Managed PVU Specification

:

The products IBM Security Guardium Standard Activity Monitor for Databases, IBM Security Guardium Advanced Activity Monitor for Databases and IBM Security Guardium Central Management and Aggregation Pack require manual steps to get proper PVU reports in IBM License Metric Tool, **in scenarios where the customer does not install a STAP on the database server.**

Product PVU calculation is based on host database server CPU Core count, where Processor Value Unit (PVU) is a unit of measure by which the Program can be licensed. The number of PVU entitlements required is based on the processor technology (defined within the PVU Table by Processor Vendor, Brand, Type and Model Number at http://www.ibm.com/software/lotus/passportadvantage/pvu_licensing_for_customers.html) and the number of processors made available to the Program. IBM continues to define a processor, for the purpose of PVU-based licensing, to be each processor core on a chip. A dual-core processor chip, for example, has two processor cores.

- ILMT Software component for all following products - IBM Security Guardium Standard Activity Monitor for Databases, IBM Security Guardium Advanced Activity Monitor for Databases and IBM Security Guardium Central Management and Aggregation Pack, is -
    - IBM Security Guardium Standard Activity Monitor for Databases
- IBM License Metric Tool automatically detect following components ***for PVU based licenses where STAP is installed on the server (as we will be storing .swidtag file while installing the STAP)***
    - IBM Security Guardium Standard Activity Monitor for Databases
- IBM License Metric Tool ***WILL NOT*** automatically detect following components ***for PVU based licenses where STAP is NOT installed on the server and it is still being monitored by Guardium (classified as managed nodes)***
    - IBM Security Guardium Standard Activity Monitor for Databases (ILMT Software component will not be found!)
    - In scenarios where Guardium STAP Agent is not installed on the database server, which is still be monitored by Guardium and data is being collected by Guardium Appliances, customer need to manually put the following managed node .swidtag file for ILMT Agent to find and list the servers in ILMT's repository.
        - ibm.com_IBM_Security_Guardium_Standard_Activity_Monitor_for_Databases_-_Managed_Node-1.0.0.swidtag on each managed server.
        - That will result in discovering the following software component:

IBM Security Guardium Standard Activity Monitor for Databases - Managed Node 1.0

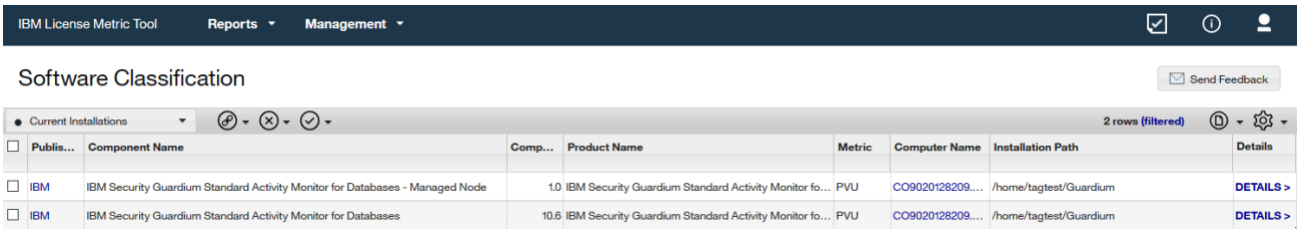
Procedure consists of several steps, described below.

Deploying tags

Step 1 - To check which server nodes are currently being reported to ILMT.

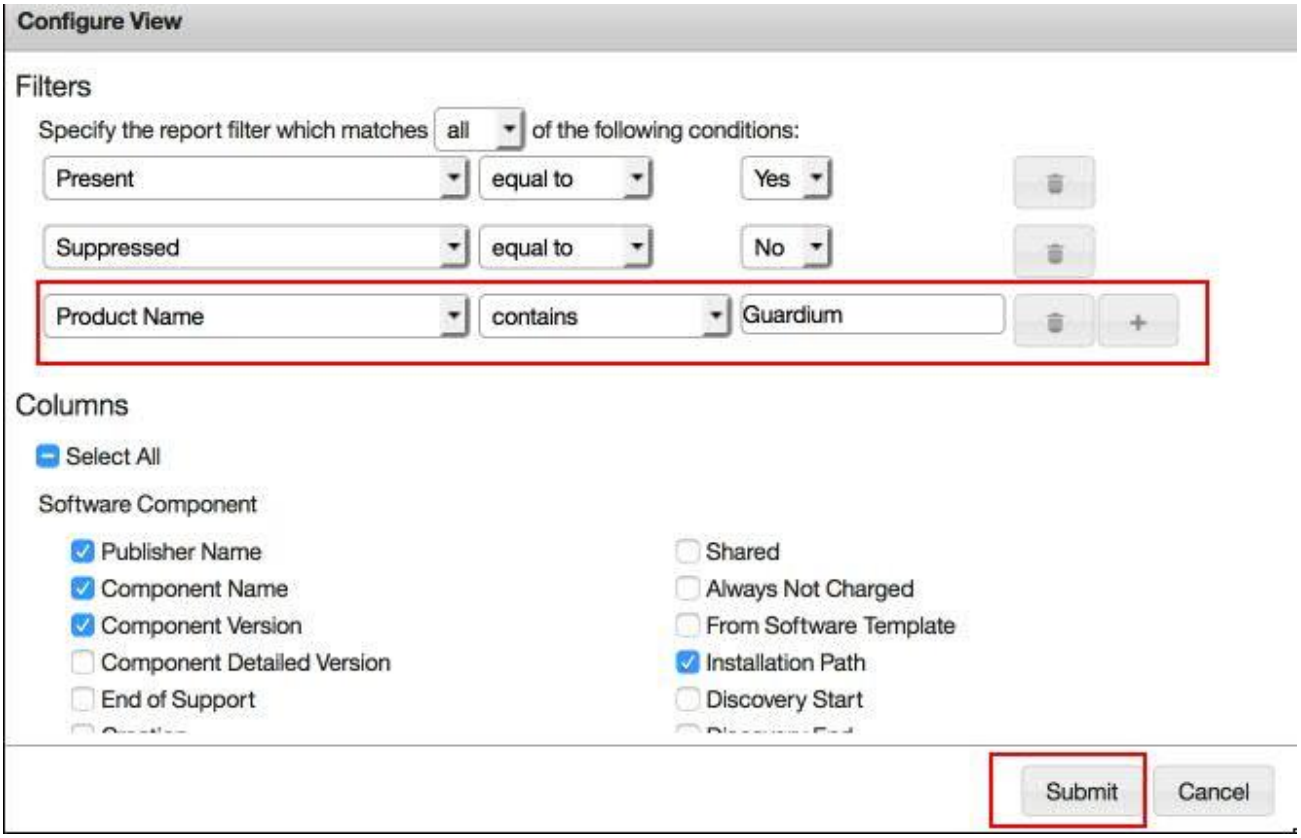
To do that, open IBM License Metric Tool console. In the navigation bar, click **Reports** > **Software Inventory** > **Software Classification.**

Click “**Configure View**…” (on the right)

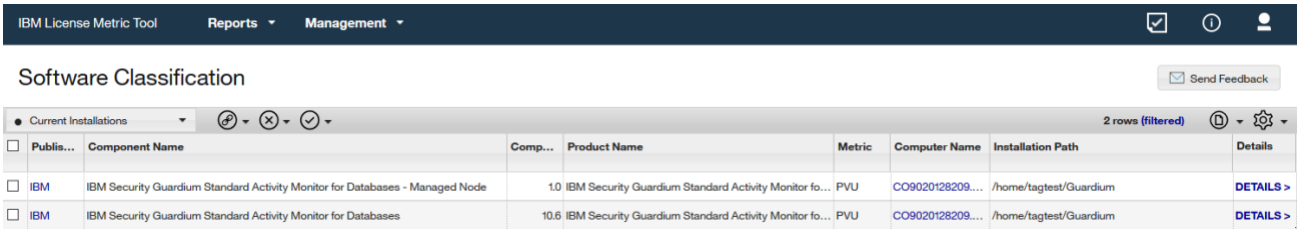


By clicking the plus button you can add new filters to the view.

Click the plus button, choose a filter, e.g. “Product Name”, choose “contains” and put the name of the component you wish to check. Below you can choose additional parameters to be listed. Click “Submit”.



You will see a list of components matching given filter. Servers, where given component is installed are listed in the column “**Computer Name**”. To get more information about the server where given component is installed, click on the name of the computer.



So now, you will see the list of servers which are currently being detected and reported in ILMT, this list will include the servers on which STAP is installed and .swidtag file is stored by STAP agent, which ILMT agent will read and update their repository.

Step 2- For servers which you are currently not seeing in ILMT, and ILMT could not detect the server, as there are no STAP's installed, you need to manually store managed node .swidtag file for ILMT to detect and report.

Follow following steps –

- A) Get the managed node .swidtag file from http://www.ibm.com/support/docview.wss?uid=ibm10787767

- B) Once you have access to the file, go to managed node server and create a new directory path and store downloaded file.
    - Example directory for customers to create to place the Managed Node SWIDTAG file:
        - Windows: C:\Program Files\IBM\swidtag
        - UNIX : /opt/IBM/GuardiumManagedNode/swidtag

Note - User should remove the Managed Node SWIDTAG file they manually placed if user ever install STAP - or the system will be counted twice

- C) After you stored this file, wait for next software scan in IBM License Metric Tool to have new component IBM Security Guardium Standard Activity Monitor for Databases - Managed Node 1.0 reported.
    - Make sure you have ILMT agent installed on this server for ILMT to detect and report managed node, to see how to install ILMT agent – refer following link about how to install ILMT agent –
    - https://www.ibm.com/support/knowledgecenter/SS8JFY_9.2.0/com.ibm.lmt.doc/Inventory/planinconf/t_installing_sua.html

ILMT Do not scan into certain directories so user should make sure, not to store swidtag file manually into those directories –

https://www.ibm.com/support/knowledgecenter/SSKLLW_9.5.0/com.ibm.bigfix.inventory.doc/Inventory/planinconf/c_excludedirs_main.html#c_excludedirs_main__exclude_dirs_list

- **Reporting of managed nodes**

Once you perform a new software scan, IBM Security Guardium Standard Activity Monitor for Databases - Managed Node 1.0 component will be detected. It will be assigned to IBM Security Guardium Standard Activity Monitor for Databases, IBM Security Guardium Advanced Activity Monitor for Databases or IBM Security Guardium Central Management and Aggregation Pack. To change the assignment to another release, follow instruction on **Assigning components to products** from IBM License Metric Tool InfoCenter:

http://www.ibm.com/support/knowledgecenter/SS8JFY_9.2.0/com.ibm.lmt.doc/Inventory/softinv/t_sc_assigning_components.html

Note –

In the event of the following situations, customer should remove the Managed Node SWIDTAG file they previously manually placed. Otherwise, ILMT will continue to discover it.

- **If customer is no longer using a managed node**
- **If customer later decides to install the Guardium STAP on the managed node server**

Periodic reviews

It is recommended to review if ILMT reporting matches currently managed hosts before signing each IBM License Metric Tool report.