Certified Implementation Specialist (CIS) - Discovery Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://cisdiscovery.examzify.com

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **What does network topology mapping provide in the context of Discovery?**

   A. It defines security protocols for network communications

   B. It shows the physical or logical layout of a network, illustrating connections between nodes

   C. It outlines the performance metrics of all network devices

   D. It establishes user access levels across the network

2. **In which phase do Infrastructure patterns use the ID Phase?**

   A. Detection

   B. Configuration

   C. Exploration

   D. Validation

3. **How can security and privacy be maintained during the Discovery process?**

   A. By conducting regular user training

   B. By utilizing credential encryption

   C. By limiting the use of remote access

   D. By implementing a strict password policy

4. **What does the "Default MID Server" signify in ServiceNow?**

   A. A designated MID Server used for all Discovery jobs

   B. A designated MID Server used when no specific one is assigned for a Discovery job

   C. A temporary MID Server for emergency use only

   D. A universal MID Server for all client interactions

5. **What characterizes the ECC queue?**

   A. It is primarily used for outputting processed data

   B. It is distinct in that it is queried and written into by external systems

   C. It is a temporary storage for new data configurations only

   D. It is only applicable for device classification processes

6. What are the two main classes of Configuration Items (CIs)?

A. Network and Software

B. Application (SW) cmdb_ci_appl and Infrastructure (HW) cmdb_ci_hardware

C. Cloud and On-premise

D. Virtual and Physical

7. What does the Default App naming Convention typically include?

A. Device type and configuration

B. Application name and host CI

C. DB name and process ID

D. User credentials and permissions

8. What is the default batch size for Shazzam?

A. 256

B. 5000

C. 10000

D. 128

9. In what scenario would you utilize Sniffers during Discovery?

A. When performing regular system updates

B. When needing to identify network traffic

C. When evaluating network security policies

D. When conducting user audits

10. What must be defined for all MID Servers in a cluster?

A. Service Level Agreements

B. Capabilities

C. Database connections

D. Authentication methods

Answers

1. B
2. C
3. B
4. B
5. B
6. B
7. B
8. B
9. B
10. B

Explanations

1. What does network topology mapping provide in the context of Discovery?

A. It defines security protocols for network communications

B. It shows the physical or logical layout of a network, illustrating connections between nodes

C. It outlines the performance metrics of all network devices

D. It establishes user access levels across the network

Network topology mapping is a vital aspect of Discovery as it visually represents the structure of a network, illustrating how different nodes (such as computers, servers, routers, switches, etc.) are interconnected. Understanding this layout is crucial in various IT processes, including troubleshooting, planning, and auditing, as it provides insight into how data flows throughout the network and identifies potential points of failure or inefficiencies. By mapping the physical or logical topology, organizations can better understand their infrastructure, which aids in network management and optimization. This insight also assists in ensuring that the network is securely configured and allows for efficient usage of resources. Recognizing how devices interconnect provides a foundation for implementing further discovery and monitoring tools, facilitating ongoing management and security compliance. Other options, while relevant to aspects of network management, do not directly pertain to the concept of topology mapping. Security protocols, performance metrics, and user access levels relate more broadly to managing and securing a network but do not focus specifically on the layout and connections of the devices within that network.

2. In which phase do Infrastructure patterns use the ID Phase?

A. Detection

B. Configuration

C. Exploration

D. Validation

In the context of the Discovery process, Infrastructure patterns are typically utilized during the Exploration phase. This phase consists of gathering information about the existing IT infrastructure to identify and map out configurations, relationships, and dependencies between various components within the environment. The ID Phase specifically refers to the step where data is being collected and identified, allowing analysts to categorize and understand the patterns present in the infrastructure. During the Exploration phase, tools and techniques are employed to uncover the current state of the environment, which is essential for building infrastructure patterns that accurately reflect how various systems and services interact. This information is crucial for later phases that focus on validation and configuration, but it is fundamentally about exploring and understanding what exists, thereby validating the collected data and ensuring patterns are correctly identified. This comprehensive understanding developed during the Exploration phase sets the foundation for successful subsequent actions in the Discovery process.

3. How can security and privacy be maintained during the Discovery process?

A. By conducting regular user training

B. By utilizing credential encryption

C. By limiting the use of remote access

D. By implementing a strict password policy

Utilizing credential encryption is crucial in maintaining security and privacy during the Discovery process because it ensures that sensitive information, such as usernames and passwords, is protected from unauthorized access. When credentials are encrypted, they are transformed into a format that is unreadable without the correct decryption key, making it significantly more difficult for attackers to intercept and misuse this information. This helps safeguard the integrity of the system and the privacy of user data throughout the Discovery process. While other options do contribute to security, they do not address the specific aspect of credential protection as directly as encryption does. For instance, user training is valuable for helping individuals recognize security threats, but it does not by itself secure credentials. Limiting remote access can enhance security by reducing potential entry points for attacks, but it may not directly involve the protection of credential data during Discovery. A strict password policy can aid in creating strong access controls, yet it is still vulnerable if credentials are not properly encrypted during transmission or storage. Therefore, the focused implementation of credential encryption is essential for ensuring robust privacy and security during the Discovery phase.

4. What does the "Default MID Server" signify in ServiceNow?

A. A designated MID Server used for all Discovery jobs

B. A designated MID Server used when no specific one is assigned for a Discovery job

C. A temporary MID Server for emergency use only

D. A universal MID Server for all client interactions

The term "Default MID Server" in ServiceNow refers specifically to a MID Server that is utilized when no particular MID Server is specified for a Discovery job. This means that if a Discovery job does not explicitly assign a MID Server to it, the system will default to this designated MID Server. Having a Default MID Server ensures that Discovery processes can still operate smoothly even when an administrator does not specify a MID Server for a task. It simplifies configurations and provides a reliable option to ensure that discovery activities are executed without delays. In contrast, the other options imply varying functionalities that do not align with the core definition of a Default MID Server. For instance, suggesting that it is a designated MID Server for all Discovery jobs implies a constant use regardless of specific configurations, which is not accurate. The notion of a temporary MID Server for emergency use or a universal MID Server for all client interactions adds ambiguity and does not reflect the intended role of the Default MID Server within the ServiceNow environment.

5. What characterizes the ECC queue?

A. It is primarily used for outputting processed data

B. It is distinct in that it is queried and written into by external systems

C. It is a temporary storage for new data configurations only

D. It is only applicable for device classification processes

The ECC (External Communication Channel) queue is indeed characterized by its function as a conduit for data exchange between external systems and the ServiceNow platform. It is specifically designed to allow external systems to write data into the queue and for ServiceNow to query that data as necessary. This characteristic enables seamless integration and facilitates the ingestion of data from various sources, which is essential for maintaining accurate and up-to-date information within the ServiceNow environment. This queuing process allows for the automation of workflows and processes initiated by information that originates outside of ServiceNow, making the ECC queue a crucial component for organizations that rely on data coming from multiple external systems. The effective use of the ECC queue enhances the platform's interoperability and functionality, allowing for a more cohesive ecosystem of applications and data sources. The other options do not accurately capture the primary function of the ECC queue, focusing instead on aspects that either exclude the external communication element or misrepresent its purpose within the ServiceNow architecture. This misunderstanding could lead to challenges in leveraging data integration effectively in real-world implementations.

6. What are the two main classes of Configuration Items (CIs)?

A. Network and Software

B. Application (SW) cmdb_ci_appl and Infrastructure (HW) cmdb_ci_hardware

C. Cloud and On-premise

D. Virtual and Physical

The correct answer identifies the two primary classes of Configuration Items (CIs) within the Configuration Management Database (CMDB) framework. The distinction is made between application components, classified under the category of "Application (SW)" specifically represented by cmdb_ci_appl, and infrastructure components which fall under "Infrastructure (HW)" represented by cmdb_ci_hardware. This classification is essential because it allows organizations to manage and track the different types of assets within their IT environment effectively. Applications are critical for delivering business services, while infrastructure components provide the underlying support necessary for those applications to function. By categorizing CIs in this manner, organizations can better understand the relationships and dependencies between applications and the hardware they rely on, enabling more effective management and issue resolution. Other options may describe various aspects or types of CIs, but they do not capture this fundamental categorization that distinguishes between software applications and hardware infrastructure, which is pivotal for effective IT service management and compliance with ITIL practices.

7. What does the Default App naming Convention typically include?

A. Device type and configuration

B. Application name and host CI

C. DB name and process ID

D. User credentials and permissions

The Default App naming Convention typically includes the application name and the host configuration item (CI). This naming convention is essential for maintaining clarity and consistency across configurations within an IT environment. By including both the application name and the host CI, it allows for easy identification of the application's association with specific hardware or virtual environments, enhancing the management and tracking of applications across the infrastructure. This structure also aids in better organization and documentation of assets, enabling IT personnel and management to quickly ascertain where applications are running and under which conditions. This clarity is crucial during troubleshooting and maintenance processes, as it simplifies the identification of potential issues related to specific applications and their respective environments. Thus, the correct answer focuses on a clear and functional approach to naming conventions in IT asset management.

8. What is the default batch size for Shazzam?

A. 256

B. 5000

C. 10000

D. 128

The default batch size for Shazzam is indeed 5000. This configuration is significant for managing the volume of data processed during discovery. A larger batch size allows Shazzam to handle more items in one operation, which can enhance performance and efficiency when scanning and importing large datasets. Choosing an appropriate batch size is crucial for optimizing resource usage and can impact the overall processing speed and memory consumption of the tool. While other options might represent different configurations, 5000 is specifically established as the default, making it the standard reference point for users when setting up Shazzam for data integrations. Understanding this default setting helps ensure that users can make informed decisions on adjustments based on their specific data processing needs.

9. In what scenario would you utilize Sniffers during Discovery?

A. When performing regular system updates

B. When needing to identify network traffic

C. When evaluating network security policies

D. When conducting user audits

Utilizing sniffers during Discovery is particularly relevant when there is a need to identify network traffic. Sniffers are tools that capture and analyze packets of data traveling over a network, which allows for an in-depth understanding of the types of data being transmitted, the protocols in use, and the communication patterns between devices. This information is critical during the Discovery phase as it helps to map out network infrastructure, identify devices and services running on the network, and understand the overall network behavior. The context in which sniffers can be valuable is quite specific to scenarios where real-time data flow needs to be monitored, allowing for assessment of performance, traffic loads, and potential anomalies. This ability to observe and analyze network traffic is a key part of effectively understanding how the various elements of the network interact, ultimately guiding decisions related to infrastructure improvements or configurations. In contrast, other scenarios such as regular system updates focus more on software maintenance and do not involve traffic analysis; evaluating network security policies usually involves reviews of existing documentation and compliance checks rather than real-time data capture; and conducting user audits tends to focus on user access and permissions rather than network traffic itself. Each of these areas has different tools and methods suited for their specific needs, which is why identifying network traffic through sniff

10. What must be defined for all MID Servers in a cluster?

A. Service Level Agreements

B. Capabilities

C. Database connections

D. Authentication methods

The correct response highlights that capabilities must be defined for all MID Servers in a cluster. In the context of ServiceNow MID Servers, capabilities refer to specific functions that a MID Server can perform, such as interacting with various systems, executing scripts, and handling certain protocols. Defining capabilities is essential for the functioning of the cluster because it allows the ServiceNow platform to efficiently route tasks to the most appropriate MID Server based on their available capabilities. This ensures optimal performance and resource utilization across the cluster. Effective capability management also plays a critical role in load balancing and fault tolerance, as it enables the system to understand which MID Server can handle a specific request, thus maintaining efficient workflow and system reliability. Without properly defined capabilities, the cluster may struggle to allocate tasks effectively, which could lead to performance issues or task failures. While other options, such as service level agreements, database connections, and authentication methods may be important in their own right, they do not directly relate to the core requirement for MID Servers in a cluster to perform their designated tasks effectively.