Provide Valid P_SECAUTH_21 Dumps To Help You Prepare For Certified Technology Professional - System Security Architect Exam Aug 26, 2023 [Q33-Q52

Provide Valid P_SECAUTH_21 Dumps To Help You Prepare For Certified Technology Professional - System Security Architect Exam Aug 26, 2023
SAP P_SECAUTH_21 Dumps Questions [2023] Pass for P_SECAUTH_21 Exam

SAP P_SECAUTH_21 exam is a certification exam that is designed to test the knowledge and skills of individuals who are interested in pursuing a career as a System Security Architect. P_SECAUTH_21 exam is intended for professionals who have experience working with SAP Security technologies and are looking to validate their expertise in the field of SAP System Security. P_SECAUTH_21 exam covers a wide range of topics, including authentication and authorization, secure communication, secure data management, and secure system configuration.

Q33. You have delimited a single role which is part of a composite role, and a user comparison for the composite role has been performed. You notice that the comparison did NOT remove the profile assignments for that single role. What program would you run to resolve this situation?
* 0 PRGN_COMPRESS_TIMES
* 0PRGN_COMPARE_ROLE_MENU
* 0 PRGN_DELETE_ACT IVITY_GROUPS
* 0 PRGN_MERGE_PREVIEW

Q34. What benefits does the SAP Cloud Connector have compared to a 3rd partyreverse proxy solution, when connecting your SAP Cloud Platform with your SAP backend systems? Note: There are 2 correct answers to this question.
* It establishes an SSL VPN tunnel to SAP Cloud Platform
* It allows for remote invocation by the SAP Cloud Platform only
* It can cache SAP proprietary OData packets to improve the response times
* It supports multiple application protocols, such as HTTP and RFC

Q35. Which platform services are available in the Cloud Foundry? Note: There are 2 correct answers to this question.
* Analytics
* Integration
* Commerce
* Data Quality
Explanation

Analytics and Integration are two of the platform services available in the Cloud Foundry environment of SAP Cloud Platform. Analytics provides capabilities for data visualization, reporting, and dashboarding. Integration provides capabilities for connecting applications, data sources, and processes across different environments.

References: https://help.sap.com/viewer/product/SAP_CLOUD_PLATFORM/Cloud/en-US

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

Q36. Which of the objects do you assign to an SAP Fiori tile to make it visible in the SAP Fiori Launchpad? Note: There are 2 correct answers to this question.
* Group
* Role
* User
* Catalog

Q37. To which services package does SAP Security Optimization Services (SOS) belong?
* Application Integration Optimization
* Performance Optimization
* System Administration Optimization
* EarlyWatch Reporting

Explanation

This is one of the services packages that SAP Security Optimization Services (SOS) belongs to. SOS is a service that enables you to assess and improve the security level of your SAP systems and landscapes based on best practices and recommendations from SAP experts. SOS belongs to System Administration Optimization services package, which is a package that provides services for optimizing various aspects of system administration and operation, such as performance, availability, backup, or security.
References:

https://support.sap.com/en/security/security-optimization-services.html

https://support.sap.com/en/security/security-optimization-services.html

Q38. How are security relevant objects related in the Cloud Foundry?Note: There are 2 correct answers to this question.
* Role Collections have 0 or many roles.
* Role Templates have 0 or many attributes.
* Role Collections have 0 or many role templates.
* Role Templates have 1 or many scopes.

Explanation

These are some of the ways that security relevant objects are related in the Cloud Foundry. Cloud Foundry is a platform-as-a-service (PaaS) that enables developers to deploy and run cloud-native applications using various services and frameworks. Cloud Foundry uses different security relevant objects to manage user access and authorization, such as role collections, roles, role templates, and scopes. Role collections are groups of roles that can be assigned to users or groups. Roles are sets of permissions that define what actions users can perform on resources or services. Role templates are predefined roles that can be reused for different role collections or services. Scopes are strings that represent specific permissions or attributes of a user or service.

References:

https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/en-US/9e1bf57130ef466e8017eab298

Q39. You are evaluating the &#8220;Cross-client object change&#8221; option using transact on SCC4 for your Unit Test Client in the development environment. Which setting do you recommend?
* Changes to repository and cross-client customizing allowed
* No changes to repository and cross-client customizing objects
* No changes to cross-client customizing objects
* No changes to repository objects

Q40. What is the User Management Engine (UME) property &#8220;connect on pooling&#8221; used for? Note: There are 2

correct answers to this question.
* To improve performance of requests to the LDAP directory server
* To avoid unauthorized request to the LDAP directory server
* To create a new connect on to the LDAP directory server for each request
* To share server resources among requesting LDAP clients

Q41. Why should you create multiple dispatchers in SAP Identity Management? Note: There are 2 correct answers to this question.
* To accommodate scalability
* To support fail-over scenarios
* To handle password provisioning
* To handle special network access requirements

Q42. Where does SAP HANA store the values for the default Password Policy parameter? Note: there are 2 correct answers to this question.
* attributes.ini
* indexserver.ini
* nameservice.ini
* global.ini

Q43. You want to configure SNC with X.509 certificates using Common CryptoLib as the cryptographic library in a new installed AS ABAP system. Besides running SNCWIZARD, what do you need to set up for this scenario? Note: There are 2 correct answers to this question.
* Set the environment variable CCL_ PROFILE to the default profile file path
* Maintain the relevant CCL/SNC/&#8217; profile parameters
* Set the environment variable CCL_ PROFILE to SECUDIR
* Set the CCL SNC parameters using sapgenpse

Q44. 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?
* &#8220;Objects not contained in User Buffer&#8221;
* &#8220;No authorizations and does NOT have authorization object in their buffer&#8221;
* &#8220;No authorizations but does have authorization object in their buffer&#8221;
* &#8220;Too many parameters for authorization checks&#8221;

Q45. You want to launch classic SAP GUI transactions directly from the SAP Fiori Launchpad. Which of the following scenarios do you choose?
* Chrome, SAP Enterprise Portal, SAP GUI for Java
* Chrome, SAP Cloud Platform, SAP GUI for Java
* Internet Explorer, ABAP front-end server, SAP GUI for Windows
* Internet Explorer, SAP Business Client, SAP GUI for Windows

Q46. What does return code 1 2 mean when performing STAUTHTRACE?
* An invalid user name was specified in user
* Too many parameters for authorization checks
* No authorization but does have authorization object in user buffer
* No authorization and no authorization object in user buffer
Explanation

Return code 12 means that the user does not have the required authorization for an authority check but does have the authorization object in the user buffer. This means that the user has some values for the authorization object but not the ones that are needed for the specific check. 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_

Q47. What are characteristics of SAP HANA Deployment Infrastructure (HDI) roles? Note: There are 2 correct answers to this question.
* They are transportable between systems.
* They are managed by the native HDI version control.
* They are granted using database procedures.
* They are owned by the user who creates them.
Explanation

These are some of the characteristics of SAP HANA Deployment Infrastructure (HDI) roles. HDI roles are roles that are defined and deployed as part of HDI containers, which are isolated units of database objects and data in SAP HANA systems. HDI roles are managed by the native HDI version control, which tracks changes and dependencies among HDI objects and artifacts. HDI roles are granted using database procedures, such as GRANT_CONTAINER_GROUP_ROLE or GRANT_CONTAINER_SCHEMA_ROLE, which enable dynamic role assignments based on container groups or schemas. References:

https://help.sap.com/viewer/6b94445c94ae495c83a19646e7c3fd56/2.0.05/en-US/fafcbcf9d9101014b3d9a08ce33

Q48. Which authorization object is required to support trusted system access by an RFC user following the configuration of a Managed System in SAP Solution Manager?
* S_RFCACL
* S_ACL_HIST
* S_RFC_TT
* S_RFC_TTAC

Q49. How can you protect a table containing sensitive data using the authorization object S_TABU_DIS?
* The tables containing sensitive data must be named using the authorization object S_TABU_NAM for all responsible administrators. The DICBERCLS fields of the S_TABU_DIS object can then be filled with *.
* Authorization table groups containing tables with sensitive data must be defined in the TDDAT table and these must be omitted for anyone who does not need access to these tables.
* The DICBERCLS field of the authorization object must enumerate all table names of the tables containing sensitive data.
* The tables containing sensitive data must be associated with table groups in the TBRG table.
Explanation

This is one of the ways that you can protect a table containing sensitive data using the authorization object S_TABU_DIS. S_TABU_DIS is an authorization object that controls access to tables based on authorization groups, which are groups of tables that share the same access restrictions. The DICBERCLS field of this authorization object contains the name of the authorization group for a table or a range of tables. To protect a table containing sensitive data using this authorization object, you must assign it to an authorization group and enumerate all table names of the tables containing sensitive data in the DICBERCLS field. References:

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

Q50. The SSO authentication using X.509 client certificates is configured. Users complain that they can&#8217;t log in to the back-end system. The trace file shows the following error message: &#8220;HTTP request [2/5/9] Reject untrusted forwarded certificate&#8221;. What is missing in the configuration? Note: There are 2 correct answers to this question.
* On the back-end, the profile parameter icm/HTTPS/verify client must NOT be set to 0

* On the web-dispatcher, the SAPSSLS.pse must be signed by a trusted certification authority
* On the web-dispatcher, the profile parameter icm/HTTPS/verify_client must be set to 0
* The web dispatcher&#8217;s SAPSSLC.PSE certificate must be added to the trusted reverse proxies list in icm/trusted_reverse_proxy_<xx>

Q51. Who can revoke a runtime role from a user in the SAP HANA tenant database? Note: There are 2 correct answers to this question. Note: there are 2 correct answers to this question.
* Anyone with &#8220;ROLE ADMIN&#8221;
* The grating user
* The owner of the HDI container
* The DBACOCKPIT user

Q52. How is the role concept applied for modeled authorizations based on Core Data Services (CDS) views?
* 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 the CDS views and implicitly applied to each user.
* CDS roles are defined for CDS views in Object Navigator.

Explanation

The role concept for modeled authorizations based on Core Data Services (CDS) views works in this way:

CDS roles are mapped to the CDS view in the access rules that define which users can access which data from the CDS view. The access rules are defined using annotations in the CDS view definition or using a separate access control DDL source file.
References:

https://help.sap.com/viewer/cc0c305d2fab47bd808adcad3ca7ee9d/7.5.9/en-US/fafcbcf9d9101014b3d9a08ce33d

https://help.sap.com/viewer/cc0c305d2fab47bd808adcad3ca7ee9d/7.5.9/en-US/fafcbcf9d9101014b3d9a08ce33d

Achieve Success in Actual P_SECAUTH_21 Exam P_SECAUTH_21 Exam Dumps:
https://www.examslabs.com/SAP/SAP-Certified-Technology-Professional/best-P_SECAUTH_21-exam-dumps.html]