Deployment Guide

Document version 1.6

What's inside:

Deploying the BIG-IP LTM with IBM InfoSphere Guardium

Welcome to the F5 deployment Guide for building a high availability architecture for IBM® InfoSphere Guardium, IBM's database security appliance. This document provides guidance for deploying the BIG-IP Local Traffic Manager (LTM) with IBM InfoSphere Guardium.

IBM InfoSphere Guardium provides a simple, scalable and powerful solution for real-time database activity monitoring. By deploying Guardium appliances to collect information from your databases your organization gains up-to-the-second insight into the activity happening at the data level. This information allows administrators to take a variety of actions, such as preventing attacks, enforcing controls, auditing access and many other essential database tasks.

Because the integrity of this information is so critical, uptime and performance of the Guardium cluster is paramount. To achieve the levels of uptime demanded by advanced solutions, F5 and IBM have jointly created, tested, and documented this high availability solution.

Why F5

By deploying BIG-IP LTM in front of Guardium, organizations can achieve the following benefits:

- Reduced total cost of ownership through easier configuration and management,
- Health monitoring of the Guardium S-TAP Collectors to ensure traffic is sent to a Collector that is actually up and available,
- Intelligent Load Balancing to distribute incoming connections to the Guardium server with the least connections,
- Transparent pass-through of SSL connections to allow either SSL or cleartext connections between the databases and the Collectors,
- Granular control the administrators, allowing for maintenance on a particular Guardium Collector, without impacting Database information collection.

For more information of IBM Guardium see: *http://www-01.ibm.com/software/data/guardium/*
For more information on the F5 BIG-IP system, see *http://www.f5.com/products/big-ip*

To provide feedback on this deployment guide, contact us at *solutionsfeedback@f5.com*.

Important: *Make sure you are using the most recent version of this deployment guide, found at http://www.f5.com/pdf/deployment-guides/ibm-guardium-dg.pdf.*

Products and versions

Product	Version
BIG-IP LTM	11.2 HF-2
IBM InfoSphere Guardium	v 9.0 with Patch p02_GPU_October_2012 or later

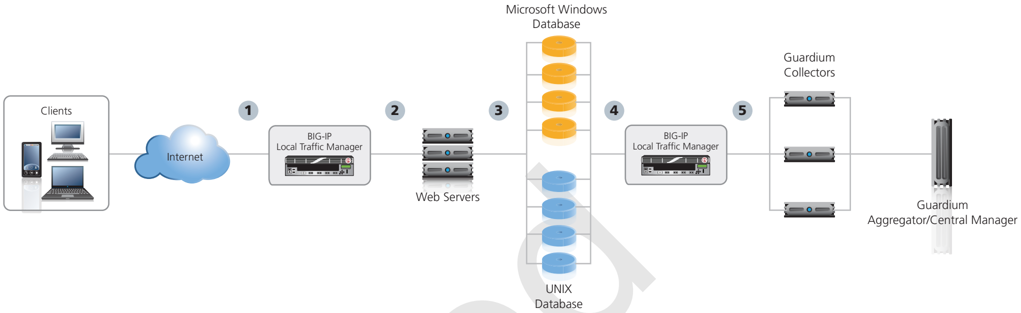
Prerequisites and configuration notes

For scalability and management, we recommended that the following be available in the Guardium configuration:

- For S-TAP, a Guardium Aggregator should be used to aggregate incoming information from all of the Guardium Collector appliances. Reports should be run using the Aggregator.
- For the Change Audit System (CAS), we recommend you use a Guardium Managed Environment, to unify the CAS settings across all Guardium appliances.
- This guide is written with the assumption that BIG-IP LTM is already on the network with initial configuration (objects such as self IP addresses and VLANs) already complete.
- Configuring the BIG-IP LTM for specific applications is not covered in this guide.
- For information on how to deploy BIG-IP Application Security Manager (ASM) with Guardium, see http://www.f5.com/pdf/deployment-guides/ibm-guardium-asm-dg.pdf.
- For Windows Database hosts, it is a networking requirement of Guardium up-to and including version 9.0 P02, that UDP connections be allowed from the Guardium appliance to the Windows Database host on UDP port 8075. These UDP connections do not need to traverse the BIG-IP system, but they are required in order for heartbeats to function properly. Configure your firewalls and networking equipment to allow these connections.

Configuration example

The following diagram shows the configuration described in this guide. In this diagram, we show the BIG-IP LTM in front of web servers/applications to provide a complete picture about the environments in which Guardium and the BIG-IP LTM are deployed. In this deployment guide, we specifically cover the configuration of the BIG-IP system between the databases and the Guardium Collector (the BIG-IP system on the right side of the following diagram).


Microsoft Windows Database
Clients
Internet
1
BIG-IP Local Traffic Manager
2
Web Servers
3
4
BIG-IP Local Traffic Manager
5
Guardium Collectors
Guardium Aggregator/Central Manager
UNIX Database

1. A client request comes into BIG-IP LTM to be load balanced to a web application.
2. The BIG-IP LTM makes the best load balancing decision at the application level to direct traffic to web servers and/or application servers.
3. The application servers use their database servers as applicable.
4. The S-TAP agent on the database servers initiate connections to the Guardium appliance through the BIG-IP LTM.
5. The BIG-IP LTM directs the S-TAP traffic to the most available Guardium Collector.

Understanding the role of the BIG-IP system in Guardium connection balancing

This section describes the key concepts of load balancing Guardium through the BIG-IP system.

The primary purpose of the BIG-IP LTM and Guardium solution is to ensure the availability and functionality of S-TAP and CAS connections between the databases and the Guardium Collectors. By routing connections through the BIG-IP system, overall administration complexity is reduced (S-TAP configuration points to the BIG-IP instead of a series of Guardium Collectors) which allows for organizations to easily handle unexpected outages, planned maintenance, and growth of the environment.

Once administrators have an understanding of the Guardium connection architecture, as well as the following potential persistence issues, they are able to properly manage the environment. Make note of the following:

- Guardium S-TAP connections are long-lived and persistent to the Collector to which they attach.
- The BIG-IP LTM ensures that new connections go to the Guardium appliance with the fewest connections.
- Guardium S-TAP connections have the ability to buffer data on the client side for a small period of time to ensure Collector data is not lost.
- Guardium S-TAP connections do not reset unless there is an outage or an administrative decision is made to restart the agents.
- Guardium S-TAP agents running the UNIX platforms contain a heartbeat connection which is used to keep the connection alive.
- Guardium S-TAP agents running Windows do not have a heartbeat.
- Guardium CAS agents reset their connections every 24 hours.

F5 has designed this deployment guidance with the following considerations in mind.

- We recommend the Least Connections load balancing method, so the BIG-IP LTM always sends new connections to the Guardium appliance with the fewest connections.
- We have implemented health monitoring to detect outages.

Because of this architecture, it is important to note that when administrative or unplanned outages cause a Guardium Collector to become unavailable, connections from S-TAP agents on the failed Collector are directed by the BIG-IP system to the next most available connector. Guardium CAS connections are also directed to the most available connector. When the failed Collector is once again available, connections do not automatically rebalance to the recovered host for S-TAP agents. However, for CAS agents, all connections rebalance within 24 hours (as noted in the list above).

For the consistency of connection balancing, after the recovery of a failed Guardium Collector we recommend you reset all of your S-TAP connections in order to rebalance your environment. Because the Guardium agents buffer data on the client side, rebalancing in this manner should not lead to data loss. Restarting agents can be done through the Guardium administrative UI, can be scripted on your database hosts (we recommend a complete stop and start of the agent), or it can be orchestrated using a solution such as IBM Tivoli Netcool Configuration Manager.

While rebalancing is not critical in the short term, large environments with many connections may suffer degraded performance if S-TAP connections are not rebalanced after repeated Guardium Collector failures.

Configuring Guardium S-TAP

To properly support load balancing, the Guardium S-TAP agents must be configured properly. Add, uncomment, or modify the settings on your S-TAP Configuration to look like the following examples.

See the Guardium product documentation on how and where to adjust the S-TAP configuration file, as well as for updated guidance from IBM.

- **`Sqlguard_ip = <Your BIG-IP Virtual Server IP address/hostname>`**

  For example: **`Sqlguard_ip = 192.0.2.123`**
- **`Participate_load_balancing = 3`**
- **`All_can_control = 1`**

Sqlguard_ip is the address you will define on BIG-IP LTM during the Virtual Server configuration.

Participate in Load balancing allows the S-TAP to send session information on every failover to the appliance.

All Can Control allows the S-TAP to be able to edit S-TAP configurations through GUI.

The BIG-IP LTM configuration starts on the following page.

Configuring the BIG-IP system for Guardium S-TAP

There are two options for configuring the BIG-IP system for S-TAP: Windows (clear text or SSL) and UNIX (Clear text or SSL).

Configuring the BIG-IP system for Windows S-TAP Agents

Use the following tables to configure the BIG-IP system for the Windows S-TAP Agents. The tables contain a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

Use the Unencrypted (Clear) or Encrypted table, as appropriate for your configuration. If you are using both clear and encrypted connections in your environment, configure both pools and virtual servers defined in the following tables.

Windows S-TAP Agents - Unencrypted (Clear)

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**TCP Half Open**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name, such as **Windows-STAP-Pool-Clear**	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**0**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the nodes	
	Service Port	**9500** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Local Traffic-->Profiles*)	***Persistence*** (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source IP Affinity**
	TCP (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
Virtual Servers (*Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**9500**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	SNAT Pool	**Auto Map**	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

Windows S-TAP Agents - Encrypted

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Local Traffic-->Monitors*)	***Name***	Type a unique name	
	Type	**TCP Half Open**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name, such as **Windows-STAP-Pool-TLS**	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**0**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the nodes	
	Service Port	**9501** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Local Traffic-->Profiles*)	***Persistence*** (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Source IP Affinity**
	TCP (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
Virtual Servers (*Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**9501**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	SNAT Pool	**Auto Map**	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

Configuring the BIG-IP system for Linux/UNIX Agents

If you have Linux/Unix S-TAP Agents in your environment use the following table to configure the BIG-IP LTM objects.

Use the Unencrypted (Clear) or Encrypted table, as appropriate for your configuration. If you are using both clear and encrypted connections in your environment, configure both pools and virtual servers defined in the following tables.

Linux/UNIX S-TAP Agents - Unencrypted (Clear)

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**TCP Half Open**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name, such as **UNIX-STAP-Pool-Clear**	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**0**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the nodes	
	Service Port	**16016** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Local Traffic-->Profiles*)	***Persistence*** (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source IP Affinity**
	TCP (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
Virtual Servers (*Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**16016**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	SNAT Pool	**Auto Map**	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

Linux/UNIX S-TAP Agents - Encrypted

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**TCP Half Open**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name, such as **UNIX-STAP-Pool-TLS**	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**0**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the nodes	
	Service Port	**16018** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Local Traffic-->Profiles*)	***Persistence*** (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Source IP Affinity**
	TCP (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
Virtual Servers (*Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**16018**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	SNAT Pool	**Auto Map**	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

This completes the configuration for Guardium S-TAP.

Configuring the BIG-IP system for Guardium CAS

In this section, you configure the BIG-IP LTM for Guardium CAS. For CAS, both Windows and Linux/UNIX use the same port, so there are only two configuration tables.

Configuring the BIG-IP LTM

Use the following tables to configure the BIG-IP system for the Guardium CAS. The tables contain a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

Use the Unencrypted (Clear) or Encrypted table, as appropriate for your configuration. If you are using both clear and encrypted connections in your environment, configure both pools and virtual servers defined in the following tables.

Unencrypted (Clear)

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**TCP Half Open**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name, such as **UNIX-CAS-Pool-Clear**	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**0**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the nodes	
	Service Port	**16017** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Local Traffic-->Profiles*)	***Persistence*** (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source IP Affinity**
	TCP (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
Virtual Servers (*Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**16017**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	SNAT Pool	**Auto Map**	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

Encrypted

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**TCP Half Open**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Local Traffic -->Pools*)	***Name***	Type a unique name, such as **UNIX-CAS-Pool-TLS**	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**0**	
	Load Balancing Method	**Least Connections (Node)**	
	Address	Type the IP Address of the nodes	
	Service Port	**16019** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Local Traffic -->Profiles*)	***Persistence*** (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source IP Affinity**
	TCP (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
Virtual Servers (*Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**16019**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	SNAT Pool	**Automap**	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

This completes the configuration for Guardium CAS.

Next Steps

After configuring the S-TAP agents as described in the Guardium documentation and in this document, and configuring the BIG-IP LTM for Guardium S-TAP and CAS load balancing, we recommend you test your environment from beginning to end. Use the following guidance to test the configuration on one database host and one Guardium Collector:

1. Start the Guardium agent on a database host,
2. Log into the Guardium UI and verify that you see a connection,
3. Generate Database activity and verify that you are seeing the database activity in the Guardium Collector or aggregator,
4. Check the BIG-IP Statistics tab (as described in the troubleshooting section below) to verify the connection you have generated is going through the BIG-IP system.

Troubleshooting

This section contains some common areas to consider when troubleshooting Guardium load balancing with BIG-IP LTM.

- **Verifying that connections are balanced properly**
  Use the BIG-IP UI to verify that connections are load balanced properly. From the Main tab of the BIG-IP Configuration utility, click **Statistics**, and then click **Module Statistics**. On the Menu bar, click **Local Traffic**, and then from the **Statistics Type** list, select **Pools**. Examine the Guardium pool members you have setup. The *Connections* column indicates how many connections are balanced through the BIG-IP system, and the Guardium hosts to which they are terminated. You should see an even distribution of connections. If not, stop and then start your Guardium S-TAP agents.

  Further, from the Guardium UI, on the Central Manager, the pre-built report **Enterprise S-TAP view** displays which Collector is managing which S-TAP.

- **Some S-TAP agents are unable to connect to the Collector**
  Verify the BIG-IP system is configured as described in this document. Verify that no other firewalls are blocking TCP communication between your databases, the BIG-IP LTM, and the Guardium Collectors. Guardium uses TCP ports 16017 (cleartext) and 16019 (encrypted) for CAS connections, 16016 (cleartext) for UNIX S-TAP connections, 16018 (encrypted) for UNIX S-TAP connections, 9500 (cleartext) for Windows S-TAP connections and 9501 (encrypted) for Windows S-TAP connections.

  Additionally, verify your S-TAP configuration was completed properly on the client side, that you have set the Sqlguard_ip to the virtual server IP address of the BIG-IP LTM and that Participate_Load_Balancing is set to 3.

- **Windows based agents are flapping or seem to get disconnected**
  Verify that in your network architecture, you have allowed UDP connections originating from the Guardium appliances to the Windows hosts on UDP port 8075. For versions of Guardium up to and including the release covered in this deployment guide, in order for Windows hosts to stay connected, a heartbeat pattern relies on TCP and UDP. Specifically, an originating message is sent from the Guardium appliance to the Windows based host on UDP port 8075. This connection does not need to traverse the BIG-IP system. Once this message is received, the BIG-IP device sends a heartbeat on TCP port 9500 or 9501 (depending on whether encryption is configured). This process occurs every 5 seconds. The functionality of this process relies on the UDP connectivity being present.

Document Revision History

Version	Description	Date
1.0	New guide	10-22-2012
1.1	Added a link to the Guardium deployment guide for BIG-IP Application Security Manager (ASM) to the prerequisites.	02-11-2013
1.2	Added a new row to the configuration tables for the TCP profiles of the Windows S-TAP agents, stating the Idle Timeout value should be adjusted according to the guidance in *Understanding the role of the BIG-IP system in Guardium connection balancing on page 4*.	03-19-2013
1.3	In the Troubleshooting section, corrected the TCP ports used by Guardium for UNIX and Windows S-TAP connections in *Some S-TAP agents are unable to connect to the Collector on page 12*.	03-26-2013
1.4	- Updated the version of Guardium to v 9.0 with Patch p02_GPU_October_2012 or later - Added a new prerequisite concerning Windows Database hosts on *page 2* - Removed the TCP Idle Timeout row from the TCP profiles of the configuration tables for Windows S-TAP agents, as well as from the guidance in *Understanding the role of the BIG-IP system in Guardium connection balancing on page 4*. - Removed the Persistence profile guidance from the Windows, and Linux/UNIX S-TAP agent configuration tables. - Added a new entry to *Troubleshooting on page 12* for Windows based agents that are flapping or getting disconnected.	04-17-2013
1.5	Updated the diagram in *Configuration example on page 3* with the proper names of the IBM servers.	07-15-2013
1.6	Added a Source Address Affinity persistence profile to all of the configuration tables in the *Configuring the BIG-IP system for Guardium S-TAP on page 6* section.	12-19-2014

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com