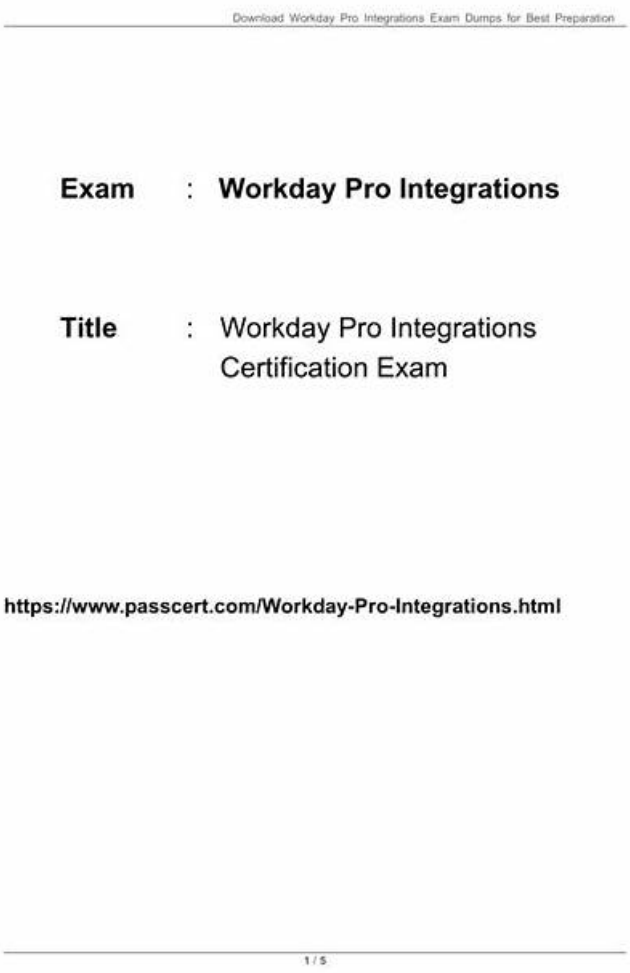
Latest Workday-Pro-Integrations Training - Latest Workday-Pro-Integrations Exam Experience



P.S. Free 2026 Workday Workday-Pro-Integrations dumps are available on Google Drive shared by NewPassLeader: https://drive.google.com/open?id=1BasnD2iR9HbLSMPBFD-Lr0mGinnJDnOP

Our Workday-Pro-Integrations preparation materials will be the good helper for your qualification certification. We are concentrating on providing high-quality authorized Workday-Pro-Integrations study guide all over the world so that you can clear Workday-Pro-Integrations exam one time. Our Workday-Pro-Integrations reliable exam bootcamp materials contain three formats: PDF version, Soft test engine and APP test engine so that our Workday-Pro-Integrations Exam Questions are enough to satisfy different candidates' habits and cover nearly full questions & answers of the Workday-Pro-Integrations real test.

Workday Workday-Pro-Integrations Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.

Topic 2	• Reporting: This section of the exam measures the skills of Reporting Analysts and focuses on building, modifying, and managing Workday reports that support integrations. It includes working with report writer tools, custom report types, calculated fields within reports, and optimizing report performance to support automated data exchange.
Topic 3	• 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.
Topic 4	• 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.

Pass Guaranteed Quiz 2026 Workday-Pro-Integrations: Workday Pro Integrations Certification Exam Marvelous Latest Training

Now on the Internet, a lot of online learning platform management is not standard, some web information may include some viruses, cause far-reaching influence to pay end users and adverse effect. Choose the Workday-Pro-Integrations Study Tool, can help users quickly analysis in the difficult point, high efficiency of review, and high quality through the Workday Pro Integrations Certification Exam exam, work for our future employment and increase the weight of the promotion, to better meet the needs of their own development.

Workday Pro Integrations Certification Exam Sample Questions (Q53-Q58):

NEW QUESTION # 53
What is the purpose of granting an ISU modify access to the Integration Event domain via an ISSG?

- A. To have the ISU own the integration schedule.
- B. To build the integration system as the ISU.
- C. To log into the user interface as the ISU and launch the integration.
- D. To let the ISU configure integration attributes and maps.

Answer: D

Explanation:
Understanding ISUs and Integration Systems in Workday
* Integration System User (ISU): An ISU is a specialized user account in Workday designed for integrations, functioning as a service account to authenticate and execute integration processes. ISUs are created using the "Create Integration System User" task and are typically configured with settings like disabling UI sessions and setting long session timeouts (e.g., 0 minutes) to prevent expiration during automated processes. ISUs are not human users but are instead programmatic accounts used for API calls, EIBs, Core Connectors, or other integration mechanisms.
* Integration Systems: In Workday, an "integration system" refers to the configuration or setup of an integration, such as an External Integration Business (EIB), Core Connector, or custom integration via web services. Integration systems are defined to handle data exchange between Workday and external systems, and they require authentication, often via an ISU, to execute tasks like data retrieval, transformation, or posting.
* Assigning ISUs to Integration Systems: ISUs are used to authenticate and authorize integration systems to interact with Workday. When configuring an integration system, you assign an ISU to provide the credentials needed for the integration to run. This assignment ensures that the integration can access Workday data and functionalities based on the security permissions granted to the ISU via its associated Integration System Security Group (ISSG).
* Limitation on Assignment: Workday's security model imposes restrictions to maintain control and auditability. Specifically, an ISU is designed to be tied to a single integration system to ensure clear accountability, prevent conflicts, and simplify security management. This limitation prevents an ISU from being reused across multiple unrelated integration systems, reducing the risk of unintended access or data leakage.

Evaluating Each Option
Let's assess each option based on Workday's integration and security practices:
Option A: An ISU can be assigned to five integration systems.
* Analysis: This is incorrect. Workday does not impose a specific numerical limit like "five" for ISU assignments to integration systems. Instead, the limitation is more restrictive: an ISU is typically assigned to only one integration system to ensure focused security and accountability. Allowing an ISU to serve multiple systems could lead to confusion, overlapping permissions, or security risks, which Workday's design avoids.
* Why It Doesn't Fit: There's no documentation or standard practice in Workday Pro Integrations suggesting a limit of five integration systems per ISU. This option is arbitrary and inconsistent with Workday's security model.
Option B: An ISU can be assigned to an unlimited number of integration systems.
* Analysis: This is incorrect. Workday's security best practices do not allow an ISU to be assigned to an unlimited number of integration systems. Allowing this would create security vulnerabilities, as an ISU' s permissions (via its ISSG) could be applied across multiple unrelated systems, potentially leading to unauthorized access or data conflicts. Workday enforces a one-to-one or tightly controlled relationship to maintain auditability and security.
* Why It Doesn't Fit: The principle of least privilege and clear accountability in Workday integrations requires limiting an ISU's scope, not allowing unlimited assignments.
Option C: An ISU can be assigned to only one integration system.
* Analysis: This is correct. In Workday, an ISU is typically assigned to a single integration system to ensure that its credentials and permissions are tightly scoped. This aligns with Workday's security model, where ISUs are created for specific integration purposes (e.g., an EIB, Core Connector, or web service integration). When configuring an integration system, you specify the ISU in the integration setup (e.g., under "Integration System Attributes" or "Authentication" settings), and it is not reused across multiple systems to prevent conflicts or unintended access. This limitation ensures traceability and security, as the ISU's actions can be audited within the context of that single integration.
* Why It Fits: Workday documentation and best practices, including training materials and community forums, emphasize that ISUs are dedicated to specific integrations. For example, when creating an EIB or Core Connector, you assign an ISU, and it is not shared across other integrations unless explicitly reconfigured, which is rare and discouraged for security reasons.
Option D: An ISU can only be assigned to an ISSG and not an integration system.
* Analysis: This is incorrect. While ISUs are indeed assigned to ISSGs to inherit security permissions (as established in Question 26), they are also assigned to integration systems to provide authentication and authorization for executing integration tasks. The ISU's role includes both: it belongs to an ISSG for permissions and is linked to an integration system for execution. Saying it can only be assigned to an ISSG and not an integration system misrepresents Workday's design, as ISUs are explicitly configured in integration systems (e.g., EIB, Core Connector) to run processes.
* Why It Doesn't Fit: ISUs are integral to integration systems, providing credentials for API calls or data exchange. Excluding assignment to integration systems contradicts Workday's integration framework.
Final Verification
The correct answer is Option C, as Workday limits an ISU to a single integration system to ensure security, accountability, and clarity in integration operations. This aligns with the principle of least privilege, where ISUs are scoped narrowly to avoid overexposure. For example, when setting up a Core Connector: Job Postings (as in Question 25), you assign an ISU specifically for that integration, not multiple ones, unless reconfiguring for a different purpose, which is atypical.
Supporting Documentation
The reasoning is based on Workday Pro Integrations security practices, including:
* Workday Community documentation on creating and managing ISUs and integration systems.
* Tutorials on configuring EIBs, Core Connectors, and web services, which show assigning ISUs to specific integrations (e.g., Workday Advanced Studio Tutorial).
* Integration security overviews from implementation partners (e.g., NetIQ, Microsoft Learn, Reco.ai) emphasizing one ISU per integration for security.
* Community discussions on Reddit and Workday forums reinforcing that ISUs are tied to single integrations for auditability (r/workday on Reddit).
This question focuses on the purpose of granting an Integration System User (ISU) modify access to the Integration Event domain via an Integration System Security Group (ISSG) in Workday Pro Integrations. Let' s analyze the role of the ISU, the Integration Event domain, and evaluate each option to determine the correct answer.
Understanding ISUs, ISSGs, and the Integration Event Domain
* Integration System User (ISU): As described in previous questions, an ISU is a service account for integrations, used to authenticate and execute integration processes in Workday. ISUs are assigned to ISSGs to inherit security permissions and are linked to specific integration systems (e.g., EIBs, Core Connectors) for execution.
* Integration System Security Group (ISSG): An ISSG is a security group that defines the permissions for ISUs, controlling what data and functionalities they can access or modify. ISSGs can be unconstrained (access all instances) or constrained (access specific instances based on context). Permissions are granted via domain security policies, such as "Get," "Put," "View," or "Modify," applied to Workday domains.
* Integration Event Domain: In Workday, the Integration Event domain (or Integration Events security domain) governs access to integration-related activities, such as managing integration events, schedules, attributes, mappings, and logs. This domain is critical for

integrations, as it controls the ability to create, modify, or view integration configurations and runtime events.
* "Modify" access to the Integration Event domain allows the ISU to make changes to integration configurations, such as attributes (e.g., file names, endpoints), mappings (e.g., data transformations), and event settings (e.g., schedules or triggers).
* This domain does not typically grant UI access or ownership of schedules but focuses on configuration and runtime control.
* Purpose of Granting Modify Access: Granting an ISU modify access to the Integration Event domain via an ISSG enables the ISU to perform configuration tasks for integrations, ensuring the integration system can adapt or update its settings programmatically. This is essential for automated integrations that need to adjust mappings, attributes, or event triggers without manual intervention. However, ISUs are not designed for UI interaction or administrative ownership, as they are service accounts.
Evaluating Each Option
Let's assess each option based on Workday's security and integration model:
Option A: To have the ISU own the integration schedule.
* Analysis: This is incorrect. ISUs do not "own" integration schedules or any other integration components. Ownership is not a concept applicable to ISUs, which are service accounts for execution, not administrative entities. Integration schedules are configured within the integration system (e.g., EIB or Core Connector) and managed by administrators or users with appropriate security roles, not by ISUs. Modify access to the Integration Event domain allows changes to schedules, but it doesn't imply ownership.
* Why It Doesn't Fit: ISUs lack administrative control or ownership; they execute based on permissions, not manage schedules as owners. This misinterprets the ISU's role.
Option B: To let the ISU configure integration attributes and maps.
* Analysis: This is correct. Granting modify access to the Integration Event domain allows the ISU to alter integration configurations, including attributes (e.g., file names, endpoints, timeouts) and mappings (e.g., data transformations like worker subtype mappings from Question 25). The Integration Event domain governs these configuration elements, and "Modify" permission enables the ISU to update them programmatically during integration execution. This is a standard use case for ISUs in automated integrations, ensuring flexibility without manual intervention.
* Why It Fits: Workday's documentation and training materials indicate that the Integration Event domain controls integration configuration tasks. For example, in an EIB or Core Connector, an ISU with modify access can adjust mappings or attributes, as seen in tutorials on integration setup (Workday Advanced Studio Tutorial). This aligns with the ISU's role as a service account for dynamic configuration.
Option C: To log into the user interface as the ISU and launch the integration.
* Analysis: This is incorrect. ISUs are not intended for UI interaction. When creating an ISU, a best practice is to disable UI sessions (e.g., set "Allow UI Sessions" to "No") and configure a session timeout of 0 minutes to prevent expiration during automation. ISUs operate programmatically via APIs or integration systems, not through the Workday UI. Modify access to the Integration Event domain enables configuration changes, not UI login or manual launching.
* Why It Doesn't Fit: Logging into the UI contradicts ISU design, as they are service accounts, not user accounts. This option misrepresents their purpose.
Option D: To build the integration system as the ISU.
* Analysis: This is incorrect. ISUs do not "build" integration systems; they execute or configure existing integrations based on permissions. Building an integration system (e.g., creating EIBs, Core Connectors, or web services) is an administrative task performed by users with appropriate security roles (e.g., Integration Build domain access), not ISUs. Modify access to the Integration Event domain allows configuration changes, not the creation or design of integration systems.
* Why It Doesn't Fit: ISUs lack the authority or capability to build integrations; they are for runtime execution and configuration, not development or design.
Final Verification
The correct answer is Option B, as granting an ISU modify access to the Integration Event domain via an ISSG enables it to configure integration attributes (e.g., file names, endpoints) and maps (e.g., data transformations), which are critical for dynamic integration operations. This aligns with Workday's security model, where ISUs handle automated tasks within defined permissions, not UI interaction, ownership, or system building.
For example, in the Core Connector: Job Postings from Question 25, an ISU with modify access to Integration Event could update the filename pattern or worker subtype mappings, ensuring the integration adapts to vendor requirements without manual intervention. This is consistent with Workday's design for integration automation.
Supporting Documentation
The reasoning is based on Workday Pro Integrations security practices, including:
* Workday Community documentation on ISUs, ISSGs, and domain security (e.g., Integration Event domain permissions).
* Tutorials on configuring EIBs and Core Connectors, showing ISUs modifying attributes and mappings (Workday Advanced Studio Tutorial).
* Integration security overviews from implementation partners (e.g., NetIQ, Microsoft Learn, Reco.ai) detailing domain access for ISUs.
* Community discussions on Reddit and Workday forums reinforcing ISU roles for configuration, not UI or ownership (r/workday on Reddit).

NEW QUESTION # 54
Refer to the following scenario to answer the question below.
You have configured a Core Connector: Worker integration, which utilizes the following basic configuration:
* Integration field attributes are configured to output the Position Title and Business Title fields from the Position Data section.
* Integration Population Eligibility uses the field Is Manager which returns true if the worker holds a manager role.
* Transaction Log service has been configured to Subscribe to specific Transaction Types: Position Edit Event.
You launch your integration with the following date launch parameters (Date format of MM/DD/YYYY):
* As of Entry Moment: 05/25/2024 12:00:00 AM * Effective Date: 05/25/2024
* Last Successful As of Entry Moment: 05/23/2024 12:00:00 AM
* Last Successful Effective Date: 05/23/2024
To test your integration, you made a change to a worker named Jared Ellis who is assigned to the manager role for the IT Help Desk department. You use the Change Business Title related action on Jared and update the Business Title of the position to a new value. Jared Ellis' worker history shows the Title Change Event as being successfully completed with an effective date of 05/24/2024 and an Entry Moment of 05/24/2024 07:58:53 AM however Jared Ellis does not show up in your output. What configuration element would have to be modified for the integration to include Jared Ellis in the output?

- A. Integration Population Eligibility
- B. Integration Field Attributes
- C. Transaction log subscription
- D. Date launch parameters

Answer: C

Explanation:
The scenario involves a Core Connector: Worker integration configured to output Position Title and Business Title fields for workers who meet the Integration Population Eligibility criteria (Is Manager = true), with the Transaction Log service subscribed to the "Position Edit Event." The integration is launched with specific date parameters, and a test is performed by updating Jared Ellis' Business Title using the "Change Business Title" related action. Jared is a manager, and the change is logged with an effective date of 05/24/2024 and an entry moment of 05/24/2024 07:58:53 AM. Despite this, Jared does not appear in the output. Let's determine why and identify the configuration element that needs modification.
In Workday, the Core Connector: Worker integration uses the Transaction Log service to detect changes based on subscribed transaction types. The subscribed transaction type in this case is "Position Edit Event," which is triggered when a position is edited via the "Edit Position" business process. However, the test scenario involves a "Change Business Title" related action, which is a distinct business process in Workday. This action updates the Business Title field but does not necessarily trigger a "Position Edit Event." Instead, it generates a different event type, such as a "Title Change Event" (as noted in Jared's worker history), depending on how the system logs the action.
The date launch parameters provided are:
As of Entry Moment: 05/25/2024 12:00:00 AM - The latest point for entry moments.
Effective Date: 05/25/2024 - The latest effective date for changes.
Last Successful As of Entry Moment: 05/23/2024 12:00:00 AM - The starting point for entry moments from the last run.
Last Successful Effective Date: 05/23/2024 - The starting point for effective dates from the last run.
Jared's change has:
Entry Moment: 05/24/2024 07:58:53 AM - Falls between 05/23/2024 12:00:00 AM and 05/25/2024 12:00:00 AM.
Effective Date: 05/24/2024 - Falls between 05/23/2024 and 05/25/2024.
The date parameters correctly cover the time window of Jared's change, meaning the issue is not with the date range but with the event detection logic. The Transaction Log subscription determines which events are processed by the integration. Since the subscription is set to "Position Edit Event" and the change was made via "Change Business Title" (logged as a "Title Change Event"), the integration does not recognize this event because it is not subscribed to the appropriate transaction type.
To include Jared Ellis in the output, the Transaction Log subscription must be modified to include the event type associated with the "Change Business Title" action, such as "Title Change Event" or a broader category like "Position Related Event" that encompasses both position edits and title changes. This ensures the integration captures the specific update made to Jared's Business Title.
Let's evaluate the other options:
B . Date launch parameters: The parameters already include Jared's entry moment and effective date within the specified ranges (05/23/2024 to 05/25/2024). Adjusting these would not address the mismatch between the subscribed event type and the actual event triggered.
C . Integration Field Attributes: These are set to output Position Title and Business Title, and the change to Business Title is within scope. The field configuration is correct and does not need modification.
D . Integration Population Eligibility: This is set to "Is Manager = true," and Jared is a manager. This filter is functioning as intended and is not the issue.
The root cause is the Transaction Log subscription not aligning with the event type generated by the "Change Business Title" action, making A. Transaction log subscription the correct answer.

Workday Pro Integrations Study Guide Reference
Workday Integrations Study Guide: Core Connector: Worker - Section on "Transaction Log Configuration" explains how subscribing to specific transaction types filters the events processed by the integration.
Workday Integrations Study Guide: Change Detection - Details how different business processes (e.g., Edit Position vs. Change Business Title) generate distinct event types in the Transaction Log.
Workday Integrations Study Guide: Event Subscription - Notes the importance of aligning subscription types with the specific business actions being tested or monitored.

NEW QUESTION # 55
What is the limitation when assigning ISUs to integration systems?

- A. An ISU can only be assigned to an ISSG and not an integration system.
- B. An ISU can be assigned to five integration systems.
- C. An ISU can be assigned to only one integration system.
- D. An ISU can be assigned to an unlimited number of integration systems.

Answer: C

Explanation:
This question examines the limitations on assigning Integration System Users (ISUs) to integration systems in Workday Pro Integrations. Let's analyze the relationship and evaluate each option to determine the correct answer.
Understanding ISUs and Integration Systems in Workday
* Integration System User (ISU):An ISU is a specialized user account in Workday designed for integrations, functioning as a service account to authenticate and execute integration processes. ISUs are created using the "Create Integration System User" task and are typically configured with settings like disabling UI sessions and setting long session timeouts (e.g., 0 minutes) toprevent expiration during automated processes. ISUs are not human users but are instead programmatic accounts used for API calls, EIBs, Core Connectors, or other integration mechanisms.
* Integration Systems:In Workday, an "integration system" refers to the configuration or setup of an integration, such as an External Integration Business (EIB), Core Connector, or custom integration via web services. Integration systems are defined to handle data exchange between Workday and external systems, and they require authentication, often via an ISU, to execute tasks like data retrieval, transformation, or posting.
* Assigning ISUs to Integration Systems:ISUs are used to authenticate and authorize integration systems to interact with Workday. When configuring an integration system, you assign an ISU to provide the credentials needed for the integration to run. This assignment ensures that the integration can access Workday data and functionalities based on the security permissions granted to the ISU via its associated Integration System Security Group (ISSG).
* Limitation on Assignment:Workday's security model imposes restrictions to maintain control and auditability. Specifically, an ISU is designed to be tied to a single integration system to ensure clear accountability, prevent conflicts, and simplify security management. This limitation prevents an ISU from being reused across multiple unrelated integration systems, reducing the risk of unintended access or data leakage.
Evaluating Each Option
Let's assess each option based on Workday's integration and security practices:
Option A: An ISU can be assigned to five integration systems.
* Analysis:This is incorrect. Workday does not impose a specific numerical limit like "five" for ISU assignments to integration systems. Instead, the limitation is more restrictive: an ISU is typically assigned to only one integration system to ensure focused security and accountability. Allowing an ISU to serve multiple systems could lead to confusion, overlapping permissions, or security risks, which Workday's design avoids.
* Why It Doesn't Fit:There's no documentation or standard practice in Workday Pro Integrations suggesting a limit of five integration systems per ISU. This option is arbitrary and inconsistent with Workday's security model.
Option B: An ISU can be assigned to an unlimited number of integration systems.
* Analysis:This is incorrect. Workday's security best practices do not allow an ISU to be assigned to an unlimited number of integration systems. Allowing this would create security vulnerabilities, as an ISU' s permissions (via its ISSG) could be applied across multiple unrelated systems, potentially leading to unauthorized access or data conflicts. Workday enforces a one-to-one or tightly controlled relationship to maintain auditability and security.
* Why It Doesn't Fit:The principle of least privilege and clear accountability in Workday integrations requires limiting an ISU's scope, not allowing unlimited assignments.
Option C: An ISU can be assigned to only one integration system.
* Analysis:This is correct. In Workday, an ISU is typically assigned to a single integration system to ensure that its credentials and permissions are tightly scoped. This aligns with Workday's security model, where ISUs are created for specific integration purposes (e.g., an EIB, Core Connector, or web service integration). When configuring an integration system, you specify the ISU in the integration setup (e.g., under "Integration System Attributes" or "Authentication" settings), and it is not reused across multiple systems

to prevent conflicts or unintended access. This limitation ensures traceability and security, as the ISU's actions can be audited within the context of that single integration.
* Why It Fits:Workday documentation and best practices, including training materials and community forums, emphasize that ISUs are dedicated to specific integrations. For example, when creating an EIB or Core Connector, you assign an ISU, and it is not shared across other integrations unless explicitly reconfigured, which is rare and discouraged for security reasons.
Option D: An ISU can only be assigned to an ISSG and not an integration system.
* Analysis:This is incorrect. While ISUs are indeed assigned to ISSGs to inherit security permissions (as established in Question 26), they are also assigned to integration systems toprovide authentication and authorization for executing integration tasks. The ISU's role includes both: it belongs to an ISSG for permissions and is linked to an integration system for execution. Saying it can only be assigned to an ISSG and not an integration system misrepresents Workday's design, as ISUs are explicitly configured in integration systems (e.g., EIB, Core Connector) to run processes.
* Why It Doesn't Fit:ISUs are integral to integration systems, providing credentials for API calls or data exchange. Excluding assignment to integration systems contradicts Workday's integration framework.
Final Verification
The correct answer is Option C, as Workday limits an ISU to a single integration system to ensure security, accountability, and clarity in integration operations. This aligns with the principle of least privilege, where ISUs are scoped narrowly to avoid overexposure. For example, when setting up a Core Connector: Job Postings (as in Question 25), you assign an ISU specifically for that integration, not multiple ones, unless reconfiguring for a different purpose, which is atypical.
Supporting Documentation
The reasoning is based on Workday Pro Integrations security practices, including:
* Workday Community documentation on creating and managing ISUs and integration systems.
* Tutorials on configuring EIBs, Core Connectors, and web services, which show assigning ISUs to specific integrations (e.g.,Workday Advanced Studio Tutorial).
* Integration security overviews from implementation partners (e.g., NetIQ, Microsoft Learn, Reco.ai) emphasizing one ISU per integration for security.
* Community discussions on Reddit and Workday forums reinforcing that ISUs are tied to single integrations for auditability (r/workday on Reddit).

NEW QUESTION # 56
You are creating an outbound connector using the Core Connector: Organization Outbound template. The vendor has provided the following requirements for how the data should appear in the output file.
The vendor would also like to change the default document retention policy of 30 days to 7 days. What tasks do you need to use to configure this in your connector?

- A. Configure Integration Maps and Configure Integration Attributes
- B. Configure Integration Maps and Configure Integration Field Attributes
- C. Configure Integration Field Overrides and Configure Integration Field Attributes
- D. Configure Integration Field Overrides and Configure Integration Attributes

Answer: D

Explanation:
When creating an outbound connector using the Workday Core Connector: Organization Outbound template, you need to configure the connector to meet specific vendor requirements, such as formatting output data and adjusting document retention policies. Let's break down the question and analyze the requirements and options based on Workday's integration framework, specifically focusing on the Core Connector and its configuration tasks.
Understanding the Requirements
* Output Data Formatting:The vendor has provided a table specifying how organization types should appear in the output file (e.g., Cost Center as "CC", Pay Group as "PAY", Supervisory as "S", and any other value as "OTHER"). This indicates a need to transform or map Workday organization data into specific output values, which is typically handled by configuring how fields are processed or mapped in the integration.
* Document Retention Policy Change:The vendor wants to change the default document retention policy from 30 days to 7 days. In Workday, document retention policies for integrations (e.g., files stored on SFTP or other delivery methods) are managed through integration settings, specifically attributes related to file retention or delivery options.
Analyzing Workday Core Connector: Organization Outbound
The Core Connector: Organization Outbound template is a pre-built Workday integration template used to extract organization-related data (e.g., cost centers, pay groups, supervisory organizations) and send it to an external system. It leverages Workday's integration framework, including integration maps, field overrides, and attributes, to customize data output and behavior.
* Integration Maps: Used to define how data is transformed or mapped from Workday to the output format, often involving XSLT or predefined mappings.

* Integration Field Overrides: Allow you to override or customize how specific fields are displayed or formatted in the output, such as mapping "Cost Center" to "CC" as per the vendor's table.
* Integration Attributes: Control broader integration settings, such as delivery methods, file formats, and retention policies (e.g., document retention duration).
* Integration Field Attributes: Typically focus on specific field-level properties but are less commonly used for retention policies or broad mappings compared to the above options.
Evaluating the Vendor's Output Requirements
The table provided (Cost Center # "CC", Pay Group # "PAY", Supervisory # "S", any other value # "OTHER") suggests a need to transform or override the default output values for organization types. This is a field-level customization, best handled by Integration Field Overrides, which allow you to specify custom values or formats for specific fields in the output.
* For example, in the Core Connector, you can use Integration Field Overrides to map the Workday organization type (e.g., "Cost_Center") to the vendor's desired output ("CC"). This is a common practice for outbound integrations where external systems require specific formatting.
Evaluating the Retention Policy Change
The default document retention policy of 30 days needs to be changed to 7 days. In Workday, retention policies for integration output files (e.g., files delivered via SFTP or email) are configured as part of the integration's attributes, not field-level settings.
* Integration Attributes are used to manage integration-wide settings, including delivery options, file retention periods, and other global configurations. You can specify the retention period (e.g., 7 days) in the attributes section of the Core Connector configuration.
* This is distinct from field-level overrides or maps, as retention is not tied to individual data fields but to the integration's output management.
Analyzing the Options
Now, let's evaluate each option to determine which tasks are needed to meet both requirements:
* A. Configure Integration Maps and Configure Integration Attributes
* Integration Maps: These are used for broader data transformations or mappings, such as converting Workday XML to another format or defining complex data relationships. While they could theoretically handle the output value mappings (e.g., Cost Center # "CC"), they are typically more complex and less granular than field overrides for simple value changes.
* Integration Attributes: Correct for configuring the retention policy (e.g., changing from 30 to 7 days), as attributes manage integration-wide settings like retention.
* Why Not Sufficient?: Integration Maps are overkill for simple field value overrides like the vendor's table, and field-level customization is better handled by Integration Field Overrides for precision and ease.
* B. Configure Integration Field Overrides and Configure Integration Field Attributes
* Integration Field Overrides: Correct for mapping specific field values (e.g., Cost Center # "CC"), as they allow granular control over output formats for individual fields.
* Integration Field Attributes: These are less commonly used and typically focus on field-specific properties (e.g., data type, length), not broad integration settings like retention policies. Retention is not managed at the field level, so this is incorrect for the retention requirement.
* Why Not Sufficient?: Integration Field Attributes do not handle retention policies, making this option incomplete.
* C. Configure Integration Field Overrides and Configure Integration Attributes
* Integration Field Overrides: Perfect for mapping the vendor's output values (e.g., Cost Center # "CC", Pay Group # "PAY", etc.), as they allow precise control over field-level output formatting.
* Integration Attributes: Correct for configuring the retention policy (e.g., changing from 30 to 7 days), as attributes manage integration-wide settings like file retention.
* Why Sufficient?: This combination addresses both requirements-field-level output formatting and integration-wide retention policy changes-making it the most accurate choice.
* D. Configure Integration Maps and Configure Integration Field Attributes
* Integration Maps: As explained, these are better for complex transformations, not simple field value overrides like the vendor's table. They could work but are less efficient than field overrides.
* Integration Field Attributes: As noted, these do not handle retention policies or broad integration settings, making them incorrect for the retention requirement.
* Why Not Sufficient?: This combination fails to address retention effectively and uses Integration Maps when Integration Field Overrides would be more appropriate for the output formatting.
Conclusion
Based on the analysis, the vendor's requirements for output formatting (mapping organization types to specific values) and changing the retention policy (from 30 to 7 days) are best met by:
* Integration Field Overrides: To customize the output values for organization types (e.g., Cost Center # "CC") as shown in the table.
* Integration Attributes: To adjust the document retention policy from 30 days to 7 days.

NEW QUESTION # 57
How many integration systems can an ISU be assigned to concurrently?

- A. Unlimited
- B. Three
- C. Five
- D. One

Answer: A

Explanation:
The Integration System User (ISU) in Workday is a specialized user account designed for automation and system-level integrations. It can be assigned to any number of integration systems concurrently - there is no limit.
From Workday documentation and Pro training:
"A single ISU can be assigned to multiple integration systems across tenants and environments, provided it has the correct permissions and security group assignments. Workday does not impose a hard limit on the number of systems an ISU can be linked to." This design provides scalability for environments with multiple integrations (e.g., EIBs, Core Connectors, Studio integrations) without needing to create redundant users.
Incorrect Options Explained:
* A, B, C: These options imply arbitrary limits (one, three, five), which do not exist in Workday's ISU architecture.
References:
Workday Pro: Integrations - Integration System Security User Management Workday Community: How ISUs Function in Multi-Integration Environments

NEW QUESTION # 58
.....

Do you want to pass the Workday-Pro-Integrations exam with 100% success guarantee? Our Workday-Pro-Integrations training quiz is your best choice. With the assistance of our study materials, you will advance quickly. Also, all Workday-Pro-Integrations guide materials are compiled and developed by our professional experts. So you can totally rely on our Workday-Pro-Integrations Exam simulating to aid you pass the exam. What is more, you will learn all knowledge systematically and logically, which can help you memorize better.

Training □ The page for free download of ☀ Workday-Pro-Integrations □☀□ on 《 www.examdiscuss.com 》 will open immediately □Workday-Pro-Integrations Training Materials

- 2026 Workday-Pro-Integrations: High Hit-Rate Latest Workday Pro Integrations Certification Exam Training □ Search for ➥ Workday-Pro-Integrations □ and obtain a free download on 「 www.pdfvce.com 」 □Latest Workday-Pro-Integrations Exam Book
- Workday Pro Integrations Certification Exam Updated Torrent - Workday-Pro-Integrations Study Questions - Workday-Pro-Integrations Updated Material □ Open [www.torrentvce.com] enter ➠ Workday-Pro-Integrations □ and obtain a free download □New Workday-Pro-Integrations Dumps Questions
- 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, www.stes.tyc.edu.tw, zenwriting.net, bbs.t-firefly.com, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 Workday Workday-Pro-Integrations dumps are available on Google Drive shared by NewPassLeader: https://drive.google.com/open?id=1BasnD2iR9HbLSMPBFD-Lr0mGinnJDnOP