IBM Security Guardium 10.1 動作検証

データベース・セキュリティ・ソリューションの IBM Security Guardium 10.1 による DB2 for IBM i のアクセス監視の検証を実施しました。DB2 や Oracle といった一般的なデータベース以外にも、IBM i のデータベースへのアクセス監視も問題なくできることを検証しました。

背景・課題

IBM i のお客様をターゲットにした Guardium の更なる拡販、提案の為、導入/構築が出来るようになる必要がありました。
以前、IBM i のお客様に別件の提案/導入を行った際、IBM i のオペレーションに不慣れなこともあり設定等で苦労した経験がありました。そのため、今回は IBM i を確実に操作するスキルを取得しつつ、対 IBM i の Guardium 動作確認として、DB2 for IBM i のアクセスログ取得ができるところまで練習を兼ねて検証を行う必要がありました。

CAMSS センターでの検証概要

使用したハード/ソフト
・IBM Power 720 (8202-E4D) ／ IBM i V7.1
・SUPERMICRO IA サーバ ／ IBM Security Guardium 10.1
(IBM Security Guardium Data Protection for Databases)

Guardium のコンポーネントは、コレクターと呼ばれるサーバー・モジュールと、S-TAP と呼ばれるクライアント・モジュールから構成されます。
コレクターは、設定された監視ポリシーやルールに基づき、S-TAP から送信されてきたアクティビティをロギングと解析を行い、アラートを発する等の処理を実行します。
S-TAP は、システム上のすべてのデータベース・アクティビティを取得して、コレクターに送信します。

今回、コレクターは、IBM ソフトウエア アクセス カタログからダウンロードしたコンポ

ーネントファイル（＝仮想アプライアンス：Guardium 用に Linux をカスタマイズした専用 OS と Guardium が同時に展開される）を IA サーバに導入。IBM i 用の S-TAP は、IBM Fix Central より最新版をダウンロードして、IBM I V7.1 に導入。

以下 URL も参考にして導入/構築を行いました。（参考資料の Guardium のバージョンは 9.0）

＜ IBM InfoSphere Guardium を使用し、IBM DB2 for i のデータベース・アクティビティーのモニタリングと監査を行う方法＞

https://www.ibm.com/developerworks/jp/data/library/i-infosphere_guardium_db2/

主な検証内容：

・Guardium と DB2 for IBM i との通信構成と疎通確認

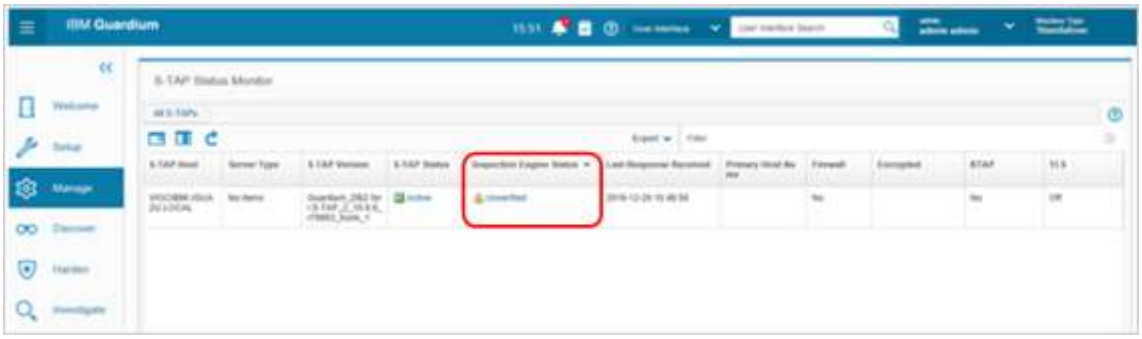
・レポート作成と表示の検証

・ポリシー、ルールの動作検証

・フィルタルールの動作検証

・ルールに抵触した際のレポート表示確認

＜Guardium と DB2 for i との接続状況画面＞

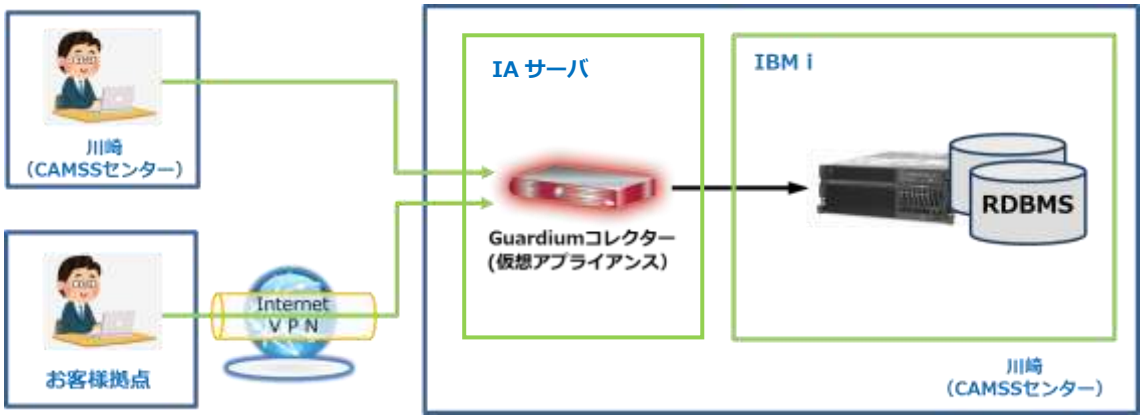


※ Inspection Engine Status（検査エンジンの状況）が、「Unverified」になっていますが、DB2 for IBM i の場合は、このステータスで問題ありません。通常は、例えば DB2 等の場合は、「Pass」になっている必要があります。

＜レポート画面＞

※ 設定したポリシーに違反したアクセスがあった場合、上記のようにレポートにアラートが表示されます

今回、IBM i に、以前導入した旧バージョン（v9.5）を上書きする形で新しいバージョンのS-TAP（v10.1）を導入しましたが、Guardium との通信が上手くできませんでした。
原因は、旧バージョン導入時に構成した IBM i のコンフィギュレーション・ファイル（QSYS2.SYSAUDIT）が、古いままで更新されなかったことと判明。手作業（SQL 文の発行）で正しい値に更新することで解決できました。



パートナーさまの声

Guardium 10.1 を使用した DB2 for IBM i へのアクセス監視が出来ることを確認できました。これで、IBM i のお客様にも自信を持って提案できます。
また、IBM i での基本動作やオペレーションも理解することができ大変助かりました。