Guardium Gap Analysis

Are STAPs Green but No Audit Traffic?

Many clients have noticed that sometimes even though STAP agents show green on Guardium dashboard, Guardium is not collecting traffic. This usually happens because a DBA made changes on a database. There are times this goes unnoticed for few days or weeks. Gap Analysis is a proprietary solution developed by Adaptive Systems Inc to identify gap in Guardium monitoring and notify within 24 hours if this is happening rather than being in a false impression that "all is well".

What it takes to implement solution?

There are four pieces to implementation.

1) Local Scripts: Implement script on each database server that is monitored by Guardium. These scripts will try to logon to monitored databases by fake ID and fake password.

2) Remote Scripts: One script per OS platform run against all OS specific databases that are monitored by Guardium. Similar to local scripts, the remote scripts will try to logon to every database monitored by Guardium with fake user ID and password. For Example: One script on XYZDBHYPQ01 will run against all MSSQL databases monitored in Test environment.

3) Schedule: Schedule above scripts to run every fifteen (OR client specified) minutes.

4) Schedule Audit job and Distribute: Audit job "--Gap Analysis" will run every morning and email the report to

WHAT WE CAN DO

By combining our domain knowledge in data protection, our hands-on engineering experience with IBM Guardium and our breadth of data management experience we can help transform and adapt our clients to the cyber security era of technological change.

Sample Gap Analysis Report: Column "Count" indicates traffic is being captured.

Database Protocol	Database Name	Server Host Name	Client IP	Count
MS SQL SERVER		LST01	28.115	1
MS SQL SERVER	AC RADE_812V2	ARQ02	28.115	5
MS SQL SERVER	AC RADE_812V2	ARQ02	26.51	2
MS SQL SERVER	AD GNQA2	ACQ171\AEC	28.115	169
MS SQL SERVER	AD GNQA2	ACQ171\AEC	28.12	168
MS SQL SERVER	CC E	COQA31\COM	28.115	15
MS SQL SERVER	CC E	COQA31\COM	28.32	14
MS SQL SERVER	CC E	COQA31\COM	8.60	14
MS SQL SERVER	EC DSTAGING	ACF133\ECMF01	28.115	167
MS SQL SERVER	ED	BLT01	28.115	167
MS SQL SERVER	ED	BLT01	28.101	166
MS SQL SERVER	HY	YPQ11\HYPD01	28.115	167
MS SQL SERVER	HY	YPQ12\HYPQ01	28.115	167
MS SQL SERVER	HY	YPQ12\HYPQ01	28.116	166