Federated Access Control in Heterogeneous Intercloud Environment: Basic Models and Architecture Patterns

Craig Lee, The Aerospace Corporation
On behalf of
Yuri Demchenko, Craig Lee, Canh Ngo, Cees de Laat

Intercloud2014 Workshop
11 March 2014, Boston
Outline

- Background to this work
- Federation in Grid and Clouds
- InterCloud Federation Framework (ICFF) and federation infrastructure patterns
- Federated Access Control and Federated Identity Management in clouds

- Additional information
  - VO based federations in Grid (retrospective view)
Background to this work

- Cloud Federation BoF at OGF and follow on
  - As the main motivation motivated work of current author team with wide consultation with Grid and Cloud community

- Research at the University of Amsterdam on developing of the Intercloud Architecture Framework (ICAF)
  - Where the Intercloud Federation Framework is defined as a component for multi-provider infrastructure integration

- EGI (European Grid Initiative) Federated Cloud Task Force
  - Building Federated Cloud model based on Grid VO based federation model
Federation in Grid and Clouds: Grid VO vs Cloud Virtual Infrastructure

• Grid federates resources and users by creating Virtual Organisations (VO)
  – VO membership is maintained by assigning VO membership attributes to VO resources and members
  – Resources remain under control of the resource owner organisation Grid Centers
  – Users remain members of their Home Organisations (HO)
    • AuthN takes place at HO or Grid portal
    • To access VO resources, VO members need to obtain VOMS certificate or VOMS credentials

• In clouds, both resources and user accounts are created/provisioned on-demand as virtualised components/entities
  – User accounts/identities can be provisioned together with access rights to virtual resources
Cloud Federation: Actors and Roles

- Cloud Service Provider (CSP)
- Cloud Customer (organisational)
  - Multitenancy is provided by virtualisation of cloud resources provided to all/multiple customers
- Cloud User (end user)
- Cloud (Service) Broker
- Identity Provider (IDP)
  - Cloud Carrier
  - Cloud Service Operator
  - Cloud Auditor
Cloud Federation – Scaling up and down

• Scalability is one of the main cloud feature
  – To be considered in the context of hybrid cloud service model
    • Cloud burst and outsourcing enterprise services to cloud
    • Cloud services migration and replication between CSP

• Scaling up
  – Identities provisioning
  – Populating sessions context

• Scaling down
  – Identity deprovisioning: Credentials revocation?
  – Sessions invalidation vs restarting

• Initiated by provider and by user/customer
Cloud Federation Models – Identified models

User/customer side federation

• (1.1) Federating users/HO and CSP/cloud domains
  – Customer doesn’t have own IDP (IDP-HO)
  – Cloud Provider’s IDP is used (IDP-CSP)

• (1.2) Federating HO and CSP domains
  – Customer has own IDP-HO1
  – It needs to federate with IDP-CSP, i.e. have ability to use HO identities at CSP services

• (1.3) Using 3rd party IDP for external users
  – Example: Web server is run on cloud and external user are registered for services

Provider (resources) side federation

• (2.1) Federating CSP’s/multi-provider cloud resources
  – Used to outsource and share resources between CSP
  – Typical for community clouds
Basic Cloud Federation model (1.1) – Federating users/HO and CSP/cloud domains (no IDP-HO)

- Simple/basic scenario 1: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for users from HO1 and managed by HO1 Admin/Management system
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those created for Service Xa
- TODO: Extend with AuthN/AuthZ service in Virtual Service Environment

User side Federation
Basic Cloud Federation model (1.2) – Federating HO and CSP domains (IDP-HO1 and IDP-CSP)

- Simple/basic scenario 1: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for users from HO1 and managed by HO1 Admin/Management system
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those created for Service Xa
- TODO: Extend with AuthN/AuthN service in Virtual Service Environment
Basic Cloud Federation model (1.3) – Using 3rd party IDP for external users

- Simple/basic scenario 2: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for external users (e.g., website) and managed by Customer 1
- Involved major actors and roles
  - CSP
  - Customer
  - User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g., KeyStone) or those IDP-Xa created for Service Xa

User side Federation

External Users (Open Internet)

Customer 1
Admin/Mngnt System

Management (Ops&Sec)

User
User2
User1
User3

Ext/3rdParty IDP-HO1

Direct or Dynamic link

Federation relations

Cloud Provider A

Cloud Customer A1 (Running Service Xa)

User Xa.1
User Xa.2
User Xa.3

User Xa

CSP IDP/Broker

IDP-Xa

User Xa can be implemented as instantiated service of the CSP IDP

IDP-Xa
Basic Cloud Federation model – Combined User side federation

- Simple/basic scenario 2: Federating Home Organisation (HO) and Cloud Service Provider (CSP) domains
- Cloud based services created for external users (e.g. website) and managed by Customer 1
- Involved major actors and roles
  - CSP – Customer – User
  - IDP/Broker
- Cloud accounts A1.1-3 are provisioned for each user 1-3 from HO with 2 options
  - Individual accounts with new ID::pswd
  - Mapped/federated accounts that allows SSO/login with user HO ID::pswd
- Federated accounts may use Cloud IDP/Broker (e.g. KeyStone) or those IDP-Xa created for Service Xa
Basic Cloud Federation model (2.1) – Federating CSP’s/multi-provider cloud resources

- Cloud provider side federation for resources sharing
- Federation and Trust relations are established between CSP’s via Identity management services, e.g. Identity Providers (IDP)
  - May be bilateral or via 3rd party/broker service
- Includes translation or brokering
  - Trust relations
  - Namespaces
  - Attributes semantics
  - Policies
- Inter-provider federation is transparent to customers/users

Provider side Federation
Cloud Federation Model - Combined

(a) Enterprise Infrastructure

- (a) HO or (b) Custmr1 MgmtSystem

(b) External Users (Open Internet)

- (a) IDP-HO1
- (b) 3rd Party IDP

User side federation

- Direct or Dynamic link
- Federation relations

Instantiated IDP-A => IDP-Xa

User side federation

Provider side federation

Inter-provider federation for resources sharing

Management (Ops&Sec)

Cloud Provider A

- Cloud Service Xa

- CSP IDP-A

- Federation & Trust relations

Intercloud2014

Cloud Federated Access Control Patterns
Basic AuthN and AuthZ services using Federated IDPs – For additional Credentials validation

PEP - Policy Enforcement Point
PDP/ADF - Policy Decision Point
IDP – Identity Provider
PAP - Policy Authority Point
CtxHandler - Context Handler
CVS – Credentials Validation Service
Basic AuthN and AuthZ services using Federated IDPs – Federation/Trust domains
Implementation: Intercloud Federation Infrastructure and Open Cloud eXchange (OCX)

OCX Services

- Broker
- Trust Broker
- Gateway
- Cloud Service Broker
- Discovery
- Directory (RepoSLA)
- Cert Repo (TACAR)
- TTP Trusted Introducer
- FedIDP

OCX and federated network infrastructure

- Federation Infrastructure and Open Cloud eXchange (OCX)
- Intercloud Federation Infrastructure

GEANT Trans-European infrastructure

- Federated Cloud Instance Customer A (University A)
- Federated Cloud Instance Customer B (University B)

Cloud Federated Access Control Patterns
Summary and Future work

• The proposed Intercloud Federation Framework is a part of the general Intercloud Architecture Framework and intends to provide a basis for further API and protocols definition.

• It is based on wide discussion among OGF, EGI and cloud security community.

• Currently the proposed approach and model are being implemented as a part of the GEANT infrastructure to support Intercloud services delivery to member universities.
Discussion and Questions
Reference information and diagrams

- VO based Grid federation model
- AuthN and AuthZ services operation
VO based Grid federation model
VO2007: VO in Collaborative applications and Complex Resource Provisioning

- Two basic use cases considered
  - Grid based Collaborative applications/environment (GCE) built using Grid middleware and integrated into existing Grid infrastructure
  - Complex resource provisioning like Optical Lightpath provisioning (OLPP), or bandwidth-on-demand (BoD)

- VO based functionality (and requirements) to support dynamic security associations
  - Dynamic Trust management
    - Establishing dynamic trust management relations between VO members
  - Attribute and metadata resolution and mapping
    - VO-based access control service requires common VO-wide attributes that however can be mapped to the original ones
  - Policy combination and aggregation
    - To allow conflict resolution and policy harmonisation between VO members
  - Flexible/distributed VO management infrastructure
VO2007: VO bridging inter-organisational barriers

- VO allows bridging inter-organisational barriers without changing local policies
  - Requires VO Agreement and VO Security policy
  - VO dynamics depends on implementation but all current implementations are rather static
Example VO Security services operation

Basic VOMS functionality in Grid

Clouds provide full resources and infrastructure services virtualisation
VO2007: VOMS – standard-de-facto for VO management

- **VO Membership Service (VOMS)** is a standard-de-facto for VO management and VO-based authorisation in Grid
  - VO is represented as a complex, hierarchical structure with groups and subgroups
    - Subgroup management may be delegated to different administrators
  - Every user in a VO is characterised by the set of attributes
    - Group/subgroup membership, roles and capabilities – so-called 3-tuples
    - Combination of all 3-tuples for the user is expressed as a Fully Qualified Attribute Name (FQAN)
    - FQAN is included into VOMS X.509 Attribute Certificate (AC)
  - **VOMS infrastructure**
    - May contain multiple VOMS serves and synchronised VODB’s
    - Supports user calls for VOMS AC’s and VOMS admin tasks
  - **VOM Registration** is developed by Open Science Grid (OSG) project to support users self-registration
VO2007: Dynamic Security Associations

- **Session** – establishes security context in the form of session key that can be a security token or simple UID bound to secure credential/context
  - Session may associate/federate users, resources and actions/processes
- **Job/workflow** – more long-lived association and may include few sessions
  - May need to associate more distributed collection of users and resources for longer time required to deliver a final product or service
  - Job and workflow may contain decision points that switch alternative flows/processes
  - Security context may change during workflow execution or Job lifetime
  - Job description may contain both user and resource lists and also provide security policy and trust anchor(s) (TA)
- **Project or mission oriented cooperation** – established for longer time cooperation (involving people and resources) to conduct some activity
  - This is actually the area of currently existing VO associations
- **Inter-organisational association or federation** – established for long-term cooperation, may have a wide scope of cooperative areas
  - This is the area of inter-university associations
    - Shibboleth Attribute Authority Services (SAAS) is designed for this kind of federations
VO2007: Conceptual VO Operational Models

- **User-centric VO (VO-U)** - manages user federation and provide attribute assertions on user (client) request
- **Resource/Provider centric VO (VO-R)** - supports provider federation and allows SSO/access control decision sharing between resource providers
- **Agent centric VO (VO-A)** - provides a context for inter-domain agents operation, that process a request on behalf of the user and provide required trust context to interaction with the resource or service
- **Project centric VO (VO-G)** - combines User centric and Provider centric features what actually corresponds to current VO use in Grid projects
VO2007: Conceptual VO Management Framework

- VO establishes own virtual administrative and security domains
  - It may be separate or simply bridge VO-member domains
- VO management service should provide the following functionalities
  - Registration and association of users and groups with the VO
  - Management of user attributes (groups, roles, capabilities)
  - Association of services with the VO
  - Association of policies with the VO and its component services
- VO Registry service for wider VO implementation may be required
  - VO naming should provide uniqueness for the VO names
VO2007: VO Security Services

– VO as a component of the Security infrastructure should provide the following security services
  • Policy Authorities (e.g. GPBox)
  • Trust management service (GridPMA)
  • Identity Management Service (by HO)
  • Attribute Authorities (VOMS)
  • Authorization service (CAS)
  • Authentication service
  • Logging, Accounting