answer is A

upvoted 1 times

**buczy** 2 years, 10 months ago

A is correct

upvoted 1 times

Question #16 *Topic 1*

Which EPM reporting tool provides a comprehensive view of threat detection activity?

A. Threat Detection Dashboard

B. Detected Threats

C. Threat Detection Events

D. McAfee ePO Reports

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/EPM-onprem/Latest/en/Content/EPM/Server%20User%20Guide/Reporting%20Capabilities.htm

upvoted 2 times

Question #17 *Topic 1*

What type of user can be created from the Threat Deception LSASS Credential Lures feature?

A. It does not create any users

B. A standard user

C. A local administrator user

D. A domain admin user

**Suggested Answer:** *C*
Official Answer: C

*Community vote distribution*
C (100%)

**buczy** Highly Voted 2 years, 10 months ago
probably C is correct
upvoted 6 times

**Shizukya** Highly Voted 2 years, 10 months ago
C confirmed (LSASS lures > Policy options > create LSAAS deception lures > create fake Local Admin accounts for LSAAS to store on your organization's computers as deception lures.)
upvoted 6 times

**Takumi** Most Recent 1 year, 11 months ago
The answer is C. https://docs.cyberark.com/epm/24.3.1/en/Content/EPM/Server%20User%20Guide/PrivilegeDeception.htm
upvoted 2 times

**cokowix230** 2 years, 1 month ago
C is the correct answer.
upvoted 3 times

**Souvik0730** 2 years, 2 months ago
C is the correct answer. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivilegeDeception.htm#Overview
upvoted 3 times

**rayjohn28** 2 years, 2 months ago
C is the correct answer. https://docs.cyberark.com/EPM/23.4.2/en/Content/EPM/Server%20User%20Guide/PrivilegeDeception.htm
upvoted 4 times

**CurryMuncher** 2 years, 9 months ago
The EPM creates policies that place user credentials in popular places and then monitor attempts to use these credentials. When the EPM agent receives that policy from the EPM server, it creates a Local Admin user to use as a credentials lure. The agent then generates a unique password for this account that cannot be used on any other endpoint.
upvoted 3 times

Question #18 *Topic 1*

What is a valid step to investigate an EPM agent that is unable to connect to the EPM server?

A. On the end point, open a browser session to the URL of the EPM server.

B. Ping the endpoint from the EPM server.

C. Ping the server from the endpoint.

D. Restart the end point

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

C (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is C.

upvoted 1 times

Question #19 *Topic 1*

Which programming interface enables you to perform activities on EPM objects via a REST Web Service?

A. EPM Web Services SDK

B. Application Password SDK

C. Mac Credential Provider SDK

D. Java password SDK

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/WebServices/WebServicesIntro.htm

upvoted 2 times

Question #20 *Topic 1*

What are the policy targeting options available for a policy upon creation?

A. AD Users and Groups, Computers in AD Security Groups, Servers

B. Computers in this set, Computers in AD Security Groups, Users and Groups

C. OS Computers, EPM Sets, AD Users

D. EPM Sets, Computers in AD Security Groups, AD Users and AD Security Groups

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

B (100%)

**buczy** Highly Voted 2 years, 10 months ago

B is correct

upvoted 7 times

**Shizukya** Highly Voted 2 years, 10 months ago

B right

upvoted 6 times

**ffb136c** Most Recent 8 months, 3 weeks ago

https://docs.cyberark.com/epm/latest/en/content/policies/windowspolicies-newui.htm#Createapolicy

upvoted 1 times

**Takumi** 1 year, 11 months ago

The answer is B

upvoted 2 times

**rayjohn28** 2 years, 2 months ago

correct answer is B https://docs.cyberark.com/EPM/23.4.2/en/Content/Policies/WindowsPolicies-NewUI.htm

upvoted 4 times

**rasputin712** 2 years, 7 months ago

B is correct

upvoted 5 times

Question #21 *Topic 1*

When enabling Threat Protection policies, what should an EPM Administrator consider? (Choose two.)

A. Some Threat Protection policies are applicable only for Windows Servers as opposed to Workstations.

B. Certain Threat Protection policies apply for specific applications not found on all machines.

C. Threat Protection policies requires an additional agent to be installed.

D. Threat Protection features are not available in all regions.

**Suggested Answer:** *A, B*

Official Answer: AB

*Community vote distribution*

AB (100%)

**0a0e828** Most Recent 1 year, 3 months ago

Correct answer

upvoted 1 times

**Takumi** 1 year, 11 months ago

The answers are A and B.

upvoted 1 times

Question #22 *Topic 1*

When working with credential rotation/loosely connected devices, what additional CyberArk components are required?

A. PTA

B. OPM

C. PVWA

D. DAP

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

C (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is C. https://cyberark.my.site.com/s/article/Better-Together-Configuring-LCD-with-CyberArk-PAM-and-CyberArk-EPM

upvoted 1 times

Question #23 *Topic 1*

What can you manage by using User Policies?

A. Just-In-Time endpoint access and elevation, access to removable drives, and Services access.

B. Access to Windows Services only.

C. Filesystem and registry access, access to removable drives, and Services access.

D. Just-In-Time endpoint access and elevation, access to removable drives, filesystem and registry access, Services access, and User account control monitoring.

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

D (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is D. https://docs.cyberark.com/epm/24.3.0/en/Content/Policies/UserPolicies-NewUI.htm

upvoted 1 times

**Pio99** 1 year, 12 months ago

Its "D" https://docs.cyberark.com/EPM/Latest/en/Content/Policies/UserPolicies-NewUI.htm

upvoted 1 times

Question #24 *Topic 1*

An end user is experiencing performance issues on their device after the EPM Agent had been installed on their machine. What should the EPM Administrator do first to help resolve the issue?

A. Verify any 3rd party security solutions have been added to EPM's Files To Be Ignored Always configuration and CyberArk EPM has also been excluded from the 3rd party security solutions.

B. Enable the Default Policy's Privilege Management Control, Unhandled Privileged Applications in Elevate mode.

C. Rerun the agent installation on the user's machine to repair the installation.

D. Uninstall or disable any anti-virus software prohibiting the EPM Agent functionalities.

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*




**Shizukya** Highly Voted 2 years, 10 months ago

A confirmed : https://cyberark-customers.force.com/s/article/EPM-User-is-experiencing-slowness-while-the-EPM-Agent-is-installed-on-the-endpoint

upvoted 5 times

**Takumi** Most Recent 1 year, 11 months ago

The answer is A.

upvoted 1 times

**cokowix230** 2 years, 1 month ago

A is correct

upvoted 3 times

**rayjohn28** 2 years, 2 months ago

D is correct. The question is what should the admin do FIRST. If you can uninstall or disable the AV, yes.. if NOT.. then proceed to A answer

upvoted 1 times

**buczy** 2 years, 10 months ago

probably A is correct

upvoted 4 times

Question #26 *Topic 1*

Before enabling Ransomware Protection, what should the EPM Administrator do first?

A. Enable the Privilege Management Inbox in Elevate mode.

B. Enable the Control Applications Downloaded From The Internet feature in Restrict mode.

C. Review the Authorized Applications (Ransomware Protection) group and update if necessary.

D. Enable Threat Protection and Threat Intelligence modules.

**Suggested Answer:** *C*
Official Answer: C

**e2a882d** Most Recent 1 year, 10 months ago
C is the correct answer
upvoted 1 times

**Takumi** 2 years, 5 months ago
The answer is C.
upvoted 1 times

Question #27 *Topic 1*

How does EPM help streamline security compliance and reporting?

A. Use of automated distribution of reports to the security team

B. Provides reports in standard formats such as PDF, Word and Excel

C. Print reports

D. Create custom reports

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

A (100%)

**e2a882d** Most Recent 1 year, 10 months ago

Correct answer is A, as we can automate distribution of reports.

upvoted 1 times

**Takumi** 2 years, 5 months ago

When you check the console, the reports section doesn't have any options for word or pdf and I don't think the answer would be C or D, so the answer must be A.

upvoted 1 times

Question #28 *Topic 1*

Select the default threat intelligence source that requires additional licensing.

A. VirusTotal

B. Palo Alto WildFire

C. CyberArk Application Risk Analysis Service

D. NSRL

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**e2a882d** Most Recent 1 year, 10 months ago

Correct answer is B.

upvoted 1 times

**Takumi** 2 years, 5 months ago

The answer is B. https://docs.cyberark.com/epm/24.3.0/en/Content/EPM/Server%20User%20Guide/Configuring%20Integration%20Settings.htm

upvoted 1 times

**ZippyZulu** 2 years, 5 months ago

Answer: B See "Note:" in CyberArk Documentation https://docs.cyberark.com/EPM-onprem/10.10/en/Content/EPM/Server%20User%20Guide/Palo%20Alto%20Wild%20Fire.htm

upvoted 1 times

Question #29 *Topic 1*

When deploying Ransomware Protection, what tasks should be considered before enabling this functionality? (Choose two.)

A. Add trusted software to the Authorized Applications (Ransomware protection) Application Group

B. Add trusted software to the Allow Application Group

C. Add additional files, folders, and/or file extensions to be included to Ransomware Protection

D. Enable Detect privileged unhandled applications under Default Policies

**Suggested Answer:** *A, C*

Official Answer: AC

*Community vote distribution*

AC (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answers are A and C. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm

upvoted 1 times

Question #30 *Topic 1*

When working with credential rotation at the EPM level, what is the minimum time period that can be set between connections?

A. 1 hour

B. 5 hours

C. 24 hours

D. 72 hours

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is B. https://docs.cyberark.com/EPM/Latest/en/Content/WebServices/LCDPolicyDefinition.htm

upvoted 2 times

**Souvik0730** 2 years, 2 months ago

B is correct.

upvoted 2 times

**rayjohn28** 2 years, 2 months ago

correct answer is 5 hrs

upvoted 3 times

**pathomas1971** 2 years, 5 months ago

The minimum interval is 5 hours

upvoted 2 times

Question #31 *Topic 1*

What unauthorized change can CyberArk EPM Ransomware Protection prevent?

A. Windows Registry Keys

B. Website Data

C. Local Administrator Passwords

D. Certificates in the Certificate Store

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/epm/24.3.0/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm

upvoted 1 times

**DaBulls** 2 years, 1 month ago

Logic here should be that Ransomware protection is available for Windows Workstations only which can be mapped to Windows registry Keys in the answer.

upvoted 2 times

**pathomas1971** 2 years, 5 months ago

A. Windows Registry Keys CyberArk EPM Ransomware Protection can prevent unauthorized changes to Windows Registry Keys. Ransomware Protection helps defend against ransomware attacks by monitoring and preventing unauthorized modifications to critical system areas, including registry keys that are often targeted by ransomware to manipulate system settings and encryption. The other options mentioned (Website Data, Local Administrator Passwords, Certificates in the Certificate Store) might be relevant to different security aspects, but they are not typically associated with unauthorized changes that CyberArk EPM Ransomware Protection directly addresses.

upvoted 1 times

Question #32 *Topic 1*

An EPM Administrator would like to enable CyberArk EPM's Ransomware Protection in Restrict mode. What should the EPM Administrator do?

A. Set Block unhandled applications to On.

B. Set Protect Against Ransomware to Restrict.

C. Set Protect Against Ransomware to Restrict and Set Block unhandled applications to On.

D. Set Control unhandled applications to Detect.

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

B (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is B. https://docs.cyberark.com/epm/24.3.0/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm

upvoted 1 times

**Souvik0730** 2 years, 2 months ago

B is the correct answer. There is no dependency on the Contro Unhandled application. We can set it to Restrict not Block. The option itself is not accurate.

upvoted 3 times

Question #33 *Topic 1*

Where would an EPM admin configure an application policy that depends on a script returning true for an end user's machine being connected to an open (no password protection) Wi-Fi?

A. Advanced Policy - Application Control - Check Wi-Fi security

B. Advanced Policy - Options: Conditional enforcement - Apply Policy according to Script execution result

C. Default policies - Check if network access is secure

D. Advanced Policy - Access - Specify permissions to be set for Wi-Fi network security

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**JM_Olympus** Most Recent 2 years, 1 month ago

B: This is the only possible answer that has anything to do with script execution result.

upvoted 1 times

**Takumi** 2 years, 5 months ago

The answer is B. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/ScriptDistributionPolicies-NewUI.htm#Script

upvoted 1 times

Question #34 *Topic 1*

An EPM Administrator would like to enable a Threat Protection policy, however, the policy protects an application that is not installed on all endpoints.
What should the EPM Administrator do?

A. Enable the Threat Protection policy and configure the Policy Targets.

B. Do not enable the Threat Protection policy.

C. Enable the Threat Protection policy only in Detect mode.

D. Split up the endpoints in to separate Sets and enable Threat Protection for only one of the Sets.

**Suggested Answer:** *D*
Official Answer: D

*Community vote distribution*
A (100%)

**Takumi** Most Recent 1 year, 11 months ago
The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/ConfigureThreatProtection-NewUI.htm
upvoted 1 times

**Souvik0730** 2 years, 2 months ago
A will be the correct answer as we can define target endpoints.
upvoted 3 times

Question #35 *Topic 1*

Which policy can be used to improve endpoint performance for applications commonly used for software development?

A. Developer Applications

B. Trusted Application

C. Trusted Source

D. Software Updater

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

A (100%)

**e2a882d** Most Recent 1 year, 10 months ago

On a new EPM deployment the only predefined policies are Developer Applications, Block, Elevate, Allow. So correct answer is A.

upvoted 1 times

**3c7ee8f** 2 years, 3 months ago

In the type of predefined policy on EPM SaaS, I can not see 'Trusted Applications' policy. I can see 'Developer Applications' policy in it. So A is correct.

upvoted 2 times

**Takumi** 2 years, 5 months ago

This is a tricky questions. If the product would be EPM On-Prem, the answer would be A, reference: https://docs.cyberark.com/EPM-onprem/10.10/en/Content/EPM/Server%20User%20Guide/Developer%20Applications.htm But if the version is EPM "SaaS", the answer would be B, reference: https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/TrustPolicies-NewUI.htm

upvoted 1 times

Question #36 *Topic 1*

What are the predefined application groups?

A. Developer group, Administrator group

B. Run as Administrator, Run as Developer, Block

C. Elevate, Allow, Block, Developer Applications

D. Block Only

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

C (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is C. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/ApplicationGroups-NewUI.htm

upvoted 1 times

Question #37 *Topic 1*

In EPM, creation of which user type is required to use SAML?

A. Local CyberArk EPM User

B. AD User

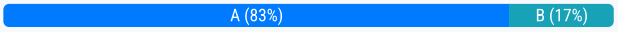
C. SQL User

D. Azure AD User

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*




**ffb136c** Most Recent 8 months, 2 weeks ago

In the article, Step 2 involves creating EPM users who will log in using SAML. This requires configuring the customer's SAML facilities to map AD users to EPM users. https://docs.cyberark.com/epm/latest/en/content/admin/samlintegration.htm#EnableSPinitiatedlogin

upvoted 1 times

**e2a882d** 1 year, 10 months ago

Question is user required to use SAML. correct answer will be D. local user for local auth AD user cant be SAML SQL user is same as above the only viable option is D: Azure AD User.

upvoted 2 times

**JM_Olympus** 2 years, 1 month ago

A: Key part of the question - created in EPM

upvoted 2 times

**Takumi** 2 years, 4 months ago

The answer is A, It needs to be create it before the SAML configuration.

upvoted 2 times

**Takumi** 2 years, 5 months ago

The answer is B. https://docs.cyberark.com/EPM/Latest/en/Content/Admin/SAMLIntegration.htm

upvoted 1 times

Question #38 *Topic 1*

For Advanced Policies, what can the target operating system users be set to?

A. Local or AD users and groups, Azure AD User, Azure AD Group

B. AD Groups, Azure AD Groups

C. Local or AD users and groups

D. Local or AD users, Azure AD Users

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*




**Takumi** Most Recent 1 year, 11 months ago

The answer is C. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/PoliciesIntro-NewUI.htm

upvoted 1 times

Question #39 *Topic 1*

A particular user in company ABC requires the ability to run any application with administrative privileges every day that they log in to their systems for a total duration of 5 working days.
What is the correct solution that an EPM admin can implement?

A. An EPM admin can generate a JIT access and elevation policy with temporary access timeframe set to 120 hours

B. An EPM admin can generate a JIT access and elevation policy with temporary access timeframe set to 120 hours and Terminate administrative processes when the policy expires option unchecked

C. An EPM admin can create an authorization token for each application needed by running: EPMOPAGtool.exe -command gentoken -targetUser -filehash -timeLimit 120 -action run

D. An EPM admin can create a secure token for the end user's computer and instruct the end user to open an administrative command prompt and run the command vfagent.exe -UseToken

**Suggested Answer:** *B*
Official Answer: B

*Community vote distribution*
A (100%)

**Rubik_07** Most Recent 7 months, 3 weeks ago
In response to the comments here, I am not sure if there is a correct answer since you can interpret the answer according to two scenarios: The first one you can only grant temporary access up to 72 hours in a JIT user policy but the timeframe of the question exceed that maximum. The second scenario is to create an Application policy and enforce it to a user/computer and enable the scheduled enforcement module in the policy options, which can allow you to exceed the timeframe that the JIT policy offers.
upvoted 1 times

**Takumi** 1 year, 11 months ago
The answer could be A because in B is mentioned: Terminate administrative processes when the policy expires option unchecked. If you want to terminate administrative processes the option has to be checked.
upvoted 2 times

**ZippyZulu** 1 year, 11 months ago
Looks like the maximum temporary access length according to the CA docs is between 1h and 72hrs.
https://docs.cyberark.com/epm/latest/en/Content/Policies/JITElevationAdmin-NewUI.htm#CreateaJITpolicy
upvoted 3 times

**Souvik0730** 2 years, 2 months ago
A is correct because as JIT we can create in Application advance policy, not user JIT policy with a time frame of 120 HRS
upvoted 3 times

Question #40 *Topic 1*

After a clean installation of the EPM agent, the local administrator password is not being changed on macOS and the old password can still be used to log in.
What is a possible cause?

A. Secure Token on macOS endpoint is not enabled.

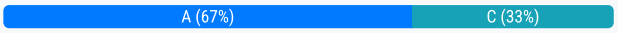
B. EPM agent is not able to connect to the EPM server.

C. After installation, Full Disk Access for the macOS agent to support EPM policies was not approved.

D. Endpoint password policy is too restrictive.

**Suggested Answer:** *A*
Official Answer: A

*Community vote distribution*




**ffb136c** Most Recent 8 months, 2 weeks ago
To activate password rotation on accounts where a secure token is enabled, the EPM user must also have a secure token. For accounts where a secure token is not enabled, the EPM user does not require a secure token to rotate password credentials. After installation, you can enable the secure token for the _cyberarkepm internal user at any time in the View the EPM agent menu or by using the following command line option: sudo CyberArkEPM --enableEPMUserSecureToken -adminUser -adminPassword
upvoted 1 times

**dru0pa** 1 year, 9 months ago
If Full Disk Access wasn't granted, the agent wouldn't be able to complete the password change, and the old password would remain usable
upvoted 1 times

**Takumi** 1 year, 11 months ago
The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/Installation/macOS-PostInstall.htm
upvoted 1 times

Question #41 *Topic 1*

If you want to diagnose agent EPM agent connectivity issues, what is the agent executable that can be used from the command line?

A. vf_agent.exe

B. epm_agent.exe

C. vault_agent.exe

D. db_agent.exe

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. https://docs.cyberark.com/EPM/Latest/en/Content/Installation/Windows-AgentCommands.htm

upvoted 2 times

**TonyC73** 2 years, 5 months ago

I also scoured the entire folder structure and did not find a single epm_agent.exe file. Only the vf_agent.exe....The answer is A.

upvoted 4 times

**pathomas1971** 2 years, 5 months ago

A. vf_agent.exe If you want to diagnose EPM (Endpoint Privilege Manager) agent connectivity issues from the command line, you would typically use the "vf_agent.exe" executable. This executable allows you to perform various tasks related to the EPM agent, including checking connectivity, troubleshooting, and gathering diagnostic information. The other options mentioned (epm_agent.exe, vault_agent.exe, db_agent.exe) are not standard executable names associated with EPM agent connectivity troubleshooting.

upvoted 3 times

Question #42 *Topic 1*

A policy needs to be created to block particular applications for a specific user group. Based on CyberArk's policy naming best practices, what should be included in the policy's name?

A. Policy creation date

B. Target use group

C. Creator of the policy

D. The policy's Set name

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is B. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PolicyGuidelines.htm

upvoted 3 times

Question #43 *Topic 1*

An application has been identified by the LSASS Credentials Harvesting Module.
What is the recommended approach to excluding the application?

A. In Agent Configurations, add the application to the Threat Protection Exclusions.

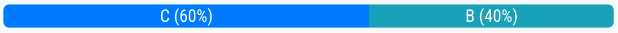
B. Add the application to the Files to be Ignored Always in Agent Configurations.

C. Exclude the application within the LSASS Credentials Harvesting module.

D. Add the application to an Advanced Policy or Application Group with an Elevate policy action.

**Suggested Answer:** *A*
Official Answer: A

*Community vote distribution*




**denianbqe** Highly Voted 2 years, 2 months ago
The correct answer is C: Exclude the application within the LSASS Credentials Harvesting module. In v23.11.1 is possible to configure the application exceptions from LSASS validation directly on LSASS CH module screen when enabled. The A and B options exclude the application from ALL EPM VALIDATIONS. This is not asked for in the question.
upvoted 7 times

**Takumi** Most Recent 1 year, 11 months ago
The answer is C. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/ConfigureThreatProtection-NewUI.htm
upvoted 3 times

**Hyper** 2 years, 5 months ago
correct answer is a To view global excluded applications, go to Agent Configuration > Threat Protection > Excluded Applications.
https://docs.cyberark.com/EPM/22.12.0/en/Content/EPM/Server%20User%20Guide/ConfigureThreatProtection.htm
upvoted 1 times

**pathomas1971** 2 years, 5 months ago
B. Add the application to the Files to be Ignored Always in Agent Configurations. The recommended approach to excluding an application that has been identified by the LSASS Credentials Harvesting Module in CyberArk EPM (Endpoint Privilege Manager) is to add the application to the "Files to be Ignored Always" list in Agent Configurations. By adding the application to this list, you are instructing EPM to ignore this application's behavior, even if it is flagged by certain modules like the LSASS Credentials Harvesting Module. This helps prevent false positives and ensures that legitimate applications are not unnecessarily blocked or restricted.
upvoted 1 times

**Hyper** 2 years, 5 months ago
correct
upvoted 1 times

Question #44 *Topic 1*

What are valid policy options for JIT and elevation policies?

A. Grant temporary access for all users, Policy name, Restart administrative processes in admin approval mode, Collect audit information

B. Grant temporary access for, Policy name, Terminate administrative processes when the policy expires, Collect audit information

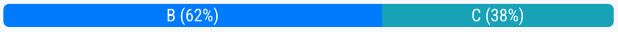
C. Grant administrative access, Policy name, Log off to apply policy, Collect policy violation information

D. Terminate administrative services, Grant policy access for, Policy name, Collect audit reports

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*




**Hyper** Highly Voted 2 years, 11 months ago

B is correct https://docs.cyberark.com/EPM/Latest/en/Content/Policies/JITElevationAdmin-NewUI.htm

upvoted 9 times

**JM_Olympus** Most Recent 2 years, 1 month ago

B: https://docs.cyberark.com/epm/24.3.0/en/Content/Policies/JITElevationAdmin-NewUI.htm#CreateaJITpolicy

upvoted 2 times

**Takumi** 2 years, 5 months ago

The answer is B. https://docs.cyberark.com/epm/24.3.0/en/Content/Policies/JITElevationAdmin-NewUI.htm

upvoted 3 times

**Souvik0730** 2 years, 8 months ago

B is the correct option.

upvoted 4 times

**pathomas1971** 2 years, 11 months ago

B. Grant temporary access for, Policy name, Terminate administrative processes when the policy expires, Collect audit information For Just-In-Time (JIT) and elevation policies in CyberArk Endpoint Privilege Manager (EPM), the valid policy options typically include: Grant temporary access for: Specifies the duration for which the elevated privileges will be granted. Policy name: Provides a name for the policy to help identify its purpose. Terminate administrative processes when the policy expires: Ensures that any processes running with elevated privileges are terminated when the policy's temporary access period expires. Collect audit information: Enables the collection of audit data and logs related to the execution of the policy for security and compliance purposes. The other options mentioned (A, C, D) do not accurately reflect the typical policy options associated with JIT and elevation policies in EPM.

upvoted 3 times

Question #45 *Topic 1*

How does a Trusted Source policy affect an application?

A. Applications will be allowed to run and will only elevate if required.

B. Applications will be allowed to run and will inherit the process token from the EPM agent.

C. Applications will be allowed to run always in elevated mode.

D. Application from the defined trusted sources must be configured on a per applicationbasis, in order to define run and elevation parameters.

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**JM_Olympus** Most Recent 2 years, 1 month ago

A: https://docs.cyberark.com/EPM/Latest/en/Content/Intro/Key%20Concepts.htm#Trustedsources

upvoted 2 times

**dru0pa** 2 years, 3 months ago

Applications on endpoint computers matching particular criteria will run with elevated privileges, if administrative privileges are required.

upvoted 2 times

**Takumi** 2 years, 5 months ago

The anwser is A. https://docs.cyberark.com/EPM/Latest/en/Content/Intro/Key%20Concepts.htm

upvoted 2 times

**Souvik0730** 2 years, 8 months ago

A is the correct answer.

upvoted 3 times

**Hyper** 2 years, 11 months ago

A is correct

upvoted 4 times

Question #46 *Topic 1*

On the Default Policies page, what are the names of policies that can be set as soon as EPM is deployed?

A. Privilege Escalation, Privilege Management, Application Management

B. Privilege Management, Application Control, Threat analysis

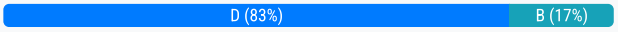
C. Privilege Management, Threat Protection, Application Escalation Control

D. Privilege Management, Privilege Threat Protection, Local Privileged Accounts Management

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*




**Hyper** Highly Voted 2 years, 5 months ago

D is correct https://docs.cyberark.com/EPM/Latest/en/Content/Policies/DefaultPolicies-NewUI.htm#:~:text=Set%20default%20policies,the%20default%20policies%20to%20apply.

upvoted 7 times

**Takumi** Highly Voted 1 year, 11 months ago

The answer is D. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/DefaultPolicies-NewUI.htm

upvoted 5 times

**Souvik0730** 2 years, 2 months ago

D is correct. For the new version of EPM, there is nothing to set up for Threat Analysis.

upvoted 4 times

**pathomas1971** 2 years, 5 months ago

B. Privilege Management, Application Control, Threat analysis On the Default Policies page in CyberArk Endpoint Privilege Manager (EPM), the names of policies that can be set as soon as EPM is deployed include: Privilege Management: This policy involves managing and controlling privileges on endpoints to ensure that users have appropriate access levels and permissions. Application Control: This policy involves controlling which applications can be executed on endpoints to prevent the execution of unauthorized or malicious applications. Threat analysis: This policy is aimed at analyzing and mitigating potential threats by monitoring and responding to suspicious or malicious activities on endpoints. These default policies provide foundational security and management capabilities for endpoints as soon as EPM is deployed.

upvoted 1 times

Question #47 *Topic 1*

An EPM Administrator is looking to enable the Threat Deception feature, under what section should the EPM Administrator go to enable this feature?

A. Threat Protection Inbox

B. Policies

C. Threat Intelligence

D. Policy Audit

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is B. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivilegeDeception.htm

upvoted 2 times

Question #48 *Topic 1*

What is required to configure SAML authentication on EPM?

A. OAuth token

B. Signed Authentication Request

C. Encrypted Assertion

D. Signed SAML Response

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

B (100%)

**Takumi** Most Recent 1 year, 10 months ago

The answer could be B.

https://docs.cyberark.com/EPM/Latest/en/Content/Admin/SAMLIntegration.htm#:~:text=In%20EPM%2C%20generate%20a%20SAML,click%20Create%20SAML%20attribute%20value.

upvoted 3 times

Question #49 *Topic 1*

Can the EPM Set Administrator configure Audit Dialog Pop-ups for the Record Audit Video option?

A. Yes, when Audit Video recording started, when Audit Video recording stopped, and when Audit Recording video reached size limit.

B. Yes, when Audit Video recording started, when not enough disk space to start the video recording, and when video recording is initializing.

C. Yes, when Audit Video recording started, when Audit Video recording is uploaded to the EPM server, and when audit recording cannot be initialized.

D. No, Audit Video is only available without the possibility of having End-User dialog pop-ups.

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

B (100%)

**pathomas1971** Highly Voted 2 years, 5 months ago

B. Yes, when Audit Video recording started, when not enough disk space to start the video recording, and when video recording is initializing. The correct answer is B. EPM administrators can configure Audit Dialog Pop-ups for the Record Audit Video option to include events such as when the Audit Video recording starts, when there's not enough disk space to start the video recording, and when the video recording is initializing. This provides transparency and alerts to end-users when audit video recording actions are taking place or facing issues.

upvoted 7 times

**Takumi** Most Recent 1 year, 11 months ago

The answer B. https://docs.cyberark.com/EPM/Latest/en/Content/EndUser/EndUserDialogs.htm

upvoted 2 times

**Souvik0730** 2 years, 2 months ago

B is the correct Answer as per the new EPM SAAS Version 23.12.

upvoted 2 times

**denianbqe** 2 years, 2 months ago

Correct answer: B - Yes, when Audit Video recording started, when not enough disk space to start the video recording, and when video recording is initializing.

upvoted 4 times

Question #50 *Topic 1*

A company is looking to manage their Windows Servers and Desktops with CyberArk EPM. Management would like to define different default policies between the Windows Servers and Windows Desktops.
What should the EPM Administrator do?

A. In the Default Policies, exclude either the Windows Servers or the Windows Desktops.

B. Create Advanced Policies to apply different policies between Windows Servers and Windows Desktops.

C. CyberArk does not recommend installing EPM Agents on Windows Servers.

D. Create a separate Set for Windows Servers and Windows Desktops.

**Suggested Answer:** *B*
Official Answer: B

*Community vote distribution*
D (100%)

**Takumi** Most Recent 1 year, 11 months ago
The answer es D.
upvoted 1 times

**Souvik0730** 2 years, 2 months ago
D is correct Default Policy can be applied over the Set only. We can add Excluded devices but we can't define the default policy for 2 different types of devices at once.
upvoted 4 times

Question #51 *Topic 1*

When blocking applications, what is the recommended practice regarding the end-user UI?

A. Show a block prompt for blocked applications.

B. Show no prompts for blocked applications.

C. Hide the CyberArk EPM Agent icon in the system tray.

D. Enable the Default Deny policy.

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is A. This is because showing a block prompt provides immediate feedback to the end-user when an application is blocked. It helps the user understand why the application isn't running and can reduce confusion and support calls. It also provides an opportunity to educate the user about the security policies and why certain applications are being blocked.

upvoted 3 times

Question #52 *Topic 1*

Where can you view CyberArk EPM Credential Lures events?

A. Application Catalog

B. Threat Protection Inbox

C. Events Management

D. Policy Audit

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

C (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is C. https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/EventsManagement.htm

upvoted 2 times

**Souvik0730** 2 years, 2 months ago

C is the correct answer for the EPM SAAS version 23.12.

upvoted 3 times

**rayjohn28** 2 years, 2 months ago

B or C.. if based on latest version, there's no more Threat Protection inbox. On later versions its Event Management

upvoted 3 times

Question #54 *Topic 1*

CyberArk EPM's Ransomware Protection comes with file types to be protected out of the box. If an EPM Administrator would like to remove a file type from Ransomware Protection, where can this be done?

A. Policy Scope within Protect Against Ransomware

B. Authorized Applications (Ransomware Protection) within Application Groups

C. Set Security Permissions within Advanced Policies

D. Protected Files within Agent Configurations

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

A (100%)

**JM_Olympus** Most Recent 2 years, 1 month ago

A: https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm?Highlight=Protect%20Against%20Ransomware

upvoted 1 times

**Takumi** 2 years, 5 months ago

The answer is A. The answer is A. Within the "Protect Against Ransomware" policy settings, the administrator can adjust the scope of file types to be protected. This includes removing specific file types from the list of protected files.

https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivMgmnt-Ransomware-NewUI.htm

upvoted 2 times

Question #55 *Topic 1*

An EPM Administrator needs to create a policy to allow the MacOS developers elevation to an application. What type of policy should be used?

A. Elevate Application Group

B. Developer Applications Application Group

C. Elevate Trusted Applications If Necessary Advanced Policy

D. Elevate MacOS Policy

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

D (100%)

**rayjohn28** Highly Voted 2 years, 8 months ago

Correct is D. There's no elevate if necessary in macOS https://docs.cyberark.com/EPM/Latest/en/Content/Policies/macOSpolicies-NewUI.htm

upvoted 5 times

**denianbqe** Highly Voted 2 years, 8 months ago

The correct is D. There is no "elevate if necessary" in macOS.

upvoted 5 times

**JM_Olympus** Most Recent 2 years, 1 month ago

D: https://docs.cyberark.com/EPM/Latest/en/Content/Policies/macOSpolicies-NewUI.htm

upvoted 2 times

**Takumi** 2 years, 5 months ago

The answer is D. https://docs.cyberark.com/EPM/Latest/en/Content/Policies/macOSpolicies-NewUI.htm

upvoted 3 times

**Souvik0730** 2 years, 8 months ago

D is the correct answer because other other options are not relevant.

upvoted 4 times

Question #56 *Topic 1*

For the CyberArk EPM Threat Deception Credential Lure feature, what is the recommendation regarding the username creation?

A. The username should match to an existing account.

B. The username should have a strong password associated.

C. The username should not match to an existing account.

D. The username should match the built-in local Administrator.

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

C (100%)

**Takumi** Most Recent 1 year, 11 months ago

The answer is C. Creating a username that does not match an existing account is recommended for the Threat Deception Credential Lure feature to avoid confusion and potential false alerts. This deception account should resemble typical organization credentials but should not correspond to an actual active account to prevent unintended access or usage.

https://docs.cyberark.com/EPM/Latest/en/Content/EPM/Server%20User%20Guide/PrivilegeDeception.htm

upvoted 2 times

Question #57 *Topic 1*

When adding the EPM agent to a pre-existing security stack on workstation, what two steps are CyberArk recommendations. (Choose two.)

A. Add any pre-existing security application to the Files to Be Ignored Always.

B. Add EPM agent to the other security tools exclusions.

C. EPM agent should never be run with any other security tools.

D. Create new advanced policies for each security tool.

**Suggested Answer:** *A, B*

Official Answer: AB

*Community vote distribution*

AB (100%)

**Takumi** Most Recent 1 year, 10 months ago

The answers are A and B

upvoted 3 times

Question #58 *Topic 1*

If Privilege Management is not working on an endpoint, what is the most likely cause that can be verified in the EPM Agent Log Files?

A. Behavior of the elevation prompt for administrators in Admin Approval Mode is set to “Prompt for Consent for non-Windows binaries”.

B. Agent version is incompatible.

C. UAC policy Admin Approval for the Built-in Administrator Account is set to “Disabled”.

D. UAC policy Run all administrators in Admin Approval Mode is set to “Enabled”.

**Suggested Answer:** *D*

Official Answer: D

*Community vote distribution*

C (100%)

**Takumi** Most Recent 1 year, 10 months ago

The answer is C. https://docs.cyberark.com/EPM/Latest/en/Content/WebServices/UACMonitoring-WS.htm

upvoted 2 times

**rayjohn28** 2 years, 2 months ago

C is correct. UAC Admin Approval for built in admins should be set to Enable for EPM to work properly

upvoted 4 times

**Hyper** 2 years, 5 months ago

C is correct. https://docs.cyberark.com/EPM-onprem/11.5.5/en/Content/EPM_PET/AccountAdministrator.htm

upvoted 4 times

Question #59 *Topic 1*

How does CyberArk EPM's Ransomware Protection feature monitor for Ransomware Attacks?

A. It compares known ransomware signatures retrieved from virus databases.

B. It sandboxes the suspected ransomware and applies heuristics.

C. It monitors for any unauthorized access to specified files.

D. It performs a lookup of file signatures against VirusTotal's database.

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

C (100%)

**pathomas1971** Highly Voted 2 years, 5 months ago

C. It monitors for any unauthorized access to specified files. CyberArk Endpoint Privilege Manager's Ransomware Protection feature monitors for ransomware attacks by focusing on detecting any unauthorized access to specified files. This approach involves tracking the access and modification of files that are commonly targeted by ransomware, such as documents, images, and other user data. By monitoring file access and detecting unexpected or unauthorized modifications, EPM's Ransomware Protection helps identify potential ransomware activity. It aims to detect the early stages of ransomware attacks by identifying and mitigating unauthorized file changes before they can fully execute and encrypt files. Options A, B, and D are not the primary methods used by EPM's Ransomware Protection feature to detect ransomware attacks.

upvoted 7 times

**Takumi** Most Recent 1 year, 11 months ago

The answer is C. https://docs.cyberark.com/EPM/Latest/en/Content/Intro/ImplementRansomware.htm

upvoted 2 times

Question #60 *Topic 1*

What is the CyberArk recommended practice when deploying the EPM agent to non-persistent VDIs?

A. A separate set

B. a VDI advanced policy

C. a separate license

D. A separate computer group

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*

A (100%)

**Takumi** Most Recent 1 year, 11 months ago

The asnwer is A. https://docs.cyberark.com/EPM/Latest/en/Content/Admin/AccountAdministrator.htm

upvoted 1 times

**TonyC73** 2 years, 5 months ago

Yes I just read this int he course documentation... A is the correct answer

upvoted 4 times

**pathomas1971** 2 years, 5 months ago

A. A separate set When deploying the CyberArk EPM (Endpoint Privilege Manager) agent to non-persistent Virtual Desktop Infrastructures (VDIs), the recommended practice is to create a separate set specifically for these non-persistent VDIs. This allows you to manage and apply policies differently to these types of endpoints compared to traditional endpoints. A separate set provides better flexibility and control over how EPM policies are applied to non-persistent VDIs, taking into account their unique characteristics and usage patterns. This approach helps ensure that privilege management is effectively tailored to the VDI environment, without affecting other types of endpoints. Options B, C, and D are not the recommended practices specifically related to deploying the EPM agent to non-persistent VDIs.

upvoted 4 times

Question #61 *Topic 1*

How many days after license expiration do EPM agents stop enforcing policies?

A. 1

B. 14

C. 30

D. 120

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

C (100%)

**omarjh21** Most Recent 12 months ago

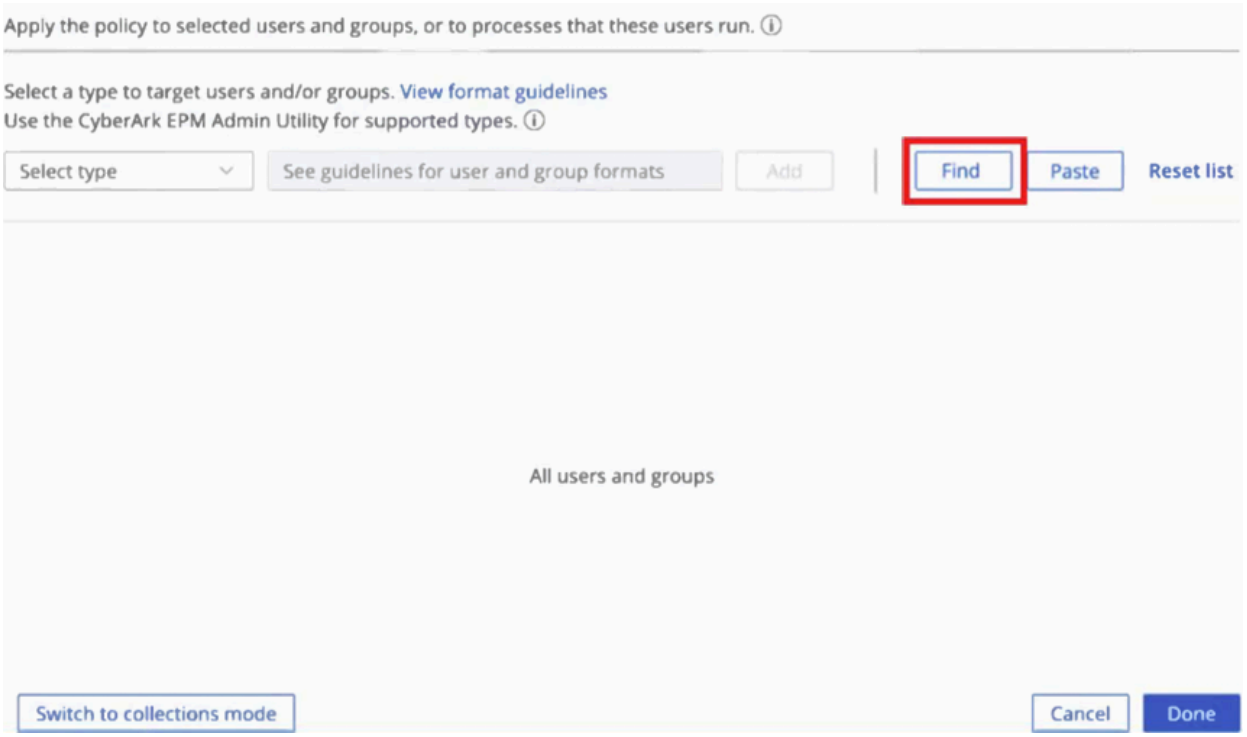
https://docs.cyberark.com/epm/latest/en/content/admin/license.htm

upvoted 1 times

Question #62 *Topic 1*

Refer to the exhibit.

When editing an application policy, what does the "Find" button do?




A. It opens all users and groups in EPM console

B. It opens CyberArk Software to check if the connection with AD is working

C. In the EPM admin utility, it opens a window to select users and group from AD or from the local endpoint

D. In the EPM admin utility, it opens a page in the EPM console for you to select the users or group

**Suggested Answer:** *C*

Official Answer: C

*Community vote distribution*

C (100%)

**omarjh21** Most Recent 12 months ago

c is correct https://docs.cyberark.com/epm/latest/en/content/policies/policiesoverview.htm?utm_source=chatgpt.com

upvoted 1 times

Question #63 *Topic 1*

What is default retention period for admin activities on the web console?

A. 14 days

B. 30 days

C. 90 days

D. 1 year

**Suggested Answer:** *B*

Official Answer: B

*Community vote distribution*

D (100%)

**b00c356** Most Recent 8 months ago

D https://docs.cyberark.com/epm/latest/en/content/intro/saas%20technical%20datasheet.htm

upvoted 1 times

**omarjh21** 12 months ago

https://docs.cyberark.com/epm/latest/en/content/intro/saas%20technical%20datasheet.htm

upvoted 2 times

Question #64 *Topic 1*

How long can a JIT policy can be granted to a user of the target resource?

A. 10 minutes to 48 hours

B. 1 to 24 hours

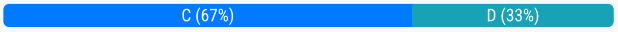
C. 1 to 72 hours

D. unlimited time range

**Suggested Answer:** *A*

Official Answer: A

*Community vote distribution*




**Rubik_07** Most Recent 8 months, 1 week ago

https://docs.cyberark.com/epm/latest/en/content/policies/jitelevationadmin-newui.htm#:~:text=Grant%20temporary%20access%20for C is correct according to the documentation.

upvoted 1 times

**ffb136c** 8 months, 2 weeks ago

https://community.cyberark.com/s/question/0D5Ht00009xO6DIKA0/provide-time-bound-administrator-access1week1month3months

upvoted 1 times

Question #65 *Topic 1*

Which statements about Privilege Threat Protection are correct? (Choose two.)

A. It only supports credential types for Windows OS and Web Browsers

B. It can detect and block credential theft for critical operating system resources.

C. It cannot create credential lures to deceive attackers

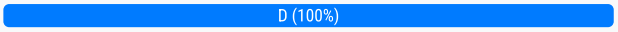
D. It helps prevent lateral movement to stop attack vectors.

E. It is limited to detecting threats in IT Applications only

**Suggested Answer:** *B, D*

Official Answer: BD

*Community vote distribution*



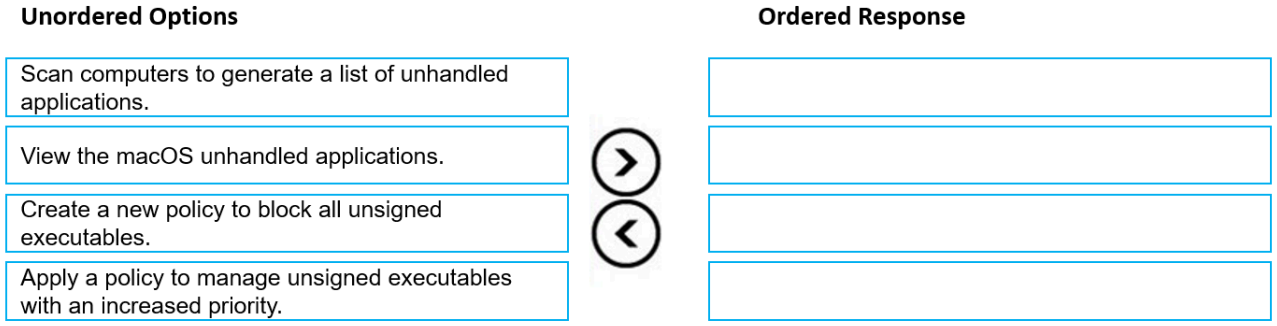

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

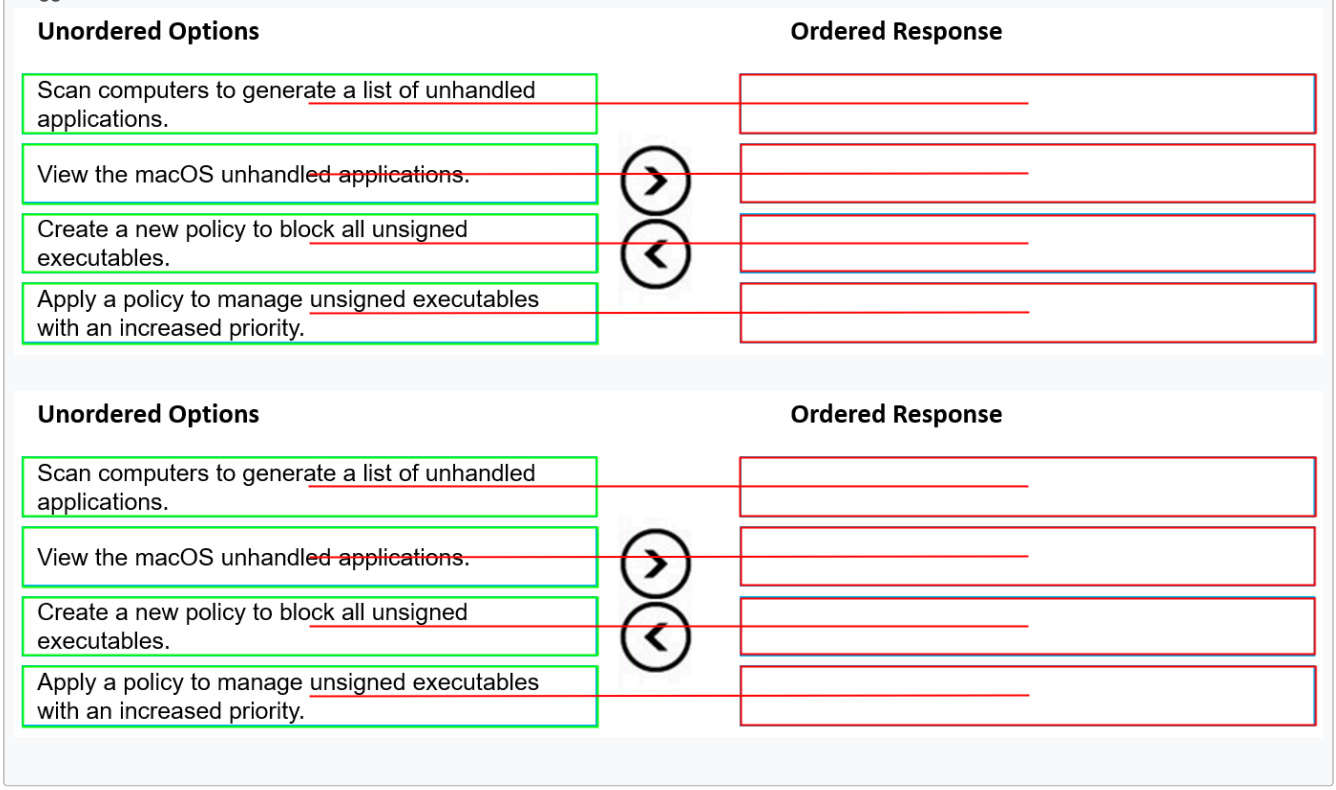
DRAG DROP

-

Arrange the steps to manage unsigned macOS executables in the correct sequence.




**Suggested Answer:**




Currently there are no comments in this discussion, be the first to comment!