May 2008

General New Features

iSecurity Central Administration (for Audit & Firewall):

The **iSecurity Central Administration** module was extensively enhanced to simplify the distribution of Audit & Firewall definitions and logs throughout a network of System i computers.

Central Administration enables copying definitions and generating reports on systems which are part of a network. This product includes:

a) Automatic distribution of definitions from a local system to networked systems
b) Automatic collection of log files from networked systems to a local system
c) Generate Firewall or Audit reports based upon information collected at run-time from a defined set of networked systems
d) Generate Firewall or Audit reports for networked systems based upon libraries copied to a local system

Benefits:

Define groups of network nodes for easy processing
Remote or local report execution
Remote or local printing of reports
User profile and definition coordination between nodes in the network
GUI and green-screen based

Features Details:

Export Definitions Commands (EXPS1DFN and EXPS2DFN) were modified to send the definitions from a source machine to a Group or All System i target systems on the network and restore the definitions on the target machine.

Import Definitions Commands (IMPS1DFN and IMPS2DFN) were modified to restore the definitions from a *SAVF file as well as a *PF file that contains the data of the *SAVF.

Added display of a full network log and current job network log for auditing distribution of definitions.

Added new commands: Export iSecurity/BASE Log (EXPS2LOG) & Import iSecurity/BASE Log (IMPS2LOG) for Audit and Firewall log distribution have been added..

Product Installation (for Audit & Firewall)

Upgrades can now be performed while Audit or Firewall are active (not applicable for "super speed"). Benefit: no need to stop the Firewall protection and Audit monitoring while upgrading. An updated Installation Manual will soon be available.

Secondary Passwords

Secondary passwords now default to *BLANK , thus not displaying a request to enter a password.

Benefit: start working faster with the product without the need to remember and enter an additional password.

Secondary passwords are now based on the SYSTEM name instead of *ALL. In the rare case that the system name is changed (via CHGNETA), the passwords are no longer valid. To establish a set of default passwords, run the command CALL GSIPWDR (QQQ 1).

Benefit: define secondary password only for the user profile who requires second level security.

iSecurity New Features

Firewall 14.0:

Additional security-related analysis has been added for CALL QCMDEXC/QCAPCMD when used in CMD, FTP, DDM, and to API calls in QSYS.

Firewall exits can be run in conjunction with other exit programs, meaning that parallel activation of Firewall and another similar product is possible. Use GO GSPRLL for description and activation.

Modifications were made to Firewall SUSPEND & RESUME commands enabling them to be scheduled during weekends for preparation of "Super Speed" install.

Audit 10.0:

New audit events which are relevant to release 5.4 and higher were added to QAUDLVL.

S/36 environment – The CD audit type was not recorded properly for OS in some releases only. In coordination with IBM, a solution was found and implemented

Capture 2.0:

Capture is now a stand alone product, completely separate from Audit.

Customers of the current combined Audit/Capture product should upgrade Audit and install Capture.

Benefit: The customer can install only Capture and not the full iSecurity-Part 2 package. This also enables distributing Capture for use as an OEM product.

Screen 14.0:

A pasthrough screen that is ended now returns to the original system, similar to SIGNOFF ENDCNN(*YES).

AP-Journal 4.1:

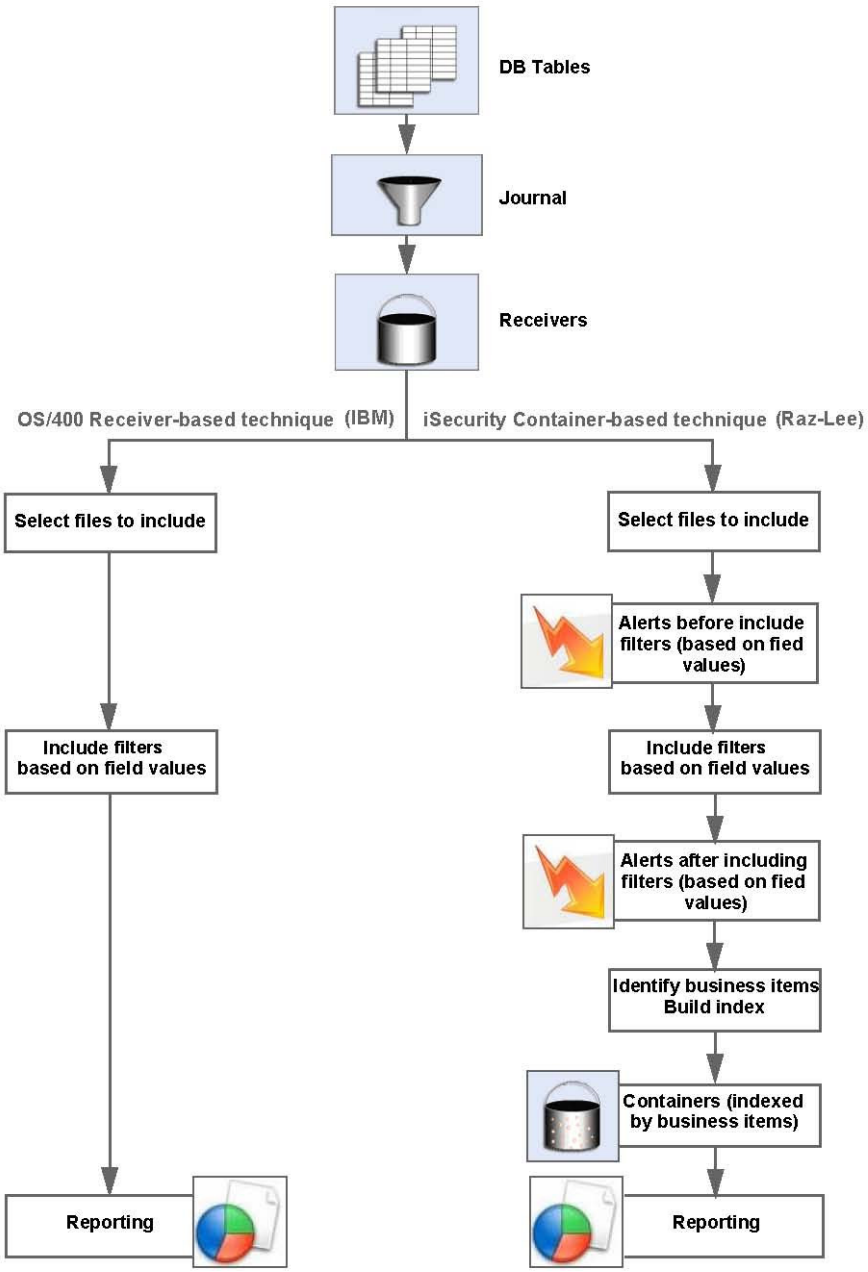
Real-time alerts on data changes have been added to "Work with Journaled Applications". An updated User Manual will soon be available.

Benefit: changes to application business critical data are alerted and reported in real-time.

Alerts can be raised both before include filters are checked & after include filters were checked
as described below.

RAZ-LEE™
The iSeries Security Experts

AP-Journal: Application Field-Level Reporting



Following is a numerical example of the use of Containers. Assume there are 1M records in the Receivers. Following the first alert, there may be 50K records and following the second alert, there may be only 5K records, which is the number of records in the Containers. This technique saves much valuable disk space.