高水準的最新C-SEC-2405考古題，最好的學習資料幫助妳壹次性通過C-SEC-2405考試

P.S. PDFExamDumps在Google Drive上分享了免費的2026 SAP C-SEC-2405考試題庫：https://drive.google.com/open?id=1p3FsUN8k_p0qXccWxwhD1GUS42me8PwD

SAP C-SEC-2405考古題是最新有效的學習資料，由專家認證，涵蓋真實考試內容。擁有高品質的考題資料，能幫助考生通過第一次嘗試的C-SEC-2405考試。我們的C-SEC-2405在線測試引擎版本不光可以模擬真實的考試環境，還支持設備離線使用，方便考生隨時隨地的學習理解。選擇最新版本的SAP C-SEC-2405考古題，如果你考試失敗了，我們將全額退款給你，因為我們有足夠的信心讓你通過C-SEC-2405考試。

SAP C-SEC-2405 考試大綱：

主題	簡介
主題 1	• Governance, Compliance, and Cybersecurity: This section of the exam measures the skills of compliance officers and covers the principles of governance, compliance, and cybersecurity of SAP systems. It includes understanding regulatory requirements and best practices for maintaining security. A critical skill evaluated is ensuring organizational compliance with relevant laws and policies.
主題 2	• Public Cloud User and Role Management: This section of the exam measures the skills of SAP IT cloud Professionals and covers managing users and roles in public cloud environments for SAP applications.
主題 3	• SAP Fiori Authorizations and SAP S • 4HANA: This section of the exam measures the skills of SAP Developers and covers authorization management specific to SAP Fiori applications within SAP S • 4HANA. It emphasizes configuring authorizations for Fiori apps to ensure appropriate access levels. A key skill assessed is understanding Fiori authorization concepts to enhance user experience.
主題 4	• Infrastructure Security and Authentication: This section of the exam measures the skills of SAP IT Professionals and covers infrastructure security measures and authentication methods used in SAP environments. It emphasizes protecting systems from unauthorized access and ensuring secure user authentication.

>> 最新C-SEC-2405考古題 <<

專業的最新C-SEC-2405考古題及資格考試領先提供者和免費下載中的C-SEC-2405：SAP Certified Associate - Security Administrator

PDFExamDumps為通過C-SEC-2405考試提供最完整有效的方案，幫祝廣大考生在考試中獲得更多的優勢。確保你只獲得最新的和最有效的SAP C-SEC-2405考古題，我們也希望客戶能隨時隨地的訪問，于是有了多個版本的題庫資料。PDF版的題庫方便你閱讀，為你真實地再現C-SEC-2405考試題目，軟件版本的題庫作為一個測試引擎，可以幫你模擬真實的C-SEC-2405考試環境，為考生做好充足的考前準備。通過SAP C-SEC-2405考試不再是夢想，我們的考古題就可以確保你成功。

最新的 SAP Certified Associate C-SEC-2405 免費考試真題 (Q12-Q17):

問題 #12
To connect to data sources that are NOT all based on OData, which of the following options does SAP recommend you use?

- A. SAP Integration Suite
- B. SAP Process Integration
- C. Cloud connector
- D. OData Provisioning service

答案：A

解題說明：
For connecting to data sources that are not exclusively based on OData, SAP recommends using the SAP Integration Suite. This comprehensive platform supports a wide range of integration scenarios, including OData, REST, SOAP, and other protocols, making it ideal for connecting diverse data sources, whether on- premise or cloud-based. The SAP Integration Suite provides tools for data mapping, transformation, and orchestration, ensuring seamless and secure data exchange across heterogeneous systems. In contrast, the OData Provisioning service is specifically designed for OData-based integrations, limiting its applicability to non-OData sources. The Cloud connector facilitates secure connectivity between SAP BTP and on-premise systems but is not a complete integration solution. SAP Process Integration, while used for integration in older SAP landscapes, lacks the flexibility and cloud-native capabilities of the SAP Integration Suite. By leveraging the SAP Integration Suite, organizations can achieve robust, scalable, and secure integrations, aligning with SAP's modern integration strategy for complex, multi-protocol environments.

問題 #13
When you maintain authorizations for SAPUI5 Fiori apps, which of the following object types is the front-end authorization object type?

- A. TADIR IWSG - SAP Gateway: Service Groups Metadata
- B. TADIR G4BA - SAP Gateway Odata V4 Backend Service Group & Assignments
- C. TADIR INA1 - InA Service
- D. TADIR IWSV - SAP Gateway Business Suite Enablement-Service

答案：D

解題說明：
For SAPUI5 Fiori apps, the front-end authorization object type is TADIR IWSV (SAP Gateway Business Suite Enablement-Service). This object type represents the OData services used by Fiori apps on the front-end server, and its authorization is managed via the S_SERVICE authorization object in PFCG roles. The IWSV type specifically defines the services that the front-end server calls to access back-end data, requiring start authorizations and default values to be included in the role. TADIR IWSG is used for service group metadata, not front-end authorizations, and TADIR G4BA pertains to OData V4 services, which are less

common in standard SAPUI5 Fiori apps. TADIR INA1 is related to InA (Information Access) services, not typical Fiori app authorizations. By using IWSV, SAP ensures that front-end authorizations are correctly aligned with the OData services powering Fiori apps, providing secure and efficient access control in SAP S/4HANA systems.

問題 #14
In SAP S/4HANA Cloud Public Edition, what can you do with the Display Authorization Trace? Note: There are 3 correct answers to this question.

- A. Analyze authorization check results for already assigned authorizations
- B. Analyze authorization check results for missing authorizations
- C. Adjust role restrictions to further limit access when performing forensic analysis
- D. Display business roles granting specific access
- E. Adjust role restrictions to account for missing authorizations

答案：A,B,D

解題說明：
The Display Authorization Trace in SAP S/4HANA Cloud Public Edition is a powerful tool for analyzing authorization issues. It allows administrators to analyze authorization check results for missing authorizations, identifying gaps where users lack necessary permissions to perform tasks, which is critical for troubleshooting access issues. Additionally, it can display business roles granting specific access, providing visibility into which roles provide permissions for particular applications or data, aiding in role management and compliance checks. The tool also supports analyzing authorization check results for already assigned authorizations, helping administrators verify whether existing permissions are functioning as intended.
However, adjusting role restrictions, either to address missing authorizations or for forensic analysis, is not a function of the Display Authorization Trace, as it is a diagnostic tool, not a maintenance interface. These capabilities make the Display Authorization Trace essential for ensuring secure and efficient access control, supporting both operational and audit requirements in SAP S/4HANA Cloud Public Edition.

問題 #15
Which access categories are available to maintain restrictions in SAP S/4HANA Cloud Public Edition? Note:
There are 3 correct answers to this question.

- A. Value Help (value help access)
- B. Write, Read, Value Help (write access)
- C. Write, Read (write access)
- D. Read, Value Help (read access)
- E. Read (read access)

答案：A,B,D

解題說明：
In SAP S/4HANA Cloud Public Edition, access restrictions are maintained using specific access categories to control user permissions granularly. The available categories include "Read, Value Help (read access)," which allows users to view data and access value help functionalities; "Value Help (value help access)," which restricts access to only value help features; and "Write, Read, Value Help (write access)," which grants permissions for creating, modifying, reading, and using value help. These categories enable precise control over user access to data and functionalities, ensuring compliance with security policies. The options "Read (read access)" and "Write, Read (write access)" are not standard access categories in this context, as they do not fully align with the system's predefined restriction types.

問題 #16
Which protocol is the industry standard for provisioning identity and access management in hybrid landscapes?

- A. SSL
- B. OIDC
- C. SAML
- D. SCIM

答案：D

解題說明：
The System for Cross-domain Identity Management (SCIM) is the industry standard protocol for provisioning identity and access management in hybrid landscapes. SCIM enables automated user provisioning and deprovisioning across different systems, including cloud and on-premise environments, by standardizing the exchange of user identity data. It supports operations like creating, updating, and deleting user accounts, making it ideal for managing identities in hybrid SAP landscapes where integration between SAP Cloud Identity Services and on-premise systems is required. SAML (Security Assertion Markup Language) is used for single sign-on authentication, not provisioning. OIDC (OpenID Connect) is an authentication protocol built on OAuth, and SSL (Secure Sockets Layer) is a security protocol for data encryption, not identity provisioning. SCIM's role as a provisioning standard ensures efficient and secure identity management, reducing administrative overhead and enhancing interoperability in complex SAP and non-SAP hybrid environments.

問題 #17
......