Safe-Update

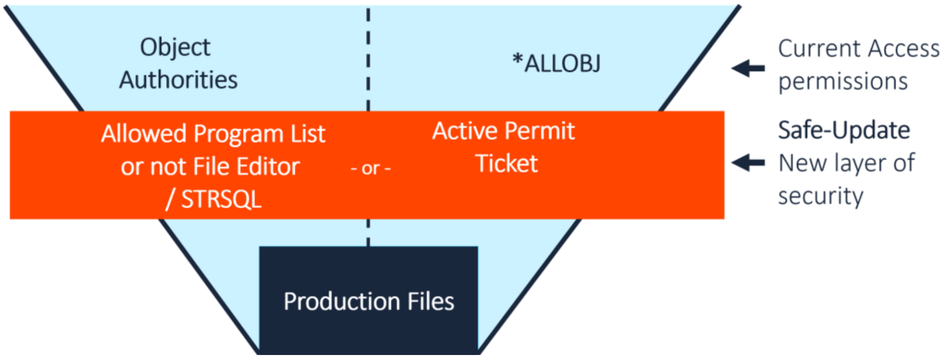
Overview

Safe-Update protects IBM i business-critical data against updates made using programming tools or programs which are not among those that are dedicated to update this data.

Security systems limit what users can do. Safe-Update adds a layer of security: it identifies the program that wishes to update the secured file and decides whether or not to allow it. The Sarbanes-Oxley Act and other regulations require that only authorized programs update critical data. Programs such as DFU, the interactive Start SQL (STRSQL) command, and third-party file editors are therefore considered potentially risky and are forbidden. Using such programs makes your systems unreliable and creates a huge risk of fraud.

Security systems that protect data by preventing the access of programmers to production environments are not enough. Occasionally programmers need to conduct some missions and temporarily get *ALLOBJ authority. As there is no way to restrict them to that mission, they became a potential risk.

Safe-Update's new security layer ensures that only authorized programs are used to update business critical files.



The Safe-Update Solution

Safe-Update is the latest component of Raz-Lee's iSecurity suite.

Once set, Safe-Update protects all updates and ensure they are done by specified programs, by creating specified whitelists or blacklists.

A whitelist specifies the programs that can update a file. It contains multiple entries, each specifying generic program names and generic library names.

A standard blacklist of programs, specifying DFU, STRSQL and other known file editors, is provided with the product. It can be modified according to the organization needs.

Safe-Update implements a workflow for situations when there is a need to update data with tools or programs that are not normally allowed. The workflow is based on work orders, created by management. A work order specifies the reason it was opened, the programmer or programmers that can perform it, the file or files the programmer can update, the time frame that it remains active, and more.

When an assigned programmer is ready, he generates a ticket under the work order. The ticket instructs Safe-Update to allow his activity and trace it. All work is logged, even if the data files themselves are not journaled.

Some organizations may allow ad-hoc tickets. These tickets are not related to existing work orders. Instead, the tickets themselves contain all the relevant information.

Key Features

- Monitors and protects updates to data according to the program used.
- Uses either a whitelist of allowed programs, or a blacklist of programs that are not allowed.
- Ensures that DFU, Start SQL and file editors are not used in production environments even when *ALLOBJ is in effect.
- Restriction of updates can be removed when the update is only for field marked in advance as “insignificant”.
- Programs that may not update data can read it. They will be stopped when an update is issued.
- Comprehensive workflow of management-approved work orders with tickets opened by preassigned programmers.

- Organizations may decide to also allow ad-hoc tickets.
- Additional permission may be requested in real time
- Ticket is opened for the current job or for the current user.
- Ticket opened for the current user, allows updates by batches jobs as well.
- Ticket become automatically invalid after few minutes of inactivity.
- Manages the full history of the activities.
- Creates full trace of updates even when the file is not journaled.
- When AP-Journal commands are used to display update information from the standard database journals, updates made under Safe-Update are highlighted.
- Possibility to undo updates.