NETWORKING FOR CLOUD

INTERNET2

COMMUNITY exchange

May 8-11, 2023
Atlanta, GA
Networking for Cloud

1. INTERNET2 PEER EXCHANGE

Use of the community’s existing 3Tbps of peering capabilities to the major cloud providers for advanced access to cloud SaaS services (e.g. Zoom or Office 365)

2. INTERNET2 CLOUD CONNECT

Enabling the Internet2 and [regional] infrastructure to offer shared “direct-connect” private Layer 2 and Layer 3 access to Microsoft, Amazon and Google cloud platforms up to 5Gbps at no additional fee (*Cloud provider fees apply*)

3. INTERNET2 RAPID PRIVATE INTERCONNECT

Private 10G interconnections at major peering points at low annual rates. Leverages current investment in local and national infrastructure to reach cloud providers, for dedicated access or improved resiliency. May be used to connect to any provider located at the peering point
CEN members can use Cloud Connect for up to 5Gbps connections to Amazon Direct Connect, Google Cloud Partner Interconnect, Microsoft Azure Express Route or Oracle Fast Connect services.

Available to CEN members today at no additional fee.
While We Were Busy with NGI it Got Very Cloudy

- Over 171 Higher Ed Members Subscribed to Cloud Connect

- Over 350-400 Connections have been created,
  - 143 Created by Regional Members
  - 122 Created by Members
  - 135 Created by Affiliate Members

- Over 24 Regionals (56%) provided Cloud Connect support to their members

- Internet2 is providing over 1Tbps of Cloud Connect capacity in 4 locations
Network Performance: Expectations and Optimization

Karl Newell
Network Software Architect, Infrastructure Systems & Software
Internet2 Network Services
knewell@internet2.edu
Who remembers the Science DMZ?

- A network architecture explicitly designed for high-performance applications, where the science network is distinct from the general-purpose network
- The use of dedicated systems for data transfer
- Performance measurement and network testing systems that are regularly used to characterize the network and are available for troubleshooting
- Security policies and enforcement mechanisms that are tailored for high performance science environments
What’s old(ish) is new again

- **Cloud is driving Wide Area Network (WAN) utilization**
  - Cloud Connect (AWS Direct Connect, Azure ExpressRoute, GCP Cloud Interconnect)
- **WAN latency has implications for TCP performance**
  - Latency > 10 ms
  - Packet loss impact is proportional to latency
  - TCP window (buffer) sizing
    - $35 \text{ ms @ 10Gbps} = 43.75 \text{ MB buffer}$
- **Applications and protocol behavior matter**
  - SSH (SCP, rsync) has a 2MB buffer (457 Mbps max throughput at 35 ms latency)
  - TCP
    - Multi-stream
    - Packet/stream pacing
Throughput vs. increasing latency on a 10Gb/s link with **0.0046% packet loss**

**Throughput (Mbps/sec)**

- **Local (LAN)**
- **Metro Area**
- **Regional**
- **Continental**
- **International**

**Round Trip Time (milliseconds)**

- **Measured (TCP Reno)**
- **Measured (HTCP)**
- **Theoretical (TCP Reno)**
- **Measured (no loss)**

**INTERNET2 2023 COMMUNITY EXCHANGE**
What’s new?

- Cloud connect circuits might be sub-10G (bandwidth == $$$)
  - If sending host is 10G and trying to maximize throughput, shapers may eventually lead to packet drops
    - Need packet/stream pacing
- New generation of Cloud Architects
  - Might not have experience with WAN network performance
  - Need to integrate and work closely with Network Engineering/Architecture
What’s different?

- Applications
- Need to deal with enterprise firewalls
- Might need to deal with cloud firewalls
- Need to understand performance in the cloud
What’s next?

- Engage with the community
  - Develop documentation and training materials
  - Develop reference architecture

- Determine cloud performance
  - Compute types, NICs, optimization
  - Storage
  - Security groups
  - Network firewalls

- On-demand perfSONAR nodes in Virtual Networks (TBD)
Case Study
Case Study

- Insert perfSONAR containers at Router A & Z
Case Study

- Routing fixes (asymmetric traffic via commercial Internet)
- MTU - full path at jumbo frames (9000 bytes)
- Host tuning - TCP window sizing
Benefits of Automation Efforts

Karl Newell
Network Software Architect, Infrastructure Systems & Software
Internet2 Network Services
knewell@internet2.edu
Benefits to Internet2

- Configuration consistency
  - Reduced issues due to manual configuration mistakes
- Simpler and faster provisioning of services
  - Cookie cutter provisioning
  - 8x config compression
    - 30,000 lines of NSO configuration results in 240,000 lines of network configuration
- NGI service migration
  - Migrated 1,200 BGP peers in 30 days
  - 250 peers in one night
- Out of band changes promote architecture review
Benefits to the community

- Reduced issues due to configuration mistakes
- Rapid provisioning of services
- Enables future provisioning of more services via Insight Console
Expanding automation efforts in the community

- NTAC Network Automation SIG
  - Kudos to Frank Seesink (UNC Chapel Hill) and Shannon Byrnes (Internet2)
- Provide guidance to help organizations get started and keep going
  - Executive support for automation
  - Cross-team buy-in
  - Integration of network engineering and software development teams
  - Iterate
    - Don’t boil the ocean
    - Don’t be afraid to start over
REACH

- **Research & Education Automation Clearing House**
  - MANRS for network automation
- Developing prescriptive practices to help the community get started with and continue their automation efforts
- Internet2, ESnet, CENIC, University of Michigan, IU GlobalNOC
- Watch for blog posts and more announcements
Q & A

INTERNET2
2023 COMMUNITY exchange
May 8-11, 2023 Atlanta, GA
The Internet2 Insight Console: Visualize, Manage, Troubleshoot

<table>
<thead>
<tr>
<th>Mike Simpson</th>
<th>Christopher Green</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director, Infrastructure Systems &amp; Software</td>
<td>User Experience Architect</td>
</tr>
<tr>
<td>Internet2 Network Services</td>
<td>Internet2 Network Services</td>
</tr>
<tr>
<td><a href="mailto:msimpson@internet2.edu">msimpson@internet2.edu</a></td>
<td><a href="mailto:cgreen@internet2.edu">cgreen@internet2.edu</a></td>
</tr>
<tr>
<td>520.314.3899</td>
<td></td>
</tr>
</tbody>
</table>
Overview

- What is the Insight Console?
- A high-level overview of the Insight Console’s architecture.
- How we handle identity and access management in the Insight Console.
- What can the Insight Console do right now?
- What will the Insight Console do next?
- How do we get it right?
- Time for Q&A.
The Premise

What is the Insight Console?
The Premise

The *I2 Insight Console* is:

- a web-based tool for **visualizing**, **managing**, & **troubleshooting**
  all Internet2 *network services*. 
The Stack

A high-level overview of the Insight Console’s architecture.
Core Architecture

- **Infrastructure under management:**
  - **Optical:** Ciena 6500s and Waveserver 5s
  - **Packet:** Cisco 820x, Juniper EX4600, Arista 7280R3
  - Other device types can be added in the future.

- **Configuration management applications:**
  - **Optical:** Ciena Manage, Control, & Plan (MCP)
  - **Packet:** Cisco Network Services Orchestrator (NSO)
  - **Source of Intent:** Netbox/Nautobot
  - **Reconciliation:** I2NS Reconciler
  - Other applications can be added in the future.

- **Middleware API microservices:**
  - **Sessions:** authentication, attribution, authorization
  - **Looking Glass:** replacement for Router Proxy
  - **Community:** organizations, people
  - **Interfaces:** locations, devices, interfaces
  - **Virtual Networks:** replacement for OESS/CC
  - **Routing Integrity (planned):** prefix management et al.
  - **Service Desk (planned):** service requests
  - Other microservices can be added in the future.

- **CLI and GUI tools and interfaces:**
  - **I2 Insight Console:** Central landing page and convenient access to all Internet2 network services.
  - Other tools can be added in the future.
Extended Architecture

- **Business services:**
  - Provide organizational, contractual, or billing information.
  - Includes Salesforce, LinkSquares, et al.

- **Document service:**
  - Provides a single point of documentation for all Internet2 Network Services-related service documentation.
  - Provides an API for search and retrieval to allow embedding specific documentation at point of need.

- **Federated identity and access management services:**
  - Externalizes credentialing, affiliation, and attribution.
  - Services provided by Internet2’s Trust & Identity division.

- **Telemetry services:**
  - Provide visibility into traffic analysis, interface monitoring, etc.
  - Services provided by GlobalNOC’s telemetry stack.

- **Ticketing and tracking services:**
  - Provides service request and other workflow management.
  - Includes monday.com as our initial target integration.

- **Logging, analysis, and reporting:**
  - Central aggregation point for system and audit event logging.
  - Current focus on Splunk and/or New Relic.
(An Aside)

How we handle identity & access management in the Insight Console.
InCommon Integration

- Technically, integration with the Internet2 Identity Services platform.

- **Authentication:**
  - Via a **home identity provider**, using familiar SSO credentials.
  - Alternatively, via an **Internet2 Guest Account**.
    - Note that if you’re interested in getting into the business of running an identity provider, Internet2 has identified several InCommon Catalysts to help you get started.

- **Identity:**
  - Authentication links you to your **Internet2 identity**.
    - msimpson @ Internet2 -> mike.simpson@at.internet2.edu
    - aadams @ UA -> alice.adams@at.internet2.edu

- **Affiliation:**
  - Identity is associated with **organizational affiliations**:
    - “Mike Simpson is an **administrator** at Internet2.”
    - “Alice Adams is an **operator** at the University of Arizona.”

- **Policy and Authorization:**
  - Affiliations intersect with **policy configuration** to determine **authorizations** for specific functions in the I2 NS API:
    - “Administrators may **assign people to roles** at their organization, and **edit organizational details.”
    - “Operators may **view BGP peering session information** associated with their organization.”
The Present

What can the Insight Console do right now?
The Present

- Looking Glass
- Community
- Docs
The Future

What will the Insight Console do next?
The Future

- Interfaces
- OESS → Virtual Networks
- API Access

---

- Dashboard
- Routing Integrity
- Service Desk

---

- DDoS
- Wave & Spectrum
- Infrastructure as Code (IaC)
- Multi-domain visualization & telemetry
The Context

How do we get it right?
The Context

**User Research**

**Groups & Committees**

**Five Year Plan**

**Design**

**Usability Testing**

**Dev**

**Ops**

**Feedback & Analytics**

User Centered Design (UCD)