Contents

Summary

The S-TAP for IBM i has been re-architected to support the following critical enterprise readiness features for scalability, high availability and security:

- S-TAP load balancing, to support:
  - Failover of monitoring traffic to another collector if the primary collector is unavailable
  - Round robin session data among a list of available collectors
  - Send duplicate data to multiple collectors for high availability
- TLS encryption between the S-TAP and the Guardium collector

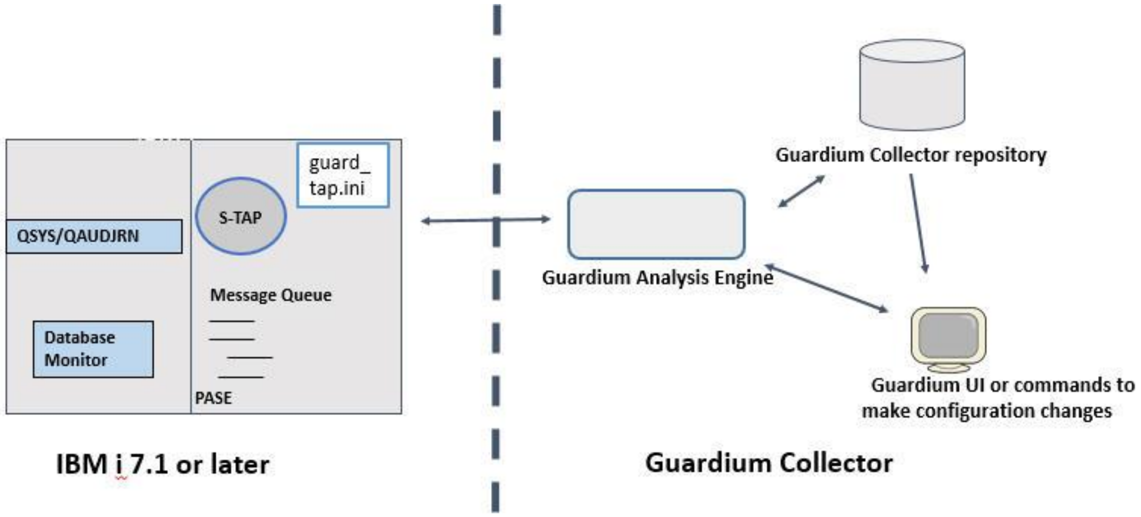
S-TAP TLS support and load balancing is supported only for IBM I 7.1 and 7.2.

Note: Even before the enhancements delivered in this patch, you can use hardware balancing (such as F5) with participate_in_load_balancing=**1** and a virtual IP address in the primary SQLGuard section of the configuration file.

As shown in Figure 1, the architecture is largely unchanged, except that now the S-TAP is more closely aligned with the way that UNIX S-TAPs behave. Similarly to UNIX S-TAPs, i S-TAP configuration parameters are saved in a guard_tap.ini file in the /usr/local/guardium directory on the IBM i server.

Administrators configure the S-TAP is done using the same APIs and UI (S-TAP Control) as other UNIX S-TAPS. When the GUI or API is used to make a change to the S-TAP configuration, Guardium sniffer sends a message to the S-TAP, which backs up the old .ini file, saves the configuration to the new .ini file and then restarts itself.

Administrators can set up encrypted communication between the S-TAP and the appliance using the S-TAP configuration controls as well as set up various load balancing options. These options will be explained in more detail in this document.



Compatibility considerations

The capabilities described in this document require both the collector and the S-TAP to be at the V10 level. In a mixed mode environment, the new capabilities are not available.

Considerations for managing the i S-TAP configuration and filtering parameters after update

After the environment is brought up to V10, you will need to change the way you interact with the S-TAP. Previously, all S-TAP configurations and filtering options were controlled using the update_istap_config API.

With the new S-TAP, you will still use the update_istap_config API to:

- Set filtering parameters (filter_user, filter_table, etc)
- Set datasource name of the DB2 for i
- Set the audit server user profile
- Restart the audit server

But for other configuration parameters such as the Guardium host IP, connection timeout, and so on, you will use the S-TAP Control GUI, the update_stap_config API, or edit the guard_tap.ini file directly as explained in Modifying S-TAP configuration parameters, below.

Configuring the environment

Installing the S-TAP

These instructions highlight new installation parameters and behavior for the DB2 for i S-TAP.

Note: GIM installation and update is not supported

If you already have a previous release i S-TAP installed, make sure you understand the implications of installing the new S-TAP such as how to modify S-TAP configuration parameters before installing the new S-TAP. When S-TAP first connects to the V10 collector, the collector will determine if this is the new or old S-TAP. It will coexist with the old S-TAP, but new capabilities are not supported, as indicated in the coexistence table above.

Steps:

In the PASE shell environment on the IBM i server, create a temporary directory to put t S-TAP installation script (such as /tmp). You can use a 5250 emulator software to connect to the IBM i system remotely and enter the PASE shell by entering **call qp2term.**

2. Use FTP to move S-TAP installation shell script to that temporary directory.

```
guard-itap-10.0.0_r79963_trunk_1-aix-5.3-aix-powerpc.sh
```

3. In the same directory, run the following command:

```
guard-itap-10.0.0_r79963_trunk_1-aix-5.3-aix-powerpc.sh --sqlguardip <guardium_host_IP>
-u | -overwrite-existing [--tls force | failover | none]
```

sqlguardip - The IP or host name of the Guardium collector this S-TAP communicates with.

If an existing i S-TAP exists, you will need to specify one of the following:
-u – Keep the existing configuration parameters and update the S-TAP configuration with the parameters entered on the command.

-overwrite-existing – Overwrites the existing installation and creates a new guard_tap.ini file with default parameters.

The following is optional:
--tls force | failover | none

- **--tls force** uses TLS encryption. If a secure protocol cannot be obtained when connecting, the S-TAP can fall back to using a nonsecure protocol.
- **--tls failover** uses TLS encryption. If it fails to connect to a collector it must continue to try using TLS.
- **--tls none** means do not encrypt the connection. This is also the default if tls is not specified

See Setting up S-TAP encryption, below, for more information about configuring encryption.

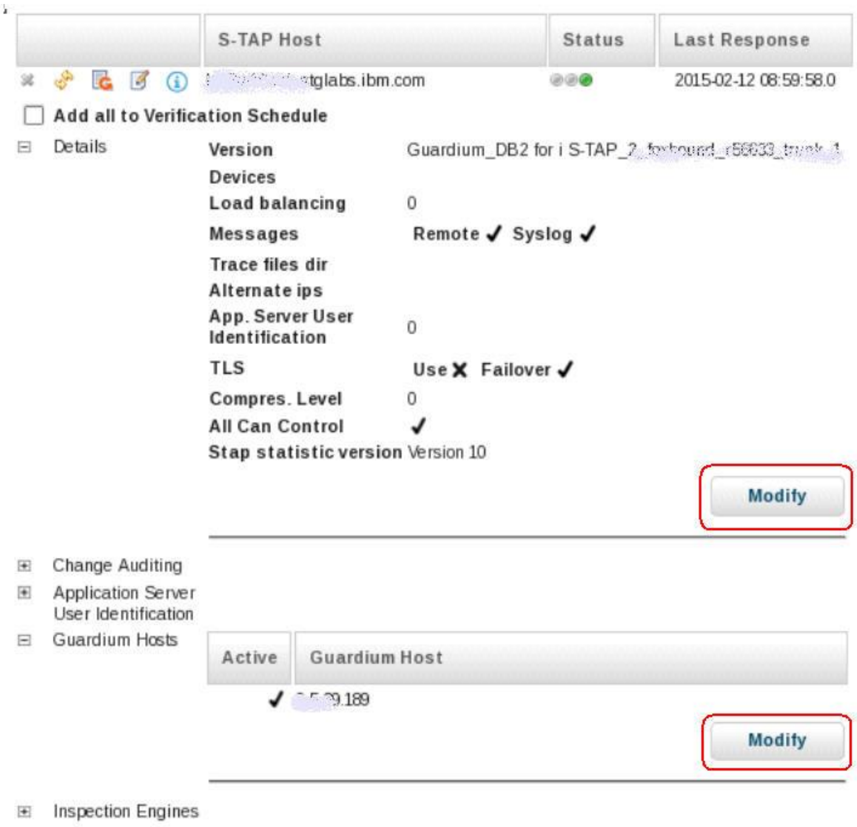
The installation program will install under /usr/local/guardium. If you have a previous S-TAP installation, it will copy the Guardium host IP to a new S-TAP configuration file guard_tap.ini.

4. In the Guardium UI, navigate to the S-TAP Status Monitor and ensure the light is green indicating that the S-TAP is communicating with the collector.

Modifying S-TAP configuration parameters

To modify S-TAP parameters, you have the following options:

- Use the S-TAP Control GUI.



	S-TAP Host	Status	Last Response
	[redacted]tglabs.ibm.com	●●●	2015-02-12 08:59:58.0

☐ Add all to Verification Schedule

⊟ Details

Version	Guardium_DB2 for i S-TAP_2_[redacted]
Devices	
Load balancing	0
Messages	Remote ✓ Syslog ✓
Trace files dir	
Alternate ips	
App. Server User Identification	0
TLS	Use ✗ Failover ✓
Compres. Level	0
All Can Control	✓
Stap statistic version	Version 10

⊞ Change Auditing

⊞ Application Server User Identification

⊟ Guardium Hosts

Active	Guardium Host
✓	[redacted]9.189

⊞ Inspection Engines

- Use the Guardium API update_stap_config
  Examples:

```
grdapi update_stap_config stapHost=lp1nnnnn6.rch.stglabs.ibm.com
updateValue=TAP.use_tls:1
```

```
grdapi update_stap_config stapHost=lp1nnnn6.rch.stglabs.ibm.com
updateValue=TAP.connection_timeout_sec:30
```

```
grdapi update_stap_config stapHost=lp1nnnn6.rch.stglabs.ibm.com
updateValue=TAP.participate_in_load_balancing:2
```

Note: For backward compatibility, when you update guardium_host through S-TAP configuration controls and grdapi, it will also update the guardium host column in the configuration table on i server. If there is only one Guardium host in guard_tap.ini and it is different than the Guardium host in the IBM i server configuration table, the Guardium host on the IBM i server will be used.

- Edit the guard_tap.ini file directly on the database server using a text editor.

The file is divided into sections: [TAP] for general parameters and [SQLGuard] for parameters related to specific Guardium collectors. There is one [SQLGuard] section for each Guardium collector.

```
************Beginning of data**************
[TAP]
remote_messages=1
all_can_control=0
tap_debug_output_level=3
use_tls=0
failover_tls=1
guardium_ca_path=NULL
sqlguard_cert_cn=NULL
guardium_crl_path=NULL
connection_timeout_sec=10
check_server_hb=0
participate_in_load_balancing=0
allow_lose=0
stap_statistic_sec=0
buffer_file_size=50
buffer_mmap_file=0
[SQLGuard_]
sqlguard_ip=9.5.12.126
sqlguard_port=16016
primary=1
connection_pool_size=0
```

Guard_tap.ini file parameters for the DB2 for i S-TAP (alphabetical order)

Table 1 describes each of the parameters in the DB2 for i S-TAP and whether it can be updated using the S-TAP Control GUI or the **update_stap_config** API. If neither of these options are available, you must edit the file directly.

Note: display_stap_config also works for the new i S-TAP.

Parameters that have [SQLGuard] in the description refer to specific Guardium collector configurations. Otherwise, the parameter is a general parameter. The S-TAP descriptions can also be found in the Knowledge Center at http://www-01.ibm.com/support/knowledgecenter/SSMPHH_10.0.0/com.ibm.guardium.doc.stap/stap/stap_parms_u.html

Table 1. S-TAP parameters in the guard_tap.ini file

Parameter	Description	GUI	GRDAPI
all_can_control	0=S-TAP can be controlled only from the primary Guardium system. 1=S-TAP can be controlled from any Guardium system (sqlguard_ip parameter)._	X	X
allow_lose	For serviceability only.		
buffer_file_size	Advanced use only. Size in MB of the buffer allocated for		

	the packets queue. The default is 50. See the IBM Redbook *Deployment Guide for InfoSphere Guardium* for information about this parameter.		
buffer_mmap_file	Advanced use only. 1=memory mapped file option. 0=virtual memory allocation The default is 0. See the IBM Redbook *Deployment Guide for InfoSphere Guardium* for information about this parameter.		
check_server_hb=0	For serviceability only.		
connection_pool_size	[SQLGuard] Number of opened connections from S-TAP to Guardium sniffer. When TLS is enabled, the feature is called Multi TLS. The value is an integer.		
connection_timeout_sec	Number of seconds after which the S-TAP will consider a Guardium server to be unavailable. At that point, the S-TAP will failover to another collector (if one is configured) after 5*connection_timeout_sec or when the limited memory buffer is half full. It can have any integer value. The default is 60.		
failover_tls	1= If an encrypted connection is not possible for any reason, fail over to using non-secure connection.	X	X

	0=use only secure connections. The default is 1.		
guardium_ca_path=	Path to CA.pem on the IBM i host. This is a file containing one or more trusted CA self-signed certificates in PEM format Default is NULL.		
guardium_crl_path	Path to crl.crl. PEM-encoded file with Certificate Revocation List from the CA. Any Guardium system certificate that has been revoked will be rejected Default is NULL.		
participate_in_load_balancing	Controls load balancing to SQL Guard servers: 0=NO, This is the default. All traffic is sent to one designated Guardium machine (1=YES. S-TAP balances all traffic to the Guardium systems listed by Client IP. If a hardware load balancer such as F5 is used, you can use a virtual IP of the hardware balancer. 2=REDUNDANCY. Fully mirrored S-TAP will send all traffic to all monitoring Guardium machines. 3=Hardware load balancing. This option is not applicable for the i S-TAP because the necessary information to support use of virtual IPs in hardware load balancing is available without specifying this option. To designate an SQL Guard server as a primary server, use the Primary property in the	X	X

	SQLGUARD section. If this parameter is set to 0, and you have more than one Guardium system monitoring traffic, then the non-primary Guardium systems are available for failover.		
primary	[SQLGuard] Indicates if the server is a primary server: 1=Primary, 2=Secondary, 3=tertiary, etc. If participate_in_load_balancing =1, there must be multiple Guardium collectors. If participate_in_load_balancing =0, there must be exactly one collector, the primary.		
remote_messages	1=Send error and diagnostic messages to the active collector. This option makes it easier to debug issues without requiring a login to the database server. 0=Do not send error messages. Default is 1.	X	X
sqlguard_cert_cn	The common name to expect from the Sqlguard certificate. The default is NULL.		
sqlguard_ip	[SQLGuard] IP v4 address or hostname of the Guardium system that will act as a host for the S-TAP.	X	
sqlguard_port	[SQLGuard] 16016 is the default. 16018 is used for encrypted communications.		
stap_statistic_sec	For serviceability only.		
tap_debug_output_level	For serviceability only.		
use_tls=0	1=use TLS to encrypt traffic between the S-TAP and the Guardium system. 0=do not encrypt. Default is 0.	X	X

Using S-TAP failover and load balancing

The failover and load balancing options for the i S-TAP are similar to what exists for UNIX S-TAPs. Use the participate_in_load_balancing parameter to determine whether to use failover or load balancing behavior, and use the SQLGuard sections of your S-TAP to set up primary, secondary, and tertiary Guardium hosts.

One difference is that there is no need for participate_in_load_balancing=3; because of the way the DB2 for i S-TAP communication is architected, complete session information is available on each message. This means that even before the enhancements delivered in this patch, you could have used hardware balancing (such as F5) with participate_in_load_balancing=**1** and a virtual IP address in the primary SQLGuard section of the configuration file.

For more information about load balancing options, see the IBM Redbook entitled *Deployment Guide for InfoSphere Guardium* at http://www.redbooks.ibm.com/abstracts/sg248129.html?Open

Failover

In a failover configuration, the S-TAP is configured to register with multiple collectors, but only send traffic to one collector at a time (participate_in_load_balancing=0). The S-TAP in this configuration sends all its traffic to one collector unless it encounters connectivity issues to that collector that triggers a failover to a secondary collector.

For example, to configure an STAP to report to primary, secondary, and tertiary collectors (should the primary and secondary become unavailable), the guard_tap.ini is configured to:

```
[SQLGuard_0]
sqlguard_ip=guard01
sqlguard_port=16016
primary=1
[SQLGuard_1]
sqlguard_ip=guard02
sqlguard_port=16016
primary=2
[SQLGuard_2]
sqlguard_ip=guard03
sqlguard_port=16016
primary=3
```

In this example, if the guard01 collector becomes unavailable, the S-TAP reports to guard02. If guard02 is also unavailable the S-TAP reports to guard03. If guard01 subsequently becomes available, the S-TAP moves back to it.

S-TAP session load balancing

If participate_in_load_balancing=1 then the S-TAP will go into load balancing mode. This means that database sessions will be split between three collectors as new connections are initiated to the database server.

S-TAP Session load balancing example:

```
[TAP]
participate_in_load_balancing=1
[SQLGuard_0]
sqlguard_ip=10.5.39.189
sqlguard_port=16016
primary=1
[SQLGuard_1]
sqlguard_ip=10.5.39.190
sqlguard_port=16016
primary=2
[SQLGuard_2]
sqlguard_ip=10.5.39.191
sqlguard_port=16016
primary=3
```

Load balancing with redundancy

In this configuration, use participate_in_load_balancing=**2** to configure the S-TAP to send traffic to multiple collectors simultaneously. All collectors receive the same information. Each collector stores all or just a portion of the overall information collected. Use policy filters on each collector to determine what information to store there.

```
 [TAP]
participate_in_load_balancing=2
[SQLGuard_0]
sqlguard_ip=10.5.39.189
sqlguard_port=16016
primary=1
[SQLGuard_1]
sqlguard_ip=10.5.39.190
sqlguard_port=16016
primary=2
[SQLGuard_2]
sqlguard_ip=10.5.39.191
sqlguard_port=16016
primary=3
```

Setting up S-TAP encryption

As described in the redbook *Deployment Guide for InfoSphere Guardium*, S-TAP traffic to the Guardium appliance can be encrypted by setting the guard_tap.ini parameter use_tls=1.

Important: Encryption uses port 16018 for its communication. Make sure that port is available for use.

The higher the volume of traffic being monitored by S-TAP, the higher the processing power required to encrypt the data. Generally speaking, it only makes sense to encrypt S-TAP traffic if the data is being sent to an appliance on a different network, or if the database traffic being monitored is itself network encrypted.

The relevant S-TAP parameters are:

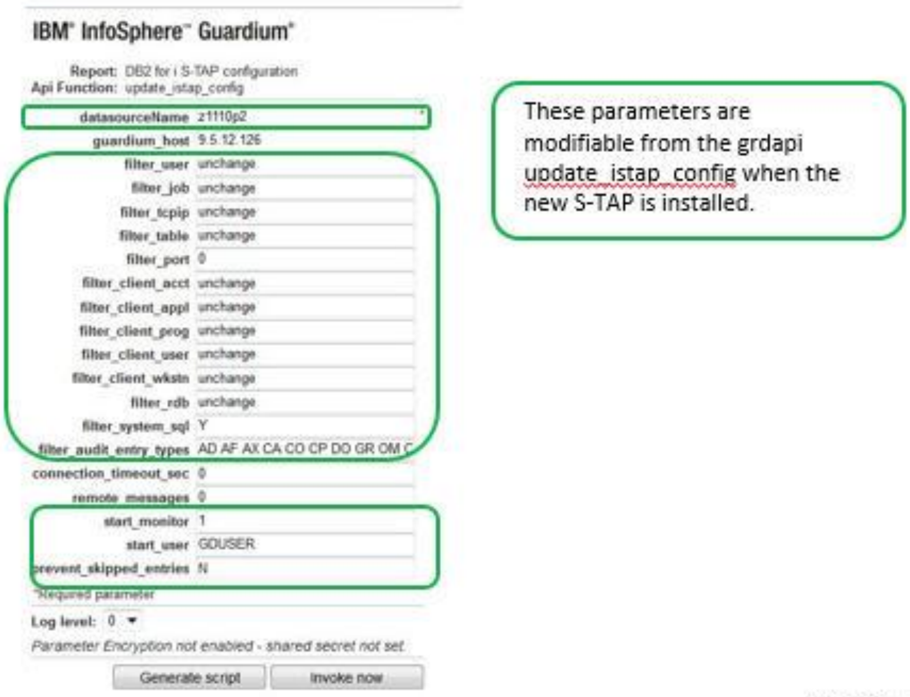
```
[TAP]
…
use_tls=1
failover_tls=1
; Where is the CA certificate
guardium_ca_path=[path to CA.pem]
; What's the CN to expect from the SqlGuard certificate?
sqlguard_cert_cn=[the full CN or partial CN (using * as a wildcard) of
the Guardium appliance]
; Path to crls file or dir
guardium_crl_path=NULL
```

The process to set up S-TAP encryption is the same as for other S-TAPs.

See http://www-01.ibm.com/support/knowledgecenter/SSMPHH_10.0.0/com.ibm.guardium.doc.stap/stap/how_to_setup_stap_authentication_with_ssl_certificates.html

Appendix A. When to use the i-specific stap configuration API (update_istap_config)

As a reminder, to be able to control filtering from the Guardium appliance, part of the i s-tap configuration still requires the creation and upload of configuration table as a custom table.



IBM® InfoSphere™ Guardium®

Report: DB2 for i S-TAP configuration
Api Function: update_istap_config

datasourceName	z1110p2 *
guardium_host	9.5.12.126
filter_user	unchange
filter_job	unchange
filter_tcpip	unchange
filter_table	unchange
filter_port	0
filter_client_acct	unchange
filter_client_appl	unchange
filter_client_prog	unchange
filter_client_user	unchange
filter_client_wkstn	unchange
filter_rdb	unchange
filter_system_sql	Y
filter_audit_entry_types	AD AF AX CA CO CP DO GR OM C
connection_timeout_sec	0
remote_messages	0
start_monitor	1
start_user	GDUSER
prevent_skipped_entries	N

*Required parameter

Log level: 0 ▾

Parameter Encryption not enabled - shared secret not set

These parameters are modifiable from the grdapi update_istap_config when the new S-TAP is installed.

© 2015 IBM Corporation

Continue to use the API update_istap_config API in the following circumstances:

- If you are connecting from a V10 collector to a 9.5 S-TAP. The behavior is the same as if you were connecting from a V9.5 collector to a V9.5 S-TAP.
- To update server-side filtering parameters from the Guardium UI.
- To restart the S-TAP using the start_monitor parameter.
- To update the prevent_skipped_entries parameter. (This parameter is described in the Guardium Activity Monitor and DB2 for i serviceability guide available on developerWorks at
    - https://ibm.biz/GuardiumOniServiceabilityGuide