IBM Security

Guardium Open Mic
Appliance Patching

Avi Walerius
IBM Security Systems

Nov 2018

Never installed a patch before?

- Courses available in IBM Security Learning Academy

IBM Security **Learning Academy**
Prepare to outthink security threats

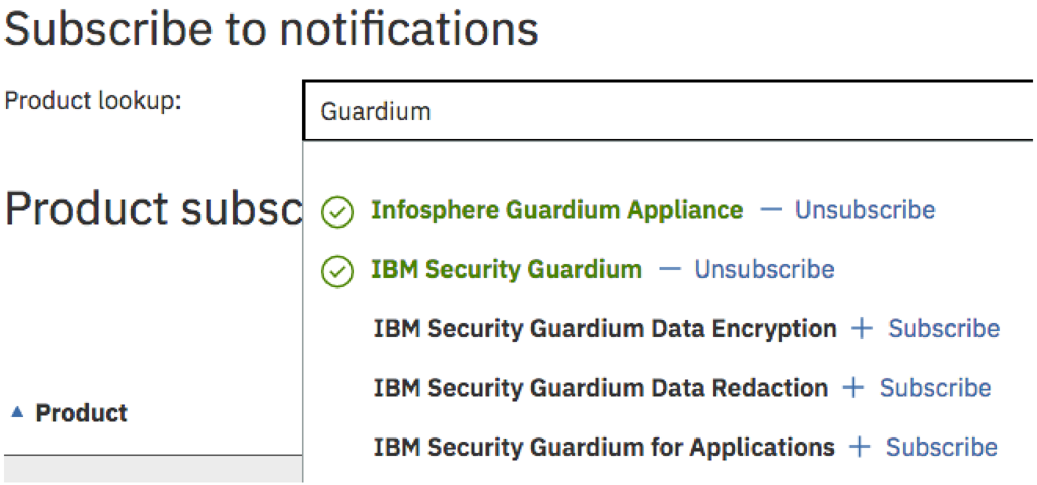
- Video Demo - How to download and install a patch
  - https://www.securitylearningacademy.com/enrol/index.php?id=842

- Lab - Upgrading from v9 to v10 with upgrade patch (similar to GPU)
  - https://www.securitylearningacademy.com/enrol/index.php?id=1853

- Video Demo - Dos and Don’ts of GPU installation
  - https://www.securitylearningacademy.com/enrol/index.php?id=2345

Not sure when patches are being released?

- Subscribe to my notifications to find out
- http://www-01.ibm.com/support/docview.wss?uid=ibm10718119



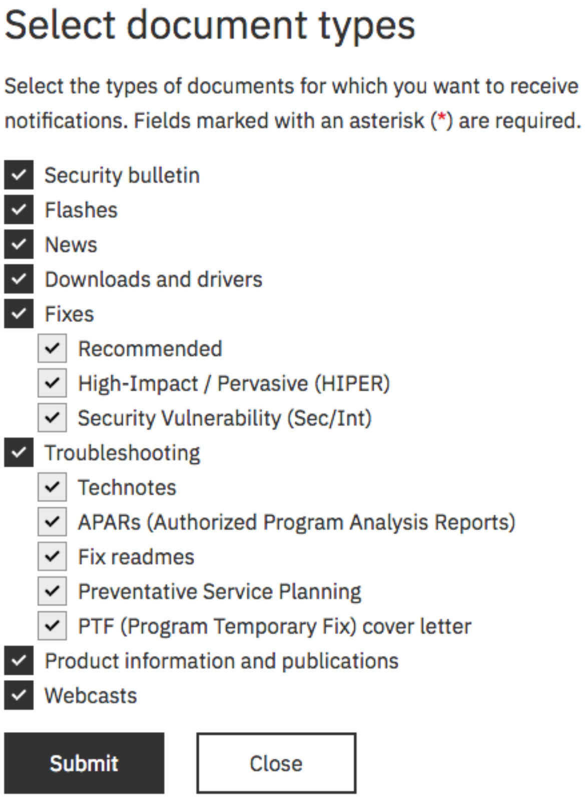
Subscribe to notifications

Product lookup: Guardium

Product subsc

- ✓ Infosphere Guardium Appliance — Unsubscribe
- ✓ IBM Security Guardium — Unsubscribe
- IBM Security Guardium Data Encryption + Subscribe
- IBM Security Guardium Data Redaction + Subscribe
- IBM Security Guardium for Applications + Subscribe

▲ Product



Select document types

Select the types of documents for which you want to receive notifications. Fields marked with an asterisk (*) are required.

- ☑ Security bulletin
- ☑ Flashes
- ☑ News
- ☑ Downloads and drivers
- ☑ Fixes
  - ☑ Recommended
  - ☑ High-Impact / Pervasive (HIPER)
  - ☑ Security Vulnerability (Sec/Int)
- ☑ Troubleshooting
  - ☑ Technotes
  - ☑ APARs (Authorized Program Analysis Reports)
  - ☑ Fix readmes
  - ☑ Preventative Service Planning
  - ☑ PTF (Program Temporary Fix) cover letter
- ☑ Product information and publications
- ☑ Webcasts

Agenda

- Appliance patch types
- Health check
- Resolving health check issues
- GPU install best practices

Appliance Patch Types

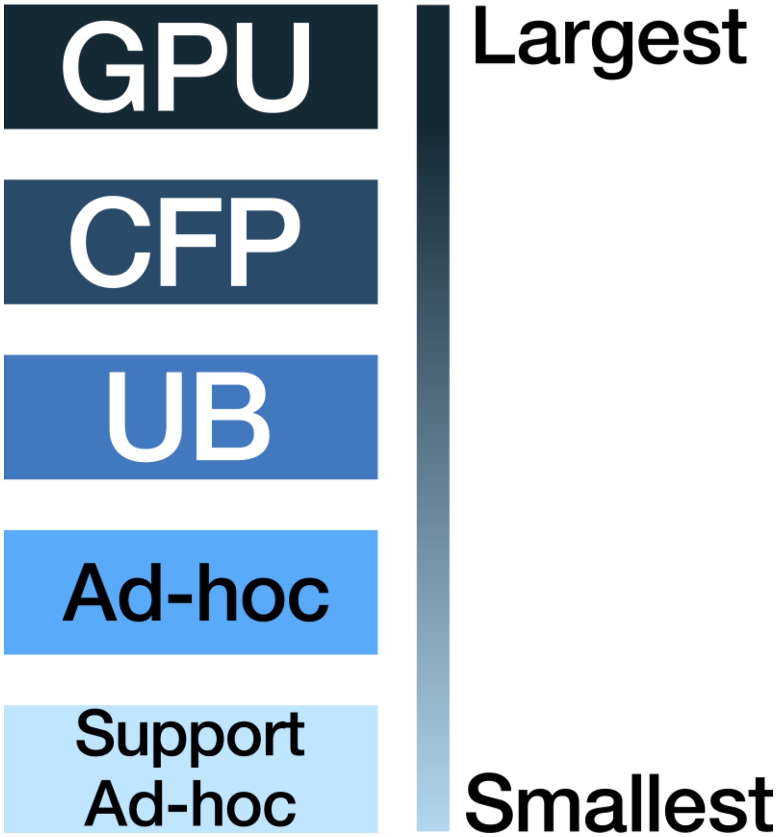
Appliance Patch Types

- There are eight types of patches
  - GPU – Guardium Patch Update
  - CFP – Combined Fix Pack
  - UB – Update Bundle
  - Ad-hoc
  - Support Ad-Hoc
  - Security Patch
  - Sniffer Patch
  - Health Check

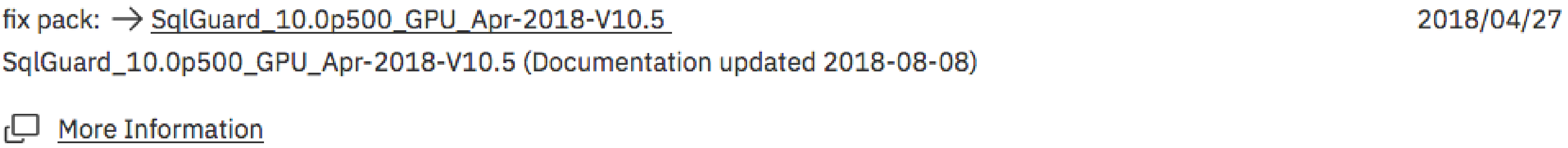
- Health Check (HC) is always patch number 9997.
  - Health Checks are always required before installing a GPU
  - All non-success outputs are intended to be covered by the Health Check release notes. You can get the patch log from fileserver for further analysis
  - It is always recommended to get the latest health check

Appliance Patch Types

- GPU’s are the largest patch we do and gets the most attention and verification
- Combined fix packs (CFP) started after v9.5. We needed something smaller than a GPU but still large enough to encapsulate a major subsystem change.
- To improve quality in testing we moved from an ad-hoc strategy to a update bundle (UB) strategy.
- Ad-hocs are generally for a single customer and single fix. Ad-hocs generally will never be put on Fix Central
- Support Ad-hocs are generally for a very specific fix (e.g. someone needs to run a root shell command on 100 systems for a site-specific issue). These generally will never be put on Fix Central



GPU



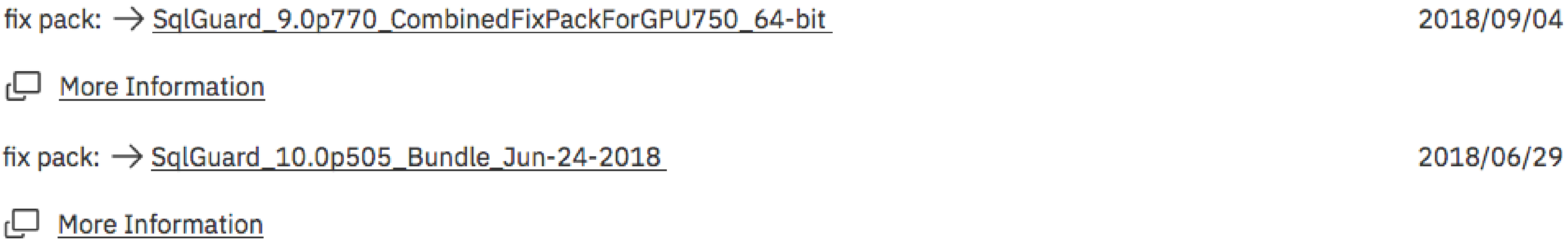
fix pack: → SqlGuard_10.0p500_GPU_Apr-2018-V10.5 2018/04/27

SqlGuard_10.0p500_GPU_Apr-2018-V10.5 (Documentation updated 2018-08-08)

More Information

- GPUs are cumulative
- P500 contains fixes in all previous GPU, CFP, UB, Adhoc, Snif and Security patch released before it, except…
- Edge case example:
  1. GPU p500 coding is finished. Testing begins
  2. New sniffer problem found, too late to be included in p500 fixes
  3. New sniffer patch p4099 released
  4. GPU p500 released
  5. P4099 might not be in p500 – If you are looking for a specific patch - **Check the release notes!**
- GPUs always restart appliance
- What changes have been made in latest GPU?
  - V9 - https://www-01.ibm.com/support/docview.wss?uid=swg21693983
  - V10 - https://www-01.ibm.com/support/docview.wss?uid=swg21997914

Combined Fix Pack / Update Bundle



fix pack: → SqlGuard_9.0p770_CombinedFixPackForGPU750_64-bit 2018/09/04

More Information

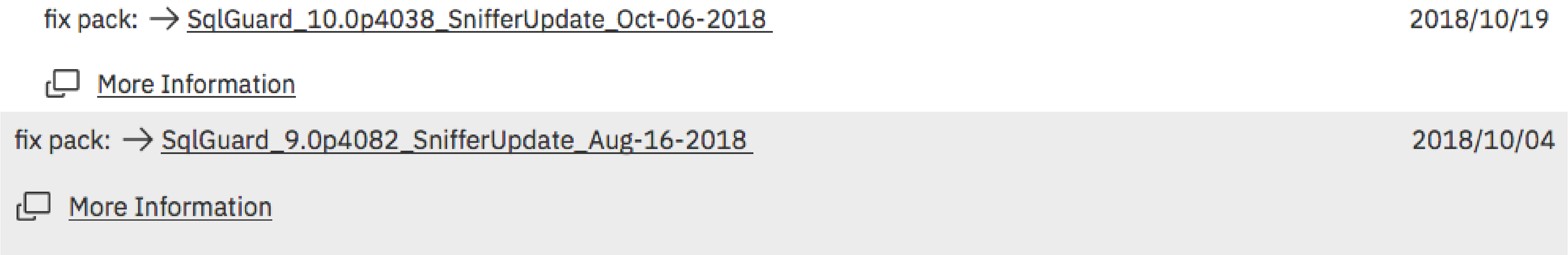
fix pack: → SqlGuard_10.0p505_Bundle_Jun-24-2018 2018/06/29

More Information

- CFP/UB cumulative back to the last GPU
- CFP likely to contain snif and security patches
  - P770 contains CFP, UB, adhoc, snif and security patches back to p750
- UB just ad-hoc patches
  - P505 contains adhoc patches back to p500

- CFP most likely restarts appliance
- UB most likely does not restart appliance but does restart other services e.g. mysql, tomcat - **Read the release notes!**

Sniffer Patches



fix pack: → SqlGuard_10.0p4038_SnifferUpdate_Oct-06-2018 2018/10/19

More Information

fix pack: → SqlGuard_9.0p4082_SnifferUpdate_Aug-16-2018 2018/10/04

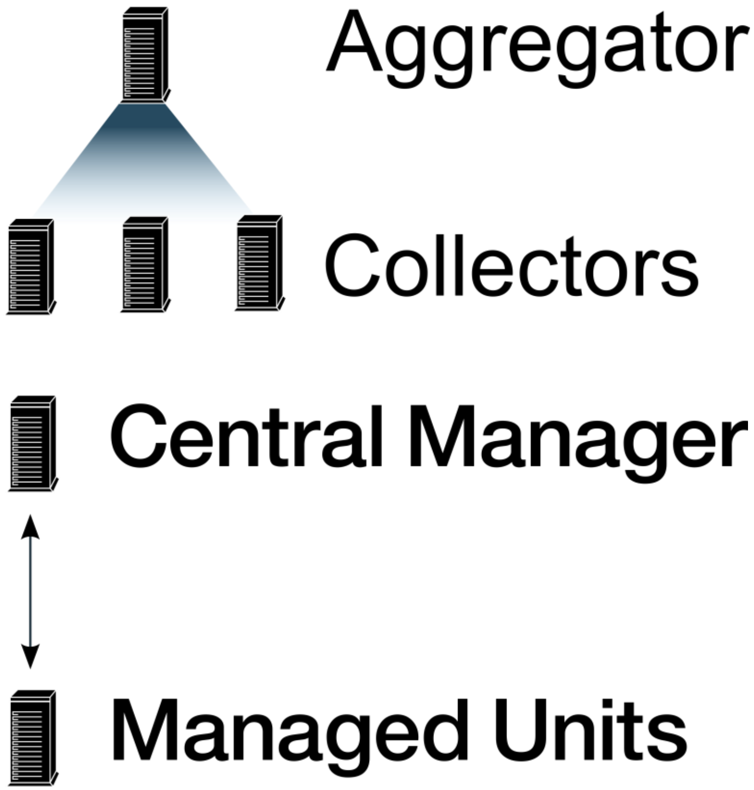
More Information

- Snif is core to our product and we get issues that need to be resolved outside the GPU cycle for many customers. The main categories of issues are:
  - Crashes
  - Parser Errors
  - Stuck Threads
  - Performance

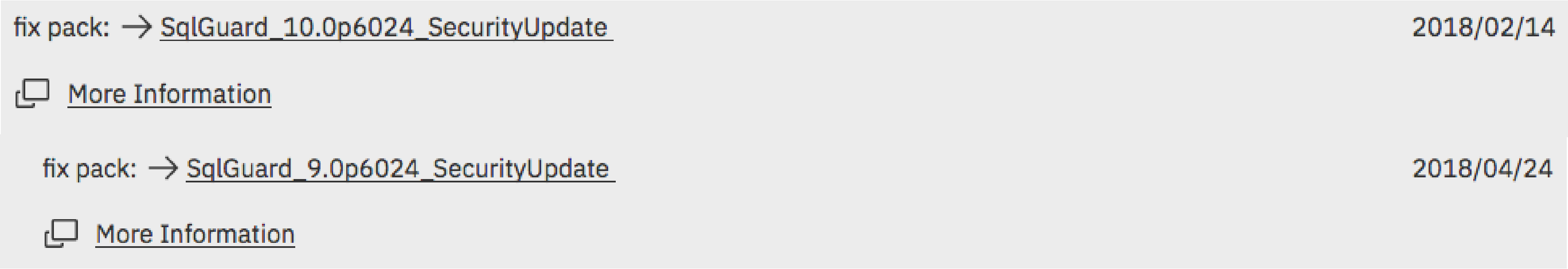
- V9 and v10 - p40xx
- Sniffer patches are cumulative
- V10 p4038 contains all sniffer patches from v10
- V10 Sniffer patches can only be installed on top of v10p100 , v9 on top of v9p50
- Sniffer patches always restart sniffer

Sniffer Patches

- Why does snif need to be installed everywhere?
  - Because snif drives our schema it needs to be reflected on the whole environment.
  - Aggregation takes data exports from collectors and then updates the schema and if you have a mismatch this can cause problems.
  - This is part of why we recommend a ‘top down’ rollout strategy
- Requirement is install it everywhere!



Security Patches



fix pack: → SqlGuard_10.0p6024_SecurityUpdate 2018/02/14

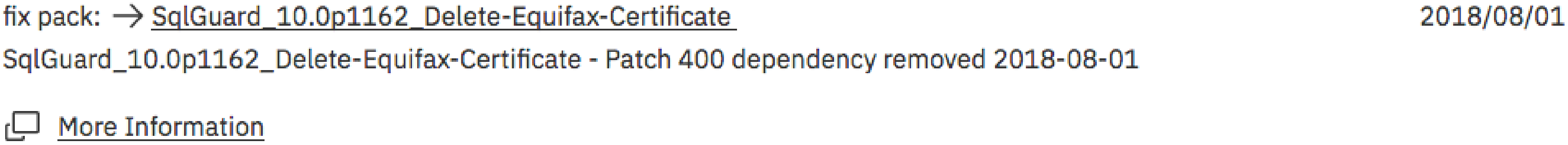
More Information

fix pack: → SqlGuard_9.0p6024_SecurityUpdate 2018/04/24

More Information

- What goes in?
  - RPM’s, System Packages
  - **No appliance code changes**
  - Configuration/Cipherlist Changes
- V9 and v10 - P60xx
- Security patches are NOT cumulative
- But some (not all) security patches contain previous ones – Read the release notes!
- Security patches always restart appliance
- Not all security fixes are in security patches – only those that don’t require appliance code change

Ad-hoc patches



fix pack: → SqlGuard_10.0p1162_Delete-Equifax-Certificate 2018/08/01

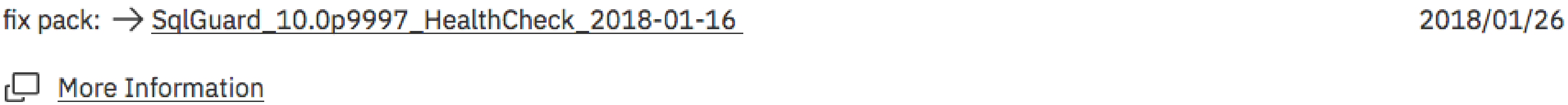
SqlGuard_10.0p1162_Delete-Equifax-Certificate - Patch 400 dependency removed 2018-08-01

More Information

- Individual fixes for specific issues
- Not cumulative
- Rarely released on fix central, except when combined in Bundles, Combined Fix Packs or GPUs
- May be provided direct from support with instructions and dependencies given at that time

Health Check Patch

Health Check Patch p9997



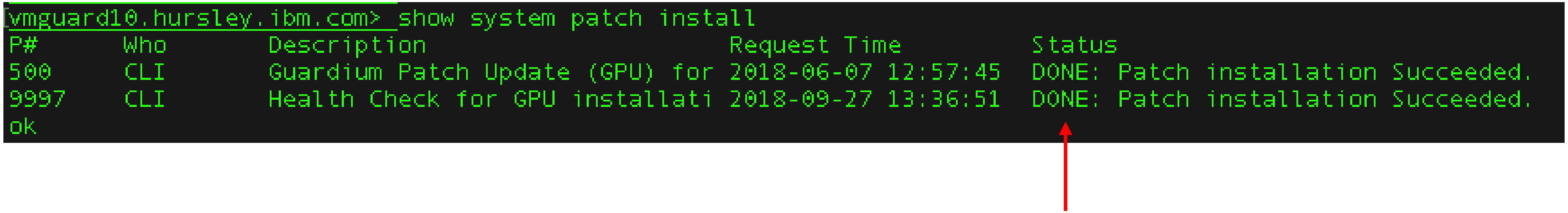
fix pack: → SqlGuard_10.0p9997_HealthCheck_2018-01-16 2018/01/26

More Information

- Checks for known issues that will cause GPU install to fail
- Always check for latest health check patch on fix central
- Install as soon as possible before GPU install
- Checks and actions in the patch (Jan 2018 patch)
  - Database free space
  - /var partition free space
  - / partition free space
  - Customer made queries with same name that will be added by GPU
  - Amount of data in outlier tables
  - Crashed tables
  - Custom domains have duplicate IDs
  - Preserving customized settings in purge object
  - Create link for Tivoli files

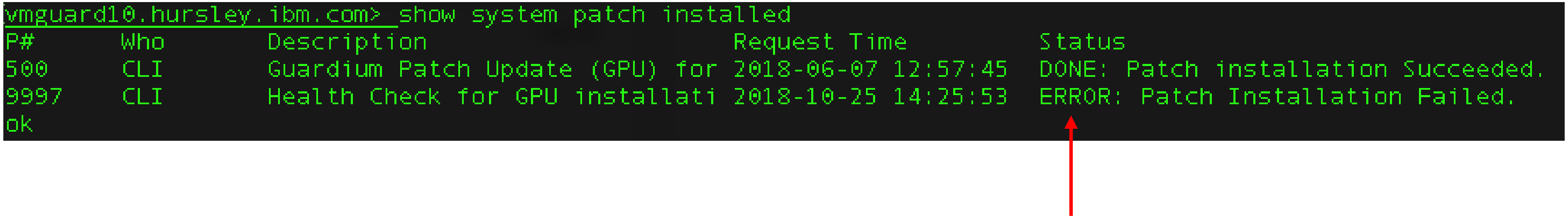
Health Check Patch

- Successful:



```
vmguard10.hursley.ibm.com> show system patch install
P#       Who        Description                         Request Time          Status
500      CLI        Guardium Patch Update (GPU) for 2018-06-07 12:57:45  DONE: Patch installation Succeeded.
9997     CLI        Health Check for GPU installati 2018-09-27 13:36:51  DONE: Patch installation Succeeded.
ok
```

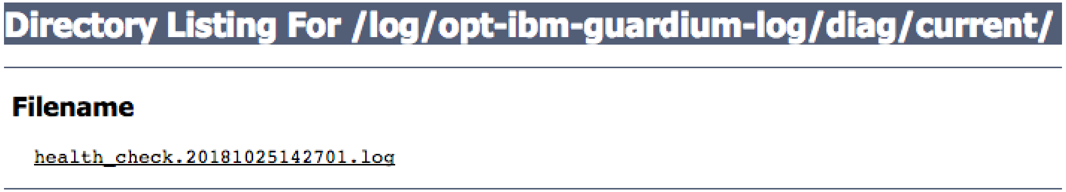
- Failed:



```
vmguard10.hursley.ibm.com> show system patch installed
P#       Who        Description                         Request Time          Status
500      CLI        Guardium Patch Update (GPU) for 2018-06-07 12:57:45  DONE: Patch installation Succeeded.
9997     CLI        Health Check for GPU installati 2018-10-25 14:25:53  ERROR: Patch Installation Failed.
ok
```

Health Check Patch Log File

- Get log from fileserver:

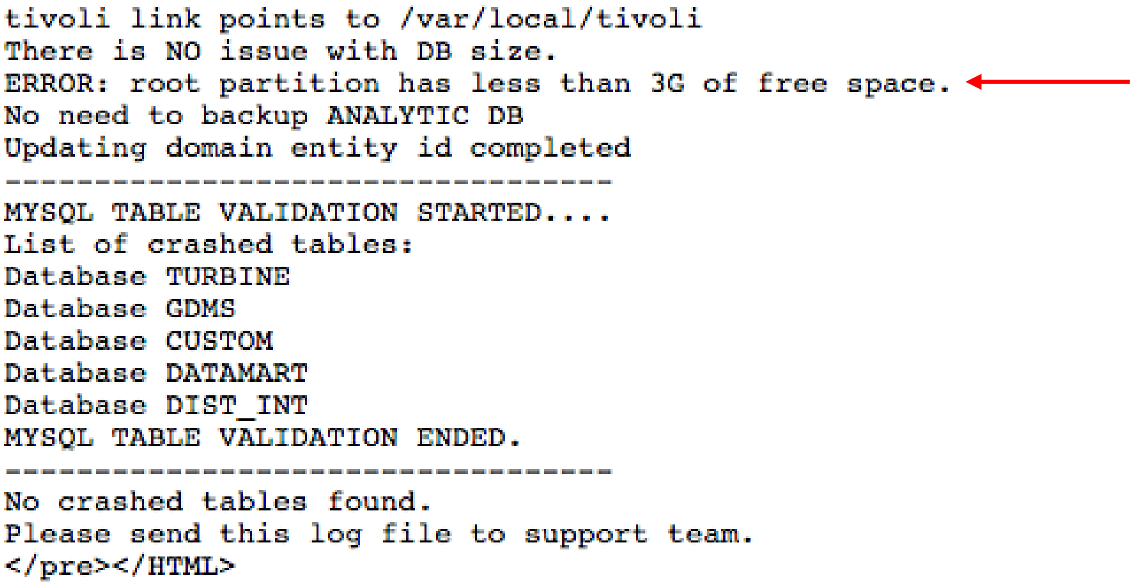


Directory Listing For /log/opt-ibm-guardium-log/diag/current/

Filename

health_check.20181025142701.log

- Example file:



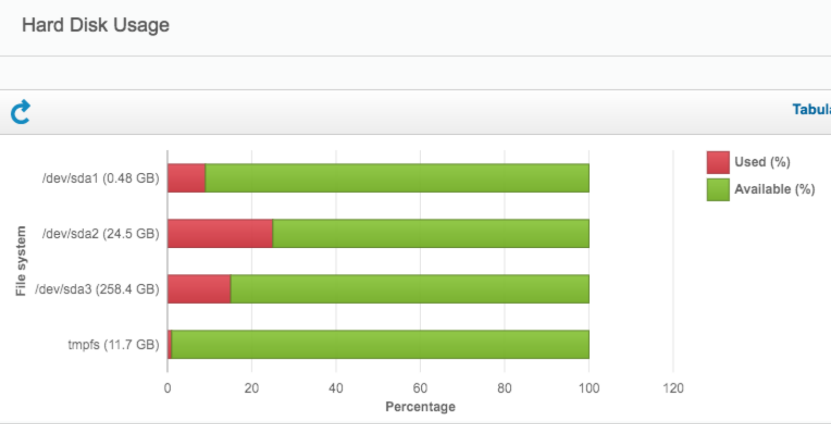
```
tivoli link points to /var/local/tivoli
There is NO issue with DB size.
ERROR: root partition has less than 3G of free space.
No need to backup ANALYTIC DB
Updating domain entity id completed
----------------------------------
MYSQL TABLE VALIDATION STARTED....
List of crashed tables:
Database TURBINE
Database GDMS
Database CUSTOM
Database DATAMART
Database DIST_INT
MYSQL TABLE VALIDATION ENDED.
----------------------------------
No crashed tables found.
Please send this log file to support team.
</pre></HTML>
```

Tips to Resolve Health Check Issues

- DB Size:
  - Purging database as much as possible is recommended before GPU install
  - Ensure scheduled archive/export purge is working as expected
  - How much data is in my top tables per day? https://www-01.ibm.com/support/docview.wss?uid=swg21981235
  - What to do if database is filling up? https://www-01.ibm.com/support/docview.wss?uid=swg21511904

- Disk Size:
  - Database can use a lot of disk, if you have DB and Disk error, resolve DB first
  - Check disk size in Manage -> System View -> System Monitor
  - To clean files: support show large_files, support clean log_files
  - Common files to *consider* removing:
    - /var/log/messages* (syslog messages files)
    - /var/IBM/Guardium/log/patches/* (patch files)
    - /var/IBM/Guardium/log/analyzer/* (slon files)

  - Only remove files if you understand what they are



Tips to Resolve Health Check Issues

- Duplicate query names found:
  - Health check contains a list of new queries to be added by GPU
  - If you already have a query of the same name there will be a problem when installing the GPU
  1. Exact names are listed in the health check output
  2. Find those queries on the system
  3. Clone the queries to rename
  4. Delete the original queries
  5. Reinstall the health check

```
*ERROR: Duplicate query names found.
Detailed Guardium User Activity
SOX - DB User Activity*
```

- Crashed tables found:
  - Produces warning, not error
  - GPU can be installed but best to check with support
  - Definitely check with support if GDM_ table is crashed

```
MYSQL TABLE VALIDATION STARTED....
List of crashed tables:
Database TURBINE
Database GDMS
Database CUSTOM
Database DATAMART
   TEST_DATAMART
Database DIST_INT
MYSQL TABLE VALIDATION ENDED.
```

GPU Install best practices

GPU Install best practices

1. Read the release notes
   Release notes explain everything contained inside the patch and steps to consider for the install. Read them before planning the installation process. Also read the health check release notes so you understand what is checked.

2. Purge as much as possible before installation
   GPUs usually make changes to the Guardium internal database schema. The less data in the database, the faster the GPU install will go.

3. Run latest health check first
   The health check confirms the system is ready for the GPU install. Installing the GPU without health check could lead to the failure of the GPU or, in worst case, corruption of the appliance.

4. Install “top down”
   Install patches first on the CM, then Aggregators, then Collectors.

GPU Install best practices

5. Install GPU as soon as possible after health check
   The health check tests for conditions like disk usage. This can increase quickly so its important to install GPU as soon as possible after the health check.

6. Allow time to install the patch
   GPU patches can take a long time to install depending on the amount of data, in some cases many hours. Allow the patch time to complete before assuming it has stalled or failed.

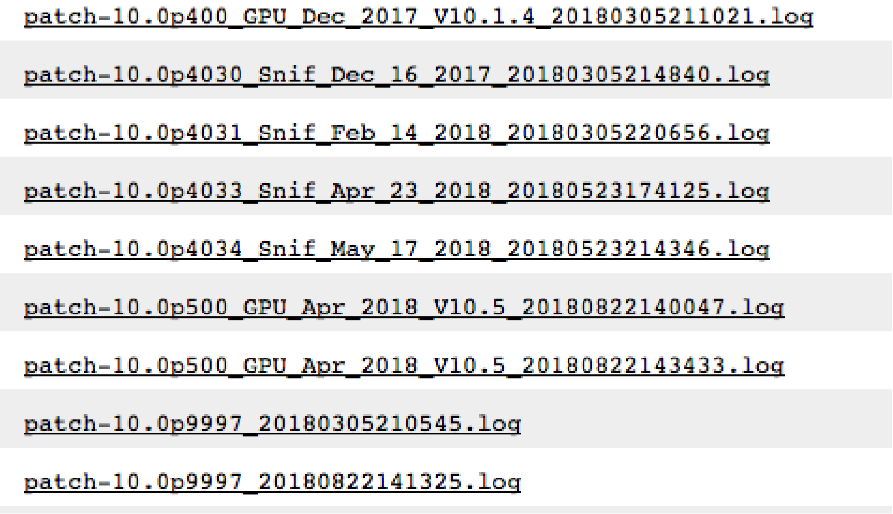
7. Don’t worry if mysql goes down during patch install
   GPUs restart the internal mysql database. Messages in the CLI saying mysql server has gone away are normal. After patch installation has moved onto the next steps and restarted mysql, start a new CLI session and the errors will be gone.

8. Don’t reboot the appliance part way through install
   If the install appears to be stuck do not reboot the appliance. In many cases the installer is still performing some steps and reboot will interrupt this. If you reboot the appliance part way through install, the patch will need to be reinstalled. If the patch appears to be stuck, check the progress in the patch install must gather.

GPU Install best practices

9. Get patch install must gather if there are any problems
   Support must_gather patch_install_issues contains the patch installation logs. If you open a case with Guardium support and the appliance is not down, you must attach this must gather.

- Specific patch logs:
- Fileserver -> opt-ibm-guardium-log -> must_gather -> patch_install_logs -> depot
- patch-<patch name>_<install date time>.log
- One log for each patch install attempt
- Start at the bottom of the log and work up



```
patch-10.0p400_GPU_Dec_2017_V10.1.4_20180305211021.log
patch-10.0p4030_Snif_Dec_16_2017_20180305214840.log
patch-10.0p4031_Snif_Feb_14_2018_20180305220656.log
patch-10.0p4033_Snif_Apr_23_2018_20180523174125.log
patch-10.0p4034_Snif_May_17_2018_20180523214346.log
patch-10.0p500_GPU_Apr_2018_V10.5_20180822140047.log
patch-10.0p500_GPU_Apr_2018_V10.5_20180822143433.log
patch-10.0p9997_20180305210545.log
patch-10.0p9997_20180822141325.log
```

Links

- Guardium appliance patch type information - https://www-01.ibm.com/support/docview.wss?uid=swg21964315
- Appliance patch naming scheme - https://www-01.ibm.com/support/docview.wss?uid=swg21698036
- How to download and install patch - https://www.securitylearningacademy.com/enrol/index.php?id=842
- Knowledge center on how to install patches - https://www.ibm.com/support/knowledgecenter/en/SSMPHH_10.5.0/com.ibm.guardium.doc.admin/adm/how_to_install_patches.html
- Upgrading from v9 to v10 with upgrade patch lab - https://www.securitylearningacademy.com/enrol/index.php?id=1853
- Dos and Don'ts of GPU installation - https://www.securitylearningacademy.com/enrol/index.php?id=2345
- V10 GPU release notes - https://www-01.ibm.com/support/docview.wss?uid=swg21997914
- V9 GPU release notes - https://www-01.ibm.com/support/docview.wss?uid=swg21693983
- What can I do if I see my Guardium appliance getting full? - https://www-01.ibm.com/support/docview.wss?uid=swg21511904

Questions?

IBM Security

THANK YOU

FOLLOW US ON:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

www.SecurityLearningAcademy.com

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®