VISUAL
message center

Security Auditing with Tango/04 Products

OS/400 Platform (AS/400, iSeries, System i)

6.0

VMC-BAS
VMC-SEC

tango04 Computing Group
Solutions for Advancing People

Security Auditing with Tango/04 Products - OS/400 Platform (AS/400, iSeries, System i)

Copyright Notice

Document date: April 2011

Document version: 2.11

Product version: 6.0

Trademarks

Technical Support

For technical support visit our web site at www.tango04.com.

Tango/04 Computing Group S.L.
Avda. Meridiana 358, 5 A-B
Barcelona, 08027
Spain

Tel: +34 93 274 0051

Table of Contents

Chapter 4

Chapter 5

Appendix

How to Use this Guide

This chapter explains how to use Tango/04 User Guides and understand the typographical conventions used in all Tango/04 documentation.

Typographical Conventions

The following conventional terms, text formats, and symbols are used throughout Tango/04 printed documentation:

Convention	Description
Boldface	Commands, on-screen buttons and menu options.
Blue Italic	References and links to other sections in the manual or further documentation containing relevant information.
Italic	Text displayed on screen, or variables where the user must substitute their own details.
`Monospace`	Input commands such as System i commands or code, or text that users must type in.
UPPERCASE	Keyboard keys, such as CTRL for the Control key and F5 for the function key that is labeled F5.
	Notes and useful additional information.
	Tips and hints that will improve the users experience of working with this product.
	Important additional information that the user is strongly advised to note.
	Warning information. Failure to take note of this information could potentially lead to serious problems.

Chapter 1
Introduction

This document is intended as a reference and assistance to administrators of AS/400 systems in implementing the necessary controls of a security auditing project for compliance with regulations such as SOX, 21 CFR Part 11, HIPAA, CA SB 1386, LOPD, etc.

For each control, the document indicates what elements of the Operating System must be activated or configured and how. It also explains what Tango/04 Computing Group product recollects and processes the auditing data generated by the controls. The information presented here does not replace the manuals of the different Tango/04 Computing Group products involved. The manuals contain detailed information regarding the configuration and use of each product.

Chapter 2
Activating the Audit

2.1 Preparing the System: General Configuration of the OS/400 system

2.1.1 System Security Audit

Auditing controls on the iSeries are implemented using Audit Journal. Audit Journal, just as any other journal, has associated objects called journal receivers, which store the auditing events generated by the Operating System.

As auditing on the iSeries is optional, the first step will be to prepare the system to register auditing events. A journal receiver must be created in a library created specifically for storing those receivers (system library `QSYS` can be used to store journal receivers but it is not recommended to do so). Next an audit journal (`QAUDJRN`) must be created in the system library, and the journal receiver must be associated to it.

Creating a separate library for the journal receivers will simplify maintenance, depending on the options set for managing the receivers by the system.

Step 1. To create the first journal receiver use the following commands:

```
CRTLIB LIB(AUDJRN) TEXT('Audit journal receivers library')
CRTJRNRCV        JRNRCV(AUDJRN/AUDRCV0001)        THRESHOLD(200000)
TEXT('Journal Receiver')
```

Tip
If you intend to manage the receivers automatically by the system, it is important that the name of the receiver end in a number. Each time a new journal receiver is created the system will pick up the last journal receiver and assign it a name in sequence (if the last journal receiver is called `AUDRCV0023` the next one will be called `AUDRCV0024`).

Step 2. To create the audit journal and associate the original journal receiver created in the previous step, use the following command:

```
CRTJRN JRN(QSYS/QAUDJRN) JRNRCV(AUDJRN/AUDRCV0001) MNGRCV(*SYSTEM)
DLTRCV (*NO) TEXT('Audit Journal')
```

Important
To avoid deleting the receivers automatically, it is important to set the parameter `DLTRCV` to `*NO`.

Once these steps have been carried out, the system is ready to activate auditing.

2.1.2 Data or Record-level Audit

The difference between auditing system security and auditing data is that the data audit does not use a system journal. Rather it uses a journal created specifically for data auditing purposes.

For record-level auditing with Data Monitor for iSeries, the procedure is as follows:

Step 1. The most important difference is that a journal and receives must be created for all each sensitive file to be audited.

```
CRTLIB LIB(DATAJRN) TEXT('Data journal receivers library')
CRTJRNRCV JRNRCV(DATAJRN/DATARCV0001) THRESHOLD(200000)
TEXT('Receiver for database file SALARIES')
```

Tip
f you intend to manage the receivers automatically it is important that the name of the journal receiver ends with a number. The system will pick up the name of the last journal receiver and create a new one with a sequential name (i.e. if the last journal receiver was called `DATARCV0023` the next one will be called `DATARCV0024`)

Step 2. To create a database journal and associate the previously created receiver, use the following command:

```
CRTJRN JRN(DATAJRN/DATAJRN1) JRNRCV(DATAJRN/DATARCV0001)
MNGRCV(*SYSTEM) DLTRCV (*NO) TEXT('Database journal - file
SALARIES')
```

Important
To avoid deleting the receivers automatically, it is important to set the parameter `DLTRCV` to `*NO`.

Note
Data Monitor for iSeries does not support minimized entries. Make sure that your system is set up to handle full entries.

Step 3. Start data storage in the database journal for each sensitive file to audit using the following command

```
STRJRNPF FILE(NAMELIB/SALARIES) JRN(DATAJRN/DATAJRN1)
IMAGES(*BOTH) OMTJRNE(*OPNCLO)
```

Important
It is important to set the parameter `IMAGES` to `*BOTH` so that both the before and after values will be stored.

2.2 System Security Audit - At Action level

Depending on the task at hand different auditing types should be enabled. For auditing purposes activate the following types:

Audit Type	Description
AD	Auditing changes
AF	Authority failure
CA	Authority changes
CD	Command string audit
CP	User profile changed
DO	Delete Object
DS	DST security password
OW	Object ownership changes
PA	Program changed to adopted authority
PW	Invalid password
ST	Use of Service tools
SV	System Values Changes

Another point to consider is that AS/400 auditing is activated by category. Each category encompasses a set of types which are automatically activated in addition to those required at system level. Thus, when we activate the audit types mentioned in the table above, the following types are also activated:

Audit Type	Description
AU	Attribute changes
CQ	Change of `*CRQD` object
CY	Cryptographic configuration
EV	System environment
GR	Generic Record
JD	Change to user parameter to a job description
JS	Actions that affect jobs
KF	Key Ring File
NA	Network attribute changed
PG	Change of an object's primary group
SE	Subsystems routing entry changed

Audit Type	Description
SG	Asynchronous Signals
SO	Server security user information actions
VA	Changing an access control list
VC	Starting or ending a connection
VN	Logging on and off the network
VP	Network password error
VS	Starting or ending a server session
VU	Changing a network profile
VV	Changing service status

When configuring the product take care to filter out superfluous information generated by these entries.

Activating these auditing categories may change the system value `QAUDLVL`, so that it contains the complete list of categories that should be enabled. The command to use, for example to audit the categories `*SECCFG` (Security Configuration) and `*AUTFAIL` (authorization errors), is:

```
CHGSYSVAL SYSVAL(QAUDLVL) VALUE('*SECCFG *AUTFAIL')
```

This configuration can also be applied from the iSeries Security Agent, which provides the user with a PDM interface to activate the required categories (the application takes care of changing the relevant system values).

`QAUDLVL` should have the following list of values:

```
*SERVICE
*DELETE
*SECRUN
*AUTFAIL
*PGMFAIL
*SECCFG
*JOBDTA
```

To deactivate auditing simply replace this list with the value `*NONE`.

We recommend you do not make the changes to system values manually. Let Security Agent do it for you.

2.3 System Security Audit - At Object Level

To audit reads (that is the read access not the information that was read) and changes to sensitive files (access for updates, not the information updated) the options ZR and ZC should be activated. These options apply to objects and activating them may cause a large increase in the number of records stored in the audit journal if the object in question already has auditing activated. Both options can be activated from iSeries Security Agent.

For the system to activate the auditing of a particular object, each object to audit must be indicated expressly.

For high-level sensitive files we recommend you use Data Monitor for iSeries to audit reads and changes at record level and store the values from before and after the modification.

Chapter 3
Maintaining the Audit

3.1 Access Over Communications Networks

iSeries systems can be accessed over Telnet sessions or via client applications that connect to the system over communications networks, whether using standard protocols like ODBC or proprietary methods. Given this environment it is impossible to secure the iSeries systems by blocking external access and access security depends entirely on the permissions defined in the individual user profiles. Controls for the remote connections should be implemented as if they were local access to the machine (similar to the controls used for local sessions on the Windows platform) as security regulations demand that you guarantee the same level of security applied to local access to access over the communications network, regardless of the platform.

3.2 Record of Incidences

All system or auditing messages on the iSeries that may be a source of incidences are retrieved by the iSeries Security Agent and VISUAL Message Center and stored in a secure DB2 database located in `B_DETECTOR/BDHST02X`. For record-level auditing with Data Monitor for iSeries, the DB2 auditing databases which may contain sensitive data are located in

- `T4DATAMON/CHDOC01P`,
- `T4DATAMON/CHHOR01P`,
- `T4DATAMON/CHLOC01P`.

When auditing with iSeries Security Agent and VISUAL Message Center the database is stored on each and every iSeries to be monitored. Each database is independent and dedicated to the server on which it resides. When auditing at record level using Data Monitor for iSeries the databases are located on the same server where the product is installed, which is not necessarily the machine containing the sensitive files to audit are located. The sensitive files may be located on other machines as they can be accessed using remote journals provided by the operating system.

Tango/04 Computing Group products allow you to automatically create a record of an incidence in a database based on the auditing messages mentioned above. It is possible to configure the SmartConsole to insert a record in an incidences database for only those messages that need to be recorded.

3.3 Back Up Copies

Using VISUAL Message Center's HST Agent you can monitor whether backup copies of sensitive files are carried out successfully. For a more elaborate control of backup copies you can use VISUAL Message Center's operations agents DVM, JBM, JDM and BCH to monitor the involved devices and jobs respectively.

3.4 Identification and Authentication

With respect to Identification and Authentication, the following checks can be employed:

- Detecting changes to passwords: receive a message each time a password for a user profile is changed.
- Detect disabled users or devices: receive a message each time a user profile or a device is disabled. Note that a user or device may be disabled automatically by the system upon repeated attempts to login unsuccessfully.

This functionality is available in the iSeries Security Agent's AUD Agent.

3.5 Access Control

To guarantee control of access to sensitive data the following risk situations can be detected:

- Authorization errors: attempt by a user to access content or programs without the appropriate authority.
- Changes to user profiles.
- Changes of ownership of sensitive objects.

This functionality is available in the iSeries Security Agent's AUD Agent.

Chapter 4
Inactive Users

VISUAL Message Center's UIN agent allows you to audit inactive users on the system. The agent can distinguish between enabled and disabled inactive users and those who have been used once or have never been used.

Some users may be inactive for a reason, for example in the case of system profiles or special users that are intended for internal use by an application. Filters can be established so that these users are not detected as inactive users and do not set off any alerts.

The following table shows the most important messages from the UIN agent.

Message ID	Description
UIM0100	User &2 has never registered any activity in the system. This user was created &3 days ago. Status: `*DISABLED`.
UIM0200	User &2 has not been registering activity in the system for &3 days. Status: `*DISABLED`.
UIM0300	User &2 has never registered any activity in the system. This user was created &3 days ago. Status: `*ENABLED`.
UIM0400	User &2 has not been registering activity in the system for &3 days. Status: `*ENABLED`.

Chapter 5
Other Controls

Other controls that should be included in the implementation are:

- Command line auditing for special users.
- Changes to applications that use adopted authority.
- Changes to authorization.
- Changes to the system.
- Changes to the audit configuration.
- Libraries operations.
- Sensitive objects operations.
- System Tools (ST).

All these controls can be implemented based on messages generated by the system audit and can be retrieved from the audit journal by the iSeries Security Agent AUD. If the AUD agent is not available the data can be retrieved using Visual Message Center's HST Agent. In addition to retrieving these messages we recommend implementing visual alert and notification systems and, where necessary, automatic actions to protect the system.

Appendix A
Contacting Tango/04

North America

Tango/04 North America
PO BOX 3301
NH 03458 Peterborough
USA

Phone: 1-800-304-6872 / 603-924-7391
Fax: 858-428-2864
sales@tango04.net
www.tango04.com

EMEA

Tango/04 Computing Group S.L.
Avda. Meridiana 358, 5 A-B
08027 Barcelona
Spain

Phone: +34 93 274 0051
Fax: +34 93 345 1329
info@tango04.net
www.tango04.com

Italy

Tango/04 Italy
Viale Garibaldi 51/53
13100 Vercelli
Italy

Phone: +39 0161 56922
Fax: +39 0161 259277
info@tango04.it
www.tango04.it

Sales Office in France

Tango/04 France
La Grande Arche
Paroi Nord 15ème étage
92044 Paris La Défense
France

Phone: +33 01 40 90 34 49
Fax: +33 01 40 90 31 01
contact@tango04.net
www.tango04.fr

Sales Office in Switzerland

Tango/04 Switzerland
18, Avenue Louis Casaï
CH-1209 Genève
Switzerland

Phone: +41 (0)22 747 7866
Fax: +41 (0)22 747 7999
contact@tango04.net
www.tango04.fr

Latin American Headquarters

Barcelona/04 Computing Group SRL (Argentina)
Avda. Federico Lacroze 2252, Piso 6
1426 Buenos Aires Capital Federal
Argentina

Phone: +54 11 4774-0112
Fax: +54 11 4773-9163
info@barcelona04.net
www.barcelona04.com

Sales Office in Peru

Barcelona/04 PERÚ
Centro Empresarial Real
Av. Víctor A. Belaúnde 147, Vía Principal 140
Edificio Real Seis, Piso 6
L 27 Lima
Perú

Phone: +51 1 211-2690
Fax: +51 1 211-2526
info@barcelona04.net
www.barcelona04.com

Sales Office in Chile

Barcelona/04 Chile
Nueva de Lyon 096 Oficina 702,
Providencia
Santiago
Chile

Phone: +56 2 234-0898
Fax: +56 2 2340865
info@barcelona04.net
www.barcelona04.com

About Tango/04 Computing Group

Tango/04 Computing Group is one of the leading developers of systems management and automation software. Tango/04 software helps companies maintain the operating health of all their business processes, improve service levels, increase productivity, and reduce costs through intelligent management of their IT infrastructure.

Founded in 1991 in Barcelona, Spain, Tango/04 is an IBM Business Partner and a key member of IBM's Autonomic Computing initiative. Tango/04 has more than a thousand customers who are served by over 35 authorized Business Partners around the world.

Alliances

Partnerships

IBM Business Partner

IBM Autonomic Computing Business Partner

IBM PartnerWorld for Developers Advanced Membership

IBM ISV Advantage Agreement

IBM Early code release

IBM Direct Technical Liaison

Microsoft Developer Network

Microsoft Early Code Release

Awards

Legal Notice

The information in this document was created using certain specific equipment and environments, and it is limited in application to those specific hardware and software products and version and releases levels.

Any references in this document regarding Tango/04 Computing Group products, software or services do not mean that Tango/04 Computing Group intends to make these available in all countries in which Tango/04 Computing Group operates. Any reference to a Tango/04 Computing Group product, software, or service may be used. Any functionally equivalent product that does not infringe any of Tango/04 Computing Group's intellectual property rights may be used instead of the Tango/04 Computing Group product, software or service

Tango/04 Computing Group may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

The information contained in this document has not been submitted to any formal Tango/04 Computing Group test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility, and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. Despite the fact that Tango/04 Computing Group could have reviewed each item for accurateness in a specific situation, there is no guarantee that the same or similar results will be obtained somewhere else. Customers attempting to adapt these techniques to their own environments do so at their own risk. Tango/04 Computing Group shall not be liable for any damages arising out of your use of the techniques depicted on this document, even if they have been advised of the possibility of such damages. This document could contain technical inaccuracies or typographical errors.

Any pointers in this publication to external web sites are provided for your convenience only and do not, in any manner, serve as an endorsement of these web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries: iSeries, iSeriese, iSeries, i5, DB2, e (logo)®Server IBM ®, Operating System/400, OS/400, i5/OS.

Microsoft, SQL Server, Windows, Windows NT, Windows XP and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries. UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group. Oracle is a registered trade mark of Oracle Corporation.

Other company, product, and service names may be trademarks or service marks of other companies.