Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.

KILL EXAMS

Servicenow-CIS-EM Practice Questions
Servicenow-CIS-EM Practice Test
Servicenow-CIS-EM Practice Exam
Servicenow-CIS-EM Exam Questions
Servicenow-CIS-EM Study Guide

PASS

killexams.com

ServiceNow

Servicenow-CIS-EM

Certified Implementation Specialist - Event Management (CIS-EM)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/Servicenow-CIS-EM

Question: 1356

What is the role of the 'Processing Order' in event processing rules within ServiceNow Event Management?

A. It defines the sequence in which rules are applied
B. It determines the event source
C. It categorizes events for reporting
D. It sets the notification frequency

Answer: A

Explanation: The 'Processing Order' defines the sequence in which event processing rules are applied. This is important for ensuring that rules are executed in the correct order to achieve the desired outcomes.

Question: 1357

In a smart city initiative's ServiceNow, Event-to-Incident rule auto-creates for severity > 3 traffic events if source = "iot_traffic" and additional_info['congestion_index'] > 8 via JSON, bound to cmdb_ci_traffic_light with a GlideAggregate on em_event count > 5 in 10 minutes, excluding weekends via gs.dateGenerateInstance().getDayOfWeek() != 1 && != 7. Which criteria trigger?

A. Bound to cmdb_ci_traffic_light
B. Congestion_index > 8
C. Event count > 5 in 10 minutes
D. Not weekend day

Answer: A,B,C,D

Explanation: The rule qualifies severity > 3 IoT traffic from "iot_traffic" source, parses congestion_index > 8 from JSON for severity, binds to cmdb_ci_traffic_light for infrastructure, aggregates em_event > 5 in 10 minutes for pattern detection, and filters non-weekends with gs.dateGenerateInstance().getDayOfWeek() to focus operational hours.

Question: 1358

When configuring event management in ServiceNow, which parameter in the JSON payload is essential for identifying the source of an event?

A. Severity
B. Metric
C. Node
D. Timestamp

Answer: C

Explanation: The "node" parameter in the JSON payload is essential for identifying the source of an event. It specifies which CI the event is related to and helps in pinpointing the issue.

Question: 1359

Integrating with pre-built ServiceNow Store connector for Splunk via IntegrationHub, events flood due to unthrottled HEC tokens. What spoke actions and ETL maps control volume for Event Management?

A. Configure token expiry in HEC with rate limit 100 events/min in the spoke connection.
B. Use ETL map with filter condition additional_info.event_count > 50 to batch aggregate.
C. Set flow throttling to 500ms delay per event in designer properties.
D. Enable dedupe in spoke with key 'splunk_sid' + timestamp for HEC duplicates.
E. Log throttled events to custom table em_throttle_log for monitoring.

Answer: A,C,D

Explanation: HEC token with 100/min limit caps Splunk pushes, preventing floods. Flow delay of 500ms spaces ingestion sustainably. Dedupe on splunk_sid + timestamp eliminates HEC retries, optimizing for EM processing.

Question: 1360

In the context of ServiceNow, what is a key advantage of using the MID Server for Discovery?

A. It facilitates secure data collection from external sources.
B. It allows for the creation of custom dashboards.
C. It automates the incident management process.
D. It provides a user-friendly interface for administrators.

Answer: A

Explanation: A key advantage of using the MID Server for Discovery is that it facilitates secure data collection from external sources. This capability is crucial for maintaining an accurate and up-to-date CMDB.

Question: 1361

Nested JSON from API: {"cluster": {"nodes": [{"id": "N1", "health": "degraded", "metrics": {"cpu": 95}}]}}. To flatten metrics to KV with encryption, script?

A. var node = payload.cluster.nodes[0]; additional_info['cpu'] = node.metrics.cpu; var encHealth = encrypt(node.health);
B. Use JSONPath $..metrics.cpu for extraction
C. Validate nesting depth <5 to avoid parse errors
D. Set severity from health: degraded=3
E. Bulk event creation for multi-node arrays

Answer: A,C,D

Explanation: Direct access flattens nested metrics to KV. Depth validation prevents stack overflows. Health-to-severity maps cluster events.

Question: 1362

A company is preparing to implement ServiceNow Event Management. They need to activate the Event Management plugin. What is the correct command to activate the plugin in the ServiceNow instance?

A. plugin.activate('com.glide.itom.event_management')
B. activate.plugin('com.glide.itom.event_management')
C. glide.plugin.activate('com.glide.itom.event_management')
D. enable.plugin('com.glide.itom.event_management')

Answer: C

Explanation: The correct command to activate the Event Management plugin in ServiceNow is `glide.plugin.activate('com.glide.itom.event_management')`, which ensures that all necessary features for Event Management are available.

Question: 1363

You are tasked with creating a business rule that logs the details of events when they are created. Which of the following methods should you use to access the event's `message` field in the business rule?

A. `current.message;`
B. `current.message.getValue();`
C. `current.getValue('message');`
D. `current.getMessage();`

Answer: A

Explanation: The correct way to access the event's `message` field is simply using `current.message;`, which directly retrieves the value of that field.

Question: 1364

A healthcare system processes patient monitoring events with additional_info as {'device_id': 'MED-456', 'patient_id': 'PAT-789', 'metric': 'heart_rate', 'value': 120, 'timestamp': '2026-10-05T14:30:00Z', 'ci_link': 'cmdb_ci_medical_device:sys_id_xyz'}. Association to cmdb_ci_medical_device must trigger impact on cmdb_ci_service_auto for critical care services. What advanced features enable this?

A. Use Regex in CI Field Matcher: current.cmdb_ci = /cmdb_ci_medical_device:(\w+)/.exec(additional_info.ci_link)[1] to extract sys_id
B. Enrich the event with gs.now() relative to additional_info.timestamp for time-based severity adjustment in the transform
C. Set up Alert Management Rule with condition JSON.parse(additional_info).value > 100 to bind and propagate via 'Affects::Affected by' relations
D. Configure a custom property evt_mgmt.additional_info.parse_depth=3 to handle nested timestamps in JSON

Answer: A, C

Explanation: Regex in the CI Field Matcher extracts the sys_id from the ci_link string in additional_info, enabling direct association to the medical device CI. The Alert Management Rule condition parses the JSON value and promotes only high heart_rate events, binding them and propagating impact through 'Affects::Affected by' cmdb_rel_ci relations to critical care services.

Question: 1365

In a scenario where you need to monitor AWS resources, which key metric should be monitored using AWS CloudWatch to ensure optimal performance?

A. CPU Utilization
B. Network Latency
C. Disk I/O
D. Memory Usage

Answer: A

Explanation: Monitoring CPU Utilization is critical for assessing the performance and health of AWS resources, allowing for proactive management.

Question: 1366

During a merger, an organization merges two ServiceNow instances, requiring Discovery to repopulate the CMDB with reconciled CIs from both sources while maintaining event correlation integrity. Which advanced steps facilitate this without data loss?

A. Use the 'cmdb_ci_service.reconcile' transform map to merge business service CIs based on the 'correlates_with' attribute from pre-merger event rules.
B. Run the 'Identify Duplicate CIs' job with the 'duplicate_ci_threshold' set to 0.8 to flag and merge overlapping infrastructure CIs before re-running Discovery schedules.
C. Export event rules from the source instance via XML, importing them with updated CI identifiers using the 'sys_update_xml' loader, preserving mapping logic.
D. Configure the MID Server failover group with 'mid.server.failover.priority=1' for the primary cluster to handle reconciliation probes without interruption.

Answer: A, C

Explanation: The cmdb_ci_service.reconcile transform map uses correlates_with

attributes derived from existing event rules to merge business services accurately, retaining correlation paths. Importing event rules via XML with sys_update_xml ensures mappings to CIs are preserved, avoiding recreation of complex identification logic tied to Discovery-populated data.

Question: 1367

When handling payload data in ServiceNow, where is the raw data typically found in an event record?

A. event_type
B. payload_data
C. additional_info
D. event_source

Answer: C

Explanation: The raw data from events is typically found in the `additional_info` field, which contains key-value pairs relevant to the event.

Question: 1368

A telecom's 5G base stations send events via MID Server, type=operational, severity=5, node=cellTowerID, description= signal strength JSON. Rule set default order 140 sets strength_dbm=JSON.dbm, but em_alert_aggregate groups tower-wide during spectrum interference. Which signal configs?

A. Dictionary strength_dbm integer, range -140 to 0 for validity.
B. Aggregation group_type='Text based', keywords 'interference' + towerID.
C. Order 130 rule: if strength_dbm <-100, set severity=2 for interference priority.
D. Bind to cmdb_ci_base_station, use 'Affects::Affected by' for spectrum CI.

Answer: B, D

Explanation: Text keywords + ID bucketing isolates interference in em_alert_aggregate. Base station binding with affects relationships correlates spectrum, optimizing default without range or priority changes.

Question: 1369

A system administrator is reviewing the configuration of the Event Management engine and notices that the event processing time is increasing. What could be a potential cause?

A. The engine is processing too few events.
B. The correlation rules are too simplistic.
C. The MID Server is underutilized.
D. There are too many events being processed simultaneously.

Answer: D

Explanation: An increase in event processing time can be caused by too many events being processed simultaneously, leading to performance bottlenecks in the Event Management engine.

Question: 1370

Correlation_id 'net-uuid-333' events not linking in Impact Tree due to missing rel_type in cmdb_rel_ci. Force UUID gen and tree refresh. Which commands?

A. Event Mapper: Set additional_info.net_uuid = gs.generateGUID() for net source
B. Fix Script: Update cmdb_rel_ci set rel_type_id = 'depends on' where parent=net_ci
C. gs.eventQueue('impact.refresh', {id: 'net-uuid-333', full: true})
D. Property em.impact.auto_refresh = true

Answer: B,C

Explanation: Updating rel_type fixes dependencies. Event queue refreshes tree for UUID. Mapper ensures future linking, property enables auto but manual is precise.

Question: 1371

What is a common challenge faced when using Discovery data for event management?

A. Too many events being processed at once
B. Insufficient documentation on event rules
C. Lack of user access to event dashboards
D. Inconsistent naming conventions for configuration items

Answer: D

Explanation: A common challenge when using Discovery data for event management is inconsistent naming conventions for configuration items. This inconsistency can lead to difficulties in correlating events with the correct CIs.

Question: 1372

A company wants to extract specific fields from a JSON payload received from a third-party application. Which transform script function should be used to parse the JSON and retrieve the "status" field?

A. getFieldValue()
B. transformJSON()
C. parseJSON()
D. JSON.parse()

Answer: D

Explanation: The `JSON.parse()` function is used to convert a JSON string into a JavaScript object, allowing you to access specific fields like "status" in the payload.

Question: 1373

Azure Sentinel events via API have encrypted claims in token field. Rules decrypt with Azure key vault integration script, filter for 'threat_level' == 'high', map to alert.threat. Secure handling?

A. Script: var claims = azureDecrypt(current.token, vault_url, client_id); alert.threat = claims.threat_level == 'high' ? claims.details : null;
B. Filter: current.source == 'sentinel' AND token.length >0; use vault_call with timeout 5s.
C. Property 'em.azure.vault_timeout' = 5000ms; fallback claims = {threat: 'medium'}.
D. Audit rule: logDecryptAttempt(current.sys_id, success); if fail, quarantine event.

Answer: B, D

Explanation: The Filter validates token presence and sets vault call timeout to prevent hangs. The audit rule logs attempts, quarantining failures to track security issues without alerting on invalid data.

Question: 1374

What is the role of the "Event Correlation" feature in ServiceNow Event Management?

A. To automatically close incidents based on event status
B. To assign events to specific teams for resolution
C. To generate reports on historical event data
D. To group related events into a single alert for easier management

Answer: D

Explanation: The Event Correlation feature groups related events into a single alert, simplifying management and allowing teams to focus on resolving the underlying issues.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, 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.

Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllbus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.