DUMPSBOSS.

IBM Cloud Pak for Watson AIOps v3.2 Administrator

IBM C1000-143

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

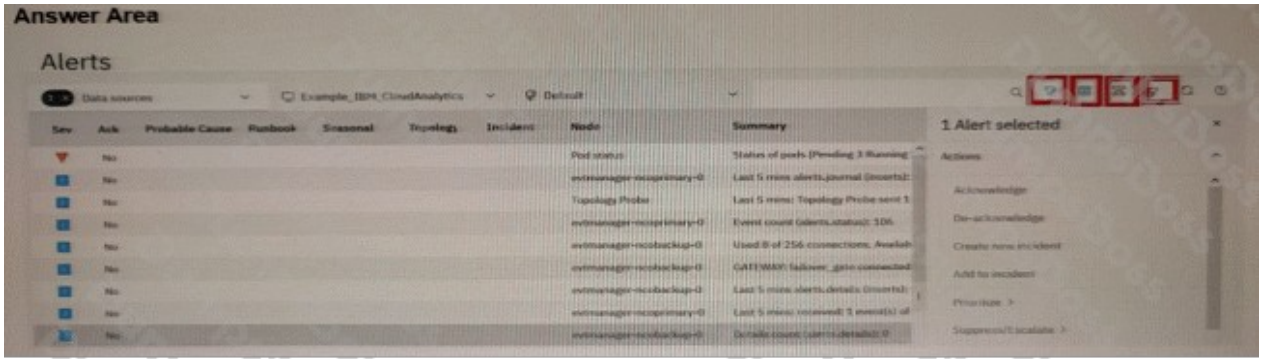
Topic Break Down

Topic	No. of Questions
Topic 1, Planning	11
Topic 2, Installation	12
Topic 3, Configuration	41
Topic 4, Administration	29
Total	93

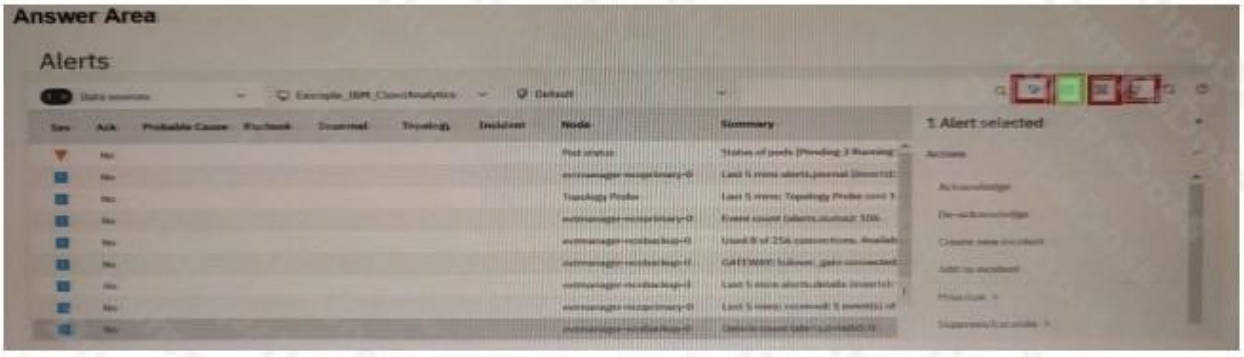
QUESTION NO: 1 - (HOTSPOT)

The following diagram shows the Alert Viewer of Event Manager. An administrator wants to define the Alert View Selection for a group of users so that only certain alert fields are shown.

Click the icon needs to be selected by the administrator



ANSWER:



Explanation:

The correct control is the Alert View Selection icon because an alert view determines the presentation of alerts in the Event Manager Alert Viewer, including which alert fields are visible to the users of that view. This is distinct from merely narrowing the currently displayed alerts. An administrator uses Alert View Selection to choose the view configuration that governs the table's displayed field set, allowing a group to work with the fields that are relevant to its operational responsibilities.

In the image, this is the second toolbar icon from the left within the highlighted group of four controls near the upper-right side of the alert table. It is directly to the right of the funnel-shaped filter icon. Selecting it is the appropriate starting point for defining the alert-view field presentation for the intended users. The resulting view configuration can then be associated with the relevant user group so that the Alert Viewer consistently presents the selected alert columns and information for that group.

IBM documentation describes Event Manager alert management and the Alert Viewer as the interface for viewing and working with alerts in Cloud Pak for Watson AIOps. The product documentation is available at IBM Cloud Pak for Watson AIOps 3.2 documentation, and IBM's Event Manager overview is available at Event Manager overview. These resources provide the administrative context for controlling how alert data is presented to users.

QUESTION NO: 2

Which field in the Netcool/OMNIbus `alerts.status` table indicates the seriousness of an event?

A. Severity

B. NodeAlias

C. Manager

D. Identifier

ANSWER: A

Explanation:

Severity indicates the seriousness of an event in the ObjectServer. Event sources assign a severity value that can be used in event lists, filters, automations, and escalation procedures. Operators use severity with other event context, such as the affected node, summary, occurrence count, and event age, to prioritize investigation. Severity does not identify the originating probe or uniquely identify the event. IBM documents Severity and other standard event columns in the alerts.status table reference.

QUESTION NO: 3

Which two resource types can be specified as container resource requests and limits in an OpenShift pod specification?

A. CPU

B. Memory

C. Persistent volume

D. Route

E. Namespace

ANSWER: A B

Explanation:

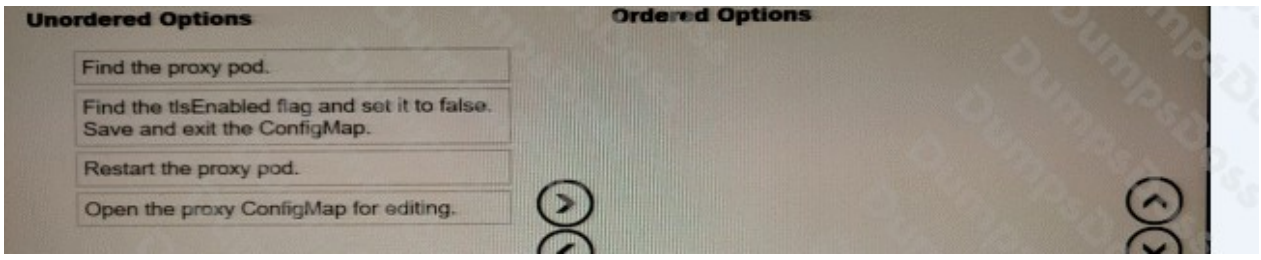
CPU and **Memory** are correct. Resource requests specify the minimum amount of CPU or memory that the scheduler considers when placing a pod on a node. Resource limits define the maximum resource usage that a container is allowed to consume. Appropriate requests and limits are important for Cloud Pak for Watson AIOps workloads because they help OpenShift schedule workloads predictably and protect the cluster from uncontrolled resource consumption.

Persistent storage and network bandwidth can be managed through other OpenShift and Kubernetes mechanisms, but they are not the standard CPU and memory resource request and limit values configured for a container. See the Kubernetes documentation on managing resources for containers.

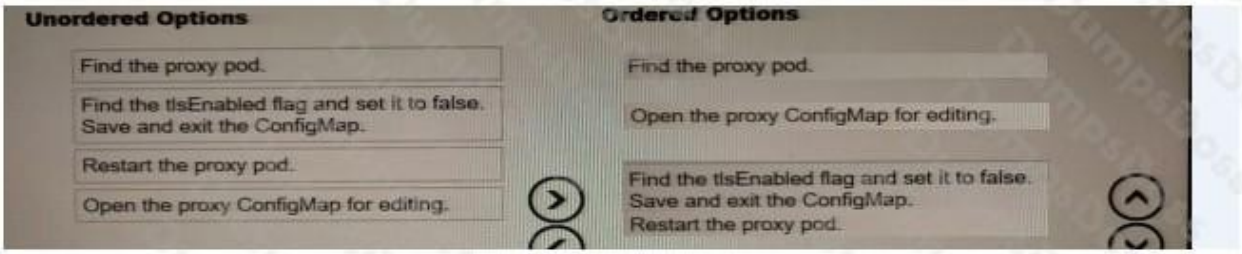
QUESTION NO: 4 - (DRAG DROP)

Select all that apply

What is the correct sequence of steps to disable TLS in Event Manager?



ANSWER:



Explanation:

Disabling TLS for the Event Manager proxy follows a configuration-change workflow: first identify the running proxy workload, then update the configuration used by that workload, and finally restart the workload so it reads the new setting. Start by finding the proxy pod. This establishes the specific Event Manager proxy component being administered and provides the context needed to work with its configuration safely. Next, open the proxy ConfigMap for editing. A ConfigMap is the Kubernetes resource used to externalize non-secret configuration data for workloads, as described in the Kubernetes ConfigMap documentation.

Within that ConfigMap, locate the `tlsEnabled` setting, change its value to `false`, then save and exit the editor. This is the actual configuration action that disables TLS for the proxy. Saving the ConfigMap persists the revised configuration in the cluster, but an already-running pod normally retains configuration loaded when it started. The proxy pod must therefore be restarted after the ConfigMap update. Restarting causes the proxy process to start again and consume the revised configuration, making the TLS setting effective. Kubernetes documents that mounted ConfigMap data can be refreshed eventually, but applications may need a restart or reload to use configuration values that were read at startup; see Updating Configuration via a ConfigMap.

The correct operational sequence is consequently discovery of the proxy pod, editing of its proxy configuration, changing and saving the TLS flag, and restarting that proxy pod. This ordering ensures the correct component is targeted and that the saved configuration change is applied to the active Event Manager proxy.

QUESTION NO: 5 - (SIMULATION)

Select all that apply

What is the correct sequence of steps to disable TLS in Event Manager?

ANSWER: See the explanation for the answer

Explanation:

Correct sequence:

1. Edit the Event Manager proxy ConfigMap:

   ```
   kubectl edit configmap <release_name>-proxy-config -n <namespace>
   ```

2. Locate the TLS setting and change it to:

   ```
   tlsEnabled: "false"
   ```

   Save and exit the editor.

3. Identify the proxy pod:

   ```
   kubectl get pods --namespace <namespace> | grep proxy
   ```

4. Restart the proxy by deleting its pod. Kubernetes/OpenShift recreates it using the updated ConfigMap:

   ```
   kubectl delete pod <proxy-pod> -n <namespace>
   ```

Select the steps that edit `<release_name>-proxy-config`, set `tlsEnabled` to `false`, find the proxy pod, and delete/restart that proxy pod.

The proxy must be restarted because changing the ConfigMap alone does not apply the updated TLS setting to the already-running proxy container.

QUESTION NO: 6

Which two practices help secure credentials used by a Cloud Pak for Watson AIOps integration with an external data source?

A. Store credentials in an OpenShift Secret

B. Grant the integration account only the required permissions

C. Store passwords in a ConfigMap for easy review

D. Use the cluster administrator account for all integrations

E. Include credentials in the integration name

ANSWER: A B

Explanation:

Store credentials in an OpenShift Secret and **grant the integration account only the required permissions** are correct. OpenShift Secrets are designed to store sensitive configuration such as usernames, passwords, tokens, and certificates separately from application configuration. Referencing a Secret also avoids placing credentials directly in resource definitions, scripts, or ConfigMaps.

An external integration account should use the principle of least privilege. For example, an account used to collect event, log, topology, or ticket data should have only the read or API permissions required for its configured data collection tasks. Administrator-level access should not be assigned unless it is specifically required. See the Kubernetes documentation on Secrets and the IBM Cloud Pak for Watson AIOps 3.2 documentation.

QUESTION NO: 7

In Event Manager, which event groupings usually occur within a short time of each other?

A. Scope-based

B. Seasonal

C. Temporal

D. Topology

ANSWER: C

Explanation:

Temporal is correct because temporal event grouping identifies events that occur close together in time and associates them into a single group. In an operational environment, a fault or change can generate multiple related alerts across monitored resources within seconds or minutes. Grouping these near-simultaneous events helps operators view the related activity as one operational situation rather than investigating a stream of isolated alerts. This reduces event noise and provides a clearer starting point for incident triage and root-cause investigation. The grouping is based on the timing relationship between events, using a configured time window to determine whether incoming events should be associated with an existing group. IBM Cloud Pak for Watson AIOps Event Manager supports grouping mechanisms to organize correlated event activity and make event handling more efficient. See the IBM Cloud Pak for Watson AIOps 3.2 documentation and the IBM event grouping overview for IBM guidance on grouping related events.

QUESTION NO: 8

What are two of the automation types available in the Runbook Automation section of the Event Manager UI?

A. Netcool/OMNIbus ObjectServer trigger

B. Runbook

C. Script

D. Webhook

E. Ansible Tower

ANSWER: A B

Explanation:

Netcool/OMNIbus ObjectServer trigger and **Runbook** are automation types available from the Event Manager Runbook Automation area. A runbook provides documented, repeatable operational instructions that an operator can open and follow when investigating or resolving an event. Associating a runbook with event conditions helps ensure that responders use an approved remediation procedure and reduces time spent locating the appropriate operational guidance.

A Netcool/OMNIbus ObjectServer trigger is an ObjectServer-side automation mechanism. ObjectServer triggers execute SQL-based actions when specified database events occur, enabling controlled automated handling of event data, such as updating fields or initiating actions based on event state. In Event Manager, this automation type can be managed in the Runbook Automation context so that event-processing automation and operator remediation procedures are available from the relevant operational interface.

These types reflect the Event Manager capabilities provided with the Netcool/OMNIbus integration in Cloud Pak for Watson AIOps. For IBM's Event Manager documentation and the product documentation set for this release, see IBM Cloud Pak for Watson AIOps 3.2 documentation and IBM Netcool Operations Insight runbook automation documentation.

QUESTION NO: 9

What is an advantage of using tags in Topology Manager?

A. You can get all neighbors of the selected resource by adding a Filter tag,

B. It allows the resources used by a dynamic template to be confined to a specified set of resources.

C. They are used to identify changes in the time line.

D. It allows connecting different resource groups

ANSWER: B

Explanation:

It allows the resources used by a dynamic template to be confined to a specified set of resources. Tags are metadata labels associated with topology resources, and they can be used as matching criteria when defining a dynamic topology template. This gives an administrator a controlled way to limit the template's scope to resources that share a particular operational, organizational, application, or environment label. For example, a template can be targeted only at resources tagged for a particular application or deployment environment, rather than applying its grouping and relationship logic across every resource discovered by Topology Manager. This scoping is valuable in large or shared topology deployments because it makes dynamic templates more precise, manageable, and reusable while helping ensure that the resulting topology views reflect the intended service domain. IBM's topology documentation describes dynamic templates as rules for automatically creating resource groups and indicates that resource properties, including tags, can be used to define the resources to which a template applies. See the IBM documentation for defining dynamic templates and the Cloud Pak for Watson AIOps 3.2 documentation.