z/OS V1R13

PKI services: Optional use of DB2 for object store and JCL

Session objectives

- Digital certificates usage has been growing
- Continuous enhancements to fulfill customer requirements
- Two main components on certificate support:
  - RACF: RACDCERT command and the R_datalib callable service
  - PKI Services
- At the end of this presentation, you should have an understanding of the support from:
  - PKI Services:
    - Optional Use of DB2 for ObjectStore and Issued Certificate List backends

Overview

- **Problem Statement / Need Addressed**
  - Need to scale PKI's issued certificate list (ICL) to contain millions of certificates.
  - Provide a means to add more flexible queries and reports on PKI requests and issued certificates in later releases, if necessary.
- **Solution**
  - Allow customers the option to use DB2 for z/OS as the PKI backing store.
  - Retain VSAM as the default backing store choice.
  - Provide utilities to migrate existing PKI data from VSAM to DB2.
- **Benefit / Value**
  - DB2 scales to larger databases than the VSAM implementation.
  - DB2 allows customers to write customized queries and reports.
  - Current customers can stay with VSAM if they don't want or need DB2.

Usage and invocation

- Stop PKI Services (if using PKI within a Sysplex, shut down all PKI Service daemons)
- Update and run sample jobs IKYCDB2 (SPUFI job that sets up DB2 tables) and IKYCBIND (JCL that builds DB2 package and plan) as necessary to match you system's configuration.
- (Optional) If you already have PKI Services set up with the VSAM backend, run the utility vsam2db2 to copy the contents of the VSAM datasets to the DB2 tables, for example:

```
vsam2db2 -o \'pkisrvd.vsam.ost\'
         -i \'pkisrvd.vsam.icl\'
         -b DSN9
         -k MasterCA
         -r
         -D MasterCA
          -a
```

- Update the configuration file pkiserv.conf, setting DBType, DBSubsystem and DBPackage values as appropriate for your local system., for example:
  - DBType=DB2
  - DBPackage=MasterCA
  - DBSubsystem=DSN9
- Start the PKI Services daemon

Interactions and dependencies

- Software dependencies
  - DB2 V9 or above
    - Must be locally installed and available – no remote server support.
- Hardware dependencies
  - None
- Exploiters
  - PKI Services customers

Migration and coexistence considerations

- Migration
  - Refer to Usage and invocation
  - Note: PKI Services does not maintain VSAM datasets and DB2 tables for the same Object Store and ICL in tandem. Once a backing store is selected in the PKI Services configuration file, only that backing store is updated
- Coexistence
  - None

Installation

- Requires DB2 V9 or above to be installed and operational on the same system where PKI Services is running.
  - PKI Services must be configured to exploit DB2 if it is installed and available: no auto-detection or auto-selection of DB2 is done.

- Customer selects the backing storage mechanism by tailoring the post-installation jobs IKYSETUP, IKYCVSAM, IKYCDB2 (new) and IKYSBIND (new).

▪ Remote DB2 servers are not supported – DB2 server must be local.

Note: DB2 for z/OS is a separately installed and priced product. Customers do not get DB2 for free with PKI.

Session summary

▪ You should now have an understanding of the support from **PKI Services:**
  – Optional use of DB2 for ObjectStore and issued certificate list backends

Appendix - References

▪ Publication references
  – PKI Services Guide and Reference (*SA22-7693*)
  – Security Server Command Language Reference *(SA22-7687)*