System Control

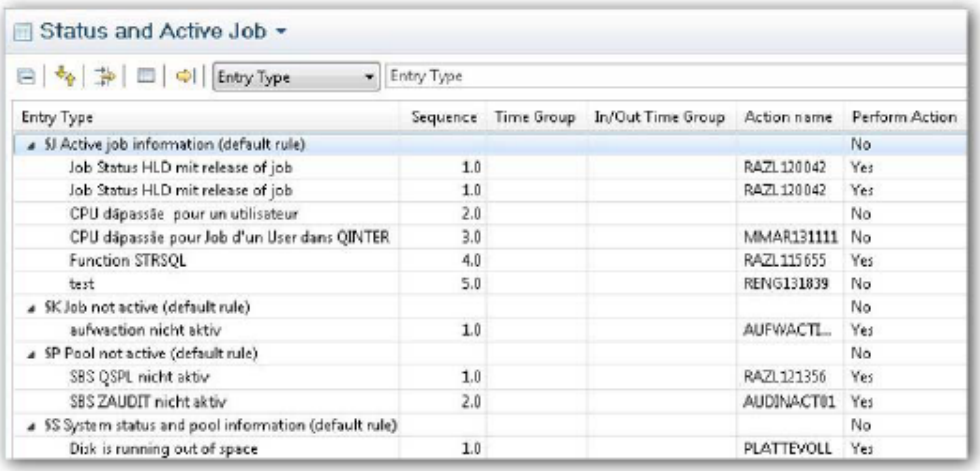
DATASHEET (iSecurity Suite Auditing & Monitoring)

Monitors CPU, subsystems, jobs, disk space and message queues

IBM i systems are usually highly automated. This means that certain jobs must be running constantly, subsystems must be active and programs must function smoothly in order to ensure operational processes. The system itself and the automated processes can be monitored and intervene manually in the event of malfunctions. It is precisely the manual component that often represents the problem. Administrators can always actively take care of it. In order to be able to work effectively, you rely on support from applications.

System Control and Audit – a Great Couple

First of all, iSecurity System Control is a module for system monitoring. It is supplied with system information via the functions of the iSecurity Audit module. In this way, System Control can be used to monitor important system functions such as CPU usage, jobs, subsystems, disk storage and message queues.



Entry Type	Sequence	Time Group	In/Out Time Group	Action name	Perform Action
$J Active job information (default rule)					No
Job Status HLD mit release of job	1.0			RAZL120042	Yes
Job Status HLD mit release of job	1.0			RAZL120042	Yes
CPU dépassée pour un utilisateur	2.0				No
CPU dépassée pour Job d'un User dans QINTER	3.0			MMAR131111	No
Function STRSQL	4.0			RAZL115655	Yes
test	5.0			RENG131839	No
$K Job not active (default rule)					No
aufwaction nicht aktiv	1.0			AUFWACTL...	Yes
$P Pool not active (default rule)					No
SBS QSPL nicht aktiv	1.0			RAZL121356	Yes
SBS ZAUDIT nicht aktiv	2.0			AUDINACT01	Yes
$S System status and pool information (default rule)					No
Disk is running out of space	1.0			PLATTEVOLL	Yes

Intervene before damage occurs

When the iSecurity **Action** module is installed, problems defined via filters can be discovered in real time, detected in real time and remedied with appropriately adapted countermeasures. This usually happens in good time before serious damage occurs.

It is possible to send rule-based warning messages via E-mail, SMS, Message queue, Syslog, etc. to those responsible, as well as to execute corrective command scripts with your own or standard IBM i commands.

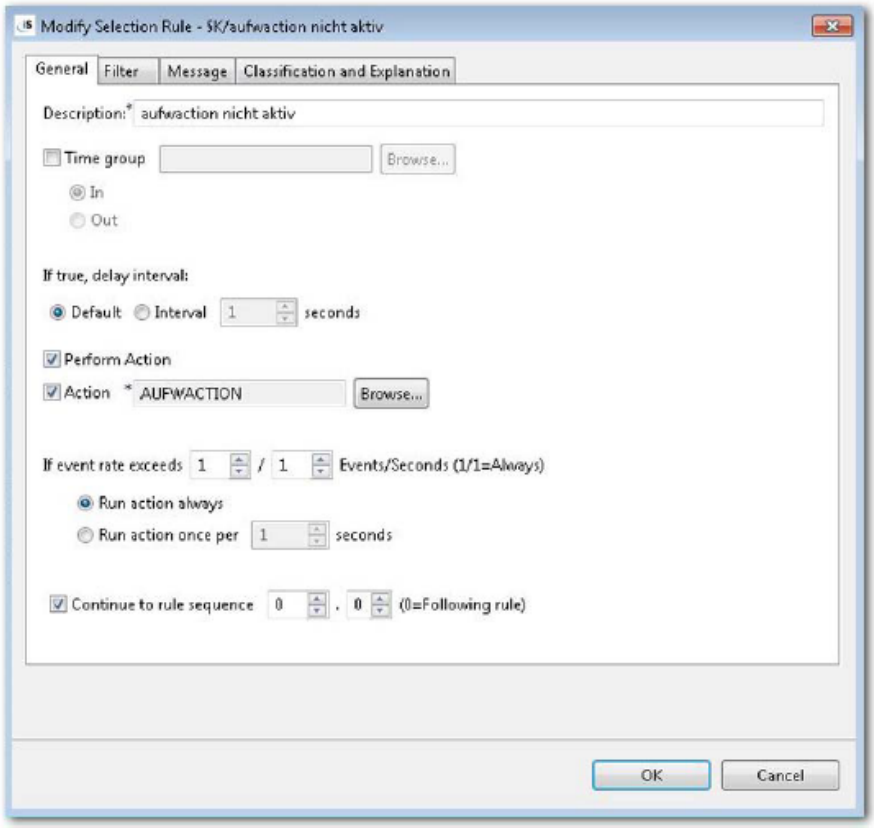
Parameters from the corresponding events can always be used for both notifications and command scripts. This ensures a highly automated set of rules that can independently eliminate disruptions in the operational process without manual intervention.

Key Features

- Uses entries from QSYSOPR or other message queues as input for iSecurity System Control
- Identifies jobs or sub-systems that are not active within production times and restarts them automatically
- Find not active jobs and forward the information to administrators e.g. via Email
- Allows corrective or preventive actions on Real-time monitoring security-related events
- Identifies critical events related to changes on CPU, disk storage and other parameters from system status
- Identifies unusual or extraordinary System behavior (e.g. such, not with behavioral patterns in WRKACTJOB)
- Allows rule creation Based on occurring messages in the system
- Monitors alongside message queues also the history (QHST)
- Finds abnormalities in the system (not running jobs, inactive ones, subsystems, etc.) and fixes them with rule-based logic
- Identifies messages in any message queues
- Able to send messages automatically and answers based on rules

News and History (QHST)

System Control monitors both arbitrary message queues as well as the system history (QHST) cyclically or in Real time. Existing messages in the system can be used to easily set up rules that are processed automatically.



The SIEM interface is used to create higher-level System supplied with IBM i information.

Let's Get Started

Schedule your Demo and start Auditing & Monitoring your Systems with iSecurity System Control.

RAZ-LEE iSecurity