Leveraging Best Practices and Infrastructure to Support Cloud Computing

How Internet2 and other community organizations are supporting the adoption of cloud at a national scale

Sara Jeanes, George Loftus and Sean O’Brien

Internet2

October 2019
Agenda

1. Overview
   a. Who are we?
   b. Why are we here?
2. Managing Your Cloud Journey
   a. Getting Started
   b. Securing and Monitoring
   c. Customizing and Optimizing
3. Next Steps and how to Get or Stay Engaged
Background

Who are we?
Why are we here?
Who are we?

George Loftus
Network Services
gkloftus@internet2.edu

Sara Jeanes
IaaS and PaaS Services and Cloud Architecture
sjeanes@internet2.edu

Sean O’Brien
NET+ Cloud Services Program
sobrien@internet2.edu

#EDU19
Internet2 by the Numbers

470+ Internet2 members

7+ petabytes of traffic on the network every day

100,000+ community anchor institutions

17.6 Tb/s capacity

15,700 miles of dark fiber capacity or 17,500 miles optical fiber infrastructure

100+ countries connected

1,000+ InCommon higher education and research participants

Nx100G+ Layer 2 and Layer 3 speed

60+ Industry Partners

43 Regional Network Partners

61 National research and education network partners

300+ U.S. universities

9 hours—length of time it takes to transfer entire Library of Congress over Internet2 Network

60 Government agencies

#EDU19
Why are we here?

• Internet2's cloud-support initiative supports research and academic collaboration.

• It includes integrated work across the entire Internet2 portfolio, with specific short-term deliverables across the organization.

• Our goals include:
  • Simplify direct access to cloud providers via Advanced R&E Networking Architectures
  • Help ensure secure cloud access, by leveraging R&E community-built trust and identity applications
  • Help researchers pay for cloud infrastructure, through cloud grants & credit applications
  • Leverage community scale and expertise to support cloud service adoption, with cloud services customized to meet R&E standards, through strategic engagement with industry providers
Managing your cloud journey
Key Themes of Internet2 Cloud Enablement

- ACCESS (GETTING STARTED)
- SECURE AND MONITOR (MOVING TO PRODUCTION AND SCALING)
- COMMUNITY OF PRACTICE (CUSTOMIZATION AND OPTIMIZATION)
Getting Started
Cloud Connectivity Goals

Make it easier for researchers to access and use cloud resources in a campus/regional friendly way.

Facilitate data movement using research and education networks in to and out of the cloud.

Facilitate movement between clouds and create alternatives to single commercial vendor lock in.
Networking in the Cloud

Internet2 Peering Exchange (I2PX)

Use of the community’s existing 800 Gbps+ of layer 3 peering capabilities to the major cloud providers for advanced, community enabled access to cloud services.

Cloud Connect

Enabling the Internet2 & Regional infrastructures to offer “direct-connect” private Layer 2 and Layer 3 access to Microsoft, Amazon and Google cloud platforms.
Cloud Connect

- Internet2 Peer Exchange (12PX)
  - Amazon AWS Direct Connect
  - Microsoft Azure
  - Blackboard
  - Desire2Learn
  - Oracle
  - Netflix
  - Dropbox
  - ServiceNow

- Regional Network

- CLOUD CONNECT
  - Google Cloud Platform
  - Google Cloud Dedicated Interconnect
  - Microsoft Azure
  - Microsoft Azure Express Route

- CAMPUS
- LIBRARY
- HOSPITAL
- GOVERNMENT
- K-12
- MUSEUM
- GENERIC

#EDU19
Cloud Services

A university has made significant investments in dedicated network connections to AWS. The university requires resiliency to reach multiple AWS Direct Connect ports and is using Cloud Connect to provide redundancy. The university is also using I2PX to reach SaaS providers that have migrated from the campus data center to the cloud.

- **Cloud Connect** - national resilient footprint for:
  - AWS Direct Connect (Hosted Interconnect >500Mbps)
  - Support for Jumbo Frames
  - Google Dedicated Interconnect
  - Microsoft Azure Express Route

- **Automated Cloud Connect Portal**
  - Provides API-based provisioning at Layer2 and Layer3

- **I2PX** – access to SaaS providers

- **perfSONAR** support for the cloud
Peering Services: Strategic Connections out of Region

A mid-Atlantic regional network had requests from colleges initiating E-Sports programs to provide direct access to a gaming internet exchange in Ashburn, VA. The regional is using the Rapid Private Interconnect (RPI) service to directly access the E-Sport provider’s exchange.

Low cost private interconnections at major peering points
- 10G & 100G **Rapid** (deployment) **Private Interconnect** Ports (RPI)
- Plans for automated deployment capabilities (Cloud Connect Portal)
- Available in packs of 1, 2, or 4 for flexible access to providers of your choice

Lower TCO with ability to use your own ASN at remote peering point
- Shared Router
- Dedicated Router

Access to the Internet2 Peer Exchange I2PX (formerly TR-CPS)
- No capacity limits on the amount of I2PX capacity available to Connectors

Enhanced self-service & telemetry
- Self-configuration & telemetry with services and API’s to drive the network from applications.
Data Egress Waiver/Discount

• Data Egress Fee Waiver/Discount available on AWS, Azure, and Google Cloud Platform
• Reduces charges for data egress destined for a registered institution
• Up to 15% of an payer/billing (read institutionally-managed) account's monthly spend
• Should the institution exceed 15% egress, they will be charged at the standard peering egress or private interconnect egress pricing rate (or in some cases receive a warning).
• For typical usages, compute makes up the vast majority of charges on an account in aggregate, offsetting most or all egress charges.
E-CAS Exploring Clouds to Accelerate Science

NSF Award #190444 under a Cooperative Agreement with Internet2 : $3,030,955; 11/2018-10/2021

A competitive process

- **Phase 1** = Cloud Providers support 6 teams with $100k each of credit to develop & demonstrate computational science at scale.
- A panel of academic reviewers select best 2 in terms of ACCELERATION of SCIENCE and INNOVATION
- **Phase 2** = 2x NSF Awards of $500k + staff + F&A

**Objectives**

- Test effectiveness of commercial cloud for large scale research
- Use accelerated hardware such as FPGA and GPUs
- Explore Cloud AI and Machine Learning frameworks
- Explore cloud provisioning and management of resources.
- Examine performance metrics and identify gaps
NET+ Cloud Services

Developed through a community led Service Evaluation Process
Reviewing services to ensure they meet higher education standards in areas such as functional, technical, security and compliance, business and legal, and other areas of importance.

Backed by a group negotiated Facilitation Agreement
Ensuring standard and differentiated higher education contract terms and conditions, and discounting for qualified institutions.

Supported and Maintained by a Service Advisory Board and Internet2 Program Manager
Convening the community in meaningful ways around cloud services while supporting ongoing management of the service offering.
Goals of NET+ agreements

• Improves risk management by evaluating service providers
• Improves risk management via standard and beneficial contract terms
• Reduces costs of administration
• Reduces price risk by leveraging purchasing power of the community to scale demand
• Providing options as the number of providers in each portfolio services category increases
InCommon: Services and Software

Includes Packaged SSO Software and Trust Registry

Designed For and By the Community

Enables Academic Collaboration AND Enterprise Cloud Access

Plugs into Regional, National, and Global Academic Collaboration and Research Access Environment

THE TRUSTED SINGLE SIGN-ON PLATFORM

1,000 members strong

COLLEGES AND UNIVERSITIES
FUNDING AGENCIES
CORPORATE PARTNERS
COMMUNITIES LEVERAGING INCOMMON
REGIONAL CONSORTIUMS
CLOUD PROVIDERS
NON-PROFIT PARTNERS
RESEARCH PROJECTS
SCHOLARLY COLLABORATIONS

JOIN YOUR PEERS THAT ARE ALREADY PART OF THE INCOMMON COMMUNITY
Identity Management Locally, Nationally and Internationally

Campus IAM

National IAM

International IAM

Seamless wireless connectivity for faculty, staff and student mobility throughout the U.S. and 89 other countries
Securing and Monitoring
InCommon: Trust and Security

A framework for trusted, shared management of access to online resources

- Provides secure, privacy-preserving trust fabric for research and higher education
- Federated identity management for US R&E community (10 million users)
- Offers Certificate service for higher education
Baseline Expectations and BE 2.0

Baseline Expectations Milestone - All Identity Providers Meet the Expectations
Demonstrating our commitment to protecting user privacy and student data

Assessing third-party vendors for security risks and data privacy policies is a crucial responsibility of any higher education institution, and this can be a time-consuming and burdensome task for campus IT professionals. To help ease these challenges, the higher education information security community, EDUCAUSE, Internet2, and the Research & Education Networks Information Sharing & Analysis Center (RENSAC) created the Higher Education Cloud Vendor Assessment Toolkit (HECVAT). Today we’re

<table>
<thead>
<tr>
<th>Software</th>
<th>Code 42</th>
<th>8/08/2018</th>
<th><a href="https://core.42.com">https://core.42.com</a></th>
</tr>
</thead>
</table>
Webinars on Connecting and Securing Cloud

Higher Education Cloud Collaboration Webinars

Created by Sara Jeanes (internet2.edu), last modified on Jul 24, 2019

More Than Just Speeds and Feeds: Architecting Cloud Connectivity for Campus Workloads (July 2019)

Hybrid cloud is a buzz term, but in reality, campuses need stable, high bandwidth connectivity until all campus workloads are cloudy. A highly-connected campus workload needs to communicate between the campus and public clouds for the migration, and in most cases, for significantly longer. These are often legacy or regulated workloads that require an additional level of control.

In this webinar, learn how colleagues at UNC Charlotte are leveraging advanced AWS networking functionality to centrally manage a sprawling cloud environment, by leveraging services like Transit Gateway and VPC Peering to solve their connectivity to the cloud. And, how campuses can create stable, high-bandwidth connectivity between the campus and public clouds with Internet2 NET+ AWS and Cloud Connect.

https://internet2.zoom.us/recording/share/UOua0478RFhNF94N8rewdk7SioTUhlQBlSg2Mjugh8mSwlumekTziMw

AWS Organizations, Control Tower and You: Are you prepared to reach for the Service Control Policy? (May 2019)

With the launch of AWS Organizations for NET+ AWS subscribers, campuses have gained a valuable new tool in managing AWS accounts sprawl on their campus. Deploying AWS Organizations is not as easy as clicking a few buttons, but we are here to help. A lot of thought is involved in deploying a sound framework from which to hang future AWS accounts, and services like network segmentation and authentication services.

Join Internet2, AWS and Indiana University for this session providing an overview of the current AWS Organizations offering for new and existing deployments, functionality now available to NET+ AWS subscribers, and lessons learned implementing organization units, service control policies, centralized management for security, monitoring, and networking. And, how peers are leveraging services like AWS Landing Zones and AWS Control Tower.

https://internet2.zoom.us/recording/share/EvYx3K2gG5v6LQ0O31n9TwanZbKyCmQwh8TrXRS9wWwlumekTziMw

#EDU19
Cloud Cost Management

Google Cloud Platform

Cost breakdown:

- Usage cost
- Sustained use discount
- Spending-based discount
- Subtotal
- Tax
- Total

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost breakdown</th>
<th>Effective ratio</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage cost</td>
<td>View report [1]</td>
<td>100%</td>
<td>$175.76</td>
</tr>
<tr>
<td>Sustained use discount</td>
<td></td>
<td>-25%</td>
<td>$42.69</td>
</tr>
<tr>
<td>Spending-based discount</td>
<td></td>
<td>-30%</td>
<td>$52.78</td>
</tr>
<tr>
<td>Subtotal</td>
<td></td>
<td></td>
<td>$171.79</td>
</tr>
<tr>
<td>Tax</td>
<td></td>
<td></td>
<td>$0.00</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>$171.79</td>
</tr>
</tbody>
</table>

Total credits (discounts & one-time credits) - $171.79

#EDU19
Common Cloud Practices

bit.ly/cloudwiki

---

**Dashboard / Cloud Architecture Home**

**Topic - Standardizing Account Configurations**

Created by Sara James (internet2.edu), last modified on Jul 03, 2018

Once an account has been provisioned, there are a number of configuration items to set before providing the account to its eventual owner. Admin role creation, linking the account with a campus Identity Provider, and enabling logging are just a few of the items. Some of these can be completed programmatically, but others are a strictly manual process. Below are some examples of how the community is tackling this work.

**Tools**

Using Shibboleth for AWS API and CLI access
http://blogs.cornell.edu/cloudification/2016/07/06/using-shibboleth-for-aws-api-and-cli-access/

awsscli-login
A plugin for the AWS command line tool that allows a user to generate temporary credentials via Amazon’s STS using SAML via ECP with support for Duo for authentication. This has the obvious security advantage that a user no longer needs to store long-term credentials on disk.

PyPI: https://pypi.org/project/awsscli-login/
GitHub: https://github.com/datto-llc/awsscli-login

**Examples**

---

#EDU19
Possible Future developments

- Community wide network analytics and tracing
- More self service
- More ‘best practice’ defaults

Community feedback drive what we work on next!
Leveraging Communities of Practice
NET+ Service Evaluation

Assessment of the service for inclusion in the catalogue, applying a consistent process, and determining how best to make it available at scale to the entire higher education community.

SV Group is led by the Sponsoring institution and Internet2 and Includes:

- Service Provider
- Sponsoring University and 5-7 University Participants

SV participants represent

- The research and education community
- Apply a consistent process to assess the service for inclusion in the catalogue
- Determine how to make it available at scale to the entire R&E community
NET+ Service Evaluation

Functional Assessment
- Review features and functionality
- Tune service for research and education community

Technical Integration
- Network: determine optimal connection and optimize service to use the Internet2 R&E network
- Identity: InCommon participation and community identity toolkit support

Security and Compliance
- Security assessments
- FERPA, HIPAA, privacy, data handling
- Accessibility

Business
- Legal: customized agreement using NET+ community contract templates
- Business model
- Define pricing and value proposition

Deployment
- Documentation
- Use cases
- Support model
NET+ Service Advisory Board Model

SV & Subscribing Campuses

Tier 2, 3 Support

Service Provider

Campus Feedback & Requests

Regular Updates in Community Requests

Community Advisory Board

Product Roadmap

Aggregate Community Feedback
Other Community Cloud Resources

• **Higher education cloud collaboration call**
  • Last Wednesday of each month at Noon ET
  • Meeting invite and materials available on the Cloud Wiki

• **Educause Community Groups** - include groups on IT Procurement and Security Management, as well as security, privacy, risk, governance, compliance, and accessibility. [https://www.educause.edu/community](https://www.educause.edu/community)

• **Internet2 Cloud Services Wiki** - includes options to join listservs for specific cloud services
  [https://spaces.at.internet2.edu/pages/viewpage.action?pageId=154764807](https://spaces.at.internet2.edu/pages/viewpage.action?pageId=154764807)
Cloud Architecture Wiki

- Contributions welcome from all participants in InCommon
- Focus on IaaS (Networking, Security, Logging/Monitoring)
**NGI and Internet2: Early Process for Gathering Community Input**

**Exploring the Problem**
- Community discussion began in late 2016
- F2F meetings with community leaders
- Research & Education Community Investment in National-footprint Network Services (RECINNS) released June 2017 [Add link]
- 14+ community leader’s calls to refine the vision and gather expectations

Listen
Define
Ideate
Prototype, Show, Iterate
Deploy

#EDU19
Cloud Networking

- Network automation and cloud networking workshops held annually - sponsored by University of Minnesota, University of Michigan and Internet2
The Community Moves Trust and Identity Forward

Working Group writes final report
Typically includes recommendations and/or implementation guidance, cookbooks, or other artifacts. Sometimes recommend a follow-on working group on the same or related topic.

Working Group Chartered and Scope Defined.
Community members join working group to explore the issue and develop recommendations. May involve information gathering or other community activities.

Problem Definition
Governing or advisory group, or InCommon executive, defines the problem.

https://spaces.at.internet2.edu/display/TI/Trust+and+Identity+Working+Groups+List
Next Steps
How to keep or stay engaged
Leverage Existing Community Resources

- Leverage the Cloud Wiki
- Higher education cloud collaboration call
  - Last Wednesday of each month at Noon ET
  - Co sponsored by EDUCAUSE and Internet2
  - Meeting invite and materials available on the Cloud Wiki
- Join the CCCG Slack channel
  - Specific topical channels, such as networking
  - Specific service channels, like AWS, Box, GCP, etc.
  - Join via the Cloud Wiki

Go to CCCG tomorrow: 10:45-12:15 Wednesday, W187b
Leverage Internet2 Facilitated Cloud Services & Capabilities

<table>
<thead>
<tr>
<th>Community Facilitated Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquia</td>
</tr>
<tr>
<td>CODE42</td>
</tr>
<tr>
<td>Blackboard</td>
</tr>
<tr>
<td>canvas</td>
</tr>
<tr>
<td>Cisco Cloudlock</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Community Delivered Cloud Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADVANCED NETWORKS</td>
</tr>
<tr>
<td>I2PX</td>
</tr>
<tr>
<td>RPI’S</td>
</tr>
<tr>
<td>eduroam</td>
</tr>
<tr>
<td>FILESENDER</td>
</tr>
</tbody>
</table>

#EDU19

http://www.internet2.edu/products-services/
Session Evaluations

There are two ways to access the session and presenter evaluations:

1. In the online agenda, click on the “Evaluate Session” link.

2. From the mobile app, click on the session you want from the schedule > then scroll down or click on the associated resources > and the evaluation will pop up in the list.
Contact Information

Thank you!

Netplus@internet2.edu