

**Exam Code: CIS-SP**

**Exam Name: ServiceNOW Certified Implementation Specialist - Service Provide**



## Exam A

### QUESTION 1

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

**Correct Answer: D**

**Section:**

**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.

\* ServiceNow Domain Separation and Service Catalog1

\* ServiceNow Product Documentation on Domain Separation2

### QUESTION 2

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

**Correct Answer: A**

**Section:**

**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.

\* ServiceNow Domain Separation Documentation

\* ServiceNow Knowledge Base Article

### QUESTION 3

To grant domain visibility to a user you can  
Choose 2 answers

- A. Associate a visibility domain to one of the user's roles
- B. Associate a visibility domain to the user record
- C. Associate a visibility domain to the user's domain
- D. Set the visibility domain's parent to the user's domain
- E. Associate a visibility domain to one of the user's groups

**Correct Answer: A, E**

**Section:**

**Explanation:**

In ServiceNow, domain visibility determines whether users from one domain can access records from another domain. To grant domain visibility to a user, you can:

A Associate a visibility domain to one of the user's roles: This allows any user with that role to see records in the associated visibility domain<sup>1</sup>.

E Associate a visibility domain to one of the user's groups: Groups grant their members the visibility domains of the group, which means when a user is part of a group, they inherit the visibility domains associated with that group<sup>1</sup>.

It's important to note that when a user leaves a group, they lose the group's visibility domains, and the use of visibility domains should be done thoughtfully as excessive use can slow performance<sup>2</sup>. Moreover, the domain hierarchy should be optimal to prevent performance issues<sup>2</sup>.

The options B, C, and D are not standard practices for granting domain visibility according to the ServiceNow documentation and best practices. Specifically, associating a visibility domain directly to a user record or setting the visibility domain's parent to the user's domain are not mentioned as recommended methods<sup>3,4,21</sup>.

#### QUESTION 4

When configuring a shared process, to avoid updating a global process a developer should:

- A. No need to worry about the domain when you are a developer
- B. Change to customer domain
- C. Change to a process domain such as TOP D Change to global domain

**Correct Answer: C**

**Section:**

**Explanation:**

When configuring a shared process in ServiceNow, it's important to ensure that the global process is not inadvertently updated. To avoid this, a developer should change to a process domain such as TOP. This is because the TOP domain is the highest level in the domain hierarchy and allows for the creation of shared processes that can be used by all subdomains without affecting the global domain. This approach aligns with best practices for maintaining clear separation between global processes and those that are domain-specific, ensuring that any modifications are contained within the intended scope.

The ServiceNow documentation on domain separation and best practices for developers emphasizes the importance of understanding the domain hierarchy and selecting the appropriate domain when making changes to shared processes. By working within a process domain like TOP, developers can leverage the benefits of domain separation to manage data, processes, and administrative tasks in a multi-tenant environment effectively.

For further details and guidelines on domain separation and process configuration, ServiceNow provides extensive documentation and resources for developers, which can be found on their official support and learning portals

#### QUESTION 5

What tables that are considered process related tables are excluded from domain separation?

Choose 3 answers

- A. UI Policies
- B. Business Rules
- C. Access Controls
- D. System Property
- E. Workflow
- F. Client Scripts
- G. Script Include

**Correct Answer: B, C, D**

**Section:**

**Explanation:**

In ServiceNow, domain separation is used to separate data, processes, and administrative tasks into logical groupings called domains. This allows for control over various aspects of this separation<sup>1</sup>. However, certain process-related tables are excluded from domain separation to maintain the integrity and functionality of the system across different domains.

\* Business Rules (B): Business rules are global by nature and are designed to apply system-wide logic before or after database operations, regardless of the domain. This is why they are excluded from domain separation.

\* Access Controls : Access controls (ACLs) define what data users can access and how they can interact with it. Similar to business rules, ACLs are also global and not domain-specific to ensure consistent security practices across the platform.

\* System Property (D): System properties are configuration settings that affect the entire ServiceNow instance. Since these settings can have far-reaching implications on the system's behavior, they are not separated by domain to avoid conflicts and ensure uniformity in configuration. These exclusions are necessary to ensure that fundamental system behaviors remain consistent and predictable, regardless of the domain context. It's important to note that while these tables are excluded from domain separation, the data within other tables can be separated and controlled as per domain requirements2.

#### QUESTION 6

With the System Property `esm_auto_account_domain_generation` set to True:

- A. Customer accounts may optionally be assigned to a domain.
- B. CSM self-service users are prevented from seeing each other's cases and requests
- C. A new domain is created automatically whenever a new account is added.
- D. A new account is created automatically whenever a new domain is added.

**Correct Answer: C**

**Section:**

**Explanation:**

When the system property `esm_auto_account_domain_generation` is set to True, it specifies that a new domain is created automatically and placed under the TOP domain whenever a new account in the Customer Service application is created. If the 'parent' field on the account form is populated and a new record is inserted, it creates that account as a subdomain of the parent. This property is particularly relevant in domain-separated environments, ensuring that new account records are properly organized within the domain hierarchy2.

#### QUESTION 7

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

**Correct Answer: C, D**

**Section:**

**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

#### QUESTION 8

What does an admin click to view only global domain process while in the global domain?

- A. Global Domain Scope



- B. Configure Domain Scope
- C. Collapse Domain Scope
- D. Revert Domain Scope

**Correct Answer: A**

**Section:**

**Explanation:**

When an admin wants to view only the global domain process while in the global domain, they need to click on the Global Domain Scope. This option allows the admin to filter and view processes that are specific to the global domain, ensuring that they are not seeing processes from other domains. This is particularly useful in a domain-separated environment where maintaining clarity and separation of processes is crucial.

\* ServiceNow Domain Separation - Basics

\* ServiceNow Domain Separation - Advanced Concepts

#### QUESTION 9

When an administrator working in a domain modifies a policy that exists in a higher domain or in global, the system automatically:

- A. Creates a new Policy and application in the current domain
- B. Modifies original policy but not current domain
- C. Creates a new record for that administrators current domain and overrides the original
- D. Modifies the module record and overrides the original

**Correct Answer: C**

**Section:**

**Explanation:**

When an administrator working in a domain modifies a policy that exists in a higher domain or in the global domain, ServiceNow automatically creates a new record for that administrator's current domain and overrides the original policy. This ensures that the changes are specific to the current domain and do not affect the policies in the higher or global domains. This behavior is part of the domain separation feature, which allows different domains to have their own customized policies and configurations without impacting each other.

For more detailed information, you can refer to the following resources:

\* ServiceNow Support Article on Domain Separation

\* Developing Domain-Separated Applications

#### QUESTION 10

What is delegated administration?

- A. Allows users without the admin role to develop applications.
- B. Allows service providers to grant admin access to their customers.
- C. Allows tasks and approvals to be handled temporarily by another user.
- D. Another name for Process Separation.

**Correct Answer: C**

**Section:**

**Explanation:**

Delegated administration in ServiceNow allows tasks and approvals to be temporarily handled by another user. This functionality is particularly useful in scenarios where the primary user is unavailable, ensuring that workflows and processes continue without interruption. It helps maintain efficiency and continuity in service management by allowing designated users to take over specific responsibilities temporarily.

\* ServiceNow Product Documentation on Delegated Administration1

\* ServiceNow Knowledge Base on Delegated Approvals and Tasks2

#### QUESTION 11

Which are required to retrieve and commit an update set?

Choose 2 answers

- A. A change request must be approved.
- B. You must be working in a non-production instance.
- C. You must have the admin role.
- D. The domain picker must be set to global.

**Correct Answer: C, D**

**Section:**

**Explanation:**

To retrieve and commit an update set in ServiceNow, certain prerequisites must be met to ensure proper management and deployment of changes across instances:

\* You must have the admin role : Having the admin role is crucial because it provides the necessary permissions to manage update sets, which includes retrieving and committing them. This role ensures that only authorized users can make significant changes to the system<sup>12</sup>.

\* The domain picker must be set to global (D): When working with domain-separated instances, the domain picker must be set to global to ensure that the update set is applied across all domains. This is important for maintaining consistency and avoiding conflicts between different domains within the instance<sup>2</sup>.

#### QUESTION 12

Given TOP as a parent domain for MSP, ACME, and Initech, and MSP contains TOP What additional domain configuration is required for UserA in MSP to read records in ACME?

- A. Add contains between MSP and ACME
- B. Add both visibility to ACME for UserA, and contains between MSP and ACME
- C. Add visibility to ACME for UserA
- D. No additional configurations

**Correct Answer: C**

**Section:**

**Explanation:**

In ServiceNow, domain separation is used to manage data visibility and access control in a multi-tenant environment<sup>1</sup>. The 'contains' relationship in domain separation defines a hierarchy where a parent domain contains child domains, and by default, users in a parent domain can see the records in child domains<sup>1</sup>.

Given that TOP is the parent domain for MSP, ACME, and Initech, and MSP contains TOP, UserA in MSP would already have visibility into TOP. However, for UserA to read records in ACME, additional configuration is required because ACME is not a child domain of MSP by default.

The correct action is to add visibility to ACME for UserA . This is typically done by configuring the user's domain membership or by adjusting the domain visibility settings to include ACME for UserA. This ensures that UserA can access records in ACME while still being primarily associated with the MSP domain<sup>1</sup>.

The 'contains' relationship between MSP and ACME (A) is not necessary because it would imply a hierarchical relationship that does not reflect the given structure. Adding both visibility to ACME for UserA and contains between MSP and ACME (B) is also not required and could potentially create an incorrect domain hierarchy. No additional configurations (D) would not suffice as it would not grant UserA the access needed to read records in ACME.

#### QUESTION 13

In a new domain separated instance, which data will a user in customer Domain X definitely have visibility to?

Choose 2 answers

- A. Primary Domain
- B. Parent domains of Domain X
- C. Child domains of Domain X
- D. Default Domain
- E. Domain X

**Correct Answer: C, E**



**Section:****Explanation:**

In ServiceNow, domain separation is used to segregate data, processes, and administrative tasks into logical groupings called domains. This allows for control over data visibility and operations within an instance. When it comes to data visibility:

\* Domain X: A user in Domain X will definitely have visibility to their own domain, as this is the primary context in which they operate<sup>1</sup>.

\* Child domains of Domain X: Users can view data in their home domain (Domain X) and any child domains of that home domain. This is because child domains inherit permissions and visibility from their parent domains, allowing users in a parent domain to see data in the child domains<sup>1</sup>.

However, users do not have access to data present in their parent domains or other unrelated domains by default. The primary domain and default domain are typically reserved for global or top-level administrative purposes and are not automatically visible to users in customer domains unless specific permissions are granted<sup>2</sup>.

It's important to configure domain separation carefully to ensure that users have the appropriate level of access to data necessary for their roles while maintaining the security and integrity of the data across the instance<sup>3</sup>.

**QUESTION 14**

If a business rule exists in the parent domain and a separate non-overriding business rule exists in the child domain, which rule will run for the child domain?

- A. The parent rule will run
- B. Both rules will run
- C. The child rule will run
- D. Neither rule will run

**Correct Answer: B****Section:****Explanation:**

In ServiceNow, domain separation allows for the partitioning of data, processes, and administrative tasks into distinct domains within the same instance. When it comes to business rules, if a business rule exists in the parent domain and another non-overriding business rule exists in the child domain, both rules will be executed for the child domain<sup>1</sup>.

This behavior is part of the domain hierarchy logic, where the child domain inherits the properties and rules of its parent unless explicitly overridden. Since the business rule in the child domain is non-overriding, it does not cancel or replace the parent domain's rule. Instead, it adds to the logic that will be processed when the conditions for the business rule are met.

Therefore, when an action occurs that triggers the business rules, the system will first run the business rule from the parent domain followed by the business rule from the child domain. This ensures that the foundational logic set by the parent domain is always applied, while still allowing for additional, domain-specific customizations in the child domains<sup>2</sup>.

It's important to note that this behavior can be controlled and configured according to the needs of the organization, and understanding the implications of domain inheritance is crucial for proper domain separation management in ServiceNow<sup>3</sup>.

**QUESTION 15**

What is the first step an admin must perform before using domain-separation for Service Catalog items?

- A. add the sysoverrides field to the catalog table
- B. assign catalog admin role to catalog administrators
- C. publish the catalog items to each domain
- D. activate the Service Catalog Domain Separation plugin

**Correct Answer: D****Section:****Explanation:**

Before using domain separation for Service Catalog items, the first step an administrator must perform is to activate the Service Catalog - Domain Separation plugin (com.glideapp.servicecatalog.domain\_separation). This plugin enables domain separation within the Service Catalog, allowing for the separation of data, processes, and administrative tasks into logical groupings called domains<sup>1</sup>. By activating this plugin, the admin ensures that the Service Catalog is prepared to handle the complexities of a domain-separated environment, which is essential for maintaining data integrity and proper access controls across different domains<sup>2</sup>.

**QUESTION 16**

On a new standalone table, what domain will a new record be created in by default?

- A. The users home domain
- B. The user's current session domain
- C. The records domain
- D. The domain of the referenced company

**Correct Answer: B**

**Section:**

**Explanation:**

In ServiceNow, when a new record is created on a standalone table, the domain of the new record is set to the user's current session domain by default. This means that the domain context in which the user is operating at the time of record creation determines the domain assignment for that record. This behavior ensures that the data is correctly categorized within the domain structure, adhering to the visibility and access controls that have been established.

The concept of domain separation in ServiceNow is integral to its multi-tenancy model, allowing for data, processes, and administrative tasks to be segregated across different domains within a single instance. This is particularly useful for managed service providers (MSPs) who need to maintain distinct operational environments for multiple customers or departments within the same ServiceNow instance.

For a new standalone table, unless explicitly defined otherwise, the system defaults to using the user's current session domain for new records. This is supported by ServiceNow's documentation on domain separation best practices and the management of data within domains<sup>12</sup>. It's important to note that while the default behavior is as described, administrators have the ability to configure domain rules and behaviors to suit specific organizational needs.

#### QUESTION 17

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

**Correct Answer: D**

**Section:**

**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.

\* ServiceNow Domain Separation - Advanced Concepts and Configurations

\* Understanding Domain Separation - Basics

#### QUESTION 18

Process Separation is also known as:

- A. proxy administration
- B. delegated administration
- C. process administration
- D. domain administration
- E. admin administration

**Correct Answer: D**

**Section:**

**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

#### QUESTION 19

To data separate a new table, add a field named:

- A. sys\_domain with a field type of String.
- B. sys\_domain with a reference to the Domain table.
- C. sys\_domain with a field type of Domain ID.
- D. Domain referencing the Company table.

**Correct Answer: B**

**Section:**

**Explanation:**

To data separate a new table in ServiceNow, you should add a field named sys\_domain with a reference to the Domain table. This approach leverages ServiceNow's domain separation capabilities, which allow for the segregation of data across different domains. By referencing the Domain table, you ensure that the new table can properly segregate data based on domain, maintaining data integrity and security.

- \* ServiceNow Domain Separation Documentation
- \* ServiceNow Knowledge Base Article

#### QUESTION 20

What is the mechanism for placing records in the Default domain?

- A. Business Rules
- B. Domain Path
- C. Process Separation
- D. Data Policy

**Correct Answer: B**

**Section:**

**Explanation:**

In ServiceNow, the mechanism for placing records in the Default domain is primarily managed through the Domain Path. The Domain Path is a hierarchical structure that determines the domain in which a record resides. When a record is created, it is assigned a domain based on the domain path of the user or process creating the record. If no specific domain is assigned, the record defaults to the "Default" domain. This mechanism ensures that records are correctly categorized and managed within the appropriate domain, maintaining the integrity of domain separation and data access controls.

For more detailed information, you can refer to the following resources:

- \* ServiceNow Domain Separation Documentation
- \* ServiceNow Knowledge Base Article

#### QUESTION 21

What is the purpose of the Domain Separation Center?

- A. Global admins ,rack domain separation activities
- B. configuring and managing domain separation
- C. domain admins to manage their specific domain
- D. configure and review domain configuration audits for errors and warnings

**Correct Answer: D**

**Section:**



**Explanation:**

The purpose of the Domain Separation Center in ServiceNow is to configure and review domain configuration audits for errors and warnings. This tool is essential for administrators to ensure that domain separation is correctly implemented and maintained. It helps in identifying and resolving any issues related to domain configurations, thereby maintaining the integrity and proper functioning of the domain-separated environment.

\* ServiceNow Domain Separation - Basics

\* ServiceNow Domain Separation - Advanced Concepts

**QUESTION 22**

The Default domain should be specifically used for which purposes?

Choose 2 answers

- A. Help identify integrations that are incorrectly creating global data
- B. contain sharable domain data across domains in an instance
- C. Capture records with no domain on tables that should not have global data
- D. to be configured as the Primary domain for an instance
- E. contain the default process for an instance

**Correct Answer: A, C**

**Section:****Explanation:**

The Default domain in ServiceNow is specifically used for the following purposes:

1. Help identify integrations that are incorrectly creating global data: The Default domain can be used to track and identify any integrations that are mistakenly creating data in the global domain instead of the intended specific domain. This helps in maintaining data integrity and ensuring that data is correctly segregated.
2. Capture records with no domain on tables that should not have global data: The Default domain is also used to capture records that do not have a domain specified on tables where global data should not be present. This ensures that such records are not incorrectly placed in the global domain, maintaining the separation and security of data.

For more detailed information, you can refer to the following resources:

\* ServiceNow Support Article on Domain Separation

\* Developing Domain-Separated Applications

**QUESTION 23**

Which represents the direction in the domain hierarchy in which can you see data?

- A. You can see data in child domains of your current domain (downstream)
- B. You can see data in parent domains of your current domain (upstream).
- C. You can only see data in your current domain.
- D. You can see data from parents and children of your current domain.

**Correct Answer: A**

**Section:****Explanation:**

In ServiceNow, domain separation allows for hierarchical data visibility. Users in a parent domain can see data in their child domains, which is referred to as downstream visibility. This ensures that higher-level domains have access to the data of their subdomains, facilitating centralized management and oversight. However, users in child domains cannot see data in their parent domains (upstream) or sibling domains unless explicitly granted access.

\* ServiceNow Domain Separation Documentation1

\* ServiceNow Knowledge Base on Domain Separation2

**QUESTION 24**

To extend a data separated base table and have the table extension also be data separated, you must:

- A. Add sys\_domain, sys\_overrides, and Domain Path fields.
- B. Add a sys\_domain and sys\_overrides field.
- C. Extend the table and it will be data-separated automatically.
- D. Add a sys\_domain field.

**Correct Answer: A**

**Section:**

**Explanation:**

To extend a data-separated base table and ensure that the table extension is also data-separated, you must add the sys\_domain, sys\_overrides, and Domain Path fields. This ensures that the new table inherits the domain separation properties of the base table, maintaining data integrity and security across different domains.

- \* sys\_domain: This field references the Domain table and is essential for domain separation.
- \* sys\_overrides: This field is used to manage overrides in the domain-separated environment.
- \* Domain Path: This field helps in maintaining the hierarchical structure of domains.
- \* ServiceNow Domain Separation Documentation
- \* ServiceNow Knowledge Base Article

#### QUESTION 25

Even though the Inbound Actions table has a domain field, records in this table should all be placed in this single location within the domain hierarchy.

- A. Default
- B. Top
- C. Service Provider
- D. Global

**Correct Answer: D**

**Section:**

**Explanation:**

In ServiceNow, even though the Inbound Actions table has a domain field, records in this table should all be placed in the Global domain. This is because inbound actions, such as inbound email actions, are designed to be accessible across the entire platform, regardless of the specific domain. By placing these records in the Global domain, ServiceNow ensures that the actions can be executed and managed universally, without domain-specific restrictions.

For example, if an inbound email action creates an incident, the system creates the incident in the same domain as the user in the Caller field. If that user is not in the User [sys\_user] table, the incident is placed in the Global domain1.

This approach maintains the integrity and accessibility of inbound actions across the platform.

1: ServiceNow Inbound Email Actions Documentation

#### QUESTION 26

Process Domains are used to consolidate process updates for easy maintenance. What is the recommendation for handling such domains?

- A. Update the Global processes rather than creating overrides in the process domain
- B. Create overrides in the process domain or update Global processes
- C. Creating overrides in the process domain and update Global processes
- D. Create overrides in the process domain rather than updating Global processes

**Correct Answer: D**

**Section:**

**Explanation:**

When handling process domains in ServiceNow, the recommended approach is to create overrides in the process domain rather than updating the global processes. This strategy ensures that any customizations or specific requirements for a particular domain do not interfere with the global processes, which are intended to be standard and consistent across the entire organization.



Creating overrides in the process domain allows for more granular control and flexibility, enabling specific adjustments without impacting the overall system's integrity. This approach aligns with best practices for maintaining system stability and ensuring that updates or changes are isolated to the relevant domain.

For more detailed information, you can refer to the following resources:

- \* ServiceNow Learning Portal
- \* ServiceNow Knowledge Base
- \* ServiceNow Developer Portal

#### QUESTION 27

Select the recommended approach to Domain Separation

- A. 50% or more Standard. 25% or more data-driven, Less than 25% Configuration
- B. 80% or more data-driven. 15% or more Standard. Less than 5% Configuration
- C. 70% or more Standard. 25% or more data-driven. Less than 5% Configuration
- D. 80% or more Standard, 15% or more data-driven, Less than 5% Configuration

**Correct Answer: D**

**Section:**

**Explanation:**

ServiceNow recommends a domain separation approach that maximizes the use of standard configurations while minimizing custom configurations. This approach ensures maintainability, scalability, and ease of upgrades.

The recommended approach is:

- \* 80% or more Standard: Utilizing out-of-the-box (OOTB) configurations as much as possible to leverage ServiceNow's built-in capabilities and best practices.
- \* 15% or more data-driven: Using data-driven configurations to adapt to specific business needs without extensive custom coding.
- \* Less than 5% Configuration: Minimizing custom configurations to reduce complexity and potential issues during upgrades.

This strategy aligns with ServiceNow's best practices for domain separation, ensuring that the system remains robust and easier to manage.

1: ServiceNow Domain Separation Best Practices 2: Understanding Domain Separation in ServiceNow

#### QUESTION 28

How should you assign user record to a specific domain other than the one based on their company?

- A. Select Managed Domain, and set their domain field to the desired domain.
- B. Use a Source Script on your LDAP transform.
- C. Set Default to true on their domain record.
- D. Change their Company reference to a company with the desired domain.

**Correct Answer: A**

**Section:**

**Explanation:**

To assign a user record to a specific domain other than the one based on their company, you should use the "Managed Domain" option and set their domain field to the desired domain. This method allows administrators to manually assign a user to a different domain, ensuring that the user has the appropriate access and permissions within that domain.

- \* ServiceNow Documentation on Domain Separation explains how to set the domain for a user.
- \* ServiceNow Developer Documentation provides detailed information on domain separation and managing domains.

#### QUESTION 29

Visibility can be granted to users by which of the following means:

Choose 2 answers

- A. User visibility domains
- B. Group Membership

- C. Role
- D. Default Domain

**Correct Answer: B, C**

**Section:**

**Explanation:**

Visibility in ServiceNow can be granted to users through Group Membership and Role.

\* Group Membership: Users can be assigned to specific groups, and these groups can be granted visibility to certain records or functionalities within ServiceNow. This method allows for efficient management of user permissions based on their group affiliations.

\* Role: Roles define a set of permissions that can be assigned to users. By assigning roles to users, administrators can control what users can see and do within the platform. Roles are a fundamental part of access control in ServiceNow.

\* ServiceNow User Criteria and Access Control

\* ServiceNow Group Management

### QUESTION 30

Why would you set Choice Action to Ignore on a transform field map?

- A. To avoid inserting dummy referenced records into global.
- B. To reject new rows that don't have choice values present.
- C. To insert missing rows in a referenced table.
- D. To transform a field value using a script.

**Correct Answer: A**

**Section:**

**Explanation:**

Setting the Choice Action to "Ignore" on a transform field map in ServiceNow is used to avoid inserting dummy referenced records into the global domain. When importing data, if the system encounters a reference field value that does not match any existing records, setting the Choice Action to "Ignore" will prevent the creation of a new, potentially incorrect record. Instead, the system will skip the field and leave it blank, ensuring data integrity and avoiding the clutter of unnecessary records.

For more detailed information, you can refer to the following resources:

\* ServiceNow Support Article on Transform Maps

\* Choice Action Field in ServiceNow

### QUESTION 31

If a user has the ITIL role and resides in the MSP domain, which is true?

- A. They have that role in all domains they have access to.
- B. They may be granted the Admin role in other domains.
- C. They can administer other domains by granting the Domain Admin role.
- D. They can be restricted to self-service in other domains by granting the Self-Service role.

**Correct Answer: A**

**Section:**

**Explanation:**

In ServiceNow, domain separation allows organizations to segregate data, processes, and administrative tasks into logical groupings called domains<sup>1</sup>. This is particularly useful for Managed Service Providers (MSPs), where multiple organizations or customers use the same ServiceNow instance but require isolation from each other<sup>2</sup>.

When a user has the ITIL role within the MSP domain, they inherently have that role across all domains they have access to. This is because roles in ServiceNow are global by default, meaning they apply across all domains unless specifically restricted<sup>3</sup>. The ITIL role is a set of permissions that typically includes the ability to manage incident, problem, and change records, which are fundamental to IT service management.

The other options, such as being granted the Admin role in other domains (B), administering other domains by granting the Domain Admin role, or being restricted to self-service in other domains by granting the Self-Service

role (D), are actions that require explicit configuration by an administrator with the appropriate level of access and are not automatic outcomes of having the ITIL role in the MSP domain<sup>4</sup>. It's important to note that while the ITIL role may be global, access to specific records and the ability to perform certain actions can still be controlled within each domain through ACLs (Access Control Lists) and other domain-specific configurations<sup>1</sup>.

### QUESTION 32

What does the system property glide.sys.domain.delegated\_administration do?

- A. Allow another user to handle approvals and task assignments, for a specified time frame.
- B. Allow users without a system admin role to develop applications.
- C. Enable Process Separation
- D. A Allow customer admins to safely configure their own domains without impacting others.

**Correct Answer: D**

**Section:**

**Explanation:**

The system property glide.sys.domain.delegated\_administration is designed to empower customer administrators by allowing them to configure their own domains. This is crucial in a multi-tenant environment where multiple customers or departments are operating within the same ServiceNow instance but need to maintain separate configurations and data. By enabling this property, customer admins can make changes specific to their domain without the risk of affecting the configurations of other domains. This property essentially enables domain separation, which is a method of separating data into logically defined domains.

### QUESTION 33

What type of detailed results or actions are included in the domain audit?

Choose 3 answers

- A. incorrect user domain logins
- B. escalate the errors as incidents
- C. records or configurations affected
- D. recommended actions to remedy errors and warnings
- E. ability to re-run the audit

**Correct Answer: C, D, E**

**Section:**

**Explanation:**

A domain audit in ServiceNow is a comprehensive review process that includes various actions and results to ensure the integrity and proper functioning of domain-separated environments<sup>1</sup>. The detailed results or actions included in a domain audit typically encompass:

\* Records or configurations affected : The audit identifies which records or configurations have been impacted by any issues. This includes changes to the operating system, applications, or devices, and is crucial for tracking system operations and use<sup>2</sup>.

\* Recommended actions to remedy errors and warnings (D): The audit provides recommendations for corrective actions to address any identified errors and warnings. This is part of the audit management process, where continuous monitoring using indicators and CMDB evidence helps in building or editing pre-built workflows for audit engagements, control or risk assessments, and remediation<sup>3</sup>.

\* Ability to re-run the audit (E): After addressing the issues, the audit can be re-run to verify that the errors have been resolved and that the domain is functioning correctly. This ensures ongoing compliance and security within the ServiceNow environment<sup>2</sup>.

Incorrect user domain logins (A) and escalating errors as incidents (B) are not typically included in the domain audit results or actions. Instead, these aspects are more related to the operational monitoring and incident management processes within ServiceNow<sup>2</sup>.

### QUESTION 34

What's a good globally unique candidate field that could be used to populate UserID?

- A. Last Name
- B. Employee Number



- C. Email
- D. SSN

**Correct Answer: B, C, D**

**Section:**

**Explanation:**

When selecting a field to populate UserID in ServiceNow, it's crucial to choose an identifier that is globally unique to ensure that each user can be distinctly identified. The best practices for such identifiers include:

\* Employee Number: Typically, an employee number is unique to an individual within an organization and does not change, making it a reliable identifier<sup>1</sup>.

\* Email: An email address is inherently unique as it is tied to an individual and is used for communication, which also makes it a suitable candidate for UserID<sup>2</sup>.

\* SSN (Social Security Number): While SSN is unique to each individual, it's important to note that using SSN as an identifier should be approached with caution due to privacy and security concerns. However, it is unique and could technically be used to populate UserID<sup>3</sup>.

The Last Name is not a good candidate for UserID because it is not globally unique; many individuals can share the same last name and it can change over time due to personal reasons.

For further details on creating unique identifiers and best practices, ServiceNow provides documentation and guidelines which can be referred to for implementing these practices within the ServiceNow environment.

### QUESTION 35

What domain must administrators choose to apply an Updates Set?

- A. Global
- B. Top
- C. The domain of the Update Set.
- D. The parent domain of the Update Set.

**Correct Answer: A**

**Section:**

**Explanation:**

In ServiceNow, when applying an Update Set, administrators must select the Global domain. This is because Update Sets are designed to be applied from the Global domain to ensure that the changes are captured and can be moved across the instance without being restricted by domain separation<sup>1</sup>. The Global domain is the default domain where all the configuration records are created and where administrators typically work unless they switch to another domain for specific tasks<sup>1</sup>.

The Update Set system in ServiceNow is a mechanism for grouping and moving customizations from one instance to another or within the same instance. It captures the configuration changes made by administrators and bundles them into a set that can be transferred and applied elsewhere. Since the Global domain is the highest level in the domain hierarchy and is not restricted by domain-specific rules, it is the appropriate choice for applying Update Sets to ensure that the changes are universally available across all domains within the instance

