SupportTalk:

Troubleshooting Agents (S-TAP and GIM)

Seema Kumari & John Adams
IBM Support – Guardium Data Protection

IBM **Security**

IBM

Agenda

Overview
Why GIM?
What Do We Install?
How S-TAP works

Troubleshooting GIM
GIM Connection issues
Install Pending
Resetting a Client
MD5sum error
Installing with –x debug flag
Central_logger.log
Verify GIM Install
Uninstall GIM

Troubleshooting STAP
Running STAP diag, reading logs
Red or Missing S-TAP
Buffer overflow
Guard_tap.ini Rollback
Guardium Resource Monitor

Troubleshooting KTAP
EXIT vs. KTAP
KTAP not loading

Demo: Finding a Compatible KTAP

Introduction to the Guardium Agents:

STAP and GIM

Guardium Installation Manager

Why use GIM?

- Centrally manage all Guardium agents from one Guardium appliance.
- Separation of Roles: SysAdmins want to limit root access to the host.
  You only need root access to install GIM once.
- GIM handles all upgrades, including upgrades to GIM.

Guardium Agent Components

What do we install?

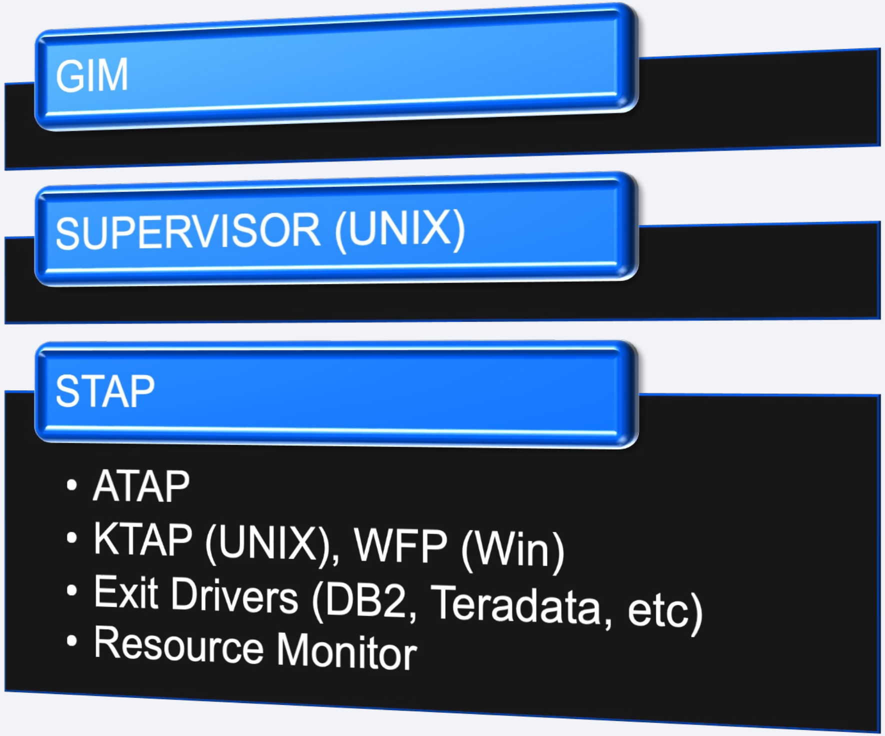
Guardium Installation Manager (GIM) handles:

- ➢ Install
- ➢ Upgrade
- ➢ Configuration
- ➢ Uninstall

Supervisor starts and stops Guardium processes on UNIX.

STAP collects data and sends it to the collector.

Resource Monitor can kill STAP and force a memory dump if CPU or other limits are exceeded.



GIM

SUPERVISOR (UNIX)

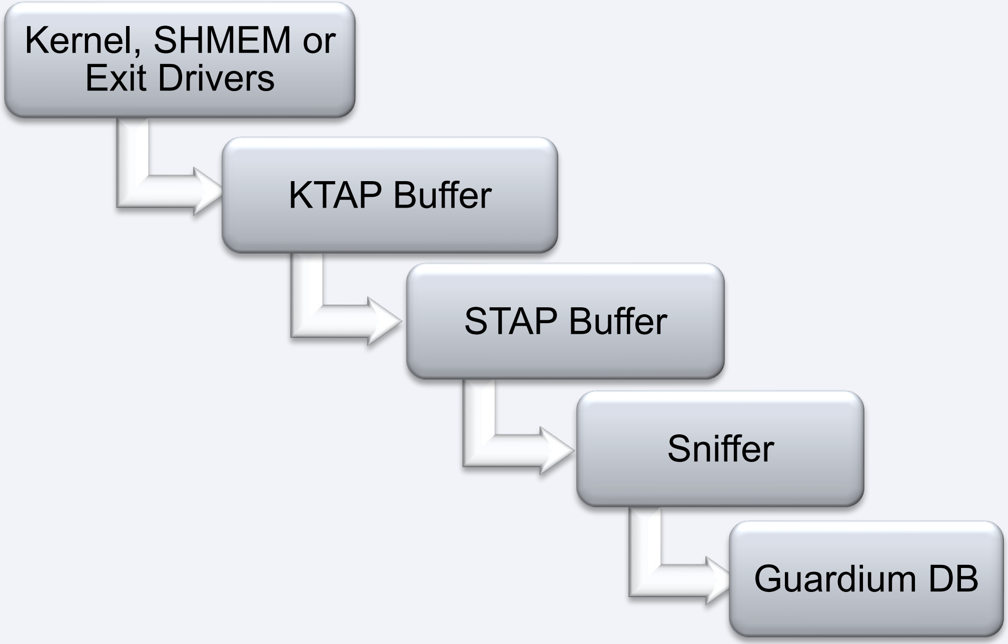
STAP

- ATAP
- KTAP (UNIX), WFP (Win)
- Exit Drivers (DB2, Teradata, etc)
- Resource Monitor

How STAP Works

Collecting and Storing Audit Data

- Lightweight agent
- Runs as a service on the DB host.
- Copies data from kernel and shared memory
- Manages the network connection to the collector
- Buffers the data stream
- All heavy processing and parsing is done on the Guardium appliance.



Troubleshooting GIM

GIM Connection Issues

What is a GIM server?

- GIM agents connect to and are managed from a Guardium appliance: the GIM Server.
- This can be any Guardium appliance, but it’s usually the CM.
- If you are concerned about performance on a CM handling too many GIM clients, designate a collector to be the GIM server.
- That collector should not handle any STAP traffic.

GIM Connection Issues

Ports

- Required Ports Documentation.
- Use native tools (nc, telnet, nslookup) to check name resolution and connectivity on the specific ports.
- Ping only proves connectivity via ICMP. Use telnet, nc or similar tools to check TCP ports.
- From CLI on the collector, “support show port open <ip> <port>” will test the connection from Guardium to the DB host.
- Check the GIM_URL parameter!
  - Windows: GIM conf file
  - UNIX: configurator.sh

GIM Connection Issues

Certificates

Custom GIM Cert Documentation.

- Used in SSL connection from agent to appliance.
- SSL is optional. Custom certs are optional.
- Will use TCP port 8446 instead of 8081
- You need ALL intermediate certificates!
- New client certs must be deployed before storing the server cert.

Check the GIM_USE_SSL parameter!

- Windows: GIM.conf file
- UNIX: configurator.sh

Stuck on “Install Pending”

It has been hours …

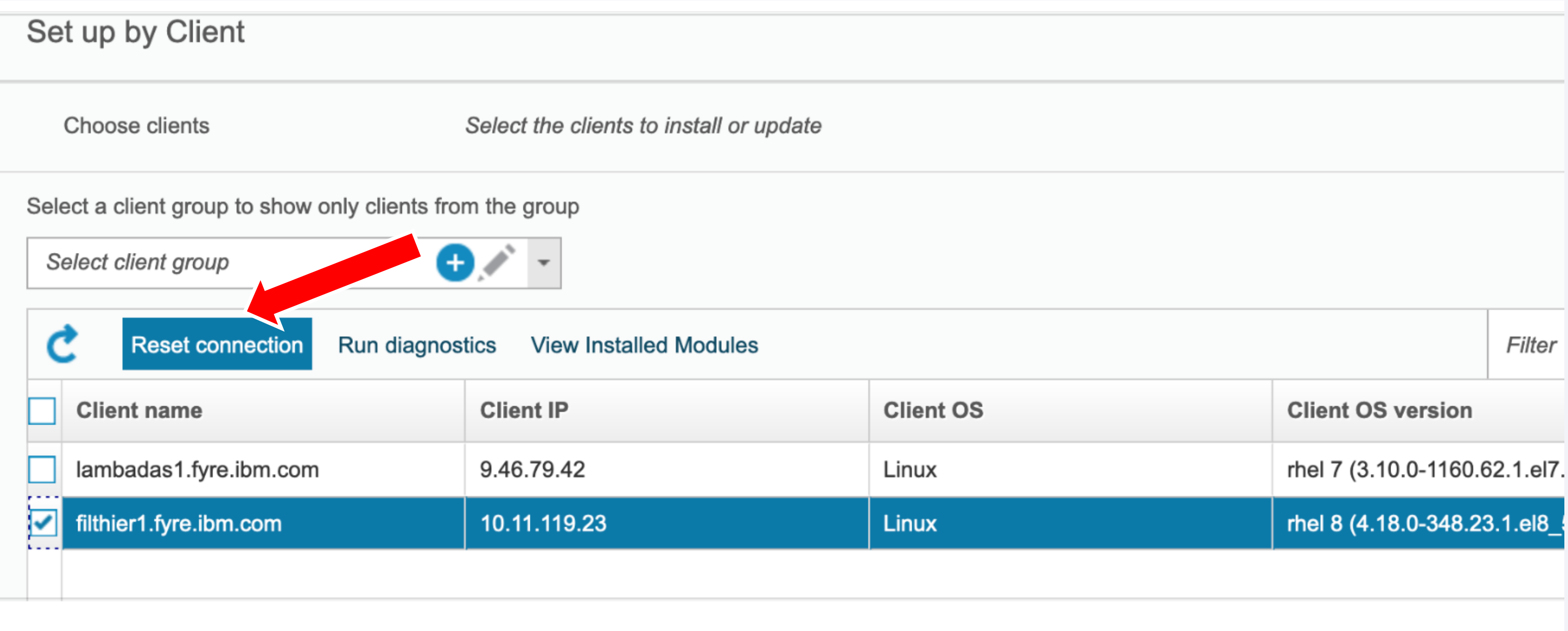
The GIM server waits for the client to poll for new updates.
This is probably a communication issue, or the client is down.

✓ Get STAP diag or check GIM.log on the host.

✓ Reset Connection from the “Setup by Client” view.

Resetting a GIM Client

Setup by Client – Reset Connection



Set up by Client

Choose clients

Select the clients to install or update

Select a client group to show only clients from the group

Select client group

☐	Client name	Client IP	Client OS	Client OS version
☐	lambadas1.fyre.ibm.com	9.46.79.42	Linux	rhel 7 (3.10.0-1160.62.1.el7.
☑	filthier1.fyre.ibm.com	10.11.119.23	Linux	rhel 8 (4.18.0-348.23.1.el8_

Resetting a GIM Client

The GIM Server caches client data …

- The client data you see in the GIM server’s GUI is reading a local cache, it might be outdated.
- The [Reset Connection] button in the “Setup by Client” view flushes the cache for selected hosts. (The button is disabled until you select 1 or more clients.)
- If the connection is good and the GIM agent is running, it will connect and send updated information to the GIM Server.
- If the host disappears from “Setup by Client” and does not return in a few seconds, there is a connection problem or the GIM client is not running.

UNIX Install throws MD5sum errors

What does it look like?

Install Command Syntax :

```
 ./<install script>  -- --dir <install_dir> --tapip <DB_SERVER IP> --sqlguardip  <GIM
Server IP> [--perl  <perl path>] [-q  ]
```

The “—” “--dir” and “—tapip” are required. The -q is for silent install, we use “which perl” if --perl is not specified.

Example of MD5sum failure:

```
root# ./guard-bundle-GIM-10.1.3_r101342_v10_1_3_1-aix-7.1-aix-powerpc.gim.sh -- --dir
/opt/guardium --sqlguardip 10.10.11.12 –tapip 10.10.35.5
```

```
Verifying archive integrity...Error in MD5 checksums:
A1C93DB63757B1BFD78B5829A79F82BF is different from c73ada0578d7e91809aab7fc301c64cb
```

MD5sum errors

Unzip the GIM install package in UNIX

If you download from Fix Central and unpack the file on your Windows workstation, it will change the MD5sum. Download the package from Fix Central again, copy it to the box where you will install GIM and unzip it there.

When you unpack the GIM bundle, you will see these files types:

guard-bundle-GIM-11.3.0.0_r111685_v11_3_1-rhel-8-linux-x86_64.gim.sh

- ➢ The *.gim.sh script used for shell installation and initial install.

guard-bundle-GIM-11.3.0.0_r111685_v11_3_1-rhel-8-linux-x86_64.gim

- ➢ The *.gim file is a GIM bundle used to upgrade GIM via the GIM Server.

GIM Install Aborts

Troubleshoot with sh -x

If your normal GIM install commands is …

```
./gim_RHEL_8_x86_64.sh -- --dir /var/gim --tapip 10.20.30.11 --sqlguardip
10.20.30.12 --perl /usr/bin
```

Try …

```
sh -x ./gim_RHEL_8_x86_64.sh -- --dir /var/gim --tapip 10.20.30.11 --sqlguardip
10.20.30.12 --perl /usr/bin | tee -a /var/tmp/gim_install_debug.txt
```

This will pipe the output of the GIM install script to a file. Errors here are very helpful in troubleshooting.

GIM Installs but Doesn’t Run

Check central_logger.log

Primary Guardium log file in UNIX:

<install path>/modules/central_logger.log

- Installer ran but encountered errors after or near the end of install
- Any issues with installing GIM bundles

```
[Thu Apr 28 14:43:13 2022] *** IN GIM RC *** :
(/opt/IBM/guardium/GIM/modules/GIM/11.3.0.0_r111685_1-
1651171392/rc install by_gim) at Thu Apr 28 14:43:13 2022

[Thu Apr 28 14:43:13 2022]  GIM client started as a service

[Thu Apr 28 14:43:13 2022]  GIM finished execution successfully
```

Verify GIM Installation

GIM and SUPERVISOR are running:

```
root# ps -aef |egrep "module|gim"

root      1217     1  0 Apr28 ?        00:00:16 /opt/IBM/guardium/GIM/modules/perl
/opt/IBM/guardium/GIM/modules/SUPERVISOR/11.3.0.0_r111685_1-
1651171397/guard_supervisor

root      4549     1  0 Apr28 ?        00:02:06 /opt/IBM/guardium/GIM/modules/perl
/opt/IBM/guardium/GIM/modules/GIM/11.3.0.0_r111685_1-1651171392/gim_client.pl

root      4661  4549  0 Apr28 ?        00:00:50 ../../perl ./guard_gimd.pl
```

Verify GIM Installation

GIM Files Installed under <installdir>/modules:

```
Root# ls -l
drwxr-x--- 3 root root   58 May  8 13:51 BUNDLE-GIM
-rw-r--r-- 1 root root 9793 May  8 13:52 central_logger.log
drwxr-x--- 3 root root   58 May  8 13:51 GIM
drwxr-x--- 3 root root   58 May  8 13:51 INIT
lrwxrwxrwx 1 root root   13 May  8 13:51 perl -> /usr/bin/perl
drwxr-x--- 3 root root   58 May  8 13:51 SUPERVISOR
drwxr-x--- 3 root root   84 May  8 13:51 UTILS
```

Uninstall GIM and STAP

Run …/modules/GIM/current/uninstall.pl

- You can also uninstall GIM from the GIM Server from the Setup by Client view.
- When you uninstall GIM, it will uninstall STAP and all Guardium agents.
- If KTAP is loaded, uninstall will not un-load it. You must reboot before installing STAP again.
- Disable ATAP before uninstalling STAP!

Note:

Uninstall Guardium agents before you decommission a DB Server to avoid inactive or orphan entries on the Guardium Appliance.

If you have inactive agents which were decommissioned, use the [Reset Connection] button in the Setup by Client view to remove a GIM client or the [X] button in the STAP Control view to remove a STAP.

Troubleshooting STAP

Must Gather

Running STAP Diag

- [How to Run STAP diag on any platform]
- Installs with STAP.
  - diag.bat (Windows)
  - guard_diag (UNIX)
- Run locally or on the STAP's collector from the STAP Control view.
- If logs are not delivered to the collector, check the host, it probably still created the diag zip file.
- Pulls together critical logs and gives a picture of the host, STAP status and key configuration files.
- We are improving diag in new STAP versions.

Must Gather

You can read STAP diag logs!

UNIX:

- central_logger.log (install and upgrade)
- GIM.log
- STAP.log
- guard_tap.ini
- verbose_debug.log (packets? encrypted?)
- modules.log (is KTAP loaded?)
- ps.log (STAP, GIM, SUPER)
- uname.log (kernel version)
- uptime.log (last reboot)
- guard_stap_analyzed_result*log (packet drops)

Windows:

- Stap.ctl (STAP errors. Check here first!)
- *.ctl files (for other drivers)
- Events.txt (Windows event log)
- System.txt (Windows OS details, KB patches list)

STAP is Red or Missing from the STAP Control View

Ports and Connectivity

- Be sure ports are open.
- Is the TAP_IP visible from the collector?
- Is the SQLGUARD_IP visible from the host?
- If you used hostnames, do they resolve correctly?
- Is the STAP running? If you start it, does it stay up?
- CLI> support show ports open <ip> <port>
- Use telnet, nc, nmap, netstat and similar tools on the DB host.

Windows STAP restarts frequently

Check the Guardium Resource Monitor!

Guardium Resource Monitor runs as a service on Windows.

- ➢ Stop the service and see if STAP stabilizes, connects and turns green on the collector.
- ➢ If it does, ResMon is killing STAP!
- ➢ You can adjust the restart thresholds in resmon.ini in the STAP install directory.
- ➢ Sometimes the defaults are too low for powerful production systems.

Problems With guard_tap.ini

Symptoms:

- You update an Inspection Engine. A few seconds later the changes disappear.
- There are many recent copies of guard_tap.ini in the STAP install directory. (*.err, *.bak)
- STAP will not start, with errors like this in the STAP.log or central_logger.log:

```
[Thu Aug 12 10:43:39 2021] -I- Sending STATUS msg to server (-1,STAP is
not running ! Failure reason :
fgets: Error 0
fgets: Error 0
/opt/IBM/guardium/modules/STAP/10.6.0.4_r108055_1-
1593585312/guard_tap.ini line 0: Inifile read error, SPECIAL_OPS=>)
```

Problems With guard_tap.ini

Solution:

- List …/modules/STAP/current/guard_tap.* and check the file dates and extensions.
- Rename guard_tap.ini and replace it with the last good INI file.
- Try removing all Inspection Engines from the INI file. Save and restart STAP.

Any kind of corruption will cause STAP to abort and try to rollback the INI file. Usual suspects:

- db_install_dir=<wrong value, not found>
- db_exec=<wrong value, not found>
- wait_for_db_exec=0

Troubleshooting KTAP

EXIT vs KTAP

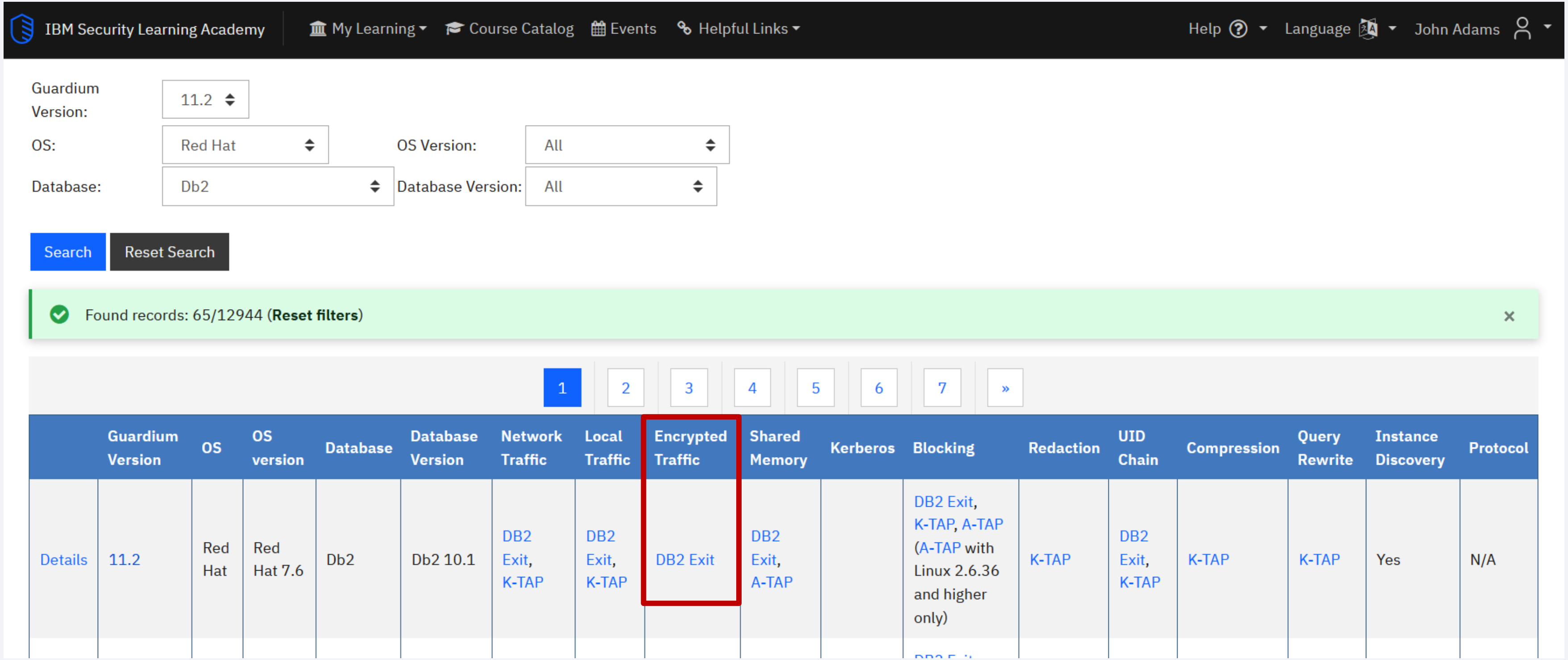
Use EXIT libraries when available. (Currently not available for Oracle.)

Advantages of using EXIT over KTAP

- ➢ It is not dependent on KTAP compatibility, less to worry about kernel upgrade
- ➢ does not require ATAP to monitor encrypted traffic, EXIT supports all traffic
- ➢ no need to worry about server reboot after uninstalling STAP because KTAP is not used
- ➢ no risk of server crashes due to Guardium, without KTAP our software only uses user space

EXIT vs KTAP

Supported Platforms Database for Data Activity Monitoring



Guardium Version: 11.2

OS: Red Hat

OS Version: All

Database: Db2

Database Version: All

Found records: 65/12944 (**Reset filters**)

	Guardium Version	OS	OS version	Database	Database Version	Network Traffic	Local Traffic	Encrypted Traffic	Shared Memory	Kerberos	Blocking	Redaction	UID Chain	Compression	Query Rewrite	Instance Discovery	Protocol
Details	11.2	Red Hat	Red Hat 7.6	Db2	Db2 10.1	DB2 Exit, K-TAP	DB2 Exit, K-TAP	DB2 Exit	DB2 Exit, A-TAP		DB2 Exit, K-TAP, A-TAP (A-TAP with Linux 2.6.36 and higher only)	K-TAP	DB2 Exit, K-TAP	K-TAP	K-TAP	Yes	N/A

KTAP not Signed for Exadata Secure Boot

What does it look like?

- No traffic from STAP
- Check modules.log in STAP diag, KTAP is not loaded.
- Error in central_logger.log:

```
modprobe: ERROR: could not insert 'ktap': Operation not permitted
[26880.290412] PKCS#7 signature not signed with a trusted key
…
[26880.296693] Lockdown: Loading of module with unavailable key is restricted;
see man kernel_lockdown.7
--- DMESG END ---
```

Solution: Secure Boot Signing in Exadata

Compatible KTAP

What should it look like?

- Traffic from STAP, KTAP loaded.
- Central_logger.log:

```
Searching for module files in /opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_1-
1651175743/modules-*.tgz
Using modules file /opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_1-
1651175743/modules-11.3.0.0_r111685_v11_3_1.tgz
guard_ktap_loader:
b305d5e334aaf51a3133524e387a2329  /opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_1
-1651175743/modules-11.3.0.0_r111685_v11_3_1.tgz
Module ktap-11.3.0.0_r111685_v11_3_1-rh7u4x64m-3.10.0-1160.31.1.el7.x86_64-x86_64-
SMP.ko selected for kernel 3.10.0-1160.31.1.el7.x86_64.
…
guard_ktap_loader: Retpoline kernel and module - OK
guard_ktap_loader: Install OK
guard_ktap_loader: Load OK
```

Best fit KTAP with Kernel

What does it look like?

- No traffic from that STAP, KTAP not loaded.

- Central_logger.log:

```
Searching for module files in /usr/local/guardium/modules/KTAP/11.1.0.11_r111160_1-
1650958591/modules-*.tgz
Using modules file /usr/local/guardium/modules/KTAP/11.1.0.11_r111160_1-
1650958591/modules-11.1.0.11_r111160_v11_1_1.tgz
…
File /lib/modules/4.18.0-305.40.2.el8_4.x86_64/build/.config not found.  Local build of
KTAP will not be attempted.  Please install kernel development packages for 4.18.0-
305.40.2.el8_4.x86_64 if you wish to build KTAP locally.
…best fit module for 4.18.0-305.40.2.el8_4.x86_64 is ktap-11.1.0.11_r111160_v11_1_1-
oe8u2x64m-4.18.0-305.10.2.el8_4.x86_64-x86_64-SMP.ko
…
guard_ktap_loader: Install OK
guard_ktap_loader: Load OK
```

Locally Build KTAP

What does it look like?

- No traffic from that STAP, KTAP not loaded.

- Central_logger.log:

```
Thu Apr 28 17:11:17 2022] Searching for module files in
/opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_1-1651175743/modules-*.tgz
guard_ktap_loader: Using modules file
/opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_1-1651175743/modules-
11.3.0.0_r111685_v11_3_1.tgz
guard_ktap_loader:
b305d5e334aaf51a3133524e387a2329  /opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_1
-1651175743/modules-11.3.0.0_r111685_v11_3_1.tgz
guard_ktap_loader: Attempting to build KTAP module using dir /lib/modules/3.10.0-
1160.62.1.el7.x86_64/build
guard_ktap_loader: Custom module ktap-111685-rhel-7-linux-x86_64-xCUSTOMxlambadas1-
3.10.0-1160.62.1.el7.x86_64-x86_64-SMP.ko built for kernel 3.10.0-1160.62.1.el7.x86_64.
guard_ktap_loader: Install OK
guard_ktap_loader: Load OK
[Thu Apr 28 17:11:17 2022] -I- KTAP finished execution successfully
```

No KTAP to load

What does it look like?

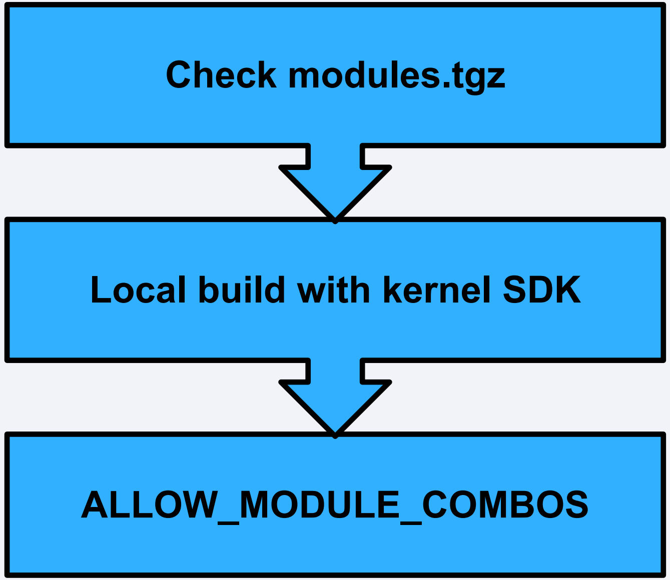
- No traffic from that STAP, KTAP not loaded.
- Central_logger.log:

```
[Thu Apr 22 12:47:46 2021] -I- Failure point : update (Can't update KTAP-
11.0.0.0_r107032_815-1608026660 :
Searching for modules in /u01/app/DID/modules/KTAP/11.0.0.0_r107032_815-
1608026660/modules-*.tgz
guard_ktap_loader: File /lib/modules/3.10.0-1160.11.1.el7.x86_64/build/.config not
found. Local build of KTAP will not
guard_ktap_loader: be attempted. Please install kernel development packages for 3.10.0-
1160.11.1.el7.x86_64 if you wish
guard_ktap_loader: to build KTAP locally.
guard_ktap_loader: ==================================================================
guard_ktap_loader: We cannot provide a module for the running kernel and no close
guard_ktap_loader: fitting combination was found. Please contact IBM and provide the
guard_ktap_loader: following information:
```

KTAP not Compatible with Kernel

How do I prevent it?

- ✓ Stay up to date on the latest STAP and KTAP bundles
- ✓ Use the tool on Security Learning Academy
- ✓ Download the KTAP list on Fix Central
- ✓ Upgrade to the latest KTAP Bundle from Fix Central
- ✓ Use KTAP_ALLOW_MODULE_COMBOS=Y
- ✓ If a new kernel is not supported yet, contact IBM.
- ✓ Consider building a custom KTAP
- ✓ Technote



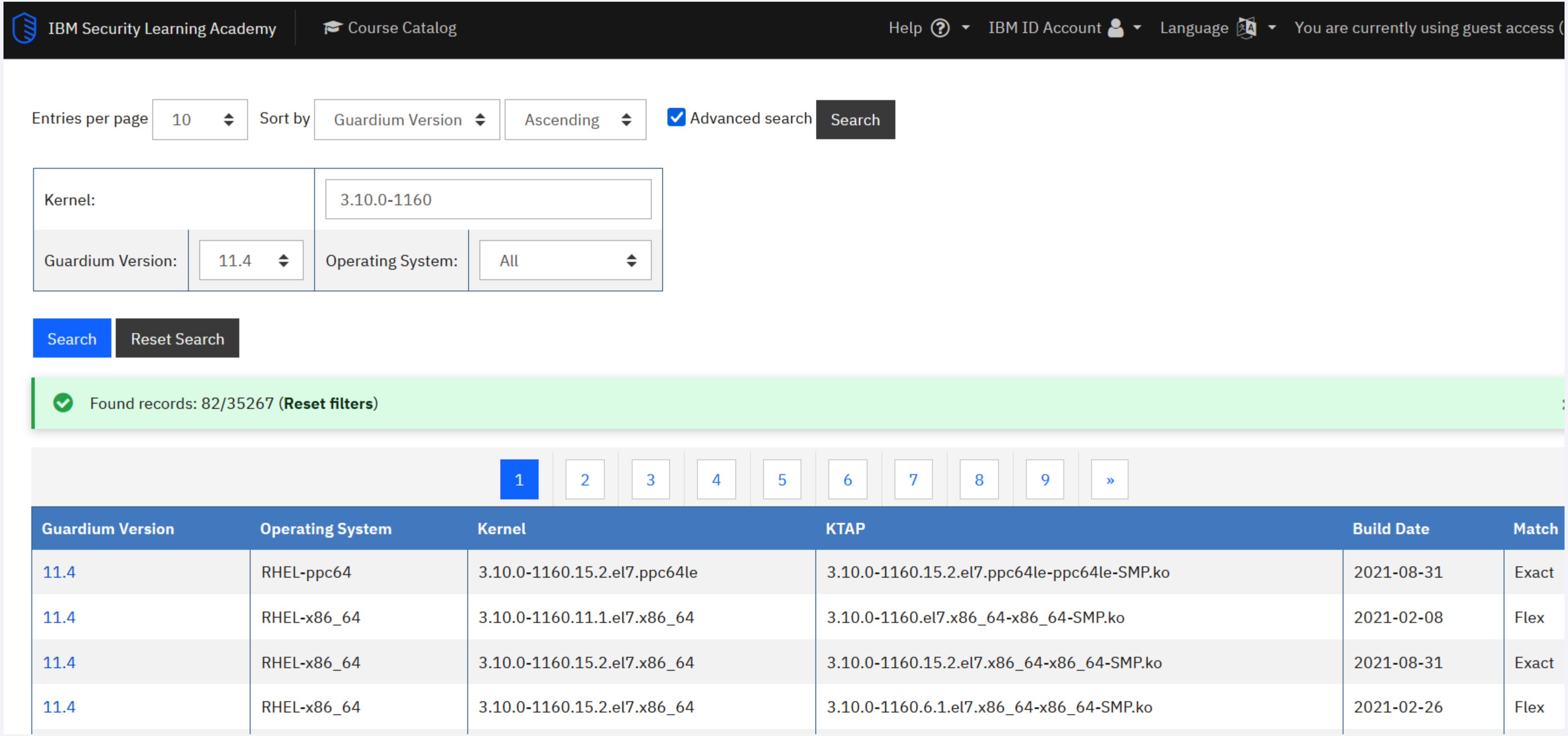
Check modules.tgz

Local build with kernel SDK

ALLOW_MODULE_COMBOS

Demo: Finding a Compatible KTAP

Check the Security Learning Academy


IBM Security Learning Academy
Course Catalog
Help
IBM ID Account
Language
You are currently using guest access (

Entries per page: 10

Sort by: Guardium Version, Ascending

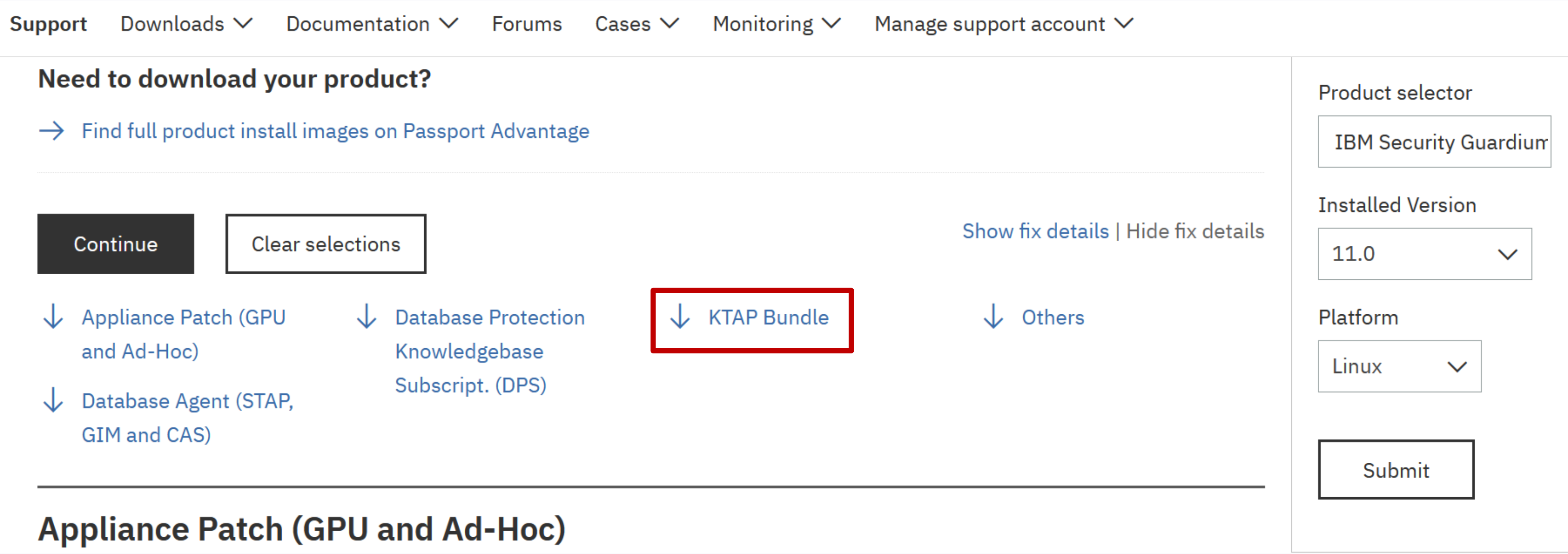
☑ Advanced search

Kernel:	3.10.0-1160		
Guardium Version:	11.4	Operating System:	All

Found records: 82/35267 (**Reset filters**)

Guardium Version	Operating System	Kernel	KTAP	Build Date	Match
11.4	RHEL-ppc64	3.10.0-1160.15.2.el7.ppc64le	3.10.0-1160.15.2.el7.ppc64le-ppc64le-SMP.ko	2021-08-31	Exact
11.4	RHEL-x86_64	3.10.0-1160.11.1.el7.x86_64	3.10.0-1160.el7.x86_64-x86_64-SMP.ko	2021-02-08	Flex
11.4	RHEL-x86_64	3.10.0-1160.15.2.el7.x86_64	3.10.0-1160.15.2.el7.x86_64-x86_64-SMP.ko	2021-08-31	Exact
11.4	RHEL-x86_64	3.10.0-1160.15.2.el7.x86_64	3.10.0-1160.6.1.el7.x86_64-x86_64-SMP.ko	2021-02-26	Flex

Fix Central



Need to download your product?

→ Find full product install images on Passport Advantage

- Appliance Patch (GPU and Ad-Hoc)
- Database Agent (STAP, GIM and CAS)
- Database Protection Knowledgebase Subscript. (DPS)
- KTAP Bundle
- Others

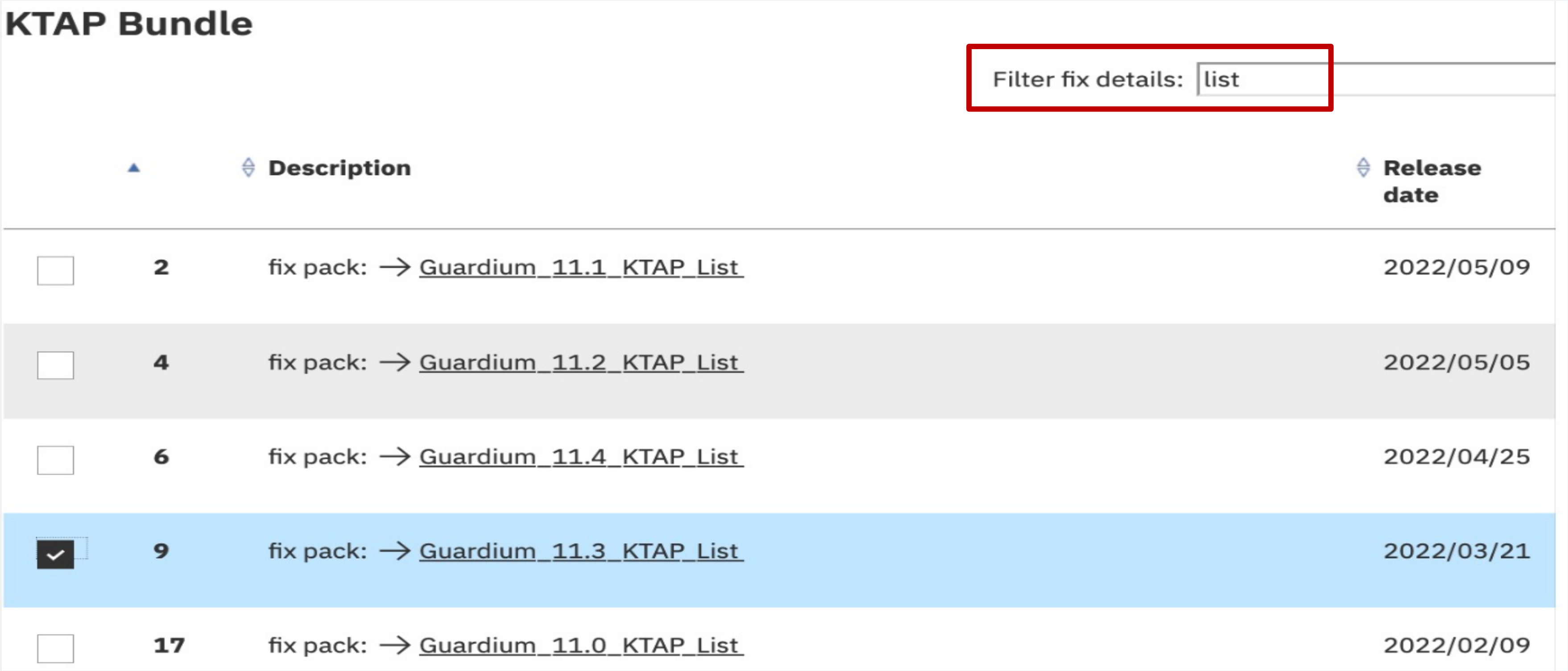
Product selector: IBM Security Guardium

Installed Version: 11.0

Platform: Linux

Appliance Patch (GPU and Ad-Hoc)

Fix Central – KTAP Lists

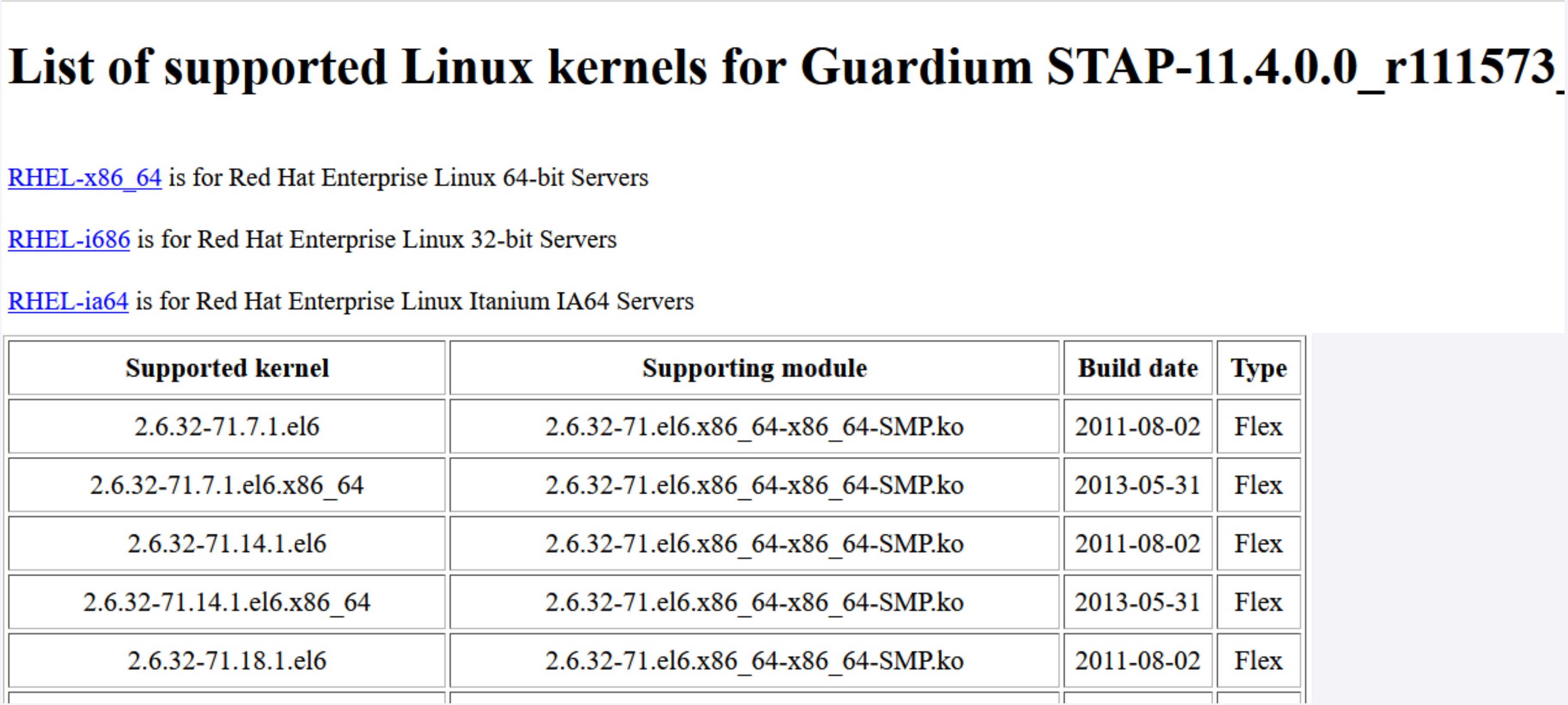


KTAP Bundle

Filter fix details: list

	▲	◆ Description	◆ Release date
□	2	fix pack: → Guardium_11.1_KTAP_List	2022/05/09
□	4	fix pack: → Guardium_11.2_KTAP_List	2022/05/05
□	6	fix pack: → Guardium_11.4_KTAP_List	2022/04/25
☑	9	fix pack: → Guardium_11.3_KTAP_List	2022/03/21
□	17	fix pack: → Guardium_11.0_KTAP_List	2022/02/09

KTAP List (HTML)



List of supported Linux kernels for Guardium STAP-11.4.0.0_r111573_

RHEL-x86_64 is for Red Hat Enterprise Linux 64-bit Servers

RHEL-i686 is for Red Hat Enterprise Linux 32-bit Servers

RHEL-ia64 is for Red Hat Enterprise Linux Itanium IA64 Servers

Supported kernel	Supporting module	Build date	Type
2.6.32-71.7.1.el6	2.6.32-71.el6.x86_64-x86_64-SMP.ko	2011-08-02	Flex
2.6.32-71.7.1.el6.x86_64	2.6.32-71.el6.x86_64-x86_64-SMP.ko	2013-05-31	Flex
2.6.32-71.14.1.el6	2.6.32-71.el6.x86_64-x86_64-SMP.ko	2011-08-02	Flex
2.6.32-71.14.1.el6.x86_64	2.6.32-71.el6.x86_64-x86_64-SMP.ko	2013-05-31	Flex
2.6.32-71.18.1.el6	2.6.32-71.el6.x86_64-x86_64-SMP.ko	2011-08-02	Flex

Search for Your Kernel

Match the First Four!

uname –a:

Linux testsev1.xx.xxx.com **3.10.0-1160.62.1.el7.x86_64** #1 SMP

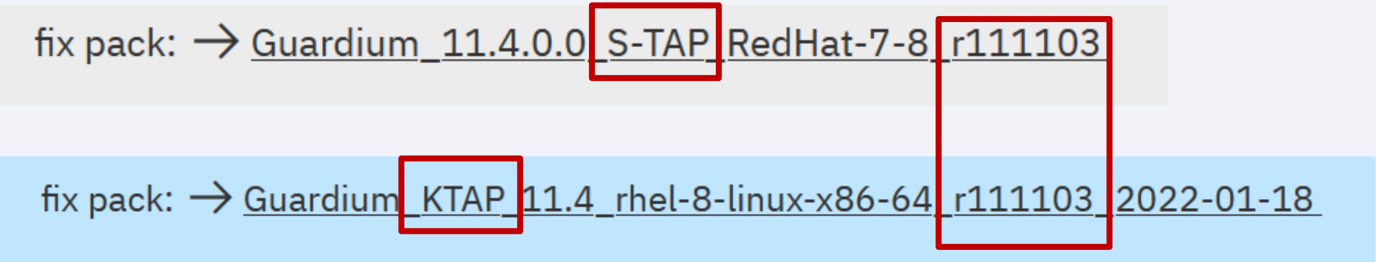
ALLOW_MODULE_COMBOS=Y will match any **3.10.0-1160.**

If ALLOW_MODULE_COMBOS=N the full kernel must match exactly.

KTAP Bundles

What is a KTAP Bundle?

- a complete STAP installer for native or GIM install
- upgrade over existing STAP with the same or lower version
- use it to install STAP for the first time
- contains the latest *.ko files: the KTAP you need!



fix pack: → Guardium_11.4.0.0_S-TAP_RedHat-7-8_r111103

fix pack: → Guardium_KTAP_11.4_rhel-8-linux-x86-64_r111103_2022-01-18

Questions?

Technotes, Training and Other Resources

Dive deeper with these links …

Master Class: GIM and STAP Installation (Avi Walarius 2020)

Doc: Signing KTAP for Exadata Secure Boot

Lab: Install STAP using GIM

Doc: How to run STAP diag for all platforms and versions

Open Mic: Installation and Deployment using GIM

Does STAP Support My New Linux Kernel?

Guardium Supported Platforms Database (v11)

When to Reboot or Restart the DB

Network Port Requirements

IBM Security **Learning Academy**

www.SecurityLearningAcademy.com

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

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

IBM