SAP
C_CPI
SAP Certified - Integration Developer

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 4.0

1. Micro Skill Drill Exam
2. Unified Scenario Exam

Topic: 1
Micro Skill Drill Exam

Question: 1

A regional textile cooperative uses SAP Integration Suite / Cloud Integration to send shipment confirmation events from a supplier portal to a cloud billing service. After a controlled release, monitoring shows that the artifact is active, but failed executions cannot be separated by supplier region during operational investigation.
The payload contains the supplier region, and receiver calls fail only for one region after a new billing validation rule. The support team requires searchable runtime evidence for triage without enabling full payload tracing across all confirmations. The developer must improve operations visibility while keeping the artifact managed through the platform lifecycle.
Which action should the developer prioritize?
Response:

A. Enable full payload tracing for all shipment confirmations so support can inspect supplier region manually.
B. Create separate artifacts for each supplier region so regional failures can be identified by artifact name.
C. Add controlled runtime attribute or logging enrichment for supplier region so monitoring can filter executions without broad payload exposure.
D. Ask the supplier portal to send only confirmations from the affected region until billing validation is corrected.

Answer: C

Explanation:
Feedback:
This addresses the correct monitoring and validation layer because the supplier region exists in the message but is not available for filtering. Controlled runtime enrichment supports triage while avoiding broad payload inspection.

Question: 2

A nonprofit fundraising organization publishes a donor lookup API through SAP Integration Suite for approved campaign applications. A new mobile campaign app authenticates and receives successful responses, but API analytics show its traffic recorded under a shared technical consumer instead of the app-specific consumer entry.

The API owner needs usage to remain traceable by application because access reviews and consumption limits depend on consumer identity. The developer must correct attribution without exposing a direct backend endpoint or disabling the existing authentication flow. The environment requires managed API behavior and operational visibility.
What should the developer validate first?
Response:

A. Validate the app-specific API credential or subscription binding so calls are associated with the correct managed consumer identity.
B. Increase the shared technical consumer's quota so the new mobile app has enough capacity during campaign periods.
C. Disable API analytics because successful responses show that the API execution path is functioning correctly.
D. Create a separate backend endpoint for the mobile campaign app so its traffic can be counted outside the managed API layer.

Answer: A

Explanation:
Feedback:
This targets the correct API management layer because the app can call the API but its usage is attributed to the wrong consumer identity. Validating the app-specific credential or subscription binding restores traceability while preserving managed authentication and policy enforcement.

Question: 3

A regional recycling authority exposes a container-status API through SAP Integration Suite for municipal apps and approved contractor systems. A new contractor application authenticates successfully, but API monitoring shows that its requests reach the backend without the contractor identifier required for response filtering.
The request initially contains the identifier, but a managed transformation policy replaces the header set before the backend routing step. The API owner requires contractor-specific filtering to remain governed through the API layer, with usage still traceable by consumer. The developer must avoid creating a direct backend endpoint.
Which action best resolves the issue?
Response:

A. Disable all transformation policies so the contractor identifier is passed unchanged to the backend service.
B. Ask the contractor application to include the identifier in the request body instead of the header.
C. Give the contractor temporary backend access until the API-layer defect is corrected.
D. Adjust the managed policy sequence so the contractor identifier is preserved for routing and filtering while API governance remains active.

Answer: D

Explanation:
Feedback:
This targets the correct API policy layer because authentication succeeds and the identifier is present before a managed policy removes it. Adjusting the policy sequence preserves contractor-specific routing and filtering while retaining governed API execution.

Question: 4

A banking technology unit is publishing an internal account reference API through SAP Integration Suite for use by several authorized application teams. The first API version is already consumed by a mobile services team. A second team now requests a response-field change that would remove a field still used by the existing mobile integration.
The developer must support the new consumer requirement while avoiding uncontrolled disruption to current consumers. The organization also wants API usage to remain discoverable and managed through the platform rather than handled by informal endpoint sharing.
Which approach best preserves API manageability and consumer stability?
Response:

A. Modify the existing API response immediately because the newest consumer requirement should define the current API contract.
B. Introduce a managed API version or compatible contract strategy so the new requirement can be supported without breaking the existing consumer.
C. Share the backend endpoint directly with the second team so the published API does not need to change.
D. Ask the mobile services team to stop using the field before any API change is documented or versioned.

Answer: B

Explanation:
Feedback:
This is the best approach because it preserves managed API lifecycle behavior and consumer stability. A versioned or compatibility-aware contract strategy allows the platform-managed API to evolve while avoiding an uncontrolled breaking change for existing consumers.

Question: 5

A seed distribution cooperative uses SAP Integration Suite / Cloud Integration to send seasonal allocation updates from a planning application to a cloud fulfillment service. The integration flow validates and maps the message, but the fulfillment service rejects allocations when a crop variety code includes a local extension segment.
The payload trace shows that the full source code is present before transformation, but the outbound request truncates the extension segment. Fulfillment requires the complete code for warehouse prioritization, while the planning application must keep its existing code structure during rollout. The developer must correct the managed artifact.
Which action best resolves the failure?

Response:

A. Ask the planning application team to remove local extension segments before sending allocation updates.
B. Configure the fulfillment service to assign a default warehouse priority when the extension segment is missing.
C. Correct the transformation logic so the complete crop variety code, including the extension segment, is passed in the outbound request.
D. Route records with local extension segments to manual handling until the rollout is complete.

Answer: C

Explanation:
Feedback:
This resolves the issue at the transformation layer because the full crop variety code exists before mapping but is incomplete in the outbound request. Correcting transformation logic preserves the source structure and satisfies the receiver contract.

Question: 6

A regional logistics provider is building an integration flow in SAP Integration Suite / Cloud Integration to pass shipment status updates from a partner API into a cloud-based order visibility process. The development tenant shows the artifact as activated, but test executions intermittently fail after a recent update to the endpoint configuration.
The monitoring view shows that the message is received successfully, but the outbound call fails only when the updated receiver configuration is used. The project team has a constraint that no unmanaged workaround can be introduced because the same flow will later be promoted through controlled platform lifecycle stages. The environment is platform-based, with mixed web tooling and API-oriented execution.
What should the integration developer validate first to resolve the failure at the correct system layer?
Response:

A. Rebuild the integration flow from a copied artifact and activate the copied version to remove any hidden runtime inconsistency.
B. Validate whether the receiver endpoint configuration, binding values, and authorization context used by the activated artifact are aligned with the updated target API.
C. Increase the retry behavior for the outbound call so failed executions can complete after the target service becomes available.
D. Add an additional mapping step before the receiver call to ensure the shipment status payload is normalized before transmission.

Answer: B

Explanation:
Feedback:

This action targets the correct execution layer because the artifact is activated and the message enters the flow, but the outbound call fails under the updated receiver configuration. Validating endpoint settings, binding values, and authorization context confirms whether the configured runtime dependency matches the target API behavior before message execution is judged as defective.

Question: 7

A regional field-equipment cooperative exposes a service-window API through SAP Integration Suite for internal dispatchers and approved maintenance partners. A maintenance partner authenticates successfully, but API monitoring shows that requests for emergency service windows are being returned with standard-window availability.
The backend service supports both service-window types. The request includes an emergency indicator when it enters the API proxy, but a managed response-shaping policy applies the standard response template before the partner receives the result. The API owner requires emergency-window access to remain governed, traceable, and limited to approved partners without exposing a direct backend endpoint.
Which action best resolves the response behavior?
Response:

A. Give the maintenance partner direct backend access for emergency service-window requests until response shaping is redesigned.
B. Ask the partner to interpret standard-window responses as emergency responses when the original request included the emergency indicator.
C. Disable all managed response policies so the backend service response reaches the partner without platform processing.
D. Adjust the managed response handling so emergency-window context selects the correct response template while API governance remains active.

Answer: D

Explanation:
Feedback:
This targets the correct API response-control layer because authentication and backend capability are available while the managed response template changes the business result. Preserving emergency context for response shaping keeps access governed and returns the correct availability meaning.

Question: 8

A regional broadcasting company uses SAP Integration Suite / Cloud Integration to send program schedule changes from a cloud scheduling application to a digital publishing service. After a package update, the integration artifact is visible as the latest version in the test environment, but monitoring still shows executions using the previous route condition for weekend schedules.
The deployment record indicates that the artifact was imported successfully, yet the runtime behavior does not reflect the updated route expression. The release lead requires the developer to correct the lifecycle issue without manually changing routing logic in the target environment. The environment is platform-based with controlled artifact movement.

What should the developer validate first?
Response:

A. Validate whether the updated artifact version was activated and bound to the runtime execution configuration used in the test environment.
B. Manually edit the weekend route condition in the test environment so the runtime behavior matches the imported package.
C. Recreate the receiver connection because route conditions usually fail when target connectivity is unavailable.
D. Increase monitoring retention so older executions can be compared against the current route condition.

Answer: A

Explanation:
Feedback:
This targets the correct lifecycle and runtime layer because the artifact is imported but execution still follows the previous route condition. Validating activation and runtime binding confirms whether the promoted version is actually the version being executed.

Question: 9

A regional training-services provider exposes a course-seat API through SAP Integration Suite for internal advisors and approved employer portals. A new employer portal authenticates successfully, but API monitoring shows that waitlist requests are routed to the standard enrollment operation.
The request contains a seat-status marker when it enters the API proxy, but a managed request policy replaces the marker before route evaluation. The API owner requires waitlist access to remain governed, traceable, and limited to approved employers. The developer must not expose a direct backend operation or remove API controls.
Which action best resolves the routing issue?
Response:

A. Give the employer portal direct backend access for waitlist operations until the managed route policy is corrected.
B. Ask the employer portal to submit waitlist requests as standard enrollments so the current route can process them.
C. Adjust the managed policy sequence so the seat-status marker is preserved for route evaluation while API governance remains active.
D. Disable all managed request policies so the backend course-seat service receives each employer request unchanged.

Answer: C

Explanation:
Feedback:

This targets the correct API policy and routing layer because authentication succeeds while route context is changed before backend selection. Preserving the seat-status marker for evaluation keeps employer access governed and allows the intended backend operation to execute.

Question: 10

A regional public library network exposes a digital access API through SAP Integration Suite for kiosk applications and approved education partners. A newly onboarded education partner authenticates successfully, but requests fail before reaching the backend entitlement service.
API monitoring shows that a required partner-context header is removed by a managed policy before the backend routing rule evaluates it. The API owner requires the header to remain governed and traceable, not passed informally outside the managed API layer. The developer must correct the policy behavior while preserving authentication and usage visibility through the platform.
Which action best resolves the issue?
Response:

A. Disable all API policies so the partner-context header reaches the backend entitlement service unchanged.
B. Give the education partner a direct backend endpoint until the managed policy sequence is redesigned.
C. Ask the partner application to remove the partner-context header because it is being stripped by the API layer.
D. Adjust the managed policy sequence or header handling so the partner context remains available for governed routing and validation.

Answer: D

Explanation:
Feedback:
This addresses the correct API policy layer because authentication succeeds and the request fails only after managed header handling removes required context. Adjusting policy sequence or header handling preserves governed routing while keeping usage traceable.
Topic: 2
Unified Scenario Exam

Question: 11

CHALLENGE 1 — Order API Exposure During Partner Onboarding
A partner application calls the order-status API using its assigned credential. The backend call succeeds, but the response does not include the regional shipment attributes required by the partner contract. Internal test calls return a broader response through an older route.
Which action best validates the API exposure before partner launch?
Response:

A. Activate the existing internal pilot route for the partner because it already returns successful backend responses.

B. Confirm the partner API product, proxy route, and response handling using the partner-scoped credential.
C. Refactor all Integration Flows before testing the API proxy because payload consistency depends only on flow design.
D. Move the partner credential to the internal test user scope so both calls return the same response structure.

Answer: B

Explanation:
Feedback:
The correct action validates the API path exactly as the partner will use it, including product assignment, route selection, and response handling. The scenario shows that internal and partner-scoped calls behave differently, so partner-scope evidence is required before launch.

Question: 12

CHALLENGE 1 — Order API Exposure During Partner Onboarding
The integration developer sees that the API product contains both a draft partner route and a reused internal route from an earlier pilot. The partner credential is active, and a test call receives a valid response, but operations cannot confirm whether the response came from the partner route.
What is the best next determination?
Response:

A. Determine the effective route used by the partner credential and verify the partner response contract from that route.
B. Approve the route because any valid response confirms the API product is available to the partner.
C. Disable the API product until all marketplace partners use the same credential scope.
D. Replace API management with direct calls to Cloud Integration for the first partner release.

Answer: A

Explanation:
Feedback:
The key dependency is the effective route used by the partner credential, not only whether the API product responds. A valid response can still come from the wrong route and fail the partner contract.

Question: 13

CHALLENGE 2 — Integration Flow Routing Across Warehouse Regions
The north-region Integration Flow enriches shipment confirmations with carrier references, while the south-region flow was adapted from a cancellation notification and produces a simpler outbound structure. Both flows complete successfully in runtime monitoring.
Which validation best addresses the regional behavior before release?
Response:

A. Compare both regional flow executions for transformation, enrichment, and outbound partner message structure.
B. Accept both flows because successful runtime completion confirms the outbound message is usable.
C. Prioritize the south-region flow only because it was adapted from a simpler notification pattern.
D. Replace both regional flows with a single generic message structure to reduce monitoring variation.

Answer: A

Explanation:
Feedback:
The correct validation checks the actual modeled behavior and runtime evidence for both regions. Successful completion alone does not confirm that enrichment and outbound structures match the partner-facing requirement.

Question: 14

CHALLENGE 2 — Integration Flow Routing Across Warehouse Regions
A performance adjustment shortens response time for the high-volume partner by bypassing a check that operations uses to confirm active marketplace partner status. Test messages process faster, and the partner receives shipment updates.
How should the developer evaluate this change?
Response:

A. Keep the faster route because launch performance is the main release constraint for the high-volume partner.
B. Validate whether the performance change preserves required partner-status control and message completeness.
C. Remove all partner-status checks from regional flows and enforce access only after production activation.
D. Delay the full integration until every regional flow is rebuilt from a new template.

Answer: B

Explanation:
Feedback:
The best evaluation weighs performance against required runtime control and message completeness. The scenario states that the faster path bypasses an operational check, so speed alone cannot justify the change.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/