IBM® Guardium®

Essentials-2025

Disclaimer:

- This session provides an introductory overview of product features and is intended solely as a supplementary learning resource. It is not suitable for implementation purposes. Accurate deployment requires a thorough understanding of the product, its intended use, and environment—none of which are covered in this session.

- Content is subject to change as the product evolves. We do not accept responsibility for decisions made based on this material, and any actions taken are at your own risk. We disclaim liability for any resulting damages.

- For the most current and accurate IBM documentation, please refer to: https://www.ibm.com/docs/en/gdp

- By continuing to participate, you acknowledge and accept these terms. If you do not agree, please disconnect from the session.

IBM

Speaker for today:

Sachin Marawar

Technical Support Professional, IBM Software Support (Data Security)

Data **Security**

IBM

IBM Guardium Essentials-2025

8-Session Kickstart Series

Master the Foundations of Data Security Monitoring & Compliance

Session	Date	Topic	Registration Link
Session 1	Aug 26 (Tue)	What is IBM Guardium & How It Works	https://ibm.biz/IBMGE-S1
Session 2	Aug 28 (Thu)	Installing & Configuring Guardium Appliances	https://ibm.biz/IBMGE-S2
Session 3	Sep 02 (Tue)	GIM & WINSTAP Deployment	https://ibm.biz/IBMGE-S3
Session 4	Sep 04 (Thu)	Introduction to Guardium Policies	https://ibm.biz/IBMGE-S4
Session 5	Sep 09 (Tue)	GIM & S-TAP for UNIX/Linux	https://ibm.biz/IBMGE-S5
Session 6	Sep 11 (Thu)	Guardium Reports, Entities & Attributes	https://ibm.biz/IBMGE-S6
Session 7	Sep 16 (Tue)	Guardium Alerts & Audit Process	https://ibm.biz/IBMGE-S7
Session 8	Sep 18 (Thu)	Aggregation, Backup & Restore in Guardium	https://ibm.biz/IBMGE-S8

TODAY

Use above links to Register for each session!

IBM

Session 5:

IBM® Data Security

GIM & S-TAP for Unix/Linux

-Sachin Marawar

Technical Support Professional, IBM Software Support (Data Security)

Agenda

- What is GIM?

↓

- GIM Communication

↓

- What is S-TAP?

↓

- Installation Pre-requisites

↓

- Demo

↓

- Q&A

Feedback & Suggestions are welcome at:
datasec_ap_support@wwpdl.vnet.ibm.com

IBM

GIM Terminology

- GIM Agent – Collection of perl scripts run on each managed server allowing for centralized management
- GIM Server – Guardium appliance (deploy, modify, update, uninstall)
- GIM Bundle – A package of software that can be deployed with GIM. File extension .gim
  Example: **guard-GIM-12.0_r120001295_1-x86_x64.gim**
- Module – Components of a bundle. A.gim file containing one or more modules or sub-modules.
  Examples: CAS, S-TAP, FAM, KTAP, ATAP, SUPERVISOR and more.
- Listener Mode – GIM Agent not yet associated with a GIM Server
- Standard Mode – GIM Agent associated with a GIM server

What is GIM?

```
[redacted]ibm.com> grdapi commands gim
ID=0
Matching API Function list :
gim_assign_bundle_or_module_to_client_by_version
gim_assign_latest_bundle_or_module_to_client
gim_cancel_install
gim_cancel_uninstall
gim_get_available_modules
gim_get_client_last_event
gim_get_global_param
gim_get_modules_running_status
gim_list_bundles
gim_list_client_modules
gim_list_client_params
gim_list_mandatory_params
gim_list_registered_clients
gim_list_unused_bundles
gim_load_package
gim_remote_activation
gim_remove_bundle
gim_reset_client
gim_schedule_install
gim_schedule_uninstall
gim_set_diagnostics
gim_set_global_param
gim_unassign_client_module
gim_uninstall_module
gim_update_client_params

ok
[redacted]ibm.com>
```

GIM Server can be any Guardium Appliance

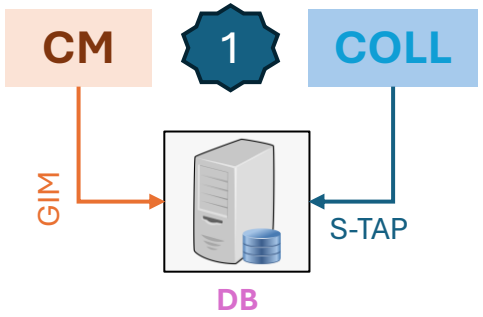
- GIM stands for Guardium Installation Manager
  - Client/Server architecture:
    - GIM Server is the appliance (can be a CM, AGG, Coll)
    - GIM Client is the agent
  - Allows for the centralized deployment of STAP modules/bundles on DB servers
  - Allows for centralized updating of STAP parameters
  - Allows for updating/upgrading of STAP software
  - Can be used both via CLI or GUI
  - Restart STAPs and gather STAP diags remotely
  - Deploy STAPs in groups
  - If planned properly very easy to use
  - ".gim" extension for bundles, modules

GIM Processes Monitor

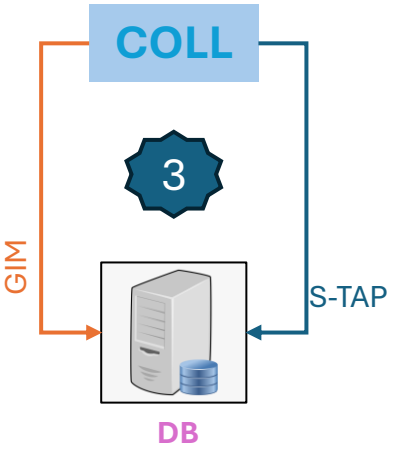
Filter status by Up Unknown Down Filter

Server name	Server IP	Module name	Status	Module version	Last response
[redacted]db01	9.[redacted]49	GIM		12.1_r120100162_1	2025-09-05 16:13:07
[redacted]db21.[redacted]m	[redacted]db21.[redacted]m	GIM		12.1.1.2_r119073_1	2025-09-05 16:12:41
[redacted]db21.[redacted]m	[redacted]db21.[redacted]	SUPERVISOR		12.1.1.2_r119073_1	2025-09-05 16:12:41

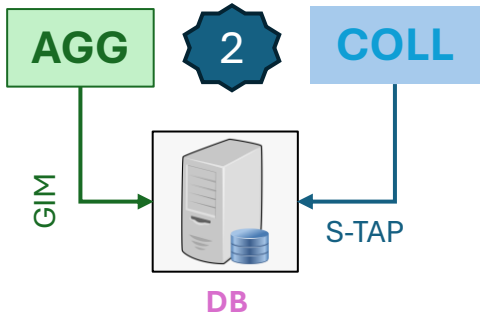
GIM Deployment Planning:



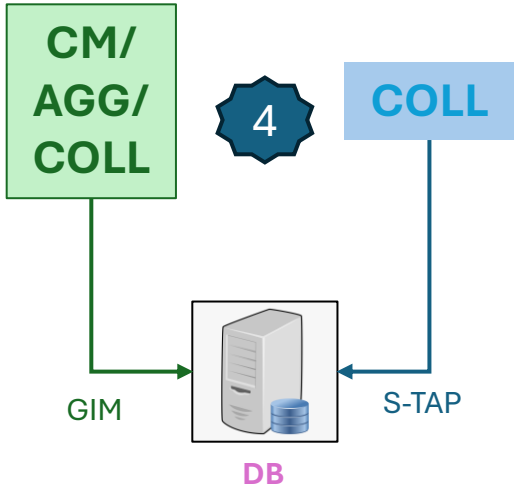
- Designate a Guardium Server
- Common Deployment Models:
  - Central Manager can act as GIM Server
    Designate an appliance as the “GIM Server”
  - Up to 4000 clients can be managed from a single server



- Fail-over Mode
  - If the GIM Server cannot be reached, the client will automatically connect to the fail-over server
  - When the original GIM server is available, the client will switch back

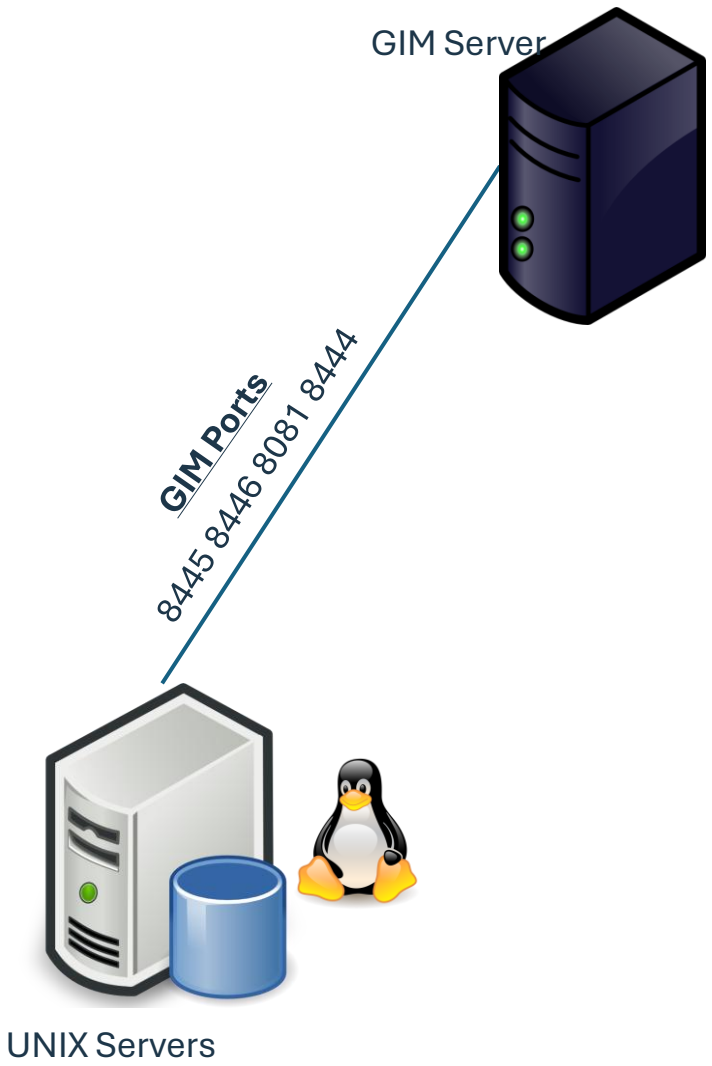


- Installation Modes
  Standard
  Listener



root or a user with root privileges will be needed for installation

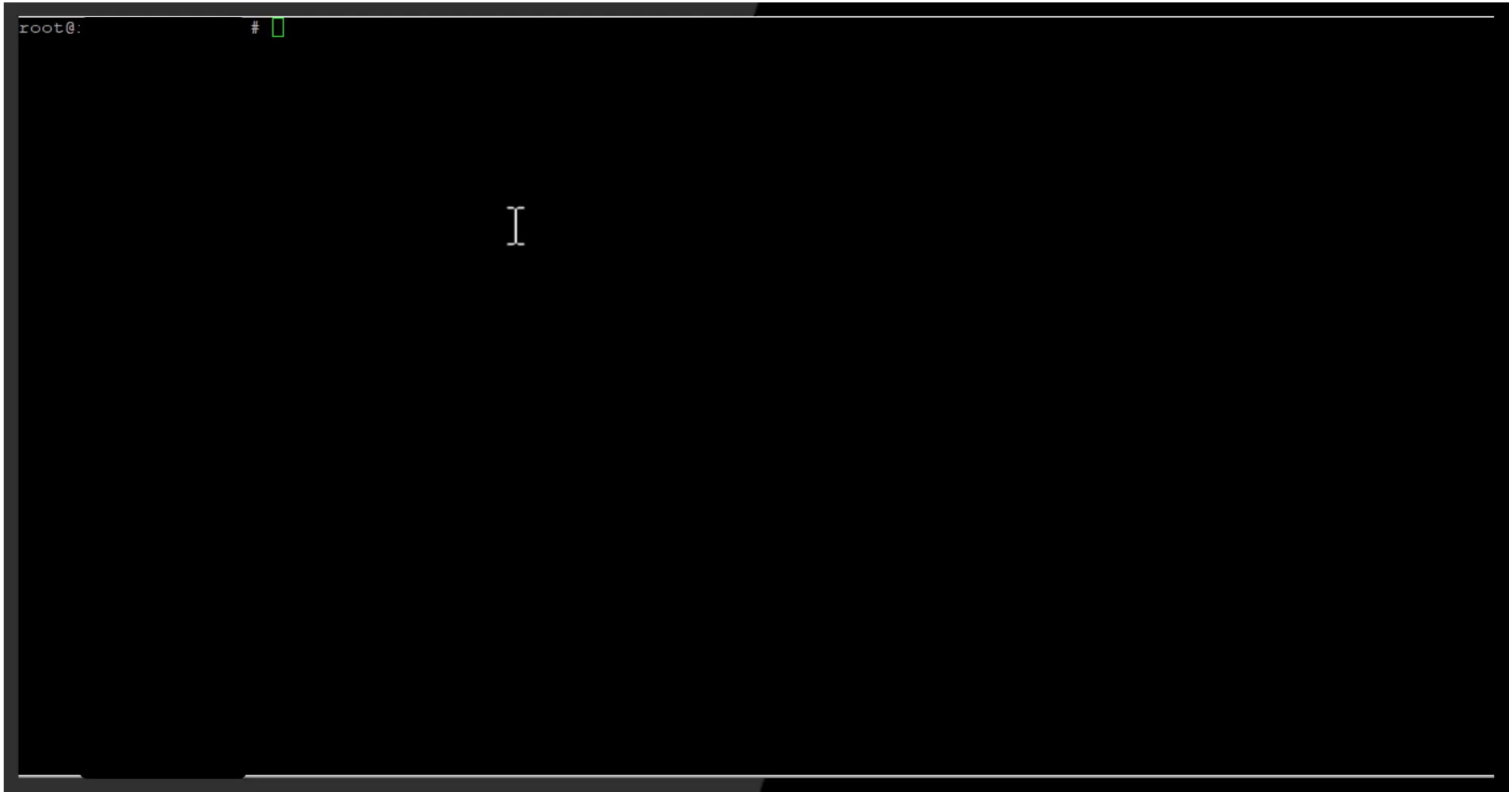
GIM Agent Requirements:



- Agent must be directly installed on DB Server
- GIM Agent = set of perl scripts
- Perl 5.8 (and up)
- root or user with root privileges
- 1 GB of space to accommodate all GIM modules
- Without FAM, 300 MB.

Port	Purpose	Direction	Conditions / Notes
8445	GIM client listener	Bidirectional	Allows communication between any GIM server (on CM or Collector) and GIM client
8446	Authenticated TLS communication	Bidirectional	Used for secure tasks like custom kernel upload and MustGather loggers upload; requires GIM_USE_SSL enabled (default in newer versions)
8444	Fallback for 8446	Bidirectional	Used if 8446 is not open; TLS without certificate verification
8081	Non-TLS communication with message signing	Bidirectional	Used when GIM_USE_SSL=0; supports custom kernel upload and MustGather loggers upload

GIM Installation:



GIM Listener Association:

GIM Uninstallation:

GIM Uninstallation (nothing else but gim):

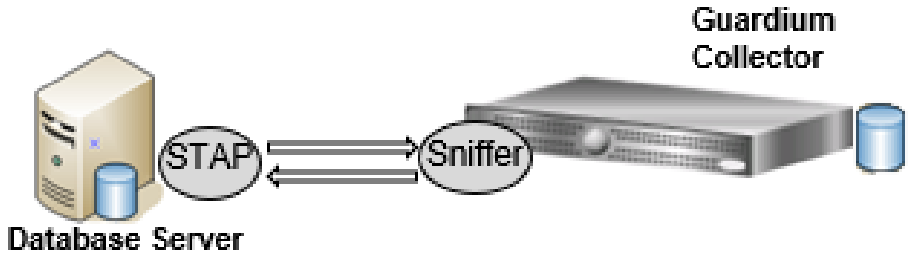
Reboot guidelines

Rebooting the database server is only required when uninstalling K-TAP (whether or not K-TAP is in use).

```
[root@ home]# ps -ef | grep gim
root        9179       1  0 10:24 ?        00:00:10 /usr/local/modules/perl /usr/local/modules/GIM/12.1.1.2_r119073_1-1757093044/gim_client.pl
root        9288    9179  0 10:24 ?        00:00:06 ../../perl ./guard_gimd.pl
root       59733   59694  0 22:12 pts/0    00:00:00 grep --color=auto gim
[root@ home]# /usr/local/modules/GIM/12.1.1.2_r119073_1-1757093044/uninstall.pl
This utility completely removes Guardium software from the system
Would you like to continue? [y/N]?y
Guardium installation directory was identified as /usr/local/modules
Removing guardium modules ...
Notifying GIM client to start uninstalling
GIM was triggered to remove all modules ... please standby (might take few minutes)
.................
Guardium software was successfully removed.
[root@ home]#
```

When there is no need of unloading ktap module there is no reboot for the OS.

What is S-TAP?



- S-TAP = Software TAP = Lightweight software agent installed on DB server
- Monitors database activities
- Minimal overhead to the DB env
- One installation on one OS node
- Expected <5% performance impact on server
- No Inspection Engine = No traffic
- auto discovery list so far includes-
  oracle:db2:informix:mysql:postgres:sybase:teradata:netezza:memsql:mariadb:verticadb
- Installation Methods: GIM, RPM, shell

Protocol	Port Range	DB Real Port
oracle	1521-1521	1521

Ip	Mask	Connect To Ip	DB User
0.0.0.0 ::	0 0	127.0.0.1,::1	oracle

DB Install Dir	Process Name
/home/oracle	/u01/app/oracle/product/19.0.0/dbhome_1/bin/oracle

Identifier
oracle_[redacted](1521,1521,DB_0)

DB Version	Inspection Engine
19	

Unix Socket Marker
EXTPROC1521

```
[root@[redacted] Guardium_12.1.2.1_S-TAP_RedHat_r119768]# ll
total 1272452
drwxrwxr-x 2 root root       4096 Jun 11 12:50 GIM_Packages
drwxrwxr-x 2 root root         41 Jun  4 18:19 Kernel_Signing
-rw-rw-r-- 1 root root      74780 Jun  4 18:19 ktaposmatch.csv
-rw-rw-r-- 1 root root       3404 Jun 12 07:45 MD5SUMS
-rw-r--r-- 1 root root 1302893425 Jun 12 06:41 modules-12.1.2.1_r119768_v12_1_1.tgz
drwxrwxr-x 2 root root       4096 Jun 11 12:48 Native_Installers
drwxrwxr-x 2 root root       4096 Jun 11 12:48 Shell_Installers
drwxrwxr-x 2 root root         57 Jun 11 12:48 Unified_Shell_Installer
```

Key Monitoring Mechanisms:

Mechanism	Description
K-TAP	Kernel-level monitoring; used when Exit Libraries are not available.
A-TAP	Application-level monitoring; supports encrypted traffic and shared memory.
Exit Libraries	Preferred method for supported databases (DB2, Informix, Teradata); integrates directly with the database for high-fidelity monitoring.
PCAP	Packet capture; least preferred due to performance overhead.

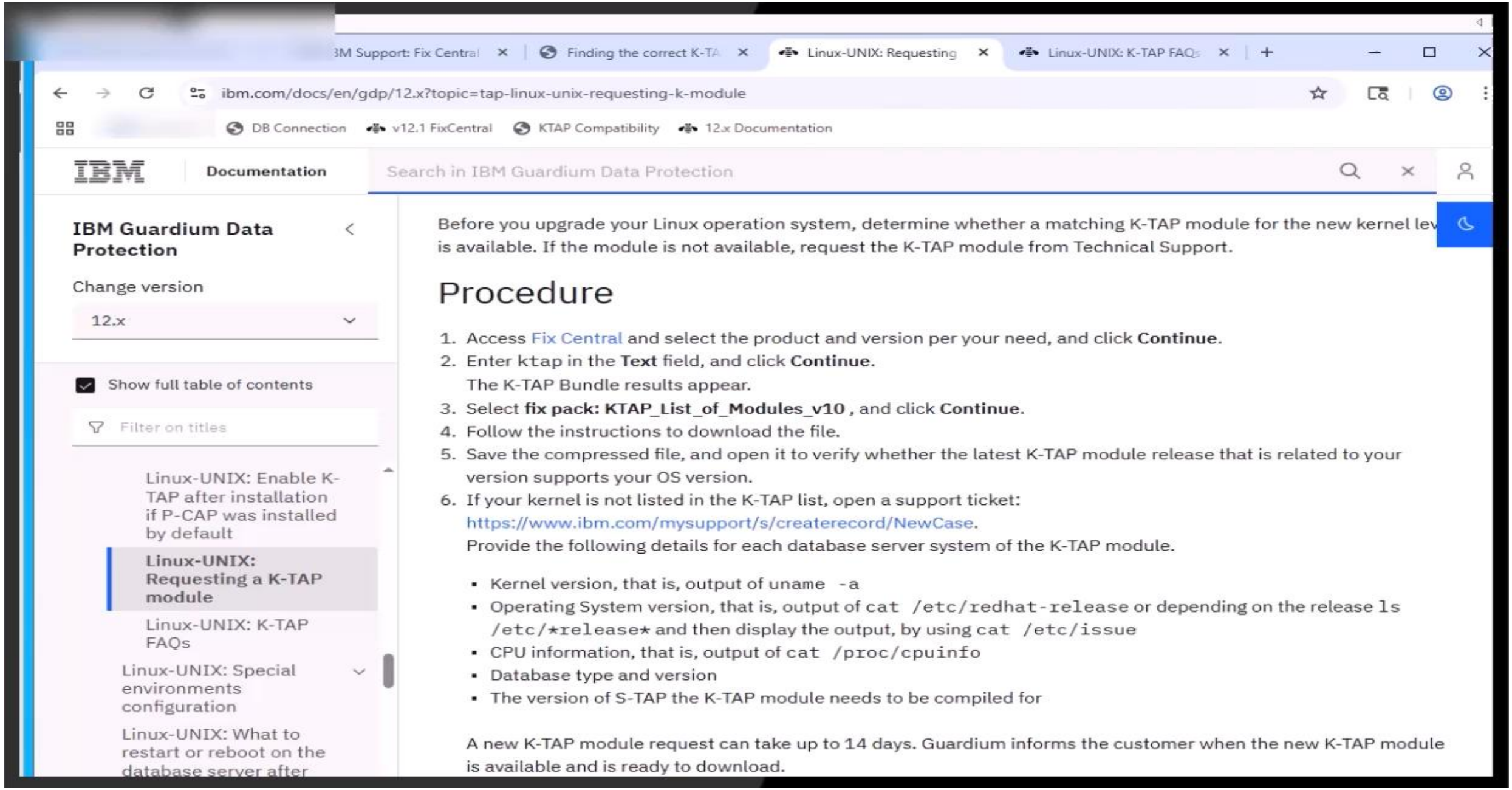
Requirements of S-TAP Installation:

Requirement	All Platforms (Linux, Solaris, AIX, HP-UX)
Essential Files	/bin/sh, /bin/sed or /usr/bin/sed
Utilities Required	tar, awk, grep, tr
Additional Files	dd and /dev/zero (HP-UX: prealloc)
Decoding Tools	uudecode in /usr/bin or /tmp; perl executable

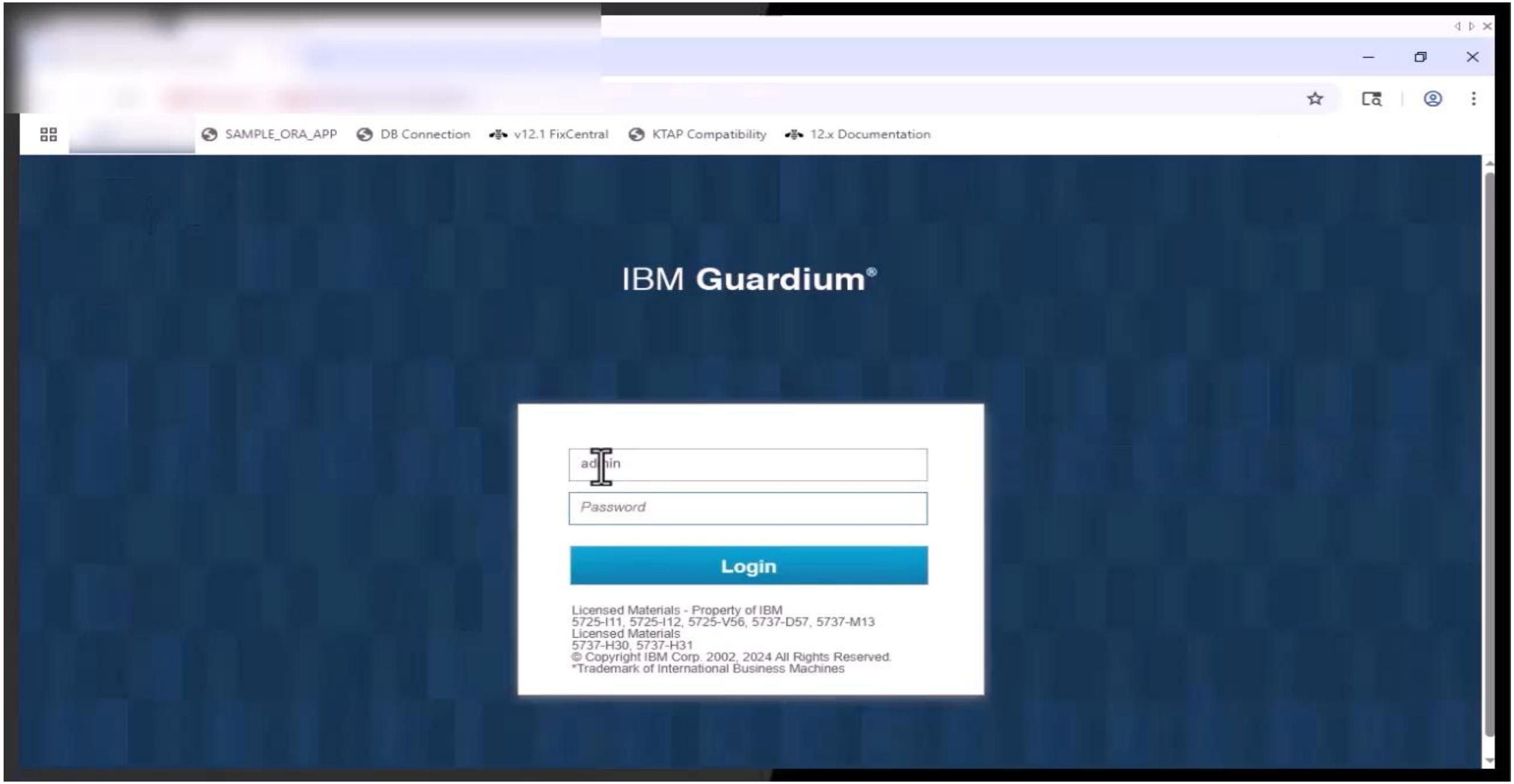
Port	Protocol	Purpose
16016	TCP	Clear S-TAP communication
16018	TLS	Encrypted S-TAP communication
16020	TCP	Regular pooled connections
16021	TLS	TLS pooled connections
16022	TCP	Feed Protocol
16023	TLS	Encrypted Feed Protocol

IBM

Find K-TAP Compatibility:



Installation of S-TAP via GIM:



STAP Uninstall & Reboot:

References:

https://www.ibm.com/docs/en/gdp/12.x?topic=guardium-installation-manager

https://www.ibm.com/docs/en/gdp/12.x?topic=gim-install-upgrade-uninstall-gim-clients-linux-unix-servers

https://www.ibm.com/docs/en/SSMPHH_12.x/com.ibm.guardium.doc.stap/gim/manage_gim_client_linux_server.html

https://www.ibm.com/docs/en/gdp/12.x?topic=gim-error-installing-guardium-installation-manager

https://www.ibm.com/docs/en/gdp/12.x?topic=guide-linux-unix-s-tap-functionality

https://www.ibm.com/docs/en/SSMPHH_12.x/com.ibm.guardium.doc.stap/stap/unix_stap_operation.html

https://www.ibm.com/docs/en/gdp/12.x?topic=lustug-linux-unix-installing-upgrading-uninstalling-s-tap-agents

https://www.ibm.com/docs/en/gdp/12.x?topic=tap-linux-unix-installing-s-agent-rpm

https://ibm.github.io/guardium-ktap/

Q&A

Any Questions?

Thank you for your attention!

- Register for-
11-September-2025
Thursday
Session 6: ibm.biz/IBMGE-S6

Reports (Entities & Attributes)

Feedback & Suggestions are welcome at:
datasec_ap_support@wwpdl.vnet.ibm.com