Free Questions for CV0-003 by certsdeals

Shared by Johnston on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A systems administrator is attempting to gather information about services and resource utilization on VMS in a cloud environment. Which of the following will BEST accomplish this objective?

Options:

A- Syslog

B- SNMP

C- CMDB

D- Service management

E- Performance monitoring

Answer:

E

Explanation:

Performance monitoring is the process of collecting and analyzing metrics related to the performance and availability of resources in a cloud environment1.Performance monitoring can help a systems administrator to gather information about services and resource utilization on VMs in a cloud environment by providing the following benefits2:

Identify and troubleshoot performance issues and bottlenecks before they affect the end users or business operations.

Optimize the resource allocation and configuration to meet the performance requirements and SLAs of the services.

Plan for future capacity and scalability needs based on the historical trends and patterns of resource utilization.

Compare the performance and costs of different cloud service providers, regions, and SKUs.

Some of the tools and services that can help with performance monitoring in a cloud environment are3:

Azure Monitor: A comprehensive service that provides a unified view of the health, performance, and availability of your Azure resources, applications, and services. Azure Monitor collects metrics, logs, and traces from various sources and provides analysis, visualization, alerting, and automation capabilities.

Azure Advisor: A personalized service that provides recommendations to optimize your Azure resources for performance, security, cost, reliability, and operational excellence. Azure Advisor analyzes your resource configuration and usage data and suggests best practices to improve your cloud environment.

Azure Application Insights: A service that monitors the performance and usage of your web applications and services. Application Insights collects telemetry data such as requests, dependencies, exceptions, page views, custom events, and metrics from your application code and provides powerful analytics, diagnostics, and alerting features.

Azure Log Analytics: A service that collects and analyzes data from various sources such as Azure Monitor, Azure services, VMs, containers, applications, and other cloud or on-premises systems. Log Analytics enables you to query, visualize, and correlate log data

using the Kusto Query Language (KQL) and create custom dashboards and reports.

Syslog is a standard protocol for sending log messages from network devices to a central server. Syslog can help with logging and auditing activities in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option A is incorrect.

SNMP (Simple Network Management Protocol) is a protocol for collecting and organizing information about managed devices on a network. SNMP can help with network management and monitoring in a cloud environment, but it does not provide comprehensive performance monitoring for VMs and services. Therefore, option B is incorrect.

CMDB (Configuration Management Database) is a database that stores information about the configuration items (CIs) in an IT environment. CMDB can help with configuration management and change management in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option C is incorrect.

Service management is a set of processes and practices that aim to deliver value to customers by providing quality services that meet their needs and expectations. Service management can help with service design, delivery, support, and improvement in a cloud environment, but it does not provide performance monitoring capabilities. Therefore, option D is incorrect.

Question 2

Question Type: **MultipleChoice**

A cloud security engineer needs to design an IDS/IPS solution for a web application in a single virtual private network. The engineer is considering implementing IPS protection for traffic coming from the internet. Which of the following should the engineer consider to meet

this requirement?

Options:

A- Configuring a web proxy server

B- Implementing load balancing using SSI- in front of web applications

C- Implementing IDS/IPS agents on each instance running in that virtual private network

D- Implementing dynamic routing

Answer:

C

Explanation:

AnIntrusion Detection System (IDS)is a software or hardware system that monitors network traffic for malicious activity and alerts the administrator of any potential threats. AnIntrusion Prevention System (IPS)is a software or hardware system that not only detects but also blocks or mitigates the malicious activity.Both IDS and IPS are essential for securing a web application in a cloud environment1.

A web proxy server is a server that acts as an intermediary between the client and the web server. It can provide caching, filtering, and authentication services, but it does not offer IDS/IPS functionality. Therefore, option A is incorrect.

Load balancing using SSI (Server Side Includes) is a technique that distributes the workload among multiple web servers by inserting dynamic content into web pages. It can improve the performance and availability of a web application, but it does not provide IDS/IPS protection. Therefore, option B is incorrect.

Implementing IDS/IPS agents on each instance running in that virtual private network is a valid solution for providing IPS protection for traffic coming from the internet. The agents can monitor and inspect the network traffic on each instance and block or report any suspicious activity to a central management console. This can prevent attacks from reaching the web application or spreading to other instances in the same network. Therefore, option C is correct.

Implementing dynamic routing is a technique that allows routers to select the best path for forwarding packets based on network conditions. It can enhance the reliability and efficiency of a network, but it does not offer IDS/IPS functionality. Therefore, option D is incorrect.

Question 3

Question Type: **MultipleChoice**

A web consultancy group currently works in an isolated development environment. The group uses this environment for the creation of the final solution, but also for showcasing it to customers, before commissioning the sites in production. Recently, customers of newly commissioned sites have reported they are not receiving the final product shown by the group, and the website is performing in unexpected ways. Which of the following additional environments should the group adopt and include in its process?

Options:

A- Provide each web consultant a local environment on their device.

B- Require each customer to have a blue-green environment.

C- Leverage a staging environment that is tightly controlled for showcasing

D- Initiate a disaster recovery environment to fail to in the event of reported issues.

Answer:

C

Explanation:

The answer is C. Leverage a staging environment that is tightly controlled for showcasing. A staging environment is a replica of the production environment that is used for testing and demonstrating the final product before deployment. A staging environment can help the web consultancy group avoid the issues reported by the customers, such as mismatched expectations and unexpected behavior, by ensuring that the product is shown in a realistic and consistent setting. A staging environment can also help the group catch and fix any bugs or errors before they affect the live site.

Some possible sources of information about web development environments are:

7 Web Development Best Practices: This page provides some general tips and best practices for web development, such as planning, accessibility, UX/UI, standards, code quality, compatibility, and security.

Web Development Best Practices (Building Real-World Cloud Apps with Azure): This page explains some specific best practices for web development in the cloud environment, such as stateless web tier, session state management, CDN caching, and async programming.

Web Development Best Practices: This page lists some resources for learning web development best practices in ASP.NET, such as async and await, building real-world cloud apps with Azure, and hands-on labs.

Question 4

Question Type: **MultipleChoice**

A systems administrator is trying to connect to a remote KVM host. The command line appears as follows:

```
serveradmin@localhost:~$ virsh remotehost
Error: daemon not running on remote host.
```

After logging in to the remote server, the administrator verifies the daemon is running. Which of the following should the administrator try NEXT?

Options:

A- Opening port 22 on the firewall

B- Running the command with elevated privileges

C- Checking if the SSH password is correct

D- Ensuring the private key was properly imported

Answer:

B

Explanation:

The answer is B. Running the command with elevated privileges. According to the web search results, the error message "End of file while reading data: sh: 1: nc: not found: Input/output error" indicates that the remote host does not have the nc (netcat) command installed or available in the PATH12. The nc command is used by libvirt to establish a connection between the client and the server. To fix this error, the administrator should install nc on the remote host or ensure that it is in the PATH. However, to do this, the administrator needs to have elevated privileges, such as sudo or root, on the remote host. Therefore, the administrator should try running the command with elevated privileges, such as sudo virsh remotehost or su -c 'virsh remotehost'. This will allow the administrator to install nc or modify the PATH on the remote host and then connect to it using libvirt.

Question 5

Question Type: MultipleChoice

A company has entered into a business relationship with another organization and needs to provide access to internal resources through directory services. Which of the following should a systems administrator implement?

Options:

A- sso

B- VPN

C- SSH

D- SAML

Answer:

B

Explanation:

The answer is B. A VPN tunnel. A VPN tunnel is a secure and encrypted connection between two networks over a public network, such as the Internet. A VPN tunnel can help protect data in transit by encrypting it before it leaves the company's network and decrypting it when it reaches the public cloud service provider. A VPN tunnel can also authenticate the endpoints and verify the integrity of the data.

Some possible sources of information about VPN tunnels are:

What is a VPN Tunnel? | Fortinet: This page explains what a VPN tunnel is, how it works, and what benefits it provides.

VPN Gateway: Create a Site-to-Site connection using a VPN gateway | Microsoft Docs: This page shows how to create a site-to-site connection using a VPN gateway in Azure.

[Cloud VPN overview | Google Cloud]: This page provides an overview of Cloud VPN, a service that creates secure and reliable VPN tunnels to Google Cloud.

Question 6

Question Type: MultipleChoice

A systems administrator needs to connect the companys network to a public cloud services provider. Which of the following will BEST ensure encryption in transit for data transfers?

Options:

A- Identity federation

B- A VPN tunnel

C- A proxy solution

D- A web application firewall

Answer:

B

Explanation:

The answer is A. SAML. SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between different parties, such as a user and a service provider. In a federated cluster, SAML can be used to enable single sign-on (SSO) for users across multiple clusters or cloud providers. SAML relies on the exchange of XML-based assertions that contain information about the user's identity, attributes, and entitlements. If the users' API access tokens have become invalid, it could be because the SAML assertions have expired, been revoked, or corrupted. The administrator should check the SAML configuration and logs to determine the cause of this issue.

Some possible sources of information about SAML and federated clusters are:

Authenticating | Kubernetes: This page provides an overview of authenticating users in Kubernetes, including using SAML for federated identity.

Authenticating to the Kubernetes API server - Google Cloud: This page explains how to authenticate to the Kubernetes API server on Google Cloud, including using SAML for federated identity with Google Cloud Identity Platform.

Error 403 User not authorized when trying to access Azure Databricks API through Active Directory - Stack Overflow: This page discusses a similar issue of users getting an error when trying to access Azure Databricks API using SAML and Active Directory.

Question 7

Question Type: MultipleChoice

A cloud administrator is troubleshooting an issue regarding users at one location who are reporting that their API access tokens have become invalid. The users are issued tokens based on their credentials in a federated cluster. Which of the following should the administrator check to determine the cause of this issue?

Options:

A- SAML

B- DNS

C- SSL

D- NTP

Answer:

A

Explanation:

The answer is

A) SAML. SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between different parties, such as a user and a service provider. In a federated cluster, SAML can be used to enable single sign-on (SSO) for users across multiple clusters or cloud providers. SAML relies on the exchange of XML-based assertions that contain information about the user's identity, attributes, and entitlements. If the users' API access tokens have become invalid, it could be because the SAML assertions have expired, been revoked, or corrupted. The administrator should check the SAML configuration and logs to determine the cause of this issue.

Some possible sources of information about SAML and federated clusters are:

Authenticating | Kubernetes: This page provides an overview of authenticating users in Kubernetes, including using SAML for federated identity.

Authenticating to the Kubernetes API server - Google Cloud: This page explains how to authenticate to the Kubernetes API server on Google Cloud, including using SAML for federated identity with Google Cloud Identity Platform.

Error 403 User not authorized when trying to access Azure Databricks API through Active Directory - Stack Overflow: This page discusses a similar issue of users getting an error when trying to access Azure Databricks API using SAML and Active Directory.