Guardium ATAP Management

Frederic Petit ©2023 - Context22 - Original version 2017

ATAP

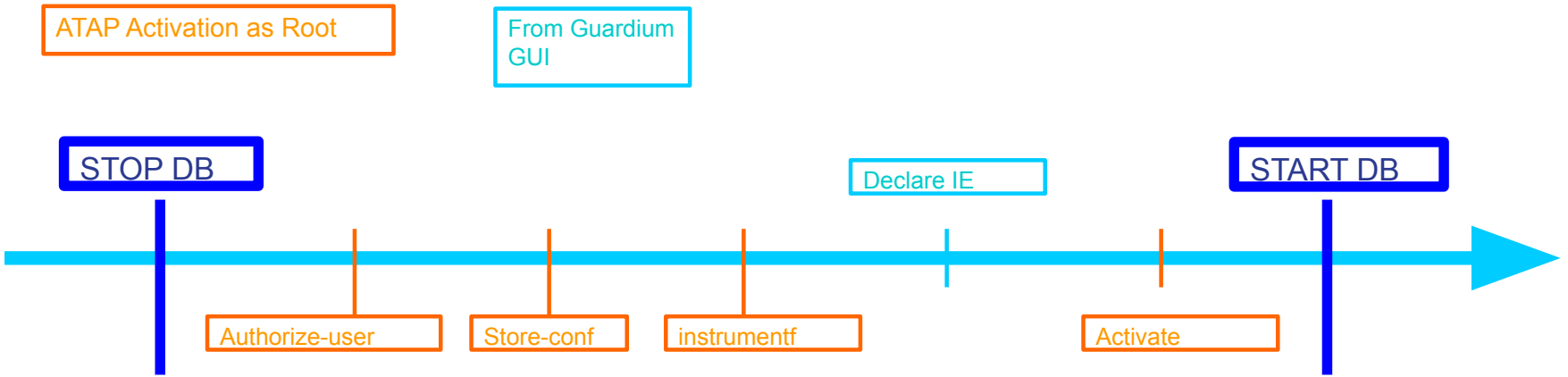
- Why ?
  - To catch in Plain-Text SSL Encrypted DB traffic
- What ?
  - NO additional process
  - Activation of a KTAP internal feature (ATAP) to access certain parts of the memory where the traffic is in plain-text
  - Does NOT decrypt. Does NOT access or need keys
- How ?
  - Series of commands to be executed as root on the DB server
  - ALL DB Instances using the same DB executable MUST be Down prior to activate the ATAP
  - Oracle executable gets RENAMED and a wrapper with the name of the oracle executable gets created
  - STAP Upgrade : Deactivation of STAP required
  - NO need to reboot the server at any point of time. Only the Instances and their listeners.

Reference: http://www.01.ibm.com/support/knowledgecenter/SSMPHH_9.5.0/com.ibm.guardium01.doc/stap/topics/atap.html

4 Commands from guardctl

- /usr/local/guardium/modules/ATAP/current/files/bin/*guardctl* **authorize_user oracle**
- *guardctl* --db-user=$usr --db-type=oracle --db-instance=$inst --db-home=$ORACLE_HOME --db-version=$ver --db-use-instrumented=yes **store-conf**
- *guardctl* --db-instance=$inst **instrument**
- *guardctl* --db-instance=$inst **activate**

ATAP Sequence of Events for First Activation



Before ATAP Activation:

/$ORACLE_HOME/bin/oracle

After ATAP Activation:

/$ORACLE_HOME/bin/oracle
/$ORACLE_HOME/bin/oracle_guard_original
/$ORACLE_HOME/bin/oracle_guard_instrumented

IMPACT on Databases

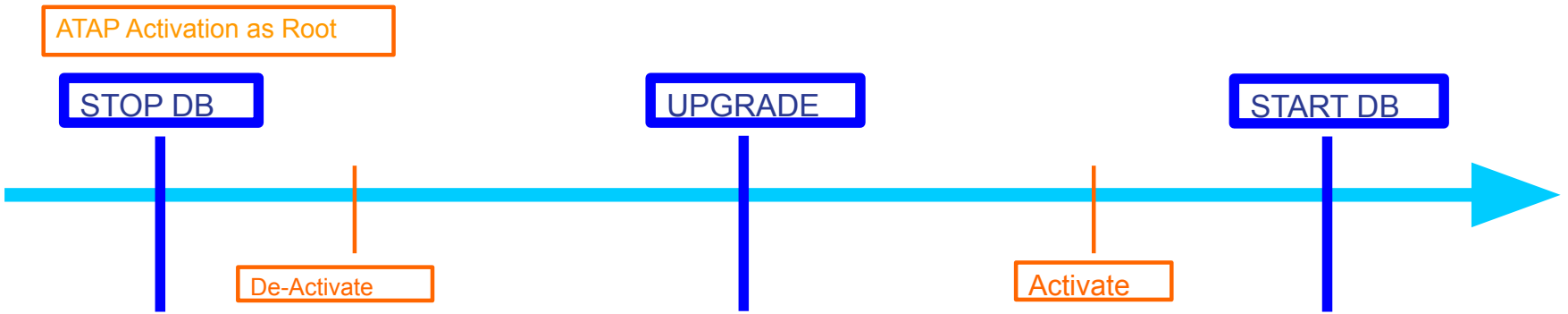
- NO Impact on Functionalities
- Impact on SEs and DBAs as the oracle executable is NOT “oracle” anymore but “oracle_guard_instrumented”.
  - All Performances analysis on oracle exe must be done on the renamed oracle executable
  - OS and DB Upgrade require ATAP be de-activated prior to the upgrade and re-activated after

ATAP Sequence of Events for Major Upgrades

- Deactivate ATAP
- Un-Install STAP/KTAP
- ReBoot Server
- Re-install STAP/KTAP
- Declare Inspection Engine
- Activate ATAP

ATAP Sequence of Events for Minor Upgrades

Applies to ALL types of upgrades: DB upgrade, STAP upgrade, OS upgrade



Before Upgrade:

/ORACLE_HOME/bin/oracle
/ORACLE_HOME/bin/oracle_guard_original
/ORACLE_HOME/bin/oracle_guard_instrumented

During Upgrade:

/ORACLE_HOME/bin/oracle

After Upgrade:

/ORACLE_HOME/bin/oracle
/ORACLE_HOME/bin/oracle_guard_original
/ORACLE_HOME/bin/oracle_guard_instrumented

What to do in case ATAP was NOT deactivated BEFORE an upgrade

- In case of Major Upgrade
  - un-Install STAP/KTAP, reboot, re-Install STAP, re-Activate ATAP
- In Case of Minor Upgrade
  - The oracle executable may have been re-installed
  - Open PMR to make sure ATAP gets properly re-activated