

VISUAL
securitysuite

Security Reports

with Tango/04 VISUAL Security Suite

VISUAL Security Suite **1.0**

tango04
Computing Group
Solutions for Advancing People

Security Reports with Tango/04 VISUAL Security Suite

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 2008 Tango/04. All rights reserved.

First Printing: September 2008

Document version: 2.0

Product version: 1.0

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of Tango/04.

Trademarks

Any references to trademarked product names are owned by their respective companies.

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

08027 Barcelona

Spain

Phone: +34 93 274 0051

Table of Contents

Table of Contents iii

Chapter 1

Overview 1

Chapter 2

Security Reports 6

- 2.1. Commands 6
 - 2.1.1. Sensitive Command Usage Control 6
 - 2.1.2. Commands Authority Control 6
- 2.2. Generic 7
 - 2.2.1. Detailed Internal Security Events 7
- 2.3. Objects 7
 - 2.3.1. Access denied to objects 7
 - 2.3.2. Object Action Auditing 7
 - 2.3.3. Object Management 7
 - 2.3.4. Object Ownership Changes 8
 - 2.3.5. Sensitive Objects Access Control 8
- 2.4. SQL 8
 - 2.4.1. Interactive SQL statements executed 8
 - 2.4.2. SQL statements executed 8
- 2.5. System 9
 - 2.5.1. Auditing Changes CHGATR 9
 - 2.5.2. Dedicated Service Tools 9
 - 2.5.3. Programs Changed to Adopt Owner Authority Control 9
 - 2.5.4. System Value and Network Attribute 9
 - 2.5.5. Jobs Ended Abnormally 9

2.6. Users.....	10
2.6.1. Authorization list control	10
2.6.2. Changes in Current User Profile (Real User) of Jobs	10
2.6.3. Enabled-Disabled Users	10
2.6.4. Executed Commands by Users.....	10
2.6.5. Inactivity Control.....	11
2.6.6. Login Failures for 2520 Telnet Session.....	11
2.6.7. Never Logged In Users	11
2.6.8. Password Changed by User Profiles	11
2.6.9. User Profile Management - Created, Changed.....	11

About Tango/04 Computing Group	6
Legal notice	7

Chapter 1

Overview

This document describes the reports that are available within Tango/04's Reporting System which are useful for controlling iSeries system security. The reporting functionality uses auditing events collected on the iSeries, gathered by the iSeries Security Agent.

The VISUAL Security Suite reporting functionality offers various clear benefits for customers:

- Centralized creation of reports for multiples systems or LPARs – reduces maintenance and allows consolidation of reporting.
- High quality graphical reports with Crystal Reports, can be exported to PDF, XLS, HTML or viewed within Crystal Reports.
- Custom report creation, using SQL parameters, and access to information from over 700 audit entry types.
- Integration with system management software, including message, job, performance management.

Chapter 2

Security Reports

This is a summary of the security reports within Reporting System. This is a summary list: all reports can be refined using filters or grouping options.

2.1 Commands

2.1.1 Sensitive Command Usage Control

Summarizes the usage of sensitive commands, grouped by command, user or job. This report uses the object read auditing. The report can be refined using filters on the server side, or using SQL within the Reporting System.

Filter or Grouping Options

Command, User, Job

Audit Journal Requirements:

Object *ON for Command

2.1.2 Commands Authority Control

Summarizes changes made to authority to use sensitive commands, using the Authority Changes audit entry type.

Filter or Grouping Options

Command, User, Job

Audit Journal Requirements

CA

2.2 Generic

2.2.1 Detailed Internal Security Events

Generic report - can be used to create new reports from over 700 audit entry types available on the server.

Filter or Grouping Options

User, Job, Msg type

Audit Journal Requirements

Various

2.3 Objects

2.3.1 Access denied to objects

Shows authority failures for objects, grouped by user, by object or by job. It can be used to quickly pinpoint security errors in applications, or suspicious behavior.

Filter or Grouping Options

User, Object, Job

Audit Journal Requirements

AF

2.3.2 Object Action Auditing

Lists relevant audited actions from the system audit journal. Action Auditing is generated by the operating system on a system-wide basis, and must be set using the iSeries Security Agent interface.

Filter or Grouping Options

Object, Job, user, Message, action, Program, System

Audit Journal Requirements

CO, DO, OM, OR

2.3.3 Object Management

Actions executed on specific objects, grouped by object, action type, user or job. Should be used for reporting access to sensitive objects.

Filter or Grouping Options

Object type, Action, User, Job

Audit Journal Requirements

CD

2.3.4 Object Ownership Changes

Changes to ownership of specific objects, using Object Ownership entry type.

Filter or Grouping Options

Administrator, Object type, Job

Audit Journal Requirements

OW

2.3.5 Sensitive Objects Access Control

Accesses to specified sensitive objects, grouped by object, job or user, and summarized by time. Various report types are available, including summary reports and detailed reports.

Filter or Grouping Options

Object

Audit Journal Requirements

Object *ON

2.4 SQL

2.4.1 Interactive SQL statements executed

Summarizes use of interactive SQL statements by job and by user. Includes information about the statement executed, and the object(s) involved.

Filter or Grouping Options

Job, User

Audit Journal Requirements

SQL Agent

2.4.2 SQL statements executed

Summarizes use of embedded SQL statements by job and by user. Includes information about the statement executed, and the object(s) involved.

Filter or Grouping Options

Job, User

Audit Journal Requirements

SQL Agent

2.5 System

Summarizes changes to Objects, Document Library Objects, Users and Attributes. The Generic report offers a summary of the changes to all of these objects.

2.5.1 Auditing Changes CHGATR

Filter or Grouping Options

Agent, System, User, Job, Message

Security Agent Requirements

You need to activate AD entry type in VISUAL Message Center

2.5.2 Dedicated Service Tools

Summarizes use of DST by action, tool, job or user.

Filter or Grouping Options

Actions, Tools, Job, User

Audit Journal Requirements

DS

2.5.3 Programs Changed to Adopt Owner Authority Control

Summarizes programs that use adopted authority by object owner, administrator profile and program. Very useful for detecting use of adopted authority.

Filter or Grouping Options

Owner, Administrator, Program

Audit Journal Requirements

PA

2.5.4 System Value and Network Attribute

Changes to system values and network attributes, summarized by system value, or by the administrator or job which has changed sysvals.

Filter or Grouping Options

Administrator, Job, SysVal

Audit Journal Requirements

SV

2.5.5 Jobs Ended Abnormally

Summary of jobs which end abnormally, including job name and the end code.

Filter or Grouping Options

Return Code, Subsystem

Audit Journal Requirements

QHST

2.6 Users

2.6.1 Authorization list control

Changes to authorization lists, include name additions, delete of list

Filter or Grouping Options

Authorization list

Audit Journal Requirements

CO, DO, CA

2.6.2 Changes in Current User Profile (Real User) of Jobs

Summarizes changes to the user profile of a job in execution, showing the Real User of a job (e.g. for an ODBC connection, it shows the user that is connecting rather than the user profile of the job)

Filter or Grouping Options

Real user, Job

Audit Journal Requirements

Object *ON

2.6.3 Enabled-Disabled Users

Summarizes user profiles that have been enabled or disabled, grouped by user profile, administrator or job.

Filter or Grouping Options

Administrator, Profile, Job

Audit Journal Requirements

CP

2.6.4 Executed Commands by Users

Lists the activity of specific user profiles, including details of commands executed by user and job.

Filter or Grouping Options

Command, User, Job

Audit Journal Requirements

CD

2.6.5 Inactivity Control

Summarizes user profiles that have been inactive for a certain period of time.

[Filter or Grouping Options](#)

User

[Audit Journal Requirements](#)

Inactivity agent

2.6.6 Login Failures for 2520 Telnet Session

Summarizes sign-on errors in interactive sessions or 5250 telnet sessions.

[Filter or Grouping Options](#)

System, User, Type of Failure

[Security Agent Requirements](#)

You need to activate PW entry type in VISUAL Message Center XX

2.6.7 Never Logged In Users

Summarizes user profiles that have never logged in, and are therefore considered dormant.

[Filter or Grouping Options](#)

User

[Audit Journal Requirements](#)

Inactivity agent

2.6.8 Password Changed by User Profiles

Summarizes changes to passwords by user profiles.

[Filter or Grouping Options](#)

User

[Audit Journal Requirements](#)

CP

2.6.9 User Profile Management - Created, Changed

Creation, change, delete etc. of user profiles, grouped by action or by user profile.

[Filter or Grouping Options](#)

Action

[Audit Journal Requirements](#)

CP

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

five-time winner of the
IBM ALL STAR
INTERNATIONAL
award for product quality



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: AS/400, AS/400e, 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.