Interoperate in Cloud with Federation

Leveraging federation standards can accelerate Cloud computing adoption by resolving vendor lock-in issues and facilitate ‘On Demand’ business requirements.

Federation in simple terms can be defined as two partners sharing some data. The data could be user's identity, resources, files, resource information or any other information. Identity Federation in particular has gained prominence because Internet users find it painful to maintain multiple access credentials to access services from multiple service vendors. Also, the Cloud service vendors need to maintain multiple access permissions for each user account. In Cloud offerings, multiple service vendors would generally interact with each other, so the need of the hour is a strong federation system built into Cloud-based offerings. The federation can play an important role in enabling two of the most important characteristics of the Cloud: Automatic Provisioning and Seamless Resource Access. Identity Federation enables authentication and authorization via trust credentials propagation.

While performing ROI analysis for Cloud offerings, enterprises must also consider the federation support from the Cloud vendors. Enterprises can avoid vendor lock-in scenarios if their associated Cloud vendors support more than one federation's standards. This paper includes various use cases where Cloud federation deployment is substantially beneficial as it supports single sign-on access as well as interoperability.

– Neha Mehrotra and Nitin Dangwal
From the Cloud vendor's perspective, it is advisable that more than one federation's protocols (like SAML, WSFED, OpenID, OAuth, etc.) are supported by the service offerings. Supporting multiple protocols provides the scalability and flexibility to federate with a wide range of products. Multiple protocols support the service offering and this is facilitated through a lightweight federation exchange layer that is deployed as a hub to convert trust attributes from one format to another. Organizations may have an established federation structure deployed within their enterprise. They would choose the Cloud vendor who either supports the same standard or provides the format conversion ability that would offer seamless access.

It is out of the scope of this document to discuss how federation in Cloud impacts billing, licensing and tracking of the service parameter quality.

**Use Case #1: Inter Cloud Federation**

IaaS (Infrastructure as a Service) is one of the Cloud offerings wherein enterprises would take infrastructure on lease from various Cloud vendors. Although Cloud is considered to have infinite resources, in the real world, there would always be an upper limit based upon restrictions on available hardware, network bandwidth, etc. When there are many infrastructure offerings provided by a Cloud vendor, there arises a situation where the Cloud vendor suffers resource exhaustion.

Under such circumstances a single Cloud vendor, by itself, may not be able to fulfill additional infrastructure requirements of enterprises (like requirement of additional servers during peak season). In such cases, Inter Cloud Federation contributes beneath the layers to fulfill the infrastructure requirements of enterprises seamlessly. The enterprise would be aware of only the primary Cloud vendor. Through the primary Cloud vendor’s single virtual interface, the enterprise must be able to add infrastructure components and administer them as per their requirements. The actual action (addition, migration, etc.) on infrastructure components in different Clouds would be handled by Cloud vendors automatically. Such operations would be opaque to the enterprise utilizing the Cloud-based IaaS.

Providing federation capabilities among the Cloud offerings require all Cloud vendors to use some standardized mechanism for sharing resources and identity among themselves. The resources could be information, files, computing resources, etc.

Inter Cloud Federation may require just-in-time identification and messaging protocol between Clouds. Technologies like XMPP (Extensible Messaging and Presence Protocol) can be used for identifying Cloud just-in-time and sharing messages between Clouds.

OASIS’s SPML (Service Provisioning Markup Language) can be used as a communication protocol between Clouds for user provisioning, resource information sharing and resource sharing. Service Provisioning Markup Language (SPML) provides XML based structures for representing provisioning or deprovisioning requests intended for identity lifecycle management. SPML can also be used for resource provisioning and resource information provisioning among partners. Hence, incorporating and adopting SPML within Cloud offerings can facilitate automatic provisioning and deprovisioning of resources without manual intervention.

Inter Cloud Federation provides more flexibility to both Cloud vendors and enterprises. Billing, licensing and usage tracking of services would play an important role in case of Inter Cloud Federation. However, this white paper only focuses on how Inter Cloud Federation can be achieved. Billing, licensing, etc., are currently not discussed in this white paper.
There could be similar business use case where an enterprise is using IaaS from more than one Cloud vendor. The reason for choosing multiple Cloud vendors could be to mitigate risk, to avoid vendor lock-in or to manage bandwidth requirements. Each enterprise would have a secure account information to access specific Cloud offerings. In the production environment, this secure information needs to be shared with other Cloud vendors for seamless connectivity. The automatic activation and provisioning to the second vendor through SPML / SAML should happen in the background without any intervention. Single sign-on is available only with the appropriate federation among Cloud vendors.

Public and Private Cloud Federation

As an extension to the Inter Cloud Federation concept, a private Cloud has restricted access and is controlled completely by the enterprise. It can host sensitive applications that are generally not suitable for deployment on a public Cloud. A private Cloud is not accessible from an outside enterprise network but can access the outside network. Consider a case wherein an enterprise has setup a private Cloud but now requires additional infrastructure. When there are many applications deployed on the private Cloud, it deploys the services of other public Clouds. In such eventuality, it results in the private Cloud to federate with the public Cloud.

Use Case #2: Federation among Applications

The following subsections discuss various deployment models for SaaS offerings and elaborates on how a federation can help in each of the deployment models.

Federation among Applications deployed within a Cloud

As more and more applications are deployed on a Cloud, communication among applications is inherently required. For instance, a travel service deployed on Cloud should successfully federate with a hotel booking service deployed on the same Cloud by a different SaaS vendor.
Federation amongst various SaaS offerings within a Cloud must be performed using some standardized mechanism like OASIS SAML (Simple Assertion Markup Language), WSFED, OAUTH, OpenID etc.

Consider a identity provider (XYZTravel.com) who has generated an XML document called ‘assertion’. The ‘assertion’ contains user’s identity information, identity provider’s identity information, and user authentication details and may also contain attribute information pertaining to the user. This information is shared with Service provider (ABCHotels.com) as per SAML standards. ABCHotels.com validates, parses the ‘assertion’ document and provides access to the user as per its policies. After successful single sign-on, the user can book the hotel through ABCHotels.com Web site without providing credentials explicitly.

Each application (XYZTravel.com and ABCHotels.com) should have its own billing and licensing system. Federation between applications helps applications to federate identity and to perform single sign-on. After single sign-on parameters like licensing, billing etc. can be tracked at each application level.

**Federation among Applications Deployed on Different Clouds**

As explained above, using SAML standards for Federations among SaaS offerings would allow individual SaaS offerings to federate with other SaaS offerings deployed on different Clouds.

Various SaaS offerings would access each other over Internet through SAML protocol to federate identity, account, service or any other information.

**Federation among On-premise and Cloud Applications**

Cloud offerings must provide capabilities to be able to federate with on-premise applications through internet.

For example, an on-premise reservation system provided by an independent vendor should be able to federate with a billing SaaS offering on Cloud. The exchange of secure information should happen similar to two SaaS offerings within a single Cloud.

There may be use cases wherein an enterprise wants to move from a SaaS Cloud offering back to being hosted as an on-premise application due to security / ROI issues. The migration from a SaaS offering to on-premise application can be made easier with a federation capability between on-premise application and SaaS offerings (like database service or federation with other SaaS offerings). The SaaS offering (or on-premise offering) of the application can then be phased out gradually.

**Use Case #3: Deprovisioning**

Automated deprovisioning is one of the concerns in Cloud. When an enterprise uses IaaS from a Cloud
vendor, the need to provide a reliable mechanism for deprovisioning of resources whenever the contract between the Cloud vendor and the enterprise terminates is required.

Deprovisioning can be considered as an extension to Use Case #1; wherein multiple Clouds are federating among themselves to provide required infrastructure services to an enterprise. On the similar lines during deprovisioning, Cloud vendors must federate among themselves to deprovision the resources as per requirements.

Deprovisioning could be further of user's license, registration, resource access etc. The SPML framework also standardizes deprovisioning message. This would enable cloud vendors and applications to send / receive deprovisioning messages and act accordingly since it is a standards based approach deprovisioning messages across Cloud vendors.

Deprovision has two important aspects associated with it:

- **Migration of Data**: The Cloud vendors must provide some mechanism to migrate data, application deployed on Cloud
- **Clean Deprovision of Data**: Removing data, application or infrastructure deployed on a Cloud is dependent on individual Cloud vendors to clean up. The clean up must happen as per the contract between the Cloud vendor and the enterprise using the Cloud services. There are risks associated with clean deprovisioning of resource and is out of scope of this white paper

### Commercial and Contractual Point of View

The below table is a proposed contractual model between enterprises and Cloud vendors from understanding perspective. Since different enterprises may have different requirements and one contractual model may not fit all. So Cloud vendors need to provide different contractual offerings to enterprises to choose from.

<table>
<thead>
<tr>
<th>Proposed Contractual models</th>
<th>Pricing</th>
<th>What is in for Enterprise</th>
<th>What is in for Cloud vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opaque</td>
<td>Cheapest</td>
<td>Lesser price. Deployment is opaque to Enterprise. Enterprise does not have any level of control.</td>
<td>Least complexity. Cloud vendors determine what infrastructure components are deployed in which cloud.</td>
</tr>
<tr>
<td>Translucent</td>
<td>More priced</td>
<td>Enterprise know what infrastructure component is deployed in which cloud.</td>
<td>Primary Cloud vendor has control on which ‘Tier 2’ clouds vendors should be used.</td>
</tr>
<tr>
<td>Transparent / Premium Service.</td>
<td>Highest</td>
<td>Primary Cloud vendor is the SPOC for Enterprise. Maximum level of control provided to enterprise. Enterprise can choose ‘Tier 2’ cloud vendors. Avoids vendor lock-in.</td>
<td>Cloud vendors get better price. Competitive: As enterprise has the flexibility to dump a cloud vendor.</td>
</tr>
</tbody>
</table>
Business Use Case

Following example demonstrates the significance of Federating Cloud Providers. Take an example of a Cloud consuming enterprise for storage. The enterprise deals in end-to-end QA assurance of products and majorly provides load testing and performance results and optimization for its clients. For one such scenario, it requires extensive storage for multiple data records to perform load testing for one of the leading Web service. Data storage is required for a short period of time and hence the enterprise is employing multiple IaaS vendors providing storage on demand. The enterprise can use multiple vendors to solicit maximum advantage and ROI using Federation.

Above diagram demonstrates how this enterprise can interact with multiple storage vendors:

- The enterprise requests storage from Cloud 1 as well as Cloud 2. Cloud 1 supports different SLA and storage parameters than Cloud 2. Enterprise may also register and employ different Cloud vendors for backup and recovery.
- Now coming to Cloud 2. Cloud 3 is federated with Cloud 2. When storage requests exceeds the Cloud 2 capacity, Cloud 3 provides extra storage units to Cloud 2. The interaction between Cloud 2 and Cloud 3 is hidden from the end enterprise. SLA and Contracts still stay between the enterprise and Cloud 2. Although, the enterprise is using the storage units from Cloud 3 in case of increase in requirements, yet the whole management and contractual details stay hidden. Hence, Federation between Cloud 2 and Cloud 3 enables the parent Cloud vendor to meet the SLA as promised to the end Cloud consuming enterprise. In turn, enterprise is assured that the even with increase in demand, Cloud vendor will be able to meet the requirements.

Market Research: Federation Solutions and Standards for Cloud

IAM software vendors have acknowledged the importance of Federation for Cloud services to support Interoperable and Open clouds. Federation solutions from various market leaders are being leveraged and deployed for Cloud Services. Major solutions and products are discussed in following sub sections.

CA Technologies®

A prominent IAM solution vendor CA Technologies® has demonstrated that its proprietary CA SiteMinder® Federation Security Services and Federation Manager can provide identity federation capabilities and enable user to federate across organizations as well as cloud services. CA Cloud Security products provide end-to-end system for identity and access management for securing:
- Enterprises leveraging Cloud services
- Cloud vendors

Cloud offerings and services CA Federation Manager’s deployment facilitates identity federation for Salesforce.com®, Google® Apps and any Cloud offering supporting SAML protocol. CA Identity Manager® facilitates auto provisioning and enterprise onboarding by supporting SPML, SAML, Web services and customized connectors. CA has a successful provisioning connector for onboarding from Salesforce.com® to Google® Apps and demonstrated the capability of just in time provisioning while identity federated SSO and managing enhanced management for Cloud federation. CA also provides additional provisioning connectors for generic SaaS offerings.

Ping Identity®

Ping Identity® primarily deals in Federation enabling products like PingFederate® and PingConnect. PingFederate® has extensive support for SAML protocols and works with any SaaS product / application that supports SAML. PingConnect is an on demand Federation offering online SSO to small

QA assurance enterprise

Cloud 1

Cloud 2

Cloud 3
and medium enterprises. More than 80 SaaS vendors like Salesforce.com®, WebEx®, Google® Apps, and ADP etc. are using Ping Identity products. Ping’s Cloud Identity Connectors support federation with Facebook, Salesforce® CRM, Google® Apps, AOL and Yahoo®. Enterprises can now apply authentication to their SaaS applications with the connectors for B2C as well as B2B.

Oracle®

Oracle Identity Federation® shares trust data securely and supports SAML protocol. Oracle® provides interoperability between Cloud vendors like Salesforce.com®, Google® Apps and Oracle® CRM as a Service. Oracle Identity Federation 11g supports leading standards based protocols that leverages on the Cloud Federation.

IBM®

IBM Tivoli® Federated Identity Manager provides federated access control and management to on-premise as well as Cloud based services. IBM® provides comprehensive support for SAML 2.0 and claims that its product enables a secure model across Cloud services by facilitating identity federation in a Cloud environment.

TriCipher™

TriCipher offers a product named ‘myOneLogin’ that enables SSO to multiple Web services with single trust credentials. ‘myOneLogin’ uses strong authentication and prevents vulnerabilities and attacks. Like Ping Identity products, myOneLogin grants access to SaaS vendors like Google® Apps, WebEx®, Salesforce.com®, and Microsoft® Outlook, eBay® and PayPalTM. The product is also available on demand.

Support & Capabilities Matrix

<table>
<thead>
<tr>
<th>Protocols</th>
<th>SAML</th>
<th>WS-Federation</th>
<th>OAuth</th>
<th>SAML</th>
<th>OpenID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA</td>
<td>✓</td>
<td>✓</td>
<td>NA*</td>
<td>✓</td>
<td>NA*</td>
</tr>
<tr>
<td>Technologies®</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle®/Sun</td>
<td>✓</td>
<td>✓</td>
<td>NA*</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Microsoft®</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ping Identity®</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>NA*</td>
<td>✓</td>
</tr>
<tr>
<td>Google®</td>
<td>✓</td>
<td>NA*</td>
<td>✓</td>
<td>NA*</td>
<td>✓</td>
</tr>
<tr>
<td>IBM®</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>TriCipher TM</td>
<td>✓</td>
<td>NA*</td>
<td>NA*</td>
<td>NA*</td>
<td>NA*</td>
</tr>
</tbody>
</table>

NA*: Information not available regarding whether the IAM vendor supports that particular protocol or not.

The support matrix above highlights the various vendors versus the federation protocols that they support. Note that most vendors do acknowledge and accept almost all Federation protocols; yet the actual support in their products may be in progress and may not be currently available in the market. SAML supports strong authentication and SSO across domains as well. It is apt for most of the Cloud vendor / user requirements and is available in all leading Federation products. Though, OpenID is extensively becoming popular open Federation protocol and is supported by organizations like Google®, Microsoft®, PayPalTM, IBM®, and Yahoo®, yet, it is not adopted for Cloud services due to some inherent trust issues.
Conclusion

This paper elucidates the importance of Federation in Cloud deployment. In today's competent business scenario, enterprises would need to support various Federation protocols to be able to provide seamless connectivity across applications and across various forms of deployments. From an enterprise perspective, Federation between clouds provides flexibility to avoid vendor lock-in scenario. From the Cloud vendor's perspective, Federation helps to maintain the Quality of Service parameters committed to enterprises. For an end user, Federation provides the capability for seamless access across various applications.

References

http://mscerts.net/programming/relevant%20iam%20standards%20and%20protocols%20for%20cloud%20services%20(part%202).aspx
http://www.xmpp.org
http://www.pingidentity.com

About the Authors

Nitin Dangwal is a Technology Architect at Infosys Engineering Services. He has more than 7 years of industry experience and almost 6 years of experience in Federation and Web Security domain. Over past 6 years, he has been involved in development and sustenance of Federation products. He can be contacted at Nitin_Dangwal@Infosys.com

Neha Mehrotra is a Technology Architect at Infosys Engineering Services, Infosys Technologies. She has almost 8 years of experience in Java and Java EE technologies. She has been involved in development and sustenance of identity and access management products. She is currently involved in research involving Testing framework for Cloud based offerings. She can be contacted at Neha_Mehrotra@Infosys.com

About Infosys

Many of the world’s most successful organizations rely on Infosys to deliver measurable business value. Infosys provides business consulting, technology, engineering and outsourcing services to help clients in over 30 countries build tomorrow’s enterprise.

For more information about Infosys (NASDAQ:INFY), visit www.infosys.com.