# NEBraskaCERT Conference 2003

## Effective Oracle Auditing

by

Aaron Grothe (CISSP)

# Overview

- Why Audit?
- Why Not Audit?
- How to Audit
- How NOT to Audit
- Basics
- Where my company is at in our Oracle auditing
- Summary
- Resources
- Contact Info
- Q & A

# *Why Audit?*

- We already have a “firewall/ids/os audit package/single sign on/magic beans”
- Most company networks aren't that well segmented once you are inside you have full access
- An audit trail can help with troubleshooting database issues
- An audit trail can be useful when reconstructing a database

# *Why Not Audit?*

- Audit can be slow – typical auditing should result in a 5% database impact, depending on what you audit of course this can be MUCH higher
- A poorly implemented audit policy can lead to a false sense of security
- If an audit policy is implemented poorly it can forever prevent the ability to implement an audit policy

# How to Audit

- Incremental
- Build on Goals
- Regularly “truncate” audit trails do not delete
- Work with Security Officer
- Size tables appropriately

# How NOT to Audit

- All or nothing
- Regularly “delete” audit table entries or better yet don't

# *Auditing at the O/S level versus the Database Level*

- If you are using syslog-ng and have an audit policy already defined for dealing with audits that may be a good fit
- Aggregation of results between multiple Databases is possible with O/S level auditing
- O/S level auditing is different between Operating Systems and not all functionality is the same
- Does DBA have access to O/S audit trail

# Examples

- Based on Pete Finnigan's website, paper and the O'reilly book
  - Showing connection attempts
  - Failed log-on attempts
  - Failed log-on attempts with return codes
  - Attempts to access the database with non-existent users
  - Attempts to access the database at unusual hours
  - Users accessing database accounts from multiple locations
  - Multiple users accessing database from same location
  - Objects being created or Changed

# Showing connection attempts

- Select username, terminal, action_name, to_char (timestamp, 'DDMMYYYY:HHMISS') timestamp, to_char(logoff_time, 'DDMMYYYY:HHMISS') logoff_time, returncode *from dba_audit_session

Output

| | |
|---|---|
| Username | Timestamp |
| Terminal | Logoff_time |
| Action | Returncode |

# *Showing Failed log-on attempts*

- Select count(*), username, terminal, to_char (timestamp, 'DD-MON-YYYY') from dba_audit_session where returncode<> 0 group by username, terminal, to_char (timestamp, 'DD-MON-YYYY');

Output

Number of failed attempts
Username
Terminal
Timestamp

# Script to show connection attempts

- Select count(*), username, terminal, to_char (timestamp, 'DD-MON-YYYY'), returncode from dba_audit_session  group by username, terminal, to_char (timestamp, 'DD-MON-YYYY');

Output

Failed attempts
Successful attempts
Username
Terminal
Timestamp

# *Script to Show Connection Attempts with non-existent users*

- Select username, terminal, to_char(timestamp, 'DD-MON-YYYY HH24:MI:SS') from dba_audit_session  where returncode <> 0 and not exists (select 'x' from dba_users where dba_users.username=dba_audit_session.username)

Output

Invalid usernames

Timestamps

Terminal

# *Script to detect attempts to access database at unusual hours*

- Select username, terminal, action_name, returncode, to_char(timestamp, 'DD-MON-YYYY HH24:MI:SS'), to_char(logoff_time, 'DD-MON-YYYY HH24:MI:SS') from dba_audit_session where to_date (to_char(timestamp, 'HH24:MI:SS'), 'HH24:MI:SS') < to_date ('08:00:00', 'HH24:MM:SS') or to_date (to_char (timestamp, 'HH24:MI:SS'), 'HH24:MI:SS') < to_date ('19:30:00', 'HH24:MM:SS')

# *Script to detect attempts to access database at unusual hours*

- Output
  - Username
  - Terminal
  - Action
  - Returncode
  - Timestamp

# *Script to detect users accessing database from multiple locations*

- Select count (distinct(terminal)), username from dba_audit_session having count(distinct(terminal)) >1) group by username

Output

Username

Number of Terminals user connected from

# *Script to detect mutiple users accessing database from one locations*

- Select count (distinct(username)), terminal from dba_audit_session having count(distinct (username))>1) group by terminal

Output

Username

Number of accounts logged in to from this location

# *Script to detect objects being created or changed*

- Select username, priv_used, obj_name, to_char (timestamp, 'DD-MON-YYYY HH24:MI') timestamp returncode from dba_audit_session where priv_used is not null and priv_used <> 'CREATE SESSION'

Output

- Username
- Privelege used
- Object accessed
- Time
- Return code

# *What can this Basic audit policy tell us?*

- Potential abuse of the database
- Shared accounts
- Modification of objects

# *Other things Audit could do*

- Audit original/changed values for important tables
  - Payroll
  - Vacation time
- Audit attempts to view database
- Summarize results into another table to preserve results and truncate database table

# *Performance Suggestions*

- Do not index audit tables
- Put on separate disks or less used devices
- Put audit trail in its own table space
- Turn off triggers on bulk operations (massive adds/deletes)

# Misc

- What happens when the audit tablespace is full?
  - Trusted Oracle is supposed to stop processing
  - Regular Oracle will have issues
    - Any trigger that is fired that generates an audit will fail since the audit failed
- Rollbacks will also rollback the audit trail preventing the existence of non-existent audits
  - Good or Bad?

# *Where we Are*

- Audit trail plans are behind schedule
- Oracle twilight support for 8.0.x series has resulted in forced migration to 8i/9i series this year
- Enormous push back on auditing plans
- Have done basic experiments audits on test databases

# Summary

- Oracle offers an amazing amount of power in its auditing facilities
  - It is enough power to shoot yourself in the foot with a machine gun
  - Used carefully with an incrementally developed policy it can be a tremendous tool

# Contact Info

- The best way to contact me is via e-mail at grothe@earthlink.net

# Resources

- Security Focus http://www.securityfocus.com/infocus/1689
- Oracle Security Handbook by Marlene Theriault and William Henry O'Reilly Press 1998 ISBN 1-56592-450-9
- Oracle Security step-by-step – A survival guide for Oracle Security Pete Finnigan 2003, published by SANS institute

# Q & A

- Comments?