KillTest

質量更高　服務更好

練習題

https://www.killtest.net

一年免費更新服務

Exam : **Archer Expert**

Title : Archer Certified Administrator-Expert

Version : DEMO

1.As an Archer administrator, you need to run calculations on Exception Requests daily to see if they have expired and update the Overall Status field accordingly. However, when you enable the Recalculation Schedule for the application, the job is taking a long time to run.
What step(s) are recommended to speed up the process?
A. Create a Schedule and use a filter to run the calculation only for those Exception Requests that are Approved.
B. Update the Overall Status calculation to include an IF statement based on the Expiration Date.
C. Use Data-Driven Events by creating a Set Values List action to update the status and associate it with a rule that evaluates the Expiration Date.
D. Update the value manually.
Answer: A
Explanation:
In the Archer platform, the Recalculation Schedule (found within the application's General Tab) is a powerful tool, but it can become a performance bottleneck if not configured efficiently. When a recalculation job is triggered, the Archer services must evaluate every record in the application to determine if calculations need to be updated. According to the Archer Administration II curriculum, the most effective way to optimize this process is by using Calculation Filters.
By selecting option A, you are instructing the system to ignore records that are irrelevant to the specific business logic (e.g., records that are already "Expired," "Rejected," or "Draft"). By filtering the schedule to run only for "Approved" requests, the job engine processes a significantly smaller subset of data, which reduces the load on the Async Service and speeds up the completion time.
Option B would likely slow the system down further by adding logical complexity to the calculation itself.
Option C (Data-Driven Events) is not suitable for date-based triggers because DDEs only fire upon a record "Save" event; they cannot proactively "watch" a date to trigger a change without user intervention or a scheduled recalculation.

2.Which statement best describes the advantages of using SSO in Archer?
A. All these answers are correct
B. Reduced Password Fatigue and Help Desk Costs
C. Increased Productivity
D. Improved Security
Answer: A
Explanation:
According to the Archer Administration and Security documentation, Single Sign-On (SSO) integration provides a multi-faceted advantage for both the end-user and the system administrator. Reduced Password Fatigue occurs because users no longer need to remember unique credentials for Archer, which directly leads to a decrease in Help Desk Costs associated with password reset requests. Increased Productivity is achieved through seamless access; users can move from their workstation or corporate portal directly into Archer without the interruption of a manual login prompt.
+1
Furthermore, Improved Security is a primary driver for SSO. By leveraging centralized authentication providers (like Active Directory via SAML 2.0 or Windows Integrated Authentication), Archer administrators ensure that corporate password policies (complexity, rotation, and MFA) are strictly enforced. When an employee leaves the organization and their account is disabled in the central

directory, their access to Archer is revoked instantaneously. This eliminates the risk of "orphan accounts" existing within the Archer user database. Therefore, because SSO addresses administrative overhead, user experience, and enterprise-grade security protocols simultaneously, "All these answers are correct" is the verified professional standard.

3.What should you do if the LDAP status remains QUEUED for an extended period?
A. Reconfigure the LDAP settings
B. Restart the server
C. Check the network connection
D. Ensure the Archer LDAP synchronization service is running
Answer: D
Explanation:
In the Archer environment, LDAP synchronization is an asynchronous process managed by the Archer Support Tools and specific Windows services. When an administrator triggers a manual LDAP sync or a scheduled sync begins, the job is placed into a processing queue within the Archer database. If the status remains "QUEUED" and never progresses to "IN PROGRESS" or "COMPLETED," the primary culprit is almost always the underlying service responsible for picking up that task.
As detailed in the Archer Administration II technical troubleshooting modules, the Archer LDAP Synchronization Service (or in newer versions, the Archer Queuing/Job Engine service) must be in a "Started" state on the web or application server to process these requests. If the service is stopped, hung, or crashed, the job will sit in the queue indefinitely. While network connections (Option C) and configuration settings (Option A) are important, they typically result in an "FAILED" status with an error log rather than a "QUEUED" status. Restarting the entire server (Option B) is an inefficient "last resort" that doesn't address the specific root cause as directly as verifying the service status in the Services console.

4.Which users are capable of performing data imports?
A. Only System Administrators
B. Only Report Administrators
C. Members of the Data Import group
D. Any user with proper access role permissions
Answer: D
Explanation:
In Archer, the ability to perform a data import is governed by Access Roles, not strictly by high-level system administrative accounts. Under the "Rights" tab of an Access Role configuration, there is a specific permission labeled “Data Import. “According to the Archer Administration II curriculum, any user assigned to a role with this right enabled—and who also possesses "Create" or "Update" permissions for the target application—can utilize the Data Import tool.
While a System Administrator (Option A) inherently has these rights, the platform is designed for delegated administration. Therefore, a business user or a "Power User" can be granted the specific ability to import data without having full system-wide control.
Options B and C are incorrect because "Report Administrators" focus on dashboard and report metadata, and while an administrator might create a custom group named "Data Import," no such hard-coded group exists by default in the Archer out-of-the-box security model. The granularity of Archer's

security ensures that data integrity is maintained by linking the import capability directly to the user's functional role and application-level permissions.

5.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.