

# Guardium architecture and deployment

MASTER CLASS  
PRODUCT PROFESSIONAL SERVICES  
YOSEF ROZENBLIT





# Agenda

- Guardium architecture
- Supported databases and operating systems
- Sizing
- Guardium appliance
- Guardium agents
- Enterprise load balancer
- Traffic interception methods
- S-TAP enhancements
- Disaster recovery and high availability
- Database responses
- Automation

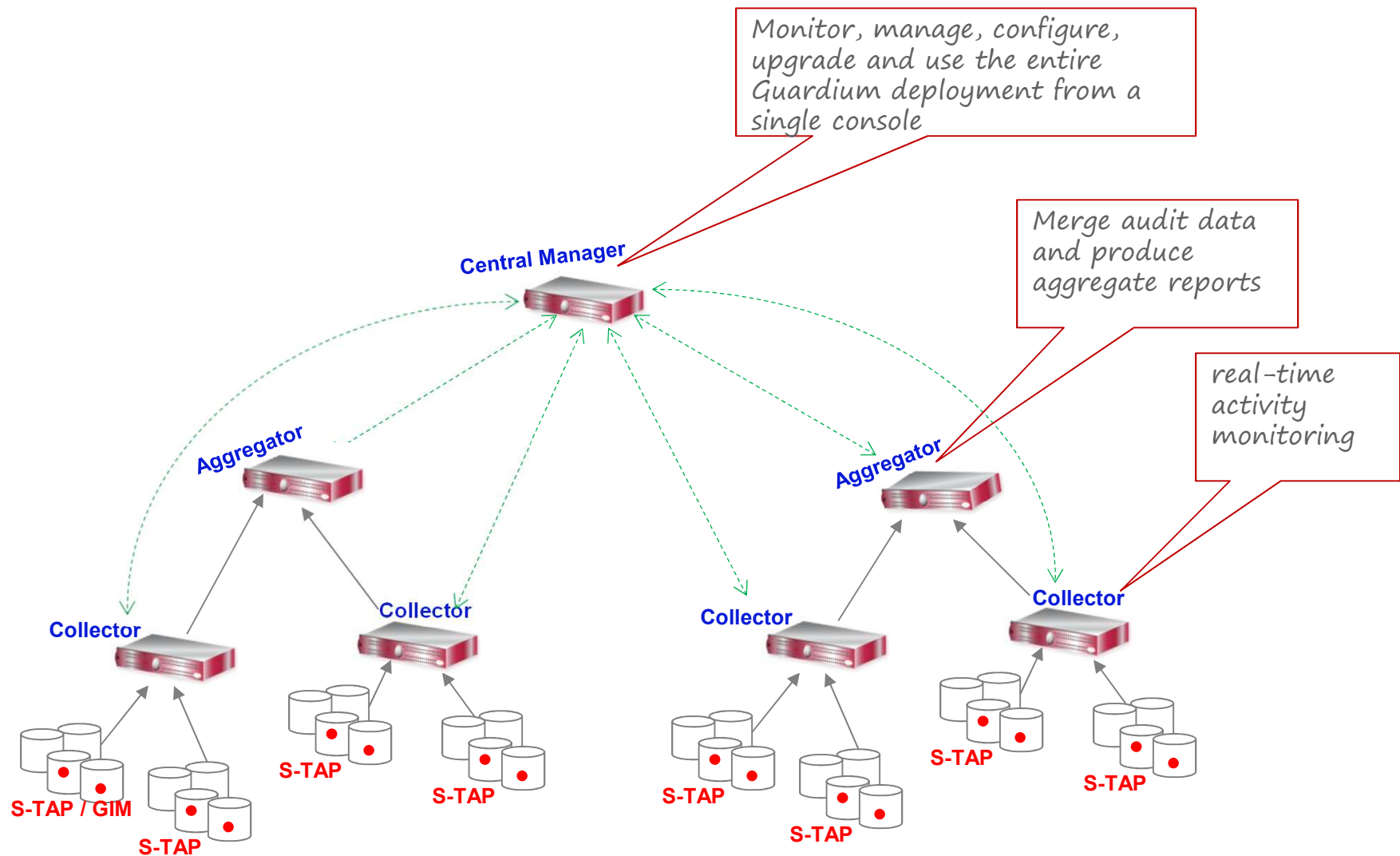


# Guardium architecture



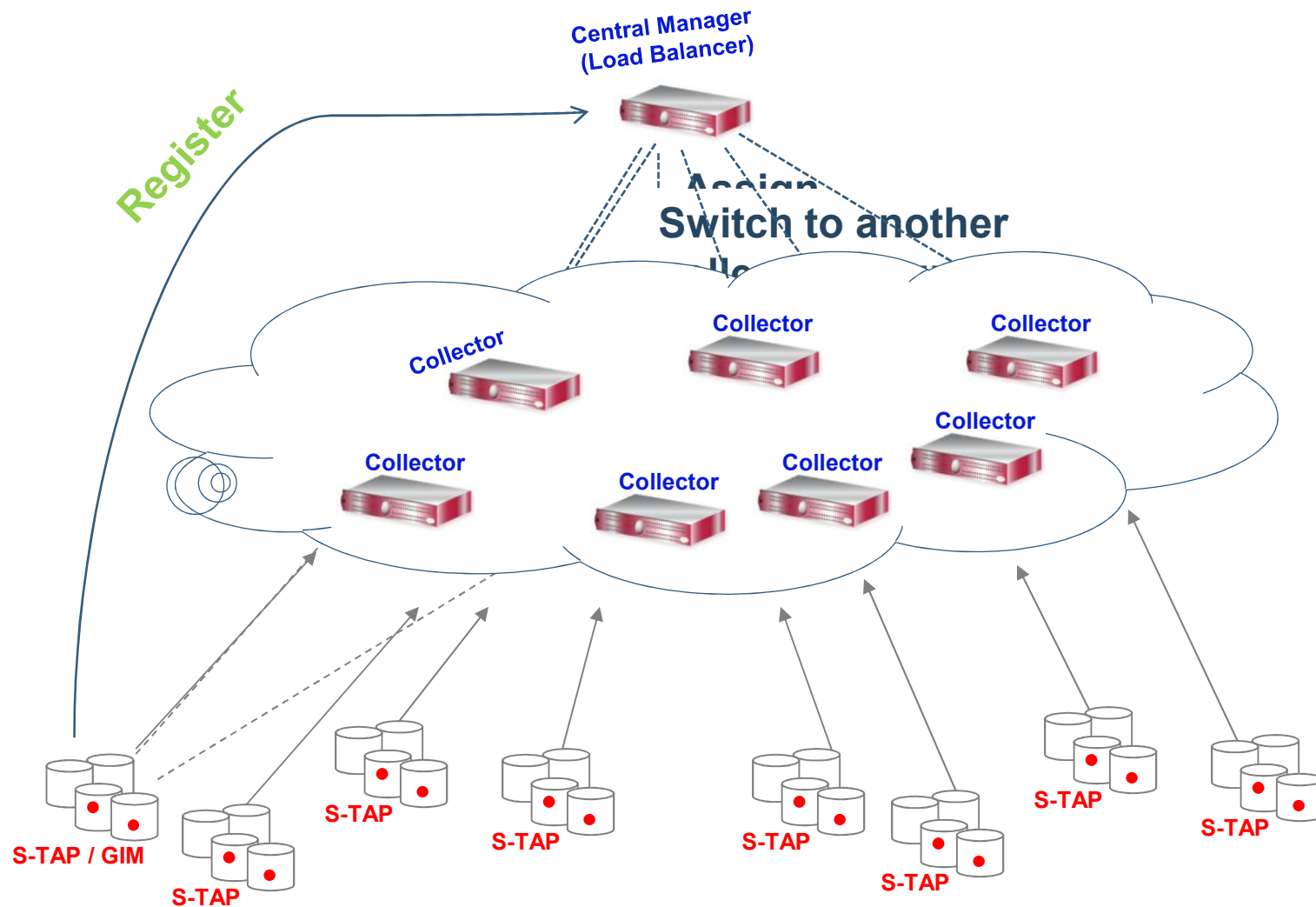
# Guardium Architecture

v9



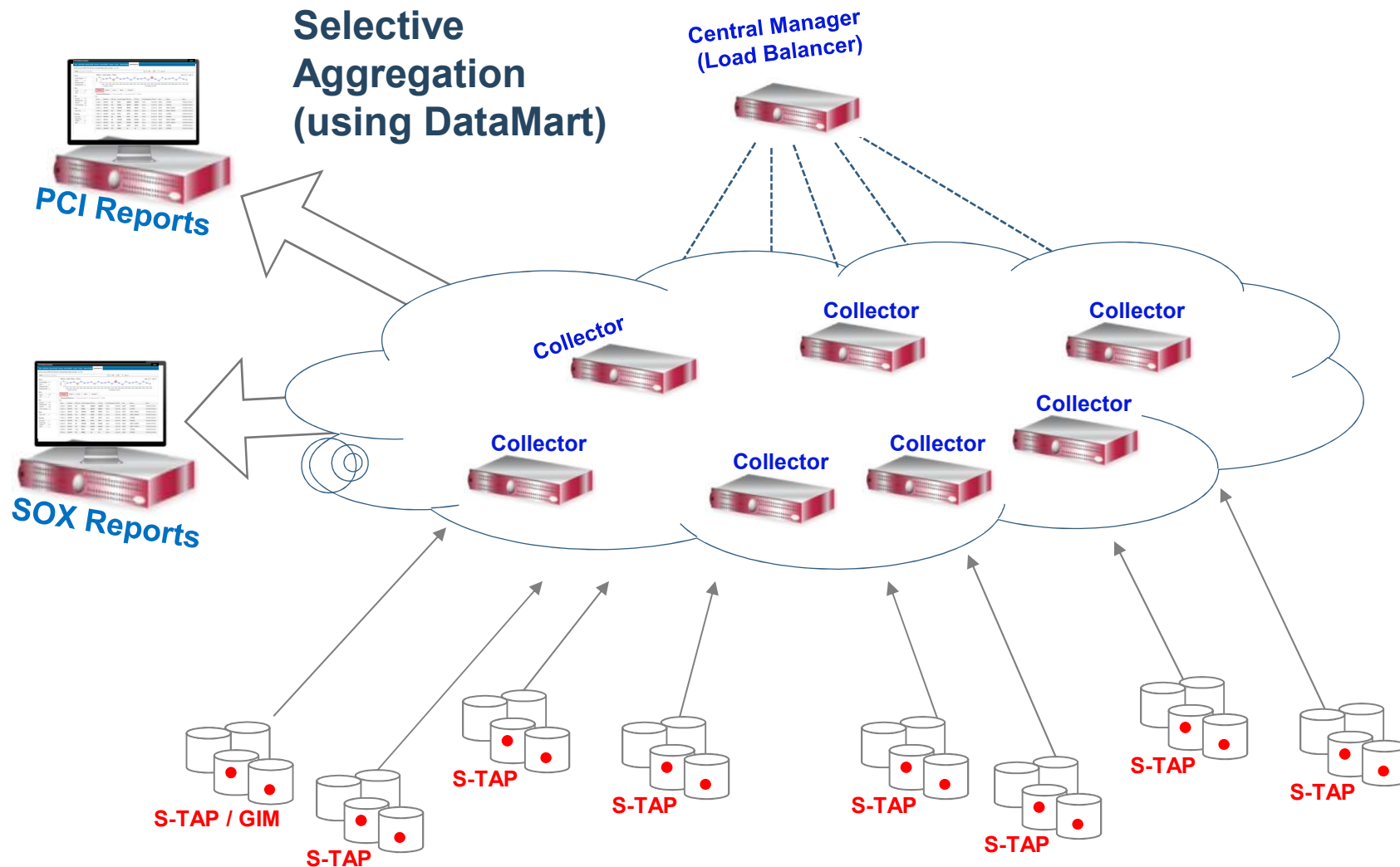
# Guardium Architecture

## v10 - ELB



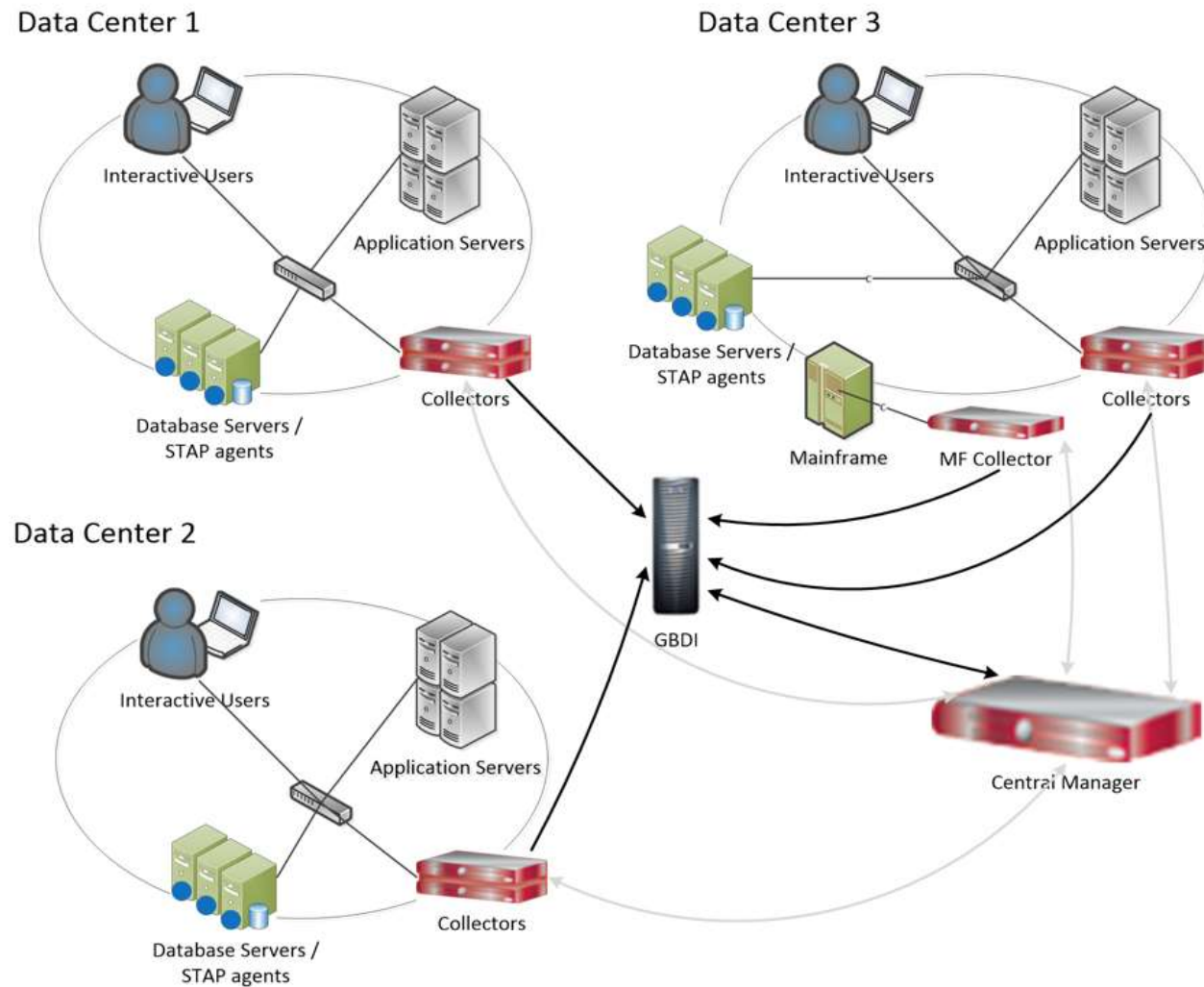
# Guardium Architecture


## v10 – Selective aggregation / datamarts



# Guardium Architecture

## v10 – GBDI





# Supported databases and operating systems







# Product coverage

- System Requirements/ Platforms Supported for v9.5  
<http://www-01.ibm.com/support/docview.wss?uid=swg27045286>
- System Requirements/ Platforms Supported for v10.0  
<http://www-01.ibm.com/support/docview.wss?uid=swg27045976>
- System Requirements/ Platforms Supported for v10.1  
<http://www-01.ibm.com/support/docview.wss?uid=swg27047802>
- System Requirements/ Platforms Supported for v10.5  
<http://www-01.ibm.com/support/docview.wss?uid=swg27047801>
- System Requirements/ Platforms Supported for v10.6  
<https://www-01.ibm.com/support/docview.wss?uid=ibm10719695>



## Product coverage

- v9.5

Data source	Supported Versions
Oracle (including ASO/SSL)	9i, 10g (r1, r2), 11gR1, 11gR2, 12c (12c Restrictions: Monitoring support for

- v10.5

Data source	Supported Versions
Oracle (including ASO/SSL)	11gR1, 11gR2, 12.1, 12.2

# Sizing



## Sizing

- Rule 1 – count small server as 600 units, medium server as 1600 units; large – as 3000 units. Divide total number of units by ratio in the table below to calculate number of standard hardware collectors.

Source Type	Platform	Standard	Comprehensive
Databases	Distributed (LUW)	20,000	8,000
	Express DP for Databases (LUW)	20,000	8,000
	Z/Linux	20,000	8,000
	Z/OS	300	150
Data	Distributed (LUW)	24,000	10,000
Warehouses	Z/Linux	24,000	10,000
BigData (semi-structured)	Distributed (LUW)	24,000	10,000
	Z/Linux	24,000	10,000
Files	Distributed (LUW)	24,000	10,000
(unstructured)	Z/Linux	24,000	10,000

- Rule 2 – prorate based on appliance type:

1.3 – VM

1 – standard HW 2264

0.85 – large HW 3164



## Sizing

- Rule 3 – prorate based on size of environment:
  - 1st collector – 100%
  - 2-3rd collectors -150%
  - 4-15<sup>th</sup> collectors – 100%
  - 16<sup>th</sup>+ collectors – 80%
- Rule 4 – calculate number of aggregators as :
  - 1 collector → 0 aggregator
  - 2-8 collectors → 1 aggregator
  - 9+ collectors → Divide number of collectors by 8, round up, and add 1 extra as CM
  - If GBDI is used → 2 aggregators.
- For VA – 1 aggregator per 750 databases.
- Add redundancy considerations: backup CM, failover collectors.
- Add sandbox/lab environment.



# Guardium appliance



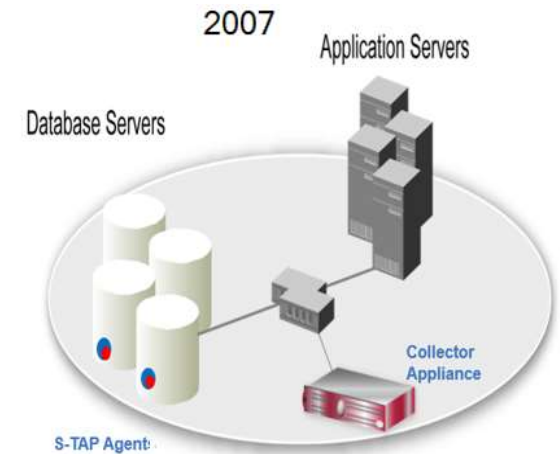
## Guardium appliance

- Guardium can be deployed on hardware or VM appliance

<https://www-01.ibm.com/support/docview.wss?uid=ibm10719695>

Resource	Required Range *	Comments
Physical CPUs	Minimum: 4 cores Recommended: 8 cores	x86 (Intel or AMD) processors required
Virtual CPUs	Minimum: 4 vCPUs Recommended: 8 vCPUs	
RAM	(64-bit) Minimum: 24 GB (min) Maximum: motherboard max Recommended: 32 GB	Guardium's features are memory intensive. To take full advantage of these features, it is recommended to have at 32 GB of RAM and 8-core CPU. For Central Managers in a large federated environment, the recommended memory is 64 GB.  If using Ecosystem, 34 GB is required.
Disk Speed	7200 RPM to 15,000 RPM	To use 7200 RPM, scale back the sizing ratio by 70%. Example: If you are using 7200 RPM disk, which is slow, you should reduce your sizing by 70%. If your sizing calls for 10 S-TAPs to a collector, if you are running with 7200 RPM drives, drop that to 3 S-TAPs to a collector.

- New IBM shipped appliances (as of Q4 2016)



# Guardium appliance

## CPU

- CPU – recommendation is 8 vCPU for VM appliance.
- CPU clock is important – faster is usually better.

```
processor : 39
vendor_id : GenuineIntel
cpu family : 6
model : 63
model name : Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz
stepping : 2
microcode : 53
cpu MHz : 2596.824
cache size : 25600 KB
```

```
processor : 31
vendor_id : GenuineIntel
cpu family : 6
model : 62
model name : Intel(R) Xeon(R) CPU E5-2667 v2 @ 3.30GHz
stepping : 4
microcode : 1064
cpu MHz : 3300.042
cache size : 25600 KB
```

```
processor : 3
vendor_id : GenuineIntel
cpu family : 6
model : 26
model name : Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz
stepping : 4
microcode : 1803
cpu MHz : 2000.000
cache size : 15360 KB
```



# Guardium appliance

## Memory

- Memory – recommendation is 32 GB for VM appliance. More memory on CM in large federated environment, if possible.

```
Cpu(s): 13.1%us,  2.5%sy,  0.0%ni, 84.4%id,  0.0%wa,  0.0%hi,  0.0%
si,  0.0%st
Mem: 65843268k total, 63234836k used,  2608432k free,  387844k
buffers
Swap: 32997372k total,          0k used, 32997372k free, 21497548k
cached
```



## Guardium appliance

### Disk

- 300 - 600 GB for VM collector (135 GB minimum for GBDI deployments).
- 600 - 1,800 GB for VM aggregator.
- Recommendation above is generic recommendation. It can be impacted, if customer has specific requirements on data retention and dependent on volume of logging.



# Guardium agents





## Guardium agents

- Guardium Installation Manager (GIM)
  - Install and upgrade agents and update their configuration

Note: available just in distributed environments
- Software Tap (S-TAP)
  - Monitors database traffic
  - Discovers new databases and configuration changes (v10)
- Instance discovery agent (v9.5, deprecated in v10)
  - Discovers new databases and configuration changes (v10)

Note: available just in distributed environments
- Configuration Audit System (CAS)
  - Track and alert on changes at the OS level (files, permissions etc..)

Note: available just in distributed environments



## Guardium Installation Manager (GIM)

- GIM allows you to centrally manage Guardium agents, easily scale your Guardium deployment without depending on other stakeholders and groups in your IT.
  - Maintain Guardium agents (S-TAP, CAS, Instance Discovery) on [database] servers.
  - Installs/Uninstalls Guardium software.
  - Apply software upgrades to the Guardium agents.
  - Updates agents configuration parameters.
  - Monitors Guardium processes on [database] servers.
- GIM can be installed as part of the server SW stack and run in listener-only mode.
- Recommendation is to point GIM clients to the Central Manager (up to ~2500-3000 clients)
- Make sure to configure secondary GIM server (GIM Failover URL parameter). It can point to secondary CM if available in the environment.

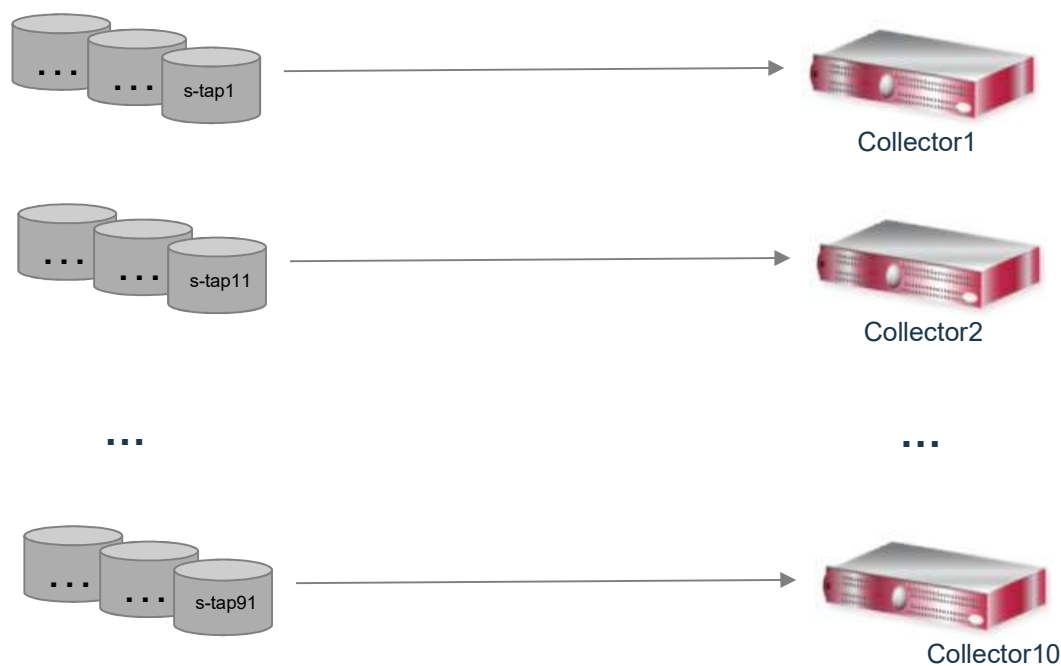
# S-TAP deployment options

## Basic

`participate_in_load_balancing = 0`

`all_can_control = 0`

One SQLGUARD section in S-TAP configuration file



### Used when...

- Usually used when redundancy is not required
- Recommendation is to use Failover instead

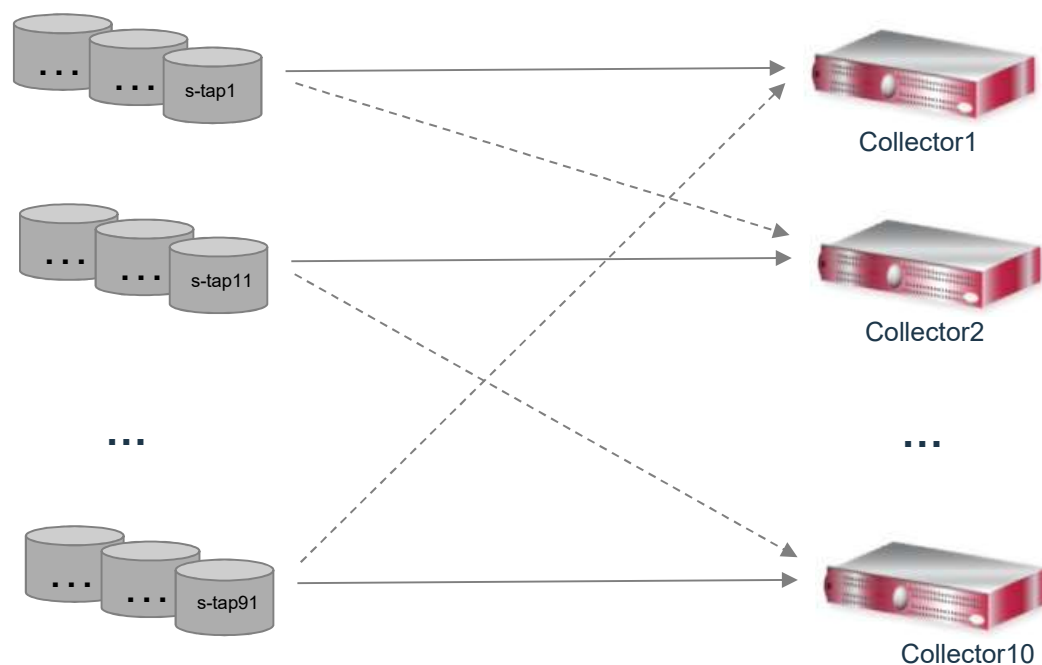
# S-TAP deployment options

## Failover

`participate_in_load_balancing = 0`

`all_can_control = 1` (optional)

Multiple SQLGUARD sections in S-TAP configuration file



### Used when...

- Currently most commonly used method in all Guardium versions
- Used when redundancy is required

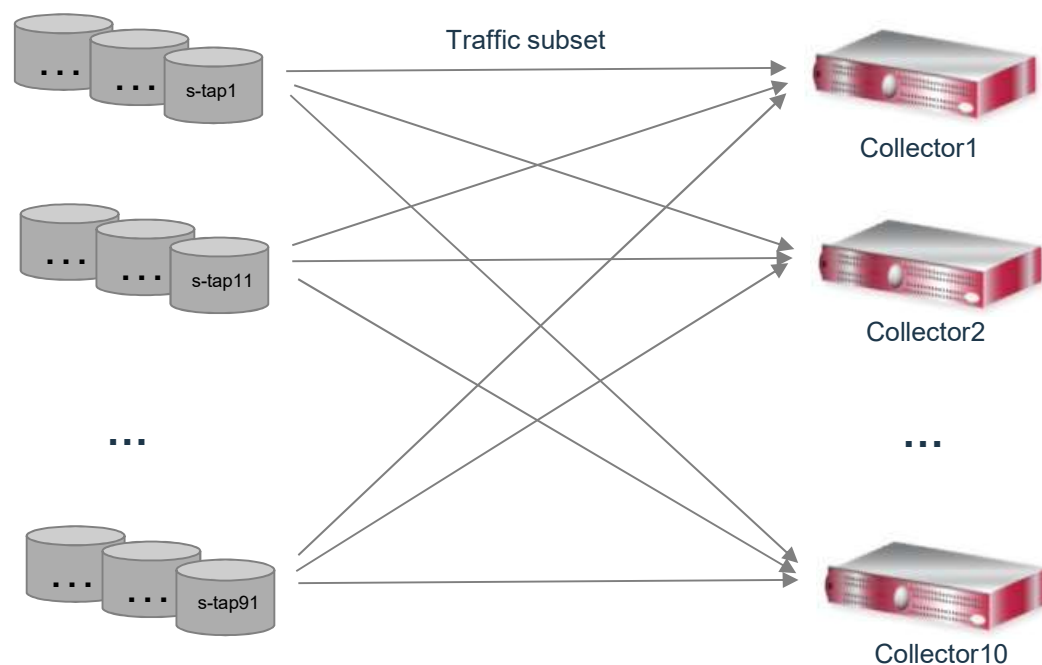
# S-TAP deployment options

## Load Balancing

`participate_in_load_balancing = 1`

`all_can_contol = 1` (optional)

Multiple SQLGUARD sections in S-TAP configuration file



### Used when...

- Used when one S-TAP generates too much traffic for one collector to handle
- Splits traffic to multiple collectors based on client port of the session



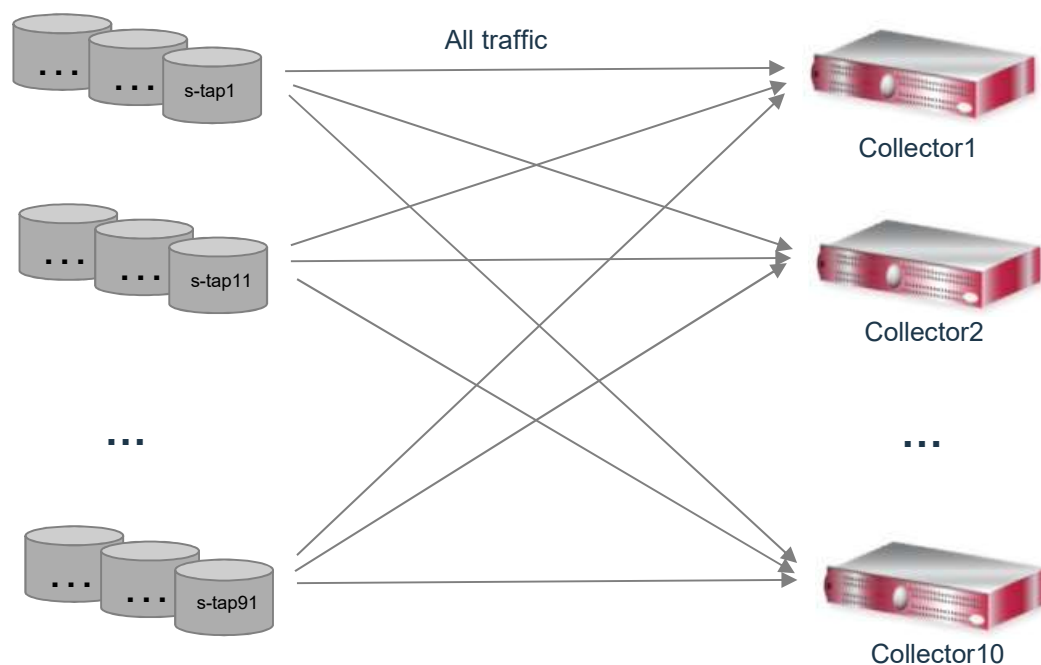
# S-TAP deployment options

## Mirroring

participate\_in\_load\_balancing = 2

all\_can\_contol = 1 (optional)

Multiple SQLGUARD sections in S-TAP configuration file



### Used when...

- Traffic is mirrored to multiple collectors
- Rarely used – when full redundancy is a requirement
- Testing purposes

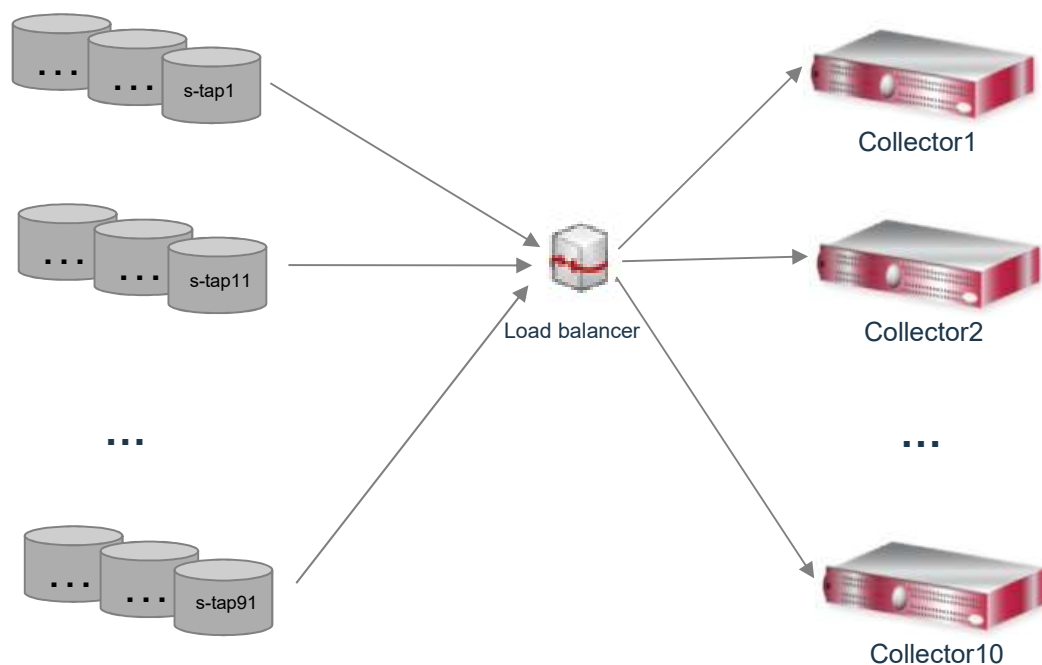
# S-TAP deployment options

## Grid / Hardware load balancer

`participate_in_load_balancing = 3`

`all_can_control = 1`

One SQLGUARD section in S-TAP configuration file (with IP of load balancer)



### Used when...

- Used to ease the deployment : same IP is used for installation; pool of collectors is maintained to manage capacity.
- Released in v8.

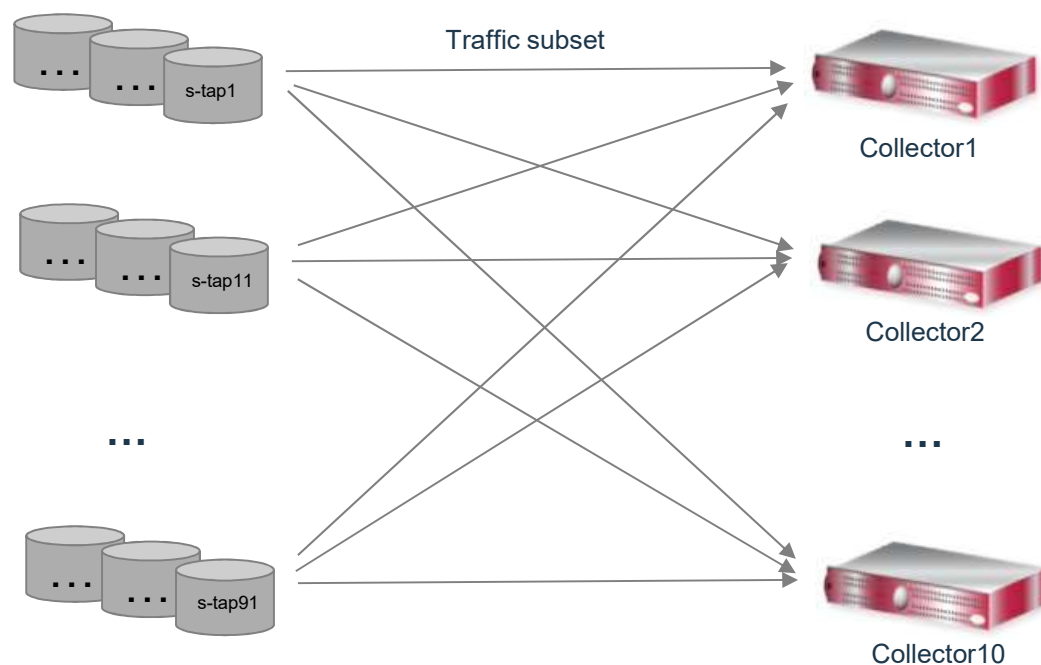
# S-TAP deployment options

## S-TAP multi-threading

participate\_in\_load\_balancing = 4

all\_can\_contol = 1 (optional)

Multiple SQLGUARD sections in S-TAP configuration file (up to 10 in 10.1.4). Number of threads as number of sections. Same collector IP can be in multiple sections



### Used when ...

- Used when S-TAP can't keep up with traffic volume
- Allows S-TAP to run multiple threads instead of single threaded process.
- Ability for each thread to send traffic to different collector.
- Released in v10.

Note: S-TAP buffer is being allocated for each thread; however up to 5 K-TAP buffers allocated for all S-TAP threads.

# S-TAP deployment options

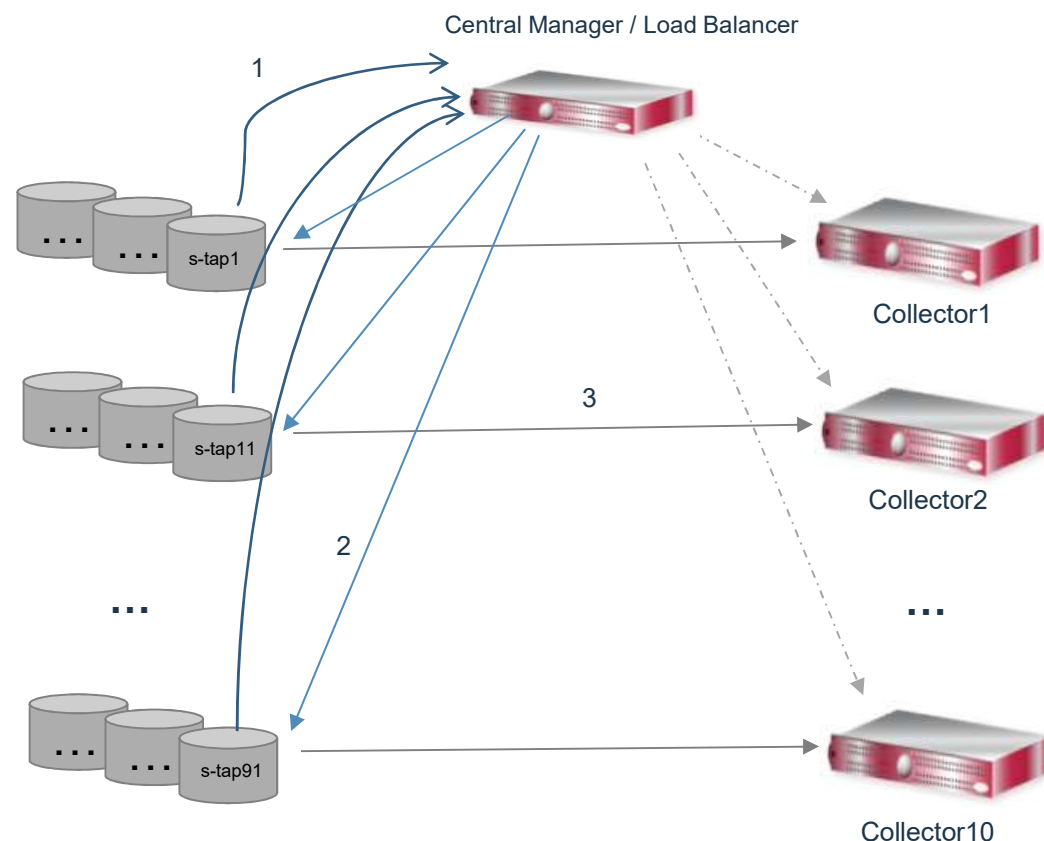
## Enterprise load balancer

load\_balancer\_ip = <central manager IP>

load\_balancer\_enabled = 1 (on all managed units, that participate in load balancing)

participate\_in\_load\_balancing = 0/1/2/4

load\_balancer\_num\_mus = 1 or >1



### Used when ...

Streamline agents' deployment and optimize appliance utilization

- At deployment

All S-TAP agents point to the Central Manager at deployment.

- ✓ Standard (same) configuration for all agents.
- ✓ Streamline S-TAP installation.
- ✓ Automate STAP-to-collector allocation.

- Ongoing

- ✓ Load-balance based on collectors' utilization.
- ✓ Automatic STAP-collector re-allocation.
- ✓ Built-in failover capability.

- Released in v10



# Enterprise Load Balancer

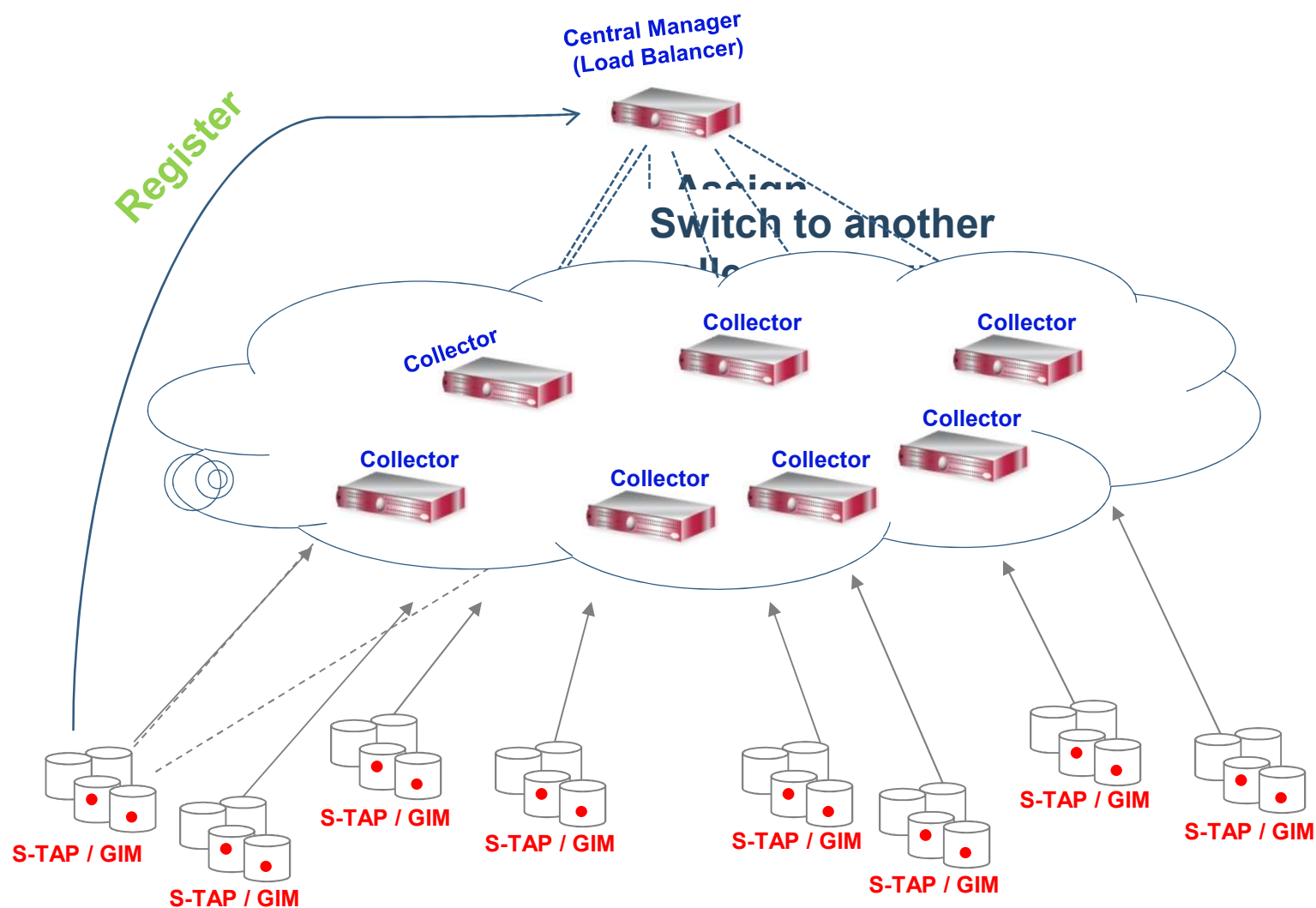




## Enterprise Load Balancer

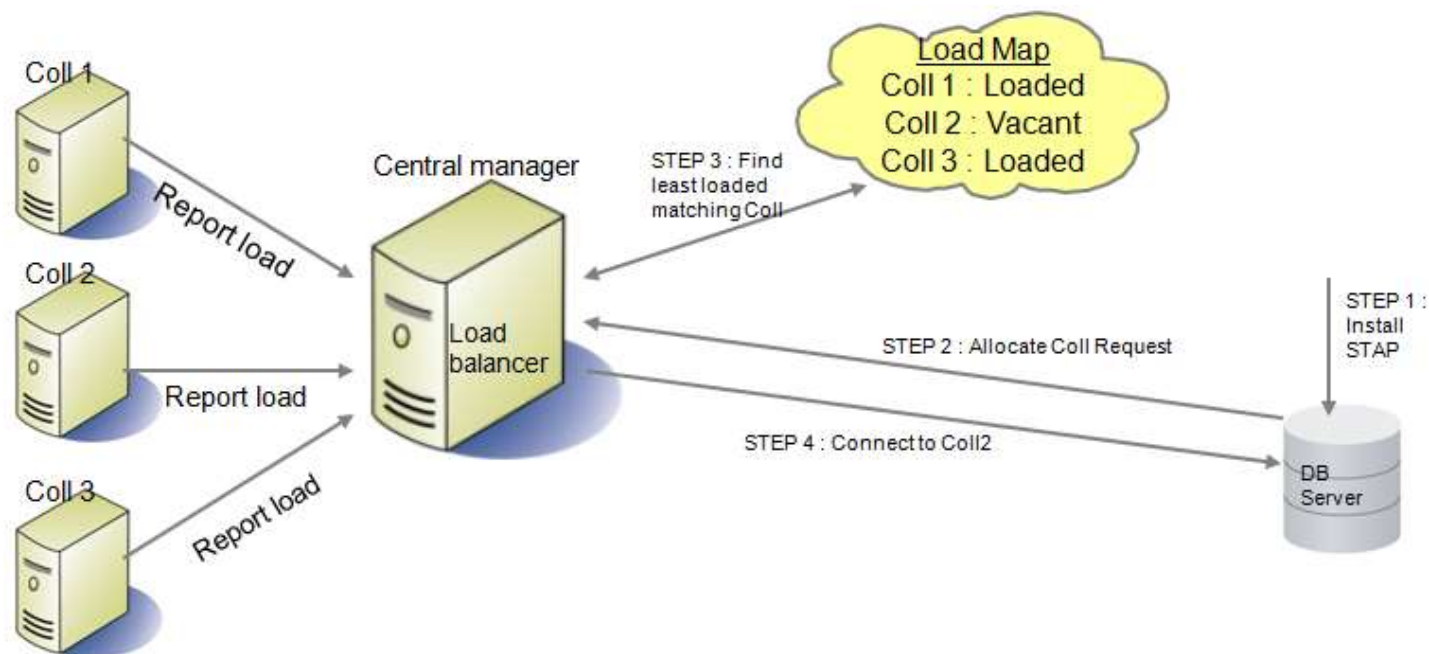
- ELB was introduced in v9.5. Initial S-TAP assignment only. No load balancing of STAPs across collectors after initial assignment.
- Load balancing functionality was introduced in v10.0. Additional enhancements are in v10.1, 10.5, 10.6. Ability to configure failover groups is introduced in 10.1.3.
- ELB is supported for distributed platforms : Windows and Unix S-TAPs. ELB is not supported for Mainframe and I-Series S-TAPs.
- ELB is software feature, that is running on Central Manager. No additional / separate license is required.

# Enterprise Load Balancer



# Enterprise Load Balancer

- ELB is running on the central manager. Managed units can be used as a proxy starting in 10.1. Port 8443 is being user for S-TAP to communicate to ELB (HTTPS request).
- ELB tracks capacity and utilization of all collectors.
- Assigns S-TAP to the most appropriate collector (based on grouping and utilization).





# Enterprise Load Balancer

- What is being collected to build load map?
  - Collectors' hardware profile.
  - Collectors' configuration parameters which impact performance.
  - Collectors' installed policy.
  - Per S-TAP load contribution metrics.
- Mapping of S-TAP to pool of collectors using group(s) of S-TAPs to group(s) of collectors mapping.
  - Geographical location (co-locate S-TAP and collector)
  - Functional considerations: monitoring requirements / policy; version / patch level
  - Audit data location considerations: group of collectors based on target aggregator
  - DB platform considerations: MSSQL DBs and DB2 DBs are mapped to different collectors
  - Other deployment considerations

# Enterprise Load Balancer

- Ability to associate group(s) of S-TAPs to group(s) of collectors.

The diagram illustrates the process of creating and associating S-TAP groups with Managed Unit Groups in the IBM InfoSphere Guardium console. It consists of three sequential screenshots connected by blue curved arrows.

**Top Screenshot:** The 'Associate S-TAPs and Managed Units' page. The 'S-TAP Group Name' dropdown shows 'RangeOfStaps' selected. The 'Managed Unit Groups' section shows 'gd01'. A callout box points to the 'Create S-TAP Group' button, stating: 'All groups of type 'STAP' are displayed'.

**Middle Screenshot:** The 'Create New S-TAP Group' dialog. The 'Group Name' field contains 'Test0'. The 'Group Member' field contains '192.168.1.1'. A list of hosts is shown below, with '192.168.1.1' selected. A callout box points to the 'Create New Group' button, stating: 'Create a new S-TAP group with at least one member'.

**Bottom Screenshot:** The 'Associate S-TAPs and Managed Units' page again. The 'S-TAP Group Name' dropdown now shows 'Test0' selected. The 'Managed Unit Groups' section shows 'gd01'. A callout box points to the 'Associate Managed Units' button, stating: 'Associate MU group to the STAP group'.

A callout box on the left side of the middle screenshot points to the 'Manage' menu item in the sidebar, stating: 'S-TAPs currently connected'.



## Enterprise Load Balancer

- GIM install:

STAP\_LOAD\_BALANCER\_IP - The IP of the load balancer this S-TAP should use (mandatory)

STAP\_INITIAL\_BALANCER\_TAP\_GROUP - The group this S-TAP belongs to (optional)

STAP\_INITIAL\_BALANCER\_MU\_GROUP - The managed unit group this S-TAP belongs to. S-TAP group must also be specified to use this option (optional)

STAP\_LOAD\_BALANCER\_NUM\_MUS - Number of managed units the load balancer should allocate for this S-TAP.

- Shell install:

[--load-balancer-ip <load\_balancer\_ip>] - The IP of the load balancer this S-TAP should use (mandatory)

[--lb-app-group <app\_group>] - The group this S-TAP belongs to (optional)

[--lb-mu-group <mu\_group>] - The managed unit group this S-TAP belongs to. S-TAP group must also be specified to use this option (optional)

[--lb-num-mus <number\_of\_mus>] - Number of managed units the load balancer should allocate for this S-TAP.



## Enterprise Load Balancer

- `LOAD_BALANCER_ENABLED` - Indicates, if appliance is part of load balancing. Values 1 - enable (default); 0 - disable;
- `ENABLE_RELOCATION` - Indicates, if load balancer will be moving S-TAPs from over-utilized collectors to under-utilized (perform actual load balancing). Values 1 - enable (default) ; 0 - disable;
- `ENABLE_DYNAMIC_LOAD_COLLECTION` - defines the load collection method. Values 1 - dynamic (default); 0 - static (parameter below defines interval);
- `STATIC_LOAD_COLLECTION_INTERVAL` - Collection interval in minutes. Values  $\geq 10$  with default of 720;
- `USE_APPLIANCE_HW_PROFILE_FACTOR` - Indicates, if load balancer accounts for appliance profile (value 1 - default) or not (0);
- `ALLOW_POLICY_MISMATCH_BETWEEN_APPLAINCES` - Indicates, if load balancer can move S-TAP between 2 appliances with different policies installed (by name). Values 1 - allowed (default); 0 - not allowed;
- `MAX_RELOCATIONS_BETWEEN_FULL_LOAD_COLLECTIONS` - Maximum number of S-TAPs moved across environment after full load collection; Values  $\geq -1$ . Default is 3; -1 is unlimited;
- `MAX_RELOCATIONS_PER_MUBETWEEN_FULL_LOAD_COLLECTIONS` - Maximum number of S-TAPs moved from specific collector after full load collection; Values  $\geq -1$ . Default is 3; -1 - unlimited



## Enterprise Load Balancer

- `grdapi get_load_balancer_params`
- `grdapi set_load_balancer_param paramName=<param name>  
paramValue=<param value> paramType=<param type>`
- `grdapi get_load_balancer_load_map`
- `grdapi assign_load_balancer_groups muGroupName=<MU group>  
appGroupName=<application group>`
- `grdapi unassign_load_balancer_groups muGroupName=<MU group>  
appGroupName=<application group>`












# Enterprise Load Balancer

## Transition to enterprise load balancer model

- Identify appliances that are part of ELB pool. Remove rest of the appliances from the pool (LOAD\_BALANCER\_ENABLED = 0).
- Open 8443 port from DB server to Central manager. Alternatively identify proxy load balancer appliances in remote data centers with 8443 opened from DB server to local managed unit.
- Create groups of collectors and groups of S-TAPs.
- Create mapping of S-TAP groups to groups (pool) of collectors.
- Review and update (if necessary) load balancer parameters.
- Phase in update of STAP\_LOAD\_BALANCER\_IP (and optionally STAP\_LOAD\_BALANCER\_NUM\_MUS) on selected STAPs (or groups of S-TAPs). Update PARTICIPATE\_IN\_LOAD\_BALANCING to 0, if you are currently using physical (F5 / Cisco) load balancer.
- Initially confirm S-TAP is properly reporting to identified collector(s).
- Monitor load balancer events report.

# Enterprise Load Balancer

- Load balancer events:

Enterprise Load Balancer Events		
Start Date: 2017-02-27 11:14:04   End Date: 2017-02-27 14:14:04 Using Merge Period Between 2016-12-29 and 2017-02-27.		
        		
Event ID	Event	Timestamp

- Load balancer map:

Load Balancer									
Start Date: 2017-02-27 11:17:58   End Date: 2017-02-27 14:17:58 Using Merge Period Between 2016-12-29 and 2017-02-27.									
        									
Managed Unit	Monitored App	Monitored App Load Level (%)	MU Loaded	Load Contributor App Type	Load Contributor App Name	Load Contributor App Max Load (MB)	Load Contributor App Avg Load (MB)	Load Contributor App Avg Load (%)	Last Collection Time



# Enterprise Load Balancer

10.5 and 10.6 enhancements

- Improvement in the process of S-TAP configuration removal from “original” collector.
- Sniffer availability verification prior to MU allocation.
- S-TAP relocation when number of managed units > 1.
- support store debug on ELB.

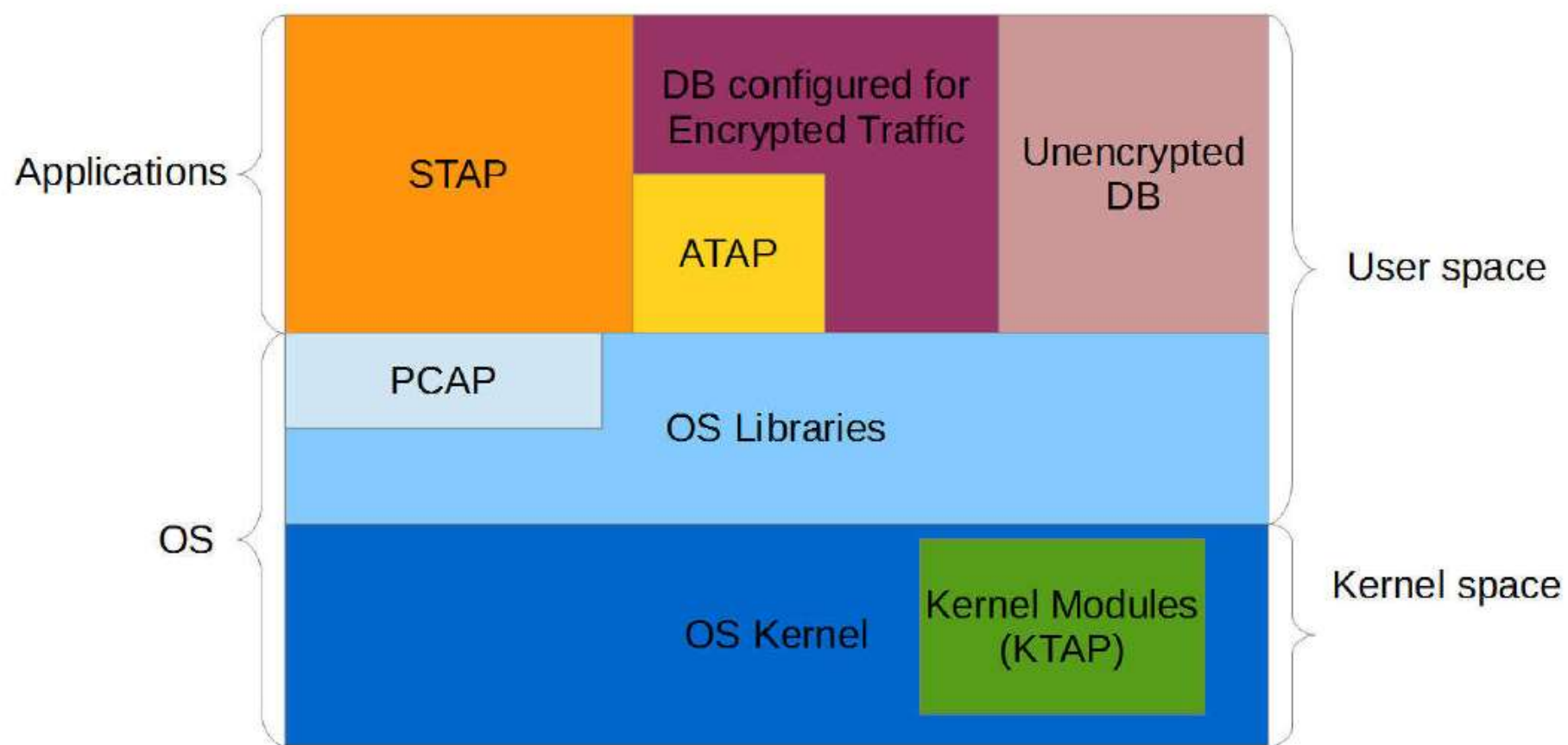




# Traffic interception methods



## Traffic interception





## A-TAP and EXIT

- Use of EXIT is generally recommended over A-TAP on the platforms where EXIT exists.
- In 10.6 EXIT exists for 3 databases : DB2, Informix, Teradata.
- EXIT doesn't require K-TAP while A-TAP does.



## A-TAP

- Maintenance general principles:
  - Database instance must be shutdown before activating or deactivating the A-TAP.
  - The inspection engine should be configured before activating the A-TAP.
  - A-TAP must be deactivated before:
    - Upgrading the database;
    - Upgrading/uninstalling S-TAP.
- High level activation steps:
  - Authorize the database instance owner (optional starting in v10.5)
  - Store required configuration parameters.
  - Activate the A-TAP.
  - Verify encrypted traffic is monitored.



## Exit

- Maintenance general principles:
  - Database instance must be shutdown before activating.
  - The EXIT inspection engine should be configured before activating the database EXIT.
  - Prior to 10.6 EXIT might need to be reactivated after:
    - Database upgrade (in case path where library is located was changed).
    - S-TAP upgrade (in case library was changed as part of the upgrade).
- High level activation steps prior to 10.6:
  - Add database instance group owner to Guardium group.
  - Copy appropriate library to defined location as DB instance owner.
  - Enable EXIT library while DB instance is down.
  - Verify traffic is monitored.

# Exit

## 10.6

- No change to installation (.sh, or gim, or rpm)
- New: Guardium shared memory library installed in system library location (e.g. /usr/lib)
- Exit libraries also installed in system library location
- When configuring an exit, you must link to the system library location
  - Do not copy the file
  - Do not link to the copy in the Guardium install directory
  - Link to the “.so” (which itself a link), not to anything else

```
[root@pantera ~]# ls -l /home/db2inst1/sqllib/security64/plugin/commexit/
total 0
lrwxrwxrwx 1 db2inst1 db2iadml 34 Nov  6 10:05 libguard_db2_exit_64.so -> /usr/lib64/libguard_db2_exit_64.so
[root@pantera ~]# ls -l /usr/lib64/libguard_db2_exit_64.so
lrwxrwxrwx 1 root root 32 Nov  5 19:04 /usr/lib64/libguard_db2_exit_64.so -> libguard_db2_exit_64.so.10.6.0.0
[root@pantera ~]# ls -l /usr/lib64/libguard_db2_exit_64.so.10.6.0.0
-r-xr-xr-x 1 root root 365729 Nov  5 19:04 /usr/lib64/libguard_db2_exit_64.so.10.6.0.0
[root@pantera ~]#
```



## Exit

- Exit live update was introduced in 10.6
- Databases using EXIT do not need to be stopped, they can continue running
  - Traffic will be captured during upgrade and sent to collector when upgrade is complete
  - If there is extremely heavy traffic, some transactions may be dropped
  - After upgrade, monitoring continues using the “old” plugin
  - The next time that database instance restarts it will use the “new” plugin
  - All new instances will use the “new” plugin
  - No time limit to restart – can be months later



# Agents Enhancements







## Agents Enhancements

- New windows driver is introduced (WFP) – **no DB restart is required**. Driver is default in v10 and in latest v9.5.
- S-TAP agent performs instance discovery for Unix and Windows platforms in v10. Enabled by default on both in latest v10.
- Windows S-TAP side encryption correlation in v10.1 (MSSQL only).
- Unix S-TAP can run multiple threads in v10. Additional UI enhancements are available in v10.1. Increased thread number in v10.1.3.
- S-TAP automatically tries to clean its configuration from collectors it is no longer configured to use. Available in v10.1.
- Identification of which Inspection Engine caused traffic to be collected is added and propagated to collector (IE Name / ID attributes in Session).
- Teradata EXIT. Available in 10.1.3.

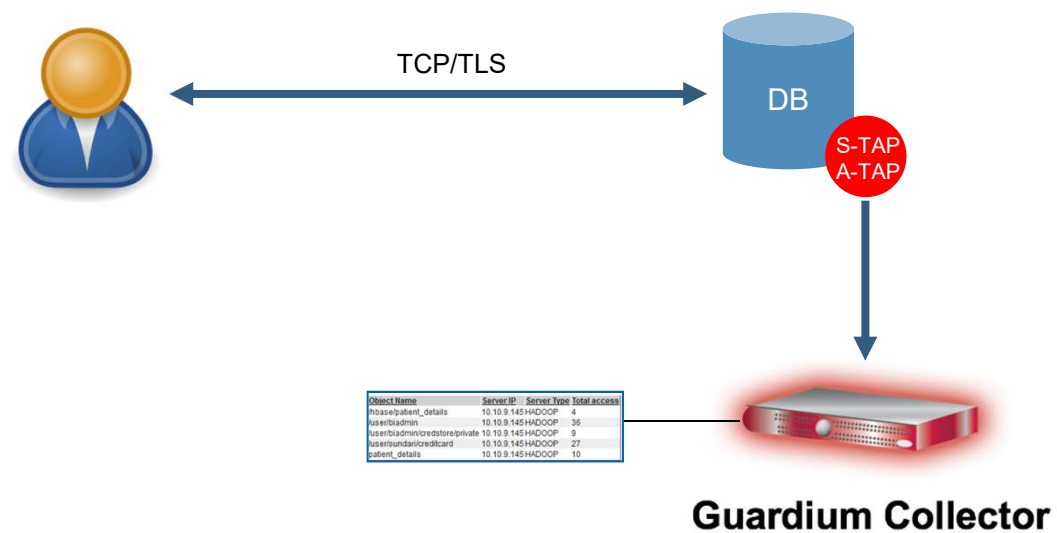


## Agents Enhancements

- GIM delayed bundle installation. Available in 10.5.
- A-TAP activation by non-root user. Available in 10.5 for non GIM installation. Available in 10.6 for GIM installation.
- New blocking mode for Unix environments (`firewall_default_state=2`) is introduced. Available in 10.5.
- S-TAP configuration mistakes are forgiving for Unix environments. Available in 10.5.
- Flexibility in Windows S-TAP buffer management with configurable additional dynamic allocation. Available in 10.5.
- Exit live update. Available in 10.6

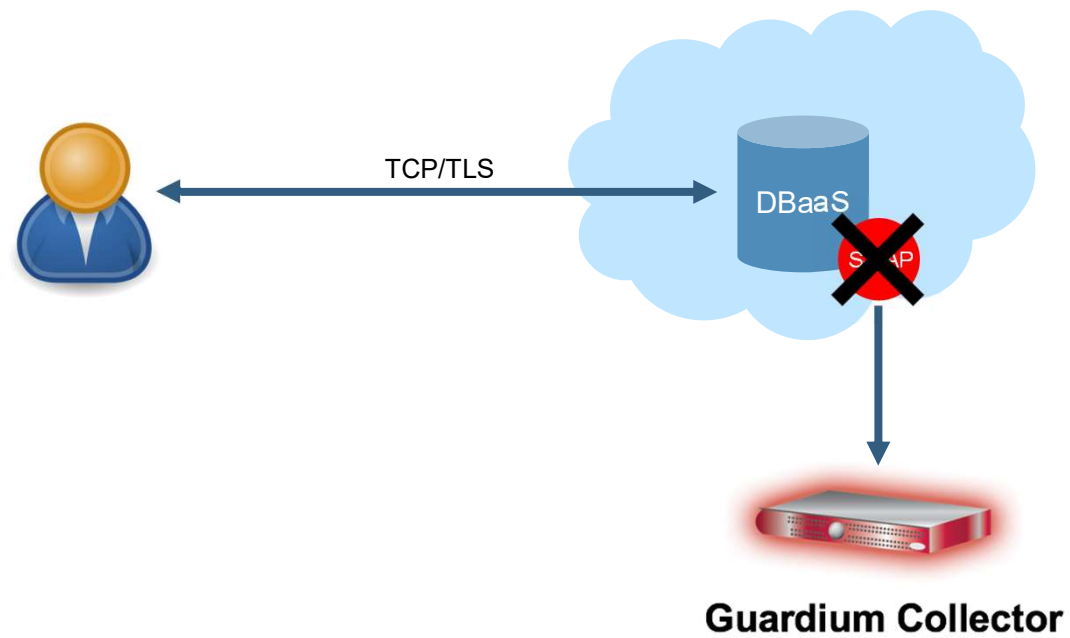
# External S-TAP

## Overview – on-prem



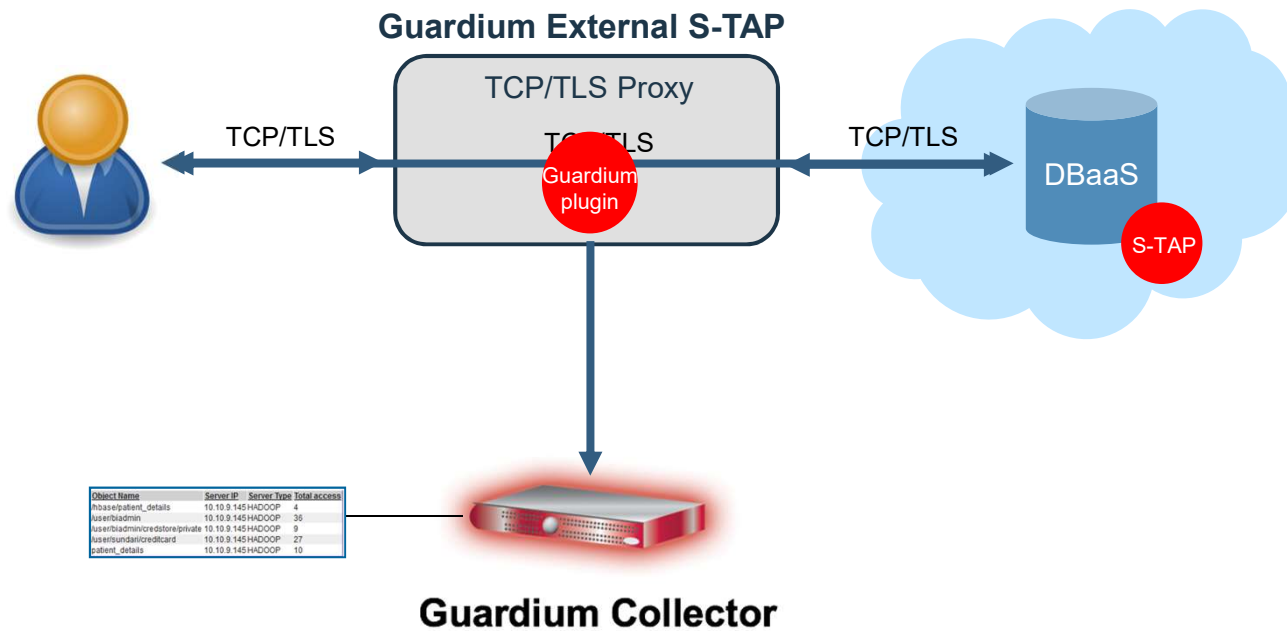
# External S-TAP

## Overview - cloud



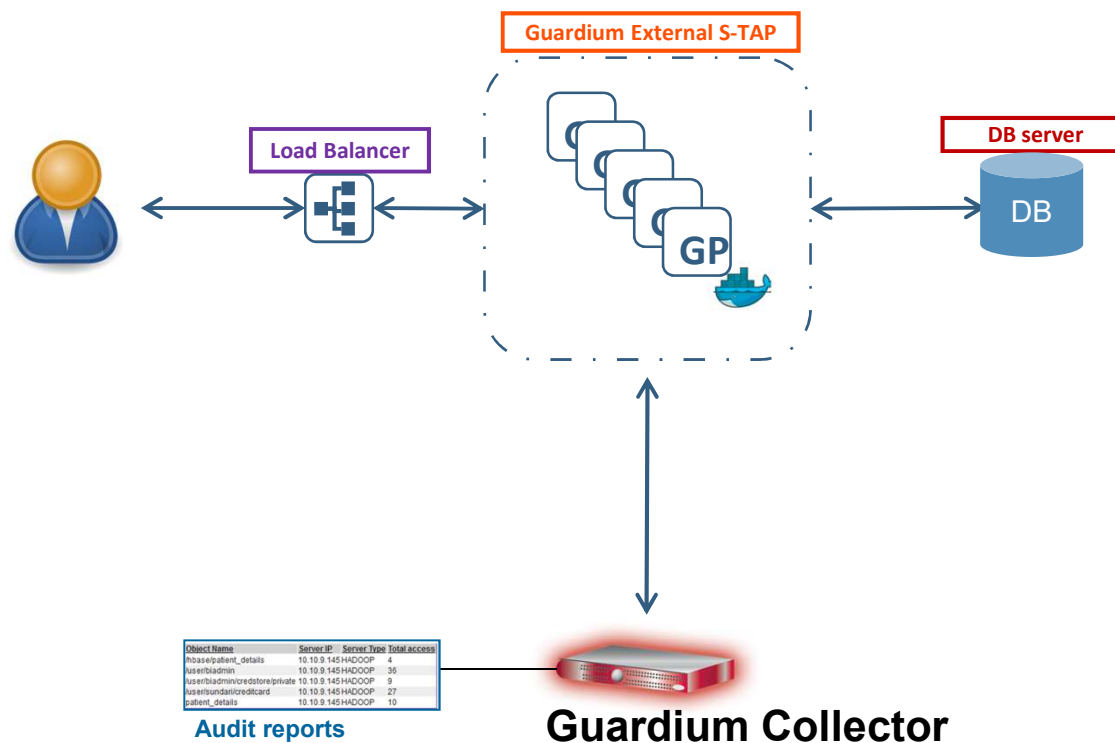
# External S-TAP

## Overview - cloud



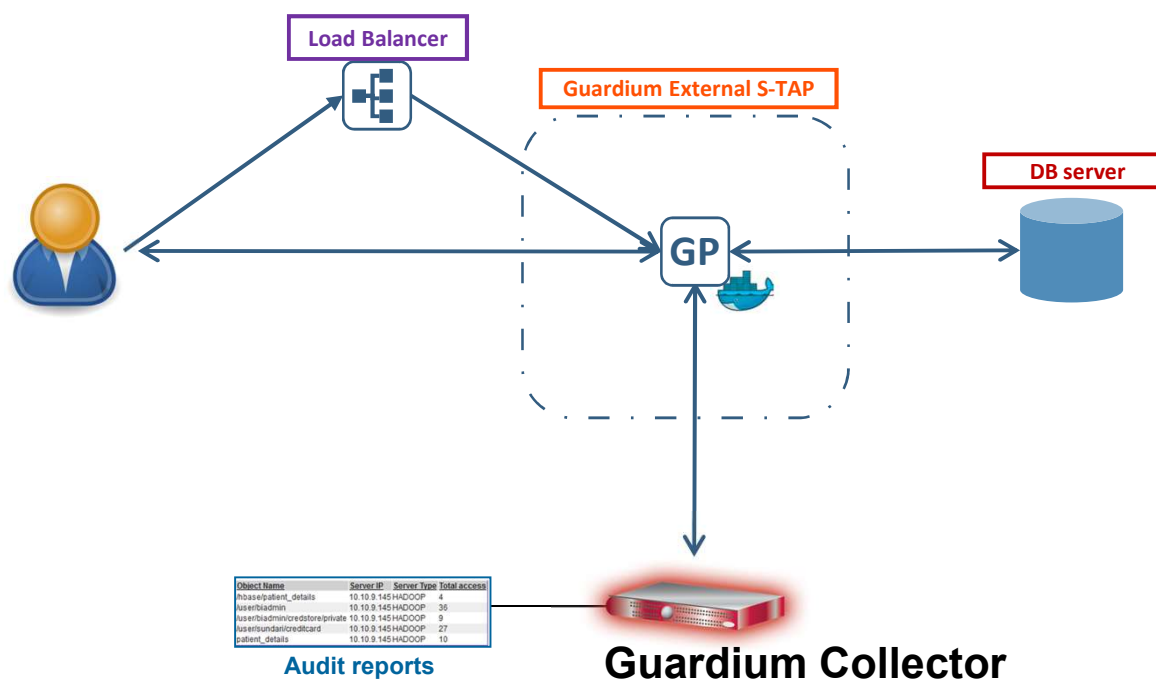
# External S-TAP

## Architecture



# External S-TAP

## Architecture





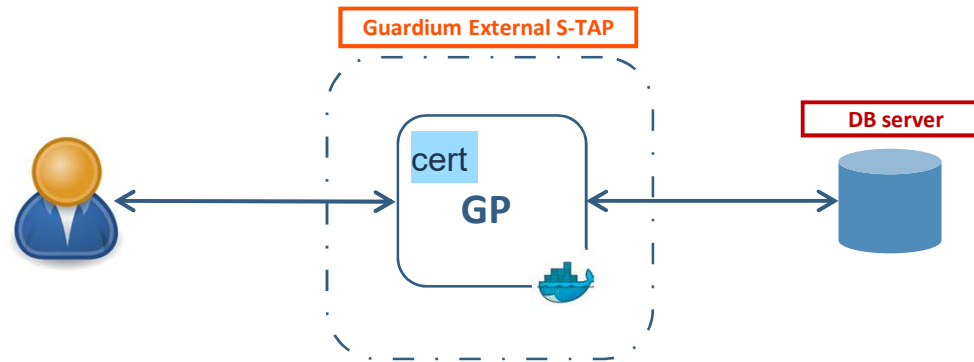
## External S-TAP Requirements

- Point DB clients to Load Balancer instead of DB server
- Install certificates (for TLS)



## External S-TAP

### TLS



To enable a TLS connection, a trusted certificate must be installed on each External S-TAP

New CLI (on CM)

- Creates CSR to be signed by a trusted CA
- Stores the signed certificate
- Distributes the certificate to appropriate External S-TAP instances



## External S-TAP

### Use cases

- Dbaas
  - Oracle on RDS, SQLServer on Azure
- Encrypted DBs traffic
- Containerized DBs on-prem and on the cloud
  - Q1'19
- More DBs in 2019



## External S-TAP

### Limitations

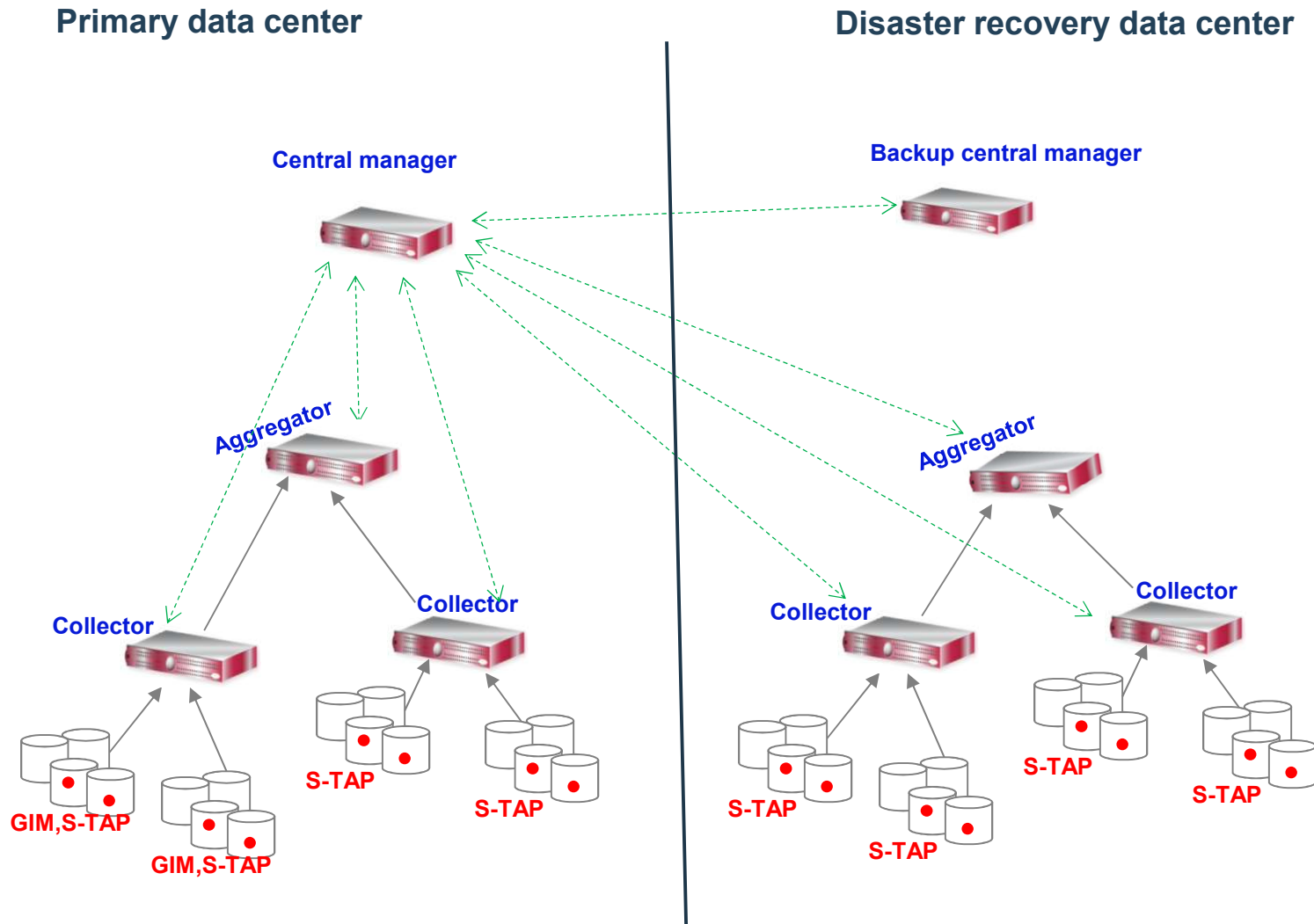
- SSL only
- No local traffic
- In 10.6 release
  - No client authentication
  - SSL version on client and server need to match



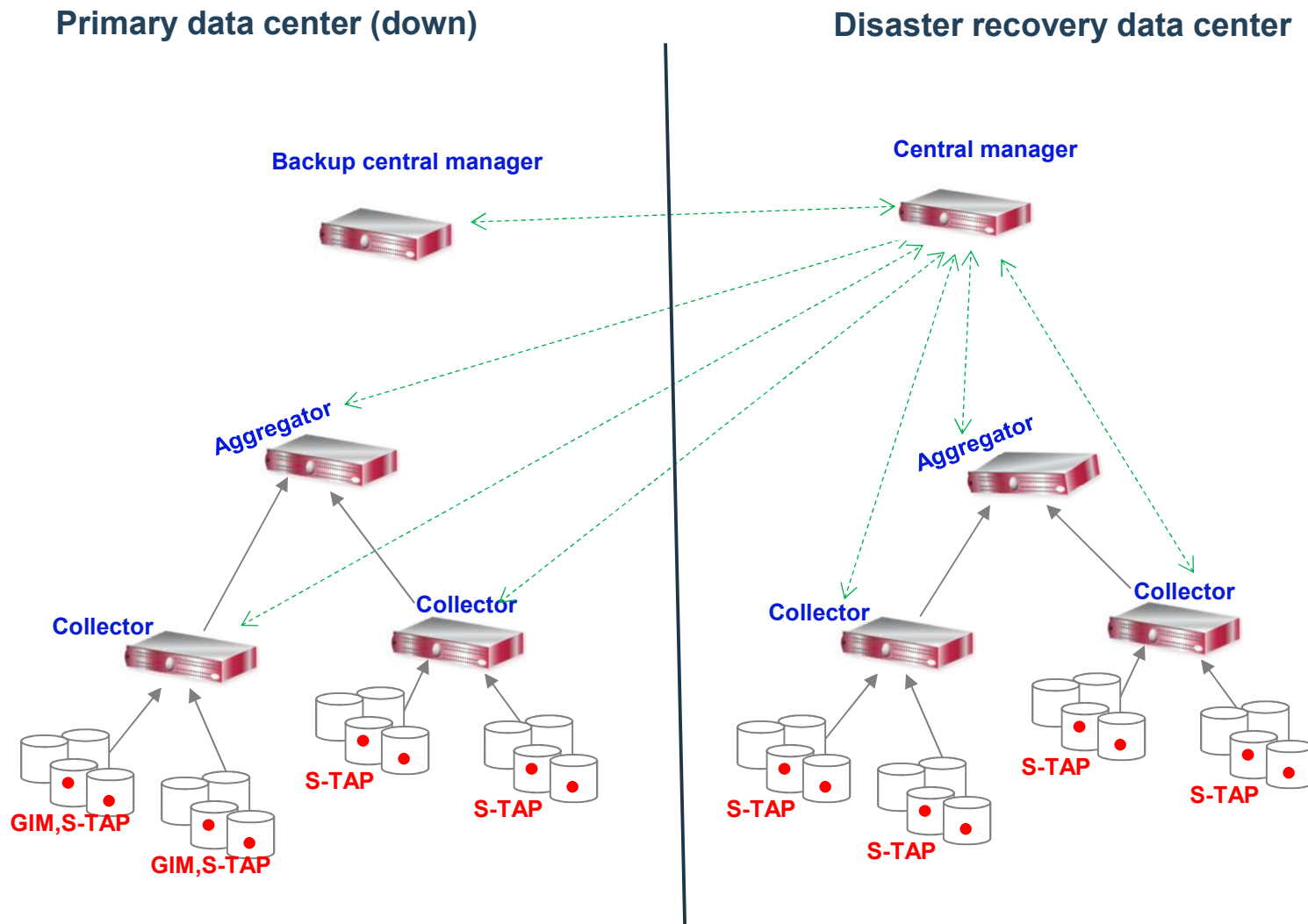
# Disaster recovery and high availability



# Disaster recovery



# Disaster recovery





## Appliance (collector / aggregator) availability

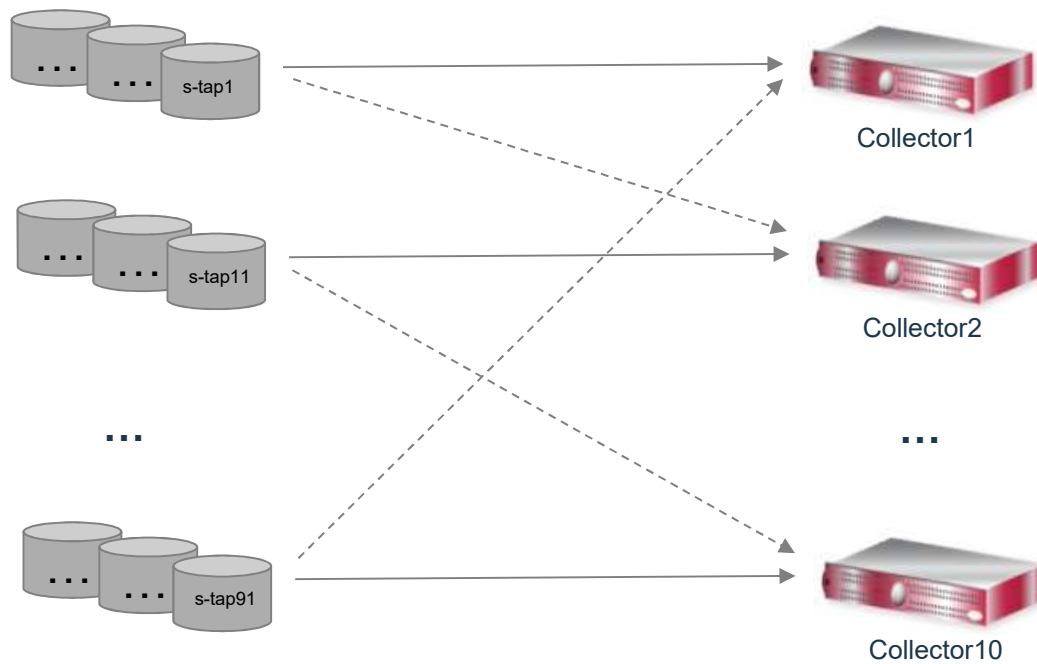
- Configuration option : port bonding

Bonding or teaming turns eth0 and another specified network interface card (NIC) into a bonded pair with standby failover.

cli : store network interface high-availability on <nic>, where nic is an available NIC.

# Collector availability

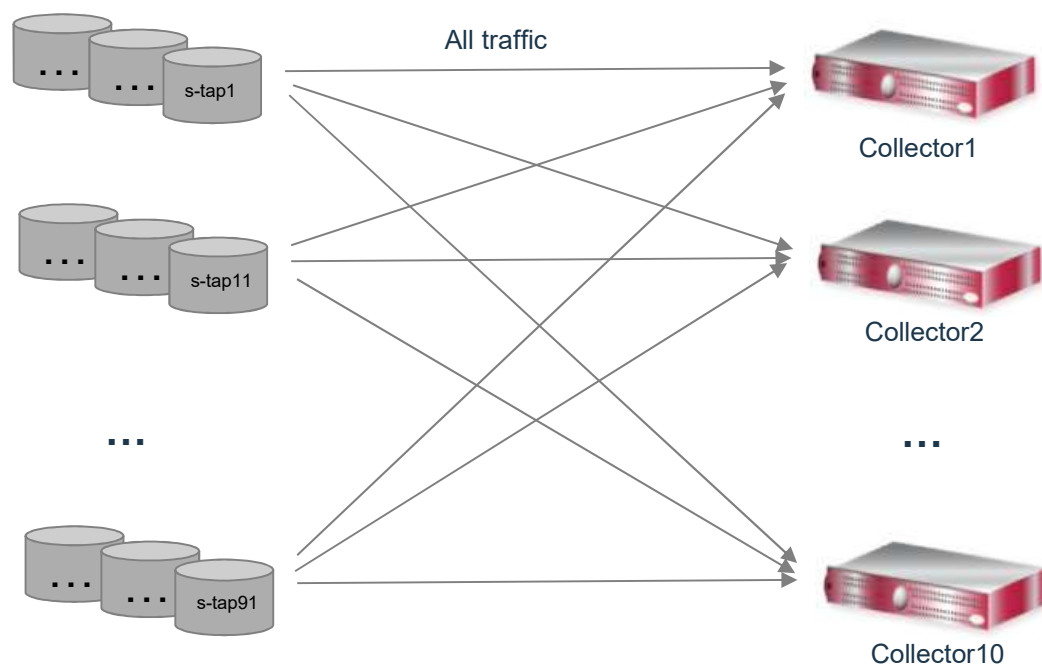
## S-TAP Failover





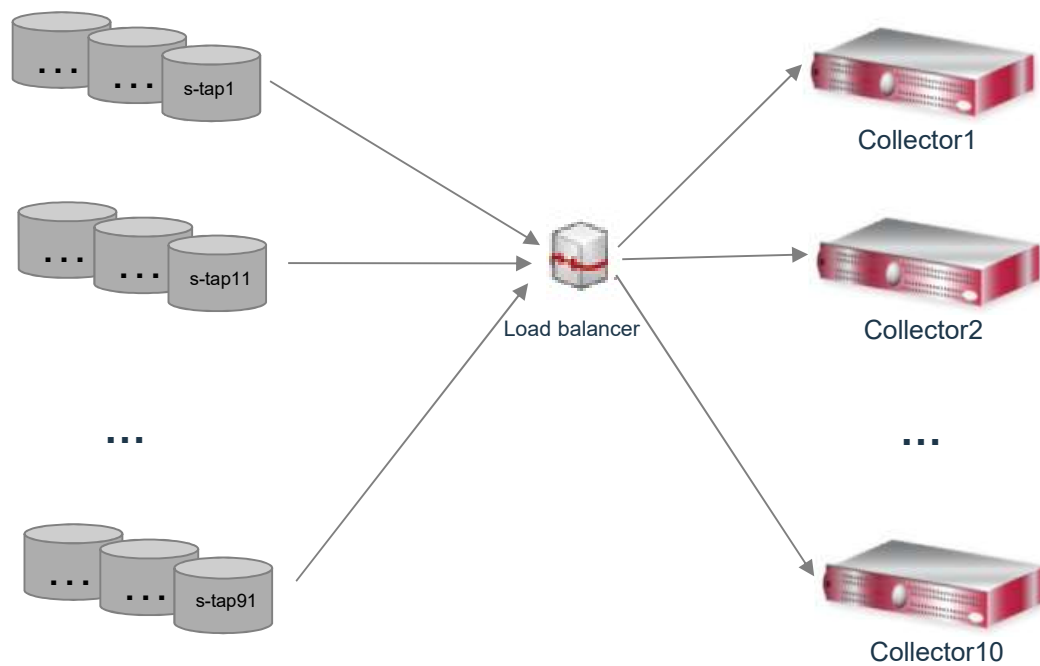
# Collector availability

## S-TAP Mirroring



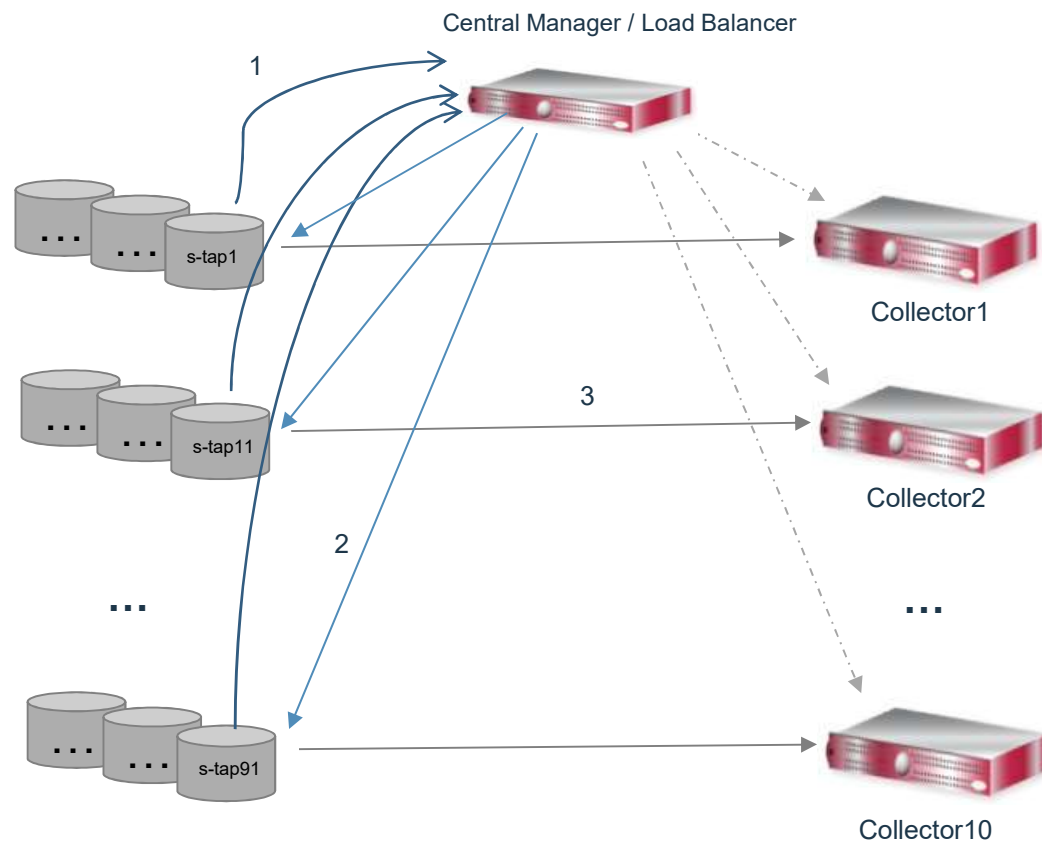
# Collector availability

## Grid / Hardware load balancer



# Collector availability

## Enterprise load balancer





## Aggregator availability

- Daily file is copied from a collector to an aggregator.
- Monthly system backup, optional daily archive.
- Ability to restore aggregator from monthly backup and daily archives of either aggregator's archive files or collectors' archive files.
- Ability to configure collectors to send export file to two aggregators: primary and secondary.



## Central manager availability

- Management of users, roles, groups, security policies, definitions of audit processes, queries, reports etc...
- Traffic is being collected by collectors even if central manager is down (policies and groups are propagated to all managed units).
- System or configuration backup (weekly).
- Ability to restore central manager from weekly backup.
- Ability to designate managed aggregator as backup central manager and make it primary when necessary.



## Agents availability

- GIM / S-TAP restart through inittab
- GIM / S-TAP restart through services
- Windows “Automatic” service for GIM / S-TAP

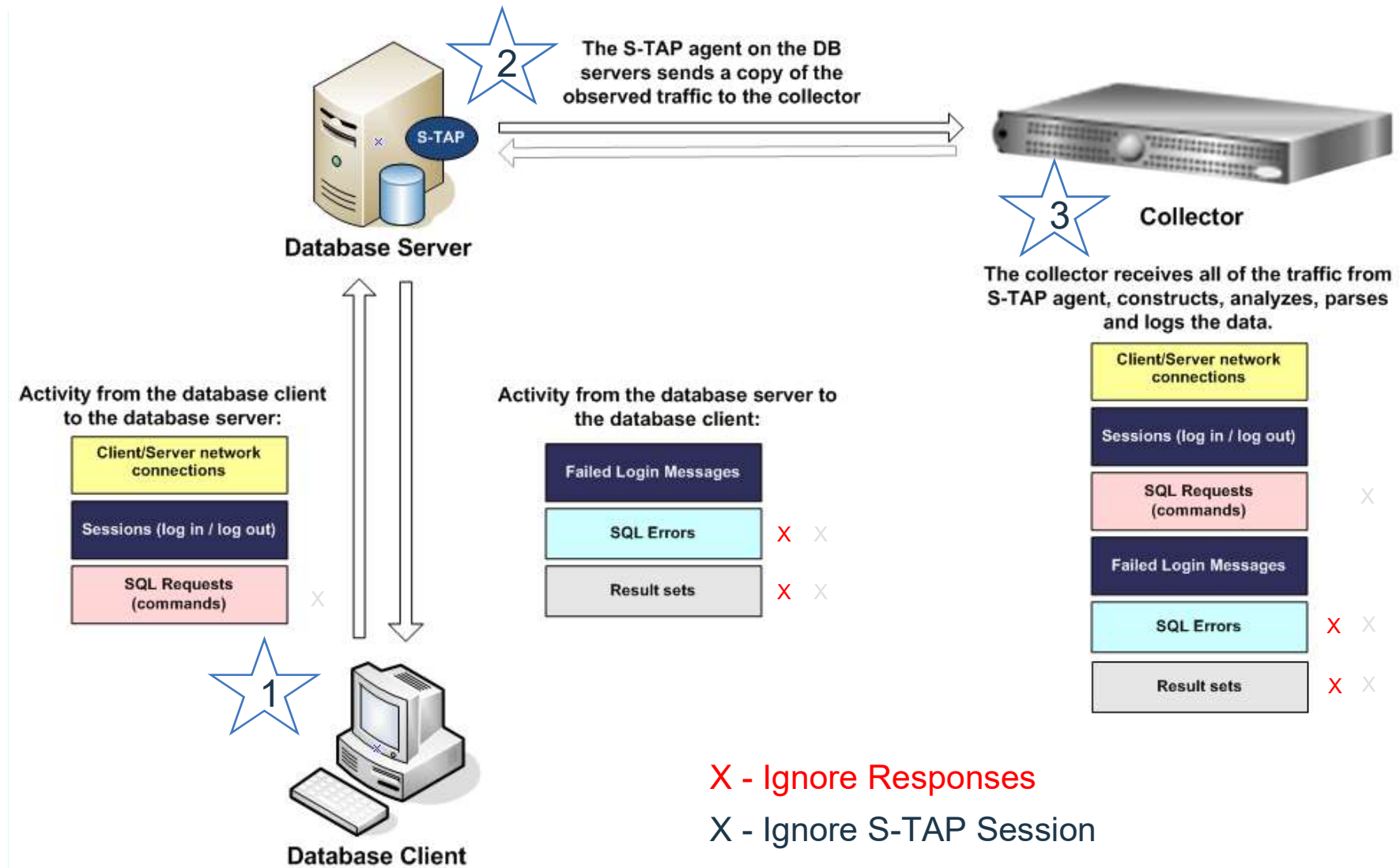


# Database responses



# Data flow

S-TAP ↔ Collector





## Database Responses

- All database responses (results sets and database exceptions) are being sent by S-TAP to collector by default in distributed environment.

Rule Suggestion

Suggest from DB

Add Access Rule

Add Exception Rule

Back Add Rules Reinstall Uninstall Policy Simulator

Rule Suggestion

Suggest from DB

Add Access Rule

Add Exception Rule

Add Extrusion Rule

Back Add Rules Reinstall Uninstall Policy Simulator

### Inspection Engine Configuration

Default Capture Value	<input type="checkbox"/>	Default Mark Auto Commit	<input checked="" type="checkbox"/>
Log Sequencing	<input type="checkbox"/>	Log Exception Sql String	<input checked="" type="checkbox"/>
Log Records Affected	<input type="checkbox"/>	Compute Avg. Response Time	<input type="checkbox"/>
Inspect Returned Data	<input type="checkbox"/>	Record Empty Sessions	<input type="checkbox"/>
Parse XML	<input type="checkbox"/>		
Logging Granularity	60 <input type="button" value="v"/>	Max. Hits per Returned Data	64
Ignored Ports List	<input type="text"/>		
Buffer Free	100 %		
<b>Restart Inspection Engines</b>		<b>Add Comments</b>	<b>Apply</b>



## Database Responses

- S-TAP configuration to manage DB responses
  - db\_ignore\_response – default is NONE; comma separated list of DB types (e.g. MYSQL,SYBASE,DB2) or ALL.
  - db\_ignore\_response\_bypass\_bytes - default is 4096 bytes. Enabled when <db\_ignore\_response> is set. S-TAP will send the initial specified bytes once for any given session.
  - db\_ignore\_response\_resets\_per\_request - default is 0. Possible values are 0 or 1. S-TAP will send <db\_ignore\_response\_bypass\_bytes> size for each request.
- Correspondent GIM parameters:
  - STAP\_DB\_IGNORE\_RESPONSE
  - STAP\_DB\_IGNORE\_BYPASS\_BYTES
  - STAP\_DB\_IGNORE\_RESETS\_PER\_REQUEST



# Blocking and S-TAP parameters



## Blocking and S-TAP parameters

- `FIREWALL_INSTALLED` – Indicates, if firewall is enable or not. Values 0 – disable (default); 1 – enable;
- `FIREWALL_DEFAULT_STATE` – indicates if blocking is configured in open or close mode. Values 0 – open; 1 – close; 2 – conditional close.
- `FIREWALL_FORCE_WATCH` – option to override open mode (set by `firewall_default_state`) for list of Client IPs;
- `FIREWALL_FORCE_UNWATCH` – option to override close mode (set by `firewall_default_state`) for list of Client IPs;
- `FIREWALL_FAIL_CLOSE` – defines S-GATE decision if verdicts is not returned by collector within defined (by `firewall_timeout`) parameter. Values 0 – lets SQL go through; 1 – block.
- `FIREWALL_TIMEOUT` – time in seconds to wait for collector verdict before making decision based on `firewall_fail_close` parameter.



# Automation





## Why automate?

- Guardium provides APIs to help automate the more common deployment tasks
- Repeatability
  - Standardization or consistency of configuration and metadata
  - Error reduction
- Reduce deployment effort
  - Especially for large, phased deployments
  - Benefits smaller deployment teams
- Improve deployment efficiency and speed
- Reduce maintenance effort due to Guardium patches and agent upgrades



## Why automate?

- Overcome typical large-customer challenges:
  - “Large” is subjective but greater than 20 appliances and roughly 200 STAPs
  - Enable large customers to scale the Guardium solution to their database platforms
    - Guardium uses a large number of appliances and orders-of-magnitude larger number of STAPs
  - Need to maintain separate managed environments due to multiple geographical regions
- Free Guardium personnel from repetitive tasks to focus on:
  - Servicing and supporting Guardium end-users
  - Leveraging more Guardium features
  - Creativity and innovation

# What can be automated?

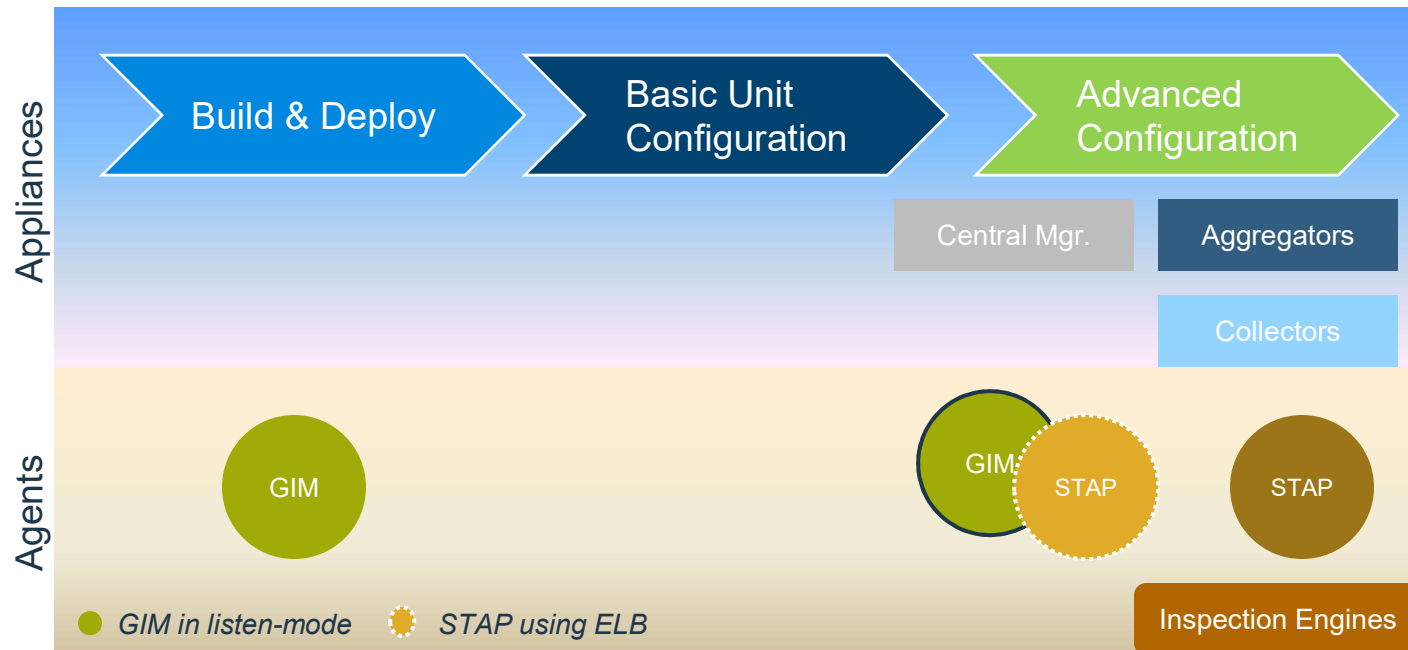
- A relatively large number of repetitive tasks in the different phases of the deployment life cycle, for the various components:
- Build > Deploy > Configure > Manage/Repair > Upgrade
- Appliances
  - Aggregator
    - CM
    - Non-CM
  - Collectors
- Agents
  - GIM
  - STAP
    - Inspection Engines
- Operations & Maintenance
  - Monitor/Repair Appliances
  - Monitor/Repair Agents
  - Monitor/Repair Inspection Engines
  - Monitor solution health e.g. scheduled jobs, aggregation, etc

*\* Monitor = Capacity and Health monitoring*





## A deployment timeline example



- In listen-mode the GIM agents can be deployed as the appliances are being built. Otherwise they are installed after the Central Manager is configured
- If using the Enterprise Load Balancer the STAPs can be deployed soon after the Central Manager is configured. Otherwise the STAPs are deployed once the Collectors are configured
- The Inspection engines are configured after the STAPs are assigned to collectors



***“Frameworks ...exist to provide structure and direction on a preferred way to do something without being too detailed or rigid. In essence, frameworks provide guidelines.”***

***“A methodology is an approach..with a defined set of rules, methods, tests activities, deliverables, and processes...”***

SCOTT ELLIS

*Frameworks, Methodologies and Processes, article*



## Automation tooling

- Need personnel with scripting, and preferably configuration management experience
- Use a configuration tool to manage agent deployment
- Build a framework for configuring and maintaining the appliances, with a focus on:
  - Modular design e.g. separate appliance deployment from agent's; platforms; deployment vs. upgrades, etc.
  - Data-driven inputs e.g. provide configuration via input files
  - Verification (error checking)
  - Encrypting and changing CLI password, or use the public-key storage (new)
  - Parser for command/report outputs e.g. Python for JSON (REST output), or text (CLI/grdAPI output)
- A controller workstation/server
  - A non-Guardium server (*RFE opportunity*)
  - Preferably Unix/Linux but depends on available scripting expertise
  - A light-weight RDBMS for metadata and performance metrics (for analysis and trending)
    - Should be supported by Guardium datasources to allow custom table loading
  - Can be used to schedule deployment or health-check scripts
  - Network-close to the Central Manager

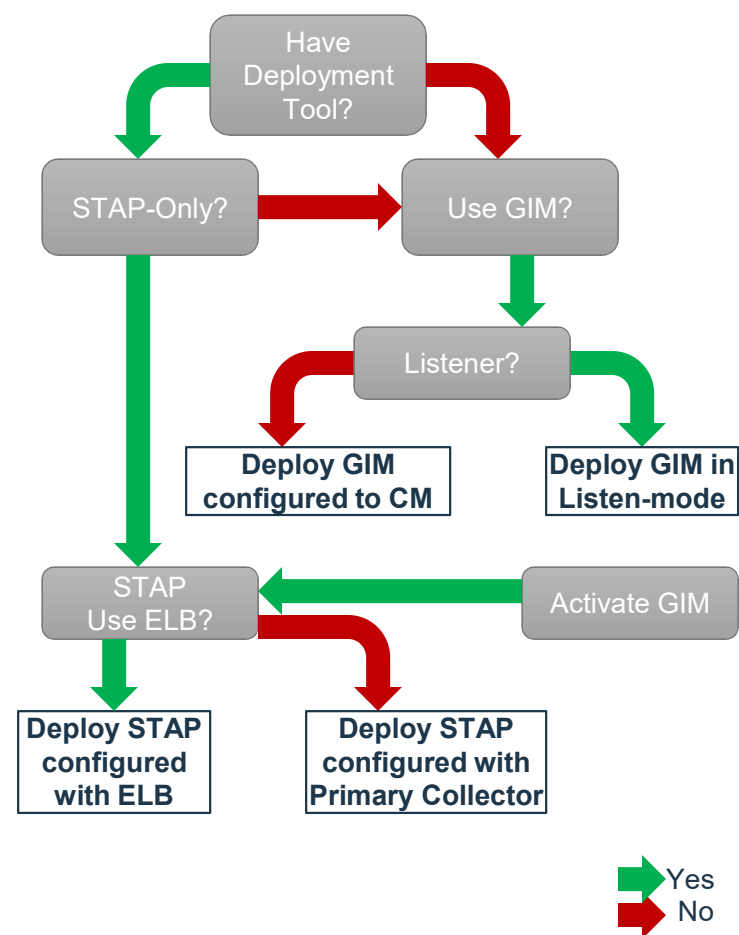


## Automation tooling

- An enterprise inventory system for server and database information that can feed the controller
- Build/leverage Guardium enterprise operational reports and deployment features e.g.
  - sniff\_buf\_usage,
  - agg/archive log,
  - scheduled jobs, etc.
  - Enterprise Load Balancer, etc
- Use source code control for versioning and recovery

# Agent Deployment options

- GIM and STAP usage-decision influences the deployment process:
  1. GIM with STAP vs. STAP-only
  2. GIM in listen-mode vs. configured
  3. STAP with ELB vs. STAP with specific primary collector
- For example:
  - GIM deployed in listen mode requires less input parameters i.e. no FQDN/IP of the CM
  - STAP with ELB uses a single FQDN/IP of the ELB, otherwise each STAP has to be mapped (in an input file) to it's primary collector
- For STAP-only deployment the Guardium team would use:
  - The SA team and deployment tool to deploy, maintain and upgrade the STAPs, including ktap module updates
  - CLI and grdApi/REST commands including `update_stap_config()`
- Even with a Deployment tool, the GIM gives the Guardium admin another option, especially for repairing some STAPs e.g.
  - Assigned collector IP is incorrect so STAP becomes inactive. This misconfiguration can be corrected using the GIM





# Inputs for agent deployment

- DB Server Inventory (GIM and STAP host):
  - Hostname, preferably, FQDN
  - Primary non-VIP IP Address
  - OS version
  - DBMS version
  - Guardium installation directory
- Collector inventory:
  - FQDN or IP address, preferably FQDN
- Map agents to server
  - GIM: map GIM installer/version to DB Server
  - STAP: map STAP (i.e. DB Server) to Collectors – both primary and secondary, unless using ELB
- Verify network routes and firewall ports
  - STAP: between DB Server and Collectors
  - STAP (ELB): between DB Server and Central Manger (or ELB Proxy)
  - GIM: between DB Server and CM (including gim listener port, if used)



# GIM deployment

- Stage GIM installers (OS and Guardium-version specific) for access by the deployment tool
- Prepare input files with input parameters, then “package”
  - Installer file; GIM host; installation directory; GIM Server IP/FQDN (unless in listen mode)
  - “Package” GIM installers for listen or configured mode, and host platform

*Note: The “package” process depends on the tool used e.g. for Ansible, create playbooks and templates.*
- Deploy GIM packages
- Activate GIM if deployed in listen-mode
- Verify GIM clients successfully reporting to assigned server e.g. Central Manager
- Identify and Repair failed GIM clients

# STAP deployment

- Using ELB - on Central Manger:
  - Create Managed Unit groups of collectors
  - Create group of STAPs i.e. STAP hosts
  - Associate (map) STAP groups to Managed Unit groups
- With GIM
  - Stage the STAP bundles (OS and Guardium-version specific) on the CM
  - Prepare the inputs for the grdAPI commands:
    - STAP Host, ELB/Collector, Bundle Name, STAP settings e.g. allow\_module\_combo, etc
  - “Package” the deployment commands
  - Deploy the STAPs
- Automation challenges (requiring DBA assistance) to configure
  - ATAP
  - EXIT
    - DB2
    - Informix
    - Teradata





# STAP deployment

- Some additional configuration considerations
  - \*Nix clusters:
    - Wait-for-dbexec
  - Failover
  - Configure STAP multi-threading
  - ATAP or EXIT
- Identify and Repair e.g.
  - KTAP not installed
  - Inactive STAPs
  - Missing Inspection Engines

# GIM deployment in listen mode using *Ansible*

- Use an Ansible playbook to copy and install an os-specific GIM installer to certain db servers

- Inputs provided

- gim installer
- install directory
- gim client host server
- Ansible playbook

```
drwxr-xr-x. 2 root root 4096 Apr 18 09:26 archive
drwxr-xr-x. 2 root root 81 Apr 17 13:17 rhel6_gim_installers
-rw-r--r--. 1 root root 1648 Apr 19 15:59 rhel_gim.yml
-rw-r--r--. 1 root root 439 Apr 17 13:18 rhel_hosts_dbs
-rw-r--r--. 1 root root 447 Apr 17 13:26 run_playbook.note
-rw-r--r--. 1 root root 423 Mar 29 13:50 win_hosts_dbs
```

```
[root@vm-rhel7-controller my_ansible]# ls -l rhel6_gim_installers
total 7508
-rwxr-x---. 1 root root 7685878 Apr 17 13:17 guard-bundle-GIM-10.1.4_r102728_v10_1_4_1-rhel-6-linux-x86_64.gim.sh
```

```
#####
# Note: indentation is crucial
# and blank lines not allowed unless commented
#####
all:
  children:
    RHEL_6:
      hosts:
        rhel6_oracle12c_1:
          ansible_host: 10.10.9.14
        rhel6_oracle11_1:
          ansible_host: 10.10.9.15
  vars:
    ansible_connection: ssh
    ansible_port: 22
    ansible_user: guardium_install
    ansible_become: yes
    install_dir: /usr/local/guardium/
```

```
#####
# gathering facts can slow down the deployment
# but can be useful to report on the target attributes
#
# The install_dir arg is defined in the hosts files
#
# Install gim in listen mode
#
#####
- hosts: RHEL_6
  gather_facts: yes
  vars:
    rhel6_gim_client: 'guard-bundle-GIM-10.1.4_r102728_v10_1_4_1-rhel-6-linux-x86_64.gim.sh'
    loc_gim_client: '/root/my_ansible/rhel6_gim_installers'

  tasks:
    - name: check if the gim client is running - not a foolproof check since it could be installed but not running
      shell: 'ps -ef | grep gim_client.pl | wc -l'
      register: gim_installed

    - name: exit if the gim client is running
      fail:
```

playbook to install gim on rhel db servers: *rhel\_gim.yml*

## GIM deployment in listen mode using *Ansible*

- Launch the Ansible playbook: `ansible-playbook -i rhel_hosts_dbs rhel_gim.yml`
  - assumes password-less configuration

```
[root@vm-rhel7-controller my_ansible]# ansible-playbook -i rhel_hosts_dbs rhel_gim.yml

PLAY [RHEL_6] *****

TASK [Gathering Facts] *****
ok: [rhel6_ora12c_1]

TASK [check if the gim client is running - not a foolproof check since it could be installed but not running]
changed: [rhel6_ora12c_1]

TASK [exit if the gim client is running] *****
skipping: [rhel6_ora12c_1]

TASK [copy the appropriate GIM] *****
ok: [rhel6_ora12c_1] => (item={u'dest': u'/tmp/', u'src': u'/root/my_ansible/rhel6_gim_installers/guard-bundle-x86_64.gim.sh'})

TASK [install GIM] *****
changed: [rhel6_ora12c_1]

RUNNING HANDLER [check the GIM client is listening] *****
changed: [rhel6_ora12c_1]

PLAY RECAP *****
rhel6_ora12c_1      : ok=5    changed=3    unreachable=0    failed=0
```

## Activate GIM using *grdAPI* via *TcL*

```
[root@vm-rhel7-controller my_grdapi]# ./grd-exp_v2_0.exp
USAGE: grd-exp_v2_0.exp <command_file> <appliance_file> <optional: cli-password>
```

```
[root@vm-rhel7-controller my_grdapi]# cat applianceList.txt
#
# List of Appliance IP or FQDN
#
10.10.9.52
```

```
[root@vm-rhel7-controller my_grdapi]# cat cmd_activate_gim.txt
#####
# Use this file to hold the cli or grdapi commands - one per line
# e.g.  grdapi list_staps onlyActive=false
#####
#
#grdapi command to  activate gim client on DB Server (targetHost)
# Can omit connectToCollector if using DNS
#
grdapi gim_remote_activation targetPort=8445 targetHost=10.10.9.14 connectToCollector=10.10.9.52
```




## Activate GIM using *grdAPI* via *TcL*

```
[root@vm-rhel7-controller my_grdapi]# ./grd-exp_v2_0.exp cmd_activate_gim.txt applianceList.txt
#####
# 10.10.9.52
#####
spawn ssh -o StrictHostKeyChecking=no cli@10.10.9.52
grdapi gim_remote_activation targetPort=8445 targetHost=10.10.9.14 connectToCollector=10.10.9.52

IBM Guardium, Command Line Interface (CLI)



Last login: Fri Apr 20 09:02:50 2018 from 10.10.9.2
grdapi gim_remote_activation targetPort=8445 targetHost=10.10.9.14 connectToCollector=10.10.9.52
Welcome cli - your last login was Thu Apr 19 21:30:08 2018
vm-coll-v10-sa-52.ps.org>_grdapi gim_remote_activation targetPort=8445 targetHost=10.10.9.14 conn
0.10.9.52
ID=0
HOST=10.10.9.14, RESULT=SUCCESS
ok
vm-coll-v10-sa-52.ps.org>_exit
Connection to 10.10.9.52 closed.
```

https://10.10.9.52:8443/#manage\_procmon

IBM Guardium 10:39    User Interface Search

GIM Processes Monitor

Filter status by ☐ Up ☐ Unknown ☐ Down

Server name	Server IP	Module name	Status	Module version
rhel65_db14.ps.org	10.10.9.14	GIM		10.1.4_r102728_1
rhel65_db14.ps.org	10.10.9.14	SUPERVISOR		10.1.4_r102728_1

## Install and configure STAP using *grdAPI* via *TcL*

- With the GIM activated and reporting to the GIM server, **install STAP**, using the *grdAPI* script:
  - First need to upload the STAP bundle to the GIM Server, if not already uploaded
  - Then prepare the *grdAPI* commands

```
# ./grd-exp_v2_0.exp cmd_ins_stap_bundle_rhel6.txt applianceList.txt

#####
# Use this file to hold the cli or grdapi commands - one per line
# e.g.  grdapi list_staps onlyActive=false
#
# This file should ideally be auto-generated with DB Host IP/FQDN, etc
#
# The moduleVersion can be obtained from the GUI > setup by client
# or use grdapi gim_list_bundles
#
#####

#
# grdapi command to install STAP gim bundles
# Note: First manually stage/upload STAP bundles to the Central Manager
#

grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=10.10.9.14 module=BUNDLE-STAP moduleVersion=10.1.4_r102728_1
grdapi gim_update_client_params clientIP=10.10.9.14 paramName=KTAP_ALLOW_MODULE_COMBOS paramValue=y
grdapi gim_update_client_params clientIP=10.10.9.14 paramName=STAP_SQLGUARD_IP paramValue=10.10.9.52
grdapi gim_update_client_params clientIP=10.10.9.14 paramName=STAP_TAP_IP paramValue=10.10.9.14
grdapi gim_schedule_install clientIP=10.10.9.14 module=BUNDLE-STAP date=now

#The End
```

*cmd\_ins\_stap\_bundle\_rhel6.txt*

# Install and configure STAP using *grdAPI* via *Tcl*

```
[root@vm-rhel7-controller my_grdapi]# ./grd-exp_v2_0.exp cmd_ins_stap_bundle_rhel6.txt applianceList.txt

#####
# 10.10.9.52
#####
spawn ssh -o StrictHostKeyChecking=no cli@10.10.9.52
grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=10.10.9.14 module=BUNDLE-STAP moduleVersion=10.1.4_r102728_1
IBM Guardium, Command Line Interface (CLI)
Last login: Fri Apr 20 10:33:58 2018 from 10.10.9.7
lby_version clientIP=10.10.9.14 module=BUNDLE-STAP moduleVersion=10.1.4_r102728_1
Welcome cli - your last login was Fri Apr 20 10:34:00 2018
vm-coll-v10-sa-52.ps.org> grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=10.10.9.14 module=BUN
DLE-STAP moduleVersion=10.1.4_r102728_1
ID=0
ok
vm-coll-v10-sa-52.ps.org> grdapi gim_update_client_params clientIP=10.10.9.14 paramName=KTAP_ALLOW_MODULE_COMBOS
paramValue=y
ID=0
ok
vm-coll-v10-sa-52.ps.org> grdapi gim_update_client_params clientIP=10.10.9.14 paramName=STAP_SQLGUARD_IP paramVa
lue=10.10.9.52
ID=0
ok
vm-coll-v10-sa-52.ps.org> grdapi gim_update_client_params clientIP=10.10.9.14 paramName=STAP_TAP_IP paramValue=1
0.10.9.14
ID=0
ok
vm-coll-v10-sa-52.ps.org> grdapi gim_schedule_install clientIP=10.10.9.14 module=BUNDLE-STAP date=now
ID=0
ok
vm-coll-v10-sa-52.ps.org> exit
Connection to 10.10.9.52 closed.
```

https://10.10.9.52:8443/#manage\_status1

ST IBM Guardium 10:57 User Interface Search

S-TAP Status

	S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response	Primary Host Name	KTAP Installed
●	10.10.9.14	STAP-10.1.4_r102728_v10_1_4_1-20171208_2019	oracle	Active	2018-04-20 10:56:54	10.10.9.52	Yes



## Some useful commands






Task	Method	Category
List available GIM bundles including version info for installing STAPs	<code>grdapi gim_list_bundles</code>	GIM
Activate GIM client in listen mode	<code>grdapi gim_remote_activation targetPort=8445 targetHost=&lt;DB Server&gt; connectToCollector=&lt;Collector&gt;</code>	GIM
Install and configure STAP on Linux	<code>grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=10.10.9.14 module=BUNDLE-STAP moduleVersion=10.1.4_r102728_1</code>  <code>grdapi gim_update_client_params clientIP=10.10.9.14 paramName=KTAP_ALLOW_MODULE_COMBOS paramValue=y</code>  <code>grdapi gim_update_client_params clientIP=10.10.9.14 paramName=STAP_SQLGUARD_IP paramValue=10.10.9.52</code>  <code>grdapi gim_update_client_params clientIP=10.10.9.14 paramName=STAP_TAP_IP paramValue=10.10.9.14</code>  <code>grdapi gim_schedule_install clientIP=10.10.9.14 module=BUNDLE-STAP date=now</code>	STAP
Update guard_tap.ini <i>STAP must be running/active</i>	<code>grdapi update_stap_config stapHost=10.10.9.14 updateValue=SQLGUARD_0.sqlguard_ip:10.10.9.52</code>	STAP
List inspection engines for specific host	<code>grdapi list_inspection_engines stapHost=10.10.9.14</code>	STAP





# THANK YOU

FOLLOW US ON:

-  [ibm.com/security](http://ibm.com/security)
-  [securityintelligence.com](http://securityintelligence.com)
-  [xforce.ibmcloud.com](http://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.

