Workday-Pro-Integrations시험대비덤프공부인기시험덤프

그리고 ITDumpsKR Workday-Pro-Integrations 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1wpnP5ugMUsu3WIRIf87LWq2yOOgjT1Au

IT인증시험을 쉽게 취득하는 지름길은ITDumpsKR에 있습니다. ITDumpsKR의Workday인증 Workday-Pro-Integrations 덤프로 시험준비를 시작하면 성공에 가까워집니다. Workday인증 Workday-Pro-Integrations덤프는 최신 시험문제 출제방향에 대비하여 제작된 예상문제와 기출문제의 모음자료입니다. Workday인증 Workday-Pro-Integrations덤프는 시험을 통과한 IT업계종사자분들이 검증해주신 세련된 공부자료입니다. ITDumpsKR의Workday인증 Workday-Pro-Integrations덤프를 공부하여 자격증을 땁시다.

Workday Workday-Pro-Integrations 시험요강:

주제	소개
주제 1	• Integrations: This section of the exam measures the skills of Integration Specialists and covers the full spectrum of integration techniques in Workday. It includes an understanding of core integration architecture, APIs, Workday Studio, and integration system user setup. The focus is on building scalable, maintainable, and secure integrations that ensure seamless system interoperability.
주제 2	• Cloud Connect: This section of the exam measures the skills of Workday Implementation Consultants and focuses on using Workday Cloud Connect solutions for third-party integration. It includes understanding pre-built connectors, configuration settings, and how to manage data flow between Workday and external systems while ensuring security and data integrity.
주제 3	• Calculated Fields: This section of the exam measures the skills of Workday Integration Analysts and covers the creation, configuration, and management of calculated fields used to transform, manipulate, and format data in Workday integrations. It evaluates understanding of field types, dependencies, and logical operations that enable dynamic data customization within integration workflows.

주제 4	• Enterprise Interface Builders: This section of the exam measures the skills of Integration Developers and covers the use of Workday's Enterprise Interface Builder (EIB) to design, deploy, and maintain inbound and outbound integrations. It evaluates the candidate's ability to create templates, configure transformation rules, schedule integrations, and troubleshoot EIB workflows efficiently.

Workday-Pro-Integrations최신버전덤프 & Workday-Pro-Integrations시험패스 인증공부

다년간 IT업계에 종사하신 전문가들이 자신의 노하우와 경험으로 제작한 Workday Workday-Pro-Integrations덤프는 Workday-Pro-Integrations 실제 기출문제를 기반으로 한 자료로서 Workday-Pro-Integrations시험문제의 모든 범위와 유형을 포함하고 있어 높을 적중율을 자랑하고 있습니다.덤프구매후 불합격 받으시면 구매일로부터 60일내 주문은 덤프비용을 환불해드립니다.IT 자격증 취득은 ITDumpsKR덤프가 정답입니다.

최신 Workday Integrations Workday-Pro-Integrations 무료샘플문제 (Q40-Q45):

질문 # 40
After configuring domain security policies, what task must you run to ensure the most recent changes go into effect?

- A. Activate All Pending Authentication Policy Changes
- B. Activate Previous Security Timestamp
- C. Activate Metadata Schedule
- D. Activate Pending Security Policy Changes

정답：D

설명：
Whenever changes are made to domain security policies, they remain in a pending state until you explicitly activate them by running the:
Activate Pending Security Policy Changes task.
This ensures that all updates to permissions are applied across the tenant for real-time enforcement.
Why the others are incorrect:
A . Activate Previous Security Timestamp reverts to a prior configuration.
B . Activate All Pending Authentication Policy Changes is only for authentication rules.
D . Activate Metadata Schedule applies to metadata changes, not security.

질문 # 41
Refer to the following XML to answer the question below.

```
1. <ps:Positions xmlns:ps="urn:com.workday/coreconnector/positions"
2.     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
3.     <ps:Position>
4.         <ps:Position_Data>
5.             <ps:Position_ID>P-00030</ps:Position_ID>
6.             <ps:Job_Posting_Title>Senior IT Analyst</ps:Job_Posting_Title>
7.             <ps:Available_For_Hire>true</ps:Available_For_Hire>
8.             <ps:Availability_Date>2021-02-04</ps:Availability_Date>
9.             <ps:Location>San Francisco</ps:Location>
10.            <ps:Worker_Type>FT</ps:Worker_Type>
11.        </ps:Position_Data>
12.    </ps:Position>
13. </ps:Positions>
```


You need the integration file to format the ps:PositionJD field to 10 characters and report any truncated values as an error.
How will you start your template match on ps:Position to use Document Transformation (DT) to do the transformation using ETV with your truncation validation?

- A.


- B.


- C.


- D.


정답：A

설명：

In Workday integrations, Document Transformation (DT) using XSLT is employed to transform XML data, such as the output from a Core Connector or EIB, into a specific format for third-party systems. In this scenario, you need to transform the ps:Position_ID field within the ps:Position element to a fixed length of 10 characters and report any truncation as an error using Workday's Extension for Transformation and Validation (ETV) attributes. The template must match the ps:Position element and apply the specified formatting and validation rules.

Here's why option D is correct:

Template Matching: The <xsl:template match="ps:Position"> correctly targets the ps:Position element in the XML, as shown in the provided snippet, ensuring the transformation applies to the appropriate node.

ETV Attributes:

etv:fixedLength="10" specifies that the Pos_ID field should be formatted to a fixed length of 10 characters. This ensures the output is truncated or padded (if needed) to meet the length requirement.

etv:reportTruncation="error" instructs the transformation to raise an error if the ps:Position_ID value exceeds 10 characters and cannot be truncated without data loss, aligning with the requirement to report truncated values as errors.

XPath Selection: The <xsl:value-of select="ps:Position_Data/ps:Position_ID"/> correctly extracts the ps:Position_ID value from the ps:Position_Data child element, as shown in the XML structure (<ps:Position_ID>P-00030</ps:Position_ID>).

Output Structure: The <Position><Pos_ID>...</Pos_ID></Position> structure ensures the transformed data is wrapped in meaningful tags for the target system, maintaining consistency with Workday integration practices.

Why not the other options?

A .

xml

WrapCopy

<xsl:template match="ps:Position">

<Position>

<Pos_ID etv:fixedLength="10">

<xsl:value-of select="ps:Position_Data/ps:Position_ID"/>

</Pos_ID>

</Position>

</xsl:template>

This option includes etv:fixedLength="10" but omits etv:reportTruncation="error". Without the truncation reporting, it does not meet the requirement to report truncated values as errors, making it incorrect.
B .
xml
WrapCopy
<xsl:template match="ps:Position">
<Position etv:fixedLength="10">
<Pos_ID etv:reportTruncation="error">
<xsl:value-of select="ps:Position_Data/ps:Position_ID"/>
</Pos_ID>
</Position>
</xsl:template>
This applies etv:fixedLength="10" to the Position element instead of Pos_ID, and etv:reportTruncation="error" to Pos_ID. However, ETV attributes like fixedLength and reportTruncation should be applied to the specific field being formatted (Pos_ID), not the parent element (Position). This misplacement makes it incorrect.
C .
xml
WrapCopy
<xsl:template match="ps:Position">
<Position etv:fixedLength="10">
<Pos_ID etv:reportTruncation="error">
<xsl:value-of select="ps:Position_Data/ps:Position_ID"/>
</Pos_ID>
</Position>
</xsl:template>
Similar to option B, this applies etv:fixedLength="10" to Position and etv:reportTruncation="error" to Pos_ID, which is incorrect for the same reason: ETV attributes must be applied to the specific field (Pos_ID) requiring formatting and validation, not the parent element.
To implement this in XSLT for a Workday integration:
Use the template from option D to match ps:Position, apply etv:fixedLength="10" and etv:reportTruncation="error" to the Pos_ID element, and extract the ps:Position_ID value using the correct XPath. This ensures the ps:Position_ID (e.g., "P-00030") is formatted to 10 characters and reports any truncation as an error, meeting the integration file requirements.
:
Workday Pro Integrations Study Guide: Section on "Document Transformation (DT) and ETV" - Details the use of ETV attributes like fixedLength and reportTruncation for formatting and validating data in XSLT transformations.
Workday Core Connector and EIB Guide: Chapter on "XML Transformations" - Explains how to use XSLT templates to transform position data, including ETV attributes for length and truncation validation.
Workday Integration System Fundamentals: Section on "ETV in Integrations" - Covers the application of ETV attributes to specific fields in XML for integration outputs, ensuring compliance with formatting and error-reporting requirements.

질문 # 42
When creating an ISU, what should you do to ensure the user only authenticates via web services?

- A. Select the Do Not Allow UI Sessions checkbox.
- B. Choose a constrained security group.
- C. Update the session timeout minutes.
- D. Generate a random password.

정답：A

설명:
When creating an Integration System User (ISU) in Workday, the goal is often to ensure that the user is restricted to performing tasks via web services (e.g., API calls or integrations) and cannot log into the Workday user interface (UI). This is a critical security measure to limit the ISU's access to only what is necessary for integration purposes, adhering to the principle of least privilege. Let's evaluate each option provided in the question to determine the correct approach based on Workday's functionality and best practices as outlined in official documentation and the Workday Pro Integrations program.
Option A: Choose a constrained security group.In Workday, security groups define the permissions and access levels for users, including ISUs. There are two types of Integration System Security Groups (ISSGs): constrained and unconstrained. A constrained ISSG limits access to specific organizations or data scopes, while an unconstrained ISSG provides broader access across the tenant. While choosing a constrained security group can enhance security by limiting the scope of data the ISU can access, it does not

directly control whether the ISU authenticates via web services or the UI. The type of security group affects data access permissions, not the authentication method or UI access. Therefore, this option does not address the requirement of ensuring authentication only via web services.
Option B: Select the Do Not Allow UI Sessions checkbox.When creating an ISU in Workday, the "Create Integration System User" task presents an option labeled "Do Not Allow UI Sessions." Selecting this checkbox explicitly prevents the ISU from logging into the Workday UI using its credentials. This setting ensures that the ISU can only authenticate and operate through programmatic means, such as web service calls (e.g., SOAP or REST APIs), which is precisely the intent of the question. This is a standard security practice recommended by Workday to isolate integration activities from interactive user sessions, reducing the risk of misuse or unauthorized access through the UI. This option directly aligns with the requirement and is the correct answer.
Option C: Update the session timeout minutes.The "Session Timeout Minutes" field in the ISU creation task determines how long an ISU's session remains active before it expires. By default, this is set to 0, meaning the session does not expire, which is suitable for integrations that require continuous operation without interruption. Updating this value (e.g., setting it to a specific number of minutes) would cause the session to time out after that period, potentially disrupting long-running integrations. However, this setting pertains to session duration, not the method of authentication or whether UI access is allowed. It does not prevent the ISU from logging into the UI or ensure that authentication occurs only via web services, making this option irrelevant to the question.
Option D: Generate a random password.Generating a random password for the ISU is a good security practice to ensure the credentials are strong and not easily guessable. However, the password itself does not dictate how the ISU authenticates or whether it can access the UI. A random password enhances security but does not inherently restrict the ISU to web service authentication. Without selecting "Do Not Allow UI Sessions," the ISU could still log into the UI with that password, assuming no other restrictions are applied. Thus, this option does not fulfill the requirement of ensuring authentication only via web services.
Why Option B is Correct
The "Do Not Allow UI Sessions" checkbox is a specific configuration in the ISU setup process that directly enforces the restriction of authentication to web services. This setting is part of Workday's security framework for integrations, ensuring that ISUs-designed as non-human accounts for programmatic access-cannot be used interactively. This aligns with Workday's best practices for securing integrations, as outlined in the Workday Pro Integrations Study Guide and related documentation. For example, when an ISU is created with this checkbox selected, any attempt to log into the Workday UI with its credentials will fail, while web service requests (e.g., via SOAP or REST APIs) will succeed, assuming proper permissions are granted via an ISSG.
Practical Application
To implement this in Workday:
Log into your Workday tenant with administrative privileges.
Search for and select the "Create Integration System User" task.
Enter a username and password for the ISU.
Check the "Do Not Allow UI Sessions" checkbox.
Leave "Session Timeout Minutes" at 0 (default) to avoid session expiration during integrations.
Save the ISU and assign it to an appropriate ISSG (constrained or unconstrained, depending on the integration's needs).
This configuration ensures the ISU is locked to web service authentication, meeting the question's objective.
Verification with Workday Documentation
The Workday Pro Integrations Study Guide emphasizes securing ISUs by restricting them to integration-specific tasks. The "Do Not Allow UI Sessions" option is highlighted as a key control for preventing UI access, ensuring that ISUs operate solely through web services. This is also consistent with broader Workday security training materials, such as those available on Workday Community, which stress isolating integration accounts from human user activities.
Workday Pro Integrations Study Guide Reference
Section: Integration Security Fundamentals - Discusses the role of ISUs and the importance of restricting their access to programmatic interactions.
Section: Configuring Integration System Users - Details the "Create Integration System User" task, including the "Do Not Allow UI Sessions" checkbox as a security control.
Section: Best Practices for Integration Security - Recommends using this setting to enforce least privilege and protect the tenant from unauthorized UI access by integration accounts.

질문 # 43
Refer to the following scenario to answer the question below.
You have been asked to build an integration using the Core Connector: Worker template and should leverage the Data Initialization Service (DIS). The integration will be used to export a full file (no change detection) for employees only and will include personal data.
What configuration is required to ensure that when outputting phone number only the home phone number is included in the output?

- A. Include the phone type integration field attribute.
- B. Configure an integration field override to include phone type.
- C. Configure the phone type integration attribute.

- D. Configure an integration map to map the phone type.

정답：A

설명：
The scenario involves a Core Connector: Worker integration using DIS to export a full file of employee personal data, with the requirement to output only the home phone number when including phone data. Workday's "Phone Number" field is multi-instance, meaning a worker can have multiple phone types (e.g., Home, Work, Mobile). Let's determine the configuration:
Requirement:Filter the multi-instance "Phone Number" field to include only the "Home" phone number in the output file. This involves specifying which instance of the phone data to extract.
Integration Field Attributes:In Core Connectors, Integration Field Attributes allow you to refine how multi-instance fields are handled in the output. For the "Phone Number" field, you can set an attribute like "Phone Type" to "Home" to ensure only home phone numbers are included. This is a field-level configuration that filters instances without requiring a calculated field or override.
Option Analysis:
A . Configure an integration map to map the phone type: Incorrect. Integration Maps transform field values (e.g., "United States" to "USA"), not filter multi-instance data like selecting a specific phone type.
B . Include the phone type integration field attribute: Correct. This configures the "Phone Number" field to output only instances where the phone type is "Home," directly meeting the requirement.
C . Configure the phone type integration attribute: Incorrect. "Integration attribute" refers to integration-level settings (e.g., file format), not field-specific configurations. The correct term is "integration field attribute." D . Configure an integration field override to include phone type: Incorrect. Integration Field Overrides are used to replace a field's value with a calculated field or custom value, not to filter multi-instance data like phone type.
Implementation:
Edit the Core Connector: Worker integration.
Navigate to the Integration Field Attributes section for the "Phone Number" field.
Set the "Phone Type" attribute to "Home" (or equivalent reference ID for Home phone).
Test the output file to confirm only home phone numbers are included.
Reference from Workday Pro Integrations Study Guide:
Core Connectors & Document Transformation: Section on "Integration Field Attributes" explains filtering multi-instance fields like phone numbers by type.
Integration System Fundamentals: Notes how Core Connectors handle multi-instance data with field-level attributes.

질문 # 44
An external system needs a file containing data for recent compensation changes. They would like to receive a file routinely at 5 PM eastern standard time, excluding weekends. The file should show compensation changes since the last integration run.
What is the recurrence type of the integration schedule?

- A. Recurs every 12 hours
- B. Dependent recurrence
- C. Recurs every weekday
- D. Recurs every 1 day(s)

정답：C

설명：
Understanding the Requirement
The question involves scheduling an integration in Workday to deliver a file containing recent compensation changes to an external system. The key requirements are:
* The file must be delivered routinely at 5 PM Eastern Standard Time (EST).
* The recurrence should exclude weekends (i.e., run only on weekdays: Monday through Friday).
* The file should include compensation changes since the last integration run, implying an incremental data pull, though this does not directly affect the recurrence type.
The task is to identify the correct recurrence type for the integration schedule from the given options:
A). Recurs every 12 hours
B). Recurs every weekday
C). Dependent recurrence
D). Recurs every 1 day(s)
Analysis of the Workflow and Recurrence Options
In Workday, integrations are scheduled using the Integration Schedule functionality, typically within tools like Enterprise Interface Builder (EIB) or Workday Studio, though this scenario aligns closely with EIB for routine file-based integrations. The recurrence

type determines how frequently and under what conditions the integration runs. Let's evaluate each option against the requirements:
Step-by-Step Breakdown
* Time Specification (5 PM EST):
* Workday allows scheduling integrations at a specific time of day (e.g., 5 PM EST). This is set in the schedule configuration and is independent of the recurrence type but confirms the need for a daily-based recurrence with a specific time slot.
* Exclusion of Weekends:
* The requirement explicitly states the integration should not run on weekends (Saturday and Sunday), meaning it should only execute on weekdays (Monday through Friday). This is a critical filter for choosing the recurrence type.
* Incremental Data (Since Last Run):
* The file must include compensation changes since the last integration run. In Workday, this is typically handled by configuring the integration (e.g., via a data source filter or "changed since" parameter in EIB), not the recurrence type. Thus, this requirement does not directly influence the recurrence type but confirms the integration runs periodically.

질문 # 45
......

myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes