Db2 13 security and IBM Z synergy

RACF contention
Decrypt only keys
Continuous compliance

Reduce RACF contention

FL 100

Db2 12 authorization caching

- Db2 does not cache plan authorization checks when Access Control Authorization Exit (ACAE) is used
  - External security via RACF vs Db2 native security
- AUTHCACH subsystem parameter sets default for plan authorization cache size
  - Override with CACHESIZE on plan
- Global authentication cache for remote TCP/IP connections purged every 3 minutes

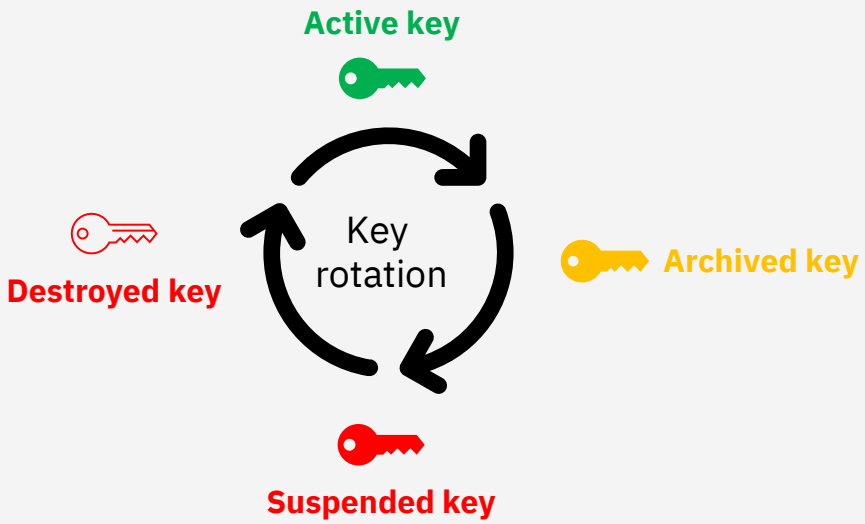
Db2 13 authorization caching

- Db2 caches plan authorization checks when ACAE used if based on RACF privilege class for plans (MDSNPN)
  - AUTHEXIT_CACHEREFRESH = ALL
  - z/OS 2.5 +
- Plan authorization cache
  - More auth IDs per plan
  - AUTHCACH hidden; behaves as if 4K
- Global authentication cache: Db2 considers timestamp; if reauthenticate with match within 3 minutes, extend validity [n/a if MFA]
  - AUTHEXIT_CACHEREFRESH = ALL

Db2 and decrypt-only archived encryption keys

FL 100

z/OS Integrated Cryptographic Service Facility (ICSF) supports decrypt-only archived encryption keys with z/OS 2.5



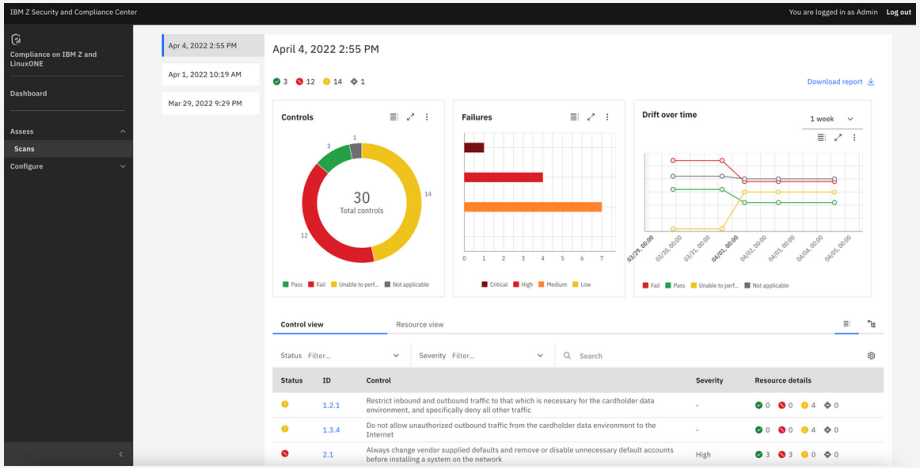
- Key label can be specified in Db2:
  - ENCRYPTION_KEYLABEL zPARM
  - KEY LABEL option in DDL
    - ALTER STOGROUP
    - ALTER TABLE
    - CREATE STOGROUP
    - CREATE TABLE
- If key label specified is decrypt-only:
  - SQLCODE -20223
  - DSNX242I message
- Discover issue earlier in process

Db2 support for z/OS continuous compliance

FL 100

Db2 gathers security information in SMF type 1154, subtype 81, records

- Use with tools, such as IBM Z Security and Compliance Center
- Information to determine whether:
  - Installation specified default ID has been changed
  - Security port is configured
  - Authorization enabled
  - Administrator authority granted to a user (native Db2 authorization)
  - RACF user access change is reflected in Db2



- Db2 receives ENF type 86 signal from z/OSMF Compliance REST API
  - On receipt of ENF 86, Db2 collects and writes compliance data to SMF 1154