SupportTalk:
How to build custom KTAP for Linux STAP

Seema Kumari
IBM Support – Guardium Data Protection

August 2022

IBM **Security**

Agenda

Custom KTAP
What is custom KTAP?
What are the advantages of compiling custom KTAP
How to compile custom KTAP?
How to distribute and use it on other DB Servers ?

Understanding Linux KTAP Installation workflow

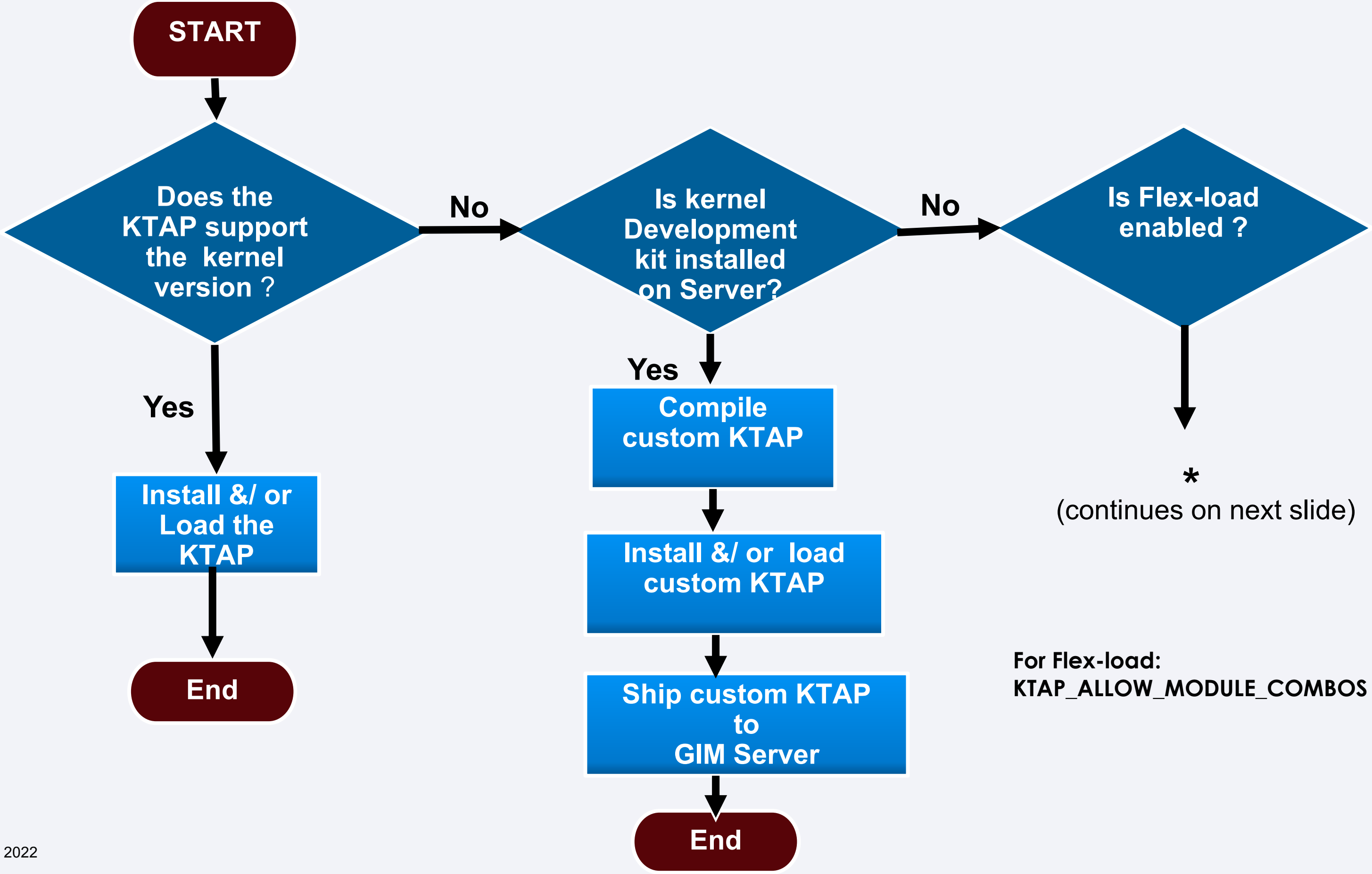
Preparing DB Server for Linux Kernel Upgrade

Reviewing central_logger.log for KTAP Installation & loading related messages

For Reference:
How to verify if your kernel version is supported?
How to use configurator utility?
Collecting STAP/ KTAP diagnostics

Linux STAP – KTAP module installation Workflow

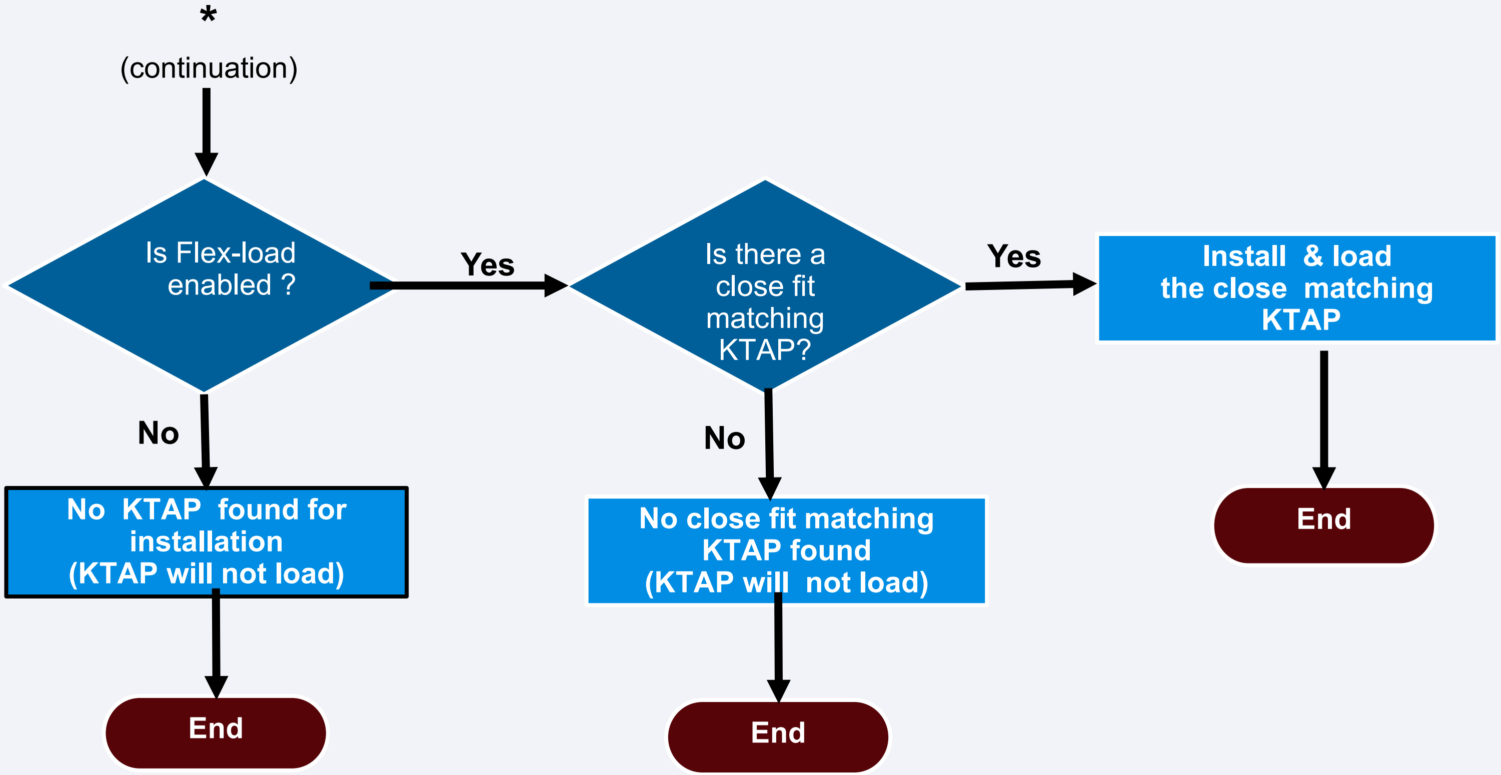
Linux STAP - KTAP module Installation Workflow


START
Does the KTAP support the kernel version ?
No
Is kernel Development kit installed on Server?
No
Is Flex-load enabled ?
Yes
Install &/ or Load the KTAP
End
Yes
Compile custom KTAP
Install &/ or load custom KTAP
Ship custom KTAP to GIM Server
End
*

(continues on next slide)

For Flex-load:
KTAP_ALLOW_MODULE_COMBOS is set to "Y"

…Linux STAP - KTAP module Installation Workflow



*

(continuation)

Is Flex-load enabled ?

Yes

Is there a close fit matching KTAP?

Yes

Install & load the close matching KTAP

End

No

No KTAP found for installation (KTAP will not load)

End

No

No close fit matching KTAP found (KTAP will not load)

End

Advantages of Compiling Custom KTAP

Advantages of compiling Custom KTAP

- Nothing to worry about KTAP compatibility on upgrading Linux kernel
- There is no need to wait for 10-15 days to get a compatible KTAP module supporting your kernel version.
- If you install the kernel development packages and other required utilities on the Production GIM Clients, you do not have to push for new STAP bundle for installation. Everything is taken care automatically.
- You can compile the custom KTAP on one DB Server and distribute it to other DB Servers using same kernel version

Compiling A Custom KTAP

Preparing to Compiling Custom module

If you do not want to wait 2-3 weeks for an updated KTAP module from IBM, you can set up for automatic KTAP compilation.

For custom KTAP compilation, it requires following components to be installed on the DB Server.

- Kernel development packages for the kernel version you are planning to upgrade to
- make utility
- gcc complier

When the DB Server reboots following the kernel upgrade, STAP detects the kernel change.

- If a matching KTAP is not found in the bundle, it will compile one and use it, assuming kernel development packages and other required utilities (like make, gcc compiler) are installed on the DB Server.

- It also ships the built custom KTAP to the GIM Server when parameter “upload_feature” in guard_tap.ini file is enabled, by default this parameter is enabled (i.e. set to 1).

Note:

Main KTAP code is already precompiled and shipped with the STAP installer. During the custom KTAP compilation, it complies only a very small kernel specific portion and for this it takes less than a minute to complete this compilation.

Cannot install Kernel Development kit / Compiler on Production Server?

- If Company policy does not allow to install kernel development packages and /or compilers on the Production Servers, you can prepare a test DB Server for automatic custom KTAP compilation.

- To prepare the test DB Server for automatic custom KTAP compilation all you need is
  - install exact same kernel version that you plan to upgrade the Production Sever to
  - install kernel development packages for that kernel version and other required utilities (make , gcc compiler)
  - and simply install the same bundle STAP that is used in Production Server.

Preparing DB Server
For Kernel Upgrade

Preparing DB Server for Kernel Upgrade

1. Prepare a test DB Server using exact same kernel patch that is scheduled for Linux Production Server upgrade.
2. Install all required packages for custom KTAP module compilation. (kernel SDK, make, gcc compiler)
3. Install Bundle S-TAP on the test DB Server using the same bundle that is used in Production Server.
4. Verify that custom KTAP is compiled and loaded on the test DB Server.
5. Verify new Custom Bundle is available on the GIM Server that is used for this test Server Installation
6. Distribute new Custom Bundle to the Production GIM Server(s).
7. Install the new Custom Bundle STAP on all Production Servers that is planned to be patched to upgrade the kernel.

Message related to shipping of custom KTAP

- On DB Server where custom KTAP is compiled, you will see message similar to following logged in the syslog.

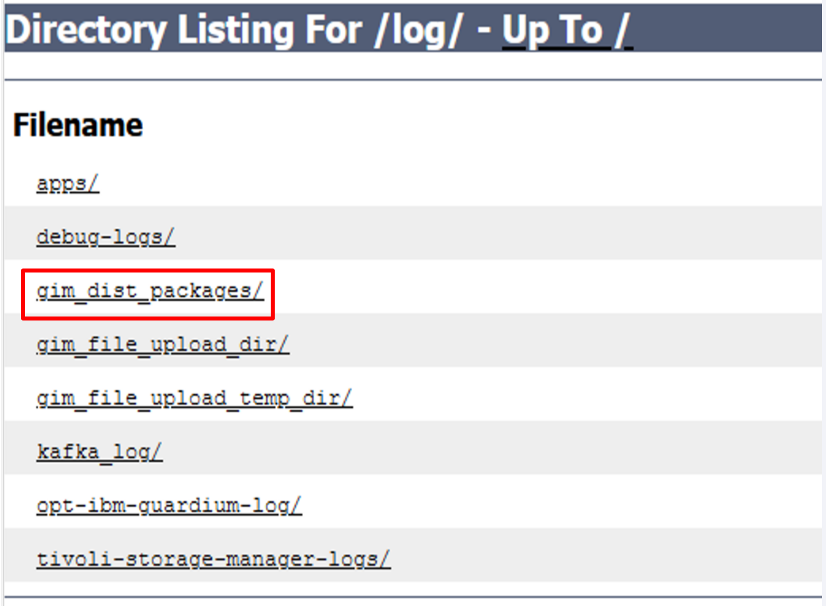
```
….
guard_tap[7630]: STAP_DAM INFO 468: tap_sendfiles.cc(337): file /usr/local/guardium/guard_stap/.upload/ktap-112874-rhel-7-linux-x86_64-xCUSTOMxrac181-4.1.12-124.23.2.el7uek.x86_64-x86_64-SMP.ko has been successfully sent to gimserver
```

Note:

Make a note of the custom bundle STAP version that gets created on the GIM Server supporting specific kernel version.

Custom KTAP distribution

- Custom bundle STAP can be distributed from one GIM Server to other GIM Servers
- custom bundle can be downloaded from GIM Server using fileserver.
- The custom bundle STAP can be found under **gim_dist_packages** folder, using fileserver



Directory Listing For /log/ - Up To /

Filename

apps/
debug-logs/
gim_dist_packages/
gim_file_upload_dir/
gim_file_upload_temp_dir/
kafka_log/
opt-ibm-guardium-log/
tivoli-storage-manager-logs/

What KTAP is in use?

How to know what KTAP is being used ?

- You can check in GUI, GIM Events List and GIM Clients Status reports
- You can also cd to KTAP folder and check where the soft link ”current” is pointing to, it shows what KTAP is being used,
- For example:

```
[root@testdb2 ~]# cd /opt/IBM/guardium/GIM/modules/KTAP
 [root@lambadas1 KTAP]# ls -l
 total 8
 drwxr-x--- 3 root root 4096 Apr 28 17:11 11.3.0.0_r111685_1-1651175743
 drwxr-x--- 3 root root 4096 Aug  2 01:04 11.3.0.0_r111685_800-1651180811
 lrwxrwxrwx 1 root root   66 Apr 28 17:20 current -> /opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_800-1651180811
 lrwxrwxrwx 1 root root   64 Apr 28 17:20 prev -> /opt/IBM/guardium/GIM/modules/KTAP/11.3.0.0_r111685_1-1651175743
```

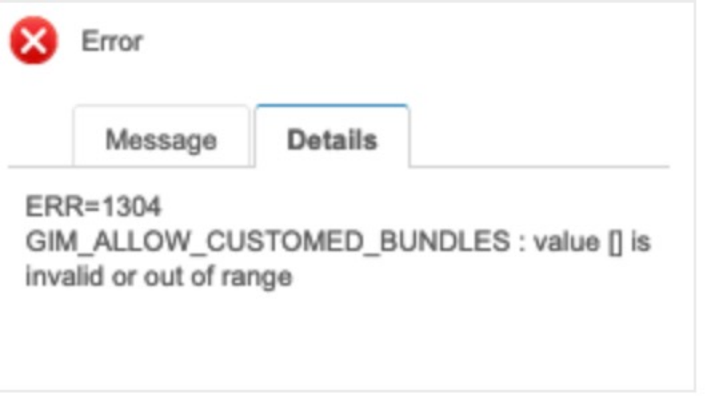
Here, we can see, the soft link “current” is pointing to a custom KTAP

Parameter controlling the use of Custom Bundle

GIM_ALLOW_CUSTOMED_BUNDLES

Installing Custom Bundle

- Installation of Custom Bundle is not allowed by default.
- Attempting to install custom bundle will fail without enabling GIM_ALLOW_CUSTOMED_BUNDLES



```
ERR=1304
GIM_ALLOW_CUSTOMED_BUNDLES : value [] is
invalid or out of range
```

PARAMETER GIM_ALLOW_CUSTOMED_BUNDLES

- Parameter GIM_ALLOW_CUSTOMED_BUNDLES controls the use of custom KTAP/ custom bundle STAP
- It can be set to 1 (enable) , or 0 (disable)
- This parameter can be enabled
    - either during fresh GIM installation by specifying –install_custom_bundles
    - Or, by the DB admin on the DB Server using the configurator utility
        - To verify: <full path>/configurator.sh --get GIM |grep GIM_ALLOW
        - To enable: <full_path>/configurator.sh –set GIM_ALLOW_CUSTOMED_BUNDLED 1
- It cannot be enabled from the GUI, but you can disable it from the GUI.
- You can use custom bundle STAP for installation only if the parameter GIM_ALLOW_CUSTOMED_BUNDLES is enabled.
- Distributed bundle with custom KTAP has _8xx number attached to the version, like 800, 801, 802, etc
    - For example:
      custom bundle STAP (STAP bundle that includes custom KTAP) **11.3.0.0_r111685**_800

Reviewing central_log.log for KTAP install/ load related messages

Case# 1: Found a KTAP matching to the kernel version

- In central_logger.log, look for the keyword “**Searching**”

```
[Thu Apr 28 15:56:16 2022] -I- Starting STAP (if enabled)
[Thu Apr 28 15:56:16 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: 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: Extracted module ktap-11.3.0.0_r111685_v11_3_1-rh7u4x64m-3.10.0-1160.31.1.el7.x86_64-x86_64-SMP.ko from /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: Retpoline kernel and module - OK
guard_ktap_loader: Install OK
guard_ktap_loader: Load OK
[Thu Apr 28 15:56:16 2022] -I- KTAP finished execution successfully
[Thu Apr 28 15:56:16 2022] *** OUT KTAP RC ***

[Thu Apr 28 15:56:16 2022] -I- STAP can be started immediately
```

Case# 2: No matching KTAP, but Kernel SDK is installed

- From <GIM installdir>/modules/**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
[Thu Apr 28 17:11:17 2022] *** OUT KTAP RC ***
[Thu Apr 28 17:11:17 2022] -I- Module KTAP was started successfully.

…..
```

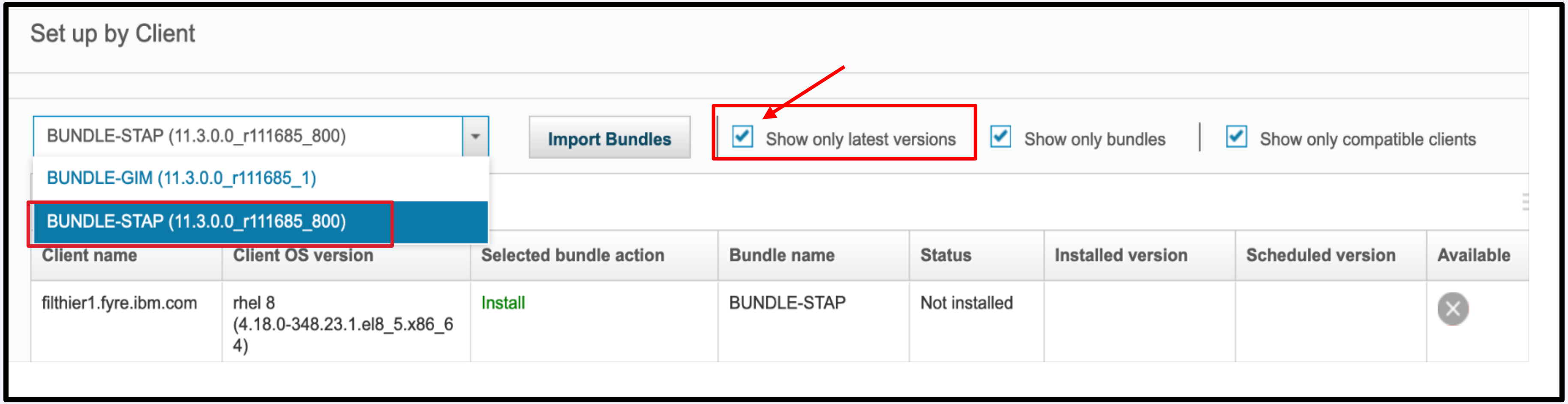
Case# 3: No matching KTAP, no Kernel SDK installed, close match found

```
……
Searching for module files in /usr/local/guardium/modules/KTAP/11.1.0.11_r111160_1-1650958591/modules-*.tgz
<13>Apr 26 11:36:40 guard_ktap_loader: 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
<13>Apr 26 11:36:40 guard_ktap_loader:
ec08d724e0202e420536126ee6d9a787  /usr/local/guardium/modules/KTAP/11.1.0.11_r111160_1-1650958591/modules-
11.1.0.11_r111160_v11_1_1.tgz
<13>Apr 26 11:36:44 guard_ktap_loader: File /lib/modules/4.18.0-305.40.2.el8_4.x86_64/build/.config not found.  Local build of
KTAP will not
<13>Apr 26 11:36:44 guard_ktap_loader: be attempted.  Please install kernel development packages for 4.18.0-
305.40.2.el8_4.x86_64 if you wish
<13>Apr 26 11:36:44 guard_ktap_loader: to build KTAP locally.
<13>Apr 26 11:36:48 guard_ktap_loader: 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
<13>Apr 26 11:36:49 guard_ktap_loader: Extracted module ktap-11.1.0.11_r111160_v11_1_1-oe8u2x64m-4.18.0-
305.10.2.el8_4.x86_64-x86_64-SMP.ko from /usr/local/guardium/modules/KTAP/11.1.0.11_r111160_1-1650958591/modules-
11.1.0.11_r111160_v11_1_1.tgz
<13>Apr 26 11:36:49 guard_ktap_loader: Retpoline kernel and module - OK
```

Common Problem:

Not finding the uploaded bundle in the drop-down menu

Not finding uploaded bundle in drop down menu



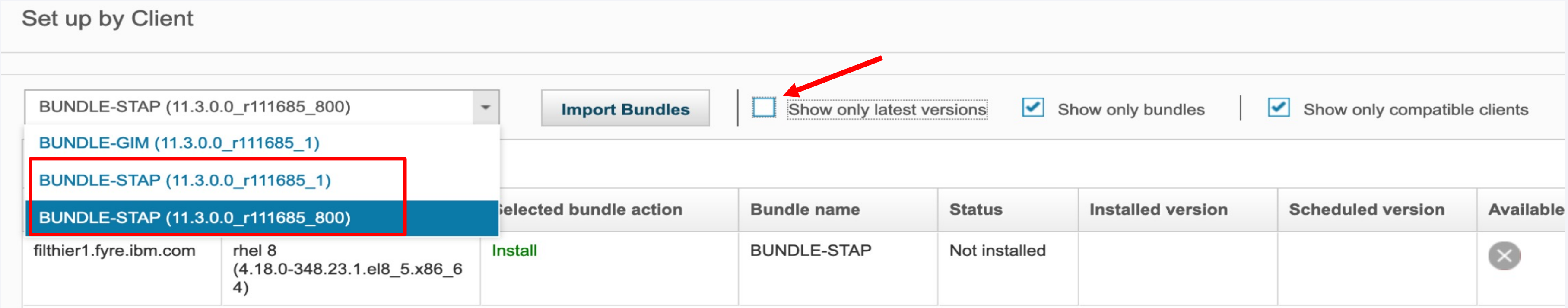
Set up by Client

BUNDLE-STAP (11.3.0.0_r111685_800)

BUNDLE-GIM (11.3.0.0_r111685_1)
BUNDLE-STAP (11.3.0.0_r111685_800)
Import Bundles

☑ Show only latest versions ☑ Show only bundles | ☑ Show only compatible clients

Client name	Client OS version	Selected bundle action	Bundle name	Status	Installed version	Scheduled version	Available
filthier1.fyre.ibm.com	rhel 8 (4.18.0-348.23.1.el8_5.x86_64)	Install	BUNDLE-STAP	Not installed			⊗



Set up by Client

BUNDLE-STAP (11.3.0.0_r111685_800)

BUNDLE-GIM (11.3.0.0_r111685_1)
BUNDLE-STAP (11.3.0.0_r111685_1)
BUNDLE-STAP (11.3.0.0_r111685_800)
Import Bundles

☐ Show only latest versions ☑ Show only bundles | ☑ Show only compatible clients

		elected bundle action	Bundle name	Status	Installed version	Scheduled version	Available
filthier1.fyre.ibm.com	rhel 8 (4.18.0-348.23.1.el8_5.x86_64)	Install	BUNDLE-STAP	Not installed			⊗

Issues

Problem: Not finding the uploaded bundle to push for installation
Uploaded STAP bundle <verXX>_y, but when attempting to select the bundle you don’t find it in the drop-down menu listing

For Example:
You upload **11.3.0.0_r111685_1** and when you want to select to push for installation from the drop-down menu, you only see **11.3.0.0_r111685**_800

Cause:
You having the “**Show only latest versions**” checkbox selected.

Solution:
Unselect this option and check again. Verify carefully what you select to push for installation. Is it EXACT same as what was uploaded? Verify the full name of the bundle, what you was uploaded and what is being selected to push for installation.

Sometimes, having the “**Show only latest versions**” checkbox selected may not even show the bundle you uploaded in the drop-down menu, depending upon what bundles exist on the GIM Server.

Additional Information for Reference

How to use configurator utility?

Configurator Utility - configurator.sh

- On Unix Servers with Guardium agent, you can use this utility to verify, assign or update parameter values for STAP modules, like GIM, STAP, KTAP and so on.

```
[root@testdb1 bin]# ./configurator.sh
Must specify full path for configurator.sh
[root@testdb1 bin]#
```

- Run the script without any parameter to get the usage.

```
 /opt/IBM/GuardiumAgent/modules/UTILS/current/files/bin/configurator.sh
usage: <full path>/configurator.sh [--set param_name param_value| --get module_name | --list | --delayed_bundle_deployment <enable|disable>]
[root@filthier1 bin]#
```

- It logs message in the central_logger.log, whenever you use this utility to modify GIM or STAP parameter value, or list the status of the Guardium agent modules.

configurator.sh

- Use **–get** <parameter name> <module name> ….. to review the current value
- Use **–set** <parameter name> <value>. ….. to modify the current value

For example:

```
]# /opt/IBM/GuardiumAgent/modules/UTILS/current/files/bin/configurator.sh --get STAP |  grep TAP_IP
STAP_PRIVATE_TAP_IP=NULL
STAP_TAP_IP=9.30.xx.xx
]#
```

```
[root@filthier1 bin]# /opt/IBM/GuardiumAgent/modules/UTILS/current/files/bin/configurator.sh --set
GIM_ALLOW_CUSTOMED_BUNDLES 1
[Tue May 10 10:29:38 2022] Parameter GIM_ALLOW_CUSTOMED_BUNDLES has been set and will take effect within a
minute (no need to restart GIM).
[root@filthier1 bin]#
```

configurator.sh

```
]# /opt/IBM/GuardiumAgent/modules/UTILS/current/files/bin/configurator.sh --get GIM |grep GIM_USE
GIM_USE_SSL=0
[root@filthier1 bin
```

```
 /# opt/IBM/GuardiumAgent/modules/UTILS/current/files/bin/configurator.sh --set GIM_USE_SSL 1
[Tue May 10 08:51:52 2022] Parameter GIM_USE_SSL has been set and will take effect within a minute (no need to restart GIM).
[]#
```

- ➢ You will see message logged in the central _logger.log when you use configurator utility to update any GIM Parameter value from the “Set up by Client” view in the GUI.

configurator.sh

- **What is logged in the central_logger.log?**

```
....
Tue May 10 08:50:14 2022] -I- Sending CHECK_UPDATES message
[Tue May 10 08:50:14 2022] -I- No packages to install are waiting on the server...checking if local updates are available
[Tue May 10 08:51:52 2022] Parameter GIM_USE_SSL has been set and will take effect within a minute (no need to restart GIM).
[Tue May 10 08:51:54 2022] -I- Found changes waiting to be processed ... time to wake up
……..
[Tue May 10 08:51:56 2022] -I- Received new (local) modules information to process
[Tue May 10 08:51:56 2022] -I- Processing new parameters
[Tue May 10 08:51:56 2022] -I- Packages to install : []
[Tue May 10 08:51:56 2022] -I- Processing parameter GIM_USE_SSL change from [0] to [1]
[Tue May 10 08:51:56 2022] -I- Assigning GIM_USE_SSL change to module GIM
[Tue May 10 08:51:56 2022] -I- Modules to uninstall : []
[Tue May 10 08:51:56 2022] -I- Modules to update : [GIM]
[Tue May 10 08:51:56 2022] -I- Finished processing new parameters
[Tue May 10 08:51:56 2022] -I- UPDATING MODULES !!!
[Tue May 10 08:51:56 2022] -I- Updating module GIM
[Tue May 10 08:51:56 2022] -I- G-Machine ip or port has changed
   old ip   = 9.37.xx.xx
   new ip   = 9.37.xx.xx
   old port = 8081
   new port = 8446
   old use_ssl = 0
   new use_ssl = 1
[Tue May 10 08:51:57 2022] -I- Server (9.37.xx.xx) is alive
```

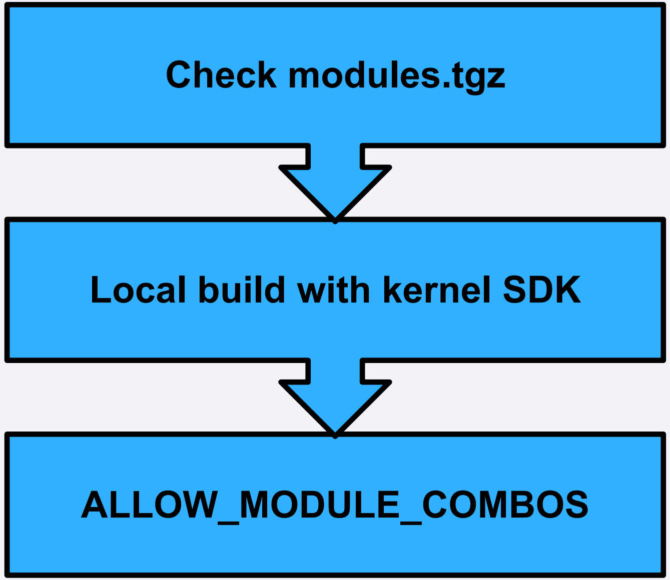
……………

Finding a Compatible KTAP

KTAP not Compatible with current kernel version

How do I prevent it?

- ✓ Stay up to date on the latest STAP and KTAP bundles
- ✓ Use the tool on to 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

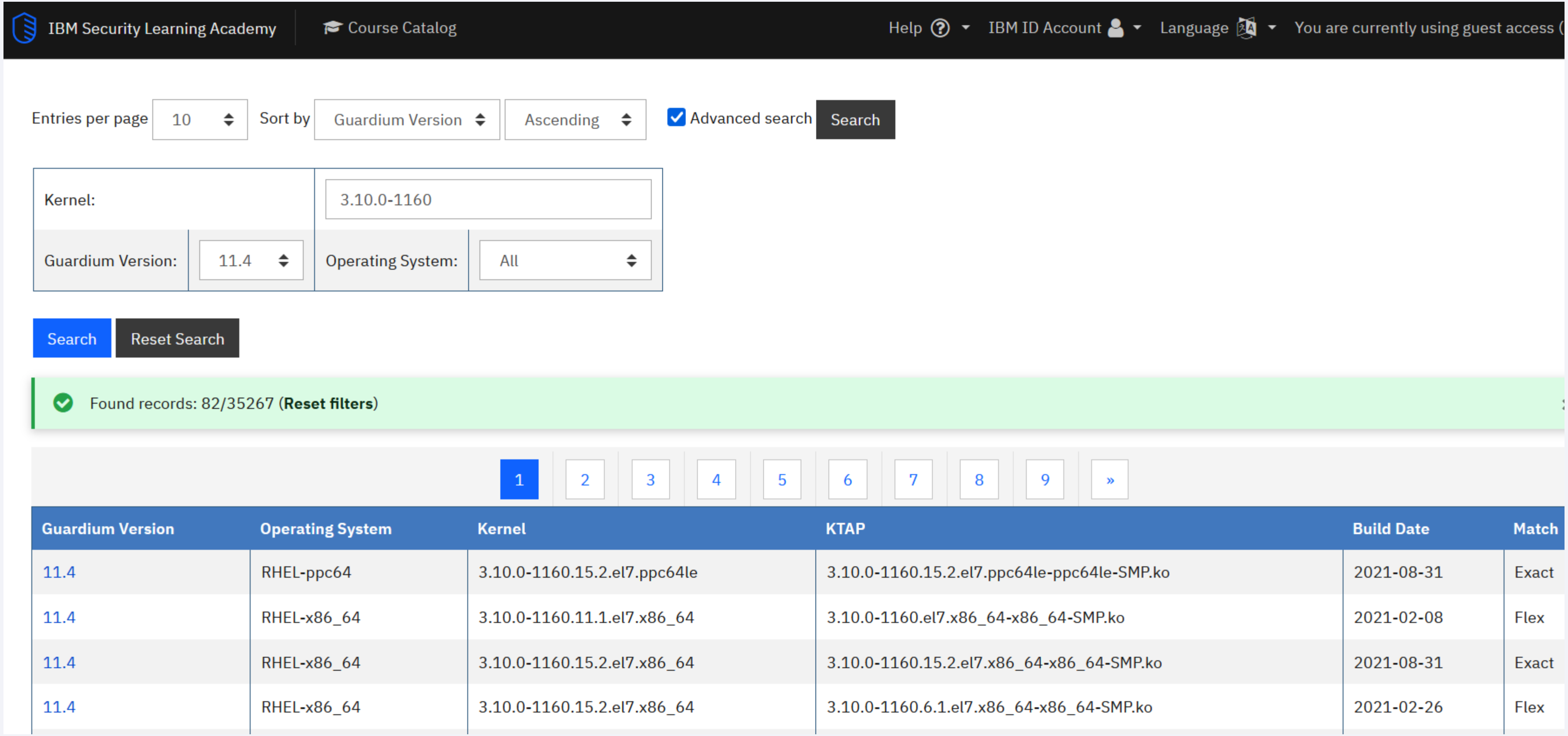


Check modules.tgz

Local build with kernel SDK

ALLOW_MODULE_COMBOS

Check the Security Learning Academy



Entries per page: 10

Sort by: Guardium Version, Ascending

☑ Advanced search

Kernel: 3.10.0-1160

Guardium Version: 11.4

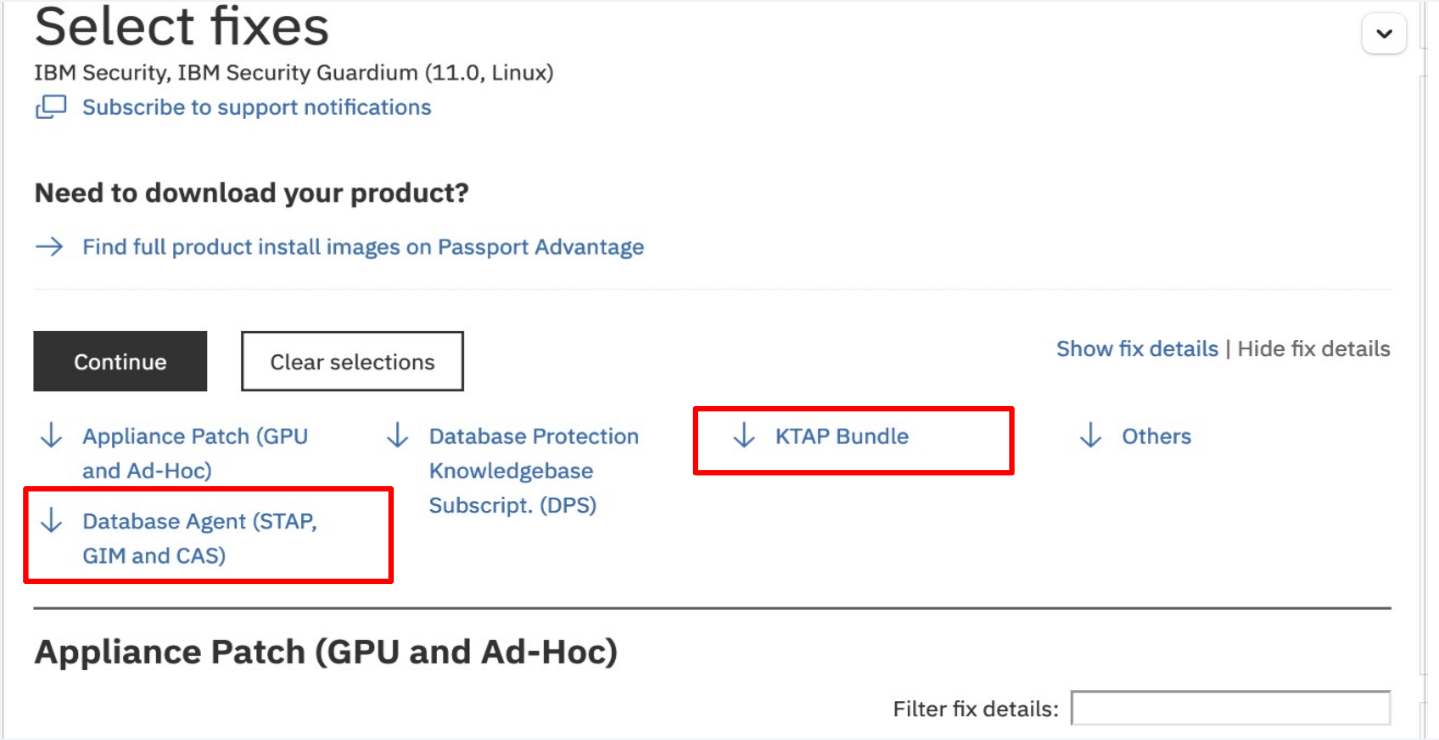
Operating System: All

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

Is my kernel directly supported?

- Check under KTAP Bundles section.



Select fixes

IBM Security, IBM Security Guardium (11.0, Linux)

Subscribe to support notifications

Need to download your product?

Find full product install images on Passport Advantage

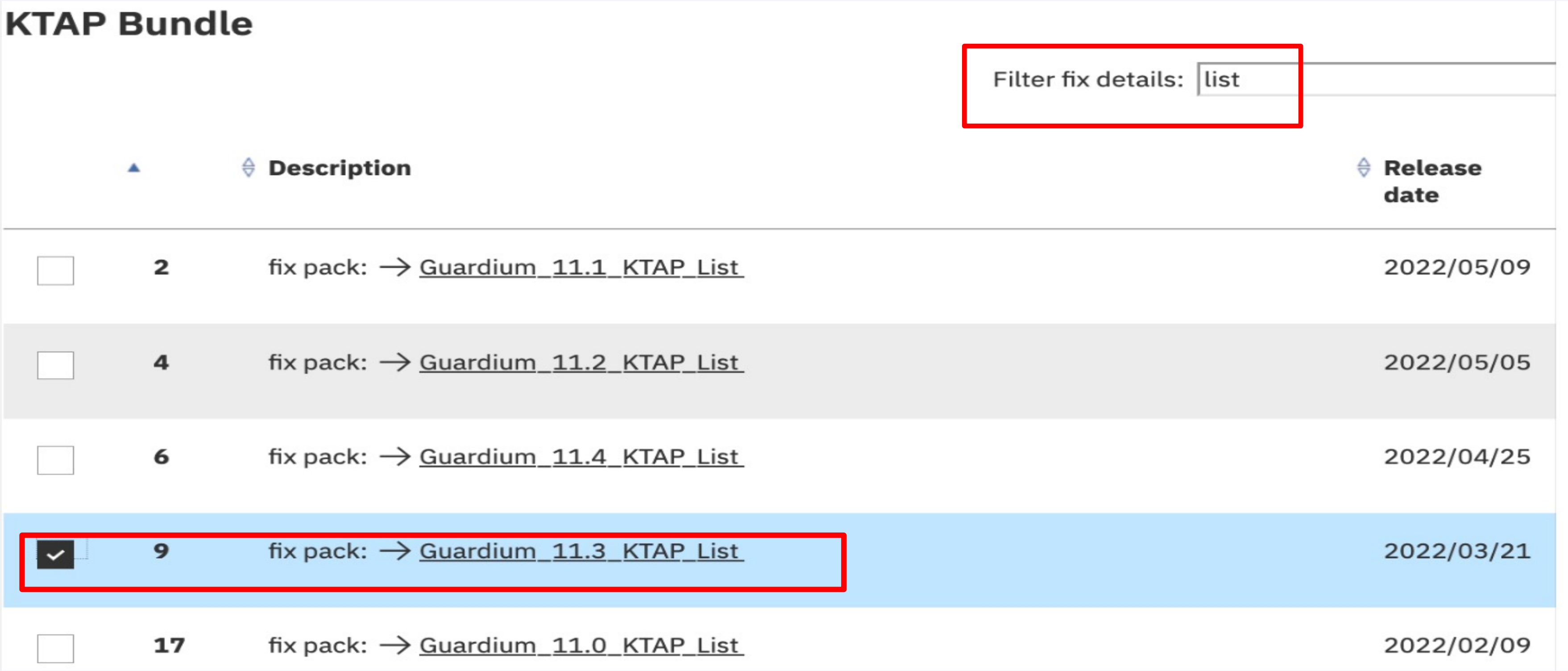
Continue
Clear selections
Show fix details | Hide fix details
Appliance Patch (GPU and Ad-Hoc)
Database Protection Knowledgebase Subscript. (DPS)
KTAP Bundle
Others
Database Agent (STAP, GIM and CAS)

Appliance Patch (GPU and Ad-Hoc)

Filter fix details:

Is my kernel directly supported?

Searching for **List** in search bar, under KTAP bundle



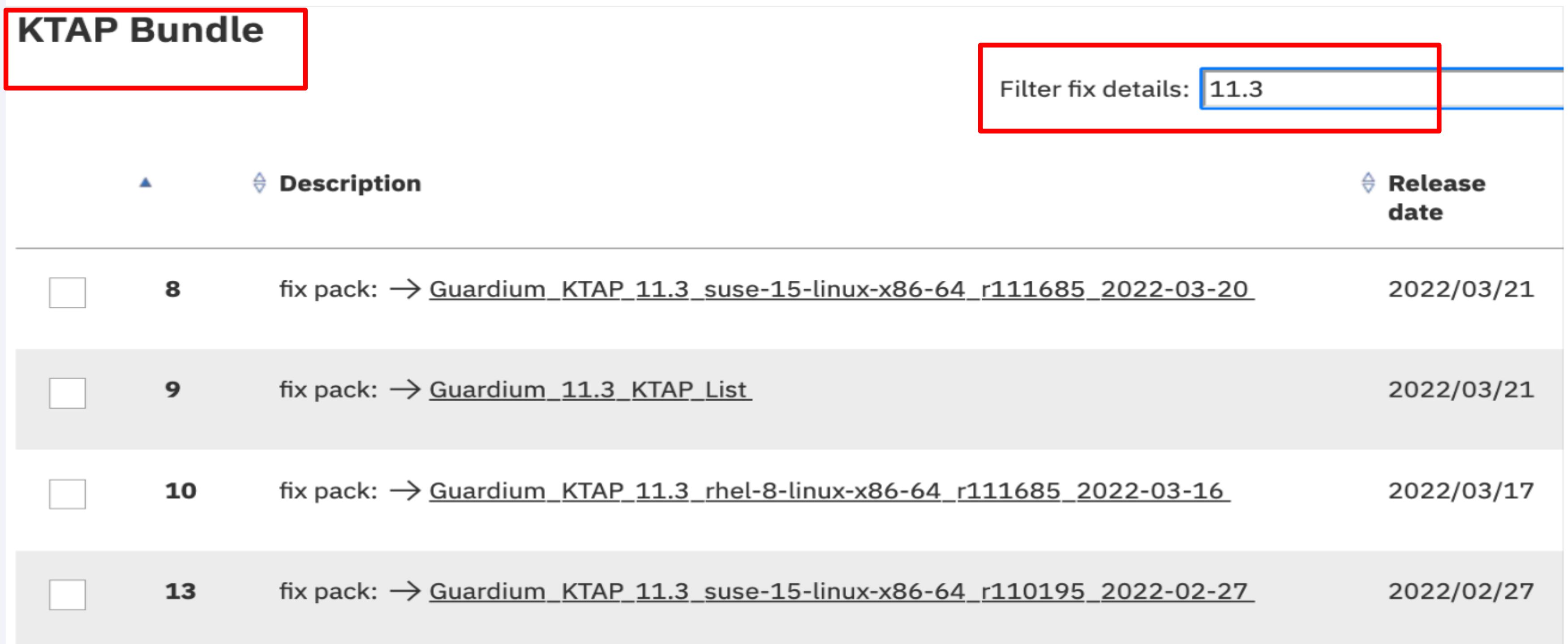
KTAP Bundle

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

Is my kernel directly supported?

- Searching for **11.3** in search bar, under KTAP bundle

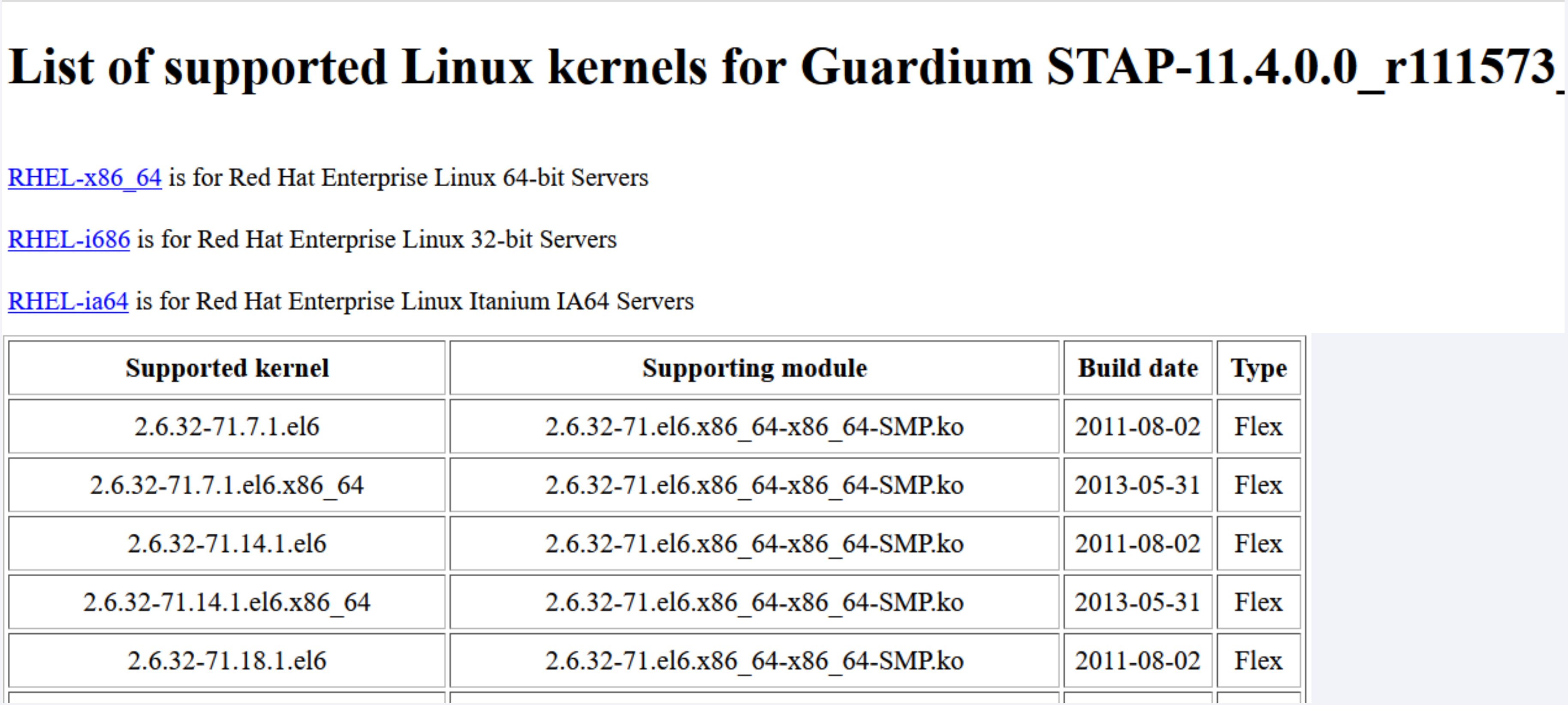


KTAP Bundle

Filter fix details: 11.3

	▲	Description	Release date
☐	**8**	fix pack: → Guardium_KTAP_11.3_suse-15-linux-x86-64_r111685_2022-03-20	2022/03/21
☐	**9**	fix pack: → Guardium_11.3_KTAP_List	2022/03/21
☐	**10**	fix pack: → Guardium_KTAP_11.3_rhel-8-linux-x86-64_r111685_2022-03-16	2022/03/17
☐	**13**	fix pack: → Guardium_KTAP_11.3_suse-15-linux-x86-64_r110195_2022-02-27	2022/02/27

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 Version

Match the First Four!

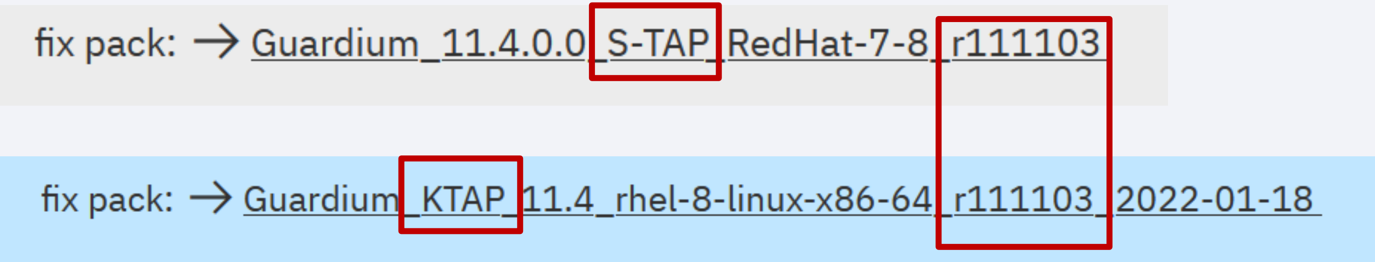
```
uname –a
Linux testsev1.xx.xxx.com 3.10.0-1160.62.1.el7.x86_64 #1 SMP
```

- 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

Troubleshooting

What to do in case of STAP/ KTAP issues

- Verify what Guardium related processes are running on the DB Server?
  - ps -aef | egrep "gim|modules" ... this will show which Guardium processes are running

- Check if KTAP is loaded? Based on the OS type you will use one of these command
  - On Solaris: modinfo | grep ktap
  - On AIX: genkex | grep ktap
  - **On Linux: lsmod | grep ktap**
  - On HP-UX: lsdev | grep ktap

- Review the logs, start with **central_logger.log**, and syslog on the Server
- Check guard_tap.ini too, to verify the basic parameter & it’s value,
- Depending up what we see in the logs, we can decide if, or what additional information is needed

Troubleshooting Unix STAP Problems.

https://www.ibm.com/docs/en/guardium/11.4?topic=performance-linux-unix-troubleshooting-s-tap-problems

Troubleshooting STAP issues

Useful information and logs to collect

1. STAP diagnostics
2. /tmp/guard_stap.stderr.txt
3. syslog
4. When and where the problem occurred?
5. Is it reproducible?
6. What is the current status?
7. Copy, or take screenshot of error message, if any

STAP diagnostics has most of the basic information we need to begin the investigation

Depending on the reported problem, we will ask for additional information.

Collecting STAP diagnostics

Collecting STAP diagnostics:

- **Run it directly on the Database Server using guard_diag**

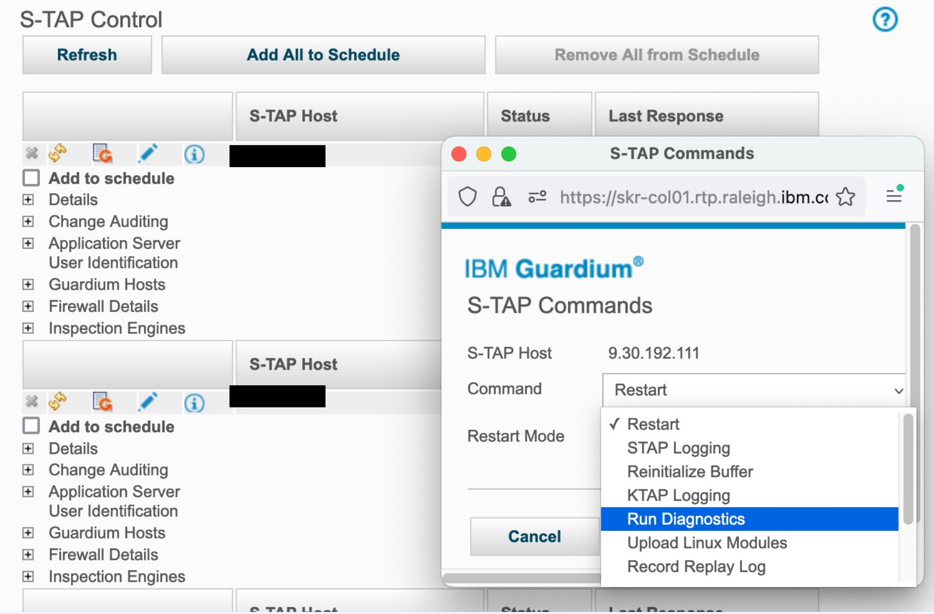
  Reference document:
  https://www.ibm.com/support/pages/ibm-mustgather-collecting-data-guardium-stap

- **Run it through Guardium UI, i.e. the GIM Server**, assuming there is no connectivity issue between the GIM Server and the GIM Client

  Reference document:
  https://www.ibm.com/support/pages/ibm-mustgather-collecting-data-guardium-stap

Executing STAP DIAG from GUI

Collecting STAP Diagnostics from Guardium UI


S-TAP Control

	S-TAP Host	Status	Last Response
	[redacted]		

☐ **Add to schedule**
- ⊞ Details
- ⊞ Change Auditing
- ⊞ Application Server User Identification
- ⊞ Guardium Hosts
- ⊞ Firewall Details
- ⊞ Inspection Engines

	S-TAP Host
	[redacted]

☐ **Add to schedule**
- ⊞ Details
- ⊞ Change Auditing
- ⊞ Application Server User Identification
- ⊞ Guardium Hosts
- ⊞ Firewall Details
- ⊞ Inspection Engines

S-TAP Commands

https://skr-col01.rtp.raleigh.ibm.c

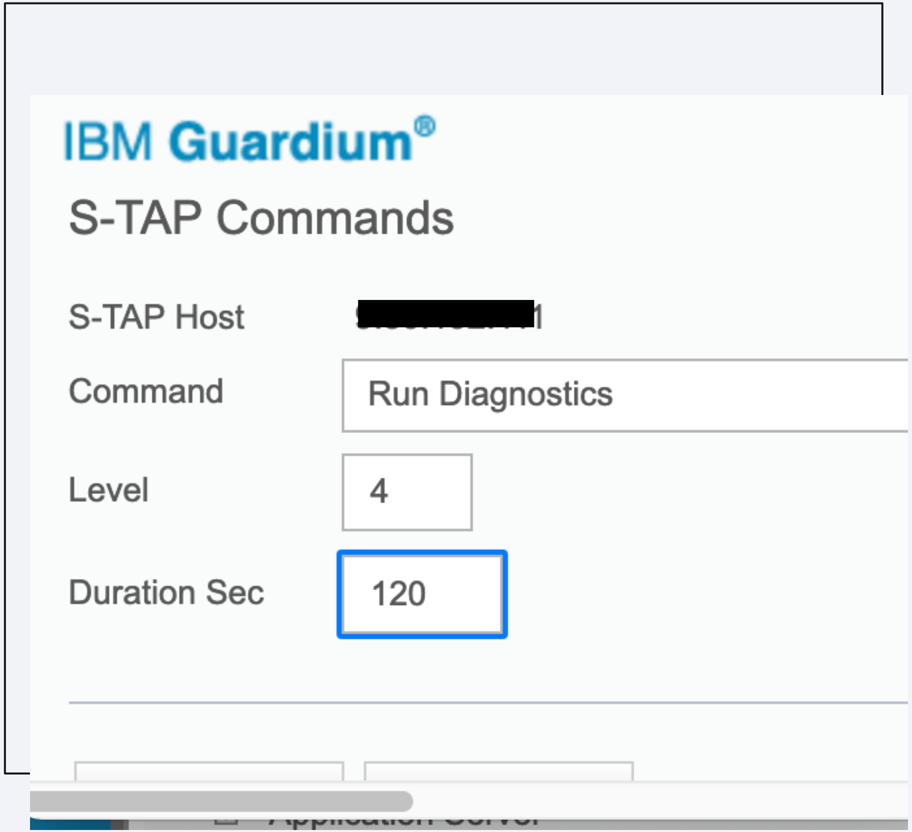
IBM Guardium®

S-TAP Commands

S-TAP Host 9.30.192.111

Command: Restart

Restart Mode


IBM Guardium®

S-TAP Commands

S-TAP Host	[redacted]
Command	Run Diagnostics
Level	4
Duration Sec	120

Executing STAP DIAG using gardapi

- **Run it using grdapi command from the GIM Server**,
  - assuming there is no connectivity issue between the GIM Server and the GIM Client
  - and “**upload**_feature” is enabled in guard_tap.ini, by default, “**upload**_feature” is enabled

```
grdapi run_diagnostics stapHost=<STAP Host Server IP>
```

- Use fileserver to download the generated diagnostic file from the appliance

Example

```
grdapi run_diagnostics stapHost=xxx.xxx.199.31
```

The diagnostics is copied to the Collector and can be found at: /opt/IBM/Guardium/log/stap_diagnostic

```
-rw-r--r-- 1 tomcat tomcat   724380 May 01 13:27 diag.ustap.testserv1.xxx.xxx.com.22-05-
01_102553.tar.gz
```

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

Custom KTAP

QUESTIONS?