Increasing DB security with Enterprise Manager 10g

Christopher Lambert

IT-DES

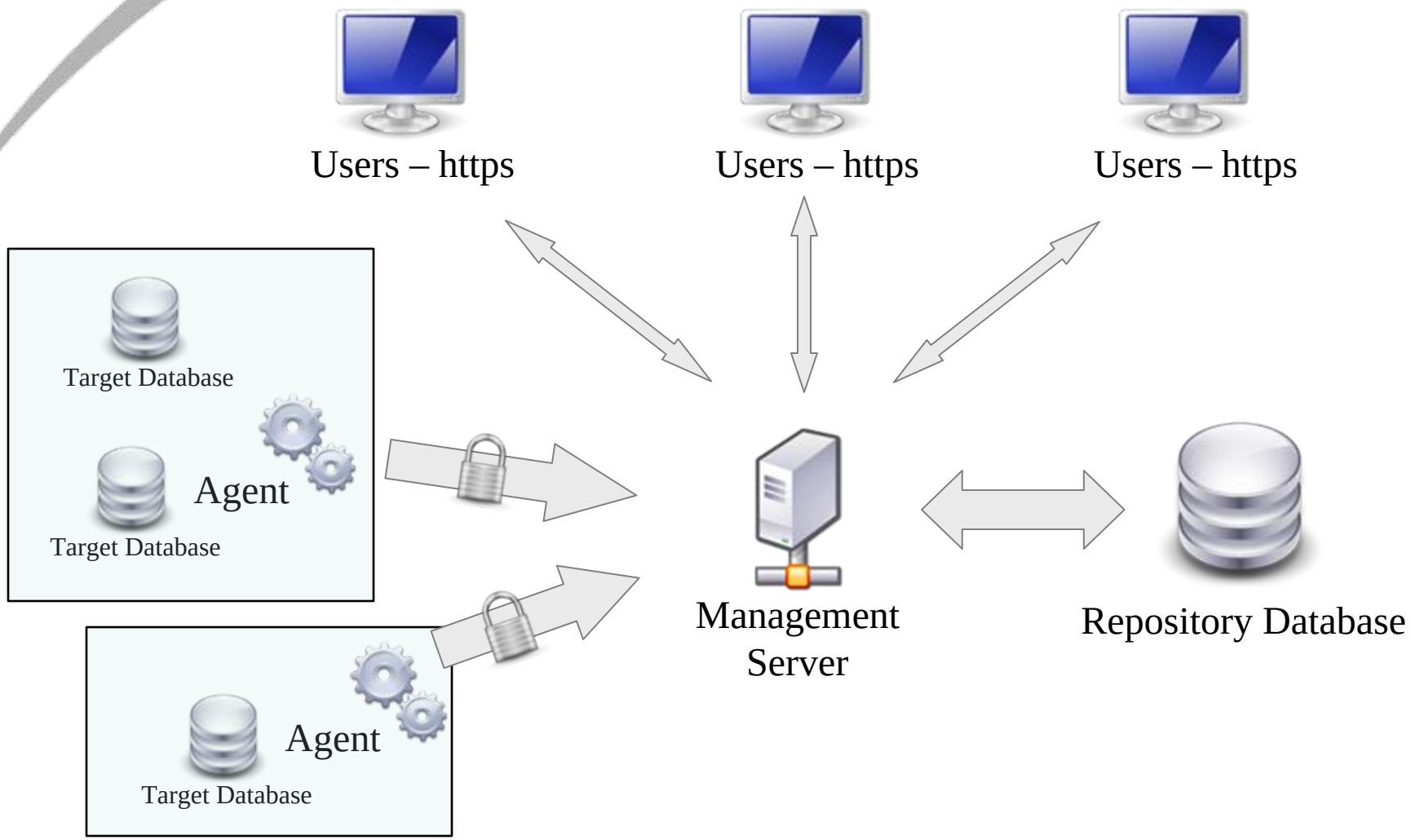
Agenda

- Current DB security concerns
- How EM10g can help us
- Specific examples
- Conclusion
- Q & A

Current DB security concerns

- Backup and Recovery
- Access
  - Account usage
  - Failed login attempts
- Activity
  - What are people doing?
  - What are they allowed to do?

EM Architecture



How we can use EM10g

- Out of the box security policies
- User defined metrics
- User defined reports

- 169 Security policies

Access to DBA_ROLES View	Informational	Security	Database Instance	Ensures restricted access to DBA_ROLES view
Access to DBA_ROLE_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to DBA_ROLE_PRIVS view
Access to DBA_SYS_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to DBA_SYS_PRIVS view
Access to DBA_TAB_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to DBA_TAB_PRIVS view
Access to DBA_USERS View	Informational	Security	Database Instance	Ensures restricted access to DBA_USERS view
Access to ROLE_ROLE_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to ROLE_ROLE_PRIVS view
Access to STATS$SQLTEXT Table	Informational	Security	Database Instance	Ensures restricted access to STATS$SQLTEXT table
Access to STATS$SQL_SUMMARY Table	Informational	Security	Database Instance	Ensures restricted access to STATS$SQL_SUMMARY table
Access to SYS.AUD$ Table	Informational	Security	Database Instance	Ensures restricted access to SYS.AUD$ table
Access to SYS.LINK$ Table	Informational	Security	Database Instance	Ensures restricted access to LINK$ table
Access to SYS.SOURCE$ Table	Informational	Security	Database Instance	Ensures restricted access to SYS.SOURCE$ table
Access to SYS.USER$ Table	Informational	Security	Database Instance	Ensures restricted access to SYS.USER$ table
Access to SYS.USER_HISTORY$ Table	Informational	Security	Database Instance	Ensures restricted access to SYS.USER_HISTORY$ table
Access to USER_ROLE_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to USER_ROLE_PRIVS view
Access to USER_TAB_PRIVS View	Informational	Security	Database Instance	Ensures restricted access to USER_TAB_PRIVS view
Audit File Destination	Critical	Security	Database Instance	Ensures that access to the audit files directory is restricted to th owner of the Oracle software set and the DBA group.
Audit File Destination(Windows)	Critical	Security	Database Instance	Ensures that access to the audit files directory is restricted to th owner of the Oracle software set and the DBA group.
Auditing of SYS Operations Enabled	Warning	Security	Database Instance	Ensures sessions for users who connect as SYS are fully audite

- User defined metrics

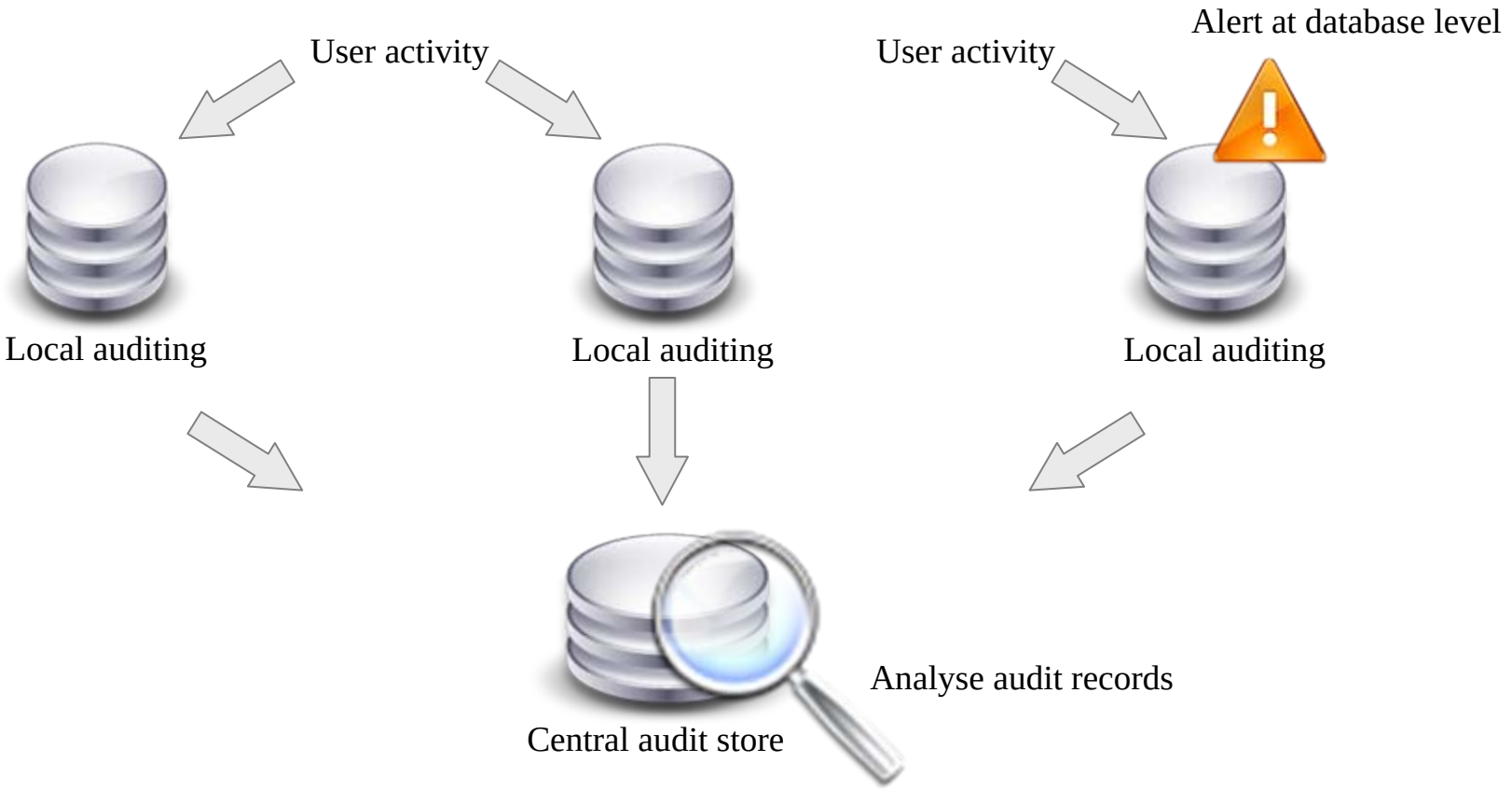
Select	Details	Name	Type	Last Known Value	Collection Timestamp	Comparison Operator	Warning	Critical	Current Severity
◉	Show	Age of datafile backup	NUMBER	30.985278	22-May-2008 09:33:53 MEST	>	96	96	✓
○	Show	Age of redolog backup	NUMBER	0.494444	22-May-2008 15:25:48 MEST	>	6	12	✓
○	Show	Apex Version	STRING	3	22-May-2008 15:25:51 MEST	=			✓
○	Show	Archive Graph	NUMBER	7.5	22-May-2008 15:27:03 MEST	=	-1	-1	✓
○	Show	Audit sys privs enabled	NUMBER	0	22-May-2008 15:28:10 MEST	!=	1	1	✗
○	Show	audited_priv_count	NUMBER	0	22-May-2008 15:25:49 MEST	<	10	10	✗
○	Show	Bad MVIEWS	NUMBER	1	22-May-2008 09:20:37 MEST	=			✓
○	Show	DB auditing enabled	NUMBER	0	22-May-2008 15:27:23 MEST	!=	1	1	✗
○	Show	Last successful pingdb	NUMBER	0	22-May-2008 15:23:22 MEST	>	0	0	✓
○	Show	Level 0 backup Graph	NUMBER	-1	22-May-2008 12:45:29 MEST	<	-1	-1	✓
○	Show	Level 1 backup Graph	NUMBER	-1	22-May-2008 09:57:35 MEST	<	-1	-1	✓
○	Show	Login audit trigger enabled	NUMBER	1	22-May-2008 15:25:44 MEST	!=	1	1	✓
○	Show	Login audit trigger exists	NUMBER	1	22-May-2008 15:28:10 MEST	!=	1	1	✓
○	Show	Max logswitch 24 hrs	NUMBER	4	22-May-2008 15:25:50 MEST	=			✓
○	Show	MTTR	NUMBER	36	22-May-2008 09:20:37 MEST	=			✓
○	Show	Rows in login audit	NUMBER	275	22-May-2008 15:25:44 MEST	>	100	100	✗
○	Show	Schemas with no password profile	NUMBER	169	22-May-2008 09:33:53 MEST	>	200	200	✓
○	Show	Schemas with permanent temp ts	NUMBER	0	22-May-2008 09:20:37 MEST	=			✓
○	Show	system stats gathered ratio	NUMBER	0.33	22-May-2008 15:25:44 MEST	!=	1	1	✗
○	Show	truncate_audit procedure exists	NUMBER	0	22-May-2008 15:27:23 MEST	!=	1	1	✗
○	Show	truncate_audit_job_broken	STRING			CONTAINS	Y	Y	✓
○	Show	truncate_audit_job_exists	NUMBER	0	22-May-2008 15:28:10 MEST	!=	1	1	✗
○	Show	Truncate_audit_last_run	NUMBER			>	7	10	✓

View Definition | Edit Definition | Create Like | Delete

- User defined reports

Target	DB Auditing enabled	No. Audit rows	Truncate Audit proc exists	Hrs since last Truncate Audit	Audited priv count	Truncate Audit job broken?	SYS operations audited	Login audit trigger exists	Login audit trigger enabled	Logon audit rows	No password profile
[redacted]											
[redacted]											
[redacted]											
[redacted]	Yes	534	Yes	0	1	No	No	Yes	Yes	74	101
[redacted]	Yes		Yes	-1	124	No	Yes	Yes	Yes	11	77
[redacted]	Yes	267	Yes	-1	0	No	Yes	Yes	Yes	8	31
[redacted]	Yes		No		0		No	No	No		32
[redacted]	Yes		Yes	25.7	0	No	Yes	Yes	Yes	7	31
[redacted]	Yes		Yes	-1	124	No	Yes	Yes	Yes	11	27
[redacted]	Yes		Yes	0	0	No	No	Yes	Yes	11	27
[redacted]	Yes		Yes	1.7	124	No	Yes	Yes	Yes	46	69
[redacted]	Yes	608	Yes	0	3	No	No	Yes	Yes		60
[redacted]	Yes	635	Yes	4	3	No	Yes	Yes	Yes		62
[redacted]	Yes	27,618	Yes	0	124	No	Yes	Yes	Yes	15	26
[redacted]	Yes		Yes	0	0	No	No	Yes	Yes	15	37
[redacted]	Yes	0	No		0		No	No	No		12
[redacted]	Yes		Yes	52.1	0	No	No	Yes	Yes	7	12
[redacted]	Yes		Yes	52.1	124	No	Yes	Yes	Yes	7	12
[redacted]	Yes	267	Yes	52.2	0	No	Yes	Yes	Yes	7	11
[redacted]	Yes		Yes	52.1	124	No	Yes	Yes	Yes	8	12
[redacted]	Yes		Yes	28.7	0	No	No	Yes	Yes	22	54
[redacted]	Yes		Yes	1.5	159	No	Yes	Yes	Yes	28	30
[redacted]	Yes		Yes	-1	2	No	Yes	Yes	Yes	19	140
[redacted]	Yes		Yes	0	3	No	No	Yes	Yes	21	58
[redacted]	Yes		Yes	-1	124	No	Yes	Yes	Yes	83	1,250
[redacted]	Yes		Yes	-1	2	No	No	Yes	Yes	331	1,340
[redacted]	No		No		0		No	Yes	Yes	101	162
[redacted]	No		No		0		No	Yes	Yes	101	162
[redacted]	No		No		0		No	Yes	Yes	129	164
[redacted]	No		No		0		No	Yes	Yes	129	164
[redacted]	No		No		0		No	Yes	Yes	131	164

- Logon and Privilege usage auditing



Example

- Factors of concern
  - Logon auditing enabled?
  - DB auditing enabled?
  - Database space containing audit logs
  - Broken data transfer
  - Correct privileges being audited?

Conclusion

- Many useful out of the box features
- Customisable
  - Define metric once, apply everywhere
  - Create Enterprise wide reports
- Highlights security concerns while providing framework for resolving them.

Q & A

chris.lambert@cern.ch