

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



ServiceNow CIS-EM MCQs ServiceNow CIS-EM TestPrep ServiceNow CIS-EM Study Guide ServiceNow CIS-EM Practice Test ServiceNow CIS-EM Exam Questions



killexams.com

**ServiceNow** 



Certified Implementation Specialist - Event Mangement











**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': '2025-10-05T14:30:00Z', '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.

KILL EXAMS





# 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.