Federation Management: What It Is, Why It Is Critical to Future Ground Systems – and What We Should Do About It

Dr. Craig A. Lee, lee@aero.org
Senior Scientist, Computers & Software Division
The Aerospace Corporation

Ground System Architectures Workshop
Cloud Computing Working Group
March 15, 2017
Big Picture Perspective: Transition of the Space Enterprise

The First 50 years... The Frontier Years

- Going where no one had gone before...
- Each mission had to develop and bring everything to that frontier
- Like building a homestead in the wilderness, each stove-piped system had to carry the full industrial base, technologies, systems development, launch, ground operations, dissemination and sustainment to the site

Imagine an urban space future... A layered, plug-in architecture/infrastructure where capabilities are families of payloads that plug in to a hosting layer
- The hosted payloads plug into a cyber-protected transport layer: akin to tying into a city's roads, power, water, sewer and network grids
- Transport layers connect to a mission management layer that manages and disseminates payload data to users
- Transformation is via customizable mission payloads, commercially available buses, launch services and provisioned operations
- Organizations will need to securely collaborate in this "urban environment", i.e., share data and resources

Enabling Technologies & Market Drivers

- Commercial & International Space Industry
- Pervasive open source software
  - High bandwidth networks
  - Commercial Services
  - Cloud Computing
  - Netcentricity
  - Nanotechnologies
  - Horizontal industries

The Future of Space... The Urban Years
This Need to Collaborate Is the Need for **Federation**

- The need to collaborate, i.e., *share information and services*, has been widely recognized, e.g.,
  - *Information Sharing Environment*
  - *Secure Information Enclave*
  - *Virtual Organization*
- Whatever the name, this requires *federation management*
  - A *federation* is a security and collaboration context that enables joint security policies to be defined, agreed upon, and enforced among participants
- Without some form of federation -- collaboration, data access, and interoperability will continue to be a problem, even in the same cloud
  - *Stove-piped systems "fork-lifted" on to a cloud will still be stove-piped*

*We need an established mechanism for “Bridging Silos” on-demand!*
A Motivating Example: Ground Enterprise View to Support Future Space

These are multiple organizations that must have a way to securely and flexibly manage how they collaborate and share data/resources.

© The Aerospace Corporation (2017)
The Future Is Going to Be Federated!

• **Federation is Fundamental**
  – Resource sharing has been a widely recognized need for decades across many, many application domains
  – Federation is the technology for managing that resource sharing
• Federation will become established technology in the form of Inter-Clouds and general, service-oriented federations
  – Federation can be done at any level in the system stack
  – The only question is when and how
• Limited forms of federation for specific business models/use cases are emerging in the marketplace
  – World-wide computing grids for international “big” science
  – Hybrid clouds – OpenStack “Federate In” and “Federate Out”
  – Web-based commercial services, e.g., MS using PingFederate to provide email
  – Cloud Security Alliance: Software-Defined Perimeter
  – EduRoam: enabling internet access for faculty/students roaming among universities
  – InCommon: provides security services to build educational/research federations
• **Federation will affect how all government systems, commercial systems, and the Internet of Things will be managed.**
Putting This in Context: A Short History of Federation

(Slide sequence from Steve Diamond, Co-chair IEEE Future Directions Committee, Chair IEEE Cloud Computing Standards Committee; NIST Cloud Forum IX Keynote.)

1878: First Commercial Telephone Exchange
New Haven, CT
21 customers $1.50/mo

1961: International Direct Distance Dialing

First Commercial Phone Exchange to IDDD = 83 Years to Federation
Network Carriers Were Initially Isolated but Finally Federated to Become The Internet

Email was Internet “Killer App” in 1980s, but Carriers were Islands

Once Internet standards emerged, the Carriers were able to dominate—and the Internet exploded

Roughly 15-20 years to get to “The”
The Current Cloud Computing Situation: *No InterCloud*

“History doesn’t repeat itself, but it does rhyme.” -- Mark Twain

---

**History Rhymes with Cloud**

“I’m seeing a possibility of inter-cloud problems mirroring the Internet problems we had thirty or forty years ago.”

-- Vint Cerf, Vice President and Chief Internet Evangelist for Google Co-Inventor of TCP/IP, Turing Award, National Medal of Technology, ... SMX Conference, Santa Clara, California, 2009
The Cloud Federation Column Remains to be Authored!

Federation Trends

<table>
<thead>
<tr>
<th>Telephony Federation</th>
<th>Internet Federation</th>
<th>Cloud Federation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Took 100 Years</td>
<td>Took 15-20 Years</td>
<td></td>
</tr>
<tr>
<td>Formal Standard for Protocols (ITU)</td>
<td>Informal Standard for Protocols (IETF)</td>
<td></td>
</tr>
<tr>
<td>No Open Source for any Protocols</td>
<td>Open Source for User Protocols (TCP/IP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No Open Source for Federation Protocols (Routing)</td>
<td></td>
</tr>
<tr>
<td>Peer-to-Peer Federation Model</td>
<td>Peer-to-Peer Federation Model</td>
<td></td>
</tr>
</tbody>
</table>

How long will/should it take?  
What standards and standards adoption are needed?  
P2P federation most likely
This Is Not Just “Cloud” Federation!

Services Can Be Federated at Any Level in the System Stack

Cloud federation is a special case of general service federation
Functionally What Does Federation Require?

The Basic AuthN/Z Process
(IdP = Identity Provider, SP = Service Provider)

The AuthN/Z Challenge in a Distributed Environment

How can User$_A$ find (discover) SP$_B$?
How can SP$_B$ validate User$_A$’s credentials and make access decision?

A Useful, User-Facing Abstraction to Manage Federations: 
*Virtual Organizations from 10000 Feet*

How can separate organizations share data and services?
Create a Virtual Organization:
- A joint security and collaboration context
- Is not “owned” by any one organization
- Members are assigned roles/attributes
- Participating organizations register services
- Managed by a VO Management System
Virtual Organizations from 10000 Feet

Participating sites register their services they wish to make available to this VO.
Virtual Organizations from 10000 Feet

When VO members authenticate, they can access different VO services based on their authorizations.
From the User’s Perspective, They Have One “Pane of Glass” that Gives Them Access to Their Authorized Services from Across Multiple Organizations

Federations and VOs Are Widely Applicable Across Many Application Domains!
International Disaster Response:
Stakeholders will need to collaborate and share data on-demand in response to an unpredictable disaster.
The Internet of Things: The IoT will involve many inherently distributed applications on a potentially global-scale.

My IoT “Things”

Skitter data depicting internet connectivity. CAIDA.org, used by permission.
The KeyVOMS Prototype

KeyVOMS is a third-party, centralized VO management system prototype based on a re-purposed OpenStack Keystone server

KeyVOMS-enabled Browser App
Used to access different VO services based on the user’s VO authz attributes

KeyVOMS Command Line Client -- Used to inspect and manage internal KeyVOMS and VO information

KeyVOMS-enabled Browser App
Used to access different VO services based on the user’s VO authz attributes

KeyVOMS Server

- Auth token with filtered svc catalog
- RSS Feeds
- Map Data
- Files

Services from different providers hosted on various EC2 and PDNS servers made available to myVO

KeyVOMS Prototype

- VO myVO
- ServiceCatalog
- Service Endpoint
- VO PEP
- RSS Feed Servers
- VO PEP
- Map Data Servers
- VO PEP
- VO File Servers

lee@aero.org
The KeyVOMS/ExoAnalytics Federation Demo

- ExoAnalytics is a US-based corporation that operates a global network of terrestrial sensors for tracking resident space objects
- We obtained data sets for three satellites in geosynchronous orbit
  - AM33: Russian TV satellite, 96.5° east (14953 obs)
  - EchoStar17: American internet communications 107.1° west (336921 obs)
  - Luch: Russian Satellite Data Relay Network satellite, 24.4° west (92548 obs)
- Data over 198-day overlapping period
- 55 sensors across 19 sites (36 sensors and 13 sites in CONUS)
The ExoAnalytics/KeyVOMS Demo Scenario

- Two separate “organizations” collect these observations and store them in completely separate clouds:

  - Northern Hemisphere Organization
  - Southern Hemisphere Organization

- They wish to collaborate and share data for specific analysis purposes
- They do so by federating in the **ExoAnalytics Virtual Organization (VO)**
- Members of the ExoAnalytics VO get access to data potentially across both clouds, based on their authorization for specific analysis projects
The ExoAnalytics VO Analysis Projects

• EchoStar17 Analysis Project
  – CONUS sensors only
  – Member: Joe

• AM33 Analysis Project
  – Australian sensors only
  – Member: Fred

• Luch Analysis Project
  – European, South African, and Australian sensors
  – Member: Sally
Example: When Sally authenticates to KeyVOMS, she gets access to all Luch data across all clouds, and can display analyses in the Satellite Orbital Analysis Program (SOAP) using a PySOAP client.

"Center cut" demo data set extracted: 82 observations
When Joe logs into the ExoAnalytics EchoStar17 Analysis project, he only gets to discover and access the EchoStar17 data on the Northern Organization’s cloud. Joe does not know of the Southern Org, nor can he access data.
When Sally logins into the Luch Analysis Project, she gets access to the Luch data from both organizations.

When Sally clicks on the Luch data link in her Service Catalog, she is authorized to access both clouds.
Sally has access to Luch data from two organizations, two clouds, from across three continents.
Sally can download the SOAP orb files into SOAP to do an analysis that would not be possible otherwise. Observations from three sites fixed in inertial space for a satellite in geosynchronous orbit.
All This Is Very Nice…

But What Can I Buy Now?

What Is the State of the Art, er…, Industry?
• Many supporting “piece parts” (standards and tools) exist
• A flexible, dominant, best practice needs to be established
State of the Art/Industry

A Precedent: *Big Science Collaborations/Federations*

- World-Wide Large Hadron Collider Grid (WLCG)
  - *Operationally runs ~200 virtual organizations*
- Trust relationships among multiple national and regional grids managed by the Interoperable Global Trust Federation ([www.igtf.net](http://www.igtf.net))
  - *Enables trust by defining and auditing PKI Certificate Authority operation*
Emerging Support for Hybrid Clouds in OpenStack

- Extending the Keystone API to support simple, manual federation management using two fundamental concepts:
  - **Federate In**: Explicitly specify which external IdPs are trusted
  - **Federate Out**: Explicitly specify which external SPs are trusted
- Enables a user from one cloud to, e.g., instantiate a VM or storage container on another cloud
State of the Art/Industry

An Example of a Commercial, Asymmetric Federation

- The BigSwifty Corporation has outsourced all email to Microsoft
  - *BigSwifty trusts Microsoft to be the email SP*
  - *Microsoft trusts and relies on the BigSwifty IdP*
    - Whenever a BigSwifty employee reads their email, Microsoft validates their credentials with the BigSwifty IdP

- This is a statically managed, asymmetric federation
  - *Only users and IdP on one side, only the SP on the other side*
State of the Art/Industry

Software-Defined Perimeters (SDPs), Cloud Security Alliance

SDP Controller is similar to Third-Party VO Management System, e.g., KeyVOMS

VO Policy Enforcement Points could be thought of as defining a software-defined perimeter

SDPs do not present the same kind of user-friendly, widely known abstraction: the organization

Used by permission, Juanita Koilpillai, Software-Defined Perimeter WG, Cloud Security Alliance
Open your laptop at any participating institution, and your credentials for wifi access are routed to your home institution for validation over a tree of Radius servers.
“The InCommon Federation is the U.S. education and research identity federation, providing a common framework for trusted shared management of access to on-line resources. Through InCommon, Identity Providers can give their users single sign-on convenience and privacy protection, while online Service Providers control access to their protected resources.”
So What Needs to Be Done?

- There is well-established, wide-spread need for flexible, on-demand, standardized, secure collaboration tools, *including federation*
- There are many existing, relevant “piece parts” and systems that address different aspects of general federation management
- *There needs to be some serious integration to identify best practices and promote an emergent dominant practice based on standardized federation tools that get widely deployed*
- This is the typical standards adoption chicken-and-egg problem:
  - *Nobody wants to adopt a standard that is not widely adopted, but standards don’t get widely adopted until people start adopting them!*
- *Some organization with a undeniable need for secure collaboration and federation (and there are many of them) needs to step-up to the plate and demonstrate that integration*
  - *Show vendors what’s needed and what’s possible*
  - *Ignite a new marketplace*
Case in Point: What the Internet Looked Like circa 2015

Skitter data depicting internet connectivity. CAIDA.org, used by permission.
What the “Internet” Looked Like in 1973

36 organizations and 41 machines, if I counted correctly

Wikipedia, in the Public Domain
Four Years Later

ARPANET LOGICAL MAP, MARCH 1977

[Map of ARPANET logical connections with various nodes, links, and labels indicating organizations and machines.]

58 organizations and 136 machines
Summary, Future Work, and Recommendations

• **Major stakeholders in the USG need to step up to the plate**
  – *The Future is Going to be Federated!*
  – *It’s fundamental! Widely applicable to many, many application domains*
    • Collaborations of many kinds, Inter-Clouds, the Internet of Things, …
  – *How much would it take to deploy a prototype federation of ~10 USG organizations?*

• **Talk to your friends in high places!**

• **Goals:**
  – **ENGAGE:**
    • Raise awareness and understanding with our government customers as to what federation is, and why it is critical to future ground systems
    • Engage with academia/industry/consortia/open source projects to promote and develop federation tools and standards
  – **DEMONSTRATE:**
    • KeyVOMS prototype built to demonstrate the concepts and benefits for international disaster response, commercial satellite data, etc.
    • New NIST/IEEE Joint Federated Cloud WG to do the same
  – **BUILD:**
    • Build out prototype tooling (and demo scenarios)
Thank you

All trademarks, service marks, and trade names are the property of their respective owners.