Testpassport Q&A

La meilleure qualité le meilleur service

Exam : **CIS-SP**

Title : ServiceNOW Certified Implementation Specialist - Service Provide

Version : DEMO

1.The system automatically sets which field when an administrator attempts to modify a policy, application, or module that belongs to another domain higher in the hierarchy?
A. sys_overrides
B. sys_primary_domain
C. sys_admin_domain
D. sys_domain_owner
Answer: D
Explanation:
When an administrator attempts to modify a policy, application, or module that belongs to another domain higher in the hierarchy, the system automatically sets the sys_domain_owner field. This field ensures that the ownership of the record is correctly attributed to the domain that originally created or owns the record, maintaining the integrity and separation of data across different domains.
Reference:
• ServiceNow Domain Separation - Advanced Concepts and Configurations
• Understanding Domain Separation - Basics

2.Process Separation is also known as:
A. proxy administration
B. delegated administration
C. process administration
D. domain administration
E. admin administration
Answer: D
Explanation:
Process Separation in ServiceNow is also known as domain administration. This concept is part of the broader domain separation feature, which allows you to separate data, processes, and administrative tasks into logical groupings called domains. This is particularly useful for Managed Service Providers (MSPs) or large enterprises that need to manage multiple clients or departments within a single ServiceNow instance. Domain separation ensures that each domain can have its own set of data, processes, and administrative controls, providing a high level of customization and security.
For more detailed information, you can refer to the following resources:
• ServiceNow Support Article on Domain Separation
• Understanding Domain Separation in ServiceNow

3.Which role restricts access and allows for managing items in a domain-separated catalog?
A. catalog_manage_admin
B. catalog admin
C. catalog_manager
D. domain_catalog_admin
Answer: D
Explanation:
The role domain_catalog_admin is specifically designed to manage items within a domain-separated catalog in ServiceNow. This role restricts access and allows for the management of catalog items, ensuring that only users with the appropriate permissions can make changes within their designated

domain. This is crucial for maintaining data privacy and integrity across different domains, especially in environments where multiple customers or departments are served by a single ServiceNow instance.
Reference:
• ServiceNow Domain Separation and Service Catalog1
• ServiceNow Product Documentation on Domain Separation2

4.Which of the following is a good practice to allow Service Providers to view all customer data?
A. Setup a domain contains relationship
B. Put customer data in Global
C. No action required
D. Setup a visibility group
Answer: A
Explanation:
Setting up a domain contains relationship is a good practice to allow Service Providers to view all customer data. This approach leverages ServiceNow's domain separation capabilities, which enable data segregation and access control across different domains. By configuring a domain contains relationship, you can ensure that Service Providers have the necessary visibility into customer data while maintaining proper data governance and security.
Reference: • ServiceNow Domain Separation Documentation
• ServiceNow Knowledge Base Article

5.Name the methods available to provide data access to a user outside of their domain hierarchy.
Choose 2 answers
A. Contains
B. Domain scope
C. Access Control Lists
D. sys_visibility.domain system property
E. Visibility
Answer: CD
Explanation:
In ServiceNow, providing data access to a user outside of their domain hierarchy can be achieved through the following methods:
1. Access Control Lists (ACLs): ACLs are used to define permissions for accessing data within ServiceNow. By configuring ACLs, you can grant specific users or groups access to data outside their domain hierarchy. This is done by setting up rules that allow or deny access based on various conditions, such as roles, user attributes, or specific field values1.
2. sys_visibility.domain system property: This system property can be configured to control the visibility of records across different domains. By setting this property, you can define which domains' data should be visible to users outside their own domain hierarchy. This allows for more granular control over data access and visibility2.
These methods ensure that users can access the necessary data while maintaining the integrity and security of the domain separation model.
1: ServiceNow ACL Documentation
2: ServiceNow Domain Separation Documentation