ISACA®
Trust in, and value from, information systems
San Francisco Chapter

P23
IT Audit Tests with ACL/Arbutus

Back to Business

Agenda

- Why you should use DA tools
- Accessing the data
- IT Test Examples
- Creating a script execution log
- Wrap-up

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Why You Should Use DA Tools

Using DA Tools

- Independence
- Diversity of data sources
- Automation of analysis
- Audit log

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Accessing Your Data

Variety of Sources

- Database tables
- XML exports
- DEL or CSV exports
- Excel/Access exports

Database Tables

- Identify configuration table
- Identify required fields
- Use ODBC import
- Can use REFRESH command in script for continuous monitoring/auditing

XML Exports

- Some applications allow XML exports of configurations
- For one table extract per file: Use XML import capability
- For multiple tables per file: Use script

XML Import Script

- Identify opening and closing tags for each record group
- For users, opening tag is <users> and closing tag is </users>
- Identify tags for fields in record group
- Use script to import XML file as a flat file
- Use GROUPs to process each set of records

DEL/CSV Exports

- Widespread use
- Potential data integrity issues
- Standard import routine in ACL/Arbutus

Excel/Access Exports

- Very common
- Potential data integrity issues
- Standard import routine in ACL/Arbutus
- Recommend ODBC

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

IT Tests

Scripting Tests for High-Risk Areas

- Frequent coverage
- Timely response
- Reduced time and effort

Tests for Review

1) Password configurations
2) SOD: Users and Roles
3) SOD: Users and Groups
4) Terminated Users
5) Keyword Search
6) Data Integrity

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

1) Password Configurations

Types of Password Settings

- Alphabetic characters
- Numeric characters
- Special characters
- Days for forced change

Demonstration-1

- Identify table of configurations
- Regular extraction and testing
- Maintain log of results

Demonstration-2

- Test: password_expiry_period should be 90 days
- Command: *EXTRACT FIELDS ALL DATE() AS "Test_date " TO PW_expiry_except_20111123 IF password_expiry_period <> 90*

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

2) SOD: Users and Roles

Segregation of Duties

- Compare table of users and roles against table of unacceptable combinations of roles
- Can require advanced scripting based on tables

Tables

Conflicts

Type	Role1	Role2
1	A	C
2	B	C
3	C	D

Users_Roles

Name	Role
Bob	A
Suresh	B
Alice	A
Ernst	B
Suresh	A
Bob	C
Alice	C
Ernst	A
Alice	D

Manual Solution

- Works for small number of possible user-roles pairs (<50 million)
- Execute many-to-many join of Users_Roles permissions against itself matching on Name
- Execute many-to-many join of Users_Roles_Join result against Conflicts

Step 1: Join Users_Roles With Itself

- EXTRACT RECORD TO Users_Roles_2
- OPEN Users_Roles SECONDARY
- JOIN MANY PKEY Name FIELDS ALL SKEY Name WITH Role IF *Role* <> *Users_Roles.Role* TO "Users_Roles_Join" OPEN PRESORT SECSORT

Step 1: Result

Users_Roles_Join

User	Role	Role2
Alice	A	C
Alice	A	D
Alice	C	A
Alice	C	D
Alice	D	A
Alice	D	C
Bob	A	C
Bob	C	A
Ernst	B	A
Ernst	A	B
Suresh	B	A
Suresh	A	B

Step 2: Join Users_Roles_Join With Conflicts

- OPEN Conflicts SECONDARY
- JOIN PKEY Role Role2 FIELDS ALL SKEY Role1 Role2 WITH ALL TO "Users_Roles_Conflicts" OPEN PRESORT SECSORT

Step 2: Result

Users_Roles_Conflict

User	Role	Role2	Conflict_Type	Role1	Role2
Alice	A	C	1	A	C
Bob	A	C	1	A	C
Alice	C	D	3	C	D

from Users_Roles_Join **from Conflicts**

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

3) SOD: Users and Groups

Users and Groups

User	Group
Cleopatra	APAC-1
Ozymandias	Admin
Ozymandias	APAC-1
Cleopatra	APAC-2
Ozymandias	EU-1
Viking	Admin
Ozymandias	NA-1
Viking	APAC-1
Shrine1	LA-3
Shrine1	LA-2
Viking	EU-1
Cleopatra	Admin

Users and Groups

- Users may belong to multiple groups
- Need rapid way to identify user-group combinations
- Use CROSSTAB to produce pivot table of user and group combinations : *CROSSTAB ON user COLUMNS group TO "User_Group_Xtab.FIL" OPEN*

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

4) Terminated Users

Terminated Users

- Compare Active Directory list against HR list of terminated employees
- Use join based on e-mail address or user name
- Best Practice: Harmonize case for key fields

Key Field Case Harmonization

Create computed field c_email_address_UPPER with formula *UPPER(email_address)*

Email_address	c_email_address_UPPER
Nkerrigan@Where.com	NKERRIGAN@WHERE.COM
Sjain@where.Com	SJAIN@WHERE.COM
aMoskovitz@Where.com	AMOSKOVITZ@WHERE.COM

Process

- Use *csvde –f outputfilename.csv* command on AD server to extract data
- Import .CSV file into ACL/Arbutus
- Import HR file into ACL/Arbutus
- Harmonize key fields
- Execute JOIN on key field to test for matches
- Use Levenshtein difference functionality in Arbutus Analyzer to identify fuzzy matches

Tables

Terminated Users

email_address	F_name	L_name	ID
sjain@where.com	Suresh	Jain	2598
amoskovitz@where.com	Anton	Moskovitz	3286
ewindsor@where.cOM	Edwina	Windsor	1127

Active AD Accounts

email_address
Nkerrigan@Where.com
Mokintyre@where.COM
aMoskovitz@Where.com
rtufali@where.com
RFROST@where.com
cspenser@WHERE.COM
NWebster@Where.COM

Join Command

- Execute with Terminated_Employees as Primary
- Use harmonized e-mail fields as key fields
- Use Matched_Primary JOIN
- *JOIN PKEY c_Email_Upper_HR FIELDS email_address F_name L_name ID c_Email_Upper_HR SKEY c_Email_Address_UPPER_AD TO "Terminated_HR_Active_in_AD" OPEN PRESORT SECSORT*

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

5) Keyword Search

Keyword Search

- Search memo fields for keywords
- Keyword list in editable .txt for updates
- Use script to isolate each word in memo field in new file with source record number
- Use JOIN on keyword to identify records where each keyword appears

What the script does

- Parses memo field word-by-word
- Writes each word and the record number to a record in a new file
- Use JOIN against keyword file to identify records containing keywords

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

6) Data Integrity

Data Integrity

Field Type	Issue	Command	What to look for
Numeric	Unacceptable values	STATISTICS	Maximum, minimum values, # of zeros
Numeric	Corruption	VERIFY	See log
Date	Bounds	STATISTICS	Maximum, minimum values
Date	Corruption	COUNT IF *date_field = `19000101`*	COUNT1 > 0

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Creating a Script Execution Log

Script Execution Log

- Records test name, execution date, start/end times, number of exceptions
- Use variables to capture data
- Provides historical perspective
- Documents efficiency gains
- Table independent of ACL log

Use Variables: Initialize at Beginning

v_Test = “<name of test>”

v_Test_Date = DATE()

v_Start_Time = TIME()

v_End_Time = BLANKS()

v_Exceptions = 0

Use Variables: Set and Extract at End

OPEN <exceptions table>

COUNT

v_End_Time = TIME()

v_Exceptions = COUNT1

EXTRACT FIELDS SUB(v_Test,1,30) AS "Test"
v_Date as "Test_Date" v_Start_Time AS "Start_Time" v_End_Time as " End_Time " v_Exceptions as "Number_Exceptions" TO Test_Log FIRST 1 APPEND

Final Notes

- Document your procedures
- Document your procedures
- Maintain relationships with application owners

QUESTIONS?

Michael Kano

Audit Tools and Automation Specialist

mkano@ebay.com

(408) 967-3681