Provenance-based Access Control in Cloud IaaS

August 23, 2013
Dissertation Proposal

Dang Nguyen
Institute for Cyber Security
University of Texas at San Antonio

Data Provenance in Computer Systems

"In computer systems, activities are carried out by processes that take input data, input state, input configuration, and produce output data and output state. Such processes are compositional by nature and can be the result of sophisticated compositions (sequential, parallel, conditional, etc) of simpler processes." (Luc Moreau, "The Foundation for Provenance on the Web")

Characteristics of Provenance Data

- Information of operations/transactions performed against data objects and versions
  - Actions that were performed against data
  - Acting Users/Subjects who performed actions on data
  - Data Objects used for actions
  - Data Objects generated from actions
  - Additional Contextual Information of the above entities

- Directed Acyclic Graph (DAG)
- Causality dependencies between entities (acting users / subjects, action processes and data objects)
- Dependency graph can be traced/traversed for the discovery of Origin, usage, versioning info, etc.

Provenance and Access Control

- Compared to traditional access control, Provenance-based Access Control (**PBAC**) provides richer access control mechanisms.
  - For example: dynamic separation of duties issues.

- Provenance Data Model
- Base PBAC Model
- Contextual PBAC Model
- Provenance data sharing approaches

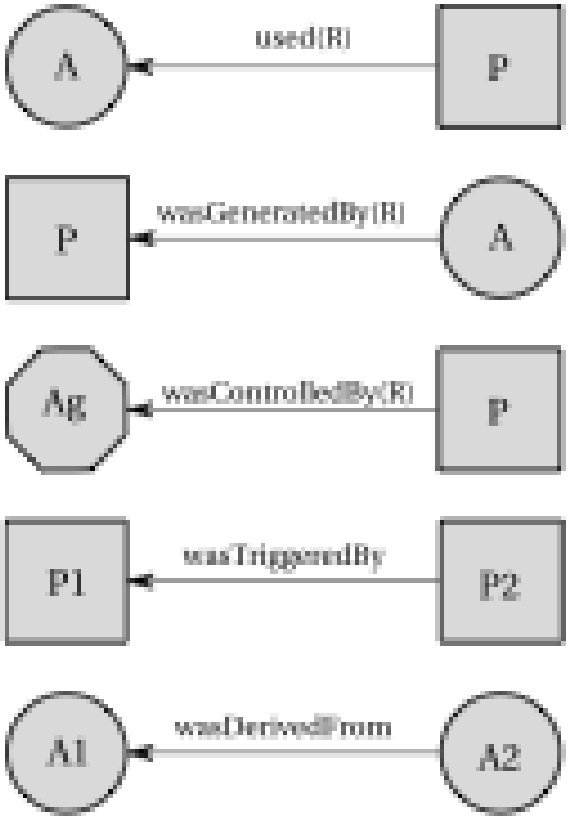
Provenance-aware Systems

- Capturing provenance data
- Storing provenance data
- Querying provenance data

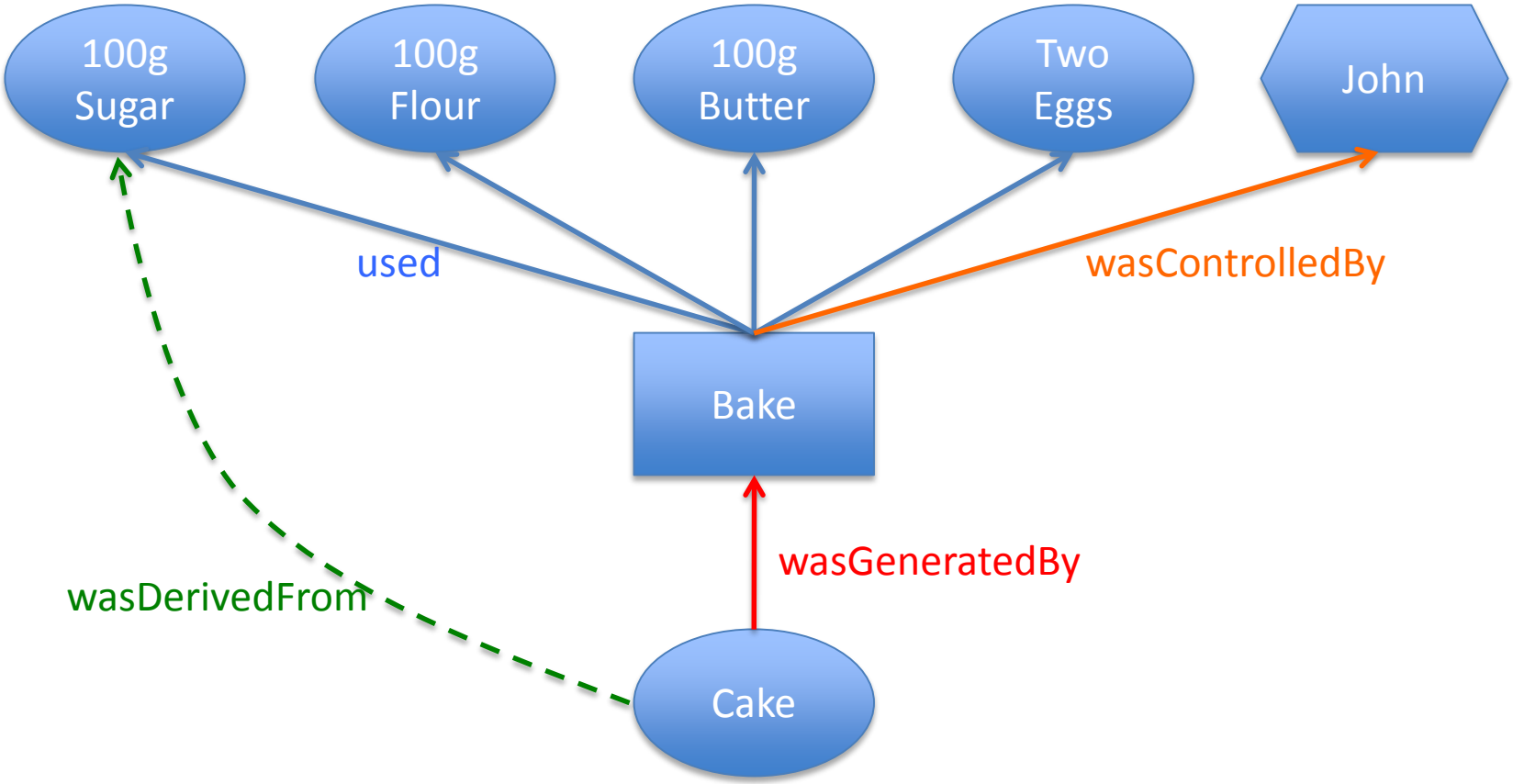
- Using provenance data
- Securing provenance data

Open Provenance Model (OPM)

- 3 Node Types
  - Artifact (ellipse): Object
  - Process (Rectangle): Action
  - Agent (Octagon/Hexagon): User/Subject
- 5 Causality dependency edge Types (not a dataflow)
  - U: Used(Role)
  - G: wasGeneratedBy(Role)
  - C: wasControlledBy(Role)
  - wasDerivedFrom
  - wasTriggeredBy

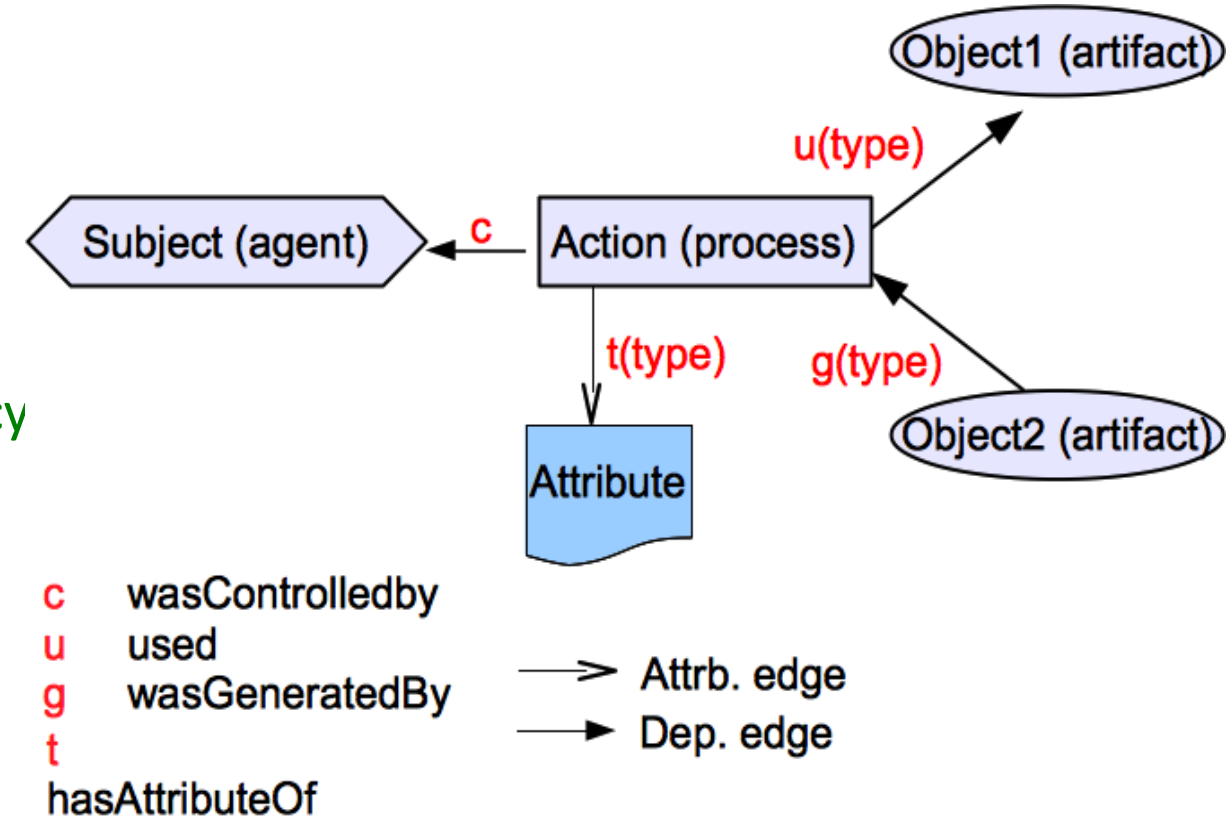


OPM Example


100g Sugar
100g Flour
100g Butter
Two Eggs
John
used
wasControlledBy
Bake
wasGeneratedBy
wasDerivedFrom
Cake

Provenance Data Model

- 4 Node Types
  - Object (Artifact)
  - Action (Process)
  - Subject (Agent)
  - Attribute
- 5 Causality dependency edge Types
  (not a dataflow) and
  Attribute Edge



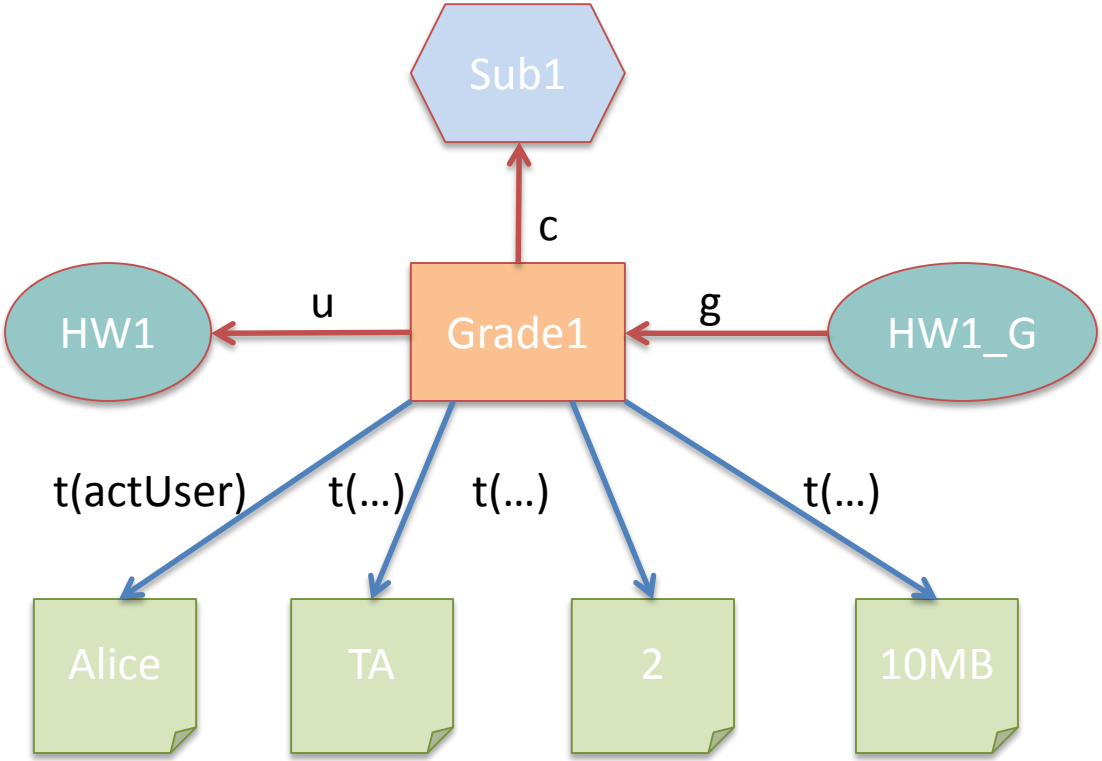
Capturing Provenance Data

(Subject1, Grade1, HW1, GradedHW1, ContextualInfoSet-Grade1)

(Grade1, u, HW1)
(Grade1, c, Subject1)
(GradedHW1, g, Grade1)

(Grade1, t[actingUser], Alice)
(Grade1, t[activeRole], TA)
(Grade1, t[weight], 2)
(Grade1, t[object-size], 10MB)

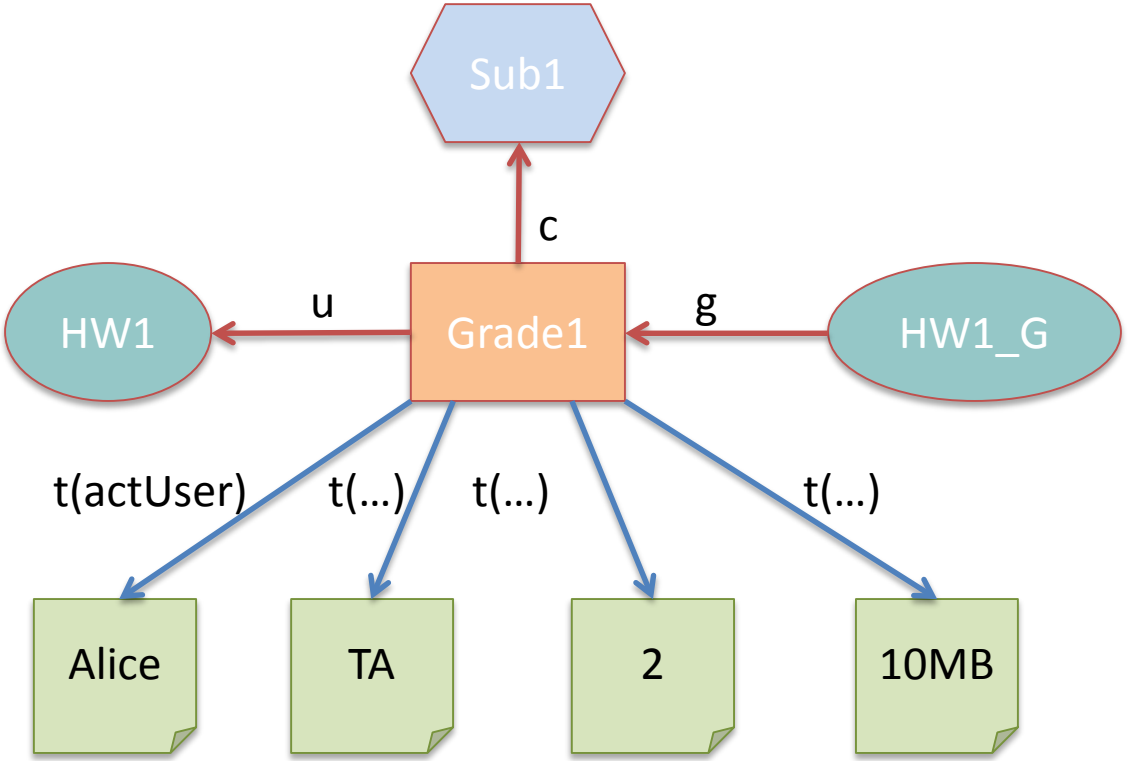
Provenance Graph



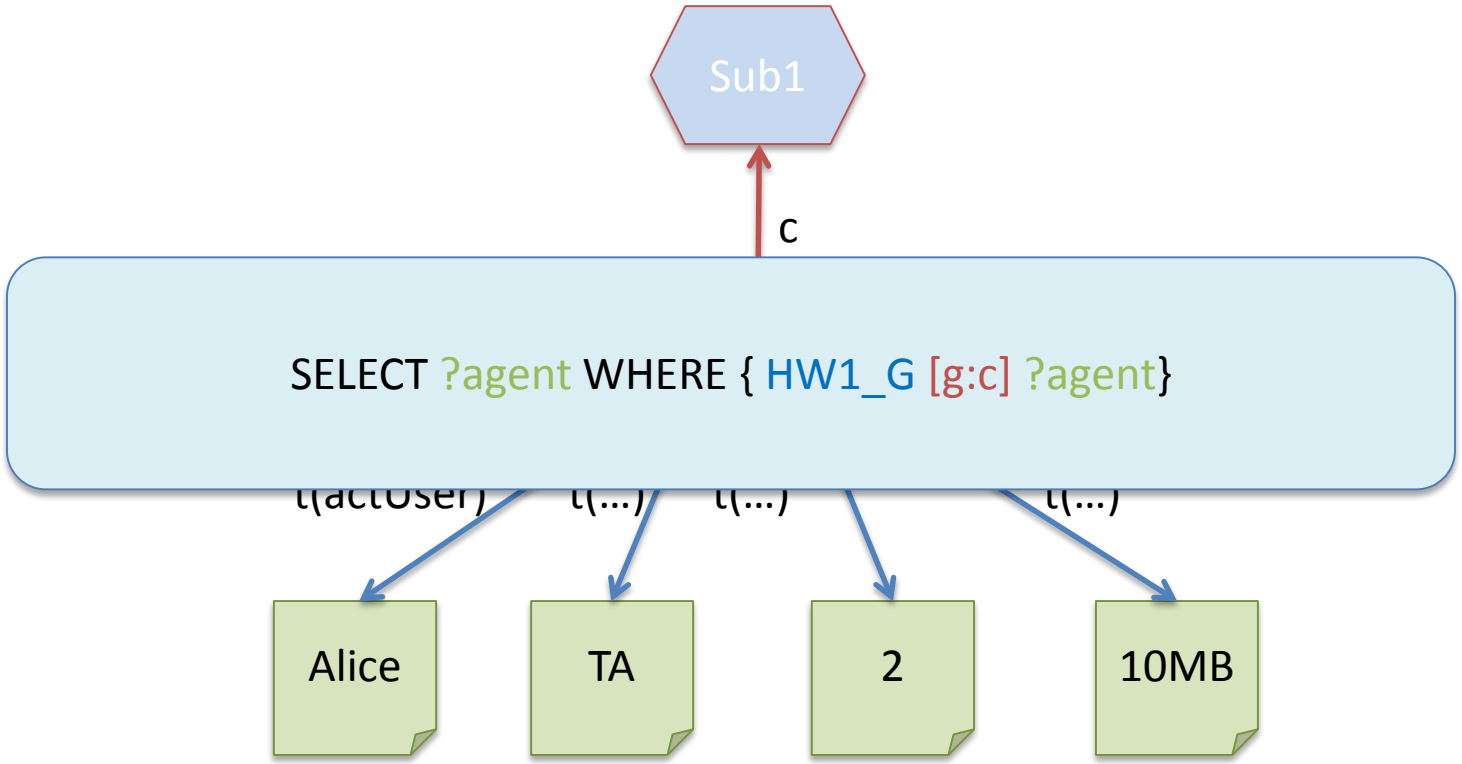
Storing and Querying Provenance Data

- Resource Description Framework (RDF) provides natural representation of triples.
- RDF-format triples can be stored in databases.
- Utilizes SPARQL Protocol and RDF Query Language for extracting useful provenance information.
  - Starting Node: any entities (not attribute nodes)
  - A matching path pattern: combination of dependency edges

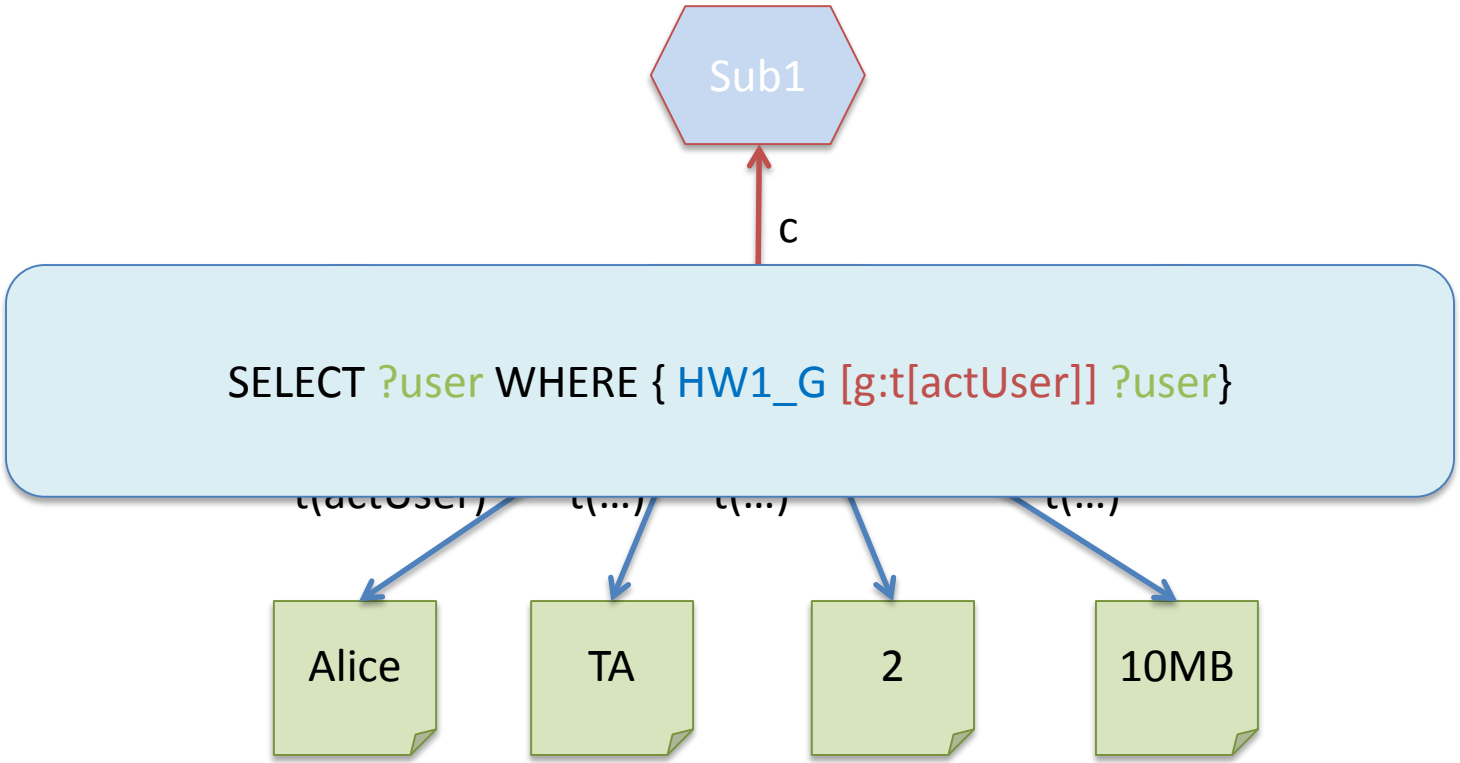
Provenance Graph



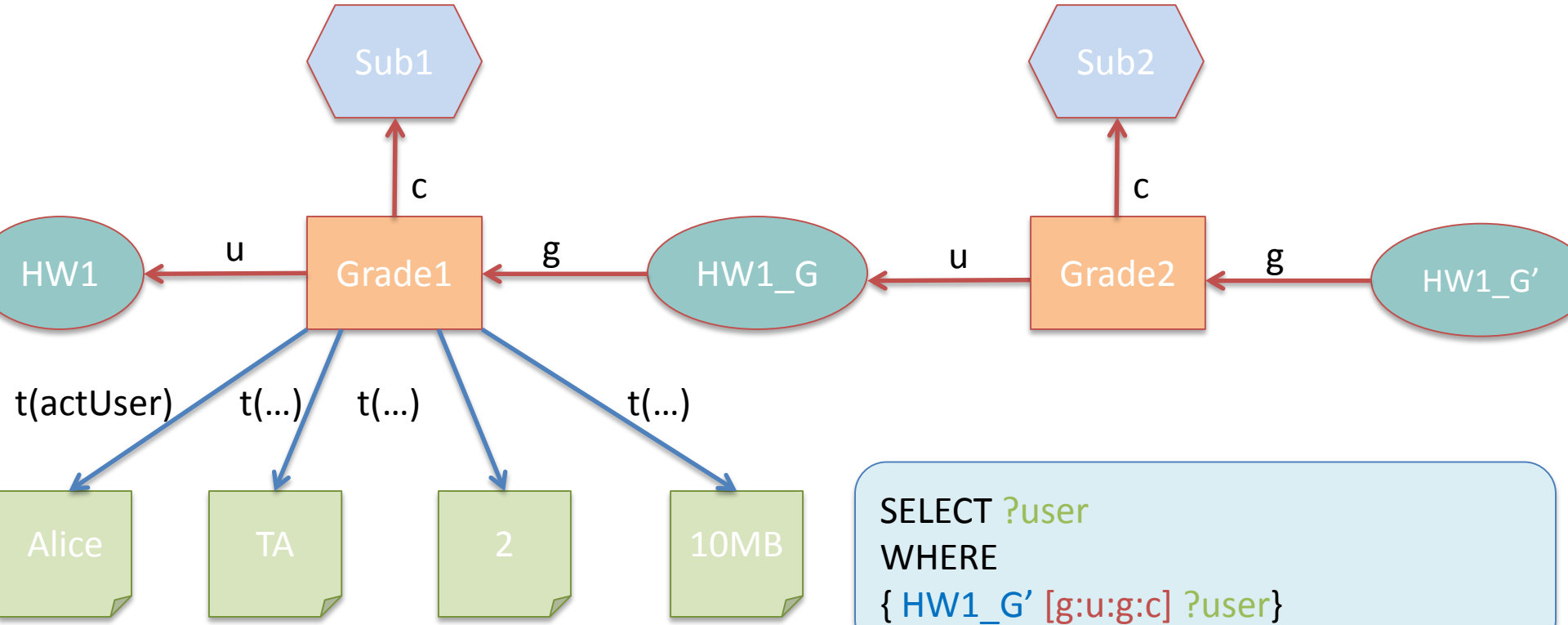
Provenance Graph



Provenance Graph



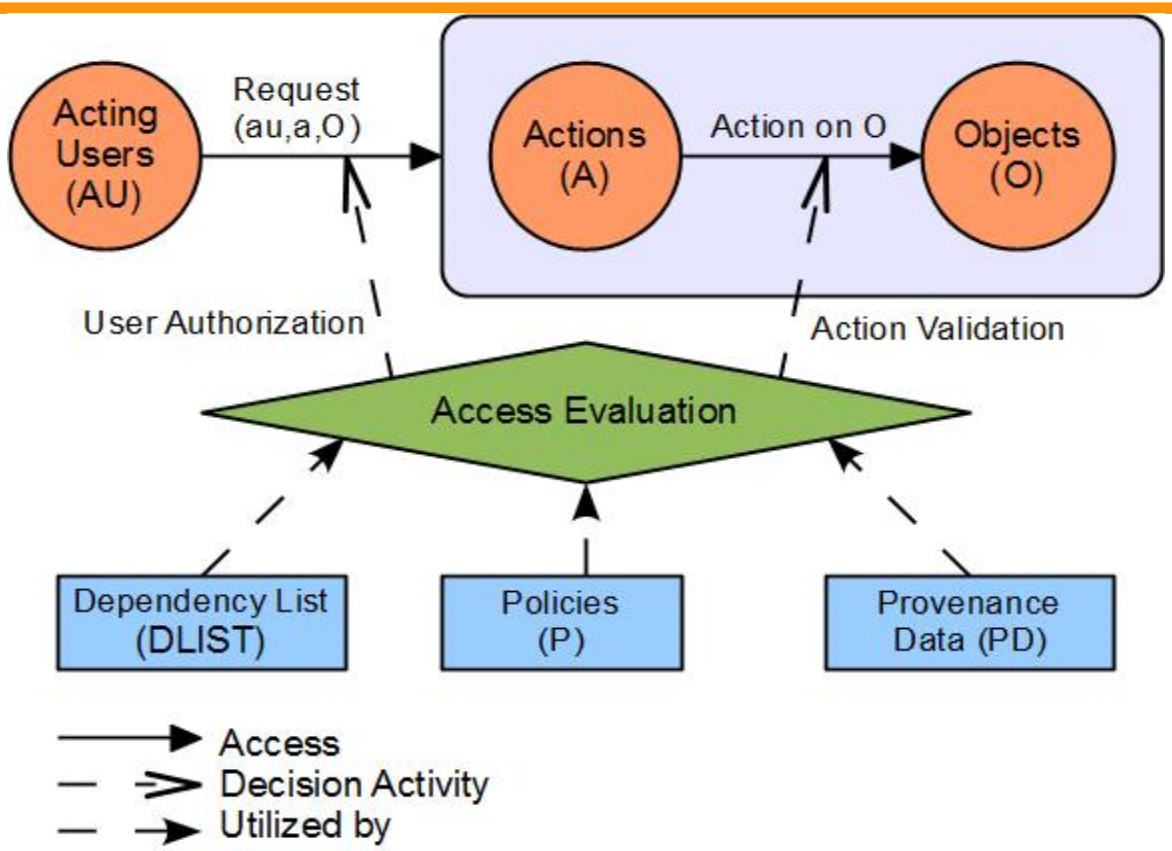
Provenance Graph



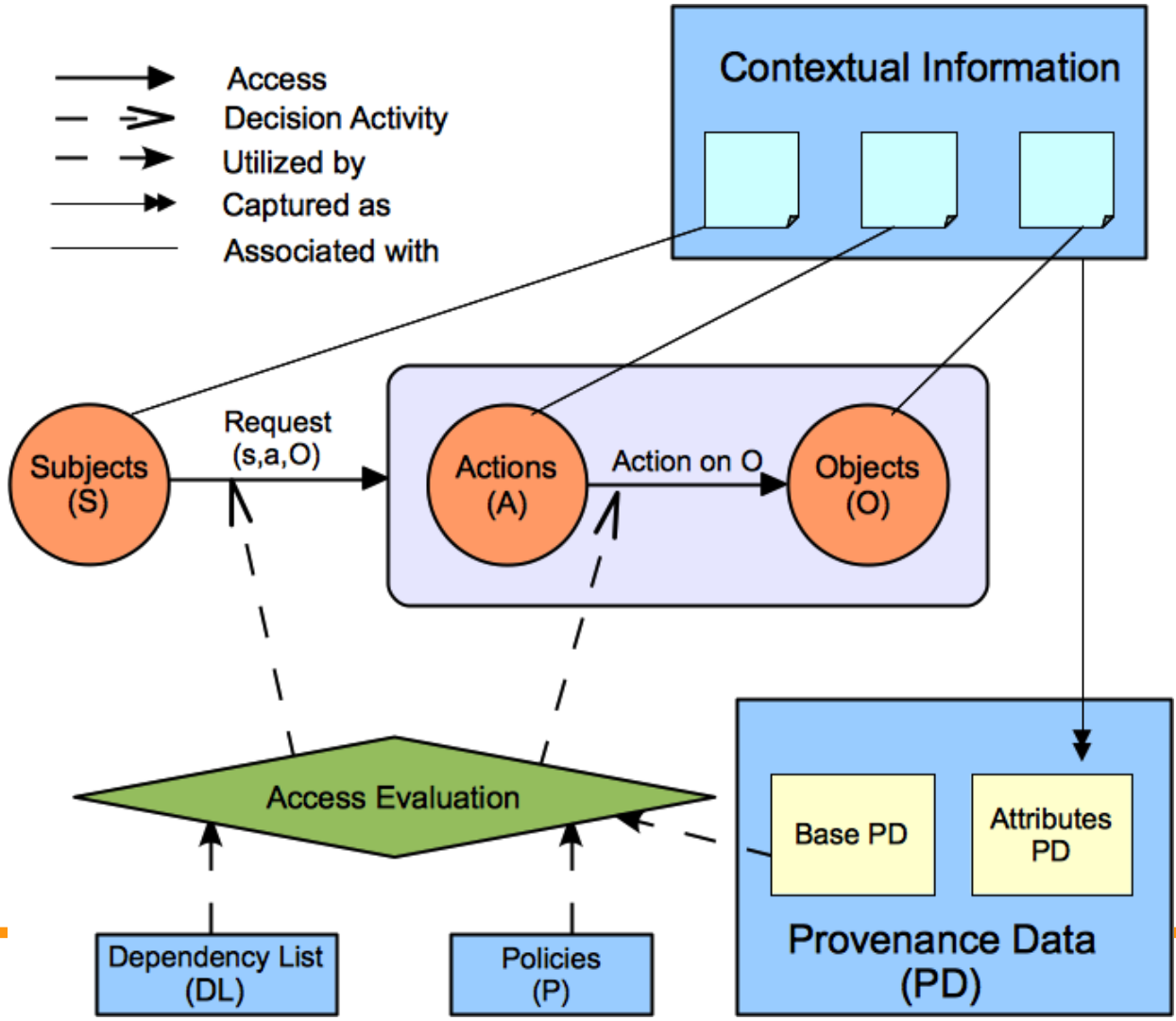

```
SELECT ?user
WHERE
{ HW1_G' [g:u:g:c] ?user}
```

```
{ HW1_G' [[g:u]*:g:c] ?user}
```

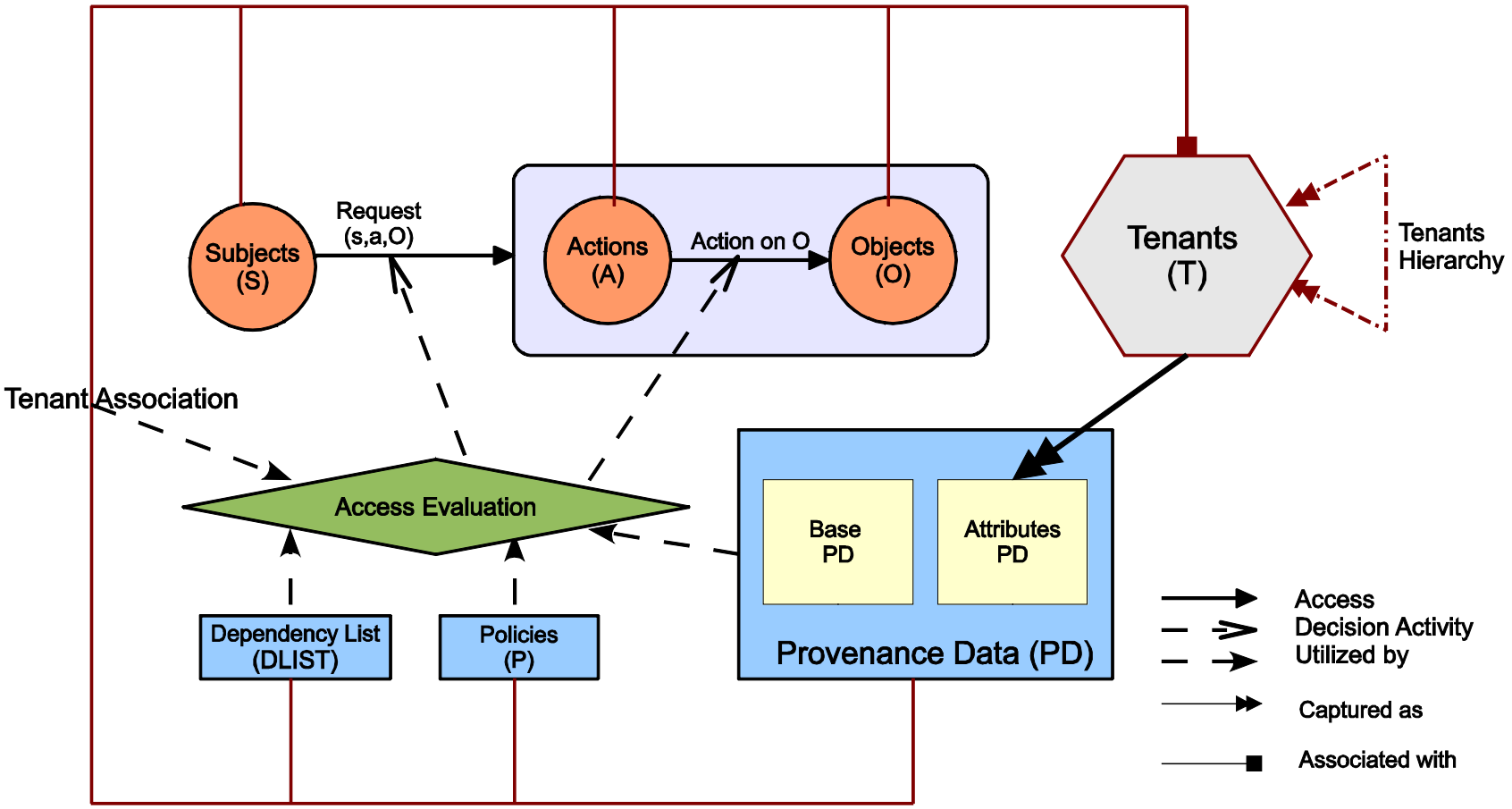
PBAC Model Components



$PBAC_C$: $PBAC_B$ + Contextual Info.



PBAC_C in Cloud IaaS



Capturing Provenance Data

(Subject1, Create1, VMI1, ContextualInfoSet-Create1)

Create1, c, Subject1)
(VMI1, g, Create1)

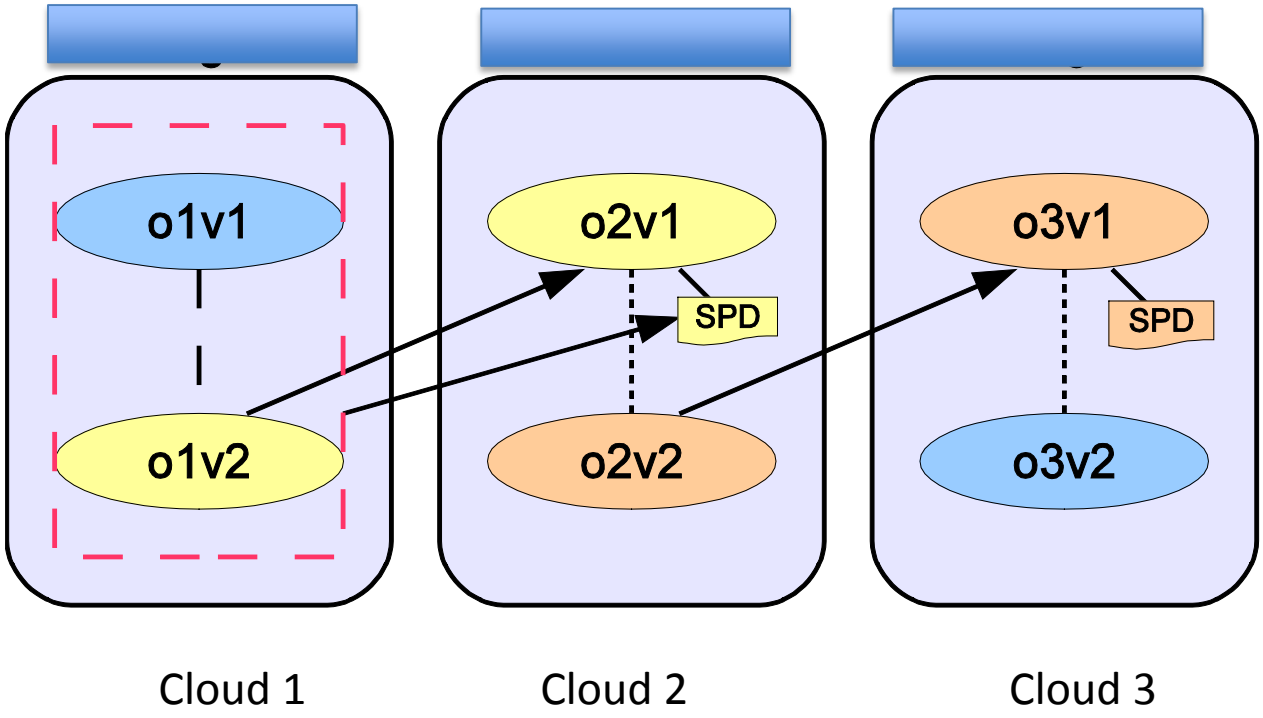
Create1, t[tenant], “Development”)

Single- vs Multi-Cloud (IaaS)

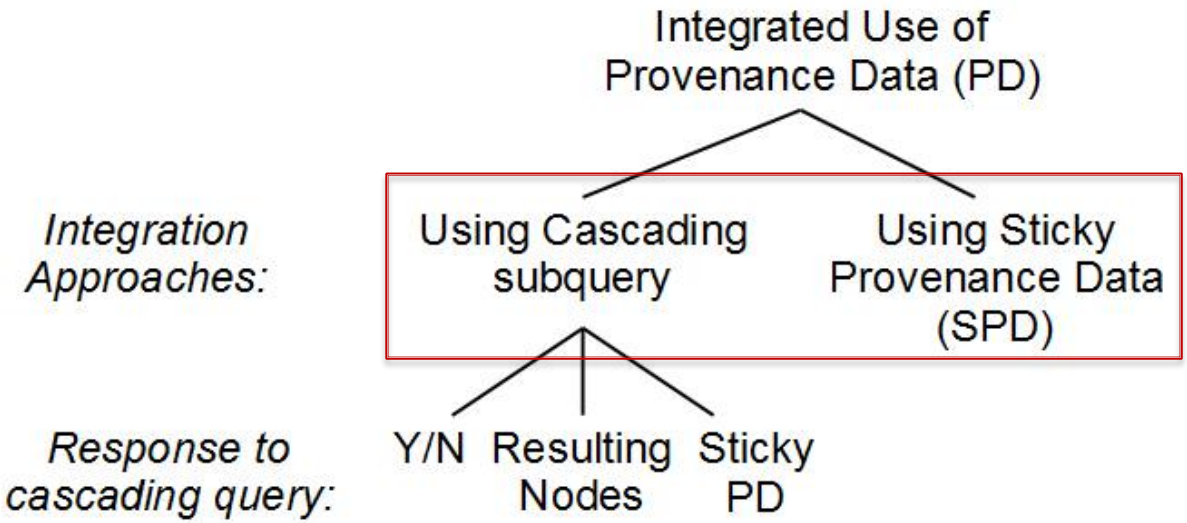
- Most single-cloud CSP provides centralized service.
  - Facilitates data sharing (provenance).

- Multi-cloud CSPs require collaboration for sharing data.

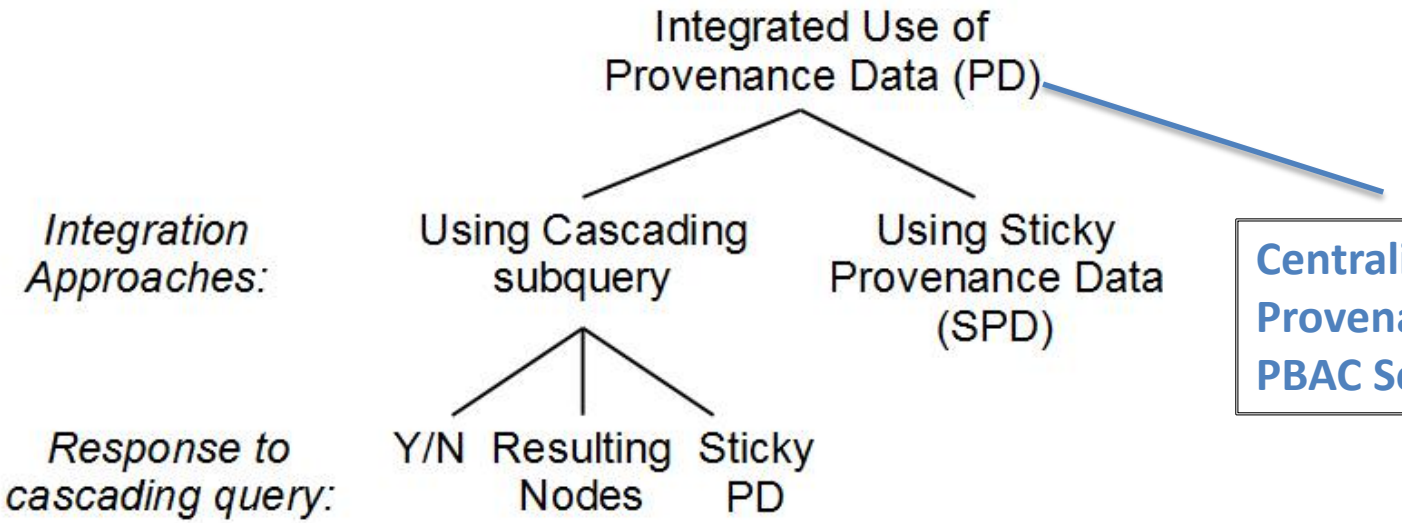
Multi-cloud PBAC



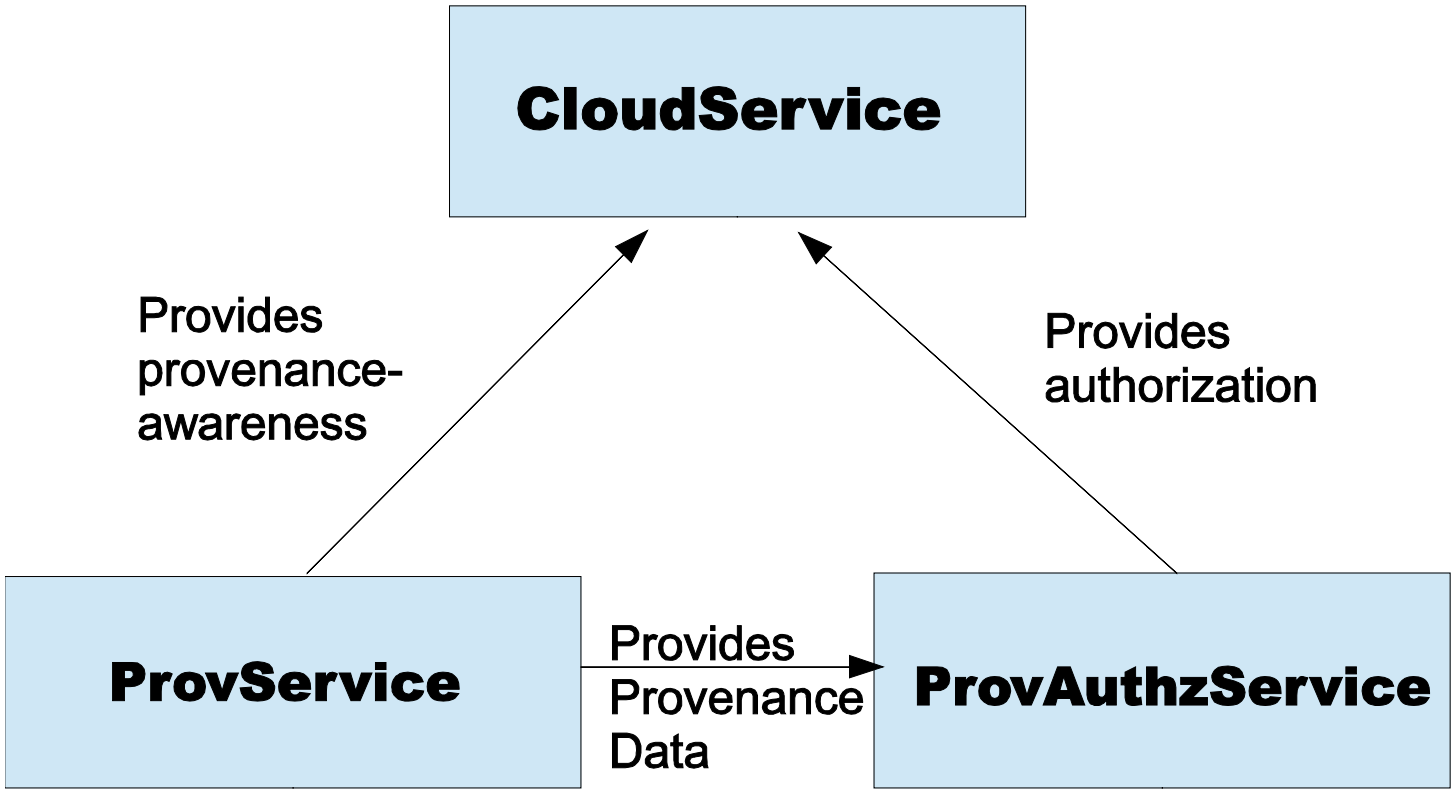
Provenance Data Sharing



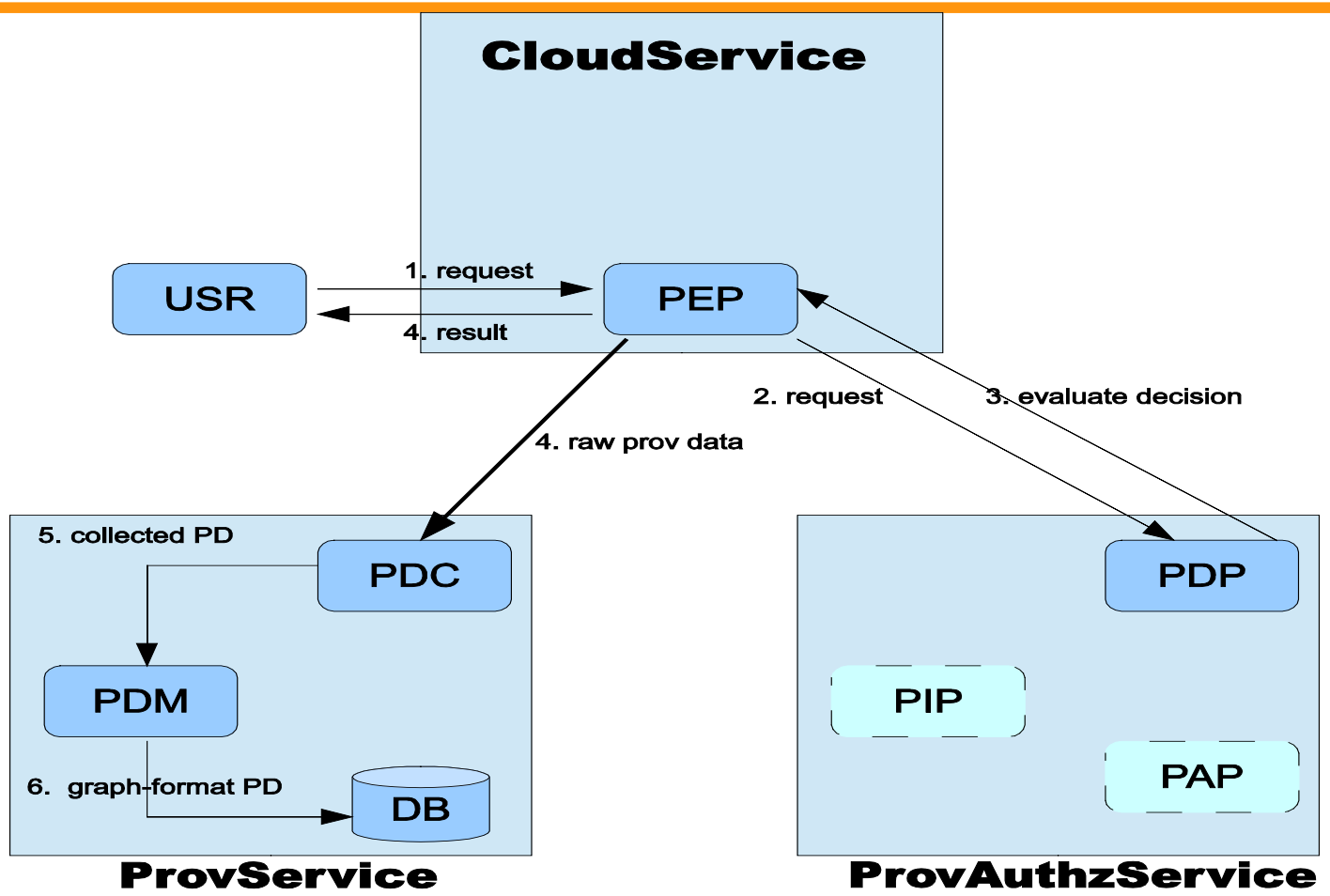
Provenance Data Sharing



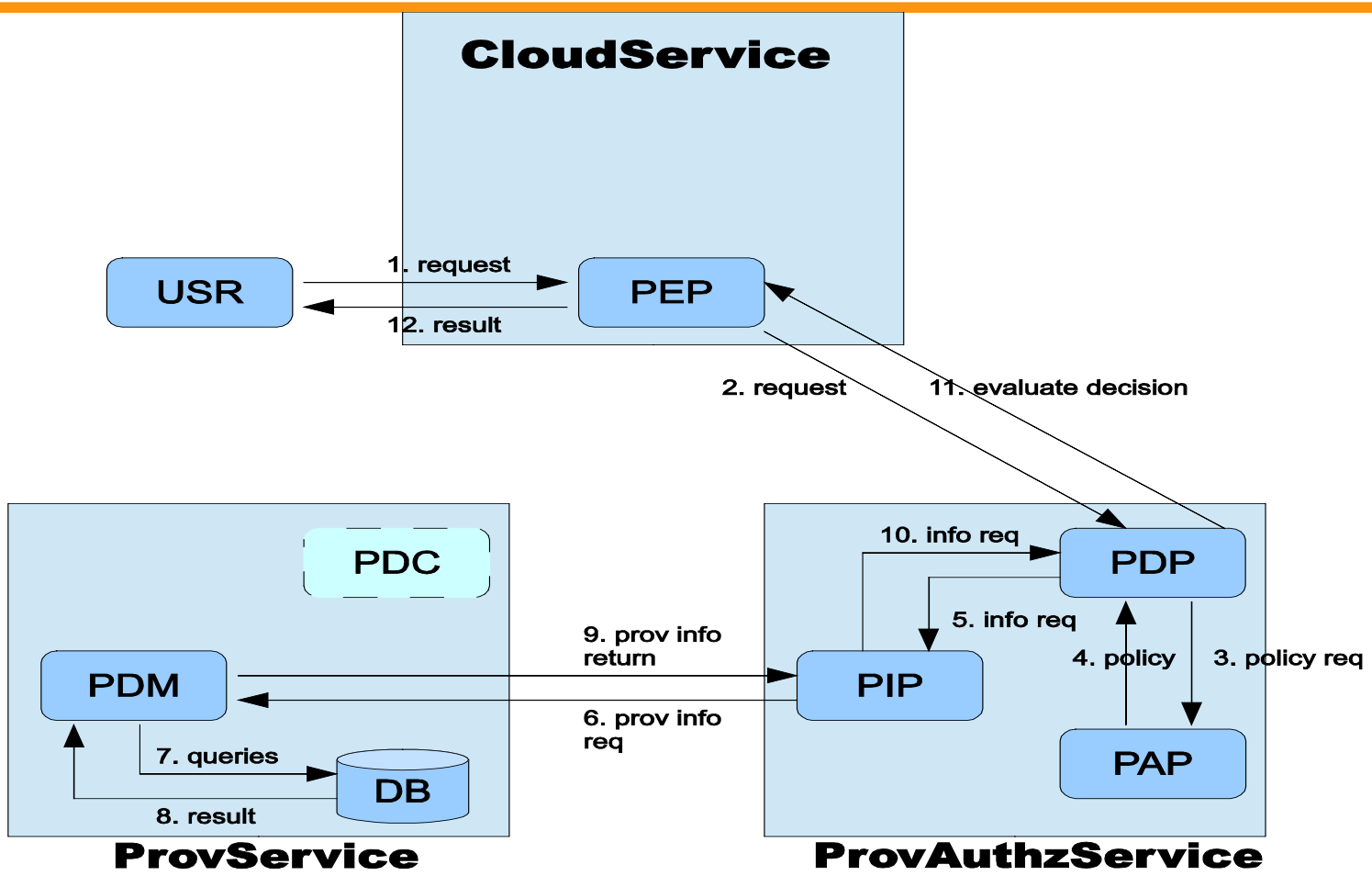
Single MT-Cloud PBAC Architecture



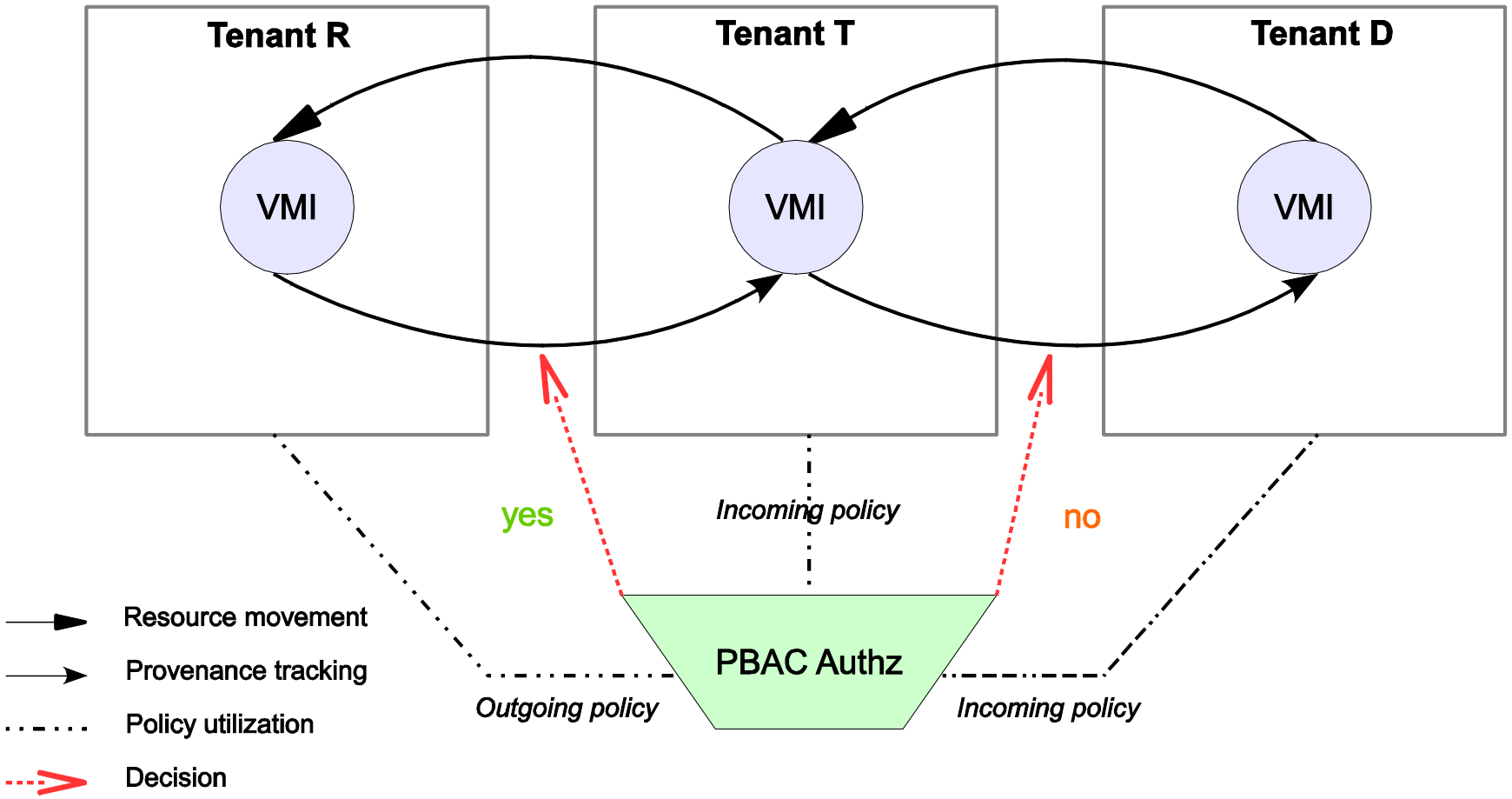
Provenance Service



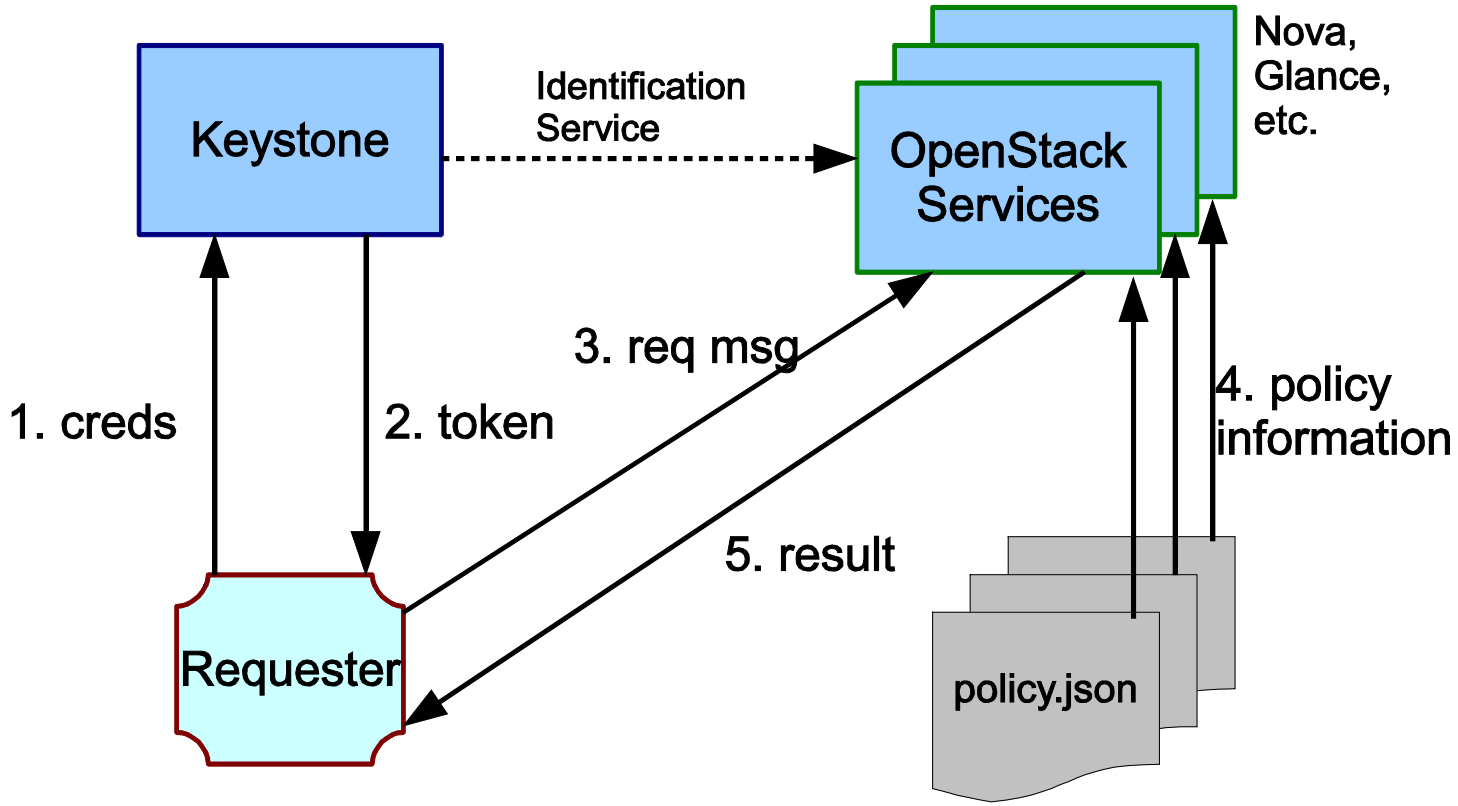
PBAC Service



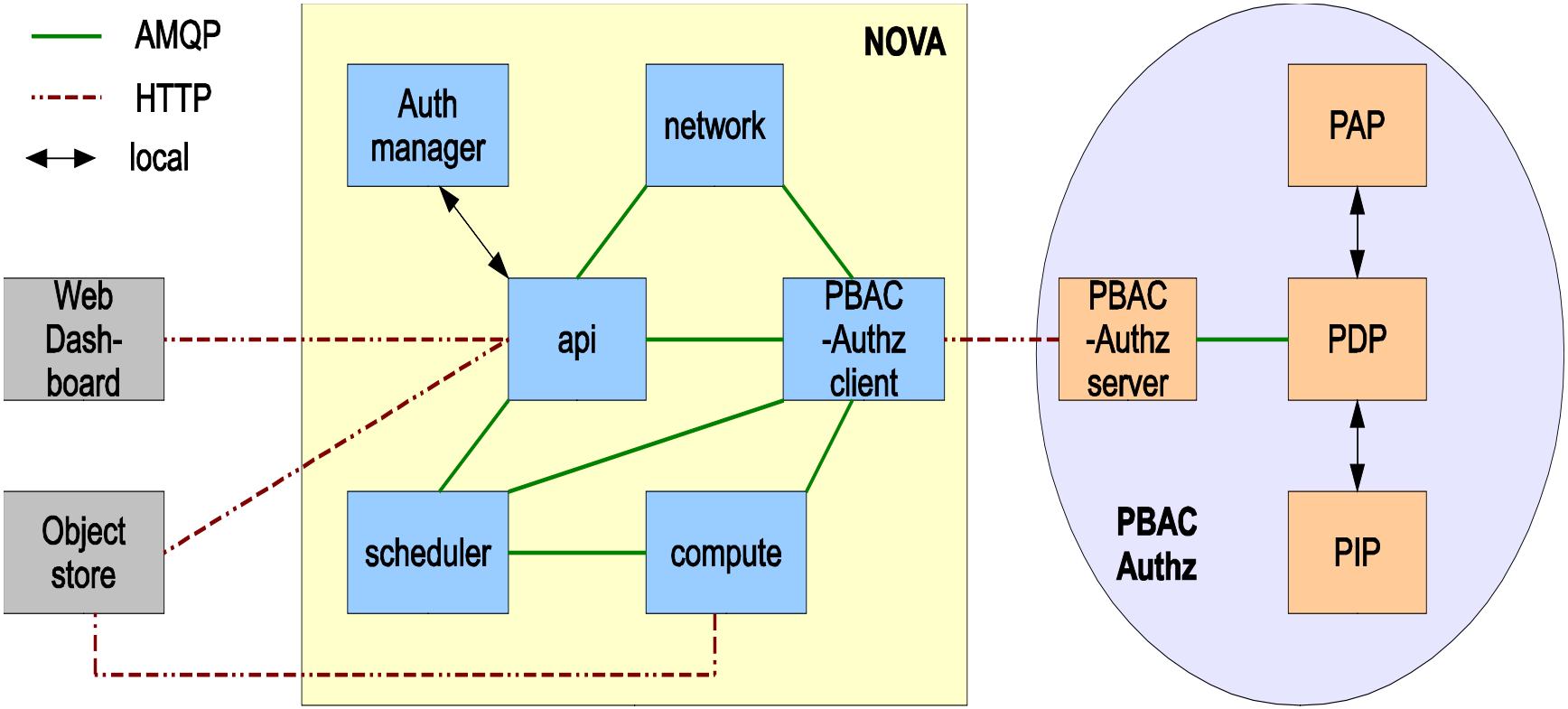
Cross-tenant PBAC



OpenStack Authz



Nova Architecture



Thank you!!!

- Questions and Comments?