ServiceNow Discovery Fundamentals Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. What does "Include alive" mean in the context of discovery?

A. Devices that are currently operational

B. Devices with no ports opened and responding.

C. Devices on which one port responded to the scan

D. Devices that have been discovered successfully

2. What is the result of executing a Network discovery?

A. Identifying all IP addresses and updating the CMDB

B. Only IP addresses using network routers are identified

C. No data is gathered during the process

D. Enhanced network performance analysis

3. What two sections are present in the Horizontal Discovery pattern?

A. Identification and Verification

B. Identification and Extension

C. Identification and Analysis

D. Identification and Querying

4. Which aspect is included in the 'Compliance' metrics of the CMDB Health Dashboard?

A. Required Fields

B. Certification Filters

C. Orphan Entries

D. Staleness

5. What is used to enable the display of the list of classifiers during the classification phase?

A. glide.discovery.classifiers.show = true

B. glide.discovery.debug.classification = true

C. glide.discovery.classification.list = true

D. glide.discovery.enable.classifiers = true

6. Which phase focuses on collecting information about existing CIs?

A. Exploration Phase

B. Identification Phase

C. Horizontal Exploration Phase

D. Configuration Phase

7. What role typically handles SSH configurations on a server?

A. Database Administrator

B. Network Administrator

C. Systems Administrator

D. Security Administrator

8. What happens when there are no available MID Servers in the auto-select process?

A. The process fails and reports an error

B. The default MID Server for the Discovery application is used

C. No action is taken, and the discovery is skipped

D. The system auto-invokes a new MID Server

9. What types of discovery can utilize the Application pattern?

A. Only Horizontal Discovery

B. Only Vertical Discovery

C. Both Horizontal and Vertical Discovery

D. Neither Horizontal nor Vertical Discovery

10. What is a fixed key used for in the context of credential management?

A. Decrypting the credentials

B. Enabling secure connections

C. Encrypting user data

D. Creating backup keys

Answers

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

Explanations

1. What does "Include alive" mean in the context of discovery?

A. Devices that are currently operational

B. Devices with no ports opened and responding.

C. Devices on which one port responded to the scan

D. Devices that have been discovered successfully

In the context of discovery, "Include alive" refers to including devices that have successfully responded during a scan, indicating they are operational or reachable within the network. Specifically, when considering the interpretation of the answer option regarding devices on which one port responded to the scan, this aligns with the concept of identifying devices as "alive." When a device responds to a network scan, perhaps by returning information from one or more open ports, it confirms that the device is active and participating in the network. Therefore, having at least one port respond during the scan is a key criterion for considering a device as "alive" and making it eligible for discovery processes, such as cataloging its configuration items within ServiceNow. The other options describe different scenarios that do not specifically address the functionality of the discovery process. For instance, operational devices might not respond if they are configured not to communicate over certain ports. Additionally, devices with no responding ports or those that have not been discovered successfully do not meet the criteria for being classified as "alive." Consequently, the most accurate understanding of "Include alive" in this instance is related to devices that have at least one responding port during the discovery scan.

2. What is the result of executing a Network discovery?

A. Identifying all IP addresses and updating the CMDB

B. Only IP addresses using network routers are identified

C. No data is gathered during the process

D. Enhanced network performance analysis

Executing a Network Discovery in ServiceNow involves identifying devices on the network and collecting information about their properties. The primary aim is to gather data about various network elements, including IP addresses, associated devices, and their relationships. When a network discovery is successfully executed, it generally identifies all active IP addresses within the specified range, along with other contextual information about devices such as their location and attributes. This information is critical for maintaining an accurate Configuration Management Database (CMDB). The aspect that highlights the comprehensive nature of network discovery is that it is not limited to just IP addresses connected through network routers. It can recognize devices beyond the routers, including servers, printers, switches, and other endpoints that have an IP address, and subsequently update the CMDB accordingly. This makes the first choice the most accurate representation of what happens during a Network Discovery. The other options do not encapsulate the full function of network discovery. Specifically, identifying only IP addresses using network routers fails to recognize the broader scope of devices that can be detected. Claiming that no data is gathered is inaccurate, as the primary purpose is to collect and update meaningful information. Lastly, the idea of enhancing network performance analysis is not the direct goal of network discovery but rather a potential benefit that can arise

3. What two sections are present in the Horizontal Discovery pattern?

A. Identification and Verification

B. Identification and Extension

C. Identification and Analysis

D. Identification and Querying

The two sections present in the Horizontal Discovery pattern are Identification and Extension. In the context of ServiceNow Discovery, the Identification section is crucial as it involves detecting and identifying devices on the network based on various parameters, such as IP addresses or specific protocols. This stage is essential for establishing what elements are present in the IT infrastructure. The Extension section follows, enabling the Discovery process to delve deeper into gathered information. It extends the initial identification process by collecting additional data about what has been identified, including relationships, configuration items, and more detailed attributes of the assets. This two-part process enhances ServiceNow's ability to build a comprehensive Configuration Management Database (CMDB). Understanding this structure is vital for effectively utilizing ServiceNow Discovery since proper identification and effective data extension are critical for accurate and relevant data collection, which ultimately supports IT service management processes.

4. Which aspect is included in the 'Compliance' metrics of the CMDB Health Dashboard?

A. Required Fields

B. Certification Filters

C. Orphan Entries

D. Staleness

The 'Compliance' metrics of the CMDB Health Dashboard focus on ensuring that the various Configuration Items (CIs) within the Configuration Management Database (CMDB) adhere to the defined standards and requirements. One important element that falls under compliance is the use of Certification Filters. Certification Filters are used to assess whether CIs meet specified criteria and guidelines, indicating their compliance with organizational policies or industry standards. Including certification within the compliance metrics aids in identifying CIs that may not comply with specific requirements, enabling organizations to take corrective actions. Ensuring compliance is critical for maintaining the integrity and reliability of the CMDB, as it supports decision-making processes across IT services and operations. The other aspects, while important for CMDB health, do not specifically fall under the compliance category. Required Fields are crucial for data completeness; Orphan Entries pertain to isolated CIs without relationships; Staleness deals with outdated and inactive CIs. However, all these aspects contribute to the overall CMDB health but are not classified specifically as compliance metrics like Certification Filters are.

5. What is used to enable the display of the list of classifiers during the classification phase?

A. glide.discovery.classifiers.show = true

B. glide.discovery.debug.classification = true

C. glide.discovery.classification.list = true

D. glide.discovery.enable.classifiers = true

The classification phase in ServiceNow Discovery is a crucial step where discovered devices and applications are categorized accurately so that the system can manage them effectively. To facilitate this process and enable the display of the list of classifiers used during the classification, specific configuration settings are utilized. The correct setting, glide.discovery.debug.classification = true, allows for diagnostic logging and debug-level verbosity in the classification workflow. This setting not only helps in displaying the list of classifiers but also aids administrators and developers in understanding how classifications are being processed. When this option is enabled, detailed logs may reveal which classifiers are being deemed applicable and how the classification decisions are being made, enhancing transparency in the classification process. In contrast, the other options do not directly relate to enabling the display of the list of classifiers during the classification phase. For instance, settings that reference 'classifiers.show' or 'classification.list' might suggest they control visibility or lists but do not specifically address the debugging and detail-oriented needs during classification. Additionally, 'enable.classifiers' might imply the activation of classifiers but does not inherently include the debug aspect necessary for displaying the classifiers' list.

6. Which phase focuses on collecting information about existing CIs?

A. Exploration Phase

B. Identification Phase

C. Horizontal Exploration Phase

D. Configuration Phase

The Exploration Phase is focused on collecting information about existing Configuration Items (CIs). This phase involves identifying and assessing all CIs within the environment, which allows organizations to build a comprehensive inventory. During the Exploration Phase, the Discovery process gathers detailed data about the hardware and software present in the network. This information is crucial for establishing a reliable Configuration Management Database (CMDB), as it lays the groundwork for effective configuration management practices that will follow in later phases. In this phase, various discovery methods are employed to probe networks, identify devices, and accumulate relevant property data associated with each CI. This can encompass things like specifications, relationships, and states of the CIs to ensure that the CMDB accurately reflects the organization's infrastructure. In contrast, other phases such as the Identification Phase primarily focus on recognizing and classifying CIs, the Horizontal Exploration Phase typically involves deeper analysis of relationships among CIs, and the Configuration Phase is concerned with managing and maintaining the CIs within the CMDB rather than the initial collection of data. Thus, the Exploration Phase is critical for establishing the foundational data needed for effective IT asset management.

7. What role typically handles SSH configurations on a server?

A. Database Administrator

B. Network Administrator

C. Systems Administrator

D. Security Administrator

The role that typically handles SSH configurations on a server is the Systems Administrator. Systems Administrators are responsible for the overall management and configuration of servers, including their operating systems, software applications, and security settings. This includes setting up and managing SSH (Secure Shell), which is a cryptographic network protocol used for secure data communication, remote command-line login, and other secure network services between two networked computers. Systems Administrators ensure that SSH is correctly configured, which includes setting up access controls, managing user keys, and applying security best practices to prevent unauthorized access. They also handle updates and maintenance of the server environments, making their role integral to the proper setup of SSH and other server protocols. While other roles may interact with SSH in certain contexts, such as a Security Administrator managing security policies or a Network Administrator dealing with network-level configurations, it is primarily the Systems Administrator who is focused on the server's operational aspects, thus making them the most relevant role for SSH configurations.

8. What happens when there are no available MID Servers in the auto-select process?

A. The process fails and reports an error

B. The default MID Server for the Discovery application is used

C. No action is taken, and the discovery is skipped

D. The system auto-invokes a new MID Server

When there are no available MID Servers in the auto-select process, the system resorts to using the default MID Server designated for the Discovery application. The default MID Server is defined as part of the system's configuration and serves as a fallback option to ensure that discovery processes can continue even when other MID Servers are unavailable. This mechanism is crucial for maintaining continuity in discovery operations, particularly in environments where multiple MID Servers may be configured for redundancy or load balancing. In scenarios where no MID Servers are available, using the default MID Server allows for the possibility of completing discovery tasks without interruption, ensuring the system remains functional and responsive. This capability to fall back on a default MID Server enhances the reliability of the ServiceNow Discovery process, minimizing potential disruptions in operations due to MID Server unavailability.

9. What types of discovery can utilize the Application pattern?

A. Only Horizontal Discovery

B. Only Vertical Discovery

C. Both Horizontal and Vertical Discovery

D. Neither Horizontal nor Vertical Discovery

The Application pattern is designed to identify and map the relationships between applications and the various components that support them, which includes both Horizontal and Vertical Discovery approaches. Horizontal Discovery focuses on discovering network devices, services, and nodes across an organization. It generally identifies systems, applications, and other entities that can be viewed from a horizontal perspective, emphasizing their relationships in a broad scope. The Application pattern plays a role here by helping users understand how different applications might be deployed across several devices and environments. On the other hand, Vertical Discovery dives deeper into the relationships and configurations of a specific application within a defined environment. This discovery method examines the internal components that comprise an application stack, including dependencies, configurations, and integrations that support application function. The Application pattern is essential in this context as well, as it helps to delineate how various elements within an application environment interact with one another. Thus, the Application pattern's versatility allows it to be utilized in both Horizontal and Vertical Discovery, making the combination a comprehensive method for understanding complex application landscapes within an organization.

10. What is a fixed key used for in the context of credential management?

A. Decrypting the credentials

B. Enabling secure connections

C. Encrypting user data

D. Creating backup keys

In the context of credential management, a fixed key primarily serves the purpose of decrypting the credentials. Fixed keys are specific cryptographic keys that remain constant and are used to encrypt and decrypt data. When credentials are encrypted for security reasons, they cannot be used by the system or the user until they are decrypted with the appropriate fixed key. This ensures that sensitive information, like passwords or API keys, remains secure while still being accessible to authorized users or systems when needed. The other options refer to different cryptographic functions or practices. Secure connections typically rely on various encryption protocols and techniques to establish authentication and data integrity. Encrypting user data may involve using various encryption keys, but a fixed key specifically highlights the decryption process tied to credential management. Creating backup keys relates to maintaining redundancy and data recovery options, which are distinct from the primary function of a fixed key in decrypting credentials.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://servicenowdiscoveryfund.examzify.com

We wish you the very best on your exam journey. You've got this!