Toward Single Sign-on Establishment for User-friendly Inter-Cloud Environment

International Symposium Grids & Clouds 2019
2nd – 5th April 2019
Academia Sinica, Taipei, Taiwan

Eisaku SAKANE, Takeshi NISHIMURA, Kento AIDA, Motonori NAKAMURA
National Institute of Informatics

NII
National Institute of Informatics

Outline

- Background
- Issues
- Design & Implementation
- Demo
- Discussion
- Summary

Background

- Many different clouds are available to offer a variety of services.
- Users can choose various services from multiple cloud venders according to the demands of the users.

- Single sign-on mechanism is indispensable for *inter-cloud* computing environment.

- In general, a single sign-on mechanism works within a cloud environment provided by a single cloud vendor.
- However, a single sign-on mechanism that *extends* across multiple clouds is not always established at the beginning of use.

Background (cont’d)

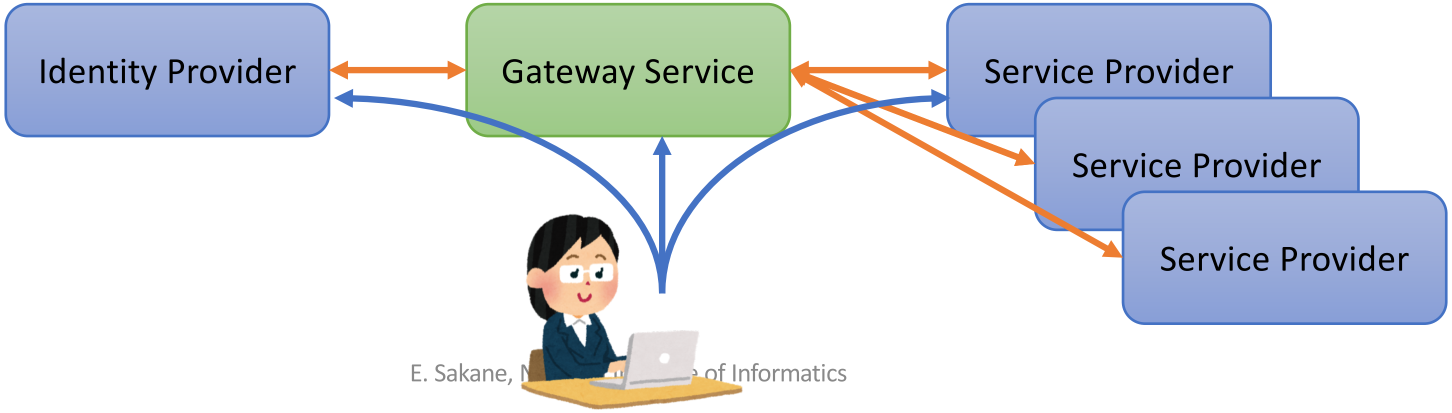
- For example, an academic researcher who can obtain a SAML assertion from the home organization should be enabled to access a public cloud with the assertion.
- Since many cloud vendors, of course, already supports major authentication technologies such as SAML and OpenID Connect, technically the credential issued by the home organization will be usable for access to public clouds.
- However, it is often hard for the identity provider operated by the home organization to manage the user attributes that the cloud vendor requires, because the operating department of the IdP is responsible only for attributes that are assigned naturally in terms of the constitute member of organization, and it will be quite a burden to manage various attributes for users individually unless the cloud service is provided for all members as a common service.

Guiding Questions

- How do we build a mechanism for handling necessary attributes information based on the credential issued by the home organization?
- What should we do in order not to impose a burden on administrators of the identity provider?

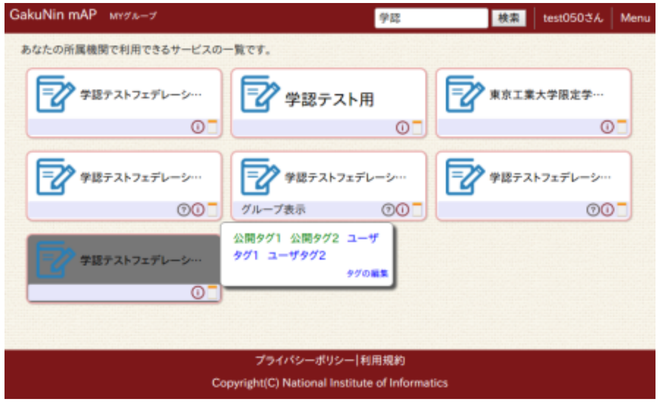
Design

- Gateway service approach
  - authenticate users with credentials issued by the home organization.
  - provide a function that allows Service Provider to set attribute *types* that the SP requires.
  - provide a function that allows users or representatives to set the *values* of the required attributes.
  - make an assertion that is composed of the required attributes and the fundamental attributes managed by the home IdP, and send it to the SP.
  - provide users with a user-friendly interface for access to available services.



GakuNin Cloud Gateway Service

- A web portal system for federated identity w/SAML.
- CGS can show available services as icon.
  - permitted by organization
  - permitted by group
- Typical flow is the following:
  - User accesses to the CGS.
  - Internal SP in the CGS responds and embedded DS shows the list of IdP to the user.
  - The DS redirects to IdP specified by the user.
  - After the authentication succeeded, the CGS displays the available services as icon.
  - The CGS redirects to the SP that provides the service selected by clicking.
  - The service interprets the entityID of the IdP and then redirects to the IdP.
  - The service receives the assertion sent by the IdP with SSO.
  - The user now uses the service.

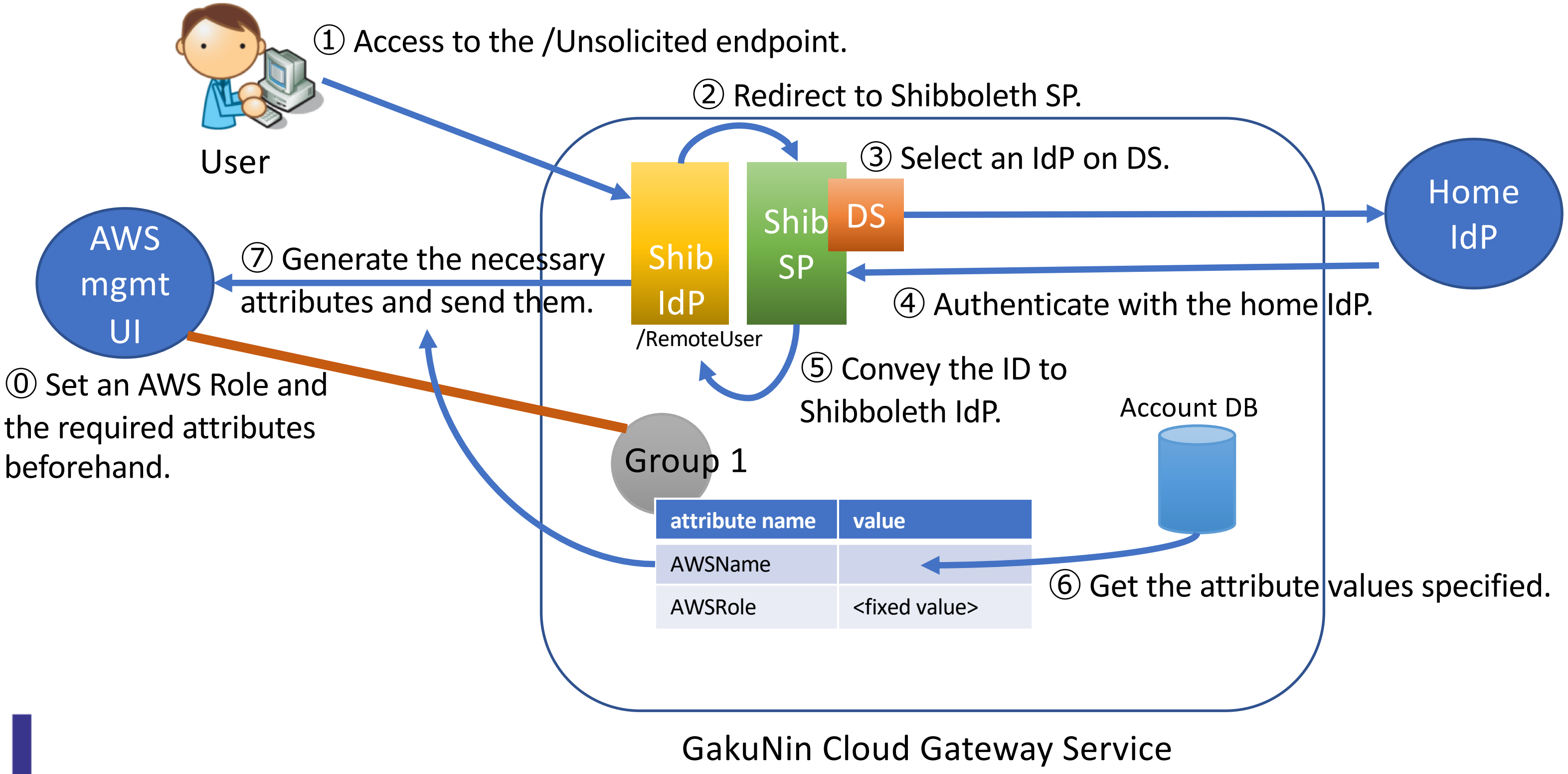


あなたの所属機関で利用できるサービスの一覧です。

Copyright(C) National Institute of Informatics

Implementation

- Access to AWS with SAML 2.0 assertion via the GakuNin CGS.



① Access to the /Unsolicited endpoint.

② Redirect to Shibboleth SP.

③ Select an IdP on DS.

④ Authenticate with the home IdP.

⑤ Convey the ID to Shibboleth IdP.

⑥ Get the attribute values specified.

⑦ Generate the necessary attributes and send them.

⓪ Set an AWS Role and the required attributes beforehand.

attribute name	value
AWSName	
AWSRole	<fixed value>

GakuNin Cloud Gateway Service

Flow for access to AWS with SAML

- AWS account user creates a Role and a SAML-ID provider according to the AWS instruction.
  - determine the set of types and values of attribute for authorization.

- Administrator of SP connector for AWS sets up the required attribute types and sets common fixed values for any AWS roles.
- Group administrator sets user configurable values, the AWS Role and SAML-ID provider.
- User, a member of the group, can access the AWS Role by just clicking the icon.

Demo

Discussion

- Required attributes can sent to AWS without any changes of setting of the home organization IdP.
- Home organization IdP does not need to modify the setting of the IdP by using the AWS support of GakuNin CGS even if the organization provides AWS services to all constitute members.

- If there are different AWS roles that require different attributes, the administrator of SP connector for AWS must setup all attributes.
- The administrator of SP connector AWS must grasp all attributes that all AWS Roles defined by any groups in the GakuNin CGS require.

Summary

- We proposed a model that realizes single sign-on in an inter-cloud environment by designing required attributes assignment mechanism.
- Based on the GakuNin CGS, we implemented the functions that allow users to access to Amazon Web Service with SAML 2.0.

- Our approach can be applied to the other services that correspond to SAML 2.0.
- We will examine more services and improve the proposed system.