IBM Security

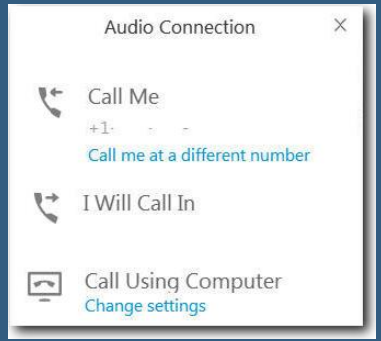
Configuring and Troubleshooting ATAP and EXIT Functionalities for Database Traffic Collection

IBM SECURITY SUPPORT OPEN MIC

To hear the WebEx audio, **select an option** in the Audio Connection dialog or by access the Communicate > Audio Connection menu option. To ask a question by voice, you must either Call In or have a microphone on your device.

You will not hear sound until the host opens the audio line.

For more information, visit:
http://ibm.biz/WebExOverview_SupportOpenMic



November 30, 2017

IBM

Panelists

Presenter

Serge Konevsky
Guardium Support

Moderator

Andrew McCarl
Knowledge Manager, IBM Security

Goal of session

This session is intended to educate the Guardium® user how to configure, activate and troubleshoot ATAP and EXIT functionalities to collect database traffic.

ATAP Configuration and Activation

Subject

Certain traffic can only be tapped at the database server application level due to either encryption configured or specific internal database implementation details. In these cases the ATAP (application-level tapping) mechanism which monitors communication between internal components of the database server should be used. ATAP uses K-TAP as a proxy to pass data to S-TAP, and needs to be configured separately for each database environment.

ATAP should be configured and activated for:

- Oracle (both ASO and SSL), DB2, Informix, Sybase, Postgres, Mongo encryption on all platforms
- DB2 and Informix shared memory traffic on Linux
- Teradata traffic collection

ATAP Configuration

- ATAP can be controlled by the **guardctl** utility or on some platforms (Solaris, HPUX and AIX) activated from the S-TAP GUI configuration using encryption box in the **Inspection Engine** or **encryption=1** configured in **guard_tap.ini** file
- The **guardctl** utility is installed under **<guardium_base>/guard_stap** directory where **<guardium_base>** is a Guardium® S-TAP installation directory. In case of a GIM installation, **guardctl** will be installed under **<guardium_base>/modules/ATAP/current/files/bin**.
- The **guardctl** utility provides commands that facilitate different aspects of ATAP installation, activation, and deactivation. To use the **guardctl** utility **root** access is required.
- Please note that the **guardctl** utility requires bash shell v. 3 or greater (**bash –version** command to verify), and it is not supported in the environment where a 32-bit database is located on a 64-bit server.

ATAP Configuration

Syntax and commands

<guardium_base>/xxx/guardctl [<name>=value>] [<name>=<value> ...] [command]

- *help* - default command, prints the list of supported commands, parameters and their default values
- *dump-params* - dumps current values of parameters
- *store-conf* - stores the configuration for a particular DB instance
- *store-system-conf* - stores the system configuration parameters
- *activate* – activates ATAP for the specified DB instance using the stored parameters
- *deactivate* - deactivates one DB instance
- *deactivate-all* - deactivate a list of instances, or if none given - deactivate all active instances
- *instrument* – created relinked instrumented Oracle
- *deinstrument* - remove instrumented Oracle
- *list-active* - lists DB instance user names of all active DB instances
- *is-active* - returns 1 if there is at least one active instance with ATAP, 0 otherwise list-configured - lists DB instances with configured but inactive ATAP mechanism
- *is-user-authorized* - checks whether the db-user (running ATAP) is authorized to log database traffic to KTAP/S-TAP
- authorize-user - adds user to 'guardium' authorization group
- *oracle-relink - db-exec* - relinks Oracle
- *prepare-libs* - prepares libraries for use in Zone/WPAR installation
- *get-statistics* - get ATAP statistics

ATAP Configuration Steps

❑ Authorizing user

- Stop the database. Logoff from all active DB sessions.
- As a **root** user, authorize user to log traffic by running the following command:
  <guardium_base>/xxx/guardctl authorize-user <user-name>

  Example:
  /usr/local/guardium/guard_stap/guardctl authorize-user postgres

❑ Storing parameters

- As a **root** user, store configuration for the db-instance as follows:
  <guardium_base>/xxx/guardctl db_instance=<instance> [<name>=<value> ...] store-conf

  Example:

  /usr/local/guardium/guard_stap/guardctl--db-user=oracle11 --db-type=oracle --db-instance=on12rh60
  --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf

Please use the following platform and database specific requirements for ATAP configuration.

Oracle

Required Parameter	Value	How to determine
db-user	Oracle username	Points to the DB instance user name
db_instance	Oracle instance name	use $ORACLE_SID value
db_type	oracle	
db_home	Points to where the DB version is installed	use $ORACLE_HOME value
db_version	The database version	run SELECT * FROM V$VERSION

Optional Parameter	Value	How to determine	When required
db_base	Home directory of db_user	DB instance user home directory. Value for db_base should match the correct path for $ORACLE_BASE or DB instance user home directory. It cannot be ~DB_USER.	db-base is not the same as db-home
db_relink	no/yes	ATAP activation method	
db_use_instrumented	no/yes	ATAP activation uses relinked version of Oracle previously created with instrument command.	Instrument is required for: • Oracle 12 SSL • Oracle 11.2 SSL on AIX • Oracle < 11.2 ASO and SSL on AIX
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	

Please note that on AIX platform Oracle instance needs to be instrumented using the **instrument** command prior to activation. Starting 10.1, instrumentation is done automatically within the **activate** command.

Example:

/usr/local/guardium/guard_stap/guardctl --db-instance= on0waxwi instrument

DB2

Required Parameter	Value	How to determine
db-user	DB2 username	Points to the DB instance user name
db_instance	DB2 instance name	$ db2 LIST DATABASE DIRECTORY
db_type	Db2	
db_version	The database version	As DB2 user: $ db2level

Optional Parameter	Value	How to determine	When required
db_home	Points to where the DB version is installed	Same as db_base	
db_base	Home directory of db_user	DB instance user home directory. Value for db_base must be matching the correct path DB instance user home directory. It cannot be ~DB_USER.	db-base is not the same as db-home
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	
db2-shmsize	131072	DB2 shared memory size	Value is different than default
db2-c2soffset	61440	DB2 shared memory client area offset	Value is different than default
db2-c2soffset	20	DB2 shared memory header offset	Value is different than default

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=db2inst1 --db-type=db2 --db-instance=dn0rh7x6 --db-version=10.5 store-conf

Sybase

Required Parameter	Value	How to determine
db-user	Sybase username	Points to the DB instance user name
db_instance	Sybase instance name	Sybase Server instance name
db_type	sybase	
db_version	The database version	As Sybase user: select @@version

Optional Parameter	Value	How to determine	When required
db_base	Points to where the DB version is installed	Same as db_base	
db_base	Home directory of db_user	DB instance user home directory. Value for db_base must be matching the correct path DB instance user home directory. It cannot be ~DB_USER.	db-base is not the same as db-home
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	
db-tcp-min-port	0 to any integer	Low end of TCP port range to intercept	Using Real IPS
db-tcp-max-port	0 to any integer	High end of TCP port range to intercept	Using Real IPS

Example:
/usr/local/guardium/guard_stap/guardctl --db-user=sybase15 --db-type=sybase --db-instance=sn57rh7x --db-version=15 store-conf

Informix

Required Parameter	Value	How to determine
db-user	Informix username	Points to the DB instance user name
db_instance	Informix instance name	Informix Server instance name
db_type	informix	
db_version	The database version	As Informix user: dbaccess -V

Optional Parameter	Value	How to determine	When required
db_home	Points to where the DB version is installed	Same as db_base	
db_base	Home directory of db_user	DB instance user home directory. Value for db_base must be matching the correct path DB instance user home directory. It cannot be ~DB_USER.	db-base is not the same as db-home
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=informix --db-type=informix --db-instance=in17rh7x –d -version=11.70 store-conf

Postgres

Required Parameter	Value	How to determine
db-user	Postgres username	Points to the DB instance user name
db_instance	Postgres instance name	Postgres Server instance name
db_type	postgres	
db_version	The database version	As Postgres user: pg_ctl --version

Optional Parameter	Value	How to determine	When required
db_home	Points to where the DB version is installed	Same as db_base	
db_base	Home directory of db_user	DB instance user home directory. Value for db_base must be matching the correct path DB instance user home directory. It cannot be ~DB_USER.	Where db-base is not the same as db-home
db_bits	32 or 64	DB instance architecture (32 for 32-bit, 64 for 64-bit)	
db-tcp-min-port	0 to any integer	Low end of TCP port range to intercept	
db-tcp-max-port	0 to any integer	High end of TCP port range to intercept	

Example:

/usr/local/guardium/guard_stap/guardctl --db-user=postgres --db-type=postgres --db-instance=guardium_qa --db-version=19.4 --db-base=/home/postgres94 store-conf

MongoDB

Required Parameter	Value
db-user	Administrative user who can start and stop mongodb
db_instance	Can be any identifier such as host name
db_type	For the single instance - mongodb, for the sharded clusters - mongodb where mongod executable is present and mongodbs where mongos executable is present

Example:

/usr/local/guardium/guard_stap/guardctl --db-instance=rhmongodbssl07 --db-type=mongodbs --db-user=mongodb store-conf

ATAP Activation

❑ Activating ATAP

As root user:
<guardium_base>/xxx/guardctl db_instance=<instance> activate

- **Example:**

/usr/local/guardium/guard_stap/guardctl --db-instance=onrh60x activate

❑ Verifying activated instances

<guardium_base>/xxx/guardctl list-active
<guardium_base>/xxx/guardctl list-configured

Enabling encryption using S-TAP configuration (available on Solaris, HP-UX and AIX)

❑ Authorizing user

- Stop the database. Logoff from all active DB sessions.
- As a **root** user, authorize user to log traffic by running the following command:
  <guardium_base>/xxx/guardctl authorize-user <user-name>

- **Example:**

  /usr/local/guardium/guard_stap/guardctl authorize-user oracle

❑ Set encryption=1 in guard_tap.ini or check encryption box in the GUI for desired inspection engine

❑ Oracle SSL proper DB Version setting required for associated Inspection Engine

❑ Oracle 12 configured with SSL encryption and Oracle 11 configured with both ASO and SSL on AIX platform required instrumentation

- **Example:**

  <guardium_base>/xxx/guardctl --db-instance= $ORACLE_SID instrument

❑ Start Database

Teradata ATAP Configuration & Activation

- Determine user running **gtwgateway** and path

  Example:

  # ps -ef | grep gtwgateway

  teradata 5000 4608 0 Jan03 ? 00:00:05 /usr/tgtw/bin/gtwgateway

- **gtwgateway** runs as user **teradata**
- Set parameter **--db-user=teradata** to **guardctl**
- Default path to **gtwgateway** is **/usr/tgtw/bin/gtwgateway**, otherwise **tdc_gtwgateway** parameter should be configured:

  --tdc_gtwgateway=/usr/tgtw/bin/gtwgateway

- Determine path to **pdemain**
- Typically, this will be /usr/pde/bin/pdemain

- **Example**

  # ls -l /proc/4608/exe

  lrwxrwxrwx 1 root tdtrusted 0 2015-01-03 01:20 /proc/4608root 20620 20063

  0 12:40 pts/0 00:00:00 grep pdemain/exe -> /opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

- Checking the **inodes** for this file and **/usr/pde/bin/pdemain** to find out they are the same:

  # ls -li /opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

  1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

  # ls -li /usr/pde/bin/pdemain

  1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

- Since the inodes are the same and the default value for **--db-home=/usr/pde**, parameter in this case does not need to be set. Otherwise, it can be set to either

  --db-home=/opt/teradata/tdat/pde/15h.00.00.07

  --db-home=/usr/pde

Teradata ATAP Configuration & Activation

- Stop Teradata instance
- **Example:**

  # /etc/init.d/tgtw stop

  tgtw Shutdown complete

  # /etc/init.d/tpa stop

  PDE stopped for TPA shutdown

- Authorize DB user to the guardium group
- **Example:**

  /usr/local/guardium/guard_stap/guardctl --db-instance=teradata authorize-user

- Store ATAP configuration

  /usr/local/guardium/guard_stap/guardctl --db-instance=teradata --tdc_gtwgateway=/usr/tgtw/bin/gtwgateway --db-type=teradata --db-home=/opt/teradata/tdat/pde/15h.00.00.07 --db-user=teradata store-conf

- Activate **ATAP**
- **Example:**

  /usr/local/guardium/guard_stap/guardctl –db -instance=teradata activate

- Start Teradata instance
- **Example:**

  # /etc/init.d/tpa start

  Teradata Database Initiator service is starting...

  Teradata Database Initiator service started successfully.

  # /etc/init.d/tgtw start

  tgtw Startup complete

Configuration & Activation in Solaris Zones and AIX WPARs environment

- Please refer to:

  https://www.ibm.com/support/knowledgecenter/en/SSMPHH_10.1.0/com.ibm.guardium.doc.stap/stap/atap_zones_install_wpars.html

  https://www.ibm.com/support/knowledgecenter/en/SSMPHH_10.1.0/com.ibm.guardium.doc.stap/stap/atap_zones_upgrade_wpars.html

  for ATAP installation, activation and upgrade in Solaris Zones and AIX WPARs environment.

S-TAP Upgrade and Database patching

- Stop the database. Logoff from all active DB sessions

- **Deactivate ATAP**
  - Stop the database. Logoff from all active database sessions.
  - Deactivate ATAP either for a specific database instance:

<guardium_base>/xxx/guardctl –db-instance=<instance-name> deactivate

or for all active instances:

<guardium_base>/xxx/guardctl deactivate-all

Please note that in S-TAP prior to version 10.1, if the instance was instrumented, it has to be deinstrumented before deactivation:

<guardium_base>/xxx/guardctl –db-instance=<instance-name> deinstrument
<guardium_base>/xxx/guardctl –db-instance=<instance-name> deactivate

- **Verify ATAP being deactivated**

<guardium_base>/xxx/guardctl list-active
<guardium_base>/xxx/guardctl list-configured

Failure to deactivate ATAP - Troubleshooting

- Stop the database.

- Remove "oracle-guard-original" executable
  Example:
  $ ls -lrt product/11.1.0/db_1/bin/oracle*
  -rwsr-s--x 1 oracle11 dba 200701162 Jan 17 2014 product/11.1.0/db_1/bin/oracleO
  -rwsr-s--x 1 oracle11 dba 200701162 Feb 24 15:32 product/11.1.0/db_1/bin/**oracle-guard-original**
  -rwsr-s--x 1 oracle11 dba 200701162 Feb 24 15:53 product/11.1.0/db_1/bin/oracle
  $ rm product/11.1.0/db_1/bin/**oracle-guard-original**
  $ ls -lrt product/11.1.0/db_1/bin/oracle*
  -rwsr-s--x 1 oracle11 dba 200701162 Jan 17 2014 product/11.1.0/db_1/bin/oracleO
  -rwsr-s--x 1 oracle11 dba 200701162 Feb 24 15:53 product/11.1.0/db_1/bin/oracle

- Remove ATAP configuration file and executor:
  <guardium install dir>/etc/guard/<Oracle instance>.conf
  <guardium install dir>/etc/guard/executor/<Oracle instance>

- Configure ATAP:
  /usr/local/guardium/modules/ATAP/current/files/bin/guardctl --db-instance=DPDEVUG --db-user=oracle --db-type=oracle --db-base=/orahome/u01/app/oracle --db-bits=64 --db-home=/orahome/u01/app/oracle/product/12.1.0.2/db_2 --db-version=12.1 --db-use-instrumented=no --db-relink-script=relink activate

- Activate ATAP: /usr/local/guardium/modules/ATAP/current/files/bin/guardctl --db-instance=DPDEVUG activate

- Verify that ATAP is active: /usr/local/guardium/guard_stap/guardctl list-active

- Start the database.

No traffic collection - Troubleshooting

- Enable S-TAP debug:
  tap_debug_output_level = 4 in guard_tap.ini file followed by S-TAP restart.

- Collect and analyze the output in /tmp/guard_stap.stderr.txt

- Enable KTAP debug:
  <guardium_base>/guard_stap/ktap/guard_ktap_log set 2 - shell S-TAP installation
  <guardium_base>/modules/KTAP/current/guard_ktap_log set 2 - GIM S-TAP installation

- Collect and analyze the output in
  /var/log/messages - Linux
  /var/log/ktap.log - AIX
  /var/adm/syslog/syslog.log - HP-UX
  /var/adm/messages - Solaris

  where the following messages (example) showing that TCP packets have been "pushed" to S-TAP:

  Sep 26 14:58:58 icl-mongad-vm01 kernel: (v 90390) GUARD-02: 31406 ktap_service_ioctl: GT_PUSH_PACKET ioctl (line 4109)
  Sep 26 14:58:58 icl-mongad-vm01 kernel: (v 90390) GUARD-02: 31406 ktap_ioctl: cmd 0x405a470f, arg 120217600 (line 542)
  Sep 26 14:58:58 icl-mongad-vm01 kernel: (v 90390) GUARD-02: 31406 ktap_service_ioctl: ktap_service_ioctl (405a470f) (line 4045)
  Sep 26 14:58:58 icl-mongad-vm01 kernel: (v 90390) GUARD-02: 31406 ktap_service_ioctl: GT_PUSH_PACKET ioctl (line 4109)

- Disable S-TAP debug:
  tap_debug_output_level = 0 in guard_tap.ini file followed by S-TAP restart.

- Disable KTAP debug:
  <guardium_base>/guard_stap/ktap/guard_ktap_log set 0 - shell S-TAP installation
  <guardium_base>/modules/KTAP/current/guard_ktap_log set 0 - GIM S-TAP installation

Exit Functionality Configuration and Activation

Exit Functionality

DB2, Informix and Teradata Exit are the drivers provided by DB2, Informix and Teradata to directly interface with S-TAP to collect all database traffic.

- DB2 Exit functionality was initially designed to collect traffic starting with DB2 v10 and higher, but later backported to DB2 v9.7 using patch DB2 9.7.0.9
- DB2 Exit does not support data redaction functionality, S-GATE support started in v10.1.2
- UID chain is supported with the following DB2 patches: V97FP10, V101FP4 and V105FP3
- Informix Exit functionality designed to collect traffic starting with Informix 12.10xC5W1
- Informix Exit supports both redact and S-GATE functionalities
- Teradata Exit functionality designed to collect traffic starting with Teradata v16
- Teradata Exit does not support UID chain and data redaction, but supports S-GATE functionality
- Neither KTAP kernel module needed to be loaded, nor ATAP configured when using Exit functionality

DB2 Exit

DB2 Exit libraries:

- DB2 32 bit installations on ***Linux/Solaris/HP-UX***: libguard_db2_exit_32.so
- DB2 64 bit installations on ***Linux/Solaris/HP-UX*** : libguard_db2_exit_64.so
- DB2 32 bit installations on ***AIX***: libguard_db2_exit_32.a
- DB2 64 bit installations on ***AIX***: libguard_db2_exit_64.a

DB2 Exit configuration:

1. Use **db2level** command to find DB2 version and bitwise.
2. In the DB2 directory create **commexit** directory to copy the Exit library:
   32 bit installation - **mkdir $DB2_HOME/sqllib/security/plugin/commexit**
   64 bit installation - **mkdir $DB2_HOME/sqllib/security64/plugin/commexit**
3. Copy Exit library to the **commexit** directory. The Exit library is located in the following directories:
   - Shell STAP installation: **~/guard_stap**
   - GIM STAP installation: **~/modules/STAP/current/files/lib**
4. Change the owner of **commexit** directory and library files in this directory.

   Example:

   # su - db2inst2
   db2inst2@<host_name>:~> id
   uid=1028(db2inst2) gid=114(db2iadm1) groups=114(db2iadm1),16(dialout),33(video),113(dasadm1)
   db2inst2@<host_name>:~> exit
   logout
   # chown db2inst2:db2iadm1 /home/db2inst2/sqllib/security64/plugin/commexit/
   # chown db2inst2:db2iadm1 /home/db2inst2/sqllib/security64/plugin/commexit/libguard_db2_exit_64.so

DB2 Exit

5. Add DB2 user to **guardium** group.

   Example:

   /usr/local/guardium/guard_stap/guardctl authorize-user db2inst2

6. Enable Exit library as a DB2 user:

   32 bit installation - **db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit**

   64 bit installation - **db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64**

7. Configure DB2 Exit Inspection Engine:
   - **Protocol**: DB2 Exit
   - **DB Install Dir**:
     - log into DB2
     - run **echo $DB2_HOME**
     - DB Install Dir is the output of the above command without **sqllib**
   - **Process name**: full path to **db2sysc**
8. Restart DB2 database.

Useful Commands:

- disabling DB2 Exit library - **db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL**
- verifying if Exit library is used :

  db2 get database manager configuration

  and check the line **Communication buffer exit library list**

DB2 Exit

No traffic collection - troubleshooting

- **tap_debug_output_level = 10** - debug info will be logged into S-TAP log and db2diag.log (db2_exit log)
- **tap_debug_output_level = 11** - debug info will only be logged into db2diag.log (db2_exit log)

1. **Messages in DB2diag.log:**

2017-03-28-13.52.33.666892-300 E10694A499 LEVEL: Severe
PID : 8519682 TID : 4628 PROC : db2sysc 0
INSTANCE: db2tord1 NODE : 000
APPHDL : 0-11108
HOSTNAME: cf11n01-e0
EDUID : 4628 EDUNAME: db2agent () 0
FUNCTION: DB2 UDB, DRDA Communication Manager, sqljcCommexitLogMessage, probe:219
DATA #1 : String with size, 108 bytes
Register: setting send_data to 0 - client protocol is 6, conf_msg is a00000023f5c000, guard_intercept_flag 0

Cause and Troubleshooting:

DB2 tried to open a shared memory connection with S-TAP to send traffic, but failed.

- log into DB2
- run **echo $DB2_HOME**
- update **DB Install Dir** in **Inspection Engine** leaving out **sqllib**
- verify traffic collection
- if no traffic collection, then restart DB2

DB2 Exit

2. Message in DB2diag.log:

Warning : Shmem_access /.guard_writer0 failed Error opening shared memory area errno=2 err=8

Cause and Troubleshooting:

DB2 started before the S-TAP.

- S-TAP with Inspection Engine configured must be up before DB2 started, therefore restart DB2
- verify traffic collection
- verify in DB2diag.log the following message :
  Attached /.guard_writer0 shmem comm exit shm initialization successful

❑ Improvement in v10.1.3:

- order in which S-TAP and DB2 started is no longer relevant
- if S-TAP started after DB2, it will create a shared memory segment DB2 Exit library can access whenever there is a new DB2 connection
- Exit library needs to open a shared memory region to pass the data to S-TAP, 15 seconds interval was added between each try until it has been successfully opened

DB2 Exit

3. **Message in DB2diag.log:**

2017-09-25-14.58.18.204732-240 E27465E476 LEVEL: Severe
PID : 7719 TID : 70366894420400 PROC : db2sysc 0
INSTANCE: db2inst3 NODE : 000
APPHDL : 0-7
HOSTNAME: rh7le64t
EDUID : 22 EDUNAME: db2agent () 0
FUNCTION: DB2 UDB, DRDA Communication Manager, sqljcCommexitLogMessage, probe:219
DATA #1 : String with size, 92 bytes
WARNING: Shmem_access /.guard_writer0 failed Error opening shared memory area errno=13 err=8

Cause and Troubleshooting:

User is not authorized

- Logoff from all active DB sessions
- Authorize user using guardctl command

Example:

/usr/local/guardium/guard_stap/guardctl authorize-user db2inst2

Informix Exit

Informix Exit libraries:

- Informix 32 bit installations: libguard_informix_exit_32.so
- Informix 64 bit installations: libguard_informix_exit_64.so

Informix Exit configuration

1. Stop Informix database
2. Add Informix user to **guardium** group

   Example:

   /usr/local/guardium/guard_stap/guardctl authorize-user Informix
3. Configure Informix Exit
   - as Informix user, set up the environment variable:

     Example:

     source in2thor0.ksh
   - use **which oninit** command to find Informix version and **oninit** full path
   - use **file xxx/xxx/oninit** command to determine bitwise
4. Copy Exit library to Informix library directory. The Exit library is located in the following directories:
   - Shell STAP installation: **~/guard_stap**
   - GIM STAP installation: **~/modules/STAP/current/files/lib**

Informix Exit

5. Configure Informix Exit Inspection Engine:
   - **Protocol**: Informix Exit
   - **DB Install Dir**:
     - log into Informix
     - run **echo $HOME**
     - **DB Install Dir** is the output of the above command
   - **Process name**: full path to **oninit**

6. Setup ifxguard:

   Create configuration file under **$INFORMIXDIR/etc/ifxguard.$INFORMIXSERVER**

   Example:

   NAME ol_informix1210
   WORKERS 2
   LIBPATH /home/informix/12.10.FC6/lib/libguard_informix.so
   DEBUG 1
   LOGFILE /home/informix/12.10.FC6/etc/ifxguard.msg.txtg.txt

   where **$INFORMIXDIR=/home/informix/12.10.FC6**

Informix Exit

7. Start ifxguard:

   - use onstat – command to make sure that Informix database server is online:
     $ id
     uid=501(informix) gid=205(informix) groups=215(guardium)
     $ onstat -
     IBM Informix Dynamic Server Version 12.10.FC6 -- On-Line -- Up 6 days 00:22:25 -- 253104 Kbytes

   - as user **informix** start **ifxguard**:
     $ ifxguard
     15:20:17 ifxguard set instance name ol_informix1210
     Starting ifxguard ol_informix1210 ...
     check log file: /home/informix/12.10.FC6/etc/ifxguard.msg.txt

   - if **ifxguard** configuration file is not setup, agent can be brought up after specifying the .so library using full path with **-p** option and message log file with **-l** option, and file **$INFORMIXDIR/etc/ifxguard.$INFORMIXSERVER** will be generated:

     Example:
     $ ifxguard -p /home/informix/12.10.FC6/lib/libguard_informix_exit_64.so -l home/informix/12.10.FC6/etc/ifxguard.msg.txt

8. Start Informix database

Informix Exit

No traffic collection – troubleshooting:

- after starting ifxguard verify there is no errors in log file /tmp/logfile.txt
- verify if ifxguard started before configuring **Inspection Engine** by checking date of process
- if not, then stop **ifxguard** using **ifxguard -k** command
- configure **Inspection Engine**
- start ifxguard

When patching Informix:

- stop ifxguard
- patch the database
- start ifxguard

When upgrading S-TAP with ifxguard activated:

- stop ifxguard
- upgrade S-TAP
- copy the **libguard_informix_exit_64.so** from guard_stap directory to Informix library directory
- start ifxguard

Please note that Informix Exit library can be disabled as following:

```
ifxguard -kill $INFORMIXSERVER
```

Teradata Exit

- Teradata Exit is the same as DB2 Exit with the only difference that **DB Install Dir** in the **Inspection Engine** needs to be set to **/root** because **gtwgateway** runs as **root**

- Configure Teradata Exit Inspection Engine:
  - **Protocol**: TRD Exit
  - **DB Install Dir**: /root
  - **Process Name:** full path to **gtwgateway**

    Example:
    /opt/teradata/tdat/tgtw/16.00.00.05sks/bin/gtwgateway

- Authorize users and activate:

ln -s /usr/local/guardium/lib64/libguard_teradata_exit_64.so /opt/teradata/tdat/tgtw/site/libtgtwmonitoring.so
/usr/local/guardium/guard_stap/guardctl --db-user=tdatuser authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=teradata authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=root authorize-user
/usr/tgtw/bin/gtwcontrol --monitorlib load=yes

Questions for the panel

Now is your opportunity to ask questions of our panelists.

<u>To ask a question now:</u>

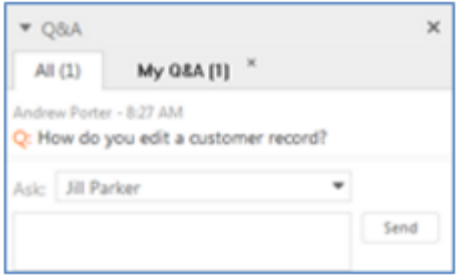
Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

Type a question in the box below the Ask drop-down menu in the Q&A panel.

Select *All Panelists* from the Ask drop-down-menu.

Click Send. Your message is sent and appears in the Q&A panel.



<u>To ask a question after this presentation:</u>

You are encouraged to participate in the dW Answers forum: <https://developer.ibm.com/answers/topics/TAG.html>

IBM Security Learning Academy

www.SecurityLearningAcademy.com

New content published daily!

Learning at no cost!

Learning Videos • Hands-on Labs • Live Events

Where do you get more information?

Questions on this or other topics can be directed to the product forum: <hotspot to forum for this product>.

More information you can review:

- **Security Learning Academy: <link>**
- **Technote x: <link>**
- **IBM developerWorks articles: <link>**
- **IBM Knowledge Center: <link to product welcome page>**

Useful links:

Get started with IBM Security Support

IBM Support Portal | Sign up for “My Notifications”

FREE learning resources on the Security Learning Academy

Follow us:

IBM Security

THANK YOU

FOLLOW US ON:

facebook.com/IBMSecuritySupport

youtube/user/IBMSecuritySupport

@askibmsecurity

SecurityLearningAcademy.com

securityintelligence.com

xforce.ibmcloud.com

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM

Configuring and Troubleshooting ATAP and EXIT Functionalities for Database Traffic Collection

IBM Security
Support