Question 1

The AppDynamics Controller is instrumented by an internal, out-of-the-box, AppDynamics Java agent. Which account and user name are used to connect to the Controller to view the information provided by the internal AppDynamics agent?

Options:

A- The account is 'root' and the user is 'admin'.

B- The account is 'customer!' and the user is 'root'.

C- The account is 'system' and the user is 'root.

D- The account is internal' and the user is 'admin'.

Answer:

C

Explanation:

The AppDynamics Controller is instrumented by an internal, out-of-the-box, AppDynamics Java agent that monitors the performance and health of the Controller itself1.To access the information provided by the internal agent, you need to log in to the Controller UI with the following credentials2:

Account = system

Username = root

Password = <root_user_password>

The system account is a special account that is used only for internal monitoring and troubleshooting purposes.It is not visible in the normal Controller UI and requires a special URL to access it2.The root user is the default administrator user for the system account and has the same password as the admin user for the customer1 account3.Reference:Controller Self-Monitoring,Monitoring a Controller Using the Internal Monitoring Agent,Controller Accounts

Question 2

Question Type: **MultipleChoice**

Which two preparatory tasks are required prior to installing an AppDynamics Controller on Linux? (Choose two.)

Options:

A- Install JRE.

B- Ensure that MySQL port (3388) is opened.

C- Install SSH.

D- Install libaio.

E- Verify that sufficient temporary (tmp) space is available (at least 1 GB).

Answer:

D, E

Explanation:

Before installing an AppDynamics Controller on Linux, you need to perform some preparatory tasks to ensure the system meets the requirements and the installation runs smoothly. Two of these tasks are:

Install libaio on the host machine if it does not already have it installed. This library facilitates asynchronous I/O operations on the system, which are required by the Controller. You can use the package manager of your Linux distribution to install libaio, such as yum or apt-get.For example, on CentOS, you can runyum install libaio1.

Verify that you have enough temporary (tmp) space available on the system, at least 1 GB. The Controller installation uses the tmp space to extract and install the software components.You can check the tmp space by runningdf -h /tmp2.If the tmp space is insufficient, you can either free up some space by deleting unnecessary files, or specify a different temporary directory for the installation by passing

Question 3

Question Type: **MultipleChoice**

Which AppDynamics Controller port(s) does the EUM Server require access to in a configuration where the EUM Server and Controller are on separate hosts (split-host configuration)?

Options:

A- dedicated EUM HTTP(s) ports

B- GlassFish administration port

C- Controller database and HTTP(s) ports

D- Controller primary HTTP{s) port

Answer:

D

Explanation:

In a split-host configuration, where the EUM Server and Controller are on separate hosts, the EUM Server requires access to the Controller primary HTTP(s) port. This is because the EUM Server needs to communicate with the Controller API server to send data and receive configuration information.The default primary HTTP port for the Controller is 8090 and the default primary HTTPS port is 81811.The dedicated EUM HTTP(s) ports are used by the EUM agents to send data to the EUM Server, not by the EUM Server to access the Controller2.The GlassFish administration port is used to access the Controller Admin Console, not by the EUM Server3.The Controller database port is used by the Controller to connect to the MySQL database, not by the EUM Server4.Reference:Controller Port Settings,Configure the Port for the EUM Agent,Access the Administration Console,Controller System Requirements

Question 4

Question Type: **MultipleChoice**

What are two valid reasons for using the REST API to retrieve health rule violations? (Choose two.)

Options:

A- For updating an AppDynamics dashboard

B- For determining which actions have been executed

C- When searching for historical events

D- For sending emails

E- When pushing events to the Event Management System is NOT possible

Answer:

B, C

Explanation:

According to the Cisco AppDynamics Professional Implementer (CAPI) documents, the REST API for health rule violations allows you to retrieve information about the health rule violations that occurred in a specified time range for a given application1. You can use the REST API for health rule violations for the following valid reasons:

For determining which actions have been executed (B): The REST API response includes the details of the actions that were triggered by the health rule violation, such as email, SMS, HTTP request, or custom action1. You can use this information to verify if the actions were executed successfully, or to troubleshoot any issues with the action execution.

When searching for historical events : The REST API allows you to specify a custom time range for retrieving the health rule violations, such as BEFORE_TIME, AFTER_TIME, BETWEEN_TIMES, or BEFORE_NOW1. You can use this feature to search for historical

events that occurred in the past, or to analyze the trends and patterns of the health rule violations over time.

The incorrect options are:

For updating an AppDynamics dashboard (A): This is not a valid reason for using the REST API for health rule violations, because the AppDynamics dashboards already display the health rule violations that occurred in the selected time frame, along with the severity, status, affected entities, and actions2. You do not need to use the REST API to update the dashboard, as the dashboard is automatically refreshed with the latest data from the Controller.

For sending emails (D): This is not a valid reason for using the REST API for health rule violations, because the REST API does not send emails directly. The REST API only returns the information about the health rule violations, and the actions that were triggered by them.If you want to send emails based on the health rule violations, you need to configure an email action in the health rule configuration, or use a custom action that invokes an external email service3.

When pushing events to the Event Management System is NOT possible (E): This is not a valid reason for using the REST API for health rule violations, because the REST API does not push events to the Event Management System. The REST API only returns the information about the health rule violations, and the actions that were triggered by them.If you want to push events to the Event Management System, you need to configure an HTTP request action in the health rule configuration, or use a custom action that invokes an external API3.

1: Health Rule Violations API - AppDynamics

2: Health Rule Violations - AppDynamics

3: Actions - AppDynamics

Question 5

Default configuration of the Mobile SDK enables_____and_____ . (Choose the two correct options to complete the sentence.)

Options:

A- Crash Reports

B- User Data

C- Network Requests

D- Custom Timers

E- Breadcrumbs

Answer:

A, C

Explanation:

The default configuration of the Mobile SDK enablescrash reportsandnetwork requests12.Crash reports capture and report any unhandled exceptions or signals that cause the app to terminate abnormally1.Network requests monitor the performance and errors of

Question 6

Question Type: **MultipleChoice**

Which implementation mode should be used when deploying an EUM Server with reverse proxy from a security and performance standpoint in a production environment?

Options:

A- Install the EUM Server on the same host as the Controller, behind the reverse proxy.

B- Install the EUM Server on a separate host from the Controller, in front of the reverse proxy.

C- Install the EUM Server on the same host as the Controller, in front of the reverse proxy.

D- Install the EUM Server on a separate host from the Controller, behind the reverse proxy.

Answer:

D

Explanation:

The EUM Server is the on-premises version of the EUM Cloud that receives, processes, and stores data from EUM agents. For production installation, AppDynamics recommends that the EUM Server and the Controller sit on different hosts, and the EUM Server hosts its own MySQL instance. This improves the scalability and performance of both components. Moreover, AppDynamics strongly recommends that SSL traffic from agents to the EUM Server is terminated at a reverse proxy that sits in front of the EUM Server in the network path, and forwards connections to the EUM Server using HTTP. This relieves the SSL processing load from the EUM Server, simplifies the certificate management, and enhances the security by isolating the EUM Server from the external Internet. Therefore, the best implementation mode for deploying an EUM Server with reverse proxy in a production environment is option D.Reference:EUM Server Deployment,Install a Production EUM Server,Reverse Proxy configuration for EUM, andBrowser EUM installationin the AppDynamics documentation and community.

Question 7

Question Type: **MultipleChoice**

Which type of Alert and Respond action is available only on an on-premises Controller?

Options:

A- Remediation action

B- Cloud auto-scaling

C- Diagnostic action

D- Custom action

Answer:

D

Explanation:

A custom action is a type of Alert and Respond action that allows you to integrate AppDynamics notifications with your own alerting or ticketing system. You can create a custom action by writing an executable script and an XML file that describe how to pass information from AppDynamics to your system. A custom action can be triggered by a policy based on a health rule violation or an event. A custom action is available only on an on-premises Controller, because it requires access to the Controller file system and the ability to execute scripts on the Controller host machine.For a SaaS Controller, you can use HTTP request templates instead of custom actions to integrate with external systems.Reference:Build a Custom Action,Alert and Respond,Actions,Custom Actions

Question 8

Question Type: MultipleChoice

An administrator is asked to improve the capacity of an Events Service cluster. What is the recommended way to add capacity to the cluster?

Options:

A- Add a new Events Service cluster to share the load.

B- Add nodes running on machines with identical hardware matching the existing nodes.

C- Add more storage to the master nodes of the cluster.

D- Add more storage to as many of the existing nodes as possible.

Answer:

B

Explanation:

According to the Cisco AppDynamics Professional Implementer (CAPI) documents, the recommended way to add capacity to the Events Service cluster is to add nodes running on machines with identical hardware matching the existing nodes12. This will increase the data storage, replication, and redundancy of the cluster, as well as the processing power for queries.The Events Service cluster is horizontally scalable, so nodes can be added as your data storage requirements grow32.The Events Service must run on dedicated machines with identical directory structures, user account profiles, and hardware profiles1.For heap space allocation, AppDynamics recommends allocating half of the available RAM to the Events Service process, with a minimum of 7 GB up to 31 GB1.Solid-state drives (SSD) can

significantly outperform hard disk drives (HDD), and are therefore recommended for production deployments1.

The incorrect options are:

Add a new Events Service cluster to share the load. (A) This is not recommended because it will create additional complexity and overhead for managing multiple clusters and routing data and queries to the appropriate cluster. It will also require more license units to enable analytics on multiple clusters.

Add more storage to the master nodes of the cluster. This is not recommended because it will not increase the data replication and redundancy of the cluster, nor the processing power for queries. It will also create an imbalance in the cluster, as the master nodes will have more storage than the worker nodes, which may affect the performance and stability of the cluster.

Add more storage to as many of the existing nodes as possible. (D) This is not recommended because it will not increase the data replication and redundancy of the cluster, nor the processing power for queries. It will also create an imbalance in the cluster, as some nodes will have more storage than others, which may affect the performance and stability of the cluster.

1: Cisco AppDynamics Professional Implementer (500-430)

2: Events Service Requirements - AppDynamics

3: Events Service Deployment - AppDynamics

4: Events Service Deployment - AppDynamics

Question 9

Which artifacts are needed, at minimum, to add a custom extension to a Machine Agent?

Options:

A- Directory

Jar or Script file

Monitor.xml file

B- Directory

Manitor.xml file

Custom-gxtension.xml file

C- Directory

Zip Extension

Monitor.xml file

D- Directory

Script file

Config.json file

Answer:

A

Explanation:

To add a custom extension to a Machine Agent, you need at least three artifacts: a directory, a jar or script file, and a monitor.xml file12. The directory is where you place your extension files under the <machine_agent_home>/monitors directory. The jar or script file is the executable file that collects and reports the custom metrics to the Machine Agent. The monitor.xml file is the configuration file that defines the name, frequency, and parameters of your extension.You can also optionally include other files such as libraries, configuration files, or templates for your extension12.Reference:Build a Monitoring Extension Using Scripts,Extensions and Custom Metrics

Question 10

Question Type: **MultipleChoice**

If using SSL for agent communication with an AppDynamics Controller, it is recommended that agent SSL traffic

Options:

A- is encrypted with a 64-bit encryption key

B- is decrypted and then encrypted again at the firewall

C- terminates at a reverse proxy or a load balancer in front of the Controller

D- terminates at the Controller

Answer:

C

Explanation:

AppDynamics recommends that you terminate SSL connections from agents at a reverse proxy or a load balancer in front of the Controller, rather than at the Controller itself. This improves the performance and scalability of the Controller by offloading the SSL processing to the proxy or load balancer. It also simplifies the configuration and management of SSL certificates and truststores. To enable this option, you need to configure the proxy or load balancer to accept SSL connections from agents and forward them to the Controller using HTTP. You also need to configure the agents to use SSL and point to the proxy or load balancer host and port. SeeEnable SSL for the Java Agentfor an example.Reference:Agent-to-Controller ConnectionsandEnable SSL and SSH for Database Agent Communicationsin the AppDynamics documentation.

Question 11

Question Type: **MultipleChoice**

What are two settings that an administrator can configure from the AppDynamics Controller Admin Console? (Choose two.)

Options:

A- Metrics baseline calculation

B- Controller log file rotation

C- Controller heap size

D- License allocation

E- Retention periods

Answer:

D, E

Explanation:

The AppDynamics Controller Admin Console lets you configure certain global settings for the Controller, such as metric retention periods, UI notification triggers, tenancy mode, and accounts in multi-tenancy mode1. Two of the settings that an administrator can configure from the AppDynamics Controller Admin Console are:

License allocation: This setting allows you to view and manage the license usage and availability for your Controller. You can see the total number of licenses, the number of licenses in use, the number of licenses available, and the license expiration date for each agent

type.You can also allocate licenses to specific applications or accounts, and set license limits and alerts2.

Retention periods: This setting allows you to specify how long the Controller retains the metric data and the event data for your monitored applications. You can configure the retention periods for different types of data, such as minute-level metrics, hour-level metrics, day-level metrics, transaction snapshots, and events.You can also configure the data purge schedule and the data backup schedule3.