Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

CyberArk EPM MCQs
CyberArk EPM TestPrep
CyberArk EPM Study Guide
CyberArk EPM Practice Test
CyberArk EPM Exam Questions

killexams.com

CyberArk

EPM

CyberArk Endpoint Privilege Manager (EPM) Defender Certification

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/CyberArk-EPM

Question: 932

Integrating EPM with Microsoft Defender for Endpoint in a 10,000-user org, enforcement drops to 70% on Windows 11 due to overlapping NGAV blocks on EPM elevations. Logs show "Defender-Overlap" errors. What defense-in-depth config pairs them effectively?

A. Exclude EPM processes in Defender policies, define conditional EPM policies for role-specific elevations
B. Disable Defender's ATP for EPM endpoints
C. Use EPM's bubble charts for overlap visualization only
D. Rely on Defender for privilege controls, auditing via EPM

Answer: A

Explanation: EDR/NGAV overlaps like Defender block EPM; exclusions plus conditional policies enforce least privilege in layers, boosting enforcement per 2026 briefs. Disabling ATP gaps security. Charts analytical, not config. Role reversal underutilizes EPM.

Question: 933

A new SAML integration requires the EPM Console to support Single Sign-On (SSO). What is the key benefit of this setup for administrators?

A. Increased password policies complexity
B. Decentralized authentication management
C. Centralized and secure authentication via identity provider
D. Agent-level authentication bypass

Answer: C

Explanation: SAML integration allows the EPM console to delegate authentication securely to a central identity provider, enabling Single Sign-On, simplifying access control, and enhancing security through federated authentication.

Question: 934

Travel agency EPM blocks booking children for reservation systems, zero standing. Customer service?

A. Booking trusted, recursive reservations.
B. Detect bookings, advanced reservations, ARA.
C. Offline bookings, lures res, logs.
D. Exemptions, priorities, SIEM.

Answer: B

Explanation: Bookings time-sensitive. Advanced scopes, ARA fraud, zero standing, service logs.

Question: 935

When integrating EPM with third-party EDR solutions, what is the primary benefit regarding threat response?

A. EPM automatically blocks threats beyond EDR detection
B. Coordinated detection and response provide layered endpoint security
C. Complete replacement of EDR is possible
D. Manual intervention is required for each detected threat

Answer: B

Explanation: EPM complements EDR by blocking risky activities proactively, while EDR detects and analyzes threats for comprehensive protection.

Question: 936

During peak load, CyberArk EPM's dashboard lags on rendering aggregated audits for 10,000+ events, but agent logs stream fine; troubleshooting pins to unoptimized exception indexing. What performance tuning preserves detailed endpoint behavior insights?

A. Shard indices by event type, prioritizing exceptions in query optimizations.
B. Adopt columnar storage for audits, accelerating exception pattern queries.
C. Compress historical aggregates, archiving low-velocity behaviors off-dashboard.
D. Implement lazy loading for reports, auditing accesses with usage metrics.

Answer: B

Explanation: High-volume exceptions overwhelm EPM's default indexing, delaying dashboard audits despite streaming logs. Columnar storage optimizes for analytical

queries on behaviors, speeding renders without sharding complexity. This sustains scalability for large-scale endpoint tracking, ensuring timely compliance reviews.

Question: 937

How does the EPM Agent communicate with the EPM Server to ensure secure and reliable policy updates and event reporting?

A. Via unsecured HTTP connections on port 80
B. Through direct file-based replication on endpoints
C. Using encrypted HTTPS connections over configurable ports
D. Using SMB protocol within the corporate LAN only

Answer: C

Explanation: EPM Agents communicate with the EPM Server securely over HTTPS with encryption, ensuring integrity and confidentiality of policies and event data. Unsecured HTTP, file replication, or SMB protocols are not used for this communication in standard EPM deployments.

Question: 938

An organization uses CyberArk EPM with integration to Microsoft Entra ID. In a deployment scenario, multiple EPM agents fail authentication and log errors indicating token expiration during policy synchronization. What is the best corrective action?

A. Increase the mutual exclusion timeout in baseline configurations
B. Verify the OAuth token lifetime and adjust refresh tokens or re-registration frequency accordingly in Entra ID
C. Disable token expiration enforcement in EPM agent settings
D. Reset all agents and reinstall the EPM software

Answer: B

Explanation: Token expiration error indicates that OAuth tokens issued by Entra ID are no longer valid. Adjusting token lifetimes or ensuring agents handle refresh tokens properly aligns with best practice to maintain seamless authentication during policy sync. Disabling expiration or reinstalling does not fix token lifecycle issues.

Question: 939

An application governed by an advanced elevate policy crashes when a specific menu

item is selected. Which EPM setting, if disabled, could cause this behavior?

A. Advanced: Time options set incorrectly for user runtime
B. Users in policy do not include the app user
C. Elevate Child Processes not enabled
D. Permissions set for Services is Allow Start/Stop

Answer: C

Explanation: The Elevate Child Processes option, when not enabled, prevents child processes spawned by an elevated parent process from acquiring elevated privileges, which can cause crashes or failures in certain application actions.

Question: 940

A security team wants to correlate endpoint EPM event logs with an external SIEM platform. Which CyberArk EPM configuration is essential to ensure robust and timely forwarding of elevation and policy exception events?

A. Disable forwarding to ensure local logs are preserved
B. Enable agent integration with SIEM via syslog or API forwarding with guaranteed retries and timestamp synchronization
C. Increase agent polling frequency to hourly instead of real-time
D. Configure agent to send only health monitoring alerts to SIEM

Answer: B

Explanation: Enabling real-time or near-real-time forwarding of relevant event logs with guaranteed retries and synchronized timestamps ensures that external SIEM platforms receive robust and accurate data for analysis and alerting. Disabling forwarding or limiting events reduces effectiveness.

Question: 941

An enterprise wants to integrate EPM's database with their existing MS SQL Server infrastructure. What key consideration must be observed?

A. EPM requires a dedicated physical SQL Server to avoid performance degradation.
B. The EPM Database schema must be modified to fit enterprise standards.
C. Only Azure SQL databases are supported by EPM natively.
D. The EPM Server supports MS SQL Server integration with a predefined schema, requiring correct permissions and connectivity.

Answer: D

Explanation: CyberArk EPM supports integration with MS SQL Server using its predefined schema and requires establishing correct permissions, connectivity, and setup according to documentation. A dedicated physical server isn't mandatory, and the schema must not be manually modified. Azure SQL support depends on the product version but MS SQL Server is natively supported.

Question: 942

macOS Ventura 5,600 PKG "Extension auto-fail upgrade." What PKG flag prevents?

A. Reorg nested and rotation creds 2026
B. Update rsyslog mac and preloader tool
C. "Include system extensions" enable in PKG create
D. Bypass proxy and monitor CPU <1%

Answer: C

Explanation: Auto-fail from omitted flag in upgrade PKG; enabling includes for auto-activation per 2026. rsyslog/preloader log/tool, nested/rotation id/access, proxy/CPU net/perf.

Question: 943

A financial firm deploys EPM agents on 5,000 endpoints segmented into sets by AD OUs for compliance auditing. During a ransomware simulation, event logs from the "Finance" set show delayed threat detection due to infrequent event batching, with heartbeat logs indicating 40-second lags. To enhance real-time response without exceeding API limits, what agent configuration optimization is recommended?

A. Configure aggregated event polling at 1000 requests per 5 minutes with 30-second heartbeat.
B. Set event batching to immediate with a 15-second heartbeat.
C. Enable raw event streaming and increase Alive interval to 60 seconds.
D. Use policy audit raw events with a 300-second policy pull cycle.

Answer: A

Explanation: EPM's API enforces a 1000-request limit every 5 minutes for aggregated events, critical for threat detection in simulations; infrequent batching delays logs from

sets like "Finance." Configuring polling to this rate—aligned with CyberArk's documentation—while retaining the default 30-second heartbeat optimizes bandwidth (approx. 25 Mbps for 100,000 agents) and ensures timely unhandled event ranking for policy automation. This supports least-privilege enforcement in OUs without hitting limits, unlike immediate batching that could throttle or raw streaming that increases unencrypted transit risks. Longer pulls prioritize compliance over real-time needs.

Question: 944

An EPM policy uses "Elevate if Necessary" for a frequently used application but users report unexpected blocking prompts. What should be checked?

A. Network bandwidth during application launches
B. Whether the application’s executable hash and publisher signature are trusted in the policy
C. Endpoint agent version compatibility with OS
D. User account lockouts in Active Directory

Answer: B

Explanation: Unexpected prompts with "Elevate if Necessary" usually indicate the application executable or its publisher is not recognized as trusted in the policy, requiring user approval.

Question:
During a policy audit, an admin observes repeated "Access Denied" events for a set enforcing timed admin sessions. What troubleshooting step is most effective?

A. Verify the user’s group membership and assigned sets in EPM
B. Reinstall the endpoint agent on affected endpoints
C. Disable all security policies temporarily
D. Increase the session timeout to 24 hours

Answer: B

Explanation: Checking group membership and set assignments ensures the user actually has privilege to access the timed admin session. Reinstalling agents or disabling policies is disruptive and an increased timeout undermines security.

Question: 945

A performance bottleneck emerges on EPM-managed endpoints during mass policy

updates, where agents exhibit 80% CPU utilization from event logging, causing delays in elevation for a fleet management app. Console diagnostics link this to verbose logging in a misconfigured set. Which tuning strategy restores baseline performance without compromising audit trails?

A. Suspend logging temporarily via CLI and analyze support info for log volume spikes.
B. Reduce overall event frequency to low and rollback the update batch to process incrementally.
C. Collect aggregated performance metrics from the console and adjust agent resource caps to 50% CPU.
D. Switch logging to batched mode with a 15-minute flush interval and exclude non-critical events from verbose capture.

Answer: D

Explanation: Verbose logging during updates floods the agent's event queue, spiking CPU as it processes and flushes logs in real-time, delaying elevations. Switching to batched mode with a 15-minute flush in the agent's data collection parameters aggregates logs efficiently, reducing I/O overhead, while excluding non-critical events (e.g., routine queries) via policy filters maintains comprehensive audits for security-relevant actions. Per EPM 25.8 agent optimization guidelines, this balances performance and compliance, avoiding low-frequency settings that under-report threats or rollbacks that prolong deployment. Resource caps throttle symptoms, and suspensions lose data irretrievably.

Question: 946

In EPM event logs, which message suggests a whitelist entry successfully allowed an application execution?

A. Privilege Blocked
B. Application Launch Allowed
C. Policy Mismatch Error
D. Trusted Source Failed

Answer: B

Explanation: "Application Launch Allowed" indicates the whitelist or elevation policy permitted execution. Other messages indicate failure or policy conflicts.

Question: 947

If a granular application group policy sets application rights based on executable hash,

what happens if the executable is updated due to a hotfix?

A. The executable will run but without elevation
B. The policy automatically adapts to time-stamped changes without manual updates
C. The updated executable will be denied until its new hash is added to the policy whitelist
D. The application group policy stops applying to that app altogether

Answer: C

Explanation: Hash-based policies require explicit inclusion of the new executable hash; otherwise, updated binaries are blocked by default deny. Policies do not adapt automatically. Running without elevation depends on policy; policy does not stop applying but enforcement denies execution.

Question: 948

Troubleshooting Entra ID-integrated CyberArk EPM reveals "Credentials rotation policy stalled - SSH connection absent" on Linux endpoints per 2026 changelog. Nested groups target sysadmins. What policy addition enforces rotation without SSH overhauls?

A. Delay rotations to quarterly and log failures in aggregated events.
B. Exempt Linux from rotation and use passwordless keys for sysadmin access.
C. Configure rotation via API calls and flatten groups for endpoint targeting.
D. Append SSH connection mandates to rotation policies and resolve nested groups via recursive claims.

Answer: D

Explanation: Appending SSH connection requirements to credentials rotation policies, as clarified in 2026 updates, ensures prerequisite fulfillment for Linux enforcement, while recursive claims resolve nested sysadmin groups for targeted application. This sustains automated rotations without exemptions that weaken security or flattening that hampers dynamic admin scaling in distributed systems.

Question: 949

A policy analyst configures elevation capabilities for a development team, using balloon notifications for UAC replacement. During testing, developers report dialog prompts overriding balloons for the same application, leading to user confusion and delayed workflows. What misconfiguration in the end-user UI settings causes this fallback behavior in EPM 25.8.x?

A. Balloon notifications are set as secondary to dialogs in the policy's notification chain, triggering only after dialog timeout.
B. The policy action is "Elevate if necessary" without specifying balloon exclusivity, defaulting to dialog for secure desktop requirements.
C. Hierarchical role permissions override UI customizations, enforcing dialogs for developer groups unless role-specific UI bindings are applied.
D. Agent configuration enables legacy UAC fallback, conflicting with custom balloons during high-load elevation requests.

Answer: B

Explanation: EPM 25.8.x elevation policies for "Elevate if necessary" default to dialog prompts on secure desktops for compliance, treating balloons as non-exclusive notifications unless explicitly set as primary in the policy's End-user UI assignment. This causes fallback when UAC-like security is needed, as balloons lack isolation. Resolution: Edit the policy to prioritize balloons via the notification dropdown, disabling secure desktop if risk-assessed, or use role-based UI customizations. This optimizes UX in dev scenarios, logging overrides for troubleshooting without compromising privilege controls.

Question: 950

EPM's Remove Local Administrators desyncs in Azure VMs with auto-scaling. Excluded "ScaleAdmins" inconsistent. What config stabilizes?

A. Resilient caching with SID exclusions for scaling events.
B. AD-pool targeting pre-scale.
C. Sign-in restores automated.
D. AI-adaptive for VMs.

Answer: A

Explanation: Agent caching in 25.8.x persists exclusions during scales, using SIDs for "ScaleAdmins." Logs track; AD suits static, restores overhead—ideal for dynamic Azure.

Question: 951

What is a limitation of relying solely on application whitelisting for ransomware mitigation in CyberArk EPM?

A. It does not restrict privilege elevation or child process creation.

B. It requires all executables to be signed by Microsoft.
C. It can cause excessive blocking of legitimate updates and applications.
D. It automatically disables zero standing privileges.

Answer: A

Explanation: Application whitelisting primarily controls which executables can run but doesn't inherently manage privilege elevations or child process trees, both critical in ransomware scenarios. It may cause false positives but does not require all executables to be Microsoft signed nor disable zero standing privileges.

Question: 952

While configuring agent baseline settings globally, you are required to ensure minimal disruption for end-user applications during policy changes. Which configuration balances this requirement?

A. Use default aggressive enforcement without baseline customization
B. Set event queue flush to minimum and mutual exclusion timeout minimum
C. Disable mutual exclusions globally to avoid conflicts
D. Increase event queue flush period and set mutual exclusion timeout moderate to reduce policy enforcement churn

Answer: D

Explanation: Increasing flush periods and setting moderate mutual exclusion timeouts reduce frequent policy enforcement changes or toggling, helping maintain application stability and user experience.

Question: 953

An EPM Administrator configures agent reporting but notices event data latency. What agent setting should they review?

A. Policy Update Rate
B. Event Queue Flush Period
C. Heartbeat Timeout
D. Condition Timeout

Answer: B

Explanation: Event Queue Flush Period impacts how frequently the agent sends

accumulated events to the EPM server, affecting real-time visibility into endpoint activity.

Question: 954

Which attack vector is most effectively mitigated by enforcing "timed admin sessions" in CyberArk EPM?

A. Lateral movement using persistent local admin rights
B. Zero-day vulnerability exploitation in system services
C. Network sniffing of user credentials
D. Phishing attacks targeting end users

Answer: A

Explanation: Timed admin sessions reduce the risk of lateral movement by limiting the duration local admin privileges are available. This minimizes the window attackers have to use compromised credentials or tools with elevated rights on an endpoint. Other vectors like zero-day exploits or phishing are not directly mitigated by timed admin controls.

Question: 955

During upgrade to v25.9, Agents report "Incompatible Cipher" on HTTPS, delaying threat policy deltas. What ensures secure flows?

A. Update Agent to support TLS 1.3 ciphers, verifying with Server handshake.
B. Fallback to reactive HTTP for upgrades.
C. Activate local OOTB until cipher fix.
D. Ignore ciphers, forcing deltas.

Answer: A

Explanation: Latest EPM (v25.9) requires TLS 1.3; Agent updates align ciphers for secure HTTPS deltas, preserving proactive protections. Fallback insecure. Local stale. Ignore breaks.

Question: 956

If a policy needs to allow execution only during business hours, which setting is essential in EPM?

A. Whitelist hash approval
B. Trusted source designation
C. Time-based conditions in elevation policy
D. Remove Local Administrators feature

Answer: C

Explanation: Time-based conditions let admins restrict privilege elevation to specified hours, enabling security with operational flexibility.

Question: 957

During a global outage response, a cloud provider's SRE team invokes EPM break-glass on on-prem hybrids for root access, but the policy's geo-fencing restricts it to HQ IPs, logging denials from remote sites. What geo-adaptive policy logic ensures distributed break-glass efficacy without geo-vector exposure?

A. Dynamically whitelist SRE device fingerprints over geo-fencing for break-glass.
B. Remove geo-fencing for all emergency procedures.
C. Mandate VPN tunneling for all invocations.
D. Limit break-glass to 5-minute bursts per site.

Answer: A

Explanation: Geo-fencing secures break-glass from location-based attacks, but rigid rules hinder distributed teams, as logs show. Fingerprinting (device traits) overrides dynamically, verifying identity beyond IP. This EPM hybrid config uses OR logic (geo OK OR fingerprint match), enabling outage fixes while mitigating spoofing, essential for cloud SRE in 2026's edge deployments.

Question: 958

A fintech firm's CyberArk EPM deployment on virtual desktops hits "UAC prompt interference" logs from incomplete mutual exclusions with Citrix. Event queues flush erratically at 20-second intervals. What desktop prep restores baseline UAC handling?

A. Add Citrix session agents to EPM mutual exclusions and standardize flush periods to 30 seconds in configs.
B. Disable UAC globally for virtual sessions and enable rush mode for queues.
C. Isolate virtual desktops in firewall zones and simulate UAC via console tests.
D. Upgrade Citrix to support EPM natively and purge old event data.

Answer: A

Explanation: Adding Citrix session agents to EPM mutual exclusions prevents interference with UAC elevations, stabilizing interactions, while standardizing flush periods to 30 seconds in agent configs normalizes queue behavior. This baseline alignment optimizes virtual desktop privilege management in fintech, avoiding UAC disables that expose sessions or isolations that complicate scaling.

Question: 959

A security team is configuring CyberArk EPM to leverage privileged account credential retrieval from PAS vault for an automation workflow that requires PowerShell scripts on servers. The workflow intermittently fails with an error stating "Credential retrieval timeout." Which of the following should be configured to mitigate this?

A. Configure EPM policies to use manual approval instead of automatic approval for JIT elevation
B. Increase the concurrency of PowerShell scripts executing credential requests
C. Disable credential caching on endpoints to force fresh credential retrieval each time
D. Increase the PAS vault API request timeout settings in the EPM server configuration

Answer: D

Explanation:
Credential retrieval timeout errors indicate that the EPM server is not receiving a timely response from the PAS vault during API calls. Increasing the timeout threshold in the EPM server configuration gives the vault more time to respond, especially during high load. Increasing script concurrency may worsen the problem, and disabling caching or changing approval modes don't directly address the timeout issue.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.