



"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks.com

Warning: Keep connected with our support team for latest updates

Question: 1

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

Explanation:

Reference: <https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/task/create-alert-management-rule.html>

Question: 2

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

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-servicenow-platform/page/product/mid-server/reference/r_MIDServerSystemRequirements.html

Question: 3

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

Explanation:

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

Question: 4

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

Explanation:

Reference: <https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/concept/operational-intelligence-overview.html>

Question: 5

The value of the Alert Priority score is a composite of what?

- A. The value of the alert's category and its relative weight
- B. The value of the alert's category and its Priority Group
- C. The value of the alert's Severity and its Priority Group
- D. The value of the alert's Severity and its relative weight

Answer: A

Explanation:

Reference: <https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/concept/alert-priority.html>

Question: 6

Which attribute is responsible for de-duplication?

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

Answer: B

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/reference/r_EMBestPractice.html

Question: 7

How would you interpret the following data in the Operational Intelligence Insights Explorer?



- A. win-ces882ierw is one of your hottest Configuration Items (CIs) that is currently experiencing a high probability of anomalies and should be checked immediately
- B. win-ces882ierw is one of your hottest Configuration Items (CIs), but is currently experiencing a low probability of anomalies

C. win-ces882ierw is one of your customized list of monitored Configuration Items (CIs) that is currently experiencing a high probability of anomalies and should be checked immediately D. win-ces882ierw is one of your customized list of monitored Configuration Items (CIs), but is currently experiencing a low probability of anomalies

Answer: D

Question: 8

What is the default collection/polling interval applied to all event connectors?

- A. Every 120 seconds
- B. Every 5 seconds
- C. Every 40 seconds
- D. Every 60 seconds
- E. Every 10 seconds

Answer: E

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-servicenow-platform/page/use/collaboration/task/t_ConfigureThePollingInterval.html

Question: 9

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-operations-management/page/product/event-management/task/t_EMViewRuleApply.html

Question: 10

What feature would you use to trigger a workflow or automatically generate tasks via templates?

- A. Event rules
- B. Task rules
- C. Alert management rules
- D. Alert correlation rules

Answer: A

Explanation:

Reference: <https://docs.servicenow.com/bundle/kingston-it-operations-management/page/product/event-management/task/create-task-template-from-existing-alert.html>

Question: 11

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-operations-management/page/product/event-management/task/t_EMSetTheAlertActiveInterval.html

Question: 12

What Event Management module allows for configuration of automatic task creation?

- A. Alert management rules
- B. Task rules
- C. Event rules
- D. Alert correlation rules

Answer: A

Explanation:

Reference: <https://docs.servicenow.com/bundle/newyork-it-operations-management/page/product/event-management/task/create-alert-management-rule.html>

Question: 13

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

Explanation:

Reference: <https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/task/configure-midwebserver-extension-metric-data.html>

Question: 14

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

Question: 15

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

Explanation:

Reference: <https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/concept/alert-priority.html>

Question: 16

Which are recommended best practices for Event Management? (Choose three.)

- A. Filter out events on ServiceNow Instance for easier consolidation and aggregation.
- B. Promote all events to alerts during initial implementation until you fully understand which should be ignored.
- C. Filter out events at source rather than in the ServiceNow instance.
- D. Base-line "normal-state" events to filter out background noise.
- E. Ignore all non-critical events during initial implementation to streamline processing; add alerts over time as time and resources allow.

Answer: BCE

Question: 17

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

Question: 18

A support agent resolves an incident associated with an alert, but the alert does not automatically close even though the `evt_mgmt.incident_closes_alert` property is set appropriately to close the alert.

What is the most likely cause of this issue?

- A. The support agent does not have the `evt_mgmt_user` role.
- B. The support agent only has the `evt_mgmt_admin` role.
- C. The support agent has the `evt_mgmt_operator` role, but not the `evt_mgmt_user` role.
- D. The support agent has the `evt_mgmt_user` role, but not the `evt_mgmt_operator` role.

Answer: A

Explanation:

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

Question: 19

What are the two most accurate statements regarding the ServiceNow CMDB (configuration management database) and CIs (configuration items)?

- A. The CMDB is a series of tables that contain only key hardware components located in critical paths within your platform that must be managed.
- B. The CMDB is a dynamic list that tracks both the CIs within your platform and the relationship between those items.
- C. All CIs stored in the CMDB must have an assigned IP address within your infrastructure.
- D. A CI is any component within your infrastructure that needs to be managed in order to deliver

Services.

Answer: BD

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-servicenow-platform/page/product/configuration-management/concept/c_CIRelationships.html

Question: 20

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

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-servicenow-platform/page/product/configuration-management/concept/c_CMDBClassifications.html

Question: 21

A four node cluster makes up the components (CIs) of a Business Service. The impact influence for the cluster is set to 60%.

How many members of the cluster must be in a Critical state in order for the Business Service to display as Critical in the Impact Tree?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C


Question: 22

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?


The screenshot shows the configuration for an alert promotion rule named "MetricOne". The rule is active and has a minimal score of 9.5. The promotion type is "MetricName" and the source is "MetricOne". The metric name is "CPU_Util".

Name	MetricOne	Active	<input checked="" type="checkbox"/>
Promotion Type	MetricName	Minimal Score	9.5
Source	MetricOne		
MetricName	CPU_Util		

A)

Description	CPU Util for C:\ value: 24.000000 exceeds the threshold range:[0.000000]-[36.869789] and has anomaly score: 9.047626
Message key	sa_920bc51e186113007f44b91107733cba-dcdb055718e553007f44b91107733c05
Additional Information	<pre>{ "anomaly_score": "9.047625541687012", "metric_lower_bound": "0.0", "metric_upper_bound": "36.869789123535156", "metric_value": "24.0", "promotion_parameter": "", "source_metric_type": "CPU_Util" }</pre> 

B)

Description	CPU_Util for C:\ value: 100.000000 exceeds the threshold range:[0.000000]-[35.410248] and has anomaly score: 9.985986
Message key	sa_e1efd05c985213007f44ad63cf1b07fb-fd174d9498d213007f44ad63cf1b07f7
Additional Information	<pre>{ "anomaly_score": "9.98598575592041", "metric_lower_bound": "0.0", "metric_upper_bound": "35.410247802734375", "metric_value": "100.0", "promotion_parameter": "", "source_metric_type": "CPU_Util" }</pre> 

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

Explanation:

Reference <https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/task/create-alert-promotion-rule.html>

Question: 23

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

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/reference/r_EMHowAlertsBindCI.html

Question: 24

The MID Server requires an outbound connection on which port?

- A. 445
- B. 161
- C. 443
- D. 143

Answer: C

Explanation:

Reference: https://docs.servicenow.com/bundle/london-servicenow-platform/page/product/mid-server/concept/c_MIDServerConnectionPrerequisites.html

Question: 25

If more than one event rule applies to a particular event or metric, which of the event rules will run

based upon the Order of execution number?

- A. Only the event rule with the highest Order of execution number will run.
- B. Only the event rule with the lowest Order of execution number will run.
- C. All event rules will run, from the lowest to the highest Order of execution numbers.
- D. All event rules will run, from the highest to the lowest Order of execution numbers.

Answer: D

Explanation:

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

Question: 26

When creating event rules, is it best practice to create:

- A. Two rules for every event
- B. As many rules as possible
- C. As few rules as possible
- D. One rule for every event

Answer: D

Explanation:

Reference: <https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/concept/create-event-rules.html>

Question: 27

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

Explanation:

Reference: https://docs.servicenow.com/bundle/orlando-it-operations-management/page/product/event-management/concept/c_EMIntegrateRequirementEvent.html

Question: 28

What two key steps must be performed after creating a new connector instance? (Choose two.)

- A. Assign a MID Server to the connector
- B. Enter credentials for the connector
- C. Debug the connector
- D. Test the connector
- E. Activate the connector

Answer: DE

Explanation:

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

Question: 29

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

Question: 30

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 tab
- B. Event rule info tab
- C. CI Binding tab
- D. Event Filter tab

Answer: B

Question: 31

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

Question: 32

How often do baseline event connectors retrieve events?

- A. Every 30 seconds
- B. Every 2 minutes
- C. Every 10 minutes
- D. Every 1 minute
- E. Every 5 minutes

Answer: B

Question: 33

Which attribute correlates multiple events to one alert?

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

Answer: B

Question: 34

What attribute is used to consolidate events into a single alert?

- A. Event Rules
- B. Message Key
- C. Alert Priority
- D. Severity

Answer: B

Question: 35

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

Question: 36

In default configuration using baseline connectors, how often is event data collected from event sources?

- A. Once every minute
- B. Every 2 minutes
- C. Twice every minute
- D. Every 5 minutes

Answer: B

Question: 37

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

Question: 38

What is one of the main benefits of using Event Management and Operational Intelligence?

- A. To improve service availability by helping IT staff pinpoint service issue causes and evaluate the impact of planned changes.
- B. To increase service agility and produce fast, predictable results by automating manual, routine, error-prone tasks.
- C. To rapidly configure and launch secure, agentless discovery of hardware and software resources and their relationships.
- D. To proactively warn against possible service outages using a range of advanced predictive machine learning methods.

Answer: D

Question: 39

MID Servers provide important functions in your ITOM Health deployment. What does MID stand for?

- A. Management, Instrumentation, and Discovery
- B. Messaging, Integration, and Data
- C. Monitoring, Insight, and Domain
- D. Maintenance, Information, and Distribution

Answer: A

Question:

40

HOTSPOT

In what sequence are events processed?

Does the event Source match the event rule?



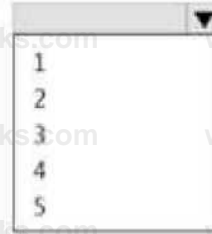
A dropdown menu with a downward arrow icon on the right. The menu is open, showing a list of five options: 1, 2, 3, 4, and 5.

Does the event message key match an existing alert?



A dropdown menu with a downward arrow icon on the right. The menu is open, showing a list of five options: 1, 2, 3, 4, and 5.

Is the event filtered out?



A dropdown menu with a downward arrow icon on the right. The menu is open, showing a list of five options: 1, 2, 3, 4, and 5.

Is a severity defined?

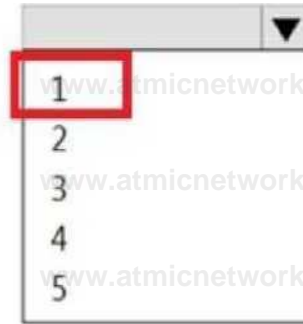


A dropdown menu with a downward arrow icon on the right. The menu is open, showing a list of five options: 1, 2, 3, 4, and 5.

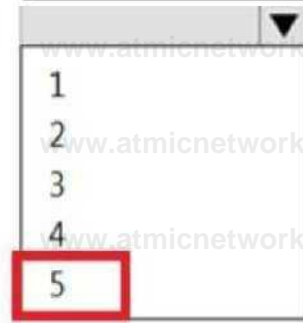
Answer:

Explanation:

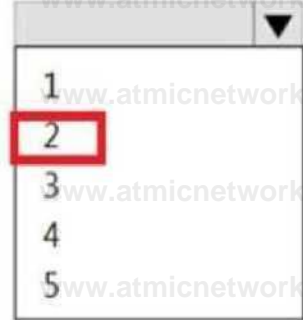
Does the event Source match the event rule?



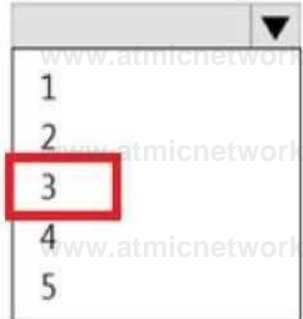
Does the event message key match an existing alert?



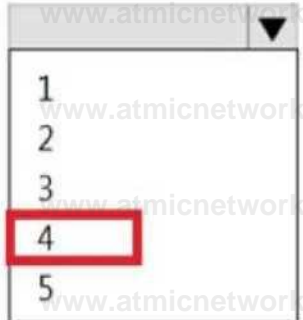
Is the event filtered out?



Is there a matching threshold?



Is a severity defined?



Question: 41

Which is not a valid method for accessing alert intelligence?

- A. In the right-click menu of an alert list, select Open in Workspace
- B. By appending/workspace to your instance URL
- C. The application navigator Alerts Console menu item

- D. The application navigator Alert Intelligence menu item
- E. Within an open alert record, click the Open in Workspace button
- F. Select the Lists tab in operator workspace

Answer: C

Question: 42

To determine the top incidents for the CI associated with an alert, where is the best place to look?

- A. Alert Insights
- B. Incident List View
- C. CMDB Health Dashboard
- D. Event Management Overview page

Answer: A

Question: 43

Agent Client Collector is built on what framework that enables you to adopt and extend monitoring checks from the community?

- A. Icinga
- B. Sensu
- C. SolarWinds
- D. Nagios
- E. Zabbix

Answer: B

Question: 44

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

Question: 45

Applying recommended Event Management best practice guidelines, which of the following events should generate an alert?

- A. Every event should generate an alert so you have the opportunity to resolve them all.
- B. Only events that necessitate action should generate an alert.
- C. Only the most critical events on every CI in the CMDB should generate an alert.
- D. Every event on every critical CI in the CMDB should generate an alert.

Answer: B

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

Question: 47

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: A, C

Question: 48

What event value will auto close an alert?

- A. Severity of -1/OK
- B. Type of Clear
- C. Resolution State of Closing
- D. Resolution State of Clear
- E. Severity of 0/Clear

Answer: C

Question: 49

Given the following Impact settings and Alerts in a three node cluster that makes up the components of a Business Service, what is the overall service health of this Business Service?

The screenshot shows a monitoring interface with three Tomcat nodes: Tomcat on win-fmsl33r70..., Tomcat on win-ub8vd8pih..., and Tomcat on win-k8739n22... The interface includes a table for impact settings and a sidebar with metadata.

Name	Impact On	Influence	Influence Units	Critical	Major	Minor	Warning
Application Cluster Member	Business Service	70	Percent	Red	Orange	Yellow	Blue
Application Impact	Business Service	100	Percent	Red	Orange	Yellow	Blue

Metadata: 2017-05-26 13:00:29, Name: http-in 198.51.100.167, updated: 2017-08-01 02:07:00

- A. Critical
- B. Error
- C. Major
- D. Minor
- E. Warning
- F. Clear

Answer: F

Question: 50

What does Operational Intelligence proactively identify before they cause service outages?

- A. Missing CMDB data
- B. Defects
- C. Alert correlations
- D. Orphaned CIs
- E. Anomalies

Answer: E

Question: 51

What is the function of the External Communication Channel (ECC) Queue? (Choose three.)

- A. It is a connection point between a ServiceNow instance and the MID Server.
- B. It contains probe records to be executed on the customer's network.
- C. It holds jobs that the MID Server needs to perform.
- D. It is a connection point between a hardware CI on a customer's network and the MID Server.
- E. It contains records of CIs that the ServiceNow admin has submitted for entry into the CMDB.

Answer: A, B, E

Question: 52

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

Question: 53

What is the recommended approach to normalizing data from a source system to the default values in Event Management?

- A. Event field mapping
- B. Transform maps
- C. Alert management rules
- D. Business rules

Answer: D

Question: 54

You have an event that needs to be bound to a non-host CI.
Which attribute needs to be removed from the Transform and Compose tab?

- A. Source Instance
- B. Metric Name
- C. Node
- D. Resource

Answer: C

Question: 55

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

Question: 56

Alerts are processed using which of the following? (Choose three.)

- A. Alert management rules
- B. Event action rules
- C. Event rules
- D. Scheduled jobs
- E. Java and Groovy scripts

Answer: A, C, D

Question: 57

The individual commands that the Agent Client Collector executes on the host are known as what? (Choose three.)

- A. Events
- B. Checks
- C. Parameters
- D. Policies
- E. Metrics
- F. Scripts

Answer: A, B, E

Question: 58

What is Event Management licensing based on?

- A. The number of unique nodes that can send events to the instance
- B. The number of connectors and listeners it will collect data from
- C. The number of connectors it will collect data from
- D. The number of CIs in the CMDB that it will be monitoring

Answer: D

Question: 59

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

Question: 60

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

Question: 61

What are the server requirements to allow Operational Intelligence to successfully collect operational metric data via a push?

- A. This requires a minimum of three MID Servers - two for Event Management and one additional MID Server dedicated for use by Operational Intelligence (OI).
- B. This requires a MID Web Server in addition to the MID Server.
- C. Nothing additional is required; this is handled by the MID Server.
- D. This requires a minimum of two MID Servers - one for Event Management and one additional MID Server dedicated for use by Operational Intelligence (OI).

Answer: B

Question: 62

What would be an appropriate use case for having to write JavaScript in Event Management?

- A. To change the value of the message key
- B. To create a custom action within a subflow
- C. To parse a node name out of your raw event data in an event rule
- D. To automatically create an incident

Answer: B

Question: 63

A dynamic grouping of CIs based upon common criteria (filtered CI classes) that can be visualized in operator

workspace is called?

- A. A business service
- B. A technical service
- C. An application service
- D. A manual service
- E. A scoped service

Answer: C

Question: 64

During CI binding, CI matching is done using which two fields? (Choose two.)

- A. Message Key
- B. Additional Information
- C. Source
- D. Node

Answer: B, D

Question: 65

What three areas of data quality does the CMDB Health Dashboard focus on? (Choose three.)

- A. Correctness
- B. Completeness
- C. Configuration
- D. Conciseness
- E. Conformity
- F. Compliance

Answer: A, B, F

Question: 66

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

Question: 67

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

Question: 68

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

Question: 69

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

Question: 70

Which is an invalid state for an alert?

- A. Flapping
- B. Closed
- C. Reopen
- D. Processed

Answer: D

Question: 71

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

Question: 72

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

Question: 73

What ServiceNow feature is an aid to rapid implementation of your Event Management and Operational Intelligence features?

- A. Deployment wizard
- B. Step-by-step guide
- C. Checklist application

D. Guided setup

Answer: C

Question: 74

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

Question: 75

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

Question: 76

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

Question: 77

The default polling time to collect events from an event source is:

- A. 5 seconds
- B. 30 seconds
- C. 60 seconds
- D. 120 seconds

Answer: D

Question: 78

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: A, C

Question: 79

The Event Management operator workspace can display all of the following except?

- A. Alert groups
- B. Manual application services
- C. Discovered application services from Service Mapping
- D. Correlation groups
- E. Technical services

Answer: B

Question: 80

Within an event rule, how would you parse a nodename out of your raw event data?

- A. JavaScript
- B. Groovy script
- C. PowerShell script
- D. Regex statement

Answer: A

Question: 81

If events are not matching to alerts as you would like, what field should be changed?

- A. Resource
- B. Message Key
- C. Node
- D. Metric Name

Answer: D

Question: 82

If the Message Key is not populated, the default value is created from which fields?

- A. Source, type, node, resource, and metric name
- B. Source, source instance, node, and resource
- C. Source, type, node, and metric name
- D. Source, source instance, node, and type
- E. Source, type, node, resource, and time of event

Answer: A

Question: 83

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

Question: 84

When performing CI Binding, what fields does Event Management match to the Node?

- A. CI Name, DNS, IP, MAC Address
- B. System class name, FQDN, IP or MAC address
- C. CI name, FQDN, SSH public host keys
- D. CI Name, FQDN, IP, MAC Address

Answer: C

Question: 85

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

Number	Group	Severity	Priority
Alert0010003		Major	7306
Alert0010042		Critical	400
Alert0010075		Critical	400
Alert0010074		Major	300

- A. Alert0010042
- B. Alert0010003
- C. Alert0010075
- D. Alert0010074

Answer: B

Question: 86

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

Question: 87

By default, when are idle alerts are closed?

- A. After 7 days
- B. After 14 days
- C. After 30 days
- D. Never

Answer: A

Question: 88

In your environment, no alert CMDB, automated, or text based grouping is occurring. What is most likely the problem?

- A. No correlation rules have been defined
- B. No event management rules have been defined
- C. Application services are not operational
- D. No CMDB is configured
- E. The alert correlation property that enables grouping is set to false

Answer: D

Question: 89

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

Question: 90

In order for SNMP trap notifications to appear in ServiceNow as events, what option must be enabled in the required MID server?

- A. MID SNMP trap listener
- B. SNMP event manager module for MID
- C. Event collector MID server extension
- D. SNMP agent for MID

Answer: A

Question: 91

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

Question: 92

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

Question: 93

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

Question: 94

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

Question: 95

What does Now Assist for ITOM use to provide alert analysis?

- A. Third-party monitoring tool connectors with out-of-box alert rules
- B. GenAI and the ServiceNow large language model
- C. Basic keyword matching in the alert description and tags
- D. The unified service map and link view topology

Answer: B

Question: 96

If a Message Key is not provided, which fields are concatenated to make our own?

- A. Source, Type, Node, Resource, Metric Name
- B. Source, DNS, Node, Additional info, Metric Name
- C. Source, Type, DNS, Additional info, Metric Name
- D. Source, Source Instance, Node, Type, Resource

Answer: A

Question: 97

Within the ServiceNow IT Operations Management solution set, which statement most accurately describes what Event Management is?

- A. The process responsible for defining, analyzing, planning, measuring, and improving all aspects of the availability of IT services
- B. The process responsible for ensuring the capacity of IT Services and IT infrastructure is able to deliver agreed upon service level targets in a cost-effective manner
- C. The process responsible for recovery action and planning through machine learning
- D. The process responsible for monitoring all abnormal occurrences throughout the IT infrastructure, allowing for normal operations, and detecting and escalating exception conditions

Answer: D

Question: 98

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

Question: 99

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

Question: 100

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: B, C

Question: 101

Where are approval requests for execution of alert remediation tasks configured?

- A. In the Flow Designer remediation subflow
- B. In Service Operations Workspace
- C. In the alert management rule's approvals related list
- D. In the alert management rule's playbook

Answer: C

Question: 102

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 Policies, Log Monitoring
- C. Event Management, Metric Intelligence, Log Monitoring
- D. Event Connectors, Metric Intelligence, Log Data inputs

Answer: D

Question: 103

Service Operations Workspace integrations Launchpad capabilities include management of which key components?

Choose 3 answers

- A. event connectors
- B. Alert management rules
- C. Metric policies
- D. Log data inputs

Answer: A, B, C

Question: 104

What applications are included in the ITOM Health solution?

Choose 3 answers

- A. Cloud Provisioning and Governance
- B. Health Log Analytics
- C. Agent Client Collector
- D. Discovery
- E. Service Mapping
- F. Event Management

Answer: B, C, F

Question: 105

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

Question: 106

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 Management dashboard
- D. State management logs module

Answer: B

Question: 107

What determines if an alert management rule's actions apply to an alert?

- A. The alert's bound configuration item
- B. The alert management rule's filter
- C. The alert management rule's field mapping
- D. The message key

Answer: B

Question: 108

If more than one alert management rule applies to a particular alert which of the rules will run based upon the Order of execution field?

- A. All alert management rule will run, from the highest to the lowest Order of execution numbers.
- B. Only the alert management rule with the highest Order of execution number will run.
- C. All alert management rule will run, from the lowest to the highest Order of execution numbers.
- D. Only the alert management rule with the lowest Order of execution number will run.

Answer: B

Question: 109

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: A, B, C, D

Question: 110

When setting up a monitoring connector definition PULL the M.O 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 in the MID Server system
- E. Internal IP address and port for communication with the MID Server system
- F. Access credentials to the monitoring system

Answer: A, B, C, F

Question: 111

In Service Operations Workspace, what tool shows relationships between configuration items and alerts with real-time updates and detailed impact paths?

- A. CMDB identification and reconciliation engine (IRE)
- B. Unified service map
- C. Dependency view map
- D. CMDB class manager

Answer: B

Question: 112

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

Question: 113

What ServiceNow feature would you configure to process incoming email to create events?

- A. Event field mapping
- B. Event processing jobs
- C. Transforms
- D. Event Filler
- E. Inbound actions

Answer: E

Question: 114

Out-of-the-box, how often do tie events get processed in ServiceNow?

- A. Every 5 seconds
- B. Depends on connectors Used
- C. Every minute via a scheduled job
- D. As soon as the event record is inserted via a business rule

Answer: C

Question: 115

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