Guardium Administration

What Are Those "?" in Guardium

Scope

- Here is an example of SQL statement you can see in Guardium :

Select * from CCN where CCID = “?” (Construct)

- Which is different from

Select * from CCN where CCID = *********** (Masked SQL Statement)

Select * from CCN where CCID = 12345678 (SQL Statement)

- **SQL Statement** : it’s what was executed
- **Masked SQL Statement** : what was executed BUT with masking of the values by the Collector (sniffer/parser)
- **Construct** : what was executed BUT re-written by the Collector AS IF the SQL statement used only **Bind Variables** for the values

What is a “Construct” in Guardium Parlance ?

Best is to know what a **Bind Variable** in SQL is. Here an example with Oracle

```
SQL> VARIABLE phone_no VARCHAR(20)

SQL> BEGIN

  2  :phone_no:=”18886663322”;

  3  END;

SQL> select * from CCN where phone = :phone_no
```

select * from CCN where phone = “?”

is called a “Construct” in Guardium

What the Parser does : re-write the SQL statement with bind variables only

Traffic

```
Select * from CCN where CCID=”12”

Select * from CCN where CCID=”99”

Select * from CCN where CCID=”18”

Select * from CCN where CCID=”22”

Select * from CCN where CCID=”44”

Select * from CCN where CCID=”55”

Select * from CCN where CCID=”67”
```

Parser (in Sniffer)

```
Select * from CCN where CCID=”?”

Select * from CCN where CCID=”?”

Select * from CCN where CCID=”?”

Select * from CCN where CCID=”?”

Select * from CCN where CCID=”?”

Select * from CCN where CCID=”?”

Select * from CCN where CCID=”?”
```

In MySQL (Instance)

```
Statement                              Counter

Select * from CCN where CCID=”?” , 7
```

Now you know what those “?” are … ;-) - Counter is called Total Access in Guardium

How is it Stored in the Database ?

The Great Design of the Guardium Database

Prerequisites to Understanding the Great Design

DAM is to know :

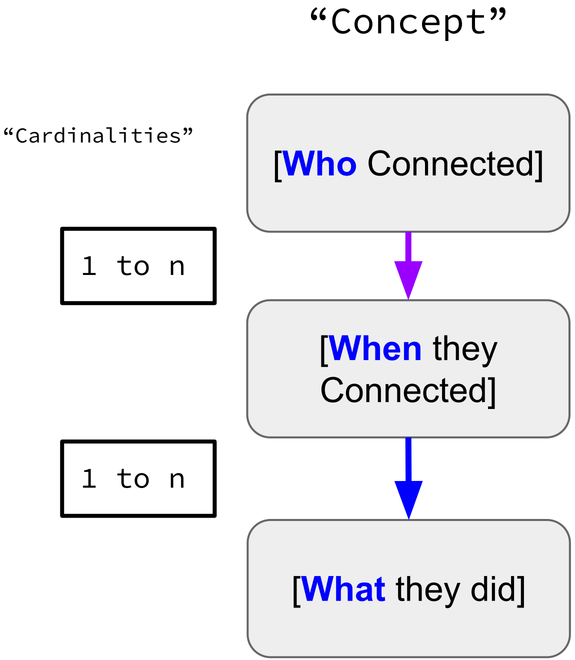
- Who connected (Database login strings)
- When they connected (Database Sessions)
- What they did while connected (SQLs)

(Who, When, What)

MySQL Database is made of **Tables with Built-in Joins**, hidden to the Users and following an **Entity-Relationship Diagram (ERD)**

Domains and Entities are Database views built with built-in managed Joins, meaning the users do NOT have to worry about those and do not have to manage them. Guardium does that for you.

Who, When, What ……Conceptually



“Concept”

“Cardinalities”

[Who Connected]

1 to n

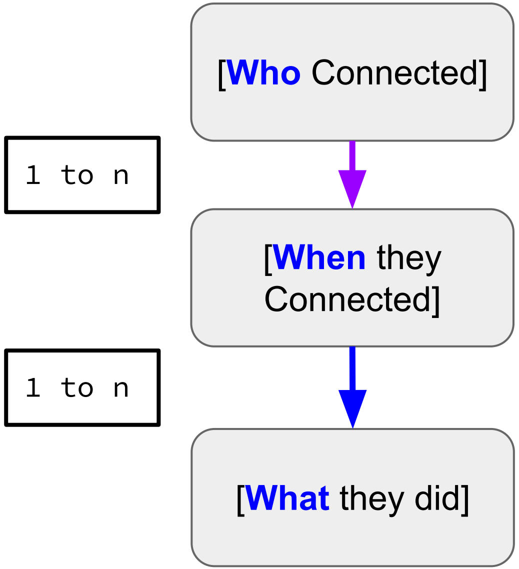
[When they Connected]

1 to n

[What they did]

Who, When, What ……Conceptually

“Concept”



[Who Connected]

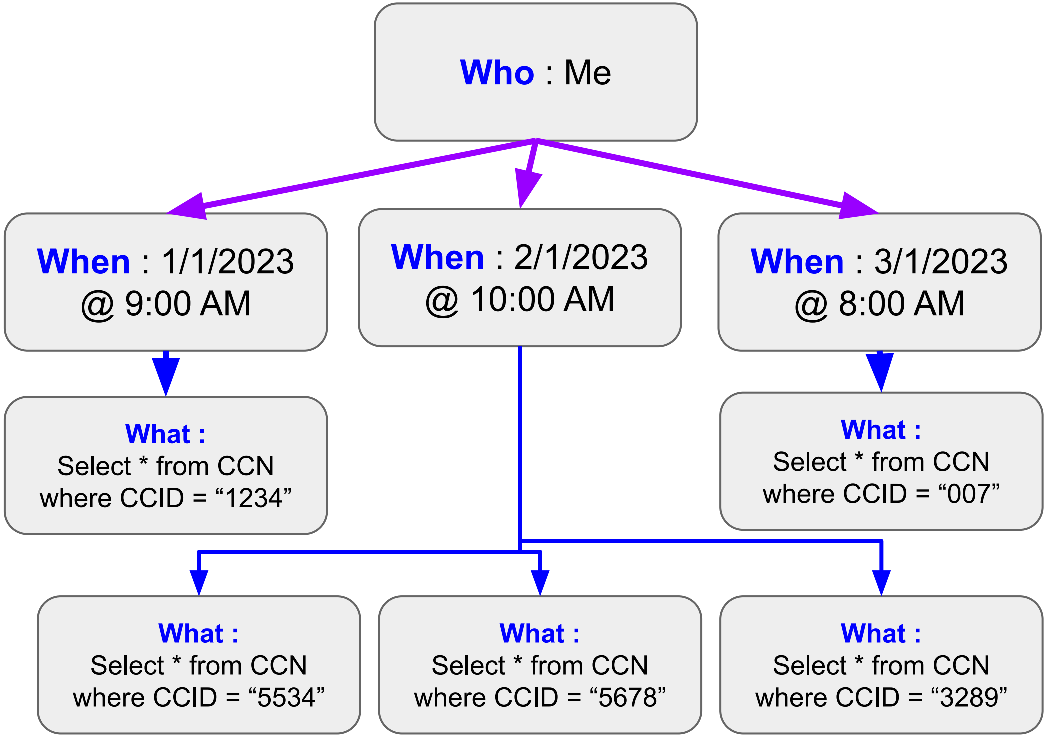
1 to n

[When they Connected]

1 to n

[What they did]

Example



Who : Me

When : 1/1/2023 @ 9:00 AM

When : 2/1/2023 @ 10:00 AM

When : 3/1/2023 @ 8:00 AM

What : Select * from CCN where CCID = “1234”

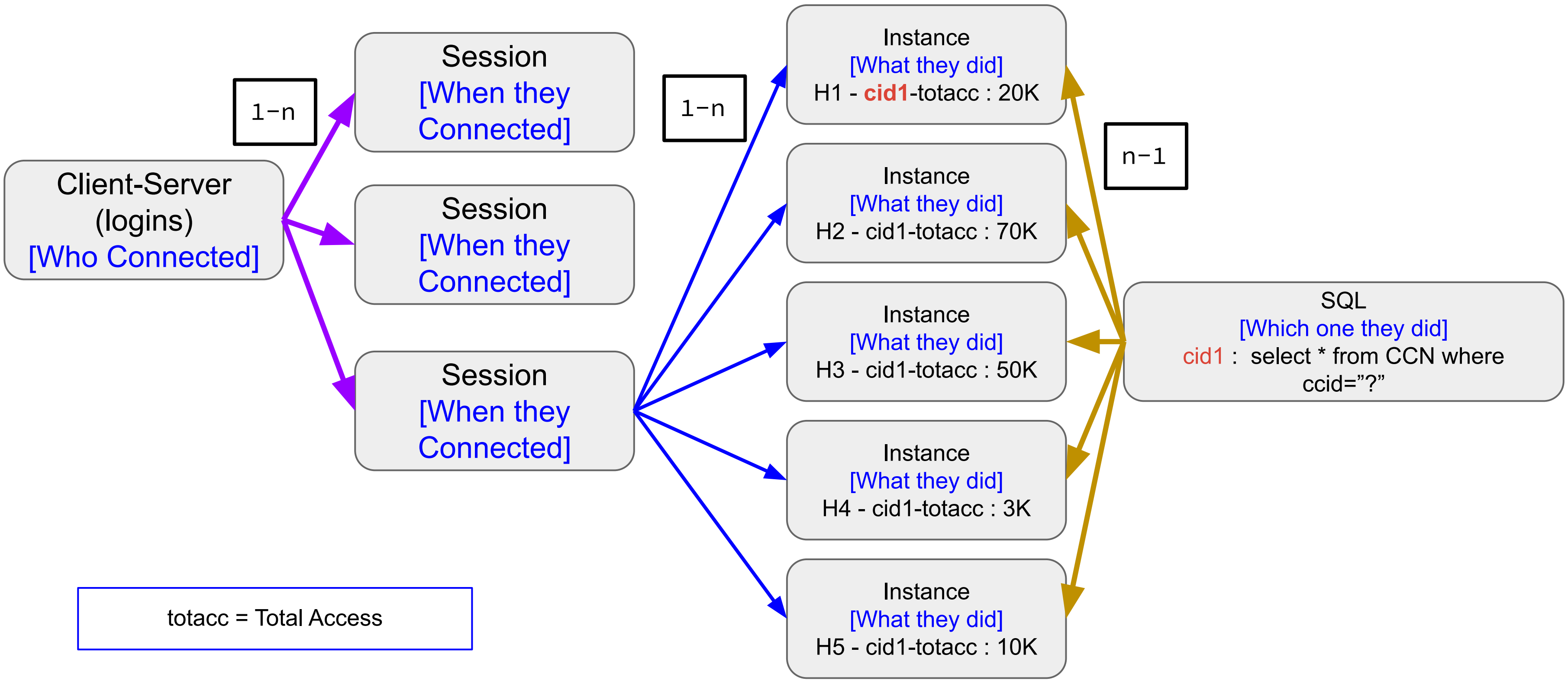
What : Select * from CCN where CCID = “007”

What : Select * from CCN where CCID = “5534”

What : Select * from CCN where CCID = “5678”

What : Select * from CCN where CCID = “3289”

Entity-Relationship Design and Diagram (1)



Client-Server (logins) [Who Connected]

1-n

Session [When they Connected]

Session [When they Connected]

Session [When they Connected]

1-n

Instance [What they did] H1 - cid1-totacc : 20K

Instance [What they did] H2 - cid1-totacc : 70K

Instance [What they did] H3 - cid1-totacc : 50K

Instance [What they did] H4 - cid1-totacc : 3K

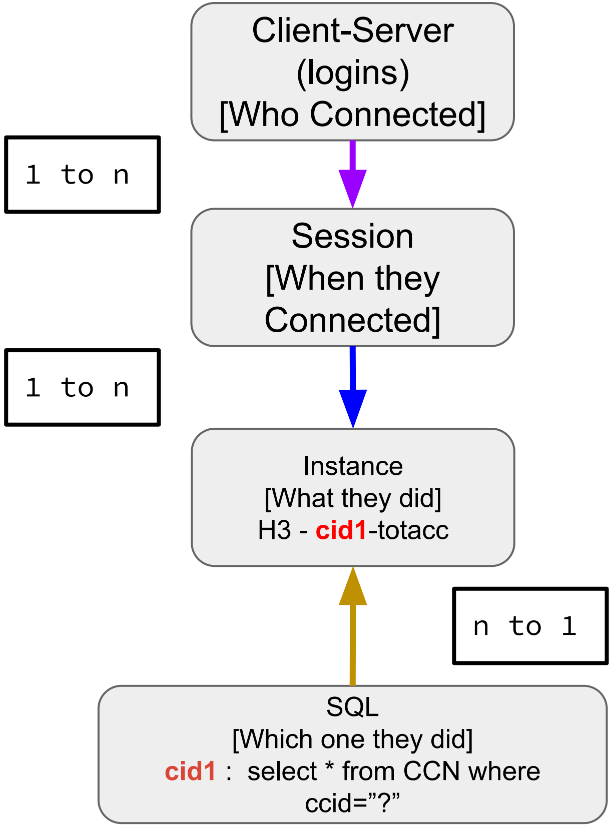
Instance [What they did] H5 - cid1-totacc : 10K

n-1

SQL [Which one they did] cid1 : select * from CCN where ccid="?"

totacc = Total Access

Entity-Relationship Design and Diagram (2)



Client-Server (logins) [Who Connected]

1 to n

Session [When they Connected]

1 to n

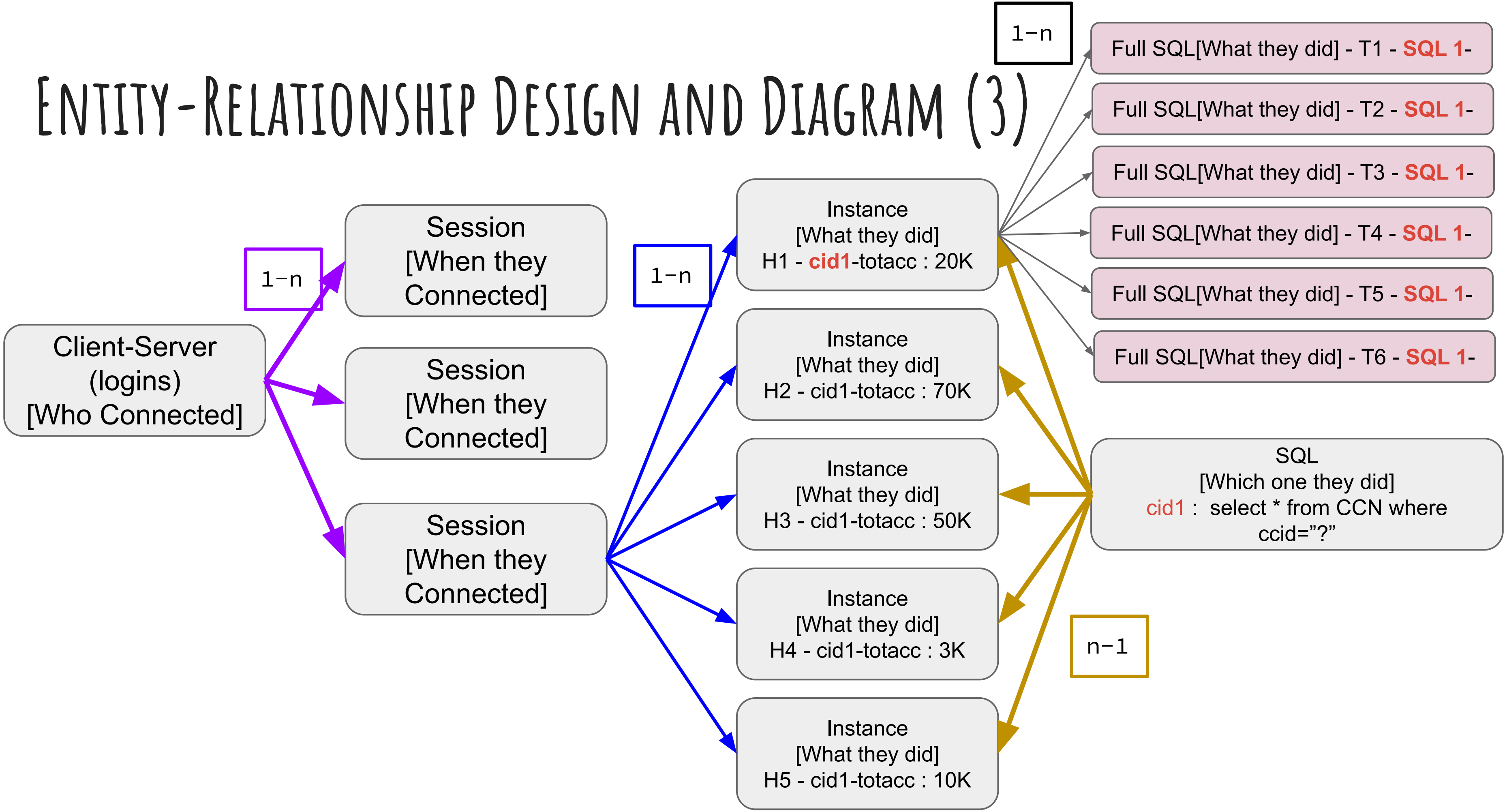
Instance [What they did] H3 - cid1-totacc

n to 1

SQL [Which one they did] cid1 : select * from CCN where ccid="?"

totacc = Total Access

Entity-Relationship Design and Diagram (3)



Client-Server (logins) [Who Connected]

1-n

Session [When they Connected]

Session [When they Connected]

Session [When they Connected]

1-n

Instance [What they did] H1 - **cid1**-totacc : 20K

Instance [What they did] H2 - cid1-totacc : 70K

Instance [What they did] H3 - cid1-totacc : 50K

Instance [What they did] H4 - cid1-totacc : 3K

Instance [What they did] H5 - cid1-totacc : 10K

1-n

Full SQL[What they did] - T1 - **SQL 1**-

Full SQL[What they did] - T2 - **SQL 1**-

Full SQL[What they did] - T3 - **SQL 1**-

Full SQL[What they did] - T4 - **SQL 1**-

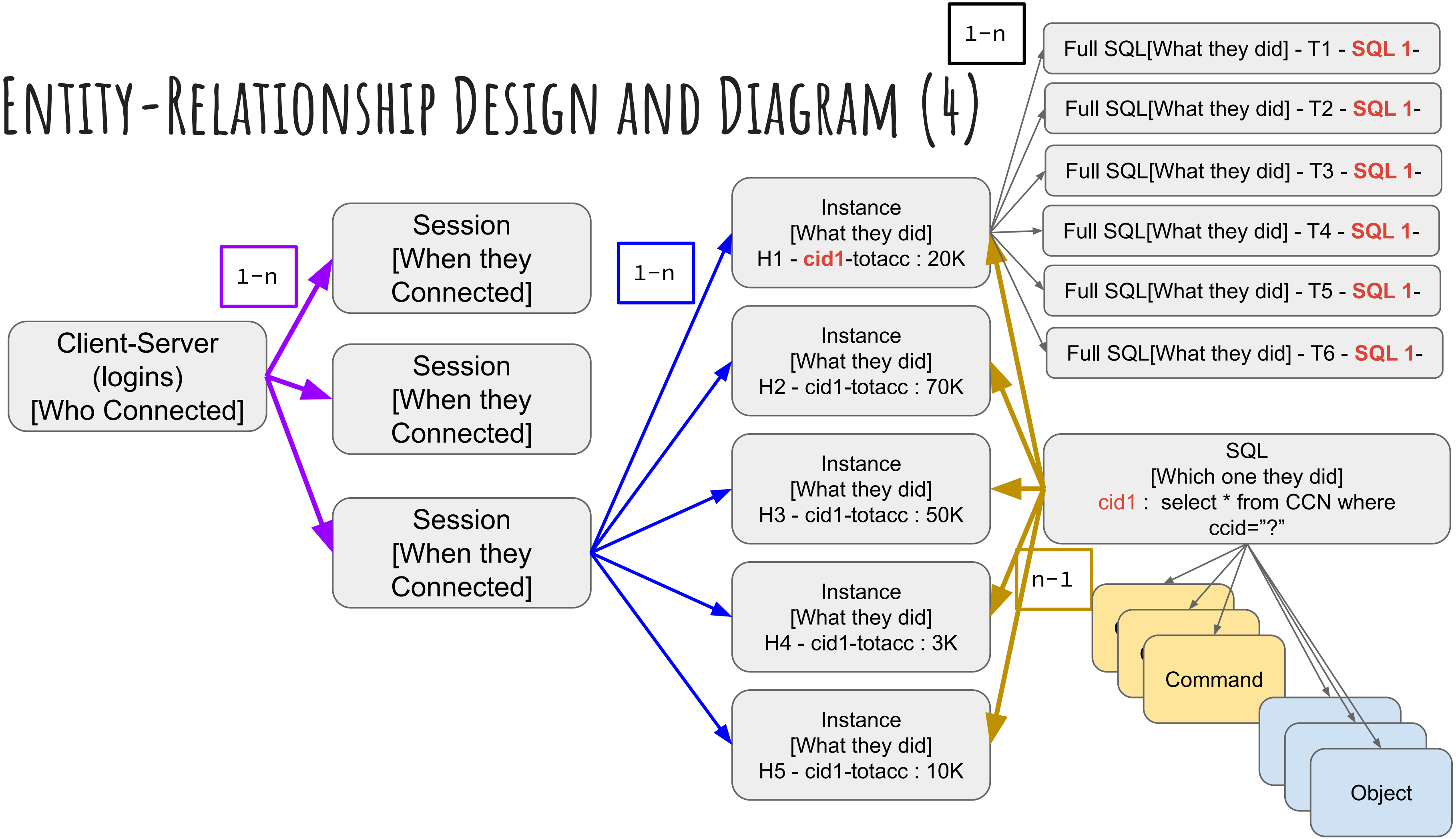
Full SQL[What they did] - T5 - **SQL 1**-

Full SQL[What they did] - T6 - **SQL 1**-

SQL [Which one they did] cid1 : select * from CCN where ccid=”?”

n-1

Entity-Relationship Design and Diagram (4)



Client-Server (logins) [Who Connected]

1-n

Session [When they Connected]

Session [When they Connected]

Session [When they Connected]

1-n

Instance [What they did] H1 - **cid1**-totacc : 20K

Instance [What they did] H2 - cid1-totacc : 70K

Instance [What they did] H3 - cid1-totacc : 50K

Instance [What they did] H4 - cid1-totacc : 3K

Instance [What they did] H5 - cid1-totacc : 10K

1-n

Full SQL[What they did] - T1 - **SQL 1**-

Full SQL[What they did] - T2 - **SQL 1**-

Full SQL[What they did] - T3 - **SQL 1**-

Full SQL[What they did] - T4 - **SQL 1**-

Full SQL[What they did] - T5 - **SQL 1**-

Full SQL[What they did] - T6 - **SQL 1**-

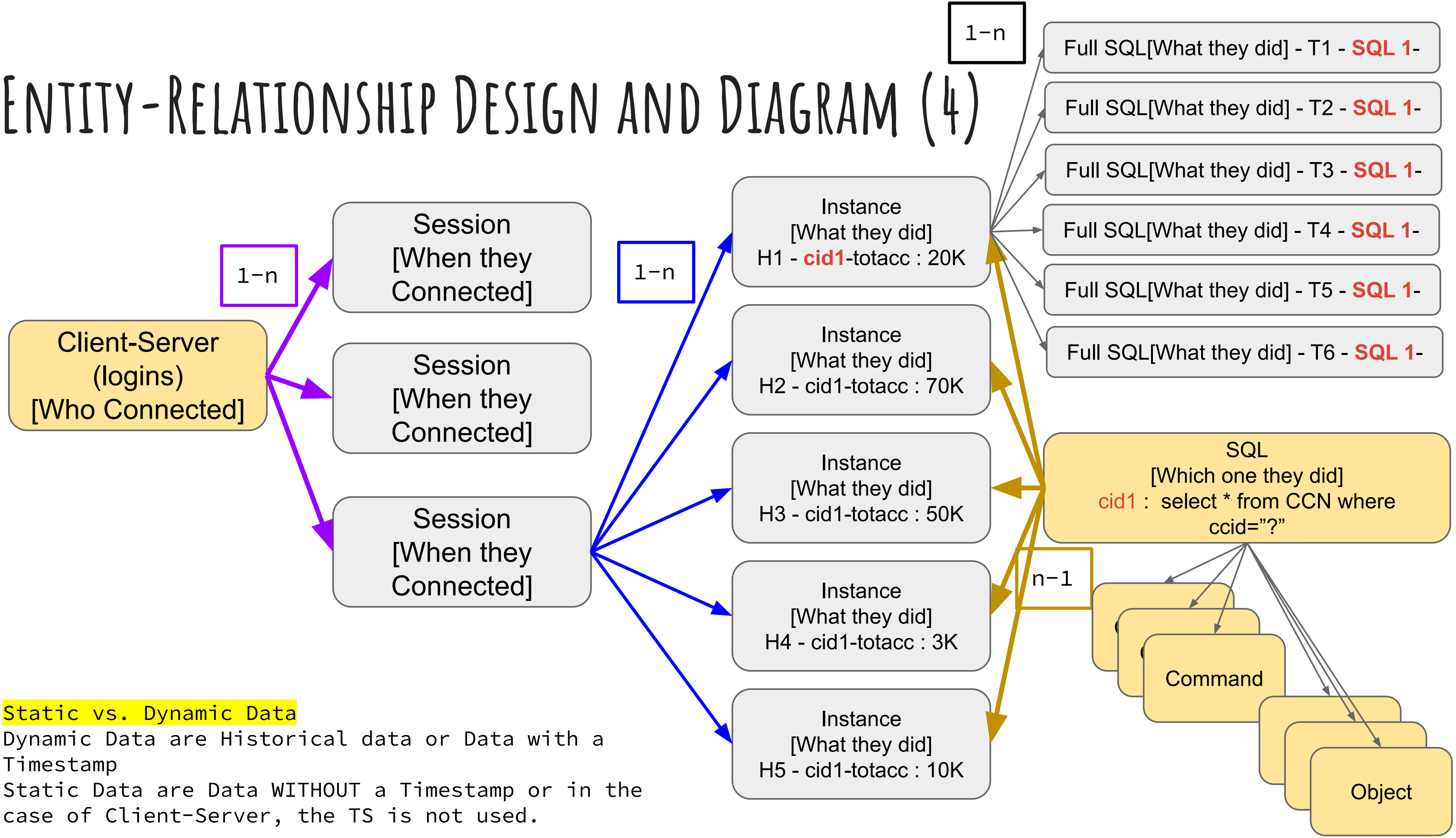
SQL [Which one they did] cid1 : select * from CCN where ccid="?"

n-1

Command

Object

Entity-Relationship Design and Diagram (4)



Client-Server (logins) [Who Connected]

1-n

Session [When they Connected]

Session [When they Connected]

Session [When they Connected]

1-n

Instance [What they did] H1 - **cid1**-totacc : 20K

Instance [What they did] H2 - cid1-totacc : 70K

Instance [What they did] H3 - cid1-totacc : 50K

Instance [What they did] H4 - cid1-totacc : 3K

Instance [What they did] H5 - cid1-totacc : 10K

1-n

Full SQL[What they did] - T1 - **SQL 1**-

Full SQL[What they did] - T2 - **SQL 1**-

Full SQL[What they did] - T3 - **SQL 1**-

Full SQL[What they did] - T4 - **SQL 1**-

Full SQL[What they did] - T5 - **SQL 1**-

Full SQL[What they did] - T6 - **SQL 1**-

SQL [Which one they did] cid1 : select * from CCN where ccid="?"

n-1

Command

Object

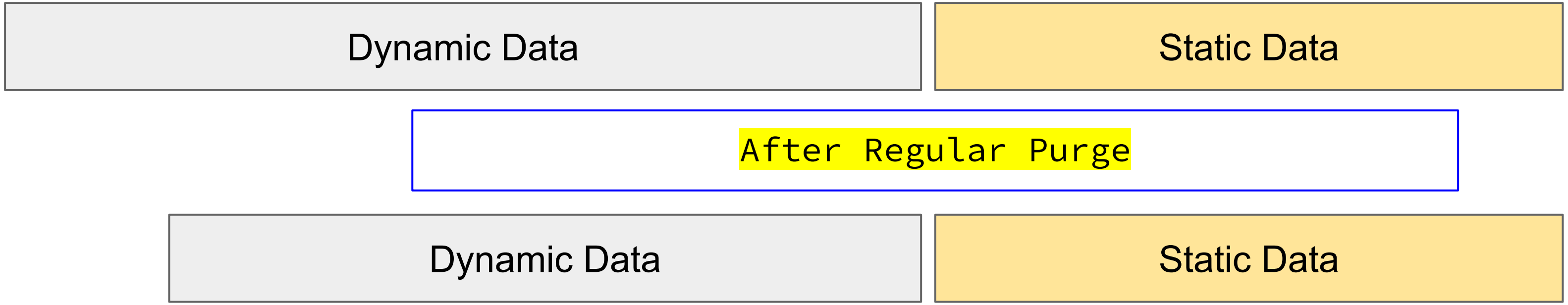
Static vs. Dynamic Data

Dynamic Data are Historical data or Data with a Timestamp

Static Data are Data WITHOUT a Timestamp or in the case of Client-Server, the TS is not used.

Impact on Purges

Static vs. Dynamic Data
Regular Purge is on Dynamic data ONLY
Purge of Static Data is a separate purge



Impact on Upgrades

Static vs. Dynamic Data
The larger the Data, the longer the upgrade

Dynamic Data

Static Data

It’s why Guardium asks for Purging basically as much as you can prior to the upgrade. But this reduces ONLY the Dynamic Data.For a long time, there was no purge of the static data, until Guardium implemented one, which relies on the “Last Used” field which gets populated if the feature is activated.

If you have SonarG or Guardium Insights or Context22 Add-on, you don’t need to upgrade a collector, especially if you have VM Collectors. You just rebuild one.

What are Domains and Entities ?

Entities : They are “DB Views”. Views are a STANDARD concept in Database. They are READ-ONLY access to tables that include the Joins. With Views, NO NEED to define or work out the Joins. Guardium takes FULL advantage of this. It’s why you can pick and choose fields in Report without having to declare the Joins

Domains :

- Domains are sub-parts of the Database as DB Views
- Entities are DB Views of Tables, WITH Joins (you don’t have to worry about DB Joins)

Main Guardium Domains

2 Types of Domains :

- DAM Data Domains
  - **Access** Domain - regular and successful traffic - (Who, When, What)
  - **Exceptions** Domain - unsuccessful traffic : failed logins, SQL errors
  - **Policy violations** Domain - successful and unsuccessful traffic flagged by your policy as violation
- Non DAM Data Domains
  - Performances
  - Configuration
  - Etc…
  - The list is LONG

How to contact us

info@context22.com
Support@context22.com
LinkedIn
www.context22.com
(under construction)

CONTEXT 22
TECHNOLOGIES