Exam Questions CIS-EM

Certified Implementation Specialist-Event Management Exam

https://www.2passeasy.com/dumps/CIS-EM/

NEW QUESTION 1
What would you use as a central location to explore the CMDB class hierarchy, CI table definitions, and CIs?

A. CI Remediations
B. CI Relation Types
C. CI Identifiers
D. Process to CI Type Mapping
E. CI Class Manager

Answer: E

NEW QUESTION 2
What are the valid states an alert can be in during its lifecycle?

A. Open, Reopen, Flapping, Closed
B. New, Updating, Waiting, Complete
C. Open, Updating, Swinging, Closed
D. Open, Warning, Flapping, Clear

Answer: A

Explanation:
Reference: https://docs.servicenow.com/bundle/orlando-it-operationsmanagement/page/product/event- management/task/t_EMSetTheAlertActiveInterval.html

NEW QUESTION 3
A customer informs you that they already have monitoring and event management tools.
Which of the following describes the extra value that ServiceNow Event Management provides? (Choose four.)

A. ServiceNow Event Management Alerts, Incidents, Problems, and changes are automatically correlated with CIs and Business Services that can be visualized in Business Service maps.
B. ServiceNow Event Management manages relationships between alerts and related incidents to maintain an end-to-end event management lifecycle.
C. ServiceNow Event Management provides a business-centric platform and single system of record for service monitoring and remediation results, to better control and manage performance and availability.
D. ServiceNow Event Management provides state-of-the-art performance monitoring capabilities across a wide array of different types of infrastructures.
E. ServiceNow Event Management utilizes the power of integration with leading monitoring systems to automatically create actionable alerts.

Answer: ABCE

NEW QUESTION 4
Which is a correct regex expression to capture only the server's hostname (webserver3) in "The server webserver3.domain.com is down."?

A. The server (.*)\..*
B. .*(\w+\Aw+VAw+).*
C. The server (.*)\s.*
D. The server (.*?)\„*

Answer: D

NEW QUESTION 5
Which is the best option to reduce latency issues when receiving events?

A. Verify bucket field in em_event table > 0
B. Verify event_processor_job_count = 2
C. Verify event_processor_job_count = 0
D. Verify event_processor_enable_multi_node = 2

Answer: D

NEW QUESTION 6
The ServiceNow standard and shared set of service-related definitions that enable and support true service level reporting is known as what?

A. Service level data model
B. Business service data model
C. Application service data model
D. Common service data model

Answer: C

NEW QUESTION 7
What event will cause Agent Client Collector self-monitoring to pause data collection?

A. Communication with the MID server is lost
B. The amount of host memory being used by the agent exceeds a threshold
C. Communication with the ServiceNow instance is lost

D. The amount of host disk space used by the agent exceeds a threshold
E. The amount of host CPU being utilized by the agent exceeds a threshold

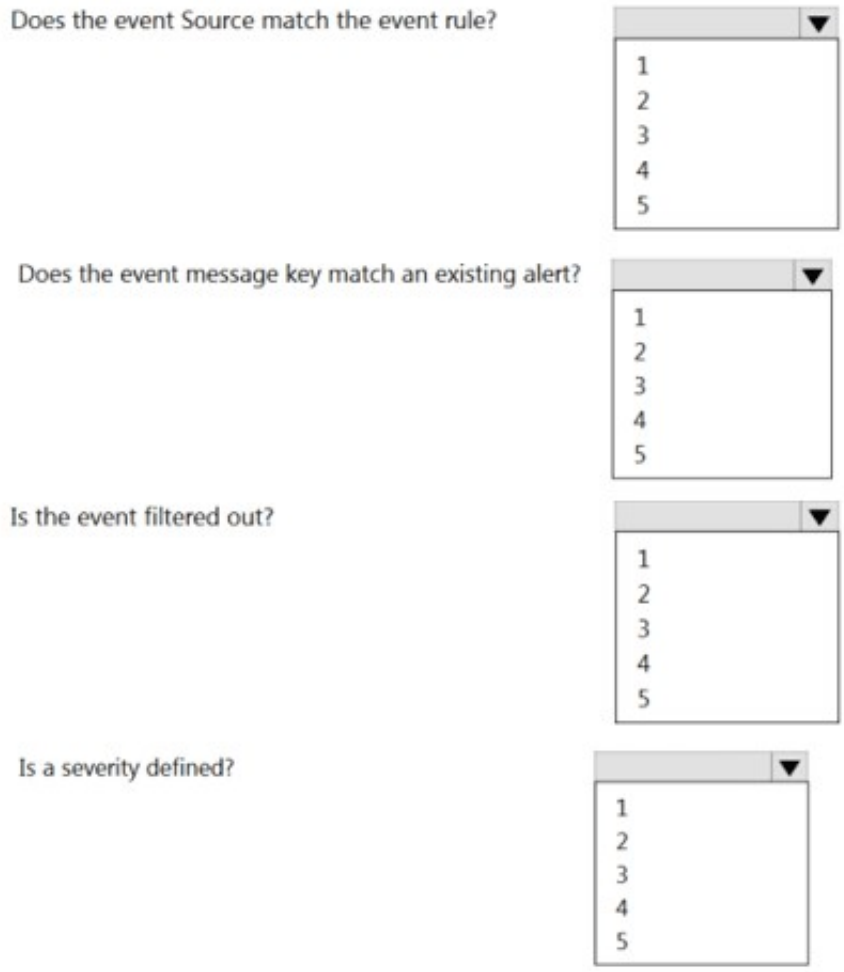
Answer: E

NEW QUESTION 8
What would be the primary use case for creating Javascripts in Event Management?

A. To create a customized pull connector to retrieve events on behalf of an event source
B. To automatically populate the Configuration Management Database (CMDB)
C. To parse a nodename out of your raw event data in an event rule
D. To run as part of a remediation workflow for IT alerts that fail to execute

Answer: A

NEW QUESTION 9
HOTSPOT
In what sequence are events processed?



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Does the event Source match the event rule?

1
2
3
4
5

Does the event message key match an existing alert?

1
2
3
4
5

Is the event filtered out?

1
2
3
4
5

Is a severity defined?

1
2
3
4
5

NEW QUESTION 10
What is the primary benefit of using Now Assist for ITOM?

A. It decreases the number of alerts generated
B. It reduces the need for licensing and store app installations
C. It provides an analysis in summary in easy-to- understand language
D. It eliminates the need for IT operators

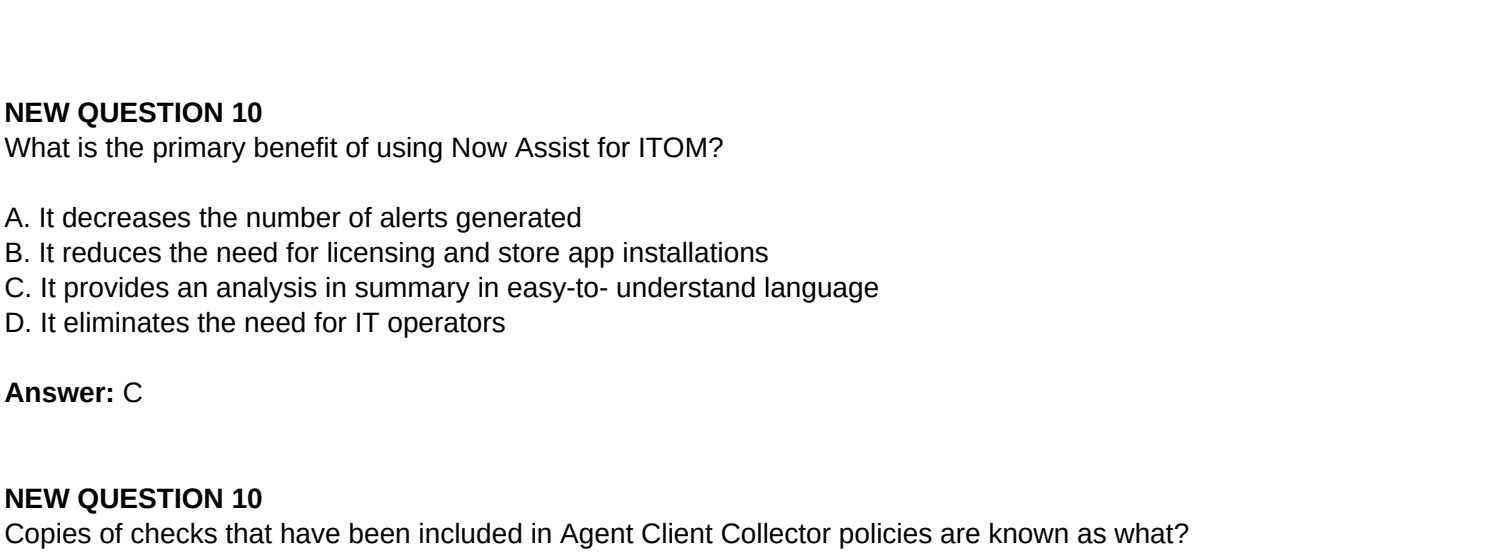
Answer: C

NEW QUESTION 10
Copies of checks that have been included in Agent Client Collector policies are known as what?

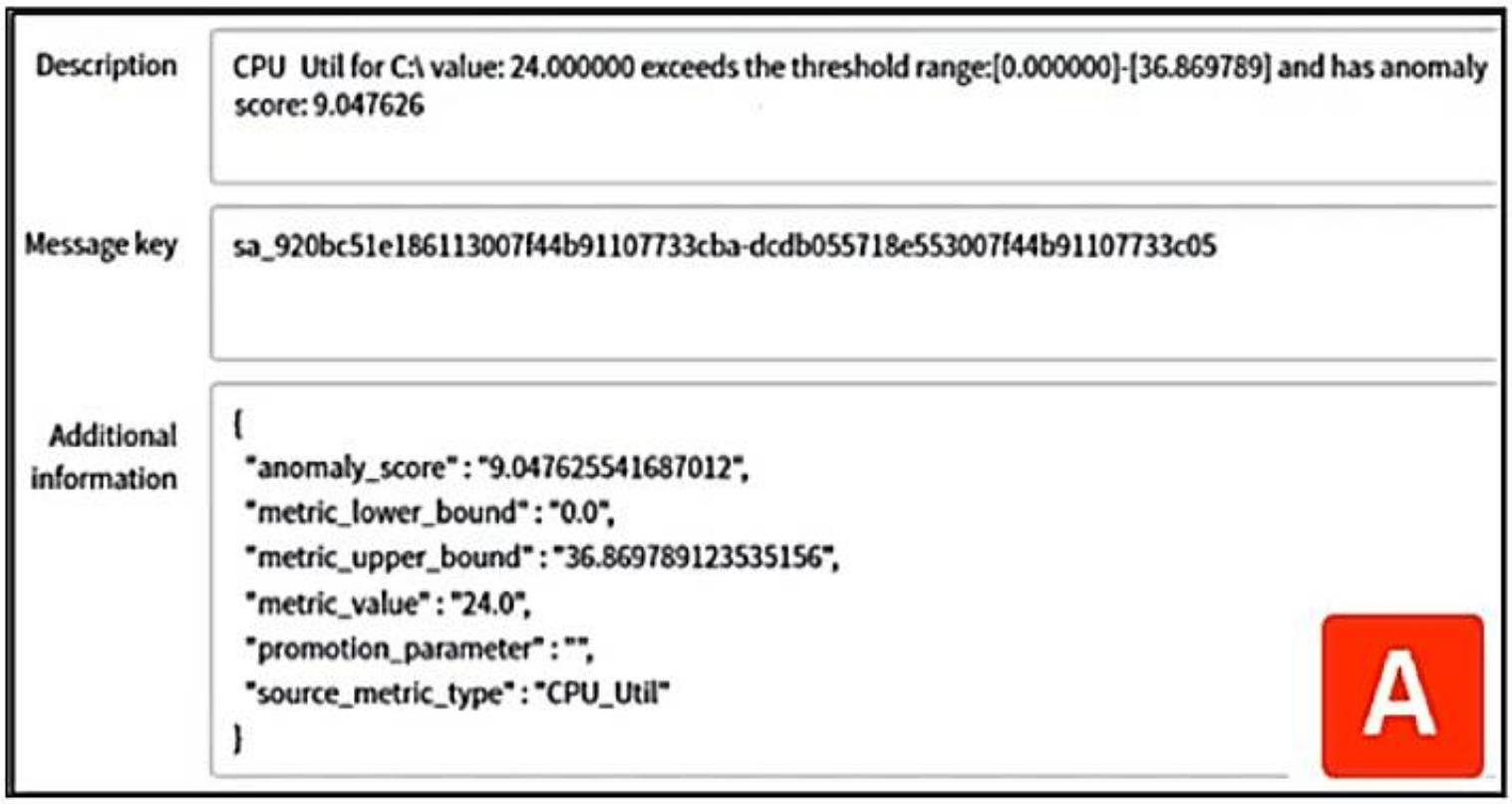
A. Check definitions
B. Check models
C. Check clones
D. Check mirrors
E. Check instances

Answer: E

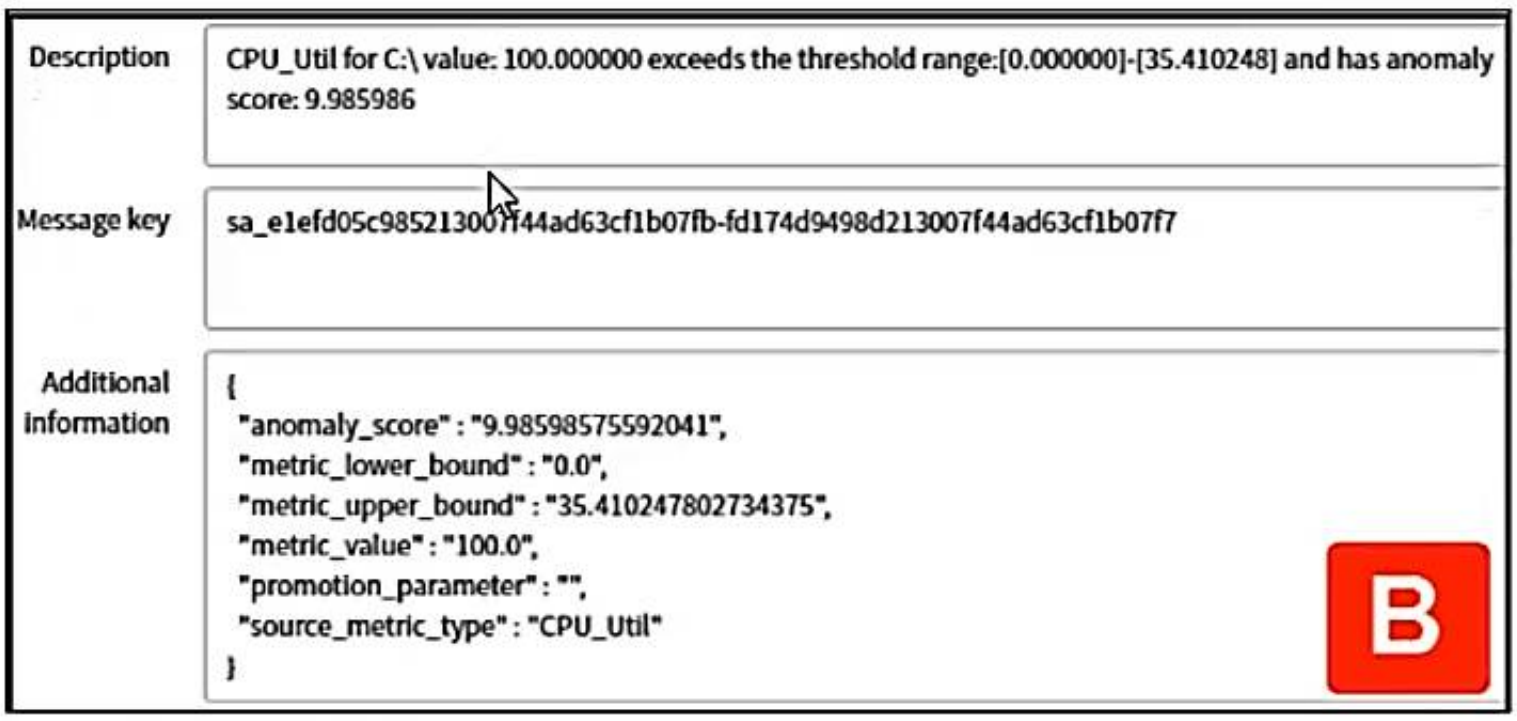
NEW QUESTION 14
Which the following alert promotion rule defined in your ServiceNow instance, which of the anomalies below would be automatically promoted into IT alerts on the Alert Console?



A)



B)



C) Both anomaly A and anomaly B
D) Neither anomaly A or anomaly B

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 16
What are the possible actions available in alert management?
Choose 3 answers

A. Execute remediation subflows
B. Execute remediation workflows
C. Launch applications
D. Evaluate business rule
E. Create a service catalog request

Answer: ABCD

NEW QUESTION 18
Modified Agent Client Collector policies do not take effect until what action is taken?

A. Agents are restarted
B. Agents re-run the discovery policy
C. MID server synchronization is initiated
D. The policy is republished
E. The check is tested on an existing agent/host

Answer: D

NEW QUESTION 21
Which attribute is responsible for de-duplication?

A. Metric_name
B. Message_key
C. Short_description
D. Additional_info

Answer: B

NEW QUESTION 22
What is one of the benefits of using alert automation in Service Operations Workspace?

A. It offers a simplified experience for creating and managing event and alert related rules
B. It uses back end tables separate from those in event management rules
C. It enables centralized administration for all alert management
D. It does not require any knowledge of the source event collection tool

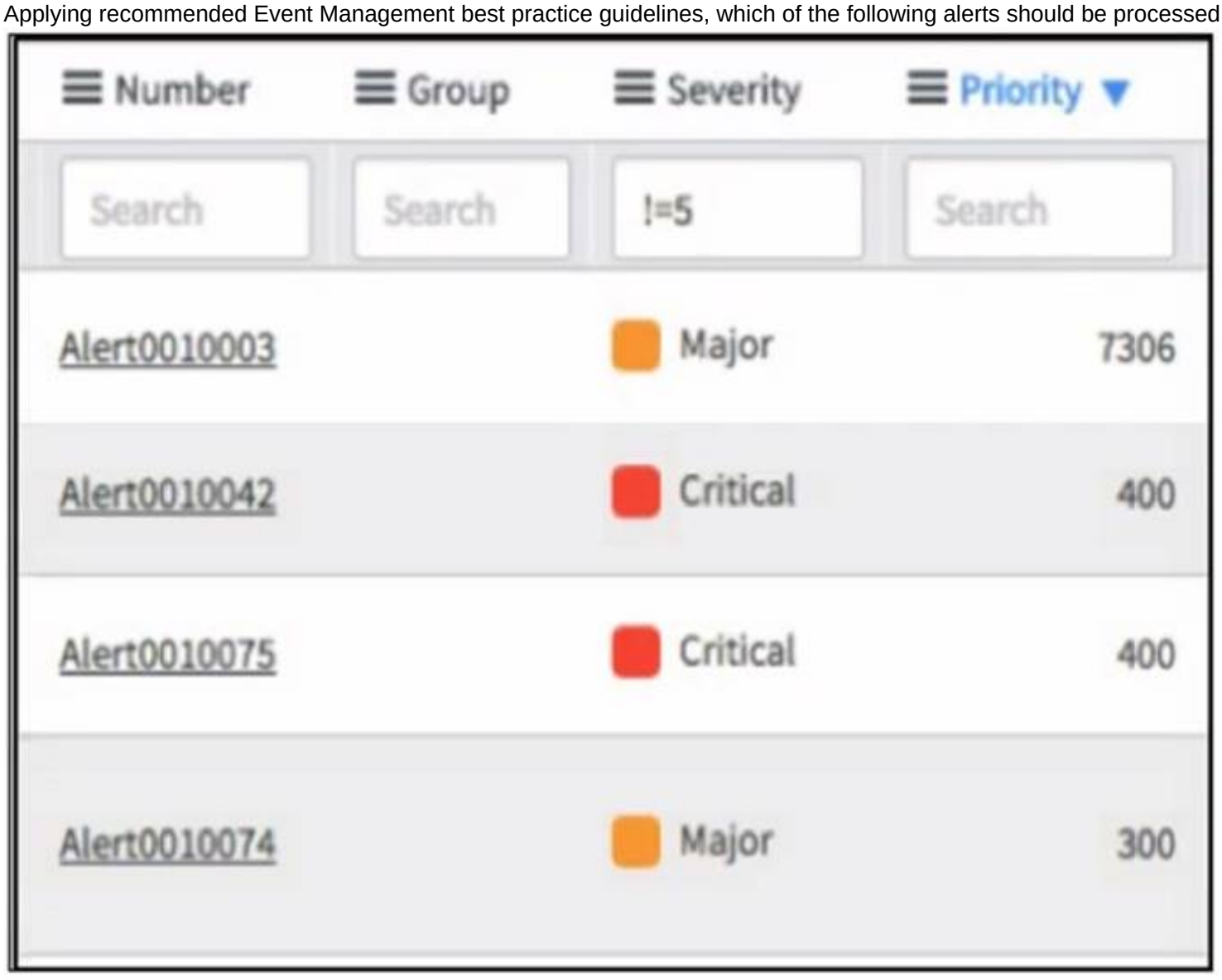
Answer: A

NEW QUESTION 26
The correct regex to capture the name of the server in ??the server webserver3.domain.com is down?? would be:

A. .*(\w+\.\w+\.\w+).*
B. The server (.*)\s.*
C. .*\s(\w+\.\w+\.\w+).*
D. the server (.*).*

Answer: A

NEW QUESTION 30
Applying recommended Event Management best practice guidelines, which of the following alerts should be processed first?



A. Alert00l0042
B. Alert0010003
C. Alert00l0075
D. Alert00l0074

Answer: B

NEW QUESTION 33
Which step in the event rule configuration process enables you to ignore events and prevent alert generation?

A. Transform and compose alert output
B. Event filter
C. Event options
D. Threshold

Answer: D

NEW QUESTION 34
What is the primary function of enrich automation in Service Operations Workspace?

A. To populate events with more meaningful information
B. To manage team roles and permissions
C. To transform and compose event rules
D. To generate alerts populated with more meaningful information

Answer: D

NEW QUESTION 37
What are the key components that can be managed using Service Operations Workspace integrations Launchpad?

A. Event Connectors, Metric Policies, Log Data Inputs
B. Event Management, Metric Policie
C. Log Monitoring
D. Event Management, Metric Intelligence, Log Monitoring
E. Event Connectors, Metric Intelligence, Log Data inputs

Answer: D

NEW QUESTION 42
What does the Service Operations Workspace express list reduce the need for?
Choose 2 answers

A. Conducting root cause analysis
B. Constantly refreshing the list of alerts
C. Navigating through different interfaces
D. Performing remediation actions

Answer: BC

NEW QUESTION 46
What makes all ServiceNow metrics, tasks, services, configuration items, assets, people, locations, and information a single system of record for IT and business processes?

A. ServiceNow is installed within your datacenter providing you complete control
B. All applications are built on the Oracle database standard, providing uniformity across products
C. All applications that are built by ServiceNow utilize the same data model and code base
D. ServiceNow runs on supported Windows servers and is managed through Windows Update
E. A single table houses all data elements within ServiceNow
F. ServiceNow utilizes the AWS MariaDB cloud database structure, providing a single system of record

Answer: B

NEW QUESTION 51
A support agent resolves an incident associated with an alert. What is the best method to close the alert?

A. Set the evt_mgmt.incident_closes_alert
B. Set the evt_mgmt.alert_closes_incident
C. Switch over to the alert form and close the alert manually
D. Create a business rule on the alert table to match the associated Incident with its respective alert
E. Create a business rule on the incident table

Answer: A

NEW QUESTION 54
What type of system can a MID Server can be installed on?

A. OpenVMS System
B. Microsoft Windows Server
C. Linux System
D. Microsoft Windows Desktop
E. Any system inside the customer firewall
F. Mac OS X System

Answer: B

NEW QUESTION 57
Processing on an event will create a state of error if what value is not set?

A. Node
B. Source

C. Severity
D. Message Key
E. Resource

Answer: B

NEW QUESTION 60
What is an alert called that moves from an open to a closed state multiple times within a designated time-frame?

A. Fluctuating
B. Swinging
C. Flipping
D. Flapping

Answer: D

NEW QUESTION 61
What is the primary function of the link view feature in the Service Operations Workspace express list?

A. To automatically generate incidents from linked alerts
B. To manage user permissions across teams
C. To visualize tag-based alert groups
D. To update the CMDB dependency map

Answer: C

NEW QUESTION 65
Which attribute correlates multiple events to one alert?

A. Additional_info
B. Message_key
C. Metric_name
D. Short_description

Answer: B

NEW QUESTION 69
When setting up a monitoring connector definition PULL the M.0 Server must be validated and have Line of Sight (LoS) to the monitoring system. This configuration requires what?
Choose 4 answers

A. Polling interval for scheduling access to the target system
B. Internal IP address and port for communication with the target System
C. An active and validated MID Server
D. Access credentials la the MID Server system
E. Internal IP address and port for communication with the MID Server system
F. Access credentials lo the monitoring system

Answer: ABCF

NEW QUESTION 73
Which attribute within an event needs to be exactly the same to allow for deduplication?

A. Metric Name
B. Message Key
C. Type & Node
D. Description
E. Correlation ID

Answer: B

NEW QUESTION 78
You have a system configured with a MID Web Server using Basic authentication to enable Operational Management Intelligence (OI) to push raw metric data to the MID Server. No data is getting through to the MID Server.
What is the most likely cause of the issue?

A. The MID Web Server needs to be Restarted
B. The MID Web Server needs to be Started
C. An invalid secret key is being passed in the header information of the URL for the REST request
D. An invalid password is set in the MID Web Server Context

Answer: A

NEW QUESTION 80
The additional information field is a JSON string that gives more information about an event. An example of a supported JSON string is:

A. {"CPU":100}
B. {"CPU":100,??Status":3}
C. {"CPU":"100","Status":3}
D. {"CPU":"100"}

Answer: C

NEW QUESTION 82
How would you ensure the quality of data in your Configuration Management Database (CMDB) over time?

A. Manually inventorying configuration items in the CMDB and eliminating duplicate configuration items (CIs)
B. Only use the ServiceNow Discovery application to populate your CMDB
C. Using only scripts to automatically monitor for and remediate duplicate configuration items (CIs)
D. Having well-defined Identification, Reconciliation, and Relationship rules

Answer: D

NEW QUESTION 85
During processing of the event and if the event Severity is blank, the state of the event is set to:

A. Ready
B. Ignored
C. Error
D. Processing

Answer: C

NEW QUESTION 88
What is the preferred method of parsing in the Transform/Compose step of an event rule?

A. Python
B. Regex
C. sed/awk
D. JavaScript

Answer: B

NEW QUESTION 92
What missing attribute would cause an event to have a state of Error?

A. Metric Name
B. Source
C. Classification
D. Node
E. Severity

Answer: E

NEW QUESTION 97
When sending data from the monitoring source to the additional_info field, what format is supported?

A. XML
B. JSON
C. YAML
D. Comma separated

Answer: B

NEW QUESTION 102
A monitoring tool notification of a notable occurrence is known as what?

A. An alarm
B. An alert
C. An incident
D. A notice
E. An event
F. A metric

Answer: C

NEW QUESTION 105
What role is required to create a Technical Service?

A. evt_mgmt_integration
B. evt_mgmt_user

C. evt_mgmt_operator
D. evt_mgmt_admin

Answer: D

NEW QUESTION 110
When creating an alert management rule, where would you specify a workflow to resolve a given condition?

A. From the Remediation tab
B. From the Actions tab
C. From the Launcher tab
D. In the Related Links section

Answer: A

NEW QUESTION 115
By default, Event Management tries to bind an alert to CI (configuration item), by matching the node name in the event to which three items in the CMDB (configuration management database)?

A. CI name, Fully qualified domain name, IP or MAC address
B. CI name, Webserver name, IP or MAC address
C. CI name, Fully qualified domain name, SSH public host keys
D. System class name, Fully qualified domain name, IP or MAC address

Answer: A

NEW QUESTION 119
When are anomaly alerts generated by Operational Intelligence displayed in alert intelligence?

A. When the statistical model threshold is breached
B. When they are promoted to IT alerts
C. When it is manually promoted in insights explorer
D. When the anomaly score is greater than 100

Answer: B

NEW QUESTION 122
Based on the information shown, which of the following three alerts should be processed first?

A. The Alert Priority score 3106020.001 was calculated according to the following factors, ordered by their respective priority (2018-06-01 19:34:01 GMT) Category (Score, Weight)* 1. Business services – (3.0, 1000000)* 2. Severity – (1.0, 100000)* 3. CI type – (60.0, 100)* 4. Role – (2.0, 10)* 5. Secondary – (0)* 6. State – (1.0, 0.001)
B. The Alert Priority score 4406020.001 was calculated according to the following factors, ordered by their respective priority (2018-05-31 20:04:47 GMT) Category (Score, Weight)* 1. Business services – (4.0, 1000000.0)* 2. Severity – (4.0, 100000.0)* 3. CI type – (60.0, 100.0)* 4. Role – (2.0, 10.0)* 5. Secondary – (0)* 6. State – (1.0, 0.001)
C. The Alert Priority score 3306020.001 was calculated according to the following factors, ordered by their respective priority (2018-05-31 19:56:54 GMT) Category (Score, Weight)* 1. Business services – (3.0, 1000000.0)* 2. Severity – (3.0, 100000.0)* 3. CI type – (60.0, 100.0)* 4. Role – (2.0, 10.0)* 5. Secondary – (0)* 6. State – (1.0, 0.001)
D. They should be processed in the order in which they were received.

Answer: B

NEW QUESTION 123
You have an event with a Source of ??Trap from Enterprise 111??, but the alert created for this event shows a Source of ??Oracle EM??. If you want to change what this is set to, where in the event rule would you do this?

A. Transform and Compose Alert Output lab
B. Event rule info tab
C. CI Binding tab
D. Event Filter tab

Answer: B

NEW QUESTION 127
Which two methods can be used to improve the processing of events in large network environments? (Choose two.)

A. Enable multi-node processing
B. Increase the source polling interval
C. Ensure the bucket value in the event table is greater than 0
D. Increase the number of scheduled jobs processing events

Answer: AC

NEW QUESTION 130
What is the minimum role needed to view alerts?

A. alert_operator
B. evt_mgmt_user
C. evt_mgmt_operator
D. alert_user

Answer: A

NEW QUESTION 134
What would you use to define the monitoring sources allowed to communicate with the ServiceNow instance for Operational Intelligence?

A. Metric Registration
B. Metric Config Rules
C. Metric Type Actions
D. Metric to CI

Answer: C

NEW QUESTION 138
Agent Client Collector can perform application service monitoring by configuring what option?

A. An alert management rule
B. A proxy agent
C. A distributed cluster
D. An event rule
E. A REST API

Answer: B

NEW QUESTION 141
By default, the Alert Console displays what type of alerts?

A. All Primary, Open alerts and anomaly alerts with a Severity of Critical, Major, Minor, and Warning that are not in Maintenance mode
B. All Primary and Secondary Open alerts and anomaly alerts with a Severity of Critical, Major, Minor, and Warning that are not in Maintenance mode
C. All Primary alerts with a Severity of Critical, Major, Minor, Warning that are not in Maintenance mode
D. All Primary, Open alerts with a Severity of Critical, Major, Minor, and Warning that are not in Maintenance mode
E. All Primary and Secondary Open alerts with a Severity of Critical, Major, Minor, and Warning that are not in Maintenance mode

Answer: E

NEW QUESTION 143
Where would you look to find and troubleshoot transactions and events that occur on your ServiceNow instance?

A. em_event table
B. System log module
C. Event Mangement dashboard
D. State management logs module

Answer: B

NEW QUESTION 146
For an incoming event with a matching message key, what allows an existing alert to be automatically closed?

A. In the event rule, set the Severity to 0
B. In the alert rule, set the Severity to 0
C. In the alert rule, set the Severity to -1
D. In the event rule, set the Severity to -1

Answer: D

NEW QUESTION 147
A Service is not viewable in Operator Workspace. What could be the issue?

A. The service is a manual service
B. The service is not set to operational
C. The service was created through Service Mapping
D. The service is a technical service

Answer: B

NEW QUESTION 151
What applications are included in the ITOM Health product?

A. Event Management and Operational Intelligence
B. ITOM Visibility
C. Discovery and Service Mapping

D. Cloud Management

Answer: A

NEW QUESTION 152
In the event table, which field maps the external attributes from the target system?

A. Resource
B. Description
C. Source
D. Additional Information

Answer: C

NEW QUESTION 156
You have a very large networking environment and have noticed that your event notifications are either not being triggered or are delayed.
What are best options to try to resolve this issue? (Choose two.)

A. Ensure all Event Management – process events jobs are set to a Ready state
B. Verify that the Bucket field in the event table is set to zero (0)
C. Add additional event processor jobs
D. Ensure multi-node event processing is disabled

Answer: AC

NEW QUESTION 157
Where can you look to determine what event rule created an alert? (Choose two.)

A. Alert Activity
B. Event Additional Information
C. Event Processing Notes
D. Alert Message Key
E. Alert Source

Answer: AE

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-it-operationsmanagement/page/product/event- management/task/t_EMViewRuleApply.html

NEW QUESTION 159
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CIS-EM Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CIS-EM Product From:

https://www.2passeasy.com/dumps/CIS-EM/

Money Back Guarantee

CIS-EM Practice Exam Features:

* CIS-EM Questions and Answers Updated Frequently

* CIS-EM Practice Questions Verified by Expert Senior Certified Staff

* CIS-EM Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CIS-EM Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year