IBM Security Guardium Data Protection and Guardium Vulnerability Assessment – Usage Reporting

Overview

Purpose

This document is intended to be used by IBM Security Guardium administration / management teams to understand and report usage of the product. This document provides guidance to help self-assess and declare Guardium usage to support Data Activity Monitoring (DAM) use case on target data sources in the organization.

Audience

While this document is intended for security teams using Guardium Data Protection, it could be used by other roles in the organization such as buyer, procurement etc. to help with understanding the required licenses and/or the entitlements.

Introduction to Guardium Data Protection

IBM Security Guardium Data Protection offers various data security use cases, however, this document is intended to provide guidance around usage reporting based on the Data Activity Monitoring (DAM) capability.

Guardium Licensing

Guardium Data Protection software offerings are distributed with various IBM parts based on the use cases – DAM and VA and platforms - distributed and mainframe/Z - supported. And these parts are packaged under different PIDs (Product IDs). And all Guardium parts are licensed based on data sources that are under monitoring and based on their type using specific metrics such as the count of database servers or data warehouse nodes or number of processor cores associated with the data source.

Guardium Data Protection parts and associated licensing has evolved over several years with various versions and data sources supported. It is not uncommon to have one or more Guardium parts that are based on one or more licensing models in your environment.

The below section provides an overview of Guardium licensing models and associated licensing metrics for various Guardium Data Protection software parts:

1. **Cloud Pak for Security (CP4S) Gen 3 licensing using Resource Units (RU) metric**

Guardium Data Protection parts are made available under Cloud Pak for Security (CP4S) licensing model with a single part number that can be used flexibly to support licensing for various IBM Security products including Guardium Data Protection (Data Activity Monitoring), Guardium Insights, and Guardium Vulnerability Assessment.

This was introduced in May 2021 and is the most modernized licensing model available, offering licensing flexibility and simplicity to report your usage.

2. **Resource Value Units (RVU) licensing using Managed Virtual Server (MVS) and Managed Activated Processor Code (MAPC) metrics**

With RVU-based licensing, Guardium products are licensed using either count of data sources (servers or nodes) or count of processing cores used by data sources that are under active production monitoring.

For Guardium Data Protection, the RVU/MVS metric refers to managed virtual servers which is equivalent to the count of data sources that is currently under active production monitoring. RVU/MAPC - Managed Activated Processor Core refers to the count of cores of each data source that is under similar monitoring.

RVU-based licensing was introduced circa 2015, it was intended to simplify licensing and to address data security use cases for data sources that are in the cloud. RVUs also provide a special discount table to help reduce the list prices and allow for bulk-purchase discounting to reduce the need for special bidding. As Guardium aligns with CloudPak for Security pricing, we need to adopt a different discounting table (Resource Units) for consistency. RVUs will eventually be phased out and RUs will take their place.

3. **Value Units (VU) licensing using Processor Value Unit (PVU) metric**

With PVU-based licensing, Guardium uses Value Units as the licensing metric. Specifically for distributed systems, Processor Value Units (PVU) is used that refers to the processing/compute capacity associated with data sources that are under monitoring. These PVUs are typically estimated to be the same as the count of processor cores referred to as CPU, vCPU or CPU cores.

PVUs have been around for a long time, lots of clients have them and don't know how to count them. PVUs are heavily tied to on-prem deployments. Please note that these are legacy parts and will be end of support soon, please work with your IBM sales contact to modernize/upgrade your licensing model.

Usage Reporting Scenarios

Generally, usage reporting is required in the following scenarios:

i. to assess your current usage
ii. to understand if you are leveraging the full value of Guardium based on your licenses and entitlements
iii. to provide usage reports and demonstrate compliance

What to report?

Guardium Usage in your Environment

Guardium Data Protection usage can be determined based on the functions enabled and for the data sources and their type that are under its active monitoring. Since Guardium does not have a metering function, it is important to assess usage based on your environment periodically to ensure you are maximizing the value of licenses you are entitled for and have appropriate level of software Subscription and Support (S&S).

Guardium customers typically have licenses to various Guardium products based on -

i) ***use cases*** – Data Activity Monitoring (DAM) and/or Vulnerability Assessment (VA) for
ii) ***data sources*** and their type – database, data warehouse etc. with information on its
iii) ***platform*** type – on-prem, Cloud (IaaS, PaaS or SaaS) ***and***
iv) ***environment*** type – test or non-production (sensitive data), production etc.

Guardium Data Protection is packaged based on a combination of the above attributes (use cases,data sources, etc.) into ***parts;***each part intended to provide specific support and is represented by a unique identifier and has an associated charge metric that is required for licensing purposes.

Typical Guardium deployments are made up of a number of parts. You have to ensure you have the required license (entitlements) for the in-use Guardium parts. An illustration of a usage report is provided below.

Active Guardium Parts	Licensing metric	Usage Qty	Total usage
<part_name>	< PVU/RVU/CP4S in addition to the count of Cores or DB servers or nodes etc. >		
	Total		

How to report?

Based on the scope of Guardium usage in your environment and available information on Guardium parts, licensing models and metrics, steps to report usage are provided in this section.

Generally, usage reporting is required in the following scenarios:

iv. to assess your current usage
v. to understand if you are leveraging the full value of Guardium based on your licenses and entitlements
vi. to provide usage reports and demonstrate compliance

Step 0: Pre-requisites

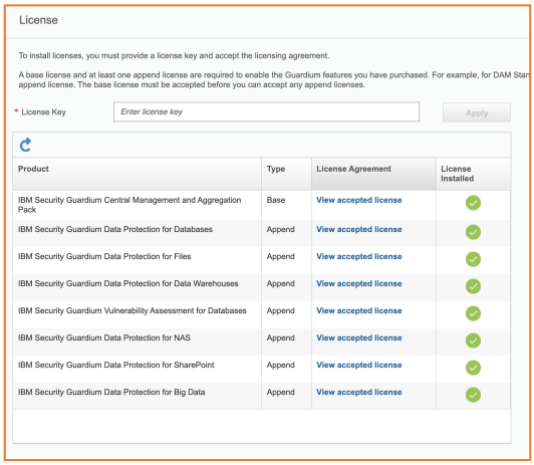
In order to report usage, it is important to find out the Guardium capabilities you have enabled in your environment and the size and type of data sources i.e. data environment.

Pre-requisites	Primary information	Additional information
use cases	Data Activity Monitoring (DAM) and/or Vulnerability Assessment (VA) for	
data sources	Their type – database (DB), data warehouse (DW), etc.	Size of deployment – > number of DB Servers or DW nodes or similar for On-prem > number of activated process cores (VPC/compute metric) associated with DBaaS or DBs in the Cloud or containerized
platform type	On-prem, Cloud (IaaS, PaaS or SaaS)	
environment type	Test or non-production (sensitive data), production etc.	

1. Determine Guardium functions enabled (licenses applied)

With the above information to get started, you can validate the licenses that are activated for Guardium Data Protection deployment in your environment. You can find this information using the 'About Guardium' link in GDP GUI and up on clicking on the Help/? button.

You can also find this information in 'License' Search in the GUI



More information on Guardium license keys is provided in Appendix I.

2. Confirm use cases and sizing

While having licenses is mandatory to access Guardium functions, your usage of Guardium Data Protection (GDP) in your environment may vary i.e. there could be deviations or changes in what you are licensed for versus what you are using. As a result, it is important to confirm with your users on this.

The primary ***use cases*** delivered with GDP are Data Activity Monitoring (DAM) and Vulnerability Assessment (VA) for ***data sources*** and their type – database, data warehouse etc. with information on its ***platform and environment*** type – on-prem, Cloud (IaaS, PaaS or SaaS) and also, production, test etc.

An inventory of your data sources with the above information is useful to determine usage of Guardium under the definition of *Production* monitoring. For each licensed part, you will have to determine the data environment size – quantity typically associated with either the number of DB Servers or DW nodes or with Processor Cores (compute) provisioned to the respective data sources. You need the quantities in order to ensure you have adequate entitlements.

For example, you can come up with a table such as -

Active Guardium Parts	Usage Qty
GDP for Databases	100 DB Servers
GDP for DB Services	10 DBaaS instance with each DBaaS instance provisioned 4 VPCs
GDP for DW	2 active + active nodes
…	
…	Etc.

You can also review the support and subscription (S&S) reports to find out more about the various Guardium product support/license entitlements you have or *declared in the past*.

S&S Part Number	Licence part Number	Description
E0MQKLL	D1NE3LL	IBM Security Guardium Data Protection for Databases Resource Value Unit (MVS) License + SW Subscription & Support 12 Months
E0MQLLL	D1NE5LL	IBM Security Guardium Data Protection for Databases for Linux on System z Resource Value Unit (MVS) License + SW Subscription & Support 12 Months
E0MQRLL	D1NEFLL	IBM Security Guardium Data Protection for Files Resource Value Unit (MVS) License + SW Subscription & Support 12 Months
E0L05LL	D1E0JLL	IBM Security Guardium Vulnerability Assessment for Databases Resource Value Unit (MVS) License + SW Subscription & Support 12 Months
E0L04LL	D1E0HLL	IBM Security Guardium Vulnerability Assessment for Databases Resource Value Unit (MVS) for z/OS for System z License + SW Subscription & Support 12 Months
E0P8TLL	D1X61LL	IBM Security Guardium Data Protection for SharePoint per Authorized User License + SW Subscription & Support 12 Months
E0P8ULL	D1X64LL	IBM Security Guardium Data Protection for SharePoint per Authorized User for IBM Z License + SW Subscription & Support 12 Months
E0L03LL	D1E0FLL	IBM Security Guardium Vulnerability Assessment for Databases Resource Value Unit (MVS) for Linux on System z License + SW Subscription & Support 12 Months
E0ELFLL	D0THQLL	IBM Security Guardium Aggregator Software Appliance Install License + SW Subscription & Support 12 Months
E0ELGLL	D0THSLL	IBM Security Guardium Collector Software Appliance Install License + SW Subscription & Support 12 Months

3. Licensing metrics to report usage

As Guardium parts are offered for specific purpose based on the 4 factors above, each part comes with its own licensing metric. It is important to important to understand the specific charge metric and its definition. And for Guardium, these typically fall under one of the following –

Licensing Metric	**Description**	**Example Parts**

What is the definition?	What does it mean? How do you compute?	What part numbers will I see for associated renewals?
Processor Value Units (PVU)	PVUs refer to Processor Value Units. Which is estimated to be the same as the count of the processor cores that are supporting the data sources being monitored/protected. PVU = (# of cores) * Value Unit (depends on platform/OS)	Typically associated with distributed data sources such as DB, DW etc. It is associated with Guardium's legacy licensing model. E0TIHLL - IBM Guardium Standard Activity Monitor E0THVLL - IBM Guardium Advanced Activity Monitor And more….
Resource Value Units (RVU)	RVUs refer to Resource Value Units. RVUs provide a special discount table to help reduce the overall cost and allow for bulk-purchase discounting. RVU is computed either based on MVS or MAPC, more information is provided below.	RVU-based licensing is a predecessor to PVU-licensing.
Managed Virtual Server (MVS)	MVS refers to Managed Virtual Servers. These are the servers or portions of the servers that are supporting the data sources that are actively being monitored/protected (Production systems). MVS = number of DB servers RVU/MVS = RVU ratio table applied to MVS	Generally used to support licensing for distributed environments and for on-prem/IaaS data sources with parts such as – GDP for Database GDP for Data Warehouse etc.
Managed Activated Processor Core (MAPC)	MAPC refers to Managed Activated Processor Cores. These are cores or the virtual cores being actively used to support the data sources that will be monitored/protected by Guardium MAPC = number of activated processor core RVU/MAPC = RVU ratio table applied to MAPC	Generally used to support licensing for cloud-native data environments and for data sources that are delivered as PaaS or SaaS or those that are containerized. Parts include– GDP for Database Services GDP for SAP HANA etc.
Resource Unit (RU)	RU refers to Resource Units that is the charge metric used under Cloud Pak for Security (CP4S) licensing model. RUs are computed based on either MVS or MAPC licensing metric. Ratio used to compute RU: 1 MVS = 360 RUs 1 MAPC = 36 RUs	Introduced as part of CP4S (gen 3) licensing.

A complete list of in-support Guardium parts, required licenses and charge metrics are provided in the table in the appendix.

4. Use OOTB reports to report usage

For Data Activity Monitoring, you may have multiple parts and different licensing models as described provided above. Once you have scoped your usage and ensure you have the correct Guardium software parts, you can either:

i) evaluate if you have adequate entitlements needed for licensing purposes OR
ii) understand and optimize your usage

To support Data Activity Monitoring (DAM), Guardium usage is determined based on the parts or PIDs and based on the type of target data sources and their platforms that are under *production monitoring* in your environment.

For Guardium DAM, it is also important to know the platforms –distributed and/or mainframe/Z – that are covered by Guardium as there are separate parts. This document is intended for DAM use case, however, when you enable Vulnerability Assessment (VA), you will need respective parts and licenses.

To report your usage, Guardium offers out-of-the-box (OOTB) reports to provide an inventory of data sources and the associated number of processors (activated) on each of those data sources. The list of reports available are shown below -

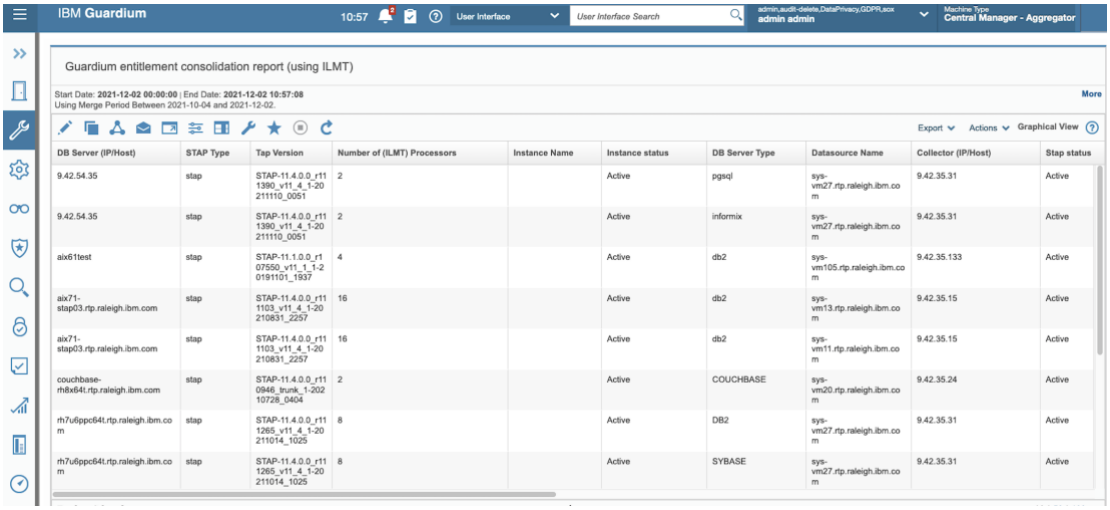
1. How to use the Entitlement Consolidation Report

'Guardium Entitlement Consolidation Report' is a pre-defined admin report that helps you understand the data sources that are under monitoring in Guardium when ILMT agents are installed. It provides details of active/inactive S-TAPs (i.e. Guardium agents) installed on respective data servers (DB. DW etc.).

If the ILMT agent is installed, the report shows the processors value of the data server. This report does not replace ILMT requirements in any sense (Follow ILMT compliance and audit requirements).

If the ILMT agent is not installed, the processor value is blank. This report helps indicate the processor value of the server with an installed, and active S-TAP. Please note that ILMT agents are available for distributed and on-prem data servers only.

To find this report, you can search for the 'Entitlement consolidation report' in the search bar from the GDP GUI homepage.



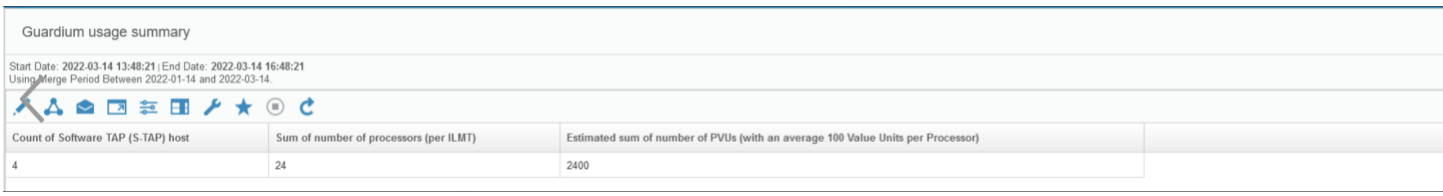
Note:
Installing ILMT is not an option for all data sources, particularly, for monitoring cloud (PaaS, SaaS) and containerized datasources. In these cases, you can choose to self-declare /self-report your usage. We have more information available here -

2. How to use the Summary table

'Guardium usage summary' report provides summary with insights into sum count of unique data sources (S-TAP hosts) and the sum of processor cores, if data servers have ILMT agents installed on them. This report can be used in combination with 'Guardium entitlement consolidation report' when you have multiple DBs on the same server/host/ip.

This report is available only with GDP versions 11.1 and onwards with the following patch bundles as released –

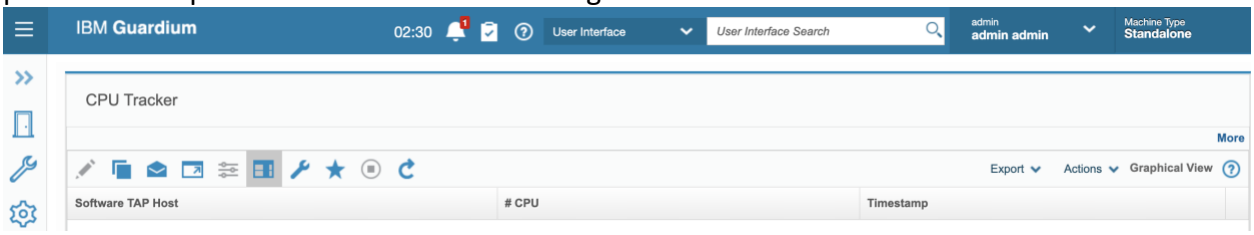
Version	Patch bundle
GDP v11.1	Mar 2022
GDP v11.2	Aug 2022
GDP v11.3	Mar 2022
GDP v11.4	Feb 2022
GDP v11.5	Base/GA



To find this report, you can search for the 'Usage summary report' in the search bar from the GDP GUI homepage.

3. How to build reports using CPU Tracker

Guardium Data Protection provides another pre-defined admin report OOTB named - 'CPU Tracker'– which can be used to create a distributed report based on it. The CPU tracker report provides a snapshot of the current monitoring in Guardium.



While the above reports provide snapshot of usage of Guardium, to report on usage for specific time periods, distributed reports can be setup. Appendix IV provides a way to these reports using the CPU tracker report.

4. Reporting without ILMT

In case of non-availability of ILMT agents especially for reporting monitoring for cloud-native (as-a-service) and containerized data sources, you can self-declare Guardium usage.

Licensing for cloud-native and containerized data sources is available only with RVU- and CP4S (gen 3)-based licensing. And it is based on MAPC charge metric which refers to the number of cores/CPUs provisioned to the respective data source, for example, 1 VPC is equivalent to 1 MAPC in case of monitoring AWS RDS MySQL and similarly, 1 vCPU of Azure SQL is equivalent to 1 MAPC.

5. Consolidate and report

Once you have one or more of the above reports, you can consolidate them for reporting purposes us. The above OOTB reports can be used to estimate your usage and find out how you can optimize the entitlements to realize the value of Guardium.

In addition, you can use these to report your usage to IBM or other external teams. You can also map the various parts you have to the above reports based on the respective Guardium parts you have (each with its own LI) and from additional screenshots, as needed. The following provides additional guidance on how to map data sources (hosts) that are under Guardium protection. These are available by GDP versions:

GDP v11.4	https://www.ibm.com/support/pages/node/6490351
GDP v11.3	https://www.ibm.com/support/pages/map-server-ips-within-ibm-security-guardium-v113-instead-using-ibm-license-metric-tool-ilmt

GDP v10.6	https://www.ibm.com/support/pages/mapping-server-ips-within-ibm-security-guardium-v106-instead-using-ibm-license-metric-tool-ilmt

Relevant information

Appendix I: Guardium Products and License Type

To enable licenses to access various features in Guardium, in addition to the Base license, an Append license key is provided. The table below provides an overview of the various Products that are activated based on the append license.

Guardium Products	Append License Type	License Description
Data Protection - Structured	DAM Standard	Adds core functionality for data activity monitoring.
	DAM Advanced	Adds DAM Standard functionality plus fine-grained access control, masking, quarantine, and blocking (Activity terminate).
	Data Protection	Advanced functionality with different pricing metric
Data Protection - Unstructured	FAM Standard	Adds core functionality for file activity monitoring.
	FAM Advanced	Adds FAM Standard functionality plus blocking.
Vulnerability Assessment	VA	Adds functionality for vulnerability assessments plus Database Protection Service (DPS), Change Audit System (CAS), and database entitlement reporting.

Appendix Guardium Parts

Find out more about the PIDs to find out Guardium parts and entitlements
Determine Guardium PIDs included, examples include the following:

PID / Product Name	Parts
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Data Protection	IBM Security Guardium Data Protection for Databases IBM Security Guardium Data Protection for Data Warehouses IBM Security Guardium Data Protection for Big Data IBM Security Guardium Data Protection for SAP HANA IBM Security Guardium Data Protection for Database Services IBM Security Guardium Data Protection for Data Warehouses IBM Security Guardium Data Protection for Big Data IBM Security Guardium Data Protection for SAP HANA IBM Security Guardium Data Protection for Database Services IBM Security Guardium Vulnerability Assessment for Databases
PID 5725-V56 - IBM Security Guardium for Files - IBM Security Guardium Data Protection for Files	IBM Security Guardium Data Protection for Files
PID 5737-H31- IBM Security Guardium for SharePoint - IBM Security Guardium Data Protection for SharePoint	IBM Security Guardium Data Protection for SharePoint

PID 5737-H30- IBM Security Guardium for NAS - IBM Security Guardium Data Protection for NAS	IBM Security Guardium Data Protection for NAS
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Database Vulnerability Assessment Solution 14	IBM Security Guardium Vulnerability Assessment for Databases
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Database Activity Monitor Group	Standard Data Activity Monitoring: IBM Security Guardium Standard Activity Monitor for Databases IBM Security Guardium Standard Activity Monitor for Data Warehouses IBM Security Guardium Standard Activity Monitor for Big Data IBM Security Guardium Standard Activity Monitor for Data Warehouses IBM Security Guardium Standard Activity Monitor for Big Data Advanced Data Activity Monitoring: IBM Security Guardium Advanced Activity Monitor for Databases IBM Security Guardium Advanced Activity Monitor for Data Warehouses IBM Security Guardium Advanced Activity Monitor for BigData IBM Security Guardium Advanced Activity Monitor for Databases IBM Security Guardium Advanced Activity Monitor for Data Warehouses IBM Security Guardium Advanced Activity Monitor for BigData
PID 5725-V56 - IBM Security Guardium for Files - IBM Security Guardium Activity Monitor for Files Group	IBM Security Guardium Standard Activity Monitor for Files IBM Security Guardium Advanced Activity Monitor for Files
PID 5725-I12 - IBM Security Guardium Data Security and Compliance - IBM Security Guardium Central Management and Aggregation Group	IBM Security Guardium Central Management and Aggregation for Databases Pack IBM Security Guardium Central Management and Aggregation for Data Warehouses Pack IBM Security Guardium Central Management and Aggregation for Big Data Pack

Appendix II: Guardium Licenses

For each of the parts listed below, based on the licensing model (as described earlier), the charge metrics vary. These are provided below -

	PVU	RVU	CP4S
IBM Security Guardium Data Protection for Databases			
IBM Security Guardium Data Protection for Data Warehouses			
IBM Security Guardium Data Protection for Big Data			
IBM Security Guardium Data Protection for SAP HANA			
IBM Security Guardium Data Protection for Database Services			
IBM Security Guardium Data Protection for Data Warehouses			
IBM Security Guardium Data Protection for Big Data			
IBM Security Guardium Data Protection for SAP HANA			
IBM Security Guardium Data Protection for Database Services			
IBM Security Guardium Vulnerability Assessment for Databases			
IBM Security Guardium Data Protection for Files			

IBM Security Guardium Data Protection for SharePoint			
IBM Security Guardium Data Protection for NAS			
IBM Security Guardium Vulnerability Assessment for Databases			
Standard Data Activity Monitoring:			
IBM Security Guardium Standard Activity Monitor for Databases			
IBM Security Guardium Standard Activity Monitor for Data Warehouses			
IBM Security Guardium Standard Activity Monitor for Big Data			
IBM Security Guardium Standard Activity Monitor for Data Warehouses			
IBM Security Guardium Standard Activity Monitor for Big Data			
Advanced Data Activity Monitoring:			
IBM Security Guardium Advanced Activity Monitor for Databases			
IBM Security Guardium Advanced Activity Monitor for Data Warehouses			
IBM Security Guardium Advanced Activity Monitor for BigData			
IBM Security Guardium Advanced Activity Monitor for Databases			
IBM Security Guardium Advanced Activity Monitor for Data Warehouses			
IBM Security Guardium Advanced Activity Monitor for BigData			
IBM Security Guardium Standard Activity Monitor for Files			
IBM Security Guardium Advanced Activity Monitor for Files			
IBM Security Guardium Central Management and Aggregation for Databases Pack			
IBM Security Guardium Central Management and Aggregation for Data Warehouses Pack			
IBM Security Guardium Central Management and Aggregation for Big Data Pack			

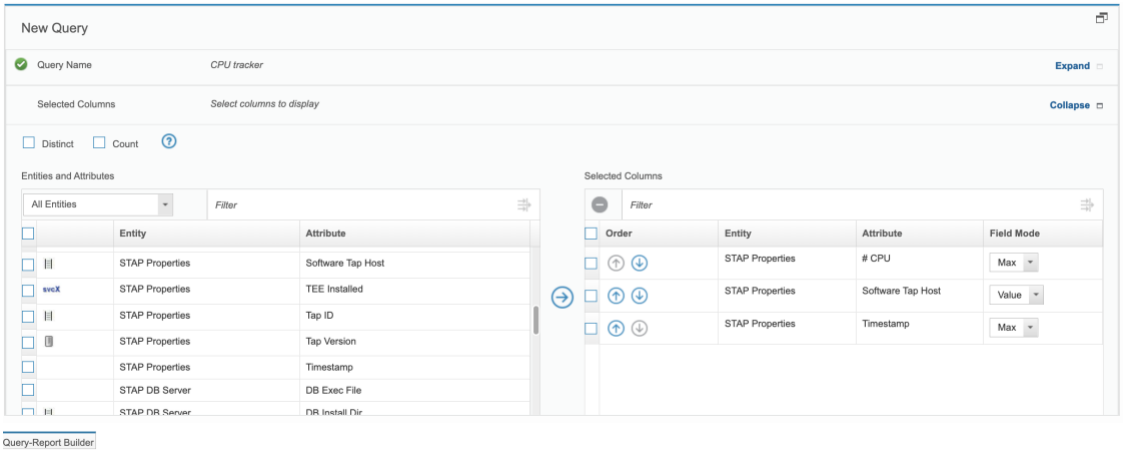
Appendix III: Licensing Metrics for Special Considerations

Appendix IV: Distributed Reports with CPU Tracker

For continuous visibility and for reporting needs, a distributed SQL-generated report can be set up that is similar to the CPU Tracker with the only difference that the new one has a time frame condition, with the ability to specify 'Query From' and 'Query To' run-time parameters as all other user-generated reports. To create distributed reports in Guardium, follow the steps below -

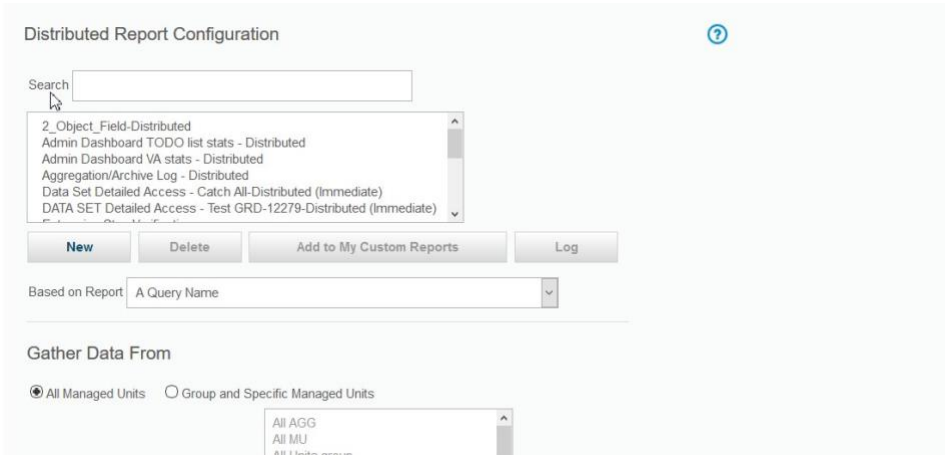
1. Go to Query Report Builder from the search field or navigate to Reports > Report Configuration Tools > Query-Report Builder and using the STAP Status domain, create a new report:

2. Add the columns as shown (for a report similar to the CPU Tracker) or add/remove columns as needed (new query is named "A Query Name"):

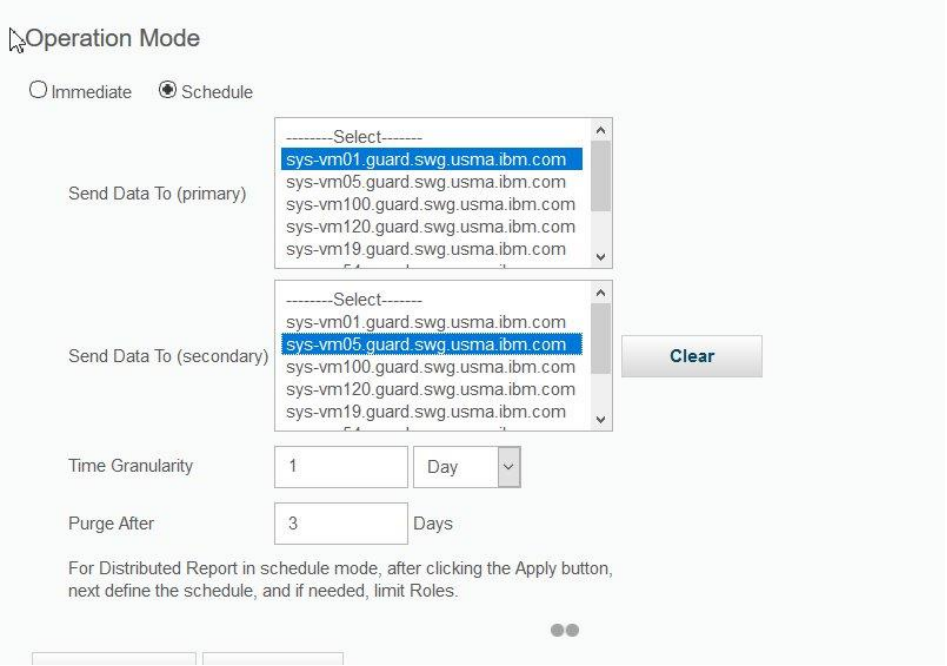


3. Create a tabular report from the Query

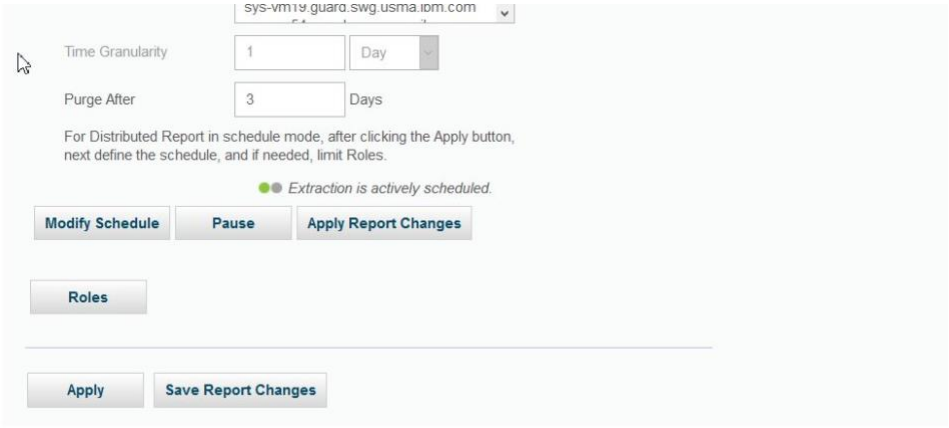
4. Go to the distributed report builder and create a new report based on the report/query you just created (note that we chose "A Query Name" In the pull down menu):



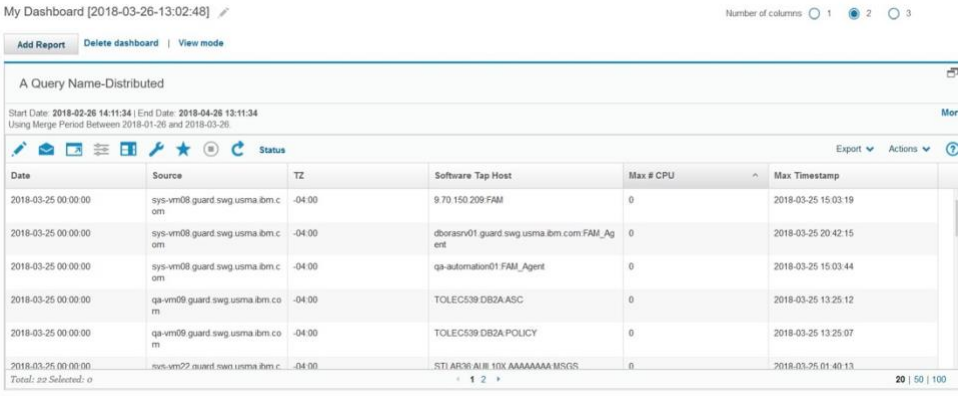
5. Choose the "Schedule" mode and set the primary and secondary destination. Recommend at least for the primary a target machine other than the CM (target machine can be define in the CLI):



6. Define the time granularity and schedule (not shown)to make it active:



7. Add the default report generated to a dashboard, this is the one that shows the consolidated data:
Note there are some additional columns for the distributed report, this is the default report generated, you can define any report/query you need based on the information gathered for the distributed report



Note that the number of processors depends on whether ILMT is installed in the database server and the S-TAP Version.

Note that this is an example which I based on the CPU Tracker, however since it is using standard tools you can add/remove columns and conditions as needed to both the base query and the distributed one.