높은통과율ACD301인증덤프공부덤프공부문제

BONUS!!! KoreaDumps ACD301 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1QeIS1K5l43lXs2nlNcO2e9__7m2ROvww

예를 들어Appian ACD301 덤프를 보면 어떤 덤프제공사이트에서는 문항수가 아주 많은 자료를 제공해드리지만 저희Appian ACD301덤프는 문항수가 적은 편입니다.왜냐하면 저희는 더 이상 출제되지 않는 오래된 문제들을 삭제해버리기 때문입니다. 문제가 많으면 고객들의 시간을 허비하게 됩니다. KoreaDumps는 응시자에게 있어서 시간이 정말 소중하다는 것을 잘 알고 있습니다.

Appian ACD301 시험요강:

주제	소개
주제 1	• Project and Resource Management: This section of the exam measures skills of Agile Project Leads and covers interpreting business requirements, recommending design options, and leading Agile teams through technical delivery. It also involves governance, and process standardization.
주제 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.

주제 3	• 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.
주제 4	• 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.

최신 Lead Developer ACD301 무료샘플문제 (Q36-Q41):

질문 # 36
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. Deploy the API/service into Appian Cloud.
- B. Add Appian Cloud's IP address ranges to the customer network's allowed IP listing.
- C. Expose the API as a SOAP-based web service.
- D. Set up a VPN tunnel.

정답：D

설명:
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.
References:
* 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).

질문 # 37
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. Active Directory
- B. CAC
- C. OAuth
- D. API Keys
- E. SAML
- F. Biometrics

정답：A,C,E

설명：
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.

References:
* 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).

질문 # 38
Your client's customer management application is finally released to Production. After a few weeks of small enhancements and patches, the client is ready to build their next application. The new applicationwill leverage customer information from the first application to allow the client to launch targeted campaigns for select customers in order to increase sales. As part of the first application, your team had built a section to display key customer information such as their name, address, phone number, how long they have been a customer, etc. A similar section will be needed on the campaign record you are building. One of your developers shows you the new object they are working on for the new application and asks you to review it as they are running into a few issues. What feedback should you give?

- A. Point the developer to the relevant areas in the documentation or Appian Community where they can find more information on the issues they are running into.
- B. Provide guidance to the developer on how to address the issues so that they can proceed with their work.
- C. Create a duplicate version of that section designed for the campaign record.
- D. Ask the developer to convert the original customer section into a shared object so it can be used by the new application.

정답：D

설명:
Comprehensive and Detailed In-Depth Explanation:The scenario involves reusing a customer information section from an existing application in a new application for campaign management, with the developer encountering issues. Appian's best practices emphasize reusability, efficiency, and maintainability, especially when leveraging existing components across applications.
* Option B (Ask the developer to convert the original customer section into a shared object so it can be used by the new application):This is the recommended approach. Converting the original section into a shared object (e.g., a reusable interface component) allows it to be accessed across applications without duplication. Appian's Design Guide highlights the use of shared components to promote consistency, reduce redundancy, and simplify maintenance. Since the new application requires similar customer data (name, address, etc.), reusing the existing section-after ensuring it is modular and adaptable-addresses the developer's issues while aligning with the client's goal of leveraging prior work. The developer can then adjust the shared object (e.g., via parameters) to fit the campaign context, resolving their issues collaboratively.
* Option A (Provide guidance to the developer on how to address the issues so that they can proceed with their work):While providing guidance is valuable, it doesn't address the root opportunity to reuse existing code. This option focuses on fixing the new object in isolation, potentially leading to duplicated effort if the original section could be reused instead.
* Option C (Point the developer to the relevant areas in the documentation or Appian Community where they can find more information on the issues they are running into):This is a passive approach and delays resolution. As a Lead Developer, offering direct support ora strategic solution (like reusing components) is more effective than redirecting the developer to external resources without context.
* Option D (Create a duplicate version of that section designed for the campaign record):
Duplication violates Appian's principle of DRY (Don't Repeat Yourself) and increases maintenance overhead. Any future updates to customer data display logic would need to be applied to multiple objects, risking inconsistencies.
Given the need to leverage existing customer information and the developer's issues, converting the section to a shared object is the most efficient and scalable solution.
References:Appian Design Guide - Reusability and Shared Components, Appian Lead Developer Training - Application Design and Maintenance.

질문 # 39
You are reviewing the Engine Performance Logs in Production for a single application that has been live for six months. This application experiences concurrent user activity and has a fairly sustained load during business hours. The client has reported performance issues with the application during business hours.
During your investigation, you notice a high Work Queue - Java Work Queue Size value in the logs. You also notice unattended process activities, including timer events and sending notification emails, are taking far longer to execute than normal.
The client increased the number of CPU cores prior to the application going live.
What is the next recommendation?

- A. Add execution and analytics shards

- B. Optimize slow-performing user interfaces.
- C. Add more application servers.
- D. Add more engine replicas.

정답：D

설명：
As an Appian Lead Developer, analyzing Engine Performance Logs to address performance issues in a Production application requires understanding Appian's architecture and the specific metrics described. The scenario indicates a high "Work Queue - Java Work Queue Size," which reflects a backlog of tasks in the Java Work Queue (managed by Appian engines), and delays in unattended process activities (e.g., timer events, email notifications). These symptoms suggest the Appian engines are overloaded, despite the client increasing CPU cores. Let's evaluate each option:
A . Add more engine replicas:
This is the correct recommendation. In Appian, engine replicas (part of the Appian Engine cluster) handle process execution, including unattended tasks like timers and notifications. A high Java Work Queue Size indicates the engines are overwhelmed by concurrent activity during business hours, causing delays. Adding more engine replicas distributes the workload, reducing queue size and improving performance for both user-driven and unattended tasks. Appian's documentation recommends scaling engine replicas to handle sustained loads, especially in Production with high concurrency. Since CPU cores were already increased (likely on application servers), the bottleneck is likely the engine capacity, not the servers.
B . Optimize slow-performing user interfaces:
While optimizing user interfaces (e.g., SAIL forms, reports) can improve user experience, the scenario highlights delays in unattended activities (timers, emails), not UI performance. The Java Work Queue Size issue points to engine-level processing, not UI rendering, so this doesn't address the root cause. Appian's performance tuning guidelines prioritize engine scaling for queue-related issues, making this a secondary concern.
C . Add more application servers:
Application servers handle web traffic (e.g., SAIL interfaces, API calls), not process execution or unattended tasks managed by engines. Increasing application servers would help with UI concurrency but wouldn't reduce the Java Work Queue Size or speed up timer/email processing, as these are engine responsibilities. Since the client already increased CPU cores (likely on application servers), this is redundant and unrelated to the issue.
D . Add execution and analytics shards:
Execution shards (for process data) and analytics shards (for reporting) are part of Appian's data fabric for scalability, but they don't directly address engine workload or Java Work Queue Size. Shards optimize data storage and query performance, not real-time process execution. The logs indicate an engine bottleneck, not a data storage issue, so this isn't relevant. Appian's documentation confirms shards are for long-term scaling, not immediate performance fixes.
Conclusion: Adding more engine replicas (A) is the next recommendation. It directly resolves the high Java Work Queue Size and delays in unattended tasks, aligning with Appian's architecture for handling concurrent loads in Production. This requires collaboration with system administrators to configure additional replicas in the Appian cluster.
Reference:
Appian Documentation: "Engine Performance Monitoring" (Java Work Queue and Scaling Replicas).
Appian Lead Developer Certification: Performance Optimization Module (Engine Scaling Strategies).
Appian Best Practices: "Managing Production Performance" (Work Queue Analysis).

질문 # 40
You have created a Web API in Appian with the following URL to call it:
https://exampleappiancloud.com/suite/webapi/user_management/users?username=john.smith. Which is the correct syntax for referring to the username parameter?

- A. httpRequest.queryParameters.users.username
- B. httpRequest.users.username
- C. httpRequest.queryParameters.username
- D. httpRequest.formData.username

정답：C

설명：
Comprehensive and Detailed In-Depth Explanation:
In Appian, when creating a Web API, parameters passed in the URL (e.g., query parameters) are accessed within the Web API expression using the httpRequest object. The URL https://exampleappiancloud.com/suite/webapi/user_management/users?username=john.smith includes a query parameter username with the value john.smith. Appian's Web API documentation specifies how to handle such parameters in the expression rule associated with the Web API.

Option D (httpRequest.queryParameters.username):
This is the correct syntax. The httpRequest.queryParameters object contains all query parameters from the URL. Since username is a single query parameter, you access it directly as httpRequest.queryParameters.username. This returns the value john.smith as a text string, which can then be used in the Web API logic (e.g., to query a user record). Appian's expression language treats query parameters as key-value pairs under queryParameters, making this the standard approach.
Option A (httpRequest.queryParameters.users.username):
This is incorrect. The users part suggests a nested structure (e.g., users as a parameter containing a username subfield), which does not match the URL. The URL only defines username as a top-level query parameter, not a nested object.
Option B (httpRequest.users.username):
This is invalid. The httpRequest object does not have a direct users property. Query parameters are accessed via queryParameters, and there's no indication of a users object in the URL or Appian's Web API model.
Option C (httpRequest.formData.username):
This is incorrect. The httpRequest.formData object is used for parameters passed in the body of a POST or PUT request (e.g., form submissions), not for query parameters in a GET request URL. Since the username is part of the query string (?username=john.smith), formData does not apply.
The correct syntax leverages Appian's standard handling of query parameters, ensuring the Web API can process the username value effectively.

질문 # 41
.....

KoreaDumps ACD301 최신 PDF 버전 시험 문제집을 무료로 Google Drive에서 다운로드하세요:
https://drive.google.com/open?id=1QeIS1K5l43lXs2nlNcO2e9__7m2ROvww