IBM Security Guardium Administrator Responsibilities Guide

Version 2 2016-03-01

This document lists your main responsibilities as a Guardium administrator for v9 and v10. To maintain a healthy environment you should consider or implement each of the points below. This guide is not exhaustive, chapters noted in red refer to chapters in the Guardium Deployment Guide which covers all areas of Guardium administration.

Over time additions may be made to this guide. Always check online to ensure you have the up to date version.

Maintaining Access

Up to date access details are crucial for smooth running of the environment for all users.

- Maintain GUI admin, accessmgr and CLI account passwords. If you do not hold the accessmgr account details you should be aware of who in your organisation does.
- Maintain list of guardcli accounts in use and their associated GUI user.
- Keep root passkey for each appliance for support access in case of emergency.

Responding to problems

Alerting should be used to quickly identify and react to common problems. Chapter 3.9.8 details the following correlation alerts to implement.

- Aggregation/Archive errors (predefined) How to troubleshoot aggregation or archive errors.
- Scheduled Jobs Exceptions (predefined) Knowledge collection: Scheduled jobs exceptions.
- Inactive STAPs Since (predefined) What to do if you get “Inactive S-TAPs Since” alerts.
- No Traffic (predefined) What to do if you receive “No Traffic” alert. How to check if the correct data is being logged on my Guardium Appliance?
- Sniffer restarts (user created) How to alert when the number of sniffer restarts is high. For further details on how to improve sniffer performance see chapter 7.1.2
- Disk space (user created). How to set up disk space alert. What to do if I see my Guardium Appliance getting full?
- If you are unsure how to contact Guardium support, check chapter 5 and appendix A of the support handbook. When assessing the severity of your problem see: What type of problem can I consider to be severity 1?

Monitoring performance

Monitoring the environment on a day to day basis is required to understand the typical behaviour. This knowledge is useful when making changes or troubleshooting problems.

- Configure unit utilization report to monitor inspection-core performance in centrally managed environments. See chapter 7.1.2 - configuring the operational dashboard.
- In Centrally managed environments, set the Enterprise STAP view report to see status of all STAPs.
- Enable S-TAP statistics to monitor UNIX STAP performance. See chapter 7.1.1

Reviewing configurations

Incorrect or inefficient configuration is the root cause of many Guardium problems. You are responsible for ensuring your environment is configured correctly.

- Ensure all appliances meet the minimum system requirements – v9. V10.
- Ensure a system backup strategy is in place for disaster recovery. See chapter 8.
- Ensure the data management configurations (chapter 3.9.3-5) and schedule (chapter 3.9.6) are set in a logical way. Common mistakes include:
  - Filling up appliance database due to purge settings.
  - Taking duplicate archive files.
  - Purging data that has not yet been archived or exported.
  - Scheduling data management processes to overlap.
- Set STAP verification schedule to verify inspection engine configurations are correct.
- Do not schedule audit process jobs to overlap with aggregation jobs, other audit processes jobs or run before 1:00 am.
- Ensure audit process results are purged correctly. How do I purge off old audit results from Guardium? Check and sign off audit process receiver to-do lists.
- Periodically review your policy against business requirements, especially if new STAPs are added. Use chapter 5.2 and 5.4 to help with policy definition.
- Periodically review report definitions and results against business requirements. Reports should be targeted to contain only relevant information for the receivers. For information on defining queries and reports see chapter 5.2 and 5.5.
- Periodically review correlation alert definitions. If you are getting many alerts but taking no action you need to review the alerting strategy. Disable alerts you do not plan to use.

Keeping informed

Guardium regularly releases alerts, fixes, documentation and tech talks. Keeping informed ensures your knowledge is up to date and you do not miss important fixes.

- The latest appliance patches and agents are available on fix central. Install the latest packages to eliminate known problems.
- Subscribe to receive support notifications.
- Check the knowledge center for the latest documentation.
- Browse or search technotes for problem troubleshooting.
- Educate yourself with previous and upcoming tech talks and the Guardium youtube channel.
- Interact with your fellow Guardium administrators and IBMers in Developerworks and LinkedIn.