# ServiceNow Discovery Fundamentals Practice Test (Sample)

## Study Guide

BY EXAMZIFY

**Everything you need from our exam experts!**

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

# Questions

1. **Where can identifiers for Configuration Items be set?**

   **A. Discovery > CI Identification > Identifiers**

   **B. CI Class Manager > Identifier Settings**

   **C. Discovery Definition > CI Identification > Identifiers**

   **D. Discovery Settings > General Configuration**

2. **Can infrastructure patterns be exclusively used by Discovery?**

   **A. Yes**

   **B. No**

   **C. Only in specific scenarios**

   **D. Only for testing purposes**

3. **What summary does the Discovery Status provide?**

   **A. A log of all scheduled processes**

   **B. A history of all discovered devices**

   **C. A summary of a Discovery launched from a schedule**

   **D. An outline of all error reports**

4. **Which of the following best describes how credentials are initially processed?**

   **A. They are encrypted on the instance before transmission**

   **B. They are stored unencrypted for performance**

   **C. They are validated against a database**

   **D. They are automatically generated**

5. **What temporary variables are always available by default in Pattern Design for Infrastructure Discovery Patterns?**

   **A. *system* variable**

   **B. *computer_system* variable**

   **C. *network_device* variable**

   **D. *application* variable**

6. **What is a requirement for MID servers in a Load Balance Cluster?**

   **A. They must be located in the same geographic region**

   **B. They have the same capabilities**

   **C. They must share the same power source**

   **D. They are configured to run independently**

7. **What might indicate a problem with a custom sensor in the Exploration Phase?**

   **A. It has a high execution time**

   **B. The logs show successful execution**

   **C. It reports incorrect CI data**

   **D. No XML payload shows up on the form**

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 credentials are needed to discover VMware?**

   **A. Linux credentials**

   **B. Windows credentials for vCenter application**

   **C. Generic VMware credentials for all functions**

   **D. Both Windows and VMware credentials**

10. **What happens to credentials during the encryption process on the instance?**

    **A. They are encrypted with SSL**

    **B. They are stored in a text file**

    **C. They are sent unencrypted over the network**

    **D. They are logged in plain text**

# Answers

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

# Explanations

### 1. Where can identifiers for Configuration Items be set?

A. Discovery > CI Identification > Identifiers

B. CI Class Manager > Identifier Settings

C. Discovery Definition > CI Identification > Identifiers

D. Discovery Settings > General Configuration

The correct answer is found within the context of Discovery Definition, specifically under CI Identification and then Identifiers. This is because within ServiceNow, the Discovery Definition module plays a vital role in controlling how Configuration Items (CIs) are identified during the discovery process. The identifiers set in this area define the crucial parameters that help in accurately determining and classifying the CIs that are discovered in your environment. When you configure identifiers in this section, you are directly affecting how ServiceNow recognizes and manages different types of CIs. These identifiers can include a range of attributes that uniquely define a CI, ensuring that there is no overlap or misclassification when multiple similar items are discovered. By managing identifiers effectively, the system can maintain a clear and organized structure for asset management and configuration, which is crucial for effective IT service management. The other options, while they may seem plausible, do not specifically pertain to the exact location and relevance of identifying CIs within the discovery process. They may reference different aspects of CI management or discovery settings but do not directly address setting identifiers, which is why they are not the correct choices.

### 2. Can infrastructure patterns be exclusively used by Discovery?

A. Yes

B. No

C. Only in specific scenarios

D. Only for testing purposes

Infrastructure patterns in ServiceNow are designed to model and represent the configuration of IT infrastructure components such as servers, applications, and networks. While they play a crucial role in the discovery process by helping to identify and map these components, their functionality extends beyond just the Discovery application. Infrastructure patterns can also be utilized in other areas of the ServiceNow platform. For instance, they are applicable in the context of Service Mapping, which goes beyond mere discovery to understand the dependencies and relationships between services and their underlying infrastructure. Additionally, these patterns can be leveraged in Incident Management, Change Management, and other ITSM processes to align infrastructure with business services and enhance overall service management capabilities. Thus, the assertion that infrastructure patterns can be exclusively used by Discovery is incorrect. Their utility spans a wide array of ITSM functions, allowing organizations to gain insights and maintain control over their entire IT landscape, not just during the discovery phase.

## 3. What summary does the Discovery Status provide?

**A. A log of all scheduled processes**

**B. A history of all discovered devices**

**C. A summary of a Discovery launched from a schedule**

**D. An outline of all error reports**

**The Discovery Status provides a summary of a Discovery launched from a schedule because it captures the details related to that particular instance of Discovery execution. This includes information such as the start and end times, the number of devices discovered, any errors encountered during the process, and the overall success or failure of the scheduled Discovery. This summary is essential for administrators and IT professionals to monitor and assess the effectiveness of their scheduled Discovery processes, enabling them to make informed decisions about infrastructure management and resource allocation. In contrast, other options describe different aspects of Discovery processes. A log of all scheduled processes refers to a broader overview of all planned Discovery activities, not just the ones that were executed. A history of all discovered devices would provide an inventory of what has been discovered over time, which is more detailed and extensive. An outline of all error reports would focus specifically on issues encountered during various Discovered instances, rather than summarizing the execution of a scheduled event itself. Thus, the answer focusing on the summary captures the essence of monitoring a specific Discovery task initiated by a schedule.**

## 4. Which of the following best describes how credentials are initially processed?

**A. They are encrypted on the instance before transmission**

**B. They are stored unencrypted for performance**

**C. They are validated against a database**

**D. They are automatically generated**

**The process of handling credentials in ServiceNow Discovery is essential for securing sensitive information during the discovery process. When credentials are initially processed, they are encrypted on the instance before being transmitted to the target system. This step ensures that any credentials used for accessing network devices or applications are not exposed in plaintext over the network, thus protecting them from potential interception or unauthorized access. The encryption of credentials enhances security, aligning with best practices for managing sensitive information. It helps maintain the integrity and confidentiality of the credentials as they are utilized during discovery scans. This level of security is particularly crucial in environments where sensitive data and resources are being accessed. In contrast, other options involve methods of handling credentials that do not prioritize security to the same extent. Storing credentials unencrypted poses significant security risks, while validating against a database does not pertain to the initial processing of credentials. Automatically generating credentials would not reflect a method of processing existing credentials but rather creating new ones, which is not the focus of this question.**

## 5. What temporary variables are always available by default in Pattern Design for Infrastructure Discovery Patterns?

A. *system* variable

B. *computer_system* variable

C. *network_device* variable

D. *application* variable

**The *computer_system* variable is the correct choice because it is a fundamental component within the context of Pattern Design for Infrastructure Discovery in ServiceNow. When creating infrastructure discovery patterns, the *computer_system* variable allows the pattern to access crucial information about the discovered computer systems, such as their attributes and configurations. This variable plays a key role in identifying specific details about the systems that the pattern aims to discover and manage, serving as a core reference point for defining and operating the pattern. In infrastructure discovery, having predefined variables like *computer_system* simplifies the design process, enabling pattern creators to directly refer to system properties without needing to define them manually within each new pattern. This leads to more efficient pattern development and enhances consistency across different patterns as they operate on the same foundational data structure. The other variables mentioned, while potentially useful depending on the specific context of the pattern in question, do not have the same ubiquitous or default applicability as the *computer_system* variable in this scenario. Thus, selecting *computer_system* reflects an understanding of its essential role in effectively implementing infrastructure discovery patterns within the ServiceNow platform.**

## 6. What is a requirement for MID servers in a Load Balance Cluster?

A. They must be located in the same geographic region

B. They have the same capabilities

C. They must share the same power source

D. They are configured to run independently

**In a Load Balance Cluster, it is essential that the MID servers possess the same capabilities to ensure consistent performance and functionality across the cluster. This uniformity allows for seamless load sharing, where tasks and requests can be efficiently distributed among the servers. When each MID server has the same capabilities, it ensures that they can handle the same types of processes and data, which prevents any potential bottlenecks or performance discrepancies when traffic is routed to different servers. Maintaining identical capabilities among the servers means that they can all respond to requests and perform Discovery tasks uniformly, ensuring reliable service availability and redundancy. This becomes crucial in scenarios where one server might be down or under heavy load; other capable MID servers in the cluster can take over without loss of service or performance degradation. The other options, while they may seem relevant in certain contexts, do not directly correlate to the requirements for load balancing. For example, while geographic proximity might improve network latency, it's not a strict requirement for a load-balanced setup. Similarly, sharing a power source or being configured to run independently does not facilitate the core advantage of balancing load effectively among MID servers, which is the essence of their capabilities.**

## 7. What might indicate a problem with a custom sensor in the Exploration Phase?

A. It has a high execution time

B. The logs show successful execution

C. It reports incorrect CI data

D. No XML payload shows up on the form

**In the Exploration Phase of ServiceNow Discovery, the absence of an XML payload on the form is a significant indicator of issues with a custom sensor. When a custom sensor operates correctly, it should generate an XML payload that contains the data collected during the discovery process. This payload is crucial for the proper functioning and integration of the sensor with the discovery framework. If no XML payload is being generated or becomes visible in the relevant form, it suggests that the sensor may not be executing as intended or that there is a fundamental problem in its configuration or logic. Moreover, while high execution time can suggest inefficiencies in performance, the actual generation and transmission of data is far more critical during the Exploration Phase. The logs showing successful execution might give a misleading sense of operability if the payload isn't produced, and incorrect CI data is more indicative of potential data processing errors rather than an issue with the sensor's basic operational capability. Thus, the lack of an XML payload directly points to a failure in the sensor's functioning to collect or report data, making it the most reliable indicator of a problem in this context.**

## 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 credentials are needed to discover VMware?

A. Linux credentials

B. Windows credentials for vCenter application

C. Generic VMware credentials for all functions

D. Both Windows and VMware credentials

To discover VMware environments effectively, both Windows credentials and VMware-specific credentials are necessary. The Windows credentials are essential because they allow the discovery process to interact with the vCenter server, which manages the VMware infrastructure. Through the vCenter, ServiceNow Discovery can retrieve details about the virtual machines, hosts, and other resources that exist within the VMware environment. Without these credentials, the discovery tool would be unable to authenticate and connect to the necessary systems. On the other hand, VMware credentials are needed to access and gather information about specific VMware components and their configurations. These credentials ensure that the discovery tool can perform necessary operations related to VMware management functions. Thus, having both sets of credentials—Windows credentials for interfacing with vCenter and specific VMware credentials for comprehensive data retrieval—allows for a complete and effective discovery process in a VMware infrastructure.

## 10. What happens to credentials during the encryption process on the instance?

A. They are encrypted with SSL

B. They are stored in a text file

C. They are sent unencrypted over the network

D. They are logged in plain text

During the encryption process on the instance, credentials are indeed encrypted with SSL (Secure Sockets Layer). This is crucial for maintaining the security and confidentiality of sensitive information, such as user credentials, during transmission. SSL encrypts the data as it travels over the network, preventing unauthorized access or interception by malicious entities. Using SSL ensures that the credentials are not vulnerable to eavesdropping or tampering while they are being sent across the network. Encryption is a standard practice for protecting data integrity and privacy in modern web communications, particularly in systems like ServiceNow Discovery, where secure handling of credentials is essential for discovering and managing IT assets effectively. The other options do not reflect the secure practices employed by the instance. Storing credentials in a text file or logging them in plain text would expose them to risks of unauthorized access, and sending them unencrypted over the network compromises their security entirely. The adherence to SSL for encryption aligns with industry standards for data protection.