Securing Your Data Warehouse

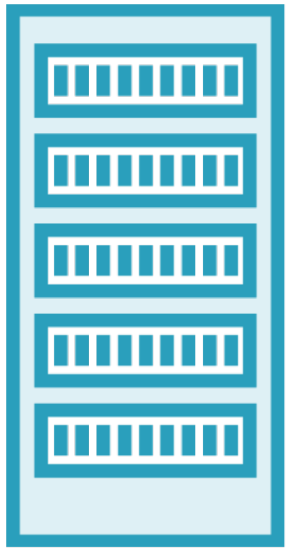
Russ Thomas
DATA ARCHITECT

@sqljudo www.sqljudo.com

Amazon Redshift Security

Users, groups, tables, schema

A Pseudo-OSI Approach To Our Topic



Physical layer

Data layer

Network layer

"Data in transit"

Application layer

Amazon Redshift Security

Users, groups, tables, schema

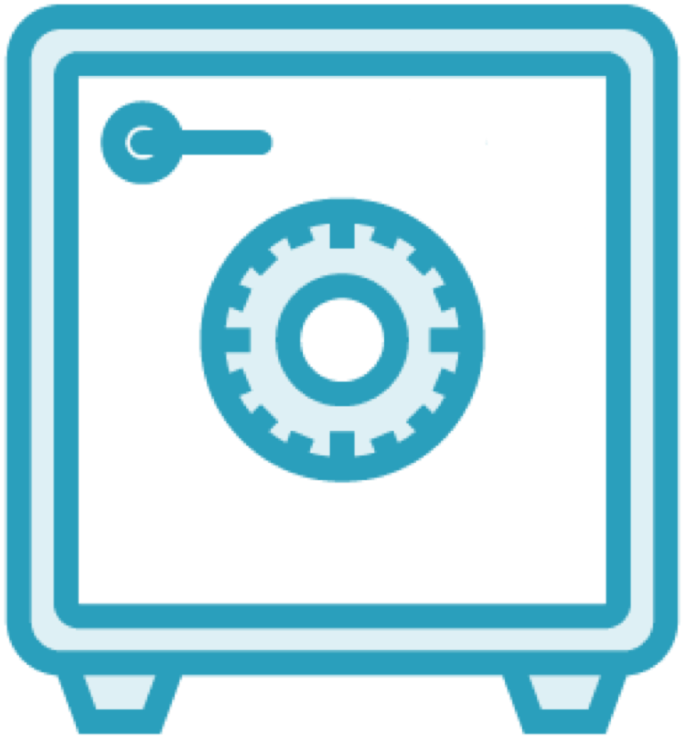
Amazon AWS Shared Responsibility

Responsibility of AWS	Responsibility of Client
Security of host operating system	Security of guest operating system
Physical security of data centers	Security of applications and platforms
Upkeep of infrastructure	Security of VPC (virtual private cloud)
Redundancies, SLAs, patching	Security of data

Securing The Virtual Private Cloud

- Virtual network similar to a companies physical network
- You are responsible for managing who can gain entrance into your VPC
- Get training or hire a professional
- An open rule allowing VPC access is an invitation to the world

Root Account Policy



- Locked away physically and forgotten

- Used once to establish security accounts and delegated areas of control

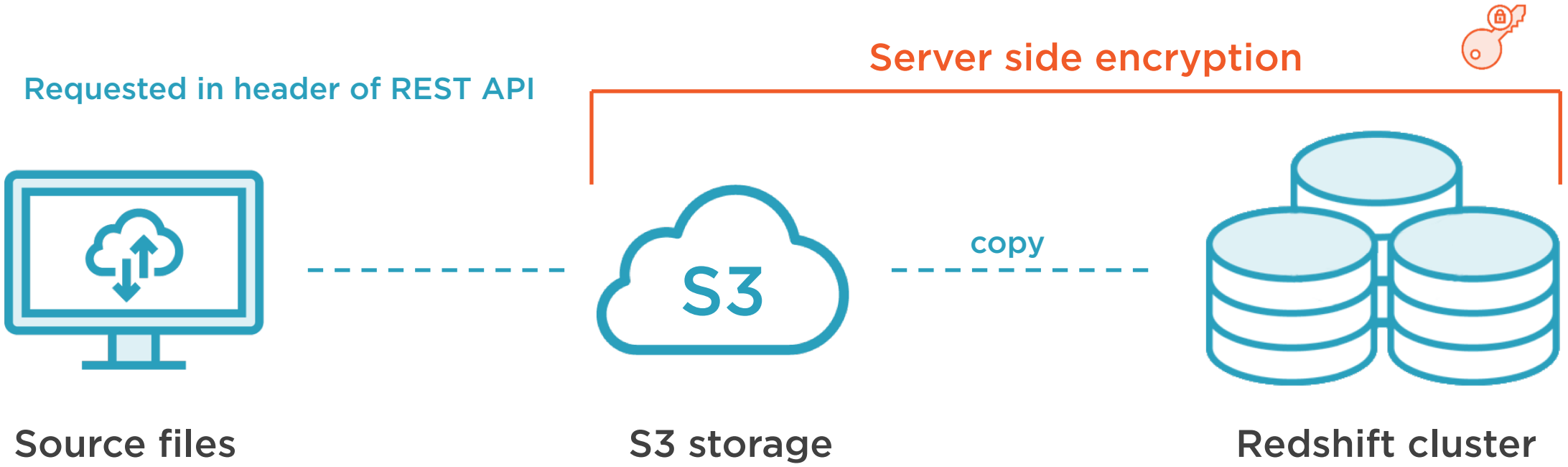
The root user and password underlying your AWS account should be one of the organizations most closely guarded assets.

Redshift Data Lifecycle

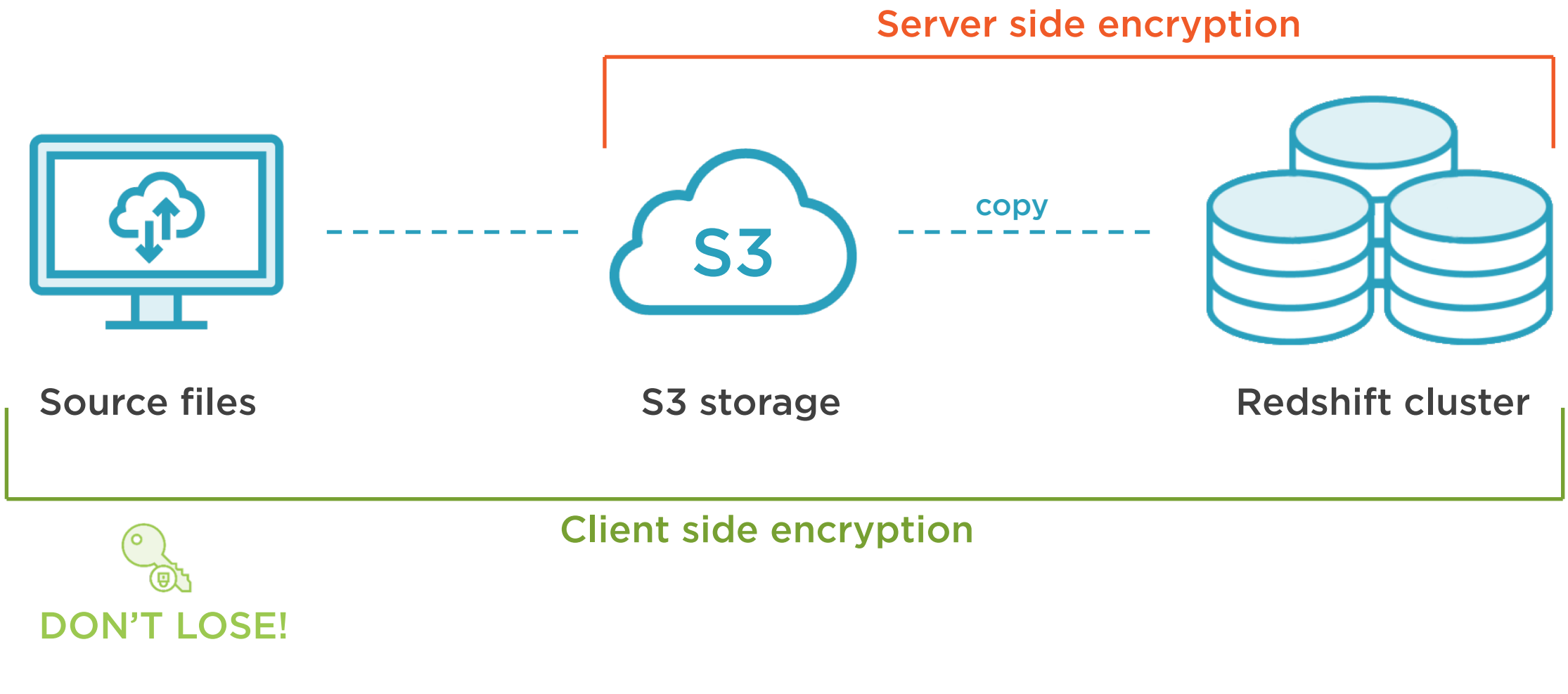
Redshift cluster

Redshift Data Loading Lifecycle

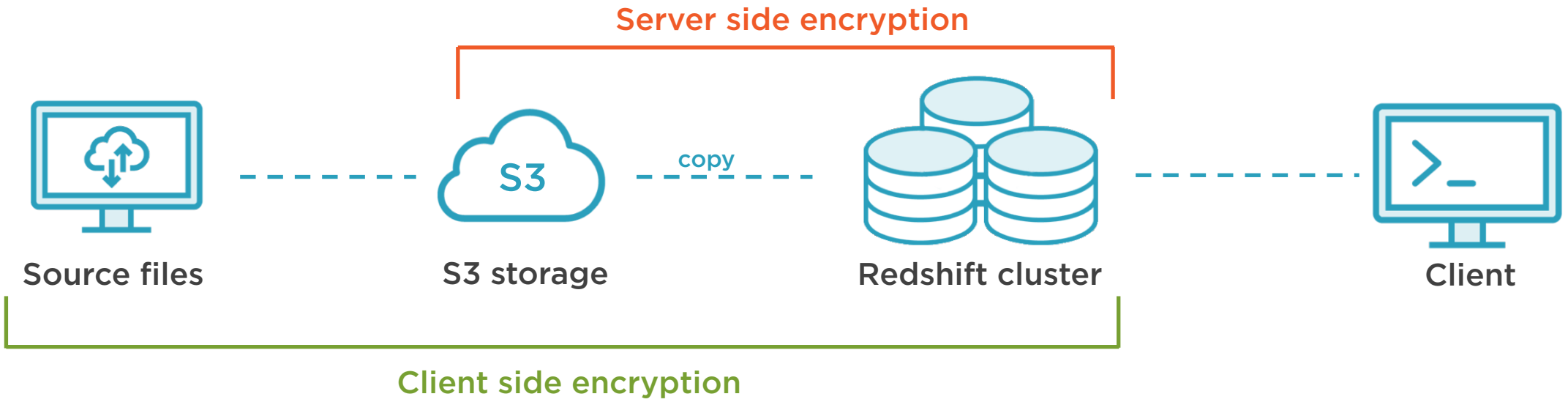
Redshift Data Loading Lifecycle



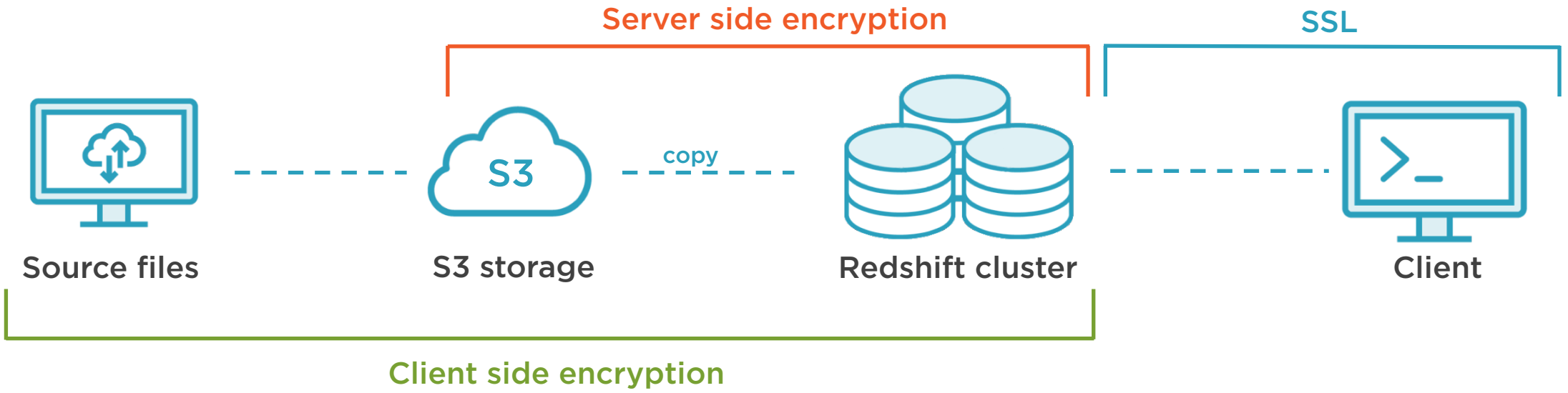
Redshift Data Loading Lifecycle



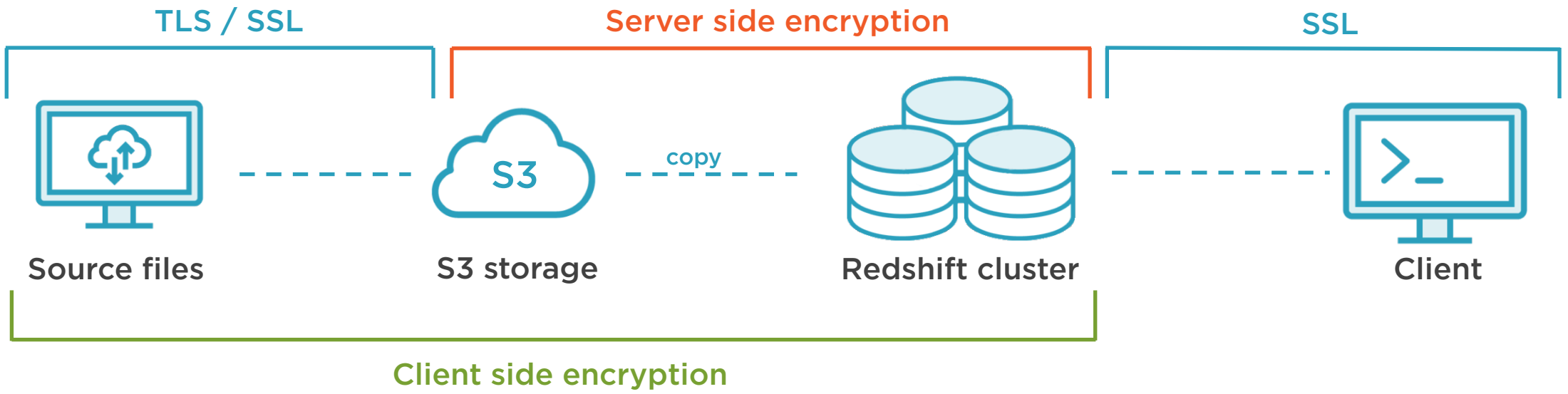
Redshift Data Lifecycle



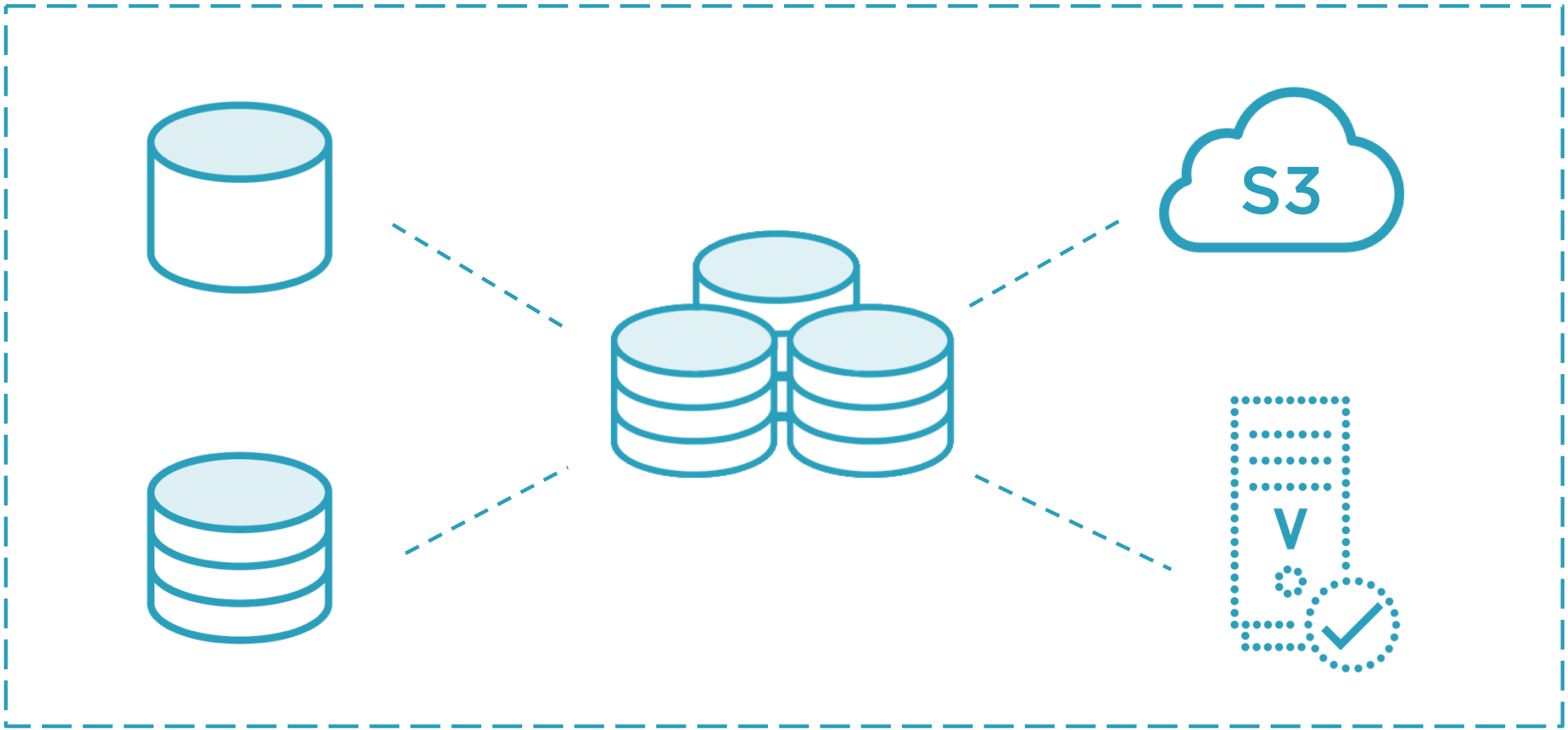
Redshift Data Lifecycle



Redshift Data Lifecycle



AWS Hardware Accelerated SSL



Amazon Redshift Security

Users, groups, tables, schema

Redshift User Security

- Similar to other RDBMS engines

- Management of GRANT and REVOKE

- USERS are grouped into GROUPS

- OBJECTS are grouped into SCHEMA

```
GRANT
[ SELECT |
  INSERT |
  UPDATE |
  DELETE | . . . ]
ON <object>
TO
[ USER | GROUP ]
```

- GRANT gives rights to perform a function on an object to a user or to a group

- Managing rights at the group level makes security management much easier to do well

Redshift Security

USERS receive no rights by default

SUPERUSER has all rights

The number of SUPERUSERs should be as limited as possible

Abacos Widgets DW User Groups

Finance

Sales

Data Warehouse Developers

REVOKE

REVOKE [GRANT OPTION FOR] { { SELECT | INSERT | UPDATE | DELETE | REFERENCES } [,...] | ALL [PRIVILEGES] } ON { [TABLE] *table_name* [, ...] | ALL TABLES IN SCHEMA *schema_name* [, ...] } FROM { *username* | GROUP *group_name* | PUBLIC } [, ...] [CASCADE | RESTRICT]

REVOKE [GRANT OPTION FOR] { { CREATE | TEMPORARY | TEMP } [,...] | ALL [PRIVILEGES] } ON DATABASE *db_name* [, ...] FROM { *username* | GROUP *group_name* | PUBLIC } [, ...] [CASCADE | RESTRICT]

REVOKE [GRANT OPTION FOR] { { CREATE | USAGE } [,...] | ALL [PRIVILEGES] } ON SCHEMA *schema_name* [, ...] FROM { *username* | GROUP *group_name* | PUBLIC } [, ...] [CASCADE | RESTRICT]

REVOKE [GRANT OPTION FOR] EXECUTE ON FUNCTION *function_name* ([[*argname*] *argtype* [, ...]]) [, ...] FROM { *username* | GROUP *group_name* | PUBLIC } [, ...] [CASCADE | RESTRICT]

REVOKE [GRANT OPTION FOR] USAGE ON LANGUAGE *language_name* [, ...] FROM { *username* | GROUP *group_name* | PUBLIC } [, ...] [CASCADE | RESTRICT]

GRANT

GRANT { { SELECT | INSERT | UPDATE | DELETE | REFERENCES } [,...] | ALL [PRIVILEGES] } ON { [TABLE] *table_name* [, ...] | ALL TABLES IN SCHEMA *schema_name* [, ...] } TO { *username* [WITH GRANT OPTION] | GROUP *group_name* | PUBLIC } [, ...]

GRANT { { CREATE | TEMPORARY | TEMP } [,...] | ALL [PRIVILEGES]] ON DATABASE *db_name* [, ...] TO { *username* [WITH GRANT OPTION] | GROUP *group_name* | PUBLIC } [, ...]

GRANT { { CREATE | USAGE } [,...] | ALL [PRIVILEGES] } ON SCHEMA *schema_name* [, ...] TO { *username* [WITH GRANT OPTION] | GROUP *group_name* | PUBLIC } [, ...]

GRANT EXECUTE ON { [FUNCTION] *function_name* ([[*argname*] *argtype* [, ...]]) [, ...] | ALL FUNCTIONS IN SCHEMA *schema_name* [, ...] } TO { *username* [WITH

GRANT OPTION] | GROUP *group_name* | PUBLIC } [, ...] GRANT USAGE ON LANGUAGE *language_name* [, ...] TO { *username* [WITH GRANT OPTION] | GROUP *group_name* | PUBLIC } [, ...]

Ownership

- Ability to CREATE can be GRANTED

- CREATE at schema level allows creation of any object

- CREATE at database level allows creation of SCHEMA

- When a user CREATES an object they OWN that object and inherently have all rights on that object

- Ownership can be transferred to another user

User Rights

- User rights should be well planned

- User rights should be well documented

- User rights should be regularly audited

Up Next

Administrative topics

System tables and views

Taking backups

Performing audits

Monitoring health and performance