Crunchy MLS PostgreSQL

Stephen Frost

November __, 2015

Crunchy MLS PostgreSQL

- Developed by Crunchy Data, provider of enterprise PostgreSQL technology, support and training, in support of MLS Ecosystem.
- Crunchy MLS PostgreSQL extends PostgreSQL through integration with the Red Hat® Enterprise Linux® 6.5+ SELinux functionality.
- Crunchy MLS PostgreSQL version 1.0 was released in July 2015
  - Built on PostgreSQL 9.4
  - Extended with Row Level Security
  - Extended with SELinux integration
- Next major release to be based on PostgreSQL 9.5 released in October __, 2015

CRUNCHY
Enterprise PostgreSQL

Crunchy MLS PostgreSQL

- Red Hat® Enterprise Linux® 6.5+ SELinux Integration provides ability to manage data creation and manipulation permissions based on Red Hat® Enterprise Linux® 6.5+ SELinux Security Policies.

- Ability to control all data access based on Red Hat® Enterprise Linux® 6.5+ SELinux
  Security Policies, network connections and users.

- Result is that users with a higher security level (such as Top Secret) can now read lower-level security data seamlessly, and the system automatically re-labels the data security level if higher-level users make changes.

CRUNCHY
Enterprise PostgreSQL

Security Labeling

- All primary objects in PostgreSQL can be labeled and access to them enforced by a label provider.
- Policies check security Labels through a hierarchy
- Labeling in PostgreSQL can be done on:
  - Databases
  - Schemas
  - Tables
  - Columns
  - Rows (with RLS and using a column to hold the label)
- If action not permitted by Security Label, User will receive Security Error

Security Policies

- Any function can be used in creating Security Policies to dictate access based on Security Labels
- Crunchy MLS PostgreSQL leverages SELinux to provide policies

Row Level Labeling

- Row Level Labeling enabled by Row Level Security – a new core PostgreSQL function that enables Crunchy MLS PostgreSQL.
- Developed by Crunchy in collaboration with PostgreSQL Community.
- Row Level Security integrated into Crunchy MLS PostgreSQL will be released in core PostgreSQL 9.5 in October __, 2015.
- With the addition of Row Level Security, rows can also be labeled and access to those rows controlled via Row-Level Security.

Row Level Security

- When row security is enabled on a table, all normal access to the table (excluding the table owner) for selecting rows or adding rows must be through a security policy.
- Row security policies can be specific to commands, or to roles, or to both. The commands available are
  - ALL
  - SELECT
  - INSERT
  - UPDATE
  - DELETE
- Multiple roles can be assigned to a given policy and normal role membership and inheritance rules apply.

SELinux Integration

- From the perspective of SELinux, Crunchy MLS PostgreSQL functions as a user-space object manager.
- Each table or function access initiated by a DML query will be checked against the system security policy.
- This check is in addition to the usual SQL permissions checking performed by PostgreSQL.

SELinux Integration

- SELinux access control decisions are made using security labels, which are represented by strings such as

  system_u:object_r:sepgsql_table_t:s0.

- Each access control decision involves two labels:
  - the label of the subject attempting to perform the action, and
  - the label of the object on which the operation is to be performed.

- Since these labels can be applied to any sort of object, access control decisions for objects stored within Crunchy MLS PostgreSQL are subjected to the same general criteria used for objects of any other type, such as files.

Performance

Performance Data to Come

More Information

- Contact Me:

  Stephen Frost
  stephen@crunchydata.com

- Contract Crunchy:

  info@crunchydata.com
  www.crunchydata.com

CRUNCHY
Enterprise PostgreSQL