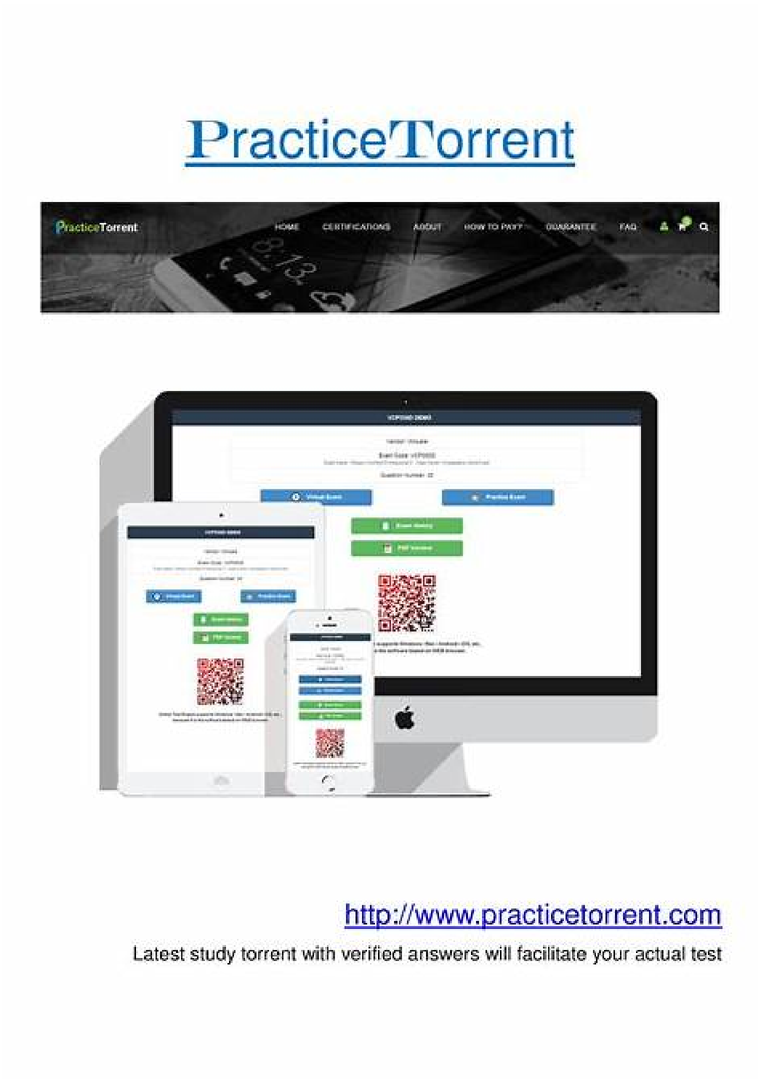
ACD301 Study Torrent & ACD301 Free Questions & ACD301 Valid Pdf


PracticeTorrent
http://www.practicetorrent.com
Latest study torrent with verified answers will facilitate your actual test

2025 Latest ValidTorrent ACD301 PDF Dumps and ACD301 Exam Engine Free Share: https://drive.google.com/open?id=1O6lsPVmvrT7pA4nfohvpQKeVHmszUEzs

Now we have PDF version, windows software and online engine of the ACD301 certification materials. Although all contents are the same, the learning experience is totally different. First of all, the PDF version ACD301 certification materials are easy to carry and have no restrictions. Then the windows software can simulate the real test environment, which makes you feel you are doing the real test. The online engine of the ACD301 test training can run on all kinds of browsers, which does not need to install on your computers or other electronic equipment. All in all, we hope that you can purchase our three versions of the ACD301 real exam dumps.

Every question from our ACD301 study materials is carefully elaborated and the content of our ACD301 exam questions involves the professional qualification certificate examination. We believe under the assistance of our ACD301 practice quiz, passing the exam and obtain related certificate are not out of reach. As long as you study our ACD301 training engine and followe it step by step, we believe you will achieve your dream easily.

>> Exam ACD301 Format <<

Valid ACD301 Torrent, ACD301 Discount Code

If you want to pass the exam smoothly buying our Appian Lead Developer guide dump is your ideal choice. They can help you learn efficiently, save your time and energy and let you master the useful information. Our passing rate of ACD301 study tool is very high and you needn't worry that you have spent money and energy on them but you gain nothing. We provide the great service after you purchase our ACD301 cram training materials and you can contact our customer service at any time during one day. It is a pity if you don't buy our ACD301 study tool to prepare for the test Appian certification.

Appian ACD301 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• Proactively Design for Scalability and Performance: This section of the exam measures skills of Application Performance Engineers and covers building scalable applications and optimizing Appian components for performance. It includes planning load testing, diagnosing performance issues at the application level, and designing systems that can grow efficiently without sacrificing reliability.
Topic 3	• Data Management: This section of the exam measures skills of Data Architects and covers analyzing, designing, and securing data models. Candidates must demonstrate an understanding of how to use Appian's data fabric and manage data migrations. The focus is on ensuring performance in high-volume data environments, solving data-related issues, and implementing advanced database features effectively.
Topic 4	• 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.

Appian Lead Developer Sample Questions (Q12-Q17):

NEW QUESTION # 12
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.

Answer: D

Explanation:
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, withAdministrator 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).
* Appian Lead Developer Certification: Application Design Module (Preventing Errors through Process).
* Appian Best Practices: "Team Collaboration in Appian Development" (Peer Review Recommendations).

NEW QUESTION # 13
You are in a backlog refinement meeting with the development team and the product owner. You review a story for an integration involving a third-party system. A payload will be sent from the Appian system through the integration to the third-party system. The story is 21 points on a Fibonacci scale and requires development from your Appian team as well as technical resources from the third-party system. This item is crucial to your project's success. What are the two recommended steps to ensure this story can be developed effectively?

- A. Identify subject matter experts (SMEs) to perform user acceptance testing (UAT).
- B. Acquire testing steps from QA resources.
- C. Maintain a communication schedule with the third-party resources.
- D. Break down the item into smaller stories.

Answer: C,D

Explanation:
Comprehensive and Detailed In-Depth Explanation:This question involves a complex integration story rated at 21 points on the Fibonacci scale, indicating significant complexity and effort. Appian Lead Developer best practices emphasize effective collaboration, risk mitigation, and manageable development scopes for such scenarios. The two most critical steps are:
* Option C (Maintain a communication schedule with the third-party resources):Integrations with third-party systems require close coordination, as Appian developers depend on external teams for endpoint specifications, payload formats, authentication details, and testing support. Establishing a regular communication schedule ensures alignment on requirements, timelines, and issue resolution. Appian's Integration Best Practices documentation highlights the importance of proactive communication with external stakeholders to prevent delays and misunderstandings, especially for critical project components.
* Option D (Break down the item into smaller stories):A 21-point story is considered large by Agile standards (Fibonacci scale typically flags anything above 13 as complex). Appian's Agile Development Guide recommends decomposing large stories into smaller, independently deliverable pieces to reduce risk, improve testability, and enable iterative progress. For example, the integration could be split into tasks like designing the payload structure, building the integration object, and testing the connection-each manageable within a sprint. This approach aligns with the principle of delivering value incrementally while maintaining quality.
* Option A (Acquire testing steps from QA resources):While QA involvement is valuable, this step is more relevant during the testing phase rather than backlog refinement or development preparation. It's not a primary step for ensuring effective development of the story.
* Option B (Identify SMEs for UAT):User acceptance testing occurs after development, during the validation phase. Identifying

SMEs is important but not a key step in ensuring the story is developed effectively during the refinement and coding stages.
By choosingCandD, you address both the external dependency (third-party coordination) and internal complexity (story size), ensuring a smoother development process for this critical integration.
References:Appian Lead Developer Training - Integration Best Practices, Appian Agile Development Guide
- Story Refinement and Decomposition.

NEW QUESTION # 14
An Appian application contains an integration used to send a JSON, called at the end of a form submission, returning the created code of the user request as the response. To be able to efficiently follow their case, the user needs to be informed of that code at the end of the process. The JSON contains case fields (such as text, dates, and numeric fields) to a customer's API. What should be your two primary considerations when building this integration?

- A. A dictionary that matches the expected request body must be manually constructed.
- B. The size limit of the body needs to be carefully followed to avoid an error.
- C. The request must be a multi-part POST.
- D. A process must be built to retrieve the API response afterwards so that the user experience is not impacted.

Answer: A,B

Explanation:
Comprehensive and Detailed In-Depth Explanation:As an Appian Lead Developer, building an integration to send JSON to a customer's API and return a code to the user involves balancing usability, performance, and reliability. The integration is triggered at form submission, and the user must see the response (case code) efficiently. The JSON includes standard fields (text, dates, numbers), and the focus is on primary considerations for the integration itself. Let's evaluate each option based on Appian's official documentation and best practices:
* A. A process must be built to retrieve the API response afterwards so that the user experience is not impacted:This suggests making the integration asynchronous by calling it in a process model (e.g., via a Start Process smart service) and retrieving the response later, avoiding delays in the UI. While this improves user experience for slow APIs (e.g., by showing a "Processing" message), it contradicts the requirement that the user is "informed of that code at the end of the process." Asynchronous processing would delay the code display, requiring additional steps (e.g., a follow-up task), which isn't efficient for this use case. Appian's default integration pattern (synchronous call in an Integration object) is suitable unless latency is a known issue, making this a secondary-not primary-consideration.
* B. The request must be a multi-part POST:A multi-part POST (e.g., multipart/form-data) is used for sending mixed content, like files and text, in a single request. Here, the payload is a JSON containing case fields (text, dates, numbers)-no files are mentioned. Appian's HTTP Connected System and Integration objects default to application/json for JSON payloads via a standard POST, which aligns with REST API norms. Forcing a multi-part POST adds unnecessary complexity and is incompatible with most APIs expecting JSON. Appian documentation confirms this isn't required for JSON-only data, ruling it out as a primary consideration.
* C. The size limit of the body needs to be carefully followed to avoid an error:This is a primary consideration. Appian's Integration object has a payload size limit (approximately 10 MB, though exact limits depend on the environment and API), and exceeding it causes errors (e.g., 413 Payload Too Large). The JSON includes multiple case fields, and while "hundreds of thousands" isn't specified, large datasets could approach this limit. Additionally, the customer's API may impose its own size restrictions (common in REST APIs). Appian Lead Developer training emphasizes validating payload size during design-e.g., testing with maximum expected data-to prevent runtime failures. This ensures reliability and is critical for production success.
* D. A dictionary that matches the expected request body must be manually constructed:This is also a primary consideration. The integration sends a JSON payload to the customer's API, which expects a specific structure (e.g., { "field1": "text", "field2": "date" }). In Appian, the Integration object requires a dictionary (key-value pairs) to construct the JSON body, manually built to match the API's schema.
Mismatches (e.g., wrong field names, types) cause errors (e.g., 400 Bad Request) or silent failures.
Appian's documentation stresses defining the request body accurately-e.g., mapping form data to a CDT or dictionary-ensuring the API accepts the payload and returns the case code correctly. This is foundational to the integration's functionality.
Conclusion: The two primary considerations are C (size limit of the body) and D (constructing a matching dictionary). These ensure the integration works reliably (C) and meets the API's expectations (D), directly enabling the user to receive the case code at submission end. Size limits prevent technical failures, while the dictionary ensures data integrity-both are critical for a synchronous JSON POST in Appian. Option A could be relevant for performance but isn't primary given the requirement, and B is irrelevant to the scenario.
References:
* Appian Documentation: "Integration Object" (Request Body Configuration and Size Limits).
* Appian Lead Developer Certification: Integration Module (Building REST API Integrations).
* Appian Best Practices: "Designing Reliable Integrations" (Payload Validation and Error Handling).

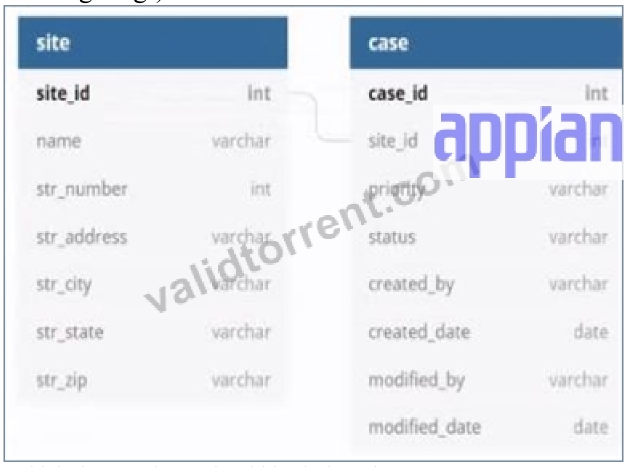
NEW QUESTION # 15
You are on a call with a new client, and their program lead is concerned about how their legacy systems will integrate with Appian. The lead wants to know what authentication methods are supported by Appian. Which three authentication methods are supported?

- A. OAuth
- B. SAML
- C. Biometrics
- D. CAC
- E. Active Directory
- F. API Keys

Answer: A,B,E

Explanation:
Comprehensive and Detailed In-Depth Explanation:
As an Appian Lead Developer, addressing a client's concerns about integrating legacy systems with Appian requires accurately identifying supported authentication methods for system-to-system communication or user access. The question focuses on Appian's integration capabilities, likely for both user authentication (e.g., SSO) and API authentication, as legacy system integration often involves both. Appian's documentation outlines supported methods in its Connected Systems and security configurations. Let's evaluate each option:
A . API Keys:
API Key authentication involves a static key sent in requests (e.g., via headers). Appian supports this for outbound integrations in Connected Systems (e.g., HTTP Authentication with an API key), allowing legacy systems to authenticate Appian calls. However, it's not a user authentication method for Appian's platform login-it's for system-to-system integration. While supported, it's less common for legacy system SSO or enterprise use cases compared to other options, making it a lower-priority choice here.
B . Biometrics:
Biometrics (e.g., fingerprint, facial recognition) isn't natively supported by Appian for platform authentication or integration. Appian relies on standard enterprise methods (e.g., username/password, SSO), and biometric authentication would require external identity providers or custom clients, not Appian itself. Documentation confirms no direct biometric support, ruling this out as an Appian-supported method.
C . SAML:
Security Assertion Markup Language (SAML) is fully supported by Appian for user authentication via Single Sign-On (SSO). Appian integrates with SAML 2.0 identity providers (e.g., Okta, PingFederate), allowing users to log in using credentials from legacy systems that support SAML-based SSO. This is a key enterprise method, widely used for integrating with existing identity management systems, and explicitly listed in Appian's security configuration options-making it a top choice.
D . CAC:
Common Access Card (CAC) authentication, often used in government contexts with smart cards, isn't natively supported by Appian as a standalone method. While Appian can integrate with CAC via SAML or PKI (Public Key Infrastructure) through an identity provider, it's not a direct Appian authentication option. Documentation mentions smart card support indirectly via SSO configurations, but CAC itself isn't explicitly listed, making it less definitive than other methods.
E . OAuth:
OAuth (specifically OAuth 2.0) is supported by Appian for both outbound integrations (e.g., Authorization Code Grant, Client Credentials) and inbound API authentication (e.g., securing Appian Web APIs). For legacy system integration, Appian can use OAuth to authenticate with APIs (e.g., Google, Salesforce) or allow legacy systems to call Appian services securely. Appian's Connected System framework includes OAuth configuration, making it a versatile, standards-based method highly relevant to the client's needs.
F . Active Directory:
Active Directory (AD) integration via LDAP (Lightweight Directory Access Protocol) is supported for user authentication in Appian. It allows synchronization of users and groups from AD, enabling SSO or direct login with AD credentials. For legacy systems using AD as an identity store, this is a seamless integration method. Appian's documentation confirms LDAP/AD as a core authentication option, widely adopted in enterprise environments-making it a strong fit.
Conclusion: The three supported authentication methods are C (SAML), E (OAuth), and F (Active Directory). These align with Appian's enterprise-grade capabilities for legacy system integration: SAML for SSO, OAuth for API security, and AD for user management. API Keys (A) are supported but less prominent for user authentication, CAC (D) is indirect, and Biometrics (B) isn't supported natively. This selection reassures the client of Appian's flexibility with common legacy authentication standards.
Reference:
Appian Documentation: "Authentication for Connected Systems" (OAuth, API Keys).
Appian Documentation: "Configuring Authentication" (SAML, LDAP/Active Directory).
Appian Lead Developer Certification: Integration Module (Authentication Methods).

NEW QUESTION # 16
You are developing a case management application to manage support cases for a large set of sites. One of the tabs in this application s site Is a record grid of cases, along with Information about the site corresponding to that case. Users must be able to filter cases by priority level and status.
You decide to create a view as the source of your entity-backed record, which joins the separate case/site tables (as depicted in the following Image).



Which three column should be indexed?

- A. case_id
- B. priority
- C. modified_date
- D. status
- E. name
- F. site_id

Answer: B,D,F

Explanation:
Indexing columns can improve the performance of queries that use those columns in filters, joins, or order by clauses. In this case, the columns that should be indexed are site_id, status, and priority, because they are used for filtering or joining the tables. Site_id is used to join the case and site tables, so indexing it will speed up the join operation. Status and priority are used to filter the cases by the user's input, so indexing them will reduce the number of rows that need to be scanned. Name, modified_date, and case_id do not need to be indexed, because they are not used for filtering or joining. Name and modified_date are only used for displaying information in the record grid, and case_id is only used as a unique identifier for each record. Verified Reference: Appian Records Tutorial, Appian Best Practices As an Appian Lead Developer, optimizing a database view for an entity-backed record grid requires indexing columns frequently used in queries, particularly for filtering and joining. The scenario involves a record grid displaying cases with site information, filtered by "priority level" and "status," and joined via the site_id foreign key. The image shows two tables (site and case) with a relationship via site_id. Let's evaluate each column based on Appian's performance best practices and query patterns:
A . site_id:
This is a primary key in the site table and a foreign key in the case table, used for joining the tables in the view. Indexing site_id in the case table (and ensuring it's indexed in site as a PK) optimizes JOIN operations, reducing query execution time for the record grid. Appian's documentation recommends indexing foreign keys in large datasets to improve query performance, especially for entity-backed records. This is critical for the join and must be included.
B . status:
Users filter cases by "status" (a varchar column in the case table). Indexing status speeds up filtering queries (e.g., WHERE status = 'Open') in the record grid, particularly with large datasets. Appian emphasizes indexing columns used in WHERE clauses or filters to enhance performance, making this a key column for optimization. Since status is a common filter, it's essential.
C . name:
This is a varchar column in the site table, likely used for display (e.g., site name in the grid). However, the scenario doesn't mention filtering or sorting by name, and it's not part of the join or required filters. Indexing name could improve searches if used, but it's not a priority given the focus on priority and status filters. Appian advises indexing only frequently queried or filtered columns to avoid unnecessary overhead, so this isn't necessary here.
D . modified_date:
This is a date column in the case table, tracking when cases were last updated. While useful for sorting or historical queries, the

scenario doesn't specify filtering or sorting by modified_date in the record grid. Indexing it could help if used, but it's not critical for the current requirements. Appian's performance guidelines prioritize indexing columns in active filters, making this lower priority than site_id, status, and priority.
E . priority:
Users filter cases by "priority level" (a varchar column in the case table). Indexing priority optimizes filtering queries (e.g., WHERE priority = 'High') in the record grid, similar to status. Appian's documentation highlights indexing columns used in WHERE clauses for entity-backed records, especially with large datasets. Since priority is a specified filter, it's essential to include.
F . case_id:
This is the primary key in the case table, already indexed by default (as PKs are automatically indexed in most databases). Indexing it again is redundant and unnecessary, as Appian's Data Store configuration relies on PKs for unique identification but doesn't require additional indexing for performance in this context. The focus is on join and filter columns, not the PK itself.
Conclusion: The three columns to index are A (site_id), B (status), and E (priority). These optimize the JOIN (site_id) and filter performance (status, priority) for the record grid, aligning with Appian's recommendations for entity-backed records and large datasets. Indexing these columns ensures efficient querying for user filters, critical for the application's performance.
Reference:
Appian Documentation: "Performance Best Practices for Data Stores" (Indexing Strategies).
Appian Lead Developer Certification: Data Management Module (Optimizing Entity-Backed Records).
Appian Best Practices: "Working with Large Data Volumes" (Indexing for Query Performance).

NEW QUESTION # 17
......