

ACD301 PDF Testsoftware & ACD301 Unterlage

The safer, easier way to help you pass any IT exams.

Appian ACD301 Exam

Appian Lead Developer

<https://www.passquestion.com/acd301.html>



Save **35% OFF** on ALL Exams

Coupon: 2025

35% OFF on All, Including ACD301 Questions and Answers

Pass Appian ACD301 Exam with PassQuestion ACD301 questions and answers in the first attempt.

<https://www.passquestion.com/>

1 / 18

P.S. Kostenlose 2026 Appian ACD301 Prüfungsfragen sind auf Google Drive freigegeben von DeutschPrüfung verfügbar:
<https://drive.google.com/open?id=1PTRHC-g36mIT8kLQP1hTRwLcaddYnl7F>

Viele auf die Appian ACD301 Prüfung vorbereitende Prüfungsteilnehmer haben schon ins Berufsleben eingestiegen. Und manche davon stehen jetzt vor Herausforderungen anderer Sachen. Deshalb bieten wir die Prüfungsteilnehmer die effizienteste Methode für die Vorbereitung der Appian ACD301. Um Sie unbesorgt unsere Produkte kaufen zu lassen, bieten wir noch kostenlose Demos von verschiedenen Versionen der Appian ACD301. Wir haben schon zahllosen Prüfungskandidaten geholfen, Appian ACD301 Prüfung zu bestehen. Wir hoffen Ihnen, auch die Vorteile unserer Produkte zu empfinden.

Appian ACD301 Prüfungsplan:

Thema	Einzelheiten
Thema 1	<ul style="list-style-type: none">Extending Appian: This section of the exam measures skills of Integration Specialists and covers building and troubleshooting advanced integrations using connected systems and APIs. Candidates are expected to work with authentication, evaluate plug-ins, develop custom solutions when needed, and utilize document generation options to extend the platform's capabilities.

Thema 2	<ul style="list-style-type: none"> • Application Design and Development: This section of the exam measures skills of Lead Appian Developers and covers the design and development of applications that meet user needs using Appian functionality. It includes designing for consistency, reusability, and collaboration across teams. Emphasis is placed on applying best practices for building multiple, scalable applications in complex environments.
Thema 3	<ul style="list-style-type: none"> • Platform Management: This section of the exam measures skills of Appian System Administrators and covers the ability to manage platform operations such as deploying applications across environments, troubleshooting platform-level issues, configuring environment settings, and understanding platform architecture. Candidates are also expected to know when to involve Appian Support and how to adjust admin console configurations to maintain stability and performance.

>> ACD301 PDF Testsoftware <<

ACD301 Unterlage & ACD301 Vorbereitungsfragen

Die Qualität muss sich bewähren, was die Appian ACD301 von uns DeutschPrüfung Ihnen genau garantieren können, weil wir immer die Test-Bank aktualisieren. Die fachliche Erklärungen der Antworten von unserer professionellen Gruppe machen unsere Produkte der Schlüssel des Bestehens der Appian ACD301. Die Versprechung „volle Rückerstattung bei der Durchfall“, ist auch Motivation für unser Team. Wir wollen für Sie die Prüfungsunterlagen der Appian ACD301 immer verbessern. Innerhalb einem Jahr nach Ihrem Kauf, können Sie die neuesten Unterlagen der Appian ACD301 weiter genießen ohne zusätzliche Gebühren.

Appian Lead Developer ACD301 Prüfungsfragen mit Lösungen (Q26-Q31):

26. Frage

You are required to configure a connection so that Jira can inform Appian when specific tickets change (using a webhook). Which three required steps will allow you to connect both systems?

- **A. Create a Web API object and set up the correct security.**
- B. Give the service account system administrator privileges.
- **C. Configure the connection in Jira specifying the URL and credentials.**
- D. Create an integration object from Appian to Jira to periodically check the ticket status.
- **E. Create a new API Key and associate a service account.**

Antwort: A,C,E

Begründung:

Comprehensive and Detailed In-Depth Explanation: Configuring a webhook connection from Jira to Appian requires setting up a mechanism for Jira to push ticket change notifications to Appian in real-time.

This involves creating an endpoint in Appian to receive the webhook and configuring Jira to send the data.

Appian's Integration Best Practices and Web API documentation provide the framework for this process.

* Option A (Create a Web API object and set up the correct security): This is a required step. In Appian, a Web API object serves as the endpoint to receive incoming webhook requests from Jira. You must define the API structure (e.g., HTTP method, input parameters) and configure security (e.g., basic authentication, API key, or OAuth) to validate incoming requests. Appian recommends using a service account with appropriate permissions to ensure secure access, aligning with the need for a controlled webhook receiver.

* Option B (Configure the connection in Jira specifying the URL and credentials): This is essential.

In Jira, you need to set up a webhook by providing the Appian Web API's URL (e.g., `https://<appian-site>/suite/webapi/<web-api-name>`) and the credentials or authentication method (e.g., API key or basic auth) that match the security setup in Appian. This ensures Jira can successfully send ticket change events to Appian.

* Option C (Create a new API Key and associate a service account): This is necessary for secure authentication. Appian recommends using an API key tied to a service account for webhook integrations. The service account should have permissions to process the incoming data (e.g., write to a process or data store) but not excessive privileges. This step complements the Web API security setup and Jira configuration.

* Option D (Give the service account system administrator privileges): This is unnecessary and insecure. System administrator privileges grant broad access, which is overkill for a webhook integration. Appian's security best practices advocate for least-privilege principles, limiting the service account to the specific objects or actions needed (e.g., executing the Web API).

* Option E (Create an integration object from Appian to Jira to periodically check the ticket status): This is incorrect for a webhook

scenario. Webhooks are push-based, where Jira notifies Appian of changes. Creating an integration object for periodic polling (pull-based) is a different approach and not required for the stated requirement of Jira informing Appian via webhook.

These three steps (A, B, C) establish a secure, functional webhook connection without introducing unnecessary complexity or security risks.

References: Appian Documentation - Web API Configuration, Appian Integration Best Practices - Webhooks, Appian Lead Developer Training - External System Integration.

The three required steps that will allow you to connect both systems are:

* A. Create a Web API object and set up the correct security. This will allow you to define an endpoint in Appian that can receive requests from Jira via webhook. You will also need to configure the security settings for the Web API object, such as authentication method, allowed origins, and access control.

* B. Configure the connection in Jira specifying the URL and credentials. This will allow you to set up a webhook in Jira that can send requests to Appian when specific tickets change. You will need to specify the URL of the Web API object in Appian, as well as any credentials required for authentication.

* C. Create a new API Key and associate a service account. This will allow you to generate a unique token that can be used for authentication between Jira and Appian. You will also need to create a service account in Appian that has permissions to access or update data related to Jira tickets.

The other options are incorrect for the following reasons:

* D. Give the service account system administrator privileges. This is not required and could pose a security risk, as giving system administrator privileges to a service account could allow it to perform actions that are not related to Jira tickets, such as modifying system settings or accessing sensitive data.

* E. Create an integration object from Appian to Jira to periodically check the ticket status. This is not required and could cause unnecessary overhead, as creating an integration object from Appian to Jira would involve polling Jira for ticket status changes, which could consume more resources than using webhook notifications. Verified References: Appian Documentation, section "Web API" and "API Keys".

27. Frage

An existing integration is implemented in Appian. Its role is to send data for the main case and its related objects in a complex JSON to a REST API, to insert new information into an existing application. This integration was working well for a while. However, the customer highlighted one specific scenario where the integration failed in Production, and the API responded with a 500 Internal Error code. The project is in Post- Production Maintenance, and the customer needs your assistance. Which three steps should you take to troubleshoot the issue?

- A. Send the same payload to the test API to ensure the issue is not related to the API environment.
- B. Ensure there were no network issues when the integration was sent.
- C. Obtain the JSON sent to the API and validate that there is no difference between the expected JSON format and the sent one.
- D. Analyze the behavior of subsequent calls to the Production API to ensure there is no global issue, and ask the customer to analyze the API logs to understand the nature of the issue.
- E. Send a test case to the Production API to ensure the service is still up and running.

Antwort: A,C,D

Begründung:

Comprehensive and Detailed In-Depth Explanation: As an Appian Lead Developer in a Post-Production Maintenance phase, troubleshooting a failed integration (HTTP 500 Internal Server Error) requires a systematic approach to isolate the root cause—whether it's Appian-side, API-side, or environmental. A 500 error typically indicates an issue on the server (API) side, but the developer must confirm Appian's contribution and collaborate with the customer. The goal is to select three steps that efficiently diagnose the specific scenario while adhering to Appian's best practices. Let's evaluate each option:

* A. Send the same payload to the test API to ensure the issue is not related to the API environment: This is a critical step.

Replicating the failure by sending the exact payload (from the failed Production call) to a test API environment helps determine if the issue is environment-specific (e.g., Production-only configuration) or inherent to the payload/API logic. Appian's Integration troubleshooting guidelines recommend testing in a non-Production environment first to isolate variables. If the test API succeeds, the Production environment or API state is implicated; if it fails, the payload or API logic is suspect.

This step leverages Appian's Integration object logging (e.g., request/response capture) and is a standard diagnostic practice.

* B. Send a test case to the Production API to ensure the service is still up and running: While verifying Production API availability is useful, sending an arbitrary test case risks further Production disruption during maintenance and may not replicate the specific scenario. A generic test might succeed (e.g., with simpler data), masking the issue tied to the complex JSON. Appian's Post-Production guidelines discourage unnecessary Production interactions unless replicating the exact failure is controlled and justified. This step is less precise than analyzing existing behavior (C) and is not among the top three priorities.

* C. Analyze the behavior of subsequent calls to the Production API to ensure there is no global issue, and ask the customer to

analyze the API logs to understand the nature of the issue. This is essential.

Reviewing subsequent Production calls (via Appian's Integration logs or monitoring tools) checks if the 500 error is isolated or systemic (e.g., API outage). Since Appian can't access API server logs, collaborating with the customer to review their logs is critical for a 500 error, which often stems from server-side exceptions (e.g., unhandled data). Appian Lead Developer training emphasizes partnership with API owners and using Appian's Process History or Application Monitoring to correlate failures- making this a key troubleshooting step.

* D. Obtain the JSON sent to the API and validate that there is no difference between the expected JSON format and the sent one. This is a foundational step. The complex JSON payload is central to the integration, and a 500 error could result from malformed data (e.g., missing fields, invalid types) that the API can't process. In Appian, you can retrieve the sent JSON from the Integration object's execution logs (if enabled) or Process Instance details. Comparing it against the API's documented schema (e.g., via Postman or API specs) ensures Appian's output aligns with expectations. Appian's documentation stresses validating payloads as a first-line check for integration failures, especially in specific scenarios.

* E. Ensure there were no network issues when the integration was sent. While network issues (e.g., timeouts, DNS failures) can cause integration errors, a 500 Internal Server Error indicates the request reached the API and triggered a server-side failure- not a network issue (which typically yields 503 or timeout errors). Appian's Connected System logs can confirm HTTP status codes, and network checks (e.g., via IT teams) are secondary unless connectivity is suspected. This step is less relevant to the 500 error and lower priority than A, C, and D.

Conclusion: The three best steps are A (test API with same payload), C (analyze subsequent calls and customer logs), and D (validate JSON payload). These steps systematically isolate the issue- testing Appian's output (D), ruling out environment-specific problems (A), and leveraging customer insights into the API failure (C). This aligns with Appian's Post-Production Maintenance strategies: replicate safely, analyze logs, and validate data.

References:

- * Appian Documentation: "Troubleshooting Integrations" (Integration Object Logging and Debugging).
- * Appian Lead Developer Certification: Integration Module (Post-Production Troubleshooting).
- * Appian Best Practices: "Handling REST API Errors in Appian" (500 Error Diagnostics).

28. Frage

You are required to create an integration from your Appian Cloud instance to an application hosted within a customer's self-managed environment.

The customer's IT team has provided you with a REST API endpoint to test with: <https://internal.network/api/api/ping>.

Which recommendation should you make to progress this integration?

- A. Expose the API as a SOAP-based web service.
- B. Add Appian Cloud's IP address ranges to the customer network's allowed IP listing.
- **C. Set up a VPN tunnel.**
- D. Deploy the API/service into Appian Cloud.

Antwort: C

Begründung:

Comprehensive and Detailed In-Depth Explanation:

As an Appian Lead Developer, integrating an Appian Cloud instance with a customer's self-managed (on-premises) environment requires addressing network connectivity, security, and Appian's cloud architecture constraints. The provided endpoint (<https://internal.network/api/api/ping>) is a REST API on an internal network, inaccessible directly from Appian Cloud due to firewall restrictions and lack of public exposure. Let's evaluate each option:

A . Expose the API as a SOAP-based web service:

Converting the REST API to SOAP isn't a practical recommendation. The customer has provided a REST endpoint, and Appian fully supports REST integrations via Connected Systems and Integration objects. Changing the API to SOAP adds unnecessary complexity, development effort, and risks for the customer, with no benefit to Appian's integration capabilities. Appian's documentation emphasizes using the API's native format (REST here), making this irrelevant.

B . Deploy the API/service into Appian Cloud:

Deploying the customer's API into Appian Cloud is infeasible. Appian Cloud is a managed PaaS environment, not designed to host customer applications or APIs. The API resides in the customer's self-managed environment, and moving it would require significant architectural changes, violating security and operational boundaries. Appian's integration strategy focuses on connecting to external systems, not hosting them, ruling this out.

C . Add Appian Cloud's IP address ranges to the customer network's allowed IP listing:

This approach involves whitelisting Appian Cloud's IP ranges (available in Appian documentation) in the customer's firewall to allow direct HTTP/HTTPS requests. However, Appian Cloud's IPs are dynamic and shared across tenants, making this unreliable for long-term integrations- changes in IP ranges could break connectivity. Appian's best practices discourage relying on IP whitelisting for cloud-to-on-premises integrations due to this limitation, favoring secure tunnels instead.

D . Set up a VPN tunnel:

This is the correct recommendation. A Virtual Private Network (VPN) tunnel establishes a secure, encrypted connection between Appian Cloud and the customer's self-managed network, allowing Appian to access the internal REST API (<https://internal.network/api/api/ping>). Appian supports VPNs for cloud-to-on-premises integrations, and this approach ensures reliability, security, and compliance with network policies. The customer's IT team can configure the VPN, and Appian's documentation recommends this for such scenarios, especially when dealing with internal endpoints.

Conclusion: Setting up a VPN tunnel (D) is the best recommendation. It enables secure, reliable connectivity from Appian Cloud to the customer's internal API, aligning with Appian's integration best practices for cloud-to-on-premises scenarios.

Reference:

Appian Documentation: "Integrating Appian Cloud with On-Premises Systems" (VPN and Network Configuration).

Appian Lead Developer Certification: Integration Module (Cloud-to-On-Premises Connectivity).

Appian Best Practices: "Securing Integrations with Legacy Systems" (VPN Recommendations).

29. Frage

The business database for a large, complex Appian application is to undergo a migration between database technologies, as well as interface and process changes. The project manager asks you to recommend a test strategy. Given the changes, which two items should be included in the test strategy?

- A. A regression test of all existing system functionality
- B. Internationalization testing of the Appian platform
- C. Penetration testing of the Appian platform
- D. Tests that ensure users can still successfully log into the platform
- E. Tests for each of the interfaces and process changes

Antwort: A,E

Begründung:

Comprehensive and Detailed In-Depth Explanation:

As an Appian Lead Developer, recommending a test strategy for a large, complex application undergoing a database migration (e.g., from Oracle to PostgreSQL) and interface/process changes requires focusing on ensuring system stability, functionality, and the specific updates. The strategy must address risks tied to the scope-database technology shift, interface modifications, and process updates-while aligning with Appian's testing best practices. Let's evaluate each option:

A . Internationalization testing of the Appian platform:

Internationalization testing verifies that the application supports multiple languages, locales, and formats (e.g., date formats). While valuable for global applications, the scenario doesn't indicate a change in localization requirements tied to the database migration, interfaces, or processes. Appian's platform handles internationalization natively (e.g., via locale settings), and this isn't impacted by database technology or UI/process changes unless explicitly stated. This is out of scope for the given context and not a priority.

B . A regression test of all existing system functionality:

This is a critical inclusion. A database migration between technologies can affect data integrity, queries (e.g., `a!queryEntity`), and performance due to differences in SQL dialects, indexing, or drivers. Regression testing ensures that all existing functionality-records, reports, processes, and integrations-works as expected post-migration. Appian Lead Developer documentation mandates regression testing for significant infrastructure changes like this, as unmapped edge cases (e.g., datatype mismatches) could break the application. Given the "large, complex" nature, full-system validation is essential to catch unintended impacts.

C . Penetration testing of the Appian platform:

Penetration testing assesses security vulnerabilities (e.g., injection attacks). While security is important, the changes described-database migration, interface, and process updates-don't inherently alter Appian's security model (e.g., authentication, encryption), which is managed at the platform level. Appian's cloud or on-premise security isn't directly tied to database technology unless new vulnerabilities are introduced (not indicated here). This is a periodic concern, not specific to this migration, making it less relevant than functional validation.

D . Tests for each of the interfaces and process changes:

This is also essential. The project includes explicit "interface and process changes" alongside the migration. Interface updates (e.g., SAIL forms) might rely on new data structures or queries, while process changes (e.g., modified process models) could involve updated nodes or logic. Testing each change ensures these components function correctly with the new database and meet business requirements. Appian's testing guidelines emphasize targeted validation of modified components to confirm they integrate with the migrated data layer, making this a primary focus of the strategy.

E . Tests that ensure users can still successfully log into the platform:

Login testing verifies authentication (e.g., SSO, LDAP), typically managed by Appian's security layer, not the business database. A database migration affects application data, not user authentication, unless the database stores user credentials (uncommon in Appian, which uses separate identity management). While a quick sanity check, it's narrow and subsumed by broader regression testing (B), making it redundant as a standalone item.

Conclusion: The two key items are B (regression test of all existing system functionality) and D (tests for each of the interfaces and process changes). Regression testing (B) ensures the database migration doesn't disrupt the entire application, while targeted testing (D) validates the specific interface and process updates. Together, they cover the full scope-existing stability and new functionality-aligning with Appian's recommended approach for complex migrations and modifications.

Reference:

Appian Documentation: "Testing Best Practices" (Regression and Component Testing).

Appian Lead Developer Certification: Application Maintenance Module (Database Migration Strategies).

Appian Best Practices: "Managing Large-Scale Changes in Appian" (Test Planning).

30. Frage

While working on an application, you have identified oddities and breaks in some of your components. How can you guarantee that this mistake does not happen again in the future?

- A. Design and communicate a best practice that dictates designers only work within the confines of their own application.
- B. Ensure that the application administrator group only has designers from that application's team.
- C. Provide Appian developers with the "Designer" permissions role within Appian. Ensure that they have only basic user rights and assign them the permissions to administer their application.
- **D. Create a best practice that enforces a peer review of the deletion of any components within the application.**

Antwort: D

Begründung:

Comprehensive and Detailed In-Depth Explanation: As an Appian Lead Developer, preventing recurring "oddities and breaks" in application components requires addressing root causes-likely tied to human error, lack of oversight, or uncontrolled changes-while leveraging Appian's governance and collaboration features.

The question implies a past mistake (e.g., accidental deletions or modifications) and seeks a proactive, sustainable solution. Let's evaluate each option based on Appian's official documentation and best practices:

* A. Design and communicate a best practice that dictates designers only work within the confines of their own application: This suggests restricting designers to their assigned applications via a policy.

While Appian supports application-level security (e.g., Designer role scoped to specific applications), this approach relies on voluntary compliance rather than enforcement. It doesn't directly address

"oddities and breaks"-e.g., a designer could still mistakenly alter components within their own application. Appian's documentation emphasizes technical controls and process rigor over broad guidelines, making this insufficient as a guarantee.

* B. Ensure that the application administrator group only has designers from that application's team: This involves configuring security so only team-specific designers have Administrator rights to the application (via Appian's Security settings). While this limits external interference, it doesn't prevent internal mistakes (e.g., a team designer deleting a critical component). Appian's security model already restricts access by default, and the issue isn't about unauthorized access but rather component integrity.

This step is a hygiene factor, not a direct solution to the problem, and fails to "guarantee" prevention.

* C. Create a best practice that enforces a peer review of the deletion of any components within the application: This is the best choice. A peer review process for deletions (e.g., process models, interfaces, or records) introduces a checkpoint to catch errors before they impact the application. In Appian, deletions are permanent and can cascade (e.g., breaking dependencies), aligning with the "oddities and breaks" described. While Appian doesn't natively enforce peer reviews, this can be implemented via team workflows-e.g., using Appian's collaboration tools (like Comments or Tasks) or integrating with version control practices during deployment. Appian Lead Developer training emphasizes change management and peer validation to maintain application stability, making this a robust, preventive measure that directly addresses the root cause.

* D. Provide Appian developers with the "Designer" permissions role within Appian. Ensure that they have only basic user rights and assign them the permissions to administer their application: This option is confusingly worded but seems to suggest granting Designer system role permissions (a high-level privilege) while limiting developers to Viewer rights system-wide, with Administrator rights only for their application. In Appian, the "Designer" system role grants broad platform access (e.g., creating applications), which contradicts "basic user rights" (Viewer role). Regardless, adjusting permissions doesn't prevent mistakes-it only controls who can make them. The issue isn't about access but about error prevention, so this option misses the mark and is impractical due to its contradictory setup.

Conclusion: Creating a best practice that enforces a peer review of the deletion of any components (C) is the strongest solution. It directly mitigates the risk of "oddities and breaks" by adding oversight to destructive actions, leveraging team collaboration, and aligning with Appian's recommended governance practices.

Implementation could involve documenting the process, training the team, and using Appian's monitoring tools (e.g., Application Properties history) to track changes-ensuring mistakes are caught before deployment.

This provides the closest guarantee to preventing recurrence.

References:

* Appian Documentation: "Application Security and Governance" (Change Management Best Practices).

- ### 31. Frage

• • • • •

- ACD301 Unterlage:** <https://www.deutschpruefung.com/ACD301-deutsch-pruefungsfragen.html>