SAP
C_CPE
SAP Certified - Backend Developer - SAP Cloud Application Programming Model

Latest Version: 4.0

1. Unified Scenario Exam
2. Micro Skill Drill Exam

Topic: 1
Micro Skill Drill Exam

Question: 1

A backend developer is onboarding to a CAP extension project for a commercial cleaning services company. The repository contains generated artifacts, service definitions, and a project script used by the team before validation. The application starts locally, but the validation task fails because the exposed service still reflects a removed entity that no longer exists in the current model.
The developer's workspace contains stale generated output from an earlier branch, while the current repository model and service definition have already been updated. The task requires validating the current project artifact state before any SAP BTP deployment package is created. The observable artifact is a mismatch between the current source model and generated service output in the development tooling environment.
What is the best corrective action before preparing the deployment package?
Response:

A. Delete the removed entity from the deployed runtime after packaging so the platform state matches the latest source model.
B. Regenerate the project artifacts from the current repository baseline and rerun local service validation before packaging.
C. Keep the stale generated output because it proves the previous service version can still start successfully.
D. Add the removed entity back into the source model so the generated output and current repository state match again.

Answer: B

Explanation:
Feedback:
This option corrects the development artifact dependency before deployment. The current repository baseline, generated artifacts, service metadata, local execution result, and validation output must align before the extension package can be trusted.

Question: 2

A CAP extension for a regional clinical training provider exposes trainee remediation records through a secured service on SAP BTP. The application launch succeeds for the assigned training supervisor, and authentication completes through the expected identity flow. During validation, the service rejects

remediation updates with an authorization error even though the supervisor has the required role collection.
The token trace shows the role collection assignment exists, but the CAP service receives a token that does not contain the role claim expected by the update rule. The task requires preserving service-level authorization while proving that the deployed update operation works for the intended supervisor group. The observable artifact is a trust-and-claim propagation mismatch between successful login and backend service execution.
Which corrective action best satisfies the validation requirement?
Response:

A. Align the security configuration so the required role claim is propagated to the CAP service before the update rule is evaluated.
B. Remove the update authorization rule because the supervisor can already authenticate and launch the application successfully.
C. Assign the supervisor a broad platform administrator role so the update request can pass regardless of missing business claims.
D. Move the remediation update check into the UI so the CAP service no longer needs to evaluate the supervisor role claim.

Answer: A

Explanation:
Feedback:
This option corrects the authorization dependency at the correct layer. User assignment, token content, role-claim propagation, CAP update rule evaluation, service execution, and validation evidence must align before the secured update can pass.

Question: 3

A CAP extension for a corporate travel audit team exposes reimbursement exception records through a secured service on SAP BTP. A travel auditor can open the application and review exceptions for the assigned cost center. During validation, the same user can approve an exception belonging to another cost center by sending the exception identifier directly to the approval action.
Authentication succeeds, and the user has the travel-auditor role, but the action checks only the role and does not compare the exception's cost center with the auditor's assigned scope. The task requires preserving normal exception review while preventing cross-cost-center approval. The observable artifact is an operation-level authorization gap caused by missing business-scope validation during action execution.
Which corrective action best satisfies the authorization validation requirement?
Response:

A. Hide exceptions from other cost centers in the generated UI so auditors cannot easily select out-of-scope records.
B. Assign auditors access to all cost centers so the approval action matches the current service behavior.
C. Enforce cost-center scope validation inside the CAP approval action before allowing the approval state to be persisted.

D. Remove approval validation because successful display access already proves the auditor can use the application.

Answer: C

Explanation:
Feedback:
This option corrects the authorization enforcement layer. User identity, assigned cost-center scope, submitted exception identifier, record ownership check, approval execution, persisted state, and validation evidence must align before approval is allowed.

Question: 4

A CAP extension for a regional employee relocation provider exposes relocation exception records through a secured service on SAP BTP. A relocation coordinator can open the application and display exceptions for the assigned business unit. During validation, the same user can execute a “release relocation allowance” action for a record marked executive-controlled by submitting the exception identifier directly to the service action.
Authentication succeeds, and the coordinator has the standard relocation-review role, but the action checks only the user’s general role and not the executive-controlled classification of the submitted record. The task requires preserving normal relocation work while restricting executive-controlled allowance release to authorized compensation leads. The observable artifact is a classification-sensitive authorization gap during action execution.
Which corrective action best satisfies the authorization validation requirement?
Response:

A. Hide executive-controlled exceptions in the generated UI so relocation coordinators cannot easily select restricted records.
B. Assign relocation coordinators the compensation lead role so the current release behavior matches restricted records.
C. Enforce classification-sensitive authorization inside the CAP release action before allowing the allowance state to be persisted.
D. Remove release-action validation because successful display access already confirms the coordinator can use the application.

Answer: C

Explanation:
Feedback:
This option corrects the authorization enforcement layer. User identity, assigned role scope, submitted record classification, release authorization check, persisted allowance state, and validation evidence must align before release is allowed.

Question: 5

A CAP extension for a private healthcare network exposes equipment service history through a secured service on SAP BTP. A biomedical technician can open the application and read general equipment records. During validation, the same technician can execute a maintenance-close action for devices assigned to another facility, even though the user should close only records within the assigned facility scope.
The role collection is assigned correctly, and authentication succeeds, but the service action checks only whether the user has the technician role. It does not evaluate the facility assignment carried in the request context. The task requires preserving technician access while enforcing facility-level restrictions during action execution. The observable artifact is an operation-level authorization gap after successful role-based access.
Which corrective action best satisfies the validation requirement?
Response:

A. Hide records from other facilities in the UI list so technicians are less likely to close the wrong maintenance record.
B. Enforce facility-scope validation inside the CAP action before allowing the maintenance-close operation to complete.
C. Assign every technician access to all facilities so the current close action behavior matches the authorization model.
D. Remove the close action from the service and require facility supervisors to update maintenance status outside the extension.

Answer: B

Explanation:
Feedback:
This option corrects the authorization dependency at the action layer. User identity, technician role, facility assignment, action input, service authorization check, status update, and validation evidence must align before the close operation succeeds.

Question: 6

A CAP extension for a laboratory equipment service company exposes maintenance inspection records through a SAP Fiori elements UI. The CAP service returns inspection records correctly, and the deployed endpoint responds in the acceptance environment. During validation, the generated object page opens, but the inspection notes section remains empty even though related note records exist in the service response.
The developer confirms that the related notes are available through the CAP service, but the UI metadata does not represent the relationship as a section on the object page. The task requires validating a metadata-driven SAP Fiori elements page without adding custom frontend logic. The observable artifact is a mismatch between related service data and generated object-page behavior.
Which corrective action best supports the required UI validation?
Response:

A. Add frontend code to call the notes endpoint separately and inject the results into the object page after rendering.

B. Align the CAP service relationship and UI annotations so the notes are exposed as a metadata-driven object-page section.
C. Remove the inspection notes section from validation because related records are already returned by the service endpoint.
D. Store inspection notes inside the main inspection entity so the UI does not need to resolve a related section.

Answer: B

Explanation:
Feedback:
This option resolves the issue at the service-to-UI metadata layer. The CAP service relationship, annotations, generated object page, related section rendering, and validation evidence must align for the notes to appear correctly.

Question: 7

A CAP extension for a regional freight audit office exposes carrier penalty records through a secured service on SAP BTP. A claims analyst can open the application and display penalties assigned to the analyst's carrier portfolio. During validation, the same user can execute a "reverse penalty" action for a record classified as finance-controlled by submitting the penalty identifier directly to the service action. Authentication succeeds, and the analyst has the standard claims role, but the action checks only the role and not the finance-controlled classification of the submitted record. The task requires preserving normal claims work while restricting finance-controlled reversal to authorized finance leads. The observable artifact is a classification-sensitive authorization gap during action execution.
Which corrective action best satisfies the authorization validation requirement?
Response:

A. Hide finance-controlled penalties in the generated UI so claims analysts cannot easily select restricted records.
B. Assign claims analysts the finance lead role so the current reversal behavior matches the submitted record classification.
C. Enforce classification-sensitive authorization inside the CAP reversal action before allowing the penalty state to be persisted.
D. Remove reversal-action validation because successful display access already confirms the analyst can use the application.

Answer: C

Explanation:
Feedback:
This option corrects the authorization enforcement layer. User identity, assigned role scope, submitted record classification, reversal authorization check, persisted penalty state, and validation evidence must align before reversal is allowed.

Question: 8

A CAP extension for a nonprofit donation compliance team exposes donor review records through a secured service on SAP BTP. The assigned compliance analyst can open the application and display donor reviews. During validation, the analyst exports a review list and the service includes restricted donor classification fields that should be visible only to a smaller audit lead group.
The authentication and route checks succeed, and the analyst has the standard review role. The validation trace shows that field-level restriction was not enforced when the export request was executed through the service. The task requires preserving normal review access while preventing restricted classification data from leaving the service for unauthorized users. The observable artifact is an access-scope discrepancy at the field-output layer.
Which action best resolves the validation failure while preserving the intended access model?
Response:

A. Disable export functionality for all users so restricted donor classification fields cannot be downloaded.
B. Hide the restricted fields in the SAP Fiori elements list report while leaving the service response unchanged.
C. Enforce the restricted field authorization in the CAP service output logic based on the user's assigned role scope.
D. Assign all compliance analysts the audit lead role so the exported field set matches the current service response.

Answer: C

Explanation:
Feedback:
This option corrects the authorization enforcement layer where the defect appears. User identity, assigned role scope, field-level service output, export execution, and validation evidence must align so restricted classification data is returned only to permitted users.

Question: 9

A CAP extension for a public recreation authority manages facility-incident review records in a side-by-side application on SAP BTP. The developer adds an action that should close an incident only when all related corrective tasks are completed. During validation, the action returns success, but follow-up reads show incidents closed even when one corrective task is still open.
The trace shows that the action reads the incident header and updates the closed status, but it does not retrieve the related corrective-task collection before persisting the state change. The task requires validating that CAP service action behavior respects related-record completion without modifying the SAP S/4HANA Cloud source application. The observable artifact is an invalid state transition caused by incomplete related-data evaluation during action execution.
What is the best corrective action to make the close action pass validation?
Response:

A. Change the response message to state that closed incidents may still require corrective-task review afterward.
B. Remove the corrective-task condition so incidents can be closed consistently during validation.

C. Retrieve and evaluate related corrective-task completion inside the CAP action before persisting the closed status.
D. Store corrective-task completion directly in the SAP S/4HANA Cloud source object so the CAP action avoids related-record checks.

Answer: C

Explanation:
Feedback:
This option corrects the service execution dependency. Incident retrieval, related corrective-task lookup, completion evaluation, persisted closure state, follow-up read behavior, and validation evidence must align before closure can be accepted.

Question: 10

A CAP extension for a regional tax advisory firm exposes filing exception records through a secured service on SAP BTP. A junior reviewer can open the application and display filing exceptions assigned to the reviewer's client portfolio. During validation, the same user can execute a "release adjustment" action for a high-risk exception by submitting the exception identifier directly to the service action. Authentication succeeds, and the reviewer has the standard filing-review role, but the action checks only the role and not the risk classification of the submitted record. The task requires preserving normal review work while allowing high-risk adjustment release only for senior reviewers. The observable artifact is an operation-level authorization gap caused by missing classification-sensitive validation during action execution.
Which corrective action best satisfies the authorization validation requirement?
Response:

A. Hide high-risk filing exceptions in the generated UI so junior reviewers cannot easily select restricted records.
B. Assign junior reviewers the senior reviewer role so the submitted release action matches the current service behavior.
C. Remove release-adjustment validation because successful display access already confirms the reviewer can use the application.
D. Enforce risk-classification authorization inside the CAP release action before allowing the adjustment state to be persisted.

Answer: D

Explanation:
Feedback:
This option corrects the authorization enforcement layer. User identity, assigned role scope, submitted record classification, action authorization check, persisted adjustment state, and validation evidence must align before release is allowed.
Topic: 2
Unified Scenario Exam

Question: 11

CHALLENGE 3 — Repeatable Deployment Parameter Control
A developer proposes inserting pilot subaccount endpoints directly into the CAP service implementation to meet the fixed onboarding date. The release manager expects the same code line to move from test to pilot.
Which response best balances delivery speed with lifecycle discipline?
Response:

A. Accept the hardcoded endpoint for the pilot and create a cleanup task after the first regional rollout.
B. Store the endpoint in a UI annotation so the backend service implementation remains unchanged.
C. Externalize environment-specific values through controlled deployment or runtime configuration and validate them before promotion.
D. Create a separate Git branch for each subaccount and maintain different endpoint values in each branch.

Answer: C

Explanation:
Feedback:
Externalized deployment or runtime configuration supports the fixed pilot timeline without changing source code per environment. It also preserves repeatability for later rollout waves and enables validation before release.

Question: 12

CHALLENGE 3 — Repeatable Deployment Parameter Control
Before pilot validation begins, the team must prove that deployment configuration is repeatable and does not rely on manual subaccount adjustment.
Which validation checkpoint gives the strongest evidence?
Response:

A. The application builds successfully from the developer's local workspace after endpoints are updated manually.
B. The same Git branch deploys to test and pilot targets using controlled environment values, and required runtime settings are verified before execution.
C. The pilot subaccount contains the required destination after a platform administrator manually creates it during rehearsal.
D. The service implementation logs the active endpoint value when the application starts.

Answer: B

Explanation:
Feedback:

This validates both code-line consistency and controlled environment-specific configuration. It also confirms that required settings are checked before pilot execution, which supports repeatable delivery.

Question: 13

CHALLENGE 4 — Role-Scoped Access for Partner Review
The pilot requires internal coordinators, partner supervisors, and regional reviewers to receive different visibility and action outcomes. The first authorization draft uses broad service-level restrictions because they are easier to test.
Which design choice best fits the pilot requirement?
Response:

A. Use one broad display permission for all pilot users and rely on hub filters in the Fiori elements interface.
B. Give partner supervisors regional reviewer access during peak periods and remove it after the pilot.
C. Combine role-based service permissions with hub-level visibility checks so each role receives the correct access outcome.
D. Restrict all partner supervisors to read-only access across every pilot hub to avoid accidental assignment confirmation.

Answer: C

Explanation:
Feedback:
The scenario requires different actions and visibility by role, not one broad control. Combining role-based permissions with hub-level checks supports internal, partner, and regional reviewer behavior within the same extension.

Question: 14

CHALLENGE 4 — Role-Scoped Access for Partner Review
The security team approves narrow partner access, while service operations wants partner supervisors to review capacity across neighboring hubs during peak periods.
Which option best handles this governance-vs-governance tension?
Response:

A. Prioritize operational continuity by allowing supervisors full regional visibility during peak periods.
B. Prioritize data boundary enforcement by denying all neighboring hub review, even where approved for pilot operations.
C. Define an approved limited review scope that allows neighboring hub capacity review without exposing unrelated assignment details or unrestricted actions.
D. Allow neighboring hub review only through exported reports so the CAP authorization model remains simple.

Answer: C

Explanation:
Feedback:
This balances operational continuity with approved data boundaries. A limited review scope can support peak-period capacity review while avoiding unrestricted visibility or actions.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer