

Archer

Archer-Expert

Archer Certified Administrator-Expert



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

What action should never be completed using the Advanced Workflow Job Troubleshooting tool?

- A. Canceling a job.
- B. Manually moving a record to the next node.
- C. Editing the Advanced Workflow.
- D. Restarting a job.

Answer: C

Explanation:

The Advanced Workflow Job Troubleshooting tool is a runtime utility designed to manage individual "instances" of records currently enrolled in a workflow. It is used to fix records that are stuck due to errors. According to the Advanced Workflow Beyond the Basics guide, this tool is purely for operational maintenance (Cancel, Reset, Restart, or "Force" movement).

Editing the Advanced Workflow structure (changing the flowchart, adding nodes, or modifying logic) cannot be done within the Troubleshooting tool. Workflow design changes must be made in the Application Builder under the Workflow tab. Attempting to "fix" a logic error by changing the design is a development task, whereas the Troubleshooting tool is an administrative task for existing data.

Furthermore, editing a workflow requires saving a new version and potentially migrating active jobs, a process entirely separate from the record-level "Reset/Cancel" functions found in the Job Troubleshooting interface.

Question: 2

Dynamic Filtering can be found in which of the following areas? Select all that apply:

- A. Record Lookup
- B. Calculated Cross Reference
- C. Report Object
- D. Advanced Search

Answer: A, B, C

Explanation:

Dynamic Filtering is a sophisticated feature that allows Archer to filter data based on the context of the current record or the current user. In Archer Administration II , this is highlighted as a tool for improving the user experience by reducing "data noise."

Record Lookup (A): Allows you to filter the available records in a lookup based on a value in the current record (e.g., only show "Users" that belong to the "Department" selected on the form).

Calculated Cross Reference (B): Uses dynamic logic to automatically link records based on matching field values.

Report Object (C): When a report is placed on a record as a "Record-Level Report," Dynamic Filtering ensures the report only shows data related to that specific record (e.g., showing only "Findings" related to "Asset A" when viewing Asset A).

Advanced Search (D) does NOT support Dynamic Filtering in the same "contextual" sense; Advanced Searches use static filters or "Current User" filters, but they do not dynamically react to field values in a specific source record during the search build process like the other three objects.

Question: 3

Which would be an accurate function(s) description for Archer LDAP Synchronization?

- A. None of these answer are correct
- B. Updates user profile data and deactivates accounts based on LDAP changes
- C. Only creates accounts for new users found on the LDAP server
- D. Only associates Archer users/groups with domain users/groups

Answer: B

Explanation:

In Archer, the LDAP Synchronization process is a comprehensive identity management tool. According to the Archer Administration II curriculum, its primary purpose is to ensure that the Archer user database mirrors the corporate directory (Active Directory/LDAP). It is not limited to just creating accounts or linking groups; its most critical function is the automation of the user lifecycle .

When the sync runs, it checks for changes in the LDAP source. If a user's department or email changes in Active Directory, Archer updates the user profile data accordingly. Most importantly for security, if a user is disabled or removed from the LDAP group/OU being synced, Archer can automatically deactivate the account (or move it to a "terminated" status) based on the "Missing Person" configuration in the LDAP setup. This prevents unauthorized access by former employees. Options C and D are "Only" statements that describe small portions of the tool's capability, whereas Option B captures the ongoing maintenance and security synchronization that is the hallmark of the Archer LDAP service.

Question: 4

What happens if an Administrator runs a Data Import source file that contains a value for a Values List field that is not an existing value?

- A. The Data Import will process and this value will be discarded.
- B. The Data Import fails unless this new value is appended to the values available for selection.
- C. The new value will be added to the record and appended to the Values List field values available for selection.
- D. The new value will be added to the record only with no change to the Values List field values.

Answer: B

Explanation:

In Archer, Values List fields are strictly validated against the pre-defined options in the field configuration. During a manual Data Import, if the source file contains a value that does not exactly match an existing entry in the Values List, the import for that specific record (or the entire process, depending on settings) will fail.

According to the Archer Administration II guide, for the import to succeed with new data, the administrator must first enable the "Create new values for Values List fields" option in the Data Import settings. If this is not enabled, Archer treats the unknown value as an error. This is a critical data integrity feature that prevents "dirty data" from entering the system. Unlike a Data Feed, which has more advanced "lookup" and "creation" logic, the Data Import tool is less flexible by default to ensure administrators are consciously deciding whether to expand the application's metadata.

Question: 5

Which of the following are automatically assigned by Archer when a new user is created?

- A. Username, default Security Parameter, and default Access Role
- B. One time password, Default Email Address
- C. Default Access Role, Default Email Address
- D. Default Security Parameter and Default Access Role

Answer: D

Explanation:

In the Manage Users section of Archer, the platform uses global defaults to ensure that new accounts are created with a baseline security posture. According to the Archer Administration II security module, every new user record is automatically assigned the Default Security Parameter and the Default Access Role defined in the instance settings.

The Security Parameter (Option D) governs password complexity, expiration, and session timeouts. The Default Access Role typically provides very limited "Read" access to ensure the user can at least log in to the workspace, but usually requires further administrative adjustment to grant functional permissions. A Username (Option A) must be manually entered or mapped from LDAP; Archer cannot guess a unique username. Similarly, email addresses and passwords require specific input or integration triggers. By automatically assigning the default Security Parameter and Access Role, Archer ensures that no user is created without essential security governance already in place.

Question: 6

Failed user login, Access Role Created and Deleted, and password change by user events are viewed in:

- A. Access Control Rights by Role Report
- B. Locked Accounts Report
- C. Security Events Report

Answer: C

Explanation:

The Security Events Report is the primary auditing tool for tracking administrative and sensitive user actions within the Archer platform. According to the Archer Administration II curriculum, this report captures a broad spectrum of "event-based" security data that standard access reports do not cover. Specifically, it logs every failed login attempt, which is critical for identifying potential brute-force attacks. It also tracks metadata changes to the security infrastructure, such as when an Access Role is created or deleted, providing an audit trail of who modified the system's permissions. Furthermore, it records password changes initiated by users. While the "Locked Accounts Report" (Option B) only shows users currently barred from the system, the Security Events Report provides the historical context of why those events occurred. It is an essential resource for compliance officers and system auditors to ensure that the integrity of the Archer environment's security configuration remains intact.

Question: 7

When selecting "Load Fields" in the Source Definition tab > Source Data sub-tab of an Archer Web Services Transporter Data Feed, no fields appear. What should you check to fix this?

- A. Confirm the Data Feed is set to Active.
- B. Confirm the Data Feed target application or questionnaire is set correctly.
- C. Confirm the settings on the Source Definition tab > Data Filter sub-tab are correct.
- D. Confirm the settings on the Transport Configuration section within the Source Connection tab are correct.

Answer: D

Explanation:

The Archer Web Services Transporter is used for "Archer-to-Archer" data feeds. For the "Load Fields" button to work, Archer must be able to successfully authenticate and connect to the source instance's API to retrieve the report metadata.

As detailed in the Archer Administration II Data Feed module, if no fields appear, it almost always indicates a communication failure between the Feed Manager and the Web Service. The Transport Configuration section (found on the Source Connection tab) contains the critical connection details: the Base URL, the Instance Name, and the User Credentials. If the credentials are incorrect, the URL is mistyped, or the "Session Token" cannot be generated, Archer cannot "see" the source report's structure, and thus the field list will remain empty. Checking the connection settings is the primary troubleshooting step before looking at filters or target mappings.

Question: 8

What feature in the Administration Menu allows you to troubleshoot users' record permissions?

- A. Manage Users
- B. Admin Notifications
- C. Access Control Reports
- D. Investigate Access

Answer: D

Explanation:

In the Archer security model, record-level access is determined by the complex intersection of Access Roles , Groups , and Record Permission Fields . According to the Archer Administration II curriculum, the Investigate Access tool is the primary diagnostic utility for troubleshooting "Why can't User X see Record Y?"

Unlike standard reports, Investigate Access allows an administrator to select a specific user and a specific record (or application) and run a simulation. The tool then provides a detailed breakdown of the "Final Access" (Read, Update, Delete) and, crucially, explains how that access was derived. It will highlight if the user is being granted access via a specific Group, if a Record Permission field is restricting them, or if their Access Role lacks the necessary rights. This is more efficient than the Access Control Reports (Option C), which provide a broad overview of permissions but do not provide the record-specific context that "Investigate Access" offers for pinpoint troubleshooting.

Question: 9

When Sarah gets to work, she logs into her Windows computer using her username and password. As part of her daily routine, she needs to view some reports inside Archer. How does Sarah access Archer reports without typing her login details again?

- A. By manually entering her credentials
- B. With biometric authentication
- C. By using a password manager
- D. Through Windows Integrated SSO

Answer: D

Explanation:

The scenario described is a classic implementation of Windows Integrated Authentication (WIA) , a form of Single Sign-On (SSO). As detailed in the Archer Installation and Troubleshooting guides, when Archer is configured for Windows Integrated SSO, it leverages the Kerberos or NTLM protocol. Since Sarah has already authenticated to the Windows Domain at the start of her shift, her browser passes her "security token" directly to the Archer web server (IIS).

The Archer Control Panel (ACP) must be configured to recognize the domain, and the user's Archer account must have their Windows account name (e.g., DOMAIN\Username) populated in the "Domain Account" field. This creates a seamless "handshake" that bypasses the Archer login screen entirely. Unlike a password manager (Option C), which still technically "types" the details, or biometrics (Option B), which requires a new physical scan, Windows Integrated SSO provides a passive experience where the existing OS-level authentication is trusted by the application, drastically improving user workflow and productivity.

Question: 10

For multi-host environments, which statement of the following is TRUE regarding the set up of the servers?

- A. File share can only be accessed by the web server.
- B. All Archer components exist on one server.
- C. A load balancer is not needed if there are more than one web server.
- D. All servers should be on the same network.

Answer: D

Explanation:

In a Multi-Host (Distributed) Environment , Archer components (Web, Application, and Database tiers) are spread across multiple physical or virtual machines to ensure high availability and scalability. According to the Archer Installation and Troubleshooting guides within the Administration II curriculum, it is a technical requirement that all servers within the Archer instance be on the same network or have high-speed, low-latency connectivity between them. This is because the Archer Control Panel (ACP) and the various services (Async, Indexing, Queuing) must communicate constantly to synchronize metadata and process jobs.

Option A is incorrect because the File Store must be accessible by both the Web and Services servers to handle attachments. Option B describes a "Single-Host" setup, not a multi-host one. Option C is false because if you have multiple Web Servers, a Load Balancer is mandatory to distribute user traffic and provide failover. Without being on the same network/segment, the latency would cause the Archer Services to "time out," leading to job engine failures and significant performance degradation across the platform.

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/archer-expert>