Working Globally at WebScale
Lessons from Leading National Research Networks Deploying Cloud Infrastructure and Platform

Presented by Ben Fineman, Sara Jeanes and Shel Waggener
Agenda

• Todays Technology Landscape
• What is Webscale?
• What is a Cloud Brokerage
• Federating Data using “Platform for Information Sharing”
• Provisional Pilot
• International Efforts
• Q&A and Wrap Up
Technology Landscape: all Mobile & Cloud
Service To Service Integration:
now a Cloud to Cloud Challenge

OF COURSE WE STILL HAVE LOCAL SERVICES TO OPERATE AND INTEGRATE!
It’s an API Economy

The API Economy
Where companies [providers] expose their (internal) digital business assets or services in the form of (Web) APIs to third parties [consumers] with the goal of unlocking additional business value through the creation of new assets.
Beyond APIs you have to standards and compliance …

Most Cloud SaaS will be built for Webscale...

• What is ”Webscale”
• How do you build software for it?
• How do you incorporate into hybrid solution?
• What does that mean for optimizing your apps?
• Will all of Higher Ed be building against the same ”Cloud Stack”?
• Shared Environments will likely ALL be build using Webscale.
• Does it matter which cloud platform or infrastructure your campus chooses?

...NEED TO KNOW YOUR IAAS AND SAAS
https://pen-testing.sans.org/blog/2012/07/05/pen-testing-in-the-cloud
<table>
<thead>
<tr>
<th>Category</th>
<th>Service</th>
<th>Amazon Web Services</th>
<th>Azure</th>
<th>Google Cloud Platform</th>
<th>IBM Bluemix</th>
<th>Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>Virtual Server</td>
<td>Amazon EC2</td>
<td>Azure VM</td>
<td>Compute Engine</td>
<td>Virtual Server</td>
<td>Compute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virtual Machine Scale Sets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute</td>
<td>Bare Metal Server</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>Compute-Bare Metal Cloud Service</td>
</tr>
<tr>
<td>Compute</td>
<td>Container Registration Service</td>
<td>Amazon EC2 Container Registry</td>
<td>Azure Container Registry</td>
<td>Container Registry</td>
<td>IBM Bluemix Container Registry Archives</td>
<td>Oracle Container Registry</td>
</tr>
<tr>
<td>Compute</td>
<td>Container Management Service</td>
<td>Amazon EC2 Container Service</td>
<td>Azure Container Service</td>
<td>Container Engine</td>
<td>IBM Bluemix Container Service</td>
<td>Container</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Azure Container Instances</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute</td>
<td>Micro Services App Development Platform</td>
<td>AWS Lambda</td>
<td>Azure Service Fabric</td>
<td>Google Cloud Functions</td>
<td>OpenWhisk</td>
<td>Oracle Functions</td>
</tr>
<tr>
<td>Compute</td>
<td>Virtual Private Servers</td>
<td>Amazon Lightsail</td>
<td>Azure App Service Environment</td>
<td>Virtual servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Service</td>
<td>Amazon</td>
<td>Azure</td>
<td>Google Cloud Platform</td>
<td>IBM Bluemix</td>
<td>Oracle</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------</td>
<td>--------</td>
<td>---------------</td>
<td>-----------------------</td>
<td>-------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Database</td>
<td>Relational Database Management Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon Aurora</td>
<td></td>
<td>Azure SQL Database</td>
<td>Cloud SQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon RDS</td>
<td></td>
<td>SQL Server Stretch Database</td>
<td>Cloud Spanner</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Azure SQL Server Stretch Database</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Azure CosmosDB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Azure Database for MySQL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Azure Database for PostgresSQL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>Non Relational Database Management Service</td>
<td></td>
<td>Azure CosmosDB</td>
<td>Cloud Datastore</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon DynamoDB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon DynamoDB Accelerator (DAX)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>In-Memory Data Store</td>
<td></td>
<td>Azure RedisCache</td>
<td>Cloud BigTable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon ElastiCache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>Data Warehousing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon Redshift</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Service</td>
<td>Amazon Web Services</td>
<td>Azure</td>
<td>Google Cloud Platform</td>
<td>IBM Bluemix</td>
<td>Oracle</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------</td>
<td>---------------------</td>
<td>-------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>Storage</td>
<td>Object Storage</td>
<td>Amazon S3</td>
<td>Azure Blob Storage</td>
<td>Cloud Storage</td>
<td>Object Storage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Virtual Machine Disk Storage</td>
<td>Amazon EBS</td>
<td>Azure Premium BLOB</td>
<td>Persistent Disk</td>
<td>Block Storage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>File Storage (SMB Compatible)</td>
<td>Amazon EFS</td>
<td>Azure File Storage</td>
<td>File Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Long Term Cold Storage</td>
<td>Amazon Glacier</td>
<td>Azure Cool Storage</td>
<td>Cloud Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hybrid Storage/Storage Gateway</td>
<td>AWS Storage Gateway</td>
<td>Azure Storage Simple</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Service</td>
<td>Amazon</td>
<td>Azure</td>
<td>Google Cloud Platform</td>
<td>IBM Bluemix</td>
<td>Oracle</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td>--------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>Big Data &amp; Advanced Analytics</td>
<td>Data Warehouse</td>
<td>Redshift</td>
<td>SQL Datawarehouse</td>
<td>Big Query</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Big Data Managed Cluster as a</td>
<td>EMR</td>
<td>HDInsight</td>
<td>DataProc</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td></td>
<td></td>
<td>BigInsights for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Apache Hadoop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Streaming Service</td>
<td>Kinesis</td>
<td>Stream</td>
<td>Dataflow</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Analytics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Event Hub</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artificial Intelligence</td>
<td>Machine Learning</td>
<td>Machine</td>
<td>Learning</td>
<td>Cloud DataLab</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Learning Workbench</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Learning Services</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://ilyas-it83.github.io/CloudComparer/

#EDU17
If Everyone is Building For The Cloud....

ARE WE ON OUR OWN?

You Need to Build on the Work of Peers....
The Research Network Exploration Background

• Internet2 NET+ Cloud Program Review 2015 recommended:
  • Assume Cloud is the primary campus deployment model
  • Too many service validations, not enough resources at individual campuses nor at Internet2 to support them all
  • Sponsorship “gate” insufficient to select quality provider.
  • Information sharing: services selection, validation, deployment and ongoing management needed by members

• Initial Concepts led to proposal for “Center for Service Discovery” developed and reviewed with Internet2 Program Advisory Group
Dynamic Expanding Universe of Cloud Services
A Generic Cloud Broker

Cloud Services
- SaaS
- PaaS
- IaaS

Cloud Service Broker

Benefits
- Identity
- Access
- Performance
- Security
- Policy

Service Consumer or Aggregator
- SMB, Enterprise, End-user or Reseller
Growth & Challenge

• Facilitating discovery of needed services?
• Identification of cloud service adoptions within campus departments?
• Ensure service compliance?
• Accelerate deployment once selected?
• Streamline & improve cloud to cloud integration?
• Streamline & improve premise to cloud integration?
• Reduce provider lock-in?

...NEED A SHARED BROKERAGE PLATFORM
Higher Education has solved this before ...

- **eduROAM: Global Mesh Federation of Device Authentication**
  - Started as 2002 higher education community project. Now deployed to 80 countries and doing billions of authentications

- **eduGAIN: Mesh Person Identity Federation of Federations**
  - Started as 2005. Today over 1500 HE identity providers connecting to 40 national federations participate.
The Vision: Global Service Exchange...

- A Mesh Federation – of National Level Service Exchange
- Shared repository (ala GitHub) of API’s and locally bit extensions.
- Service API’s, Standard Attributes, compliance information, and sharable integration metadata.
Collaboration Platform

• Launched as pilot with Internet2 member campuses
• Provides campuses with Cloud Brokerage management framework
• Leverages federated identity (eduGAIN) & opportunity to add eduROAM as second factor for context aware service access
• Eliminates API integration Duplication time/costs
• Supports full provisioning, deprovisioning and capacity management by departments, campuses, systems offices.
Internet2 Cloudmore
Provisional Service:
Campus Cloud Brokerage
Supporting Students, Faculty & Staff

LabArchives
EduRoam
Google Suite
Workday HR
Hazard Mgmt
Effort Reporting
GLOBUS
Google GCP
Service Profile: Student Persona

Personal Technology

Provided Systems

Campus Brokerage

Student

Metadata Driven Visibility

Undeclared
Letters & Science
Big U

EduROAM
Google Suite
Student System
Canvas
LaundryReady
Amazon AWS
Campus Brokerage

Provided Systems

Personal Technology

Faculty

Metadata Driven Visibility

Service Profile: Faculty Persona

English

Letters & Science

Big U

Campus Brokerage

LastPass

EduROAM

Office 365

Workday HR

Canvas

Campus Finance

Amazon AWS

Pearson
Service Profile: Researcher Persona

Personal Technology

Campus Brokerage

Metadata Driven Visibility

Genetics

Medical School

Big U

Provided Systems

LabArchive

EduRoam

Google Suite

Workday HR

Hazard Mgmt

Effort Reporting

GLOBUS

Google GCP
Campus Brokerage  
Provided Systems  
Personal Technology  
Staff  
Service Profile: Staff Persona  
Metadata Driven Visibility  
Campus Brokerage  
Finance  
Medical School  
Hospital  
LastPass  
EduROAM  
Office 365  
Workday HR  
EPIC EMR  
CampusFinance  
Amazon AWS
It’s a Challenging Complex Landscape

But we need to...

THINK BIGGER!

(*and deploy local)
Three PARALLEL Projects

First Projects (Available Now)
• University Service Brokerage: Moving beyond “app store” providing NET+ Cloudmore for your local Campus

Second Project (Proposed in 2018)
• Internet2 Services Hub: Federated Campus Information Registry and Information Exchange

Third Project (Proposed 2019)
• Global Federated Service Registry sharing metadata and service to service integration exchange
Stage One: NET+ Cloudmore Brokerage

Vasser  Florida  Case Western  Boston
Next: National Service Registry and Discovery

Phase Two: Service Discovery

Services Sharing

Member Campus
Vassar
Florida
Case Western
Boston
Member Campus

Affiliated Campus

Affiliated Campus
Last: Federated Service Registries: eduCLICK
Cloudmore
Cloud Brokerage Enablement Platform

Cloudmore is a privately held Swedish company, with subsidiaries in Estonia, the UK and US. We launched in 2005 and today we empower over 6,000 organizations across the world.
“Although cloud service brokerage is an existing market, the reality for an organization of operationalizing cloud brokerage either as a service provider, as an internal IT department or as a distributor remains challenging. “

Source: Cloud Brokerage Enablement
Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
NET+ Cloudmore Campus Cloud Service Brokerage

- Service Catalog
- Internal service discovery
- Add your own products and services
- Contract management
- Price management
- Billing, metering and chargeback
- Billing reconciliation
- Monitoring, reporting and auditing
- Approval processes
- Renewal management
- Governance
- Reporting
Delegated Administration

- Access own e-store
- Contract management
- Subscription management
- Provision users, services and products
- Billing reconciliation
- Charge back
- Reporting
- Approval
- User self service
- Service desk integration
- SSO & Identity integration
Internet2 Service Brokerage

Vision:
Platform for Information Sharing (PIE) created through registration and inter-federation of local, regional, and national cloud service brokerage catalogs for institutional and cross-institutional service collaborations.

Now
• Single Sign On
• Easy on-ramp for services
• Enhanced NET+ Service listings
• Service discovery behind the login
• Cross university commenting
• Peer review and ratings
• FAQ

Future
• More collaboration and comms
NET+ Services Information

Basic Information
- Phase: early Adopter
- Eligibility: Broader Community
- Start Date: 22 Mar 2017

Service Information
- Service Email: Netplus@internet2.edu
- Contact Person: Ben Fineman
- Contact Email: bfineman@internet2.edu

Internet2 Member
- Internet2 Member: No

Comment: Scheduled for Q3 2017

Cloud Security Alliance - Consensus Assessments Initiative Questionnaire
- Yes

Link to document:
- http://internet2.edu/csa

Date Last Updated: 23 Aug 2017
Date Last Reviewed: 29 Aug 2017

Comments:
Service Loading

- Digital sales channel
- Automated sales
- Collect pertinent information at the point of purchase
- Visibility across internal and external customers
- Usage Analytics
- Customer self service
- Improved customer experience
- Simple or complex functionality
- Full service management possible
Full Service Loading – Options

Vendor Integrations
- Use your existing contractual framework
- Low monthly fee to access integration

Semi Automated
- Fast start
- No technical input required
- Full service configuration
- Email provisioning
- Analytics and reporting
- Easy upgrade to fully automated provisioning

Fully Automated
- Full service configuration
- API provisioning
- Analytics and reporting
- Monthly or annual billing frequencies
- Service API fees apply

Custom Integration
- Great for full service management
- Metered or usage based billing
- Large range of options available
- Custom pricing based on requirements

Out of scope for program
Out of scope for program
Security, Compliance and APIs

- Security Center
  - Notify on Admin login
  - Notify on organization admin login
  - 2-factor authentication
  - Activate IP Filtering

- Cloudmore APIs
  - Cloudmore Systems API
  - Outbound Service API
Internet2 Cloudmore Provisional Program

Program:

- Limited cadence of campuses (2/3 month) to join program to evaluate, test deployment scenarios, and service management processes.
- Campus deployments: full product functionality for limited number of Internet2 and campus based services
- Internet2 Hub, complete data loading of Internet2 service data for discovery functionality.
- Activate “Application” Feature for new Providers
- Further tune Cloudmore to the needs of the users by adding new features, required by the cohort, during 2017 and into 2018

Cloudmore aim to become a full production, NET+ Service ASAP
Internet2 Cloudmore Provisional Program

Some limitations...

- All participants in the program are required to agree to the Terms of the Cloudmore Platform Agreement, and associated terms, as in the Cloudmore Privacy, AUP and SLA.
- The NET+ Cloudmore Program does not include the management of students or student services.
- The NET+ Cloudmore Program does not include any bespoke service integrations.
- Unless by special arrangement, the NET+ Cloudmore program is limited to 1000 users.
- The NET+ Cloudmore Program does allow for unlimited organizations and administrators.
Internet2 Cloudmore Provisional Program

Program Support:

• The Program is supported by Cloudmore in the following ways:
  • Platform introduction workshop - 1:1 discovery and awareness workshop.
  • Service loading workshop - 1:1 opportunities for service loading (Internal and External).
  • Monthly progress sync-up - Agile session to drive progress and identify challenges and opportunities.
  • Platform Support issues - In-line logging of bugs/feature and support requests.
  • Agile in-life communications via Slack and Skype
Cloudmore initiatives

Cloudmore Federation
• Campus federation features on Cloudmore roadmap
• Global Registry Data Model Workshop in September in Copenhagen with GEANT

European Initiative
• Proof-of-concepts started with European NRENs, Service providers and universities

Vendor projects
• Projects initiation with major vendors to solve Higher-Ed challenges
Global Efforts
Expert groups and competency centers

Technology
- Legal and security
- Procurement and management

National Cloud Broker
- Portfolio manager
- Service catalogue
- Service 1, Service 2, Service 3
- Catalogue manager

Local cloud broker
- Cloud Broker Working group
- Strategic prioritization Council
- Service 1, Service 2, Service 3

IT resources close to research and education

University of Agder

HE Cloud
The challenge

Make a (group) of services accessible to HE&R in a compliant way, within reasonable time
Method 2: Cloud brokering in European HE&R

Help HE&R institutions to make a (group) of services accessible to HE&R users in a compliant way, within reasonable time.
Cloud brokering: service enrichment processes

Service 1
- Basic check

Service 2
- GDPR
- Basic check

Service 3
- Standard contract supported
- Basic check

Service 4
- SAML2 integration
- GDPR compliance support
- Basic check

Service 5
- framework procurement
Cloud Marketplace Processes

Qualification Process
Is the service interesting?
Is the service providing benefits?
Is there potential demand?

Service portfolio management

Service enrichment factory

Basic validation
- compliance with GÉANT
  - e.g., Peering, eduGAIN
  - Add to catalogue

Technical
- Pricing, discounts
  - Add to catalogue

Commercial
- T&Cs, Contract
  - Add to catalogue

Market Investigation

CSP1
CSP2
CSP3

No
Decision Gate

Yes

FAIL

Add New Service

HE&R
GÉANT
Cloud Catalogue

Communicate to NRENs/Institutions

Maintain Catalogue

Commercial / Reporting

Retire Service
Q&A and wrap up

http://web.cloudmore.com/campus-sign-up