SONARG

jSONAR
Simplifying Security

case study

Upgrading a Large Guardium Environment in Days Rather than Months

By: Kyle Clever and Ron Bennatan

This case study outlines a new approach to upgrading a large Guardium environment as undertaken by a large US bank. The bank purchased Guardium in 2008 and created one of the more mature implementations with solid processes, reliable delivery of audit reports to various bank constituents and full redundancy in all of the components needed for the Database Activity Monitoring (DAM) implementation. Recently the bank's DAM program has undergone explosive growth in capacity, increasing their collector footprint from 25 to over 150 with a plan to reach 300 collectors by the end of 2017. This is driven by the rapid expansion of database servers to be monitored, along with a desire to open their Guardium policy in order to collect more security specific data vs. audit/compliance data. The implementation now spans 150+ collectors in two data centers monitoring over 10,000 databases on 2,000+ servers, including Oracle, SQL Server and Teradata. The entire DAM environment is virtualized and running on VMWare. In order to preserve one of the lowest FTE-to-appliance ratios amongst all Guardium clients, effectively 1FTE: 150 collectors, the bank realized that it must have a more efficient architecture and a high level of automation.

In 2016 the bank implemented the SonarG Big Data solution for Guardium. In that process over 10 aggregators were eliminated and all data flowed into a single SonarG VM (supported by the same Guardium headcount), along with a second DR machine. In addition to simplifying the environment, removing 40+ TB of SAN by reducing the storage footprint of each collector from 600G to 200G, reducing costs and eliminating PMRs, SonarG allows the bank to keep 13 months of online data while also providing for fast reporting. Reports that used to take hours to generate on multiple aggregators now take minutes to generate. In addition, the increased speed of analytics, and the improved reliability of report delivery has dramatically increased due to simplifying the data processing system (SonarG).

In May of 2017 the bank upgraded the entire Guardium environment from Version 9.5 to Version 10.1.2. The industry benchmark in terms of effort for upgrading such a large environment is ~4 months and relying upon several FTEs. Instead, the bank completed the entire upgrade in a single weekend – starting Friday night and completing by Sunday evening using a single FTE.

This was made possible through an innovative upgrade procedure devised by the bank – a first-of-a-kind. Guardium upgrades are usually difficult, time-consuming and error-prone. It is normally hard to foresee how long an upgrade will take since the process of upgrading of each appliance can break, and manual processes are required. Each appliance, and especially aggregators, takes an extended time since all the data needs to be migrated from the V9 schema to the V10 schema. The bank saw these difficulties in previous upgrades and therefore devised an "upgrade-less upgrade" procedure.

The main concept adopted was not to upgrade any of the appliances. Instead, new V10 VMs were built to replace the V9 VMs. Because all the data is constantly pushed to SonarG (on an hourly basis) there was no need to keep anything on the appliances themselves. SonarG itself is version-agnostic and does not require any patches or configuration changes. This allows for SonarG; to automatically merge data, no matter what Guardium version is sending data to it. Moreover, there were no aggregators to upgrade – removing the most costly and time consuming phase of any traditional upgrade. Finally, the entire upgrade was done without a single minute of downtime for any part of the environment and all data was continuously captured and delivered to SonarG.

The procedure conceived and implemented by the bank is described below:

1. The backup CM was validated and checked.
2. The main CM was shutdown and all managed units moved to the backup CM.
3. A V10 CM was started instead of the main CM and the configuration data (groups, policy etc.) loaded. The v10 CM was linked to the SonarG node using the appropriate gradpi calls.
4. At this point, the following steps were performed for all collectors, 10-20 collectors at a time. Note that the process was done in batches since there was only one FTE doing all the work.
   a. The inspection core (the sniffer) was shut down. This caused each of the STAPs connected to any of these 10 collectors to failover to another collector (each STAP in the bank is connected to multiple collectors for redundancy).
   b. The admin then waited a little over an hour – ensuring that the last bit of data was flushed to SonarG.
   c. The v9 VM was then terminated.
   d. A new v10 VM was built using the same hostname, VM guest, and IP address as the one terminated, linked with the v10 CM and scheduled for SonarG data extracts. The registration and the scheduling were all done using sonarcli grdapi automation.
5. The v9 CM was then terminated (at this point there were no more managed units pointing to it) and the backup v10 CM became the primary CM.
6. The entire system was then checked using grdapi scripts and using CM and SonarG views. All STAPs were also checked.

By Monday the entire system was at v10.1.2. There was no system downtime, no gap in audit collection, and no gap in report delivery.

A traditional Guardium upgrade process is outlined in the graphic below. Typically a weekend is devoted to upgrading only 10 collectors and 1 or 2 aggregators while the following week is devoted to "fallout" activities and recoveries that often occur. Each such weekend usually requires attention by multiple Guardium admins and almost always involves opening PMRs, requiring help from IBM support. Moreover, many people require audit downtime on the systems while the upgrade occurs.

15 WEEK TIMELINE

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Upgrade Collectors 1-10;	Upgrade Collectors 11-20;	Upgrade Collectors 21-30;	Upgrade Collectors 31-40;	Upgrade Collectors 41-50;	Upgrade Collectors 51-60;	Upgrade Collectors 61-70;	Upgrade Collectors 71-80;	Upgrade Collectors 81-90;	Upgrade Collectors 91-100;	Upgrade Collectors 101-110;	Upgrade Collectors 111-120;	Upgrade Collectors 121-130;	Upgrade Collectors 131-140;	Upgrade Collectors 141-150;
Aggregators 1-2;	Aggregators 3-4;	Aggregators 5-6;	Aggregators 7-8;	Aggregators 9-10;	Aggregators 11-12;	Aggregators 13-14;	Aggregators 15-16;	Aggregators 17-18;	Aggregators 19-20;	Aggregators 21-22;	Aggregators 23-24;	Aggregators 25-26;	Aggregators 27-28;	Aggregators 29-30;
Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues	Fix Issues

Using the simplified data collection architecture achieved by the addition of SonarG and the bank's innovative "upgrade-less upgrade," the bank was able to reduce a process that normally required 3-4 months, substantial downtime, audit gaps, and multiple FTEs, into a highly efficiency and mostly automated process, completed in a single weekend and with no audit coverage disruption.