Authorization Federation in IaaS Multi Cloud

Navid Pustchi, Ram Krishnan and Ravi Sandhu

SCC 2015
Why Multi Cloud?

Collaboration of organizations across clouds.

Organizations with resources across multiple clouds.

World-Leading Research with Real-World Impact!
Scope of Contribution

- **Cloud Federation**
  - **Service**
    - SaaS
    - PaaS
    - **IaaS**
  - **Platform**
    - Homogenous
    - Heterogeneous
  - **Trust**
    - Circle-of-Trust
    - Peer-to-Peer
  - **Coupling**
    - Authentication Federation
    - Authorization Federation

*World-Leading Research with Real-World Impact!*
Cloud Federation

- **Service (IaaS, PaaS, SaaS)**
  - Heterogeneous: Google account (Open ID 2.0) Heterogeneous within google.
  - Homogenous: Eduroam federated network access.

- **Platform**
  - Heterogeneous: OpenStack federation with AWS.
  - Homogenous: Keystone to Keystone federation.

- **Trust**
  - Circle-of-Trust: Alliance of institutions for sharing scientific data such as CERN.
  - Peer-to-Peer: Best Buy federating with Rackspace.

- **Coupling**
  - Identity Federation: SAML, OAuth, OpenID, SSO.
Trust Framework

- **Coupling**
  - Circle-of-Trust
  - Peer-to-Peer

- **Initiation**
  - Bilateral
  - Unilateral

- **Direction**
  - Bidirectional
  - Unidirectional

- **Transitivity**
  - Non-Transitive
  - Transitive

*World-Leading Research with Real-World Impact!*
Four trust types:

- **Type – α**: (Trustor grants inter-cloud access to trustee)
  - If $A \leq_\alpha B$, cloud $A$ is authorized to assign $B$’s users to cloud $A$’s resources. In such trust type, $A$ controls trust relation existence and cross-cloud assignments.

- **Type – β**: (Trustee grants inter-cloud access to trustor)
  - If $A \leq_\beta B$, cloud $B$ is authorized to assign $A$’s users to its resources. In such trust type, $A$ controls trust relation and $B$ controls cross-cloud assignments.

- **Type – γ**: (Trustee takes inter-cloud access to trustor)
  - If $A \leq_\gamma B$, cloud $B$ is authorized to assign its users to cloud $A$’s resources. In such trust type, $A$ controls trust relation and $B$ controls cross-cloud assignments.

- **Type – δ**: (Trustee controls intra-cloud access to trustor)
  - If $A \leq_\delta B$, cloud $B$ is authorized to assign $A$’s users to $A$’s resources. In such trust type, $A$ controls trust relation and $B$ controls intra-cloud assignments within $A$. 
Administrative Realms

World-Leading Research with Real-World Impact!
Three trust scopes based on administrative realms in cloud:

- **Cross Cloud Trust**
  - Sharing cloud infrastructure resources, such as services.

- **Cross Domain Trust**
  - Sharing domain resources such as projects.

- **Cross Project Trust**
  - Sharing project resources such as VMs.
Cloud Trust

- Enables sharing cloud resources, services and domains.
  - Set of domains shared between clouds with trust type (for domain trust).
  - Sharing services by creating private domains for service allocation.

- Trust relation in Cloud Trust is Peer-to-Peer, bilateral, bidirectional, non-transitive.
Domain Trust

- Enabling cross cloud access by assigning users to PRPs between trusted domains.

- Trust relations are Peer-to-Peer, unilateral, unidirectional, non-transitive.
• Enabling cross cloud access to service instances by assigning users to PRPs between trusted projects.

• Trust relations are Peer-to-Peer, unilateral, unidirectional, non-transitive.
Related Work

- **RBAC extensions**
  - ROBAC (collaboration ins not supported).
  - GB-RBAC (group does own users).

- **Role Based delegation models**
  - Delegation chains lacks dynamicity of trust in cloud federation environments.

- **Multi-tenant trust models in single cloud.**
  - MT-RBAC (Multi-Tenant RBAC).
  - CTTM (Cross Tenant Trust model).
  - OSAC-DT (OpenStack Access Control with Domain Trust).
Conclusion & Future Work

- **Multi-cloud trust model**
  - Cloud trust.
  - Domain trust.
  - Project trust.

- **Trust framework & trust types**
  - Four types of trust applicable to administrative realms in cloud.

- **Implementation in single cloud**
  - Partial implementation of domain-trust in single cloud OpenStack.

- **Future Work**
  - Cloud trust implementation.
  - Implementation in federated OpenStack clouds.
  - Project trust implementation.
  - Hierarchical multi-domain model.
  - Attribute based models.