Vendor: ServiceNow

Exam Code: CAD

Exam Name: ServiceNow Certified Application Developer

Version: DEMO

QUESTION 1
Which roles grant access to source control repository operations such as importing applications from source control, or linking an application to source control? (Choose two.)

A. source_control
B. source_control_admin
C. admin
D. git_admin

Answer: AC
Explanation:
The following roles grant access to source control repository operations such as importing applications from source control, or linking an application to source control:
source_control. This is a role that allows users to perform basic source control operations, such as importing an application from a source control repository, updating an application from a source control repository, or committing changes to a source control repository. admin. This is a role that grants full access to all the features and functions of the ServiceNow platform, including source control operations. Users with this role can also perform advanced source control operations, such as creating or deleting source control repositories, configuring source control properties, or resolving conflicts.
The following roles do not grant access to source control repository operations:
source_control_admin. This is not a valid role in ServiceNow. There is no separate role for source control administration, as this function is included in the admin role. git_admin. This is not a valid role in ServiceNow. Git is a specific type of source control system that ServiceNow supports, but there is no role dedicated to Git administration.

QUESTION 2
When configuring the content of an Email Notification, which syntax should be used to reference the properties of an event triggering the Notification?

A. ${event. <property name>}
B. ${current. <property name>}
C. ${property name>.getDisplayValue()}
D. ${gs.<property name>}

Answer: A

QUESTION 3
Which one of the following is true for a Script Include with a Protection Policy value of Protected?

A. Any user with the protected_edit role can see and edit the Script Include
B. The Protection policy option can only be enabled by a user with the admin role
C. The Protection Policy is applied only if the glide.app.apply_protection system property value is true
D. The Protection Policy is applied only if the application is downloaded from the ServiceNow App Store

Answer: D
Explanation:
The following is true for a Script Include with a Protection Policy value of Protected:
The Protection Policy is applied only if the application is downloaded from the ServiceNow App Store. This is true because the Protection Policy is a feature that allows developers to protect

their Script Includes from being viewed or modified by other users when they distribute their applications through the ServiceNow App Store. The Protection Policy is only enforced when the application is installed from the App Store, not when it is developed or tested on the instance. The following are not true for a Script Include with a Protection Policy value of Protected:
Any user with the protected_edit role can see and edit the Script Include. This is false because the protected_edit role is not related to the Protection Policy, but to the Access Control (ACL) rules. The protected_edit role allows users to edit protected fields on a table, such as the script field on the sys_script table, which stores the Business Rules. The Protection Policy does not use roles to control access to the Script Includes, but a cryptographic key that is generated when the application is published to the App Store.
The Protection policy option can only be enabled by a user with the admin role. This is false because the Protection policy option can be enabled by any user who has the application_admin role for the scoped application that contains the Script Include. The application_admin role grants full access to the application development and administration within the scope of the application.
The Protection Policy is applied only if the glide.app.apply_protection system property value is true. This is false because the glide.app.apply_protection system property is not related to the Protection Policy, but to the Application Restricted Caller Access (ARCA) feature. The ARCA feature allows developers to restrict the access to the Script Includes from other applications based on the caller's scope. The glide.app.apply_protection system property determines whether the ARCA feature is enabled or disabled on the instance.

QUESTION 4
Which one of the following is true for GlideUser (g_user) methods?

A. Can be used in Client Scripts and UI Policies only
B. Can be used in Business Rules only
C. Can be used in Client Scripts, UI Policies, and UI Actions
D. Can be used in Business Rules, and Scripts Includes

Answer: C
Explanation:
The following is true for GlideUser (g_user) methods:
Can be used in Client Scripts, UI Policies, and UI Actions. This is true because GlideUser (g_user) methods are part of the client-side scripting APIs that provide information about the current user and the user's preferences. Client Scripts, UI Policies, and UI Actions are all types of client-side scripts that run in the web browser and manipulate the user interface. The following are not true for GlideUser (g_user) methods:
Can be used in Client Scripts and UI Policies only. This is false because GlideUser (g_user) methods can also be used in UI Actions, which are another type of client-side scripts that can be triggered by a user's click on a button, link, or choice.
Can be used in Business Rules only. This is false because GlideUser (g_user) methods cannot be used in Business Rules, which are server-side scripts that run on the ServiceNow platform and manipulate the database. Business Rules use a different API to access the current user information, which is GlideSystem (gs).
Can be used in Business Rules, and Scripts Includes. This is false because GlideUser (g_user) methods cannot be used in Business Rules or Script Includes, which are both server-side scripts. Script Includes are reusable units of code that can be called from any server-side script. Script Includes also use GlideSystem (gs) to access the current user information.

QUESTION 5
When configuring a module, what does the Override application menu roles configuration option do?

A. Users with the module role but without access to the application menu access the module
B. Self-Service users can access the module even though they do not have roles
C. Admin is given access to the module even if Access Controls would ordinarily prevent access
D. Users with access to the application menu can see the module even if they don't have the module role

Answer: A
Explanation:
Checkbox tooltip: "Show this module when the user has the specified roles. Otherwise the user must have the roles specified by both the application menu and the module." The following is true for the Override application menu roles configuration option when configuring a module:
Users with the module role but without access to the application menu access the module. This is true because the Override application menu roles option allows users to bypass the application menu role requirement and access the module directly if they have the module role. For example, if a module has the itil role and the Override application menu roles option enabled, and the application menu has the admin role, then a user who has the itil role but not the admin role can still access the module. The following are not true for the Override application menu roles configuration option when configuring a module:
Self-Service users can access the module even though they do not have roles. This is false because the Override application menu roles option does not grant access to the module to users who do not have any roles. Self-Service users are users who do not have any roles assigned to them and can only access the Self-Service portal and the Knowledge Base. To access the module, users need to have at least the module role.
Admin is given access to the module even if Access Controls would ordinarily prevent access. This is false because the Override application menu roles option does not override the Access Control (ACL) rules that apply to the module. Access Control rules are used to restrict the access to the data and functionality of the ServiceNow platform based on the user's roles and conditions.
Admin is a role

QUESTION 6
Which platform feature can be used to determine the relationships between field in an Import Set table to field in an existing ServiceNow table?

A. Business Service Management Map
B. Data Sources
C. Transform Map
D. CI Relationship Builder

Answer: C
Explanation:
The following platform feature can be used to determine the relationships between fields in an Import Set table to fields in an existing ServiceNow table:
Transform Map. This is a feature that defines the mapping between the fields of an Import Set table and the fields of a target table, such as incident, problem, or user. A transform map also specifies the logic and rules for transforming the imported data, such as coalescing, scripting, or applying data policies. The following platform features are not used to determine the relationships between fields in an Import Set table to fields in an existing ServiceNow table:
Business Service Management Map. This is a feature that provides a graphical representation of the configuration items (CIs) and their relationships in the Configuration Management Database (CMDB). A Business Service Management Map can be used to visualize the impact of incidents, changes, or problems on the CIs and the services they support.
Data Sources. This is a feature that defines the connection and authentication information for an external data source, such as a file, a JDBC database, or a web service. A data source is used to import data from the external source into an Import Set table.

CI Relationship Builder. This is a feature that creates relationships between CIs in the CMDB based on predefined or custom rules. A CI Relationship Builder can be used to populate the CMDB with the dependencies and connections between the CIs.

QUESTION 7
When configuring a REST Message, the Endpoint is:

A. The commands to the REST script to stop execution
B. The URI of the data to be accessed, queried, or modified
C. Information about the format of the returned data
D. The response from the provider indicating there is no data to send back

Answer: B
Explanation:
When configuring a REST Message, the Endpoint is:
The URI of the data to be accessed, queried, or modified. This is the correct answer because the Endpoint is the part of the REST Message that specifies the location and the resource of the REST provider. The Endpoint is composed of the base URL and the resource path, which can include query parameters or variables.
The following are not correct definitions of the Endpoint when configuring a REST Message:
The commands to the REST script to stop execution. This is not correct because the commands to the REST script to stop execution are not part of the REST Message, but of the Scripted REST API, which is a feature that allows users to create custom REST endpoints on the ServiceNow platform. The commands to the REST script to stop execution are methods of the RESTAPIResponse object, such as setStatusCode, setError, or complete.
Information about the format of the returned data. This is not correct because the information about the format of the returned data is not part of the Endpoint, but of the HTTP headers or the Accept field of the REST Message. The HTTP headers or the Accept field can be used to specify the content type of the response, such as JSON, XML, or HTML.
The response from the provider indicating there is no data to send back. This is not correct because the response from the provider indicating there is no data to send back is not part of the Endpoint, but of the HTTP status code or the response body of the REST Message. The HTTP status code or the response body can be used to indicate the result of the REST request, such as 200 OK, 404 Not Found, or 500 Internal Server Error.

QUESTION 8
When evaluating Access Controls, ServiceNow searches and evaluates:

A. Only for matches on the current table
B. Only for matches on the current field
C. From the most specific match to the most generic match
D. From the most generic match to the most specific match

Answer: C
Explanation:
When evaluating Access Controls, ServiceNow searches and evaluates:
From the most specific match to the most generic match. This is the correct answer because ServiceNow follows a top-down approach when evaluating Access Control (ACL) rules, which are used to restrict the access to the data and functionality of the ServiceNow platform based on the user's roles and conditions. ServiceNow starts with the most specific match, which is the field-level ACL rule, then moves to the table-level ACL rule, and finally to the global or * ACL rule. ServiceNow grants access if any of the ACL rules evaluates to true, and denies access if all of the ACL rules evaluate to false.

QUESTION 9
In a Business Rule, which one of the following returns true if the currently logged in user has the admin role?

A. g_form.hasRoleExactly(`admin')
B. gs.hasRole(`admin')
C. g_form.hasRole(`admin')
D. gs.hasRoleExactly(`admin')

Answer: B
Explanation:
Business Rule is server-side, so it uses GlideSystem API. gs.hasRoleExactly doesn't exist In a Business Rule, the following returns true if the currently logged in user has the admin role: gs.hasRole(`admin'). This is the correct answer because gs is the GlideSystem object, which provides methods for performing system operations, and hasRole is a method that checks if the current user has the specified role. For example, gs.hasRole(`admin') will return true if the current user has the admin role, and false otherwise.
The following do not return true if the currently logged in user has the admin role in a Business Rule:
g_form.hasRoleExactly(`admin'). This is not correct because g_form is the GlideForm object, which provides methods for manipulating forms, and hasRoleExactly is a method that checks if the current user has exactly the specified role and no other roles. For example, g_form.hasRoleExactly(`admin') will return true if the current user has only the admin role, and false if the current user has the admin role and any other role.
g_form.hasRole(`admin'). This is not correct because g_form is the GlideForm object, which provides methods for manipulating forms, and hasRole is a method that checks if the current user has the specified role or any role that contains the specified role. For example, g_form.hasRole(`admin') will return true if the current user has the admin role or any role that contains the admin role, such as admin_ui or admin_script.
gs.hasRoleExactly(`admin'). This is not correct because gs is the GlideSystem object, which provides methods for performing system operations, and hasRoleExactly is not a valid method of the gs object. There is no method that checks if the current user has exactly the specified role and no other roles in the gs object.

QUESTION 10
From the list below, identify one reason an application might NOT be a good fit with ServiceNow. The application:

A. Needs workflow to manage processes
B. Requires "as-is" use of low-level programming libraries
C. Requires reporting capabilities
D. Uses forms extensively to interact with data

Answer: B
Explanation:
From the list below, the following is a reason an application might not be a good fit with ServiceNow:
Requires "as-is" use of low-level programming libraries. This is the correct answer because ServiceNow is a high-level platform that abstracts away the low-level details of the underlying infrastructure and technology stack. ServiceNow provides a rich set of APIs, tools, and features that allow users to develop applications without coding or with minimal coding. However, ServiceNow does not support the direct

QUESTION 11
Identify the incorrect statement about Delegated Development in ServiceNow.

A. Administrators can grant non-admin users the ability to develop global applications.
B. Administrators can specify which application file types the developer can access.
C. Administrators can grant the developer access to script fields.
D. Administrators can grant the developer access to security records.

Answer: A
Explanation:
The incorrect statement about Delegated Development in ServiceNow is that administrators can grant non-admin users the ability to develop global applications. Delegated Development allows administrators to grant non-admin users the ability to develop scoped applications, not global applications. Global applications are accessible by all other applications and do not have a namespace prefix. Scoped applications are isolated from other applications and have a unique namespace identifier. Delegated Development provides more granular control over the developer permissions, application resources, and data access.

QUESTION 12
What is the REST API Explorer used to do?

A. Practice using REST to interact with public data providers
B. Find resources on the web for learning about REST
C. Convert SOAP Message functions to REST methods
D. Create sample code for sending REST requests to ServiceNow

Answer: D
Explanation:
One of the uses of the ServiceNow REST API Explorer is to create sample code for sending REST requests to ServiceNow. The REST API Explorer is a tool that allows you to discover and test the ServiceNow REST APIs. You can select an API endpoint, set the HTTP method, parameters, headers, and body, and then execute the request. The REST API Explorer will show you the response status, headers, and body, as well as generate sample code for various languages and frameworks, such as cURL, Java, JavaScript, Node.js, Python, Ruby, and more.

QUESTION 13
Which one of the following is true regarding Application Scope?

A. All applications are automatically part of the Global scope
B. Applications downloaded from 3rd party ServiceNow application developers cannot have naming conflicts
C. Any developer can edit any application
D. Developers can choose the prefix for a scope's namespace

Answer: B
Explanation:
The correct statement regarding Application Scope is that applications downloaded from 3rd party ServiceNow application developers cannot have naming conflicts. Application Scope is a feature that identifies and isolates applications and their related artifacts from other applications. Each scoped application has a unique namespace identifier that consists of a prefix and a scope name.

This prevents cross-application name collisions and ensures that only authorized scripts can access or modify data in a scoped application.

QUESTION 14
Which one of the following is the baseline behavior of a table in a privately-scoped application?

A. The table and its data are not accessible using web services
B. Any Business Rule can read, write, delete, and update from the table
C. Only artifacts in the table's application can read from the table
D. All application scopes can read from the table

Answer: D
Explanation:
The baseline behavior of a table in a privately-scoped application is that all application scopes can read from the table. A privately-scoped application is an application that restricts write access to its tables and resources to scripts within the same scope. However, read access is allowed by default for all scopes, unless the administrator explicitly denies it using an Access Control rule. This allows for data sharing between different applications while maintaining data integrity and security.

QUESTION 15
Which one of the following is NOT a purpose of application scoping?

A. Provide a relationship between application artifacts
B. Provide a way of tracking the user who developed an application
C. Provide a namespace (prefix and scope name) to prevent cross application name collisions
D. Provide controls for how scripts from another scope can alter tables in a scoped application

Answer: B
Explanation:
The purpose of application scoping is NOT to provide a way of tracking the user who developed an application. Application scoping does not store or display information about the user who created or modified an application or its artifacts. The purpose of application scoping is to provide a relationship between application artifacts, provide a namespace to prevent cross-application name collisions, and provide controls for how scripts from another scope can alter tables in a scoped application.

QUESTION 16
It is best practice to define the business requirements and the process(es) an application will manage as part of the application development plan. What are some of the considerations to document as part of the business process?

A. Business problem, data input/output, users/stakeholders, and process steps
B. Business problem, data input/output, project schedule, and process steps
C. Business problem, data input/output, users/stakeholders, and database capacity
D. Business problem, users/stakeholders, available licenses, and database capacity

Answer: A
Explanation:
It is best practice to define the business requirements and the process(es) an application will manage as part of the application development plan. The following are some of the

considerations to document as part of the business process:
Business problem. This is the description of the problem or opportunity that the application is intended to address or exploit. It should include the background, context, scope, and objectives of the problem or opportunity.
Data input/output. This is the specification of the data that the application will need to collect, store, manipulate, and display. It should include the data sources, formats, validations, transformations, and integrations of the data.
Users/stakeholders. This is the identification of the users and stakeholders who will be involved in or affected by the application. It should include the roles, responsibilities, expectations, and needs of the users and stakeholders.
Process steps. This is the definition of the steps and activities that the application will perform or support. It should include the inputs, outputs, triggers, conditions, and outcomes of each step or activity. The following are not some of the considerations to document as part of the business process: Project schedule. This is the estimation of the time and resources required to complete the application development project. It should include the milestones, deliverables, dependencies, and risks of the project. This is not part of the business process, but part of the project management plan. Database capacity. This is the measurement of the amount of data that the application will generate and store in the database. It should include the data volume, growth rate, retention policy, and backup strategy of the data. This is not part of the business process, but part of the technical design and architecture of the application.
Available licenses. This is the number and type of licenses that the application will consume or require from the ServiceNow platform. It should include the license model, cost, and allocation of the licenses. This is not part of the business process, but part of the financial and legal aspects of the application.

QUESTION 17
Which of the following statements does NOT apply when extending an existing table?

A. The parent table's Access Controls are evaluated when determining access to the new table's records and fields
B. The new table inherits the functionality built into the parent table
C. The new table inherits all of the fields from the parent table
D. You must script and configure all required behaviors

Answer: D
Explanation:
You must script and configure all required behaviors Provided link has this statement: Extending an existing ServiceNow table means the new table inherits the parent table's columns as well as its business logic.
The following statements apply when extending an existing table:
The parent table's Access Controls are evaluated when determining access to the new table's records and fields. This is true because Access Control (ACL) rules are inherited from the parent table to the child table, unless the child table has its own ACL rules that override the parent table's rules. ACL rules are used to restrict the access to the data and functionality of the ServiceNow platform based on the user's roles and conditions.
The new table inherits the functionality built into the parent table. This is true because the new table inherits the business logic and the relationships from the parent table, such as Business Rules, Script Includes, UI Actions, UI Policies, and Reference Fields. Business logic and relationships are used to define the behavior and the structure of the data on the ServiceNow platform. The new table inherits all of the fields from the parent table. This is true because the new table inherits the columns and the attributes from the parent table, such as Field Name, Data Type, Default Value, and Mandatory. Columns and attributes are used to define the properties and the characteristics of the data on the ServiceNow platform.
The following statement does not apply when extending an existing table:

You must script and configure all required behaviors. This is false because you do not have to script and configure all required behaviors when extending an existing table, as some of the behaviors are already inherited from the parent table, as explained above. However, you can script and configure additional or customized behaviors for the new table, such as adding new fields, creating new Business Rules, or modifying existing UI Actions.

QUESTION 18
Which of the following CANNOT be debugged using the Field Watcher?

A. Business Rules
B. Script Includes
C. Client Scripts
D. Access Controls

Answer: B
Explanation:
The Field Watcher is a debugging tool that allows you to monitor the values of fields on a form as they change due to scripts or other actions. It can be used to debug Business Rules, Client Scripts, and Access Controls, but not Script Includes. Script Includes are server-side scripts that define reusable functions and classes. They are not associated with any specific field or form, and therefore cannot be watched by the Field Watcher.

QUESTION 19
Which objects can be used in Inbound Action scripts?

A. current and previous
B. current and email
C. current and event
D. current and producer

Answer: B
Explanation:
Inbound Action scripts are server-side scripts that run when an email is received by the system. They can use the current object to access the record that is created or updated by the email, and the email object to access the properties and methods of the email message. The previous and event objects are not available in Inbound Action scripts. The producer object is only available in Record Producer scripts, which are used to create records from a service catalog item.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**