NIST Cloud Computing Program

IEEE P2302

“Standards for Cloud Federation”

Robert Bohn, PhD

Advanced Network Technologies Division

ITL/NIST

Martial Michel, PhD

Data Machines Corp

datamachines

IEEE COMPUTER SOCIETY

STANDARDS ACTIVITIES BOARD
WEBINAR SERIES

16 March 2021

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Today's talk

- Introduction
- The Promise of Federation
- Description of Federation
- NIST/IEEE Collaboration
- NIST Cloud Reference Architecture (NIST SP 500-332)
- IEEE/P2320: Standards for Intercloud Interoperability and Federation
- Current Status
- Applications & APIs

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

Introduction

- NIST defines a *Community Cloud* as supporting organizations that have a common set of interests, e.g., mission, security, policy
- When that community cloud cannot be implemented in one public or private cloud, there is a need to clearly define and implement mechanisms to support the governance and processes *which enable federation and interoperability between different cloud service provider environments* to form a general or mission-specific federated Community Cloud.
- This is the core of *Requirement 5: Frameworks to Support Federated Community Clouds* in the NIST *US Government Cloud Computing Technology Roadmap, NIST SP 500-293 Volume I*

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

The Promise of Federation

- We need to connect real-world collaboration needs (data and resource sharing) with practical collaboration methods and tools
- *Federation* addresses how to securely manage collaborations when the resources being shared are inherently distributed
- There is a spectrum of collaboration needs and approaches

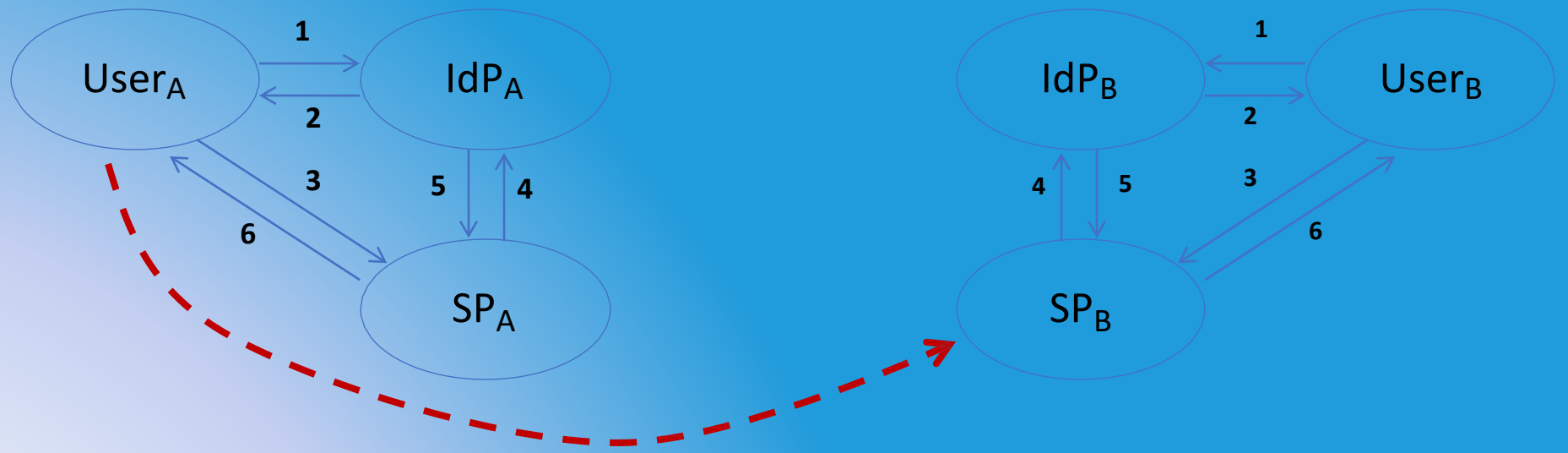
Bare-bones federation:
Small-scale, manually managed

Industrial federation: Large-scale, highly distributed, automated, accounting, auditing, legal

NIST Cloud Computing Program

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The Essence of Federation



How can User$_A$ find (discover) SP$_B$?

How can SP$_B$ manage its discoverability?

How can SP$_B$ validate User$_A$'s credentials and make access decision?

AuthN – Authentication is establishing your identity.
AuthZ – Authorization is establishing your privilege

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST/IEEE Collaboration

- NIST recognized the importance of "Frameworks to support seamless implementation of federated community cloud environments" in USG Cloud Computing Roadmap (NIST SP 500-293).
- Collaboration between NIST and IEEE P2302 will help build consensus on creating an Intercloud - an open, transparent infrastructure amongst cloud providers to support evolving technological and business models and the growing demand for standards that address Intercloud interoperability.
- From the IEEE P2302 Project Authorization Request –
  - **Purpose**: This standard creates an economy amongst cloud providers that is transparent to users and applications, which provides for a dynamic infrastructure that can support evolving business models.
  - **Scope:** This standard defines topology, functions, and governance for cloud-to-cloud interoperability and federation.

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

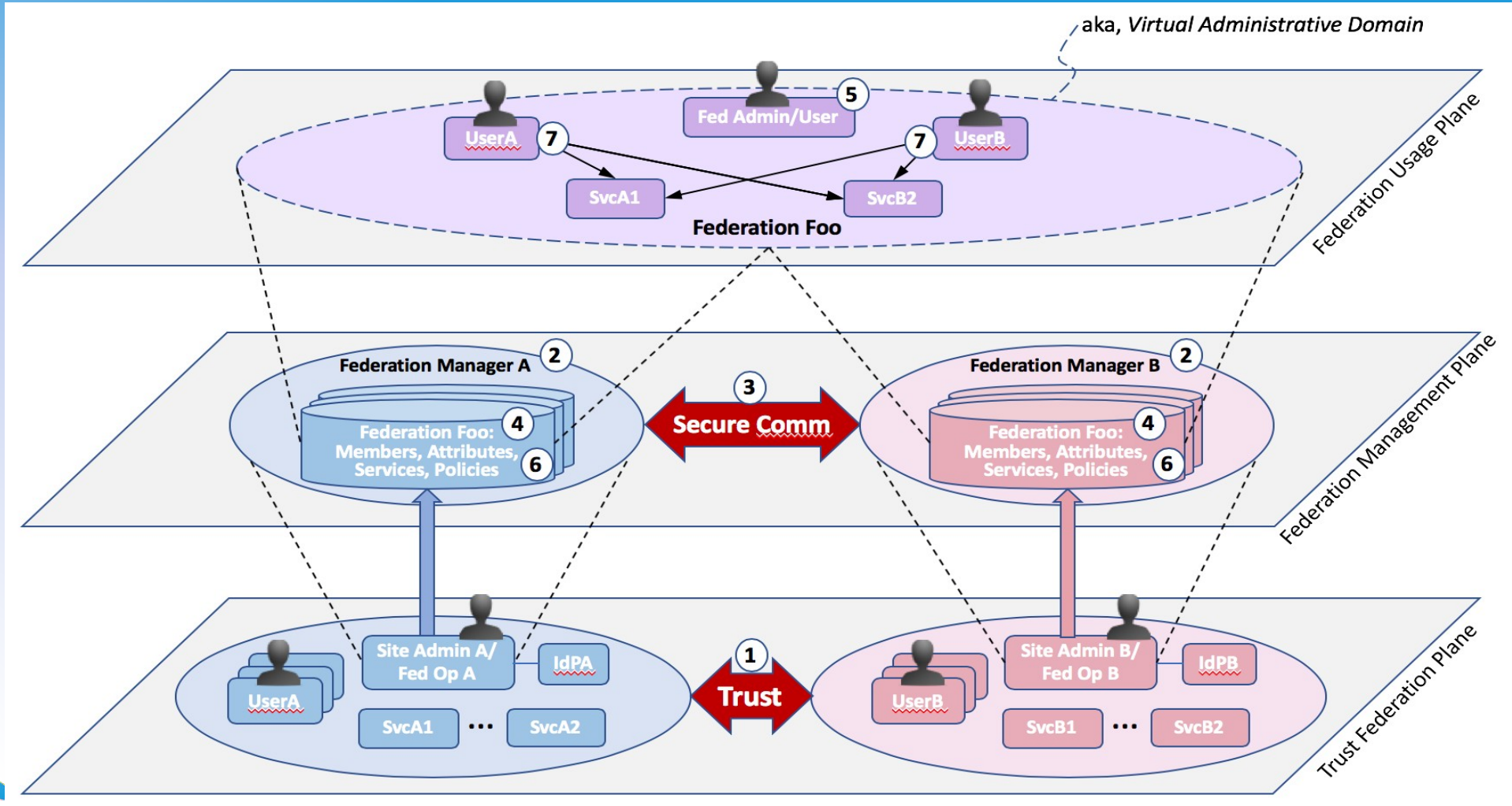
NIST PWGFC/IEEE P2302 Intercloud Goals & Outputs

- The NIST PWGFC will develop a **cloud federation vocabulary and conceptual model** based on the Scope and Purpose.
  - The PWGFC interim outputs will be contributed to the IEEE P2302 Working Group in real-time.
  - The PWGFC ultimate output will be a NIST Special Publication.
- The IEEE P2302 Intercloud Working Group will develop a **cloud federation standard** based on the Scope and Purpose.
  - The PWGFC interim contributions will serve as input.
  - Feedback on PWGFC vocabulary and conceptual architecture contributions will be provided to the PWGFC in real-time.
  - The P2302 initial output will be an IEEE Standard.
  - Plan to contribute the P2302 Standard to ISO/JTC1 to create an International Standard.

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

3-Plane Model of Cloud Federation



NIST Cloud Computing Program

National Institute of Standards and Technology
U.S. Department of Commerce

Essential Characteristics of a Cloud Federation

- A federation is a virtual security and collaboration context that is not necessarily "owned" by any one user or organization.

- Since only specific users, sites, and organizations collaborate for common goals, these participating entities have membership in the federation and identity credentials that are linked to each member.

- Users, sites, and organizations can participate in a federation by choosing to share some of their resources and metadata and making them discoverable and accessible to other federation members.

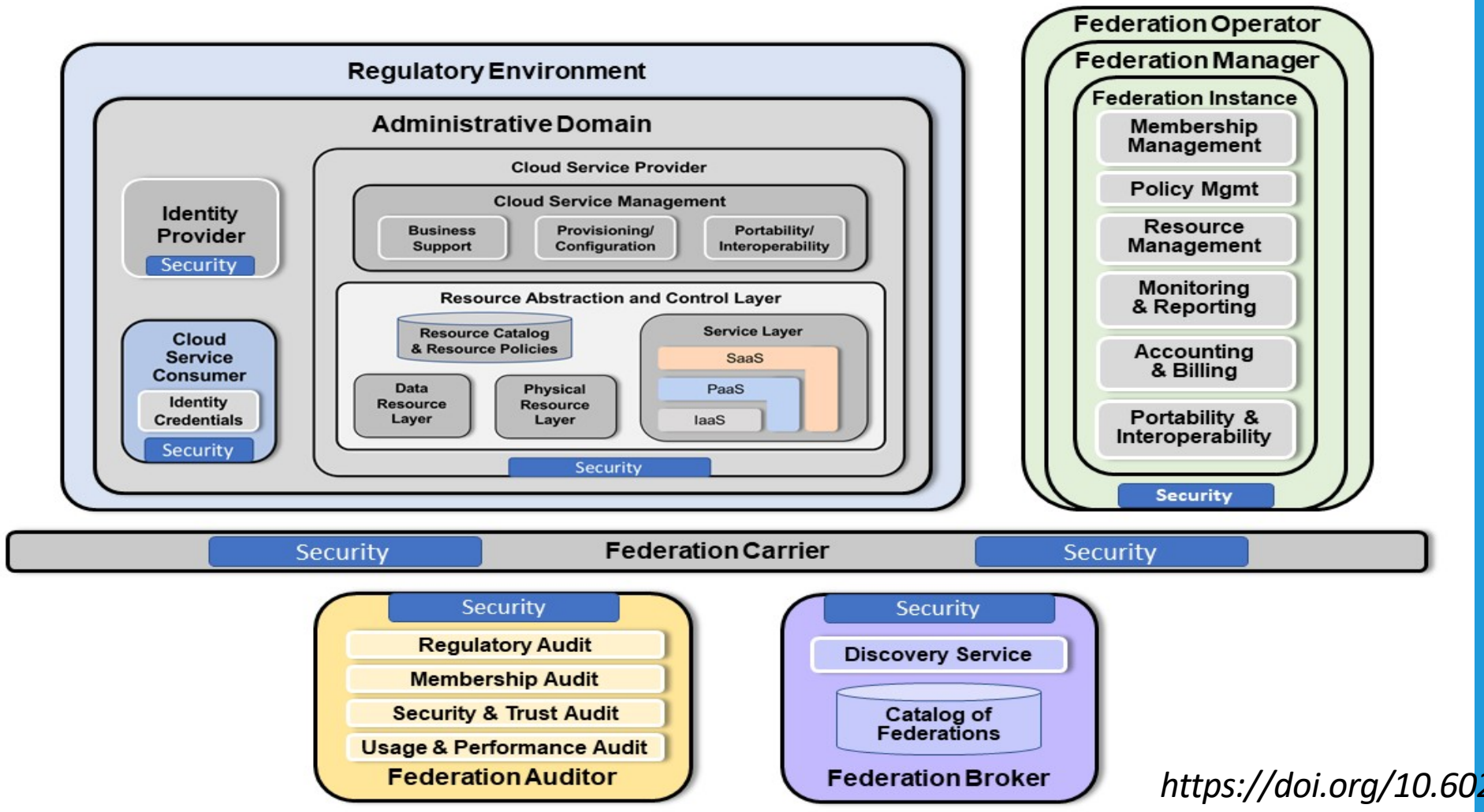
- Participating members agree upon the *common goals* and *governance* of their federation, based on well-known *roles, attributes* and *policies*.

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Cloud Federation Reference Architecture

NIST SP 500-332 (February 2020)



https://doi.org/10.6028/NIST.SP.500-332

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

Relevant Existing Tools and Standards

- *Securing the communication*:
  - SSL/TLS
  - HMAC
- *Identity, Authorization, Policy*
  - Account name and password
  - Public Key Infrastructure (PKI) and PKI Proxy Certs
  - Kerberos
  - Shibboleth
  - Grid Security Infrastructure (GSI)
  - SAML and XACML
  - OpenID, OAuth, and OpenID Connect
  - UMA
- *Catalogs and Discovery*:
  - Lightweight Directory Access Protocol (LDAP)
  - Active Directory and Active Directory Federation Services
  - Web Service API Gateways
  - DNS/DNSSEC
  - OWL-S
- *Trust and Governance:*
  - Blockchain
  - Consensus Algorithms, e.g., Proof-of-Work, Raft, PAXOS

Areas of Possible/Needed Federation-Specific Standards

How FMs interact with Users, Sites, Admins, and other FMs

- FM Admin API
- FM Federation Admin API
- FM-Site Admin API
- FM-User API
- FM-FM API

Possible to define a standard format for describing or defining a specific type of federation instance

- Resources to be shared and their metadata
- Roles & Attributes
- Resource Discovery
- Federation Membership
- Federation Member Identity Credentials
- Authorization to grant or revoke federation membership
- Authorization to grant or revoke member roles or attributes
- Governance, policies, SLAs
- Security considerations

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

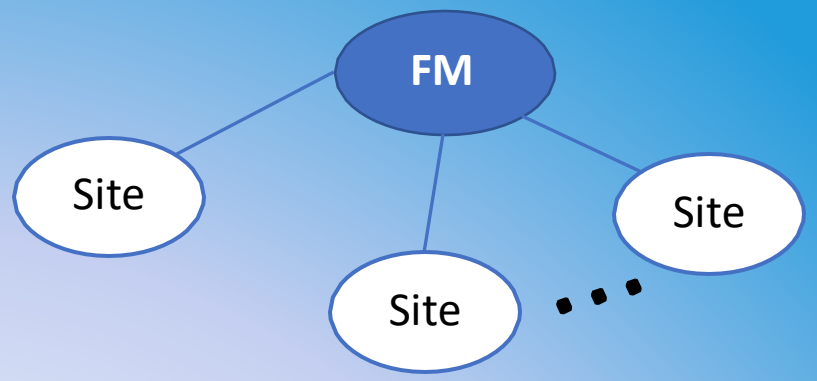
IEEE SIIF Objectives

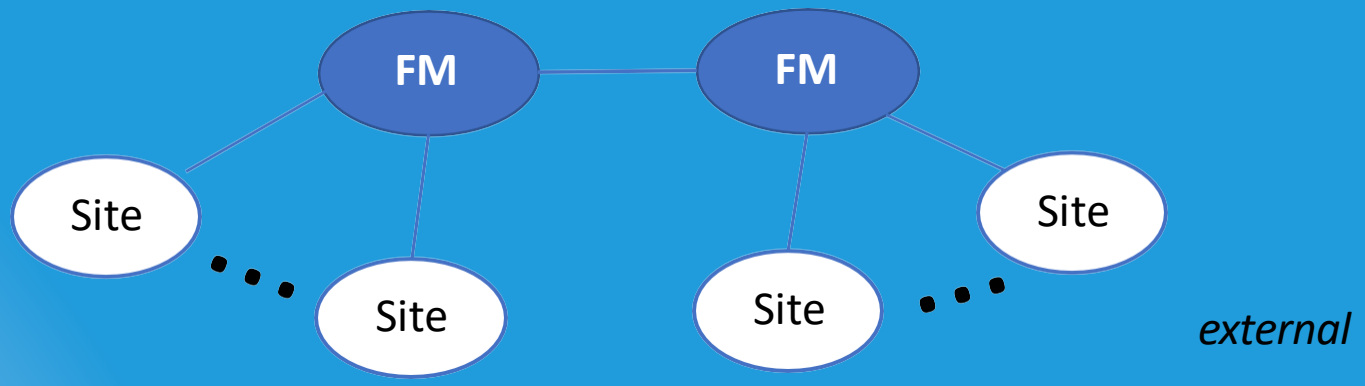
- **Purpose:** *This standard creates an economy amongst cloud providers that is transparent to users and applications, which provides for a dynamic infrastructure that can support evolving business models.*
- **Scope:** *To define topology, functions, and governance for cloud-to-cloud interoperability and federation.*
  - **Support Transparent Infrastructure**
    - Like the Internet
    - Like the Phone Network
  - **Cloud Implementation Independent**
    - Like the Internet Router
    - Like the Phone Network CO Switch
    - Based on Standards
  - **Simple Protocol Set, Easy to Join**
    - Like an ISP, simple IP based protocols enough to get started
    - Supports Regional Governance
  - **Support for Generalized Resource Federation**
    - Not Just VM's – IaaS, PaaS, *aaS
    - Extensibility to Any Describable Resource Type
    - Communities can Add Resource Types
  - **Support for Multiple (Open or Proprietary) Federation Topologies**
    - Network Abstraction
  - **Global Scale Capable**

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

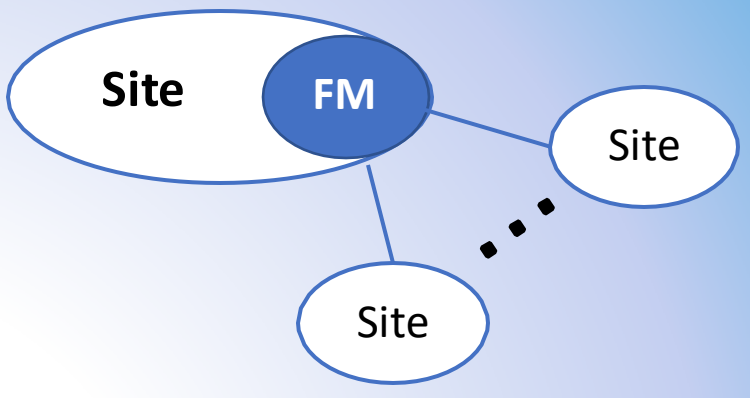
Possible Deployments

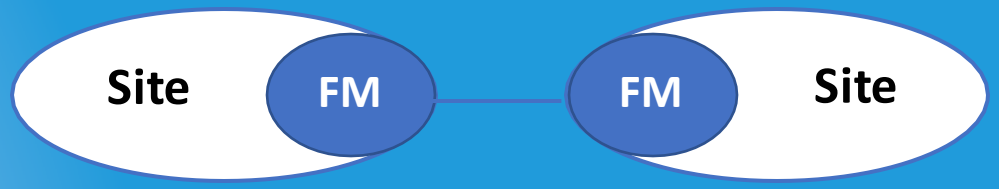




external

internal





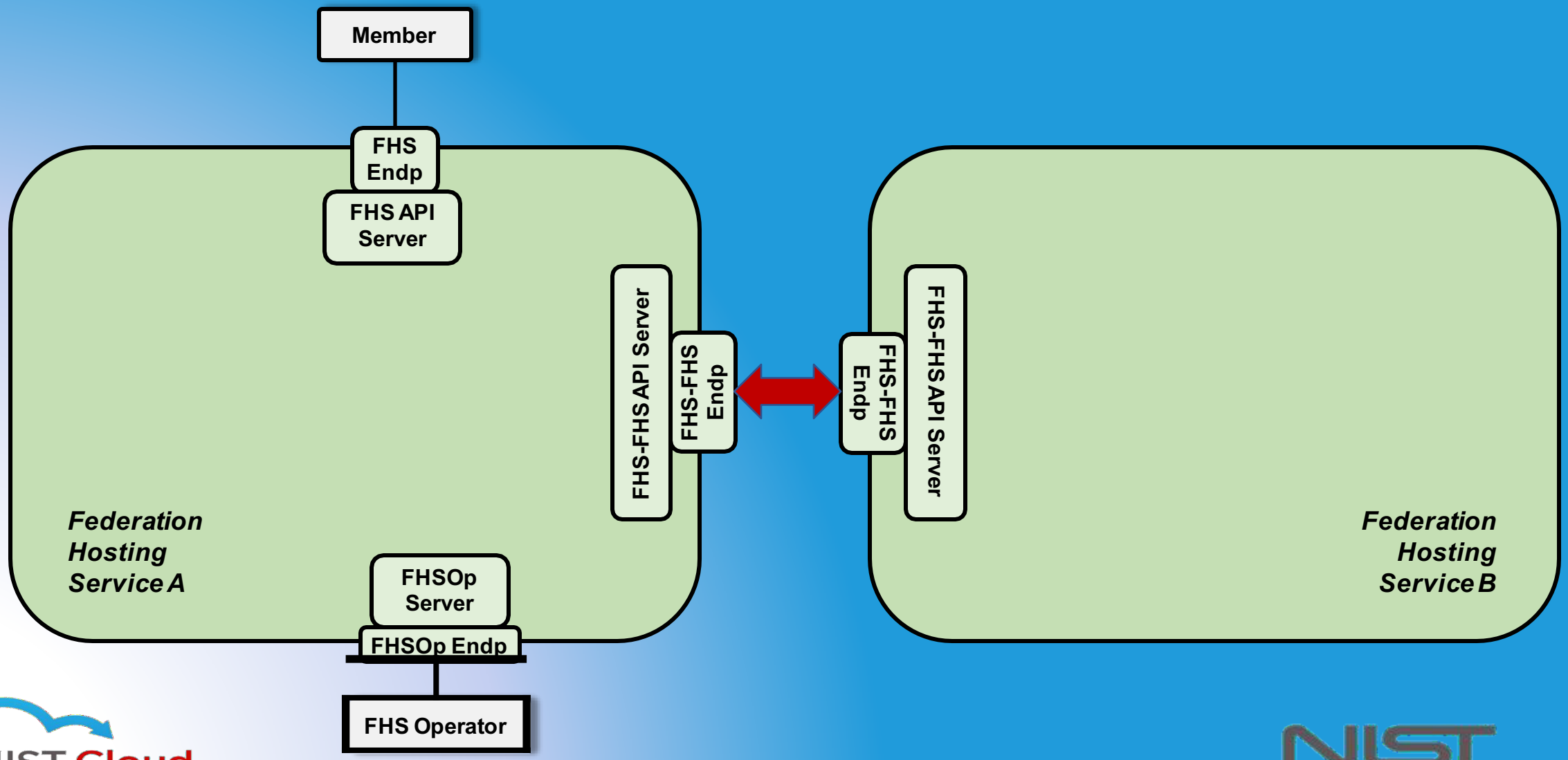
3rd Party Centralized Trust (3PCT)

Peer-to-Peer

NIST Cloud Computing Program

National Institute of Standards and Technology
U.S. Department of Commerce

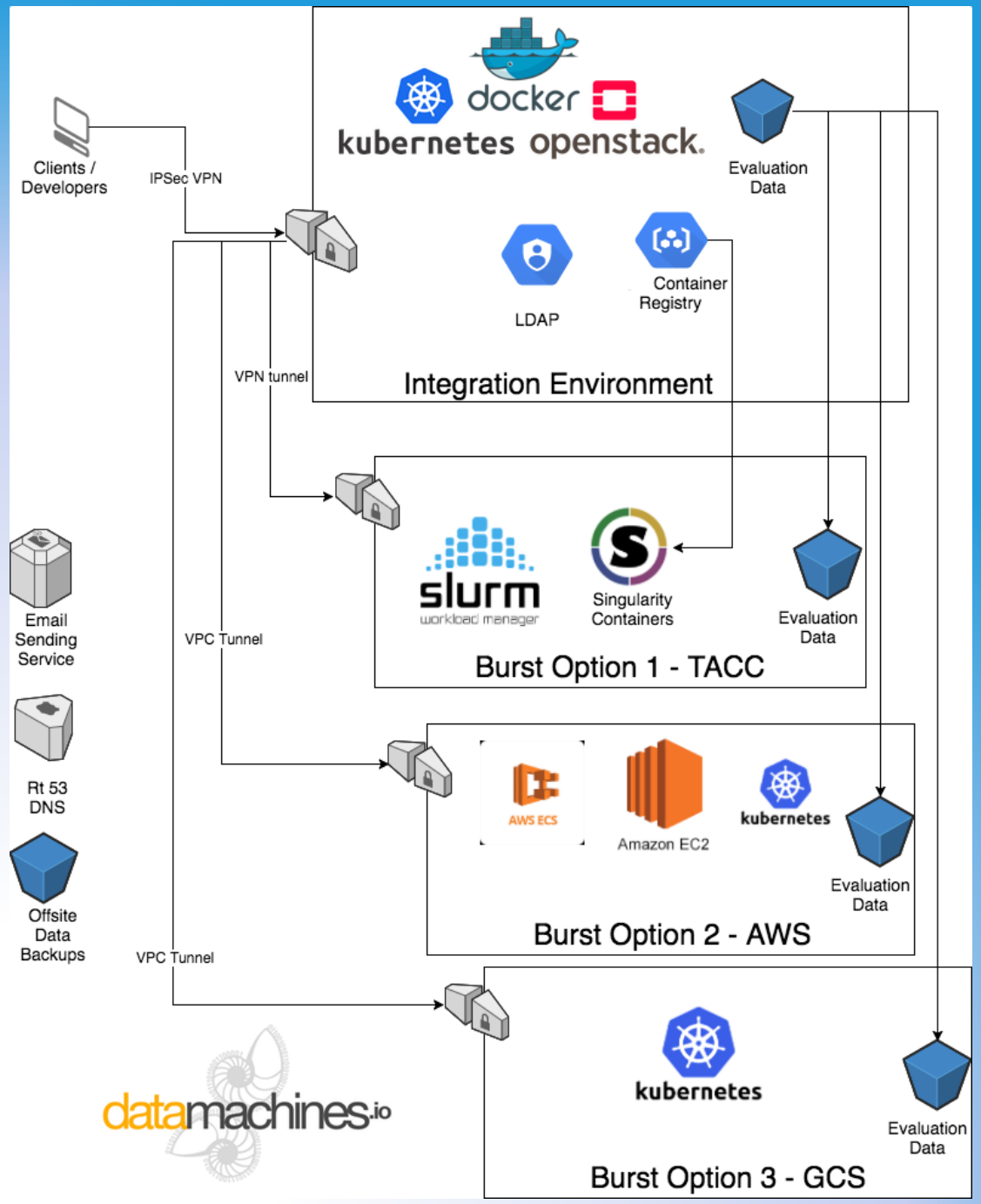
Peer to Peer



NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

Federation Matters: Cloud Bursting



Cloud to Cloud Federation is not yet commonplace

- Identity:
  - LDAP on primary
  - Matches/adapted/ignored on burst clouds
- Data:
  - copied (as needed)
  - through Virtual Private Network/Cloud tunnels
- Compute:
  - Different compute paradigm per cloud
  - migrated/pulled/transformed container images

datamachines

https://www.datamachines.io/blog/federation-matters-introducing-the-nist-cloud-federation-reference-architecture

OpenSource Technology Stacks

Kubernetes Cluster Federation https://github.com/kubernetes-sigs/kubefed
"coordinate the configuration of multiple Kubernetes clusters from a single set of APIs in a hosting cluster [...] intentionally low-level, and intended to be foundational for more complex multicluster use cases"
part of the "Multicluster Special Interest Group" "focused on solving common challenges related to the management of *multiple Kubernetes clusters*"

Federated Keystone https://docs.openstack.org/security-guide/identity/federated-keystone.html
Keystone supports multiple form of Single Sign Ons, and provide Virtual Organization mapping
- Keystone as an Identity Provider (IdP): enables federation between multiple OpenStack
- Keystone as a Service Provider (SP): consuming identity properties issued by external Identity Provider

Technology Stack to Technology Stack Federation is not yet commonplace

- Expected: different abstractions to the OS
- Federation goes beyond Identity

P2302 WG aiming to define a set of APIs that are implementation agnostic

(Draft) Federation Hosting Service Operator (FHSOperator) API

FHSOperator Core
Calls for an FHSOperator to manage a FHS

POST	/FHSOperator	Add a user authorized to create federations
GET	/FHSOperator	List federation owners
GET	/FHSOperator?param1=value1&param2=value2	Query for any kind of server data.
GET	/FHSOperator/{member_id}	Show federation owner details including federations owned.
PUT	/FHSOperator/{member_id}	Change a federation owner's password.
DELETE	/FHSOperator/{member_id}	Delete a federation owner.
DELETE	/FHSOperator/{fed_id}	Delete a federation.

FHSOperator FHS-FHS
Calls to Enable/Manage FHS-FHS Communication.

POST	/FHSOperator/AllowConnection	Allow a connection from another FHS
POST	/FHSOperator/Connect	Request connection to another FHS
GET	/FHSOperator/ListConnections	List FHS Connections
GET	/FHSOperator/ListConnection/{connection_id}	Specific Connection Info
DELETE	/FHSOperator/Disconnect/{connection_id}	Disconnect from another FHS

IEEE P2302

⚠ Work in Progress – Final version may differ

(Draft) FHS to FHS API

Connection
Calls to connect and disconnect FHS.

POST	/Connect	Connect to another FHS.
DELETE	/Disconnect	Disconnect from another FHS.

Federation
Calls to join, manage, and leave a specific Federation Instance.

POST	/JoinFederation	Join a Federation.
PUT	/UpdateFederation	Update a Federation.
GET	/ValidateMember	Validate a Member from another FHS.
DELETE	/LeaveFederation	Leave a Federation.

IEEE P2302

⚠ Work in Progress – Final version may differ

(Draft) Members to FHS API (1/2)

Log In/Out
Log in or out for a specific federation.

POST	/Login	Log into a specific federation instance.
DELETE	/Logout	Log out from a specific federation instance

Federation
Calls to create and manage federation instances.

POST	/Federation	Create a federation instance
GET	/Federation	List federations owned by the caller
GET	/Federation/{fed_id}	Get federation information
DELETE	/Federation/{fed_id}	Delete a federation

Federation FHS-FHS
Calls to join a federation at a different FHS.

GET	/Federation/Query	Get a list of federations known to this FHS at other connected FHS
POST	/Federation/Join/{fed_id}	Request to join a federation known to this FHS but at another connected FHSs
GET	/Federation/JoinRequests	Get a list of federation join requests
POST	/Federation/JoinGrant/{request_id}	Grant a federation join request
DELETE	/Federation/Leave/{fed_id}	Leave a federation that originated at another connected FHSs

(Draft) Members to FHS API (2/2)

Attributes
Calls to manage federation roles and attributes.

POST	/Attribute/{fed_id}	Create an attribute in a federation
GET	/Attribute/{fed_id}	List the attributes in this federation
DELETE	/Attribute/{fed_id}/{attr_id}	Delete an attribute from a federation.

Membership
Calls to manage federation membership.

POST	/Membership/{fed_id}	Grant membership to a federation
GET	/Membership/{fed_id}	List members of a federation
GET	/Membership/{fed_id}/{member_id}	Get specific member info
DELETE	/Membership/{fed_id}/{member_id}	Revoke a member's federation membership.

Authorization
Calls to grant/revoke authorization attributes.

PUT	/Authorization/{fed_id}/{member_id}/{attr_id}	Grant an authorization attribute to a federation member.
DELETE	/Authorization/{fed_id}/{member_id}/{attr_id}	Revoke an authorization attribute from a federation member.

Services
Calls to manage a federation's services.

POST	/Services/{fed_id}	Register a service with a federation
GET	/Services/{fed_id}/{svc_owner_id}	Get list of the svc_ids for my services in this federation
GET	/Services/{fed_id}/{svc_owner_id}/{svc_id}	Get info for a specific service in this federation
PUT	/Services/{fed_id}/{svc_owner_id}/{svc_id}	Update the metadata, discovery policy or access policy for a service in this federation
DELETE	/Services/{fed_id}/{svc_owner_id}/{svc_id}	Delete a specfic service in this federation

Discovery
Query catalog for available services in a federation.

GET	/Discovery/{fed_id}/{member_id}?param1=value1&param2=value2	Look-up services.

Invocation
Calls to invoke services available in a federation.
Any HTTP verb might be possible.

OPTIONS	/Invocation/{fed_id}/{svc_id}	Call a service I am authorized to use.
HEAD	/Invocation/{fed_id}/{svc_id}	Call a service I am authorized to use.
GET	/Invocation/{fed_id}/{svc_id}	Call a service I am authorized to use.
POST	/Invocation/{fed_id}/{svc_id}	Call a service I am authorized to use.
PUT	/Invocation/{fed_id}/{svc_id}	Call a service I am authorized to use.
PATCH	/Invocation/{fed_id}/{svc_id}	Call a service I am authorized to use.
DELETE	/Invocation/{fed_id}/{svc_id}	Call a service I am authorized to use.

IEEE P2302

⚠ Work in Progress – Final version may differ

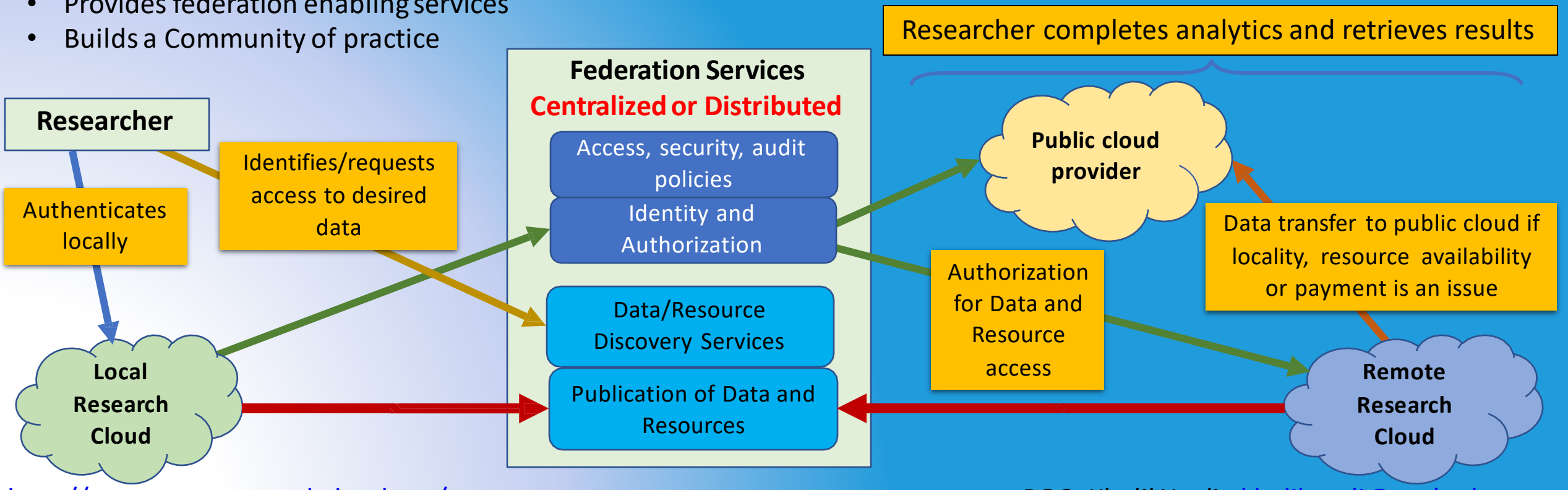
Open Research Cloud Alliance

A global research community partnership to enable access to data, compute and application services across multiple scientific research clouds

- Promotes Researcher Access to Data/Resources
- Provides Testbed Environment
- Clearinghouse/repository for federation tooling
- Promotes Shared ("best") Practices
- Provides federation enabling services
- Builds a Community of practice

Enable federation between and among:

- Academic research clusters
- Scientific research clouds
- Domain specific research and data federation organizations
- Commercial public cloud providers supporting research



http://www.openresearchcloud.org/

POC: Khalil Yazdi <khalilyazdi@outlook.com>

How to Find Information

- IEEE P2302 Intercloud Working Group URL
  - http://sites.ieee.org/sagroups-2302/
- Request to be on IEEE P2302 Intercloud Working Group List
  - STDS-P2302@ieee.org
- Robert Bohn – Chair IEEE/P2302 Robert.Bohn@nist.gov
- Martial Michel – Co-Chair IEEE/P2302, Data Machines Corp, martialmichel@datamachines.io

NIST Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

Thank You

NIST Cloud Computing Program

NIST
National Institute of Standards and Technology
U.S. Department of Commerce