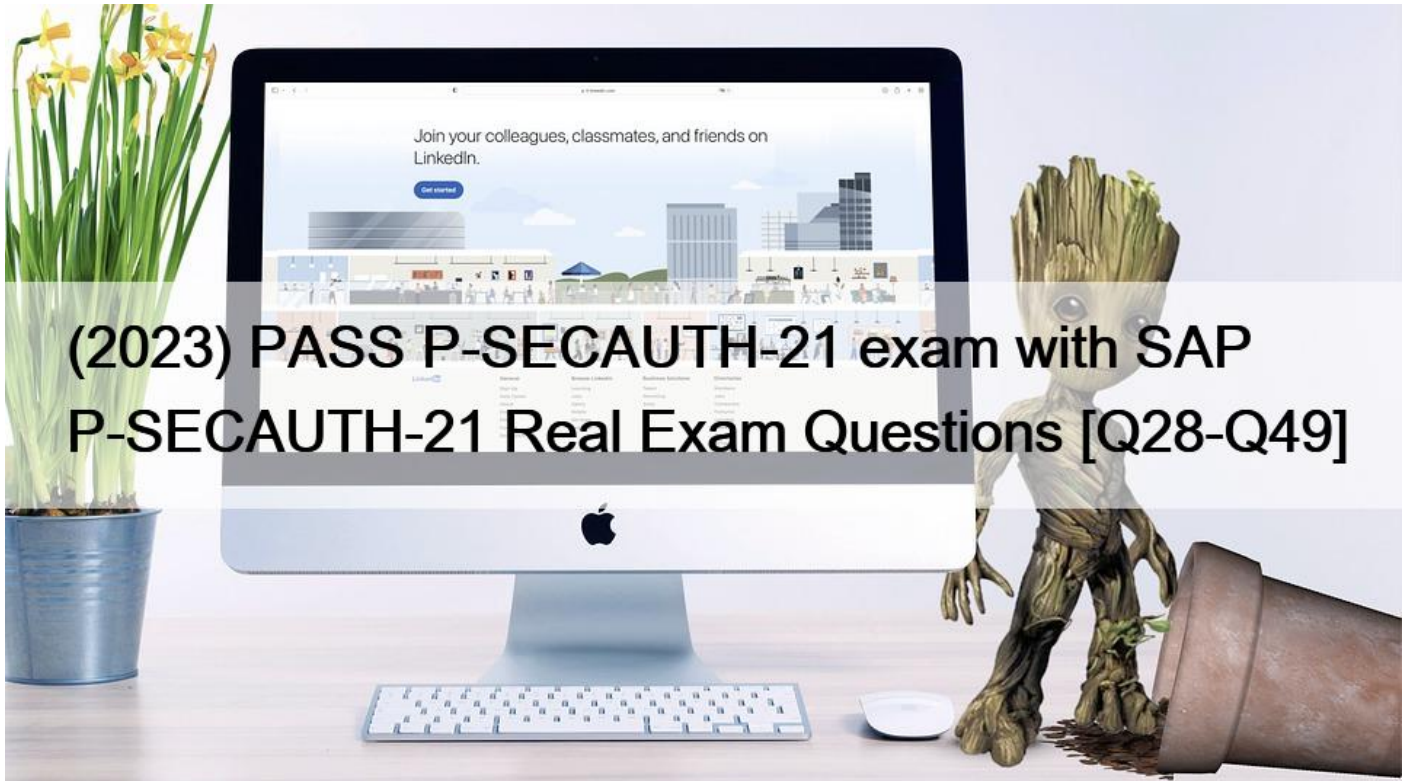


(2023) PASS P-SECAUTH-21 exam with SAP P-SECAUTH-21 Real Exam Questions [Q28-Q49]



(2023) PASS P-SECAUTH-21 exam with SAP P-SECAUTH-21 Real Exam Questions Real exam questions are provided for SAP Certified Technology Professional tests, which can make sure you 100% pass Q28. For which purpose do you use instance Secure Storage File System (SSFS) in an SAP HANA system? Note: There are 2 correct answers to this question.

- * To protect the password of the root key backup
- * To store root keys for data volume encryption
- * To store the secure single sign-on configuration
- * To protect the X.509 public key infrastructure certificates

Q29. Under which group can you find the `“System Recommendations”` file in the Solution Manager launchpad?

- * IT Service Management
- * Technical Administration
- * Change Management
- * Root Cause Analysis

Q30. You have configured a Gateway SSO authentication using X.509 client certificates. The configuration of the dual trust relationship between client (browser) and SAP Web Dispatcher as well as the configuration of the SAP Web Dispatcher to accept and forward client certificates were done. Users complain that they can't log in to the back-end system. How can you check the cause?

- * Run back-end transaction SMICM and open the trace file
- * Run back-end system trace using ST12
- * Run gateway transaction /IWFND/TRACES

* Run gateway transaction /IWFND/ ERRORJ.OG

Q31. Which measures should we implement to protect the PSEs? Note: There are 2 correct answers to this question.

- * Review the usage of the S_ADMI_FCD object
- * Encrypt the files with the transaction SNC0
- * Review the usage of the S_DATASET object
- * Restrict access to the operating system users

Explanation

These are some of the measures that should be implemented to protect the PSEs (Personal Security Environments). PSEs are files that store cryptographic information, such as keys and certificates, for various security purposes, such as SSL, SNC, or SSO. The usage of the S_ADMI_FCD object should be reviewed because it controls the access to PSE administration functions, such as creating, deleting, or displaying PSEs.

The access to the operating system users should be restricted because they can access the PSE files directly from the file system and manipulate them. References:

https://help.sap.com/doc/saphelp_nw70ehp3/7.03/en-US/c8/e8d53d35fb11d182b90000e829fbfe/content.htm?no_

https://help.sap.com/doc/saphelp_nw70ehp3/7.03/en-US/c8/e8d53d35fb11d182b90000e829fbfe/content.htm?no_

Q32. How can you describe the hierarchical relationships between technical entities in the Cloud Foundry?

- * A global account can have one or many subaccounts
- * A SaaS tenant acts as one provider account.
- * A SaaS tenant acts as one Cloud Foundry Organization.
- * A subscription is a PaaS tenant.

Q33. To prevent session fixation and session hijacking attacks, SAP's HTTP security session management is highly recommended. What are the characteristics of HTTP security session management? Note: There are 2 correct answers to this question.

- * It uses URLs containing sap-context id to identify the security session
- * The system is checking the logon credentials again for every request
- * The security sessions are created during logon and deleted during logoff.
- * The session identifier is a reference to the session context transmitted through a cookie.

Q34. How is the role concept applied for modeled authorizations based on Core Data Services (CDS) views?

- * CDS roles are defined for the CDS views and implicitly applied to each user
- * CDS roles are mapped to the CDS view in the access rules
- * CDS roles are defined in the WHERE clause when calling a CDS view in Open SQL
- * CDS roles are defined for CDS views in Object Navigator

Q35. What authorization objects do we need to create job steps with external commands in a background job? Note: There are 2 correct answers to this question.

- * S_ADMI_FCD
- * S_LOG_COM
- * S_RZL_ADM
- * S_BTCH_EXT

Q36. Which communication protocols are supported by the SAP Cloud Connector? Note: There are 2 correct answers to this question

- * NNTP
- * LDAP
- * SNA
- * RFC

Q37. SAP GRC Access Control provides risk analysis for which of the following? Note: There are 2 correct answers to this question.

- * Business Role Management
- * Access Request Management
- * Business Rule Framework
- * Password Self-Service

Explanation

SAP GRC Access Control provides risk analysis for these components. SAP GRC Access Control is a suite of applications that enables you to manage access risks and compliance across your SAP systems and landscapes.

Business Role Management is a component that allows you to design and maintain business roles based on user tasks and functions, and analyze them for potential risks or conflicts. Access Request Management is a component that allows you to request, approve, provision, and monitor access changes for users and roles, and analyze them for potential risks or violations. References:

https://help.sap.com/viewer/product/SAP_ACCESS_CONTROL/en-US

Q38. What authorization objects do we need to create job steps with external commands in a background job? Note:

There are 2 correct answers to this question.

- * S_BTCH_EXT
- * S_BTCH_ADM
- * S_RZL_ADM
- * S_LOG_COM

Explanation

These are some of the authorization objects that we need to create job steps with external commands in a background job. A background job is a process that runs in the background without user interaction and performs tasks such as data processing or report generation. A job step is a unit of work within a background job that executes a program or an external command. S_BTCH_EXT is an authorization object that controls the execution of external commands or programs in a job step. S_BTCH_ADM is an authorization object that controls the administration of background jobs, such as creating, changing, or deleting jobs. References:

https://help.sap.com/doc/saphelp_nw73ehp1/7.31.19/en-US/c8/e8d53d35fb11d182b90000e829fbfe/content.htm?

Q39. You have a load balancer in a DMZ network zone (called natl.mydomain.com) in front of 2 SAP NetWeaver AS systems (host1.mydomain.com, host2.mydomain.com). What is the recommended common name part of the distinguished name on the SSL Server's PSE?

- * It should be a combined DNS alias for host 1.mydomain.com and host2.mydomain.com and nat1.mydomain.com
- * It should be host 1.mydomain.com, host2.mydomain.com individually for each PSE
- * It should be natl.mydomain.com
- * It should be *.mydomain.com (wildcard) names

Q40. You want to create a role to provide users the ability to display and change an HR table's content based on the country groupings. Which of the steps would you take to accomplish these requirements? Note: There are 2 correct answers to this question.

- * Maintain the authorization object S_TABU_LIN

- * Create an authorization group with appropriate authorization fields for the table
- * Maintain the authorization object S_TABU_NAM
- * Define an organization criterion through transaction SPRO

Explanation

These are some of the steps that you would take to accomplish these requirements of creating a role to provide users the ability to display and change an HR table's content based on the country groupings. S_TABU_LIN is an authorization object that controls access to table entries based on organizational criteria, such as country grouping, personnel area, or personnel subarea. You would maintain this authorization object with appropriate values for your role in PFCG transaction. SPRO is a transaction that allows you to access customizing activities for various SAP applications and modules. You would define an organization criterion through this transaction by assigning an authorization field name (such as T500L-LAND1 for country grouping) to a table name (such as T500L for countries) in IMG activity “Maintain Table Names for Organizational Criteria”.

References: https://help.sap.com/doc/saphelp_nw73ehp1/7.31.19/en-

Q41. Which tools can you use to troubleshoot an authorization issue with a Fiori application? Note:

There are 2 correct answers to this question.

- * /IWFND/ERROR_LOG
- * /UI2/FLC
- * /UI2/GW_APPS_LOG
- * /IWBEP/ERROR_LOG

Explanation

These are some of the tools that you can use to troubleshoot an authorization issue with a Fiori application.

/IWFND/ERROR_LOG is a transaction that displays the error log for the SAP Gateway framework, which handles the OData requests and responses between the Fiori front-end server and the back-end system.

/IWBEP/ERROR_LOG is a transaction that displays the error log for the SAP Gateway service implementation, which contains the business logic and data access for the OData services. References:

<https://help.sap.com/viewer/a7b390faab1140c087b8926571e942b7/7.5.9/en-US/5c3d6d0f6c461014a1d99bc8a4f>

Q42. Which features does SAProuter provide?

Note: There are 2 correct answers to this question

- * HTTP conversion into HTTPS connections
- * Load-balanced RFC connections
- * Filtered and logged network connections
- * Password-protected connections

Q43. A security consultant has activated a trace via ST01 and is analyzing the authorization error with Return Code 12. What does the Return Code 12 signify?

- * “Objects not contained in User Buffer”;
- * “No authorizations and does NOT have authorization object in their buffer”;
- * “No authorizations but does have authorization object in their buffer”;
- * “Too many parameters for authorization checks”;

Q44. A user reports an issue with data not showing up in the visualization of the SAP Fiori tiles. You want to verify the target

mapping. At what level are you going to check the target mapping?

- * At the catalog level in the SAP Fiori front-end server
- * At the group level in the SAP Fiori front-end server
- * At the group level in the SAP Fiori Launchpad
- * At the application level in the Web IDE

Q45. You are evaluating the `cross-client object change` option using transaction SCC4 for your Unit Test Client in the development environment. Which setting do you recommend?

- * No changes to repository and cross-client customizing objects
- * No changes to cross-client customizing objects
- * Changes to repository and cross-client customizing allowed
- * No changes to repository objects

Explanation

This is the recommended setting for the `cross-client object change` option using transaction SCC4 for your Unit Test Client in the development environment. This setting allows you to make changes to repository objects (such as programs, function modules, classes, etc.) and cross-client customizing objects (such as number ranges, message classes, etc.) in your Unit Test Client without affecting other clients in the same system. References:

https://help.sap.com/doc/saphelp_nw70ehp3/7.03/en-US/c8/e8d53d35fb11d182b90000e829fbfe/content.htm?no_

https://help.sap.com/doc/saphelp_nw70ehp3/7.03/en-US/c8/e8d53d35fb11d182b90000e829fbfe/content.htm?no_

Q46. In addition to the authorization `/UI2/LAUNCHPAD`, which other authorizations are required to assign to an SAP Fiori Launchpad user? Note: There are 2 correct answers to this question.

- * `/UI2/INTEROP`
- * `/UI2JPAGE_BUILDER_CUST`
- * `/UI2/FLC`
- * `/UI2JPAGE_BUILDER_PERS`

Q47. How are assertion tickets used?

- * They are used for user-to-system trusted login.
- * They are used for encrypting Web service communication.
- * They are used for system-to-system encryption.
- * They are used for system-to-system communication.

Explanation

Assertion tickets are used for system-to-system communication in SAP systems. They are based on the SAML (Security Assertion Markup Language) standard and contain information about the identity and attributes of a user or a system. Assertion tickets can be used to establish trust relationships between systems and enable single sign-on scenarios. References:

https://help.sap.com/doc/saphelp_nw70ehp3/7.03/en-US/c8/e8d53d35fb11d182b90000e829fbfe/content.htm?no_

https://help.sap.com/doc/saphelp_nw70ehp3/7.03/en-US/c8/e8d53d35fb11d182b90000e829fbfe/content.htm?no_

Q48. Which of the following function can be used to troubleshoot authorization errors for ABAP CDS views with Authorization based on Access Control?

- * E2E TRACE ANALYSIS
- * ABAP TRACE
- * REPORT RSUSR008_009

* STAUTHTRACE

Q49. The SAP HANA database is installed with multi database container (MDC) mode with multiple tenant databases configured. What are the required activities to enable access between tenants? Note: There are 2 correct answers to this question.

- * Create user mapping between local and remote tenant databases
- * Configure smart data access (SDA) between the relevant HANA tenants
- * Set whitelist of cross-tenant database communication channel
- * Decrease the level of isolation mode on all MDC tenants

SAP P_SECAUTH_21 certification is suitable for IT professionals who have experience in SAP system security architecture. Certified Technology Professional - System Security Architect certification is ideal for system architects, security consultants, administrators, and engineers who want to validate their skills and knowledge in the field of system security architecture. Certified Technology Professional - System Security Architect certification can help professionals enhance their career prospects and increase their earning potential.

The topics covered in the exam aim to cover essential knowledge areas on SAP system security architecture. Some of the domains that the candidate must demonstrate proficiency in are Access Management, Network Security, System Hardening, Audits, and Compliance Regulations. These domains aim to equip the candidate with relevant knowledge to identify vulnerabilities and recommend measures aimed at minimizing the risk to an organization.

Latest P-SECAUTH-21 Pass Guaranteed Exam Dumps Certification Sample Questions:

<https://www.examlabs.com/SAP/SAP-Certified-Technology-Professional/best-P-SECAUTH-21-exam-dumps.html>