
INTERNET2
TECH ex 23
WHEN LIGHTNING TALKS STRIKE
NAVIGATING STORM CLOUDS
Technology Exchange 2023

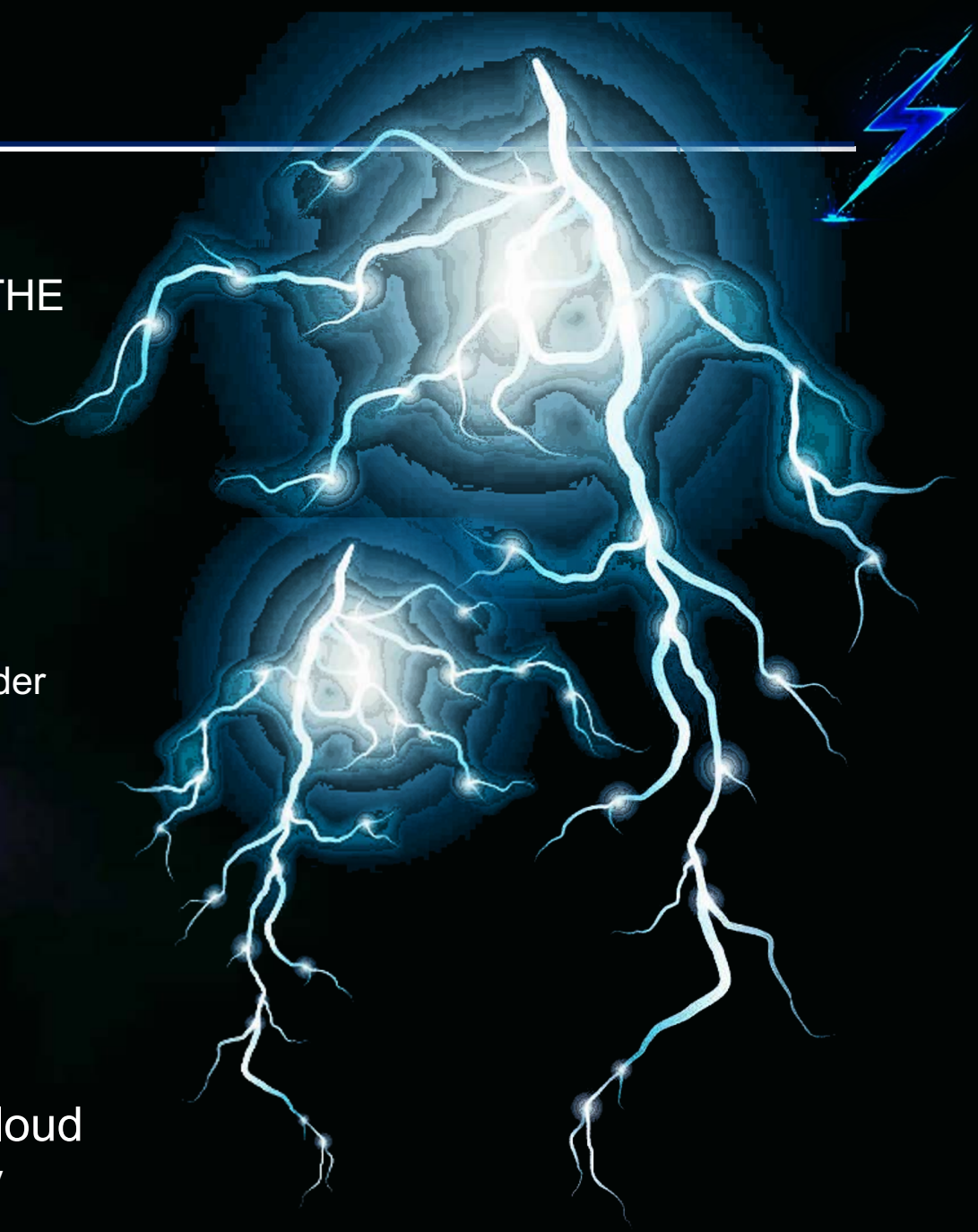
Lightning Round Rules

10 Minutes – Strictly Enforced

Countdown Notifications at 3 and 1 min remaining

Questions are not allowed during presentations, please save them for the end

Click to add the title text



NETWORKING WAYS TO *FAIL* IN THE CLOUD
Scott Taylor, Internet2

SECURITY CONSCIOUS CLOUD ENABLEMENT
Chris Horen, University of Colorado Boulder

IAM IN THE CLOUD
Ananya Ravipati, Internet2

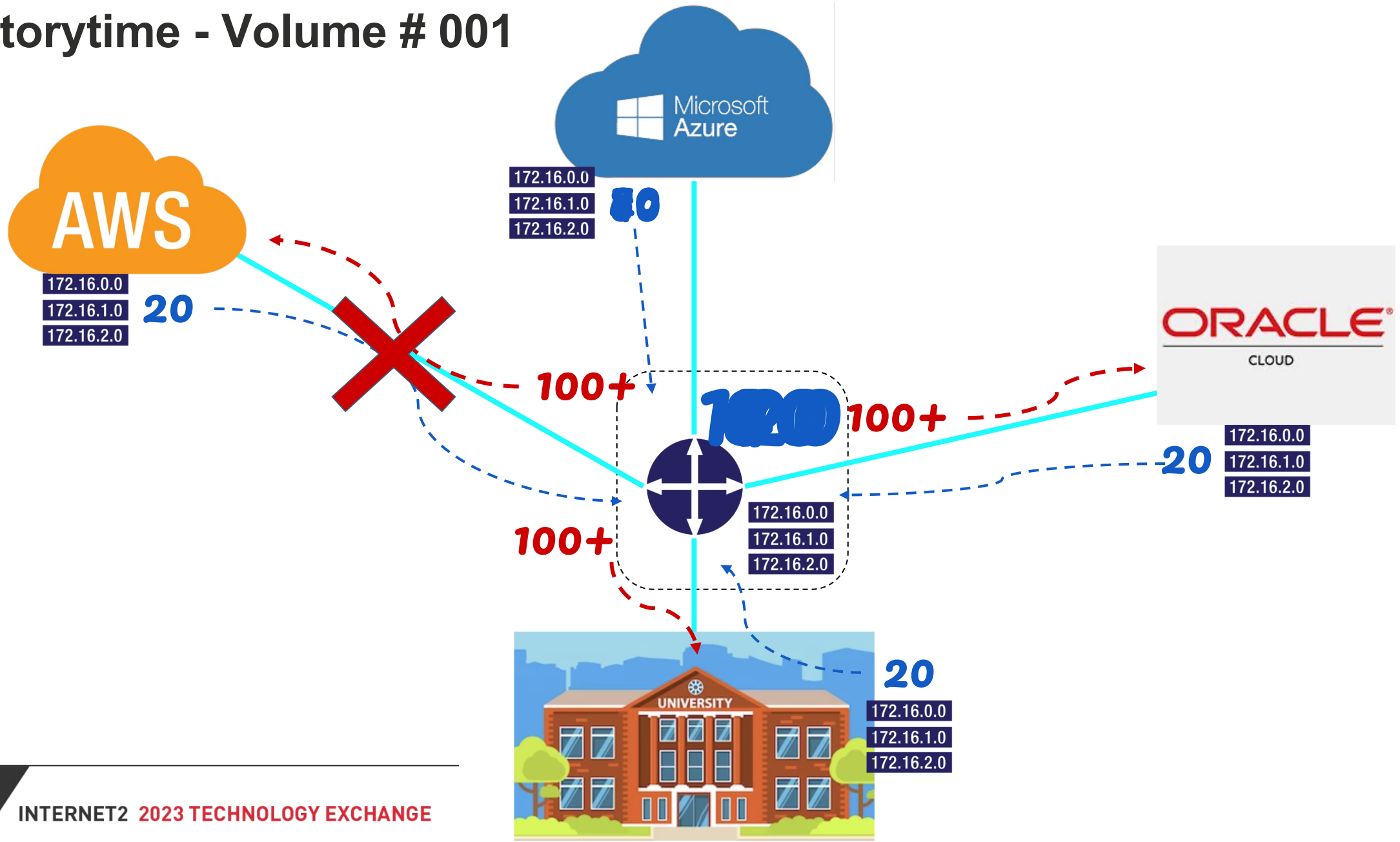
DIRECTIONS TO THE CLOUD
Supporting Research in Public Cloud
Dan Landerman, Northwestern University


PART ONE
NETWORKING WAYS TO FAIL IN THE CLOUD
Scott Taylor
Internet2

NETWORKING WAYS TO *FAIL* IN THE CLOUD

Scott Taylor | Internet2

Storytime - Volume # 001



Know your CSP prefix limits

AWS Direct Connect
Private peering: Accepts up to 100 prefixes each for IPv4 and IPv6
Public peering: Accepts up to 1000 prefixes
BGP state goes to idle (BGP peering goes down)

Azure Express Route
Private peering: Accepts up to 4000 prefixes[1]
Public peering: Accepts up to 200 prefixes
BGP session is dropped

Oracle FastConnect
Public peering: Accepts up to 200 prefixes
Private peering: Accepts up to 2000 prefixes
BGP session brought down[2]

Google Cloud Interconnect/Cloud Router
Less straightforward, no published limits on Interconnect; limits exist on Cloud Router[3]
Important number to keep in mind is 250 prefixes
BGP does not go down instead uses deterministic route dropping behavior

Common causes

- Poor planning
- Accidental routing change
- Creep over time

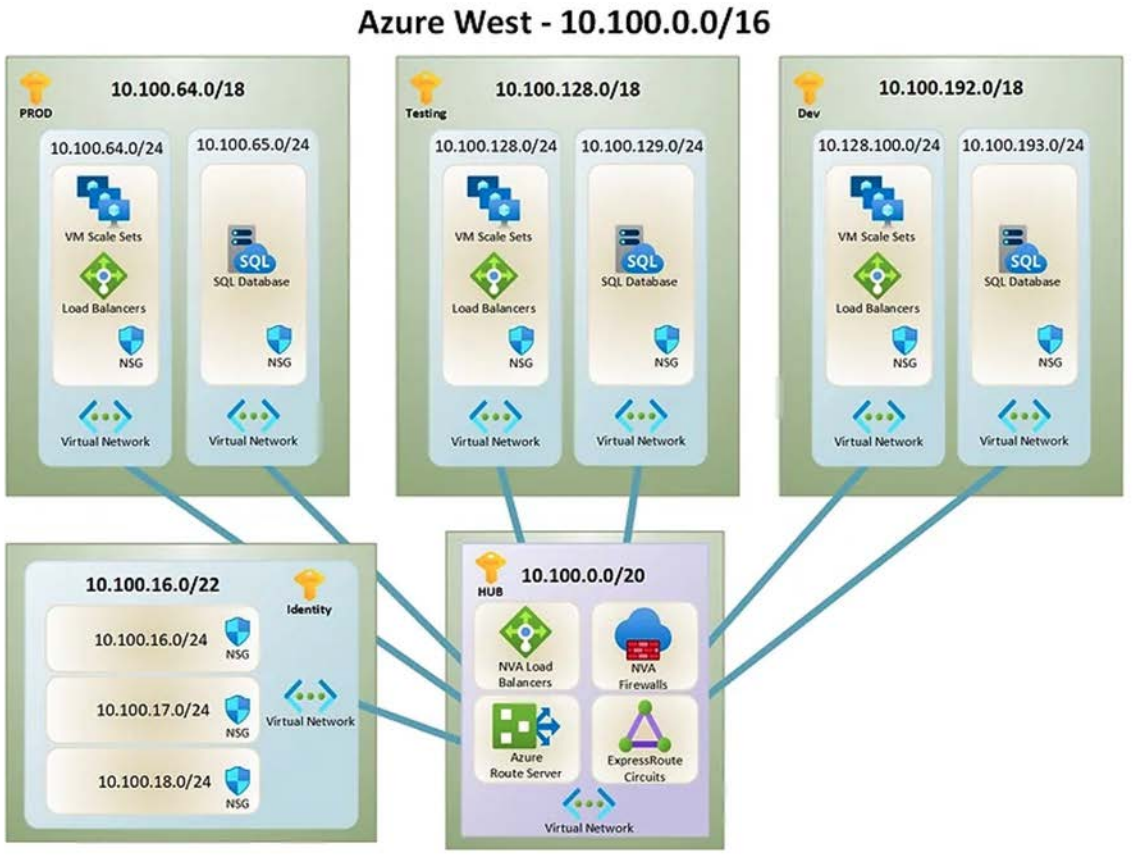
  (*maybe not completely poor planning*)
- New subnets/connections
- Workarounds

Creating layered protection

- ✓ **Planning**
  - Can you aggregate addresses?
  - Does every subnet need to be accessible?
- ✓ **Redundancy**
  - Multiple connectivity strategies (Dedicated + VPN backup; multi region)
- ✓ **Filtering**
  - Use “allow” prefix-lists with routing tables to protect from accidental advertisements
- ✓ **Monitoring**
  - Know how many prefixes are in your routing table
- ✓ **Alerting**
  - Set threshold to alert ops before you hit the limit

IP Address Planning

- Plan for expansion
- Reserve space to grow
- Plan for multiple regions
- Plan for multiple Clouds
- Do *NOT* overlap addressing!
- Plan for future cloud architectures
- Don’t forget IPv6!



Identity-West-Vnet - 10.100.16.0/22

1. Production-DC-Subnet 10.100.16.0/24
2. Testing-DC-Subnet 10.100.17.0/24
3. Dev-DC-Subnet 10.100.18.0/24

Identity-East-Vnet - 10.200.16.0/22

1. Production-DC-Subnet 10.200.16.0/24
2. Testing-DC-Subnet 10.200.17.0/24
3. Dev-DC-Subnet 10.200.18.0/24

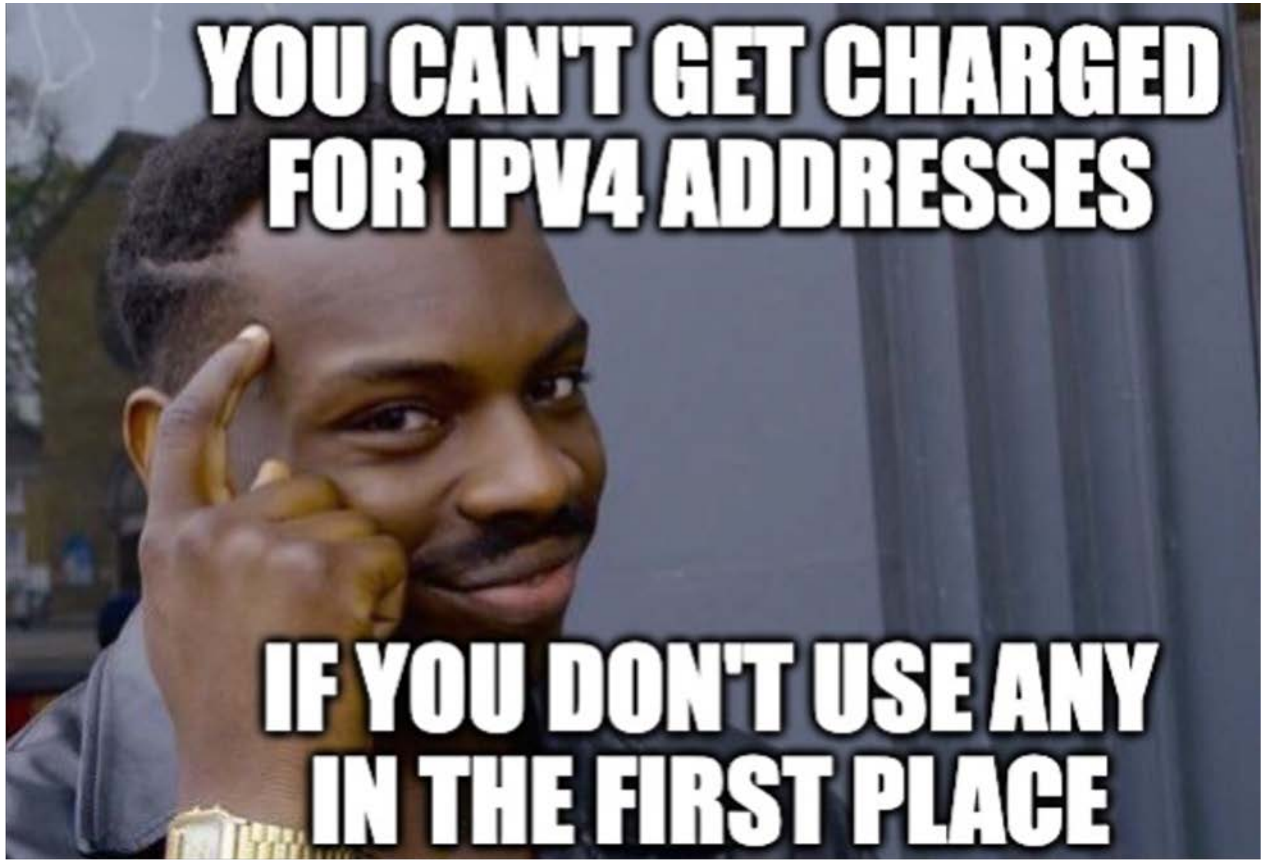
Quick PSA

AWS to start charging for all IPv4 addresses[1]

IPv4 hourly charge:
$0.005 / address / hour

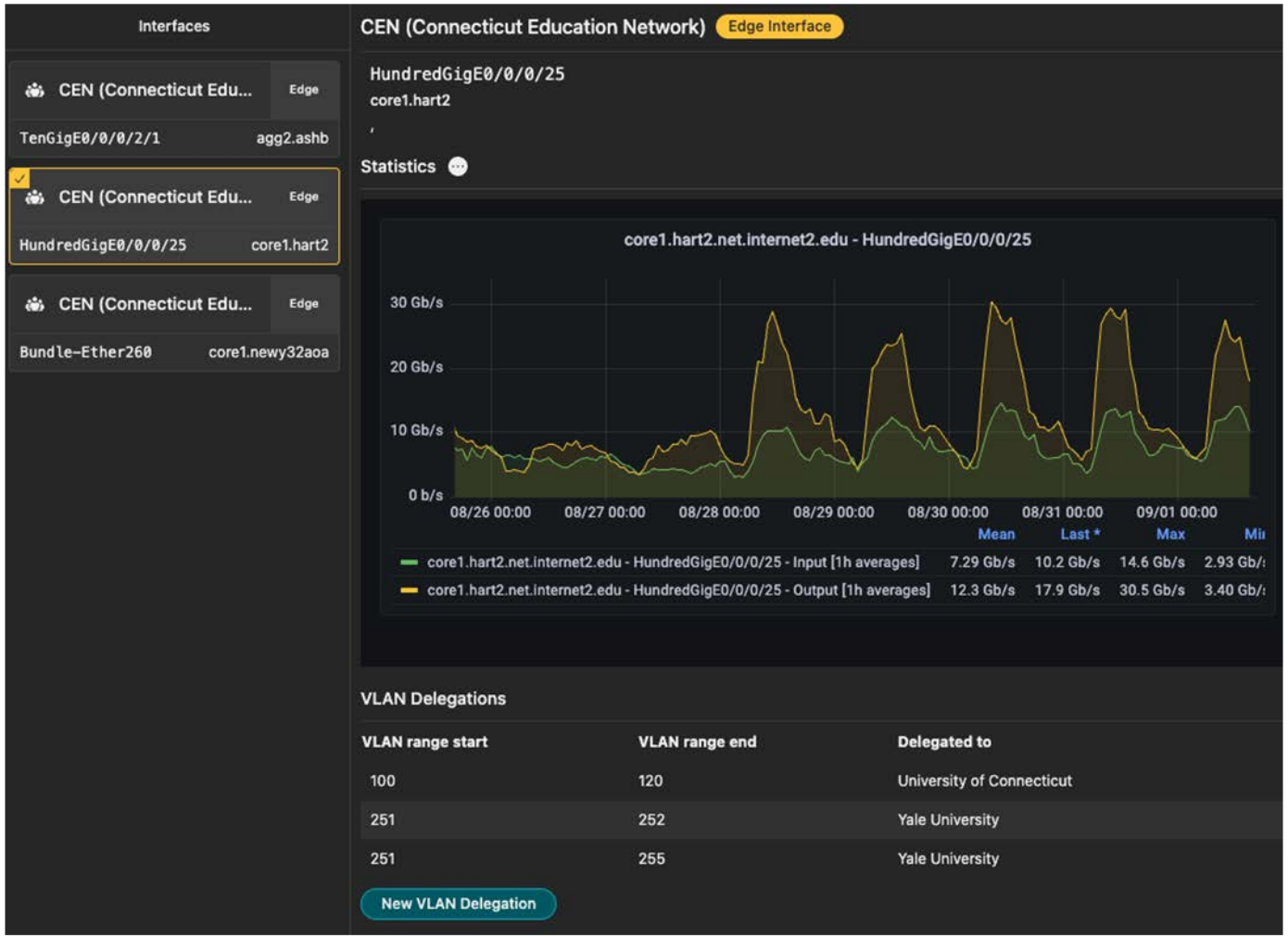
Cost / IPv4 address / year:
$0.005 * 24 hrs * 365 days = $43.80

Annual cost for a /24 = $11,169



Internet2 Cloud Connect (I2CC) changes

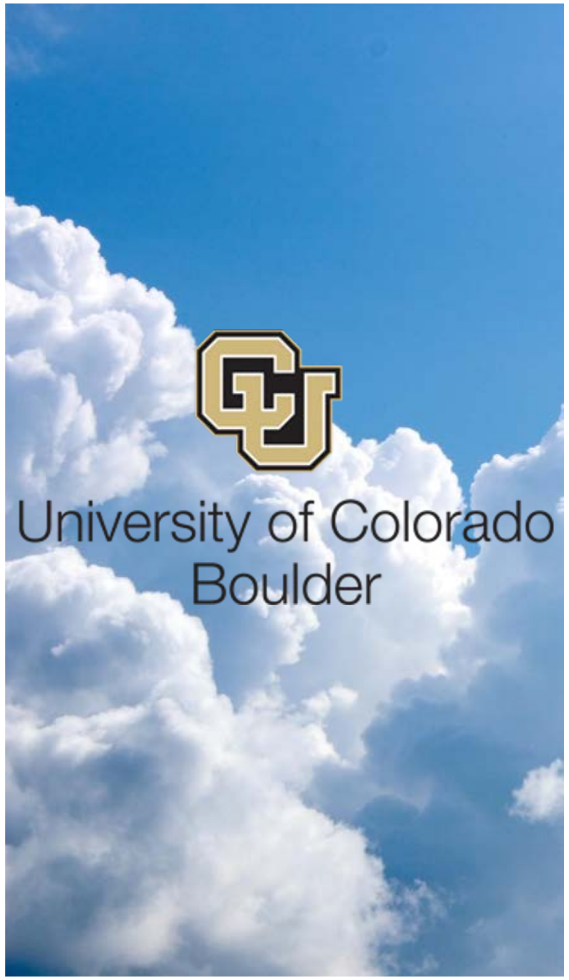
- Demo at TechEX 23!
- Internet2 network provisioning platform change:
  OESS → Virtual Networks
- Migration will be non-disruptive
- Migration late October 2023



Have a *stormy* cloud story?


PART TWO
SECURITY CONSCIOUS CLOUD ENABLEMENT
CHRIS HOREN
University of Colorado Boulder


Security Conscious Cloud Enablement
University of Colorado Boulder



01 Support The Mandate For Security

02 Clear Vision of Design

03 Don’t Reinvent the Wheel

04 Cloud Native Tools

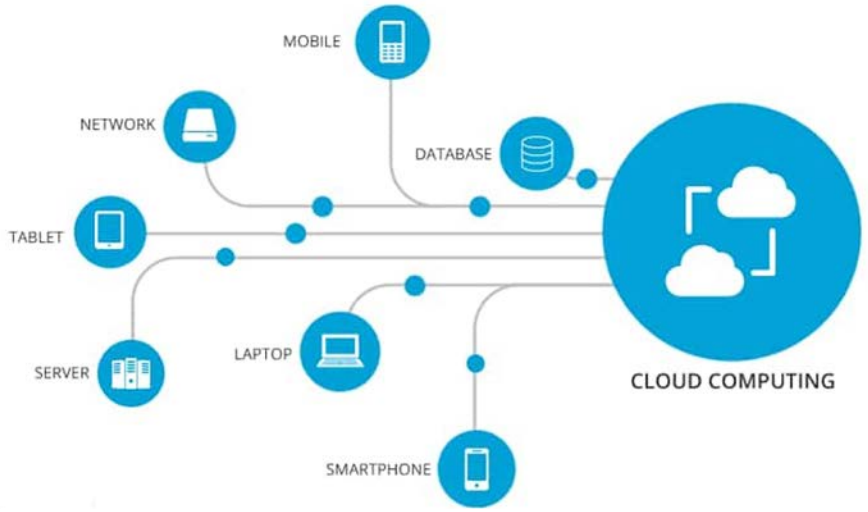
04 Data Classifications Collaboration

Support the Mandate for Security

What You Can Do

- Help facilitate culture change
- Be willing to change current or implement new processes
- Design with long term intention when possible
- Help with leaning into the new norm and sharing the pain
- Clarify roles and responsibilities of each team
- Document, document, document

Clear Vision of Design



Design Vision

- The why?
- What are we trying to accomplish?
- Have we identified at a high level what we need to implement?
- Do we understand the needs of the end users and their interfaces?

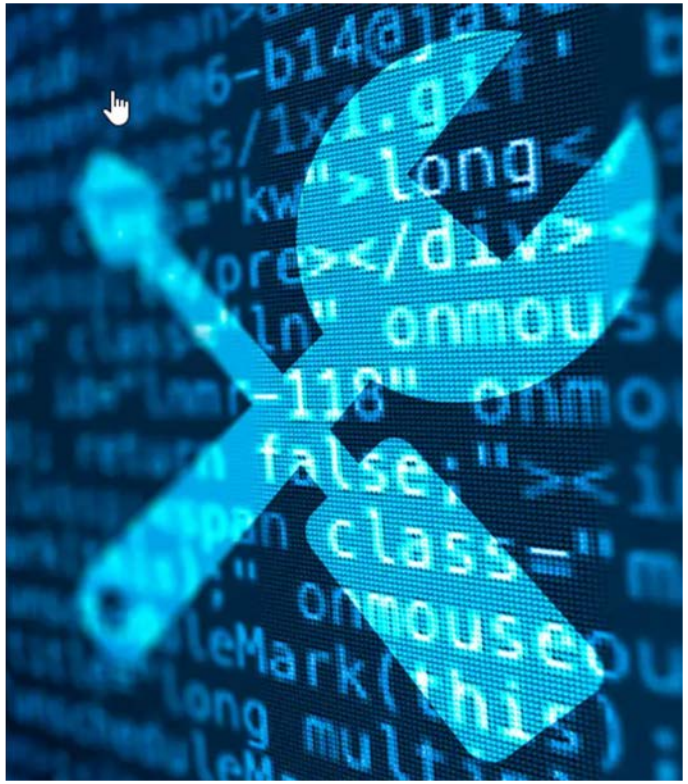
Don’t Reinvent the Wheel

Prepackaged Infrastructure	Azure Blueprints AWS CloudFormation templates
Vendor Solutions	Marketplace offerings vs self hosted Open-source vs paid
Leverage Existing Policies	Can you leverage existing on-premise policies for IAM, incident response, etc.

Cloud Native Tools

Demonstrating Tools

- Be ready with a proof of concept so security engineers can really test the product
- Demonstrate areas that the tools may help close SecOps technical or compliance gaps
- Does unify multiple tools?
- Does it streamline compliance?
- Does it streamline security operations?



Data Classifications

A Quick Win?

- What types of data will the environment be holding?
- Link implementation solutions to data management strategy by explaining the why and how
- Easy, early inroad to collaboration between cloud and security teams
- Addressing early avoids the dreaded outcome of having to rework solutions


PART THREE
IAM IN THE CLOUD
Ananya Ravipati
Internet2

2023 INTERNET2 TECHNOLOGY exchange

IAM in the cloud

Ananya Ravipati, Internet2

Identity and Access management

- Why do you care about it?
- How does it help?

4 A’s

- Administration – define your users
- Authentication – platform native users & federated users
- Authorization – define access scopes
- Auditing – cloud native tooling

Administration

- Understand different sets of users
- Example: Research collaboration teams – is everyone an admin?
- This is a foundational exercise that will define your cloud platform experience

Authentication

- Identities
  - Users
  - Federated users (SSO)
- Federation
  - All platforms support multiple identity providers and protocols
  - Determine what works for your use case
- Identity protection
  - MFA
  - Password rotation
  - Short term credentials

Access keys

- Avoid User access keys
- If there is valid use case, use tools like aws-vault
- Federated users look into tools like saml2aws

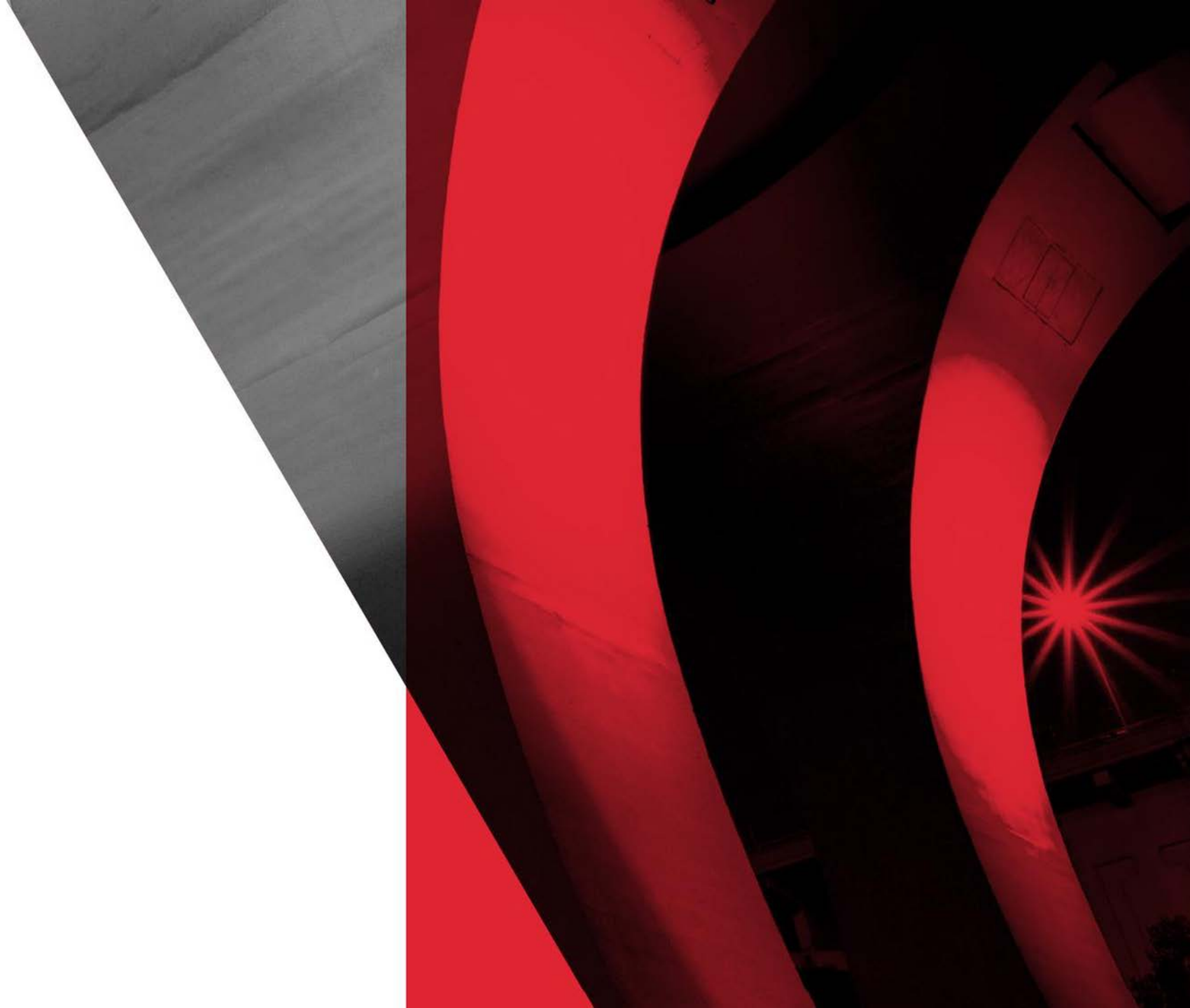
Authorization

- Scoping the permissions
- Using right roles
- Avoid custom policies and roles as much as you can
- Look into attribute based or conditional access scopes

Audit

- Native access analyzers
- Logs
- Security recommendations

Thank you




INTERNET2
TECH ex 23
PART FOUR
DIRECTIONS TO THE CLOUD
Supporting Research in Public Cloud
Dan Landerman
Northwestern University

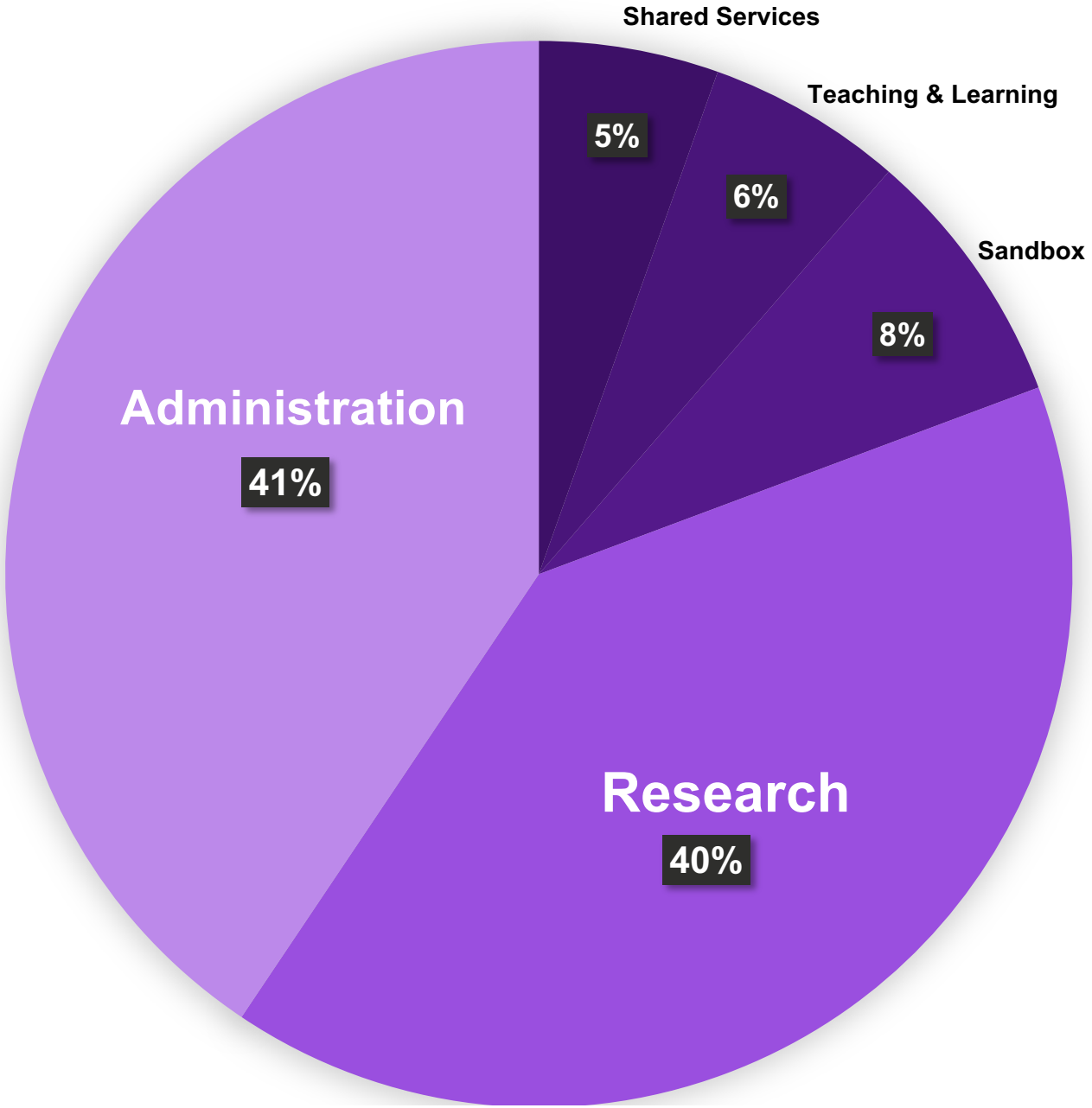
DIRECTIONS TO THE CLOUD

Supporting Research in Public Cloud

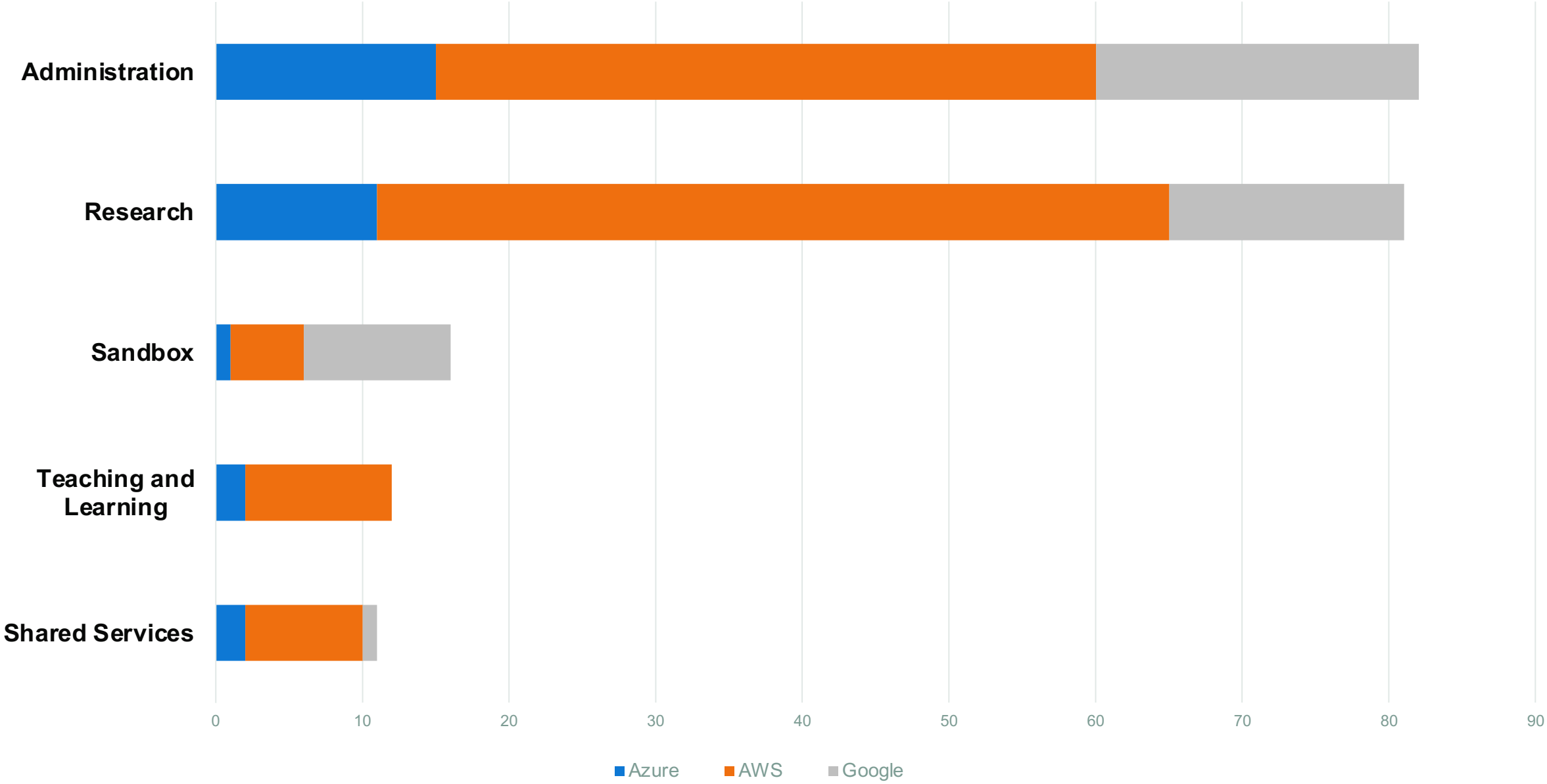
Tech Exchange 2023 Lightning Talk

Dan Landerman
Sr. Cloud Engineer,
Northwestern University

Cloud Accounts at Northwestern



Cloud Accounts at Northwestern



Multi-Cloud by Default

Blog post:
https://matthewrich.com/2022/12/16/multicloud-in-higher-ed/

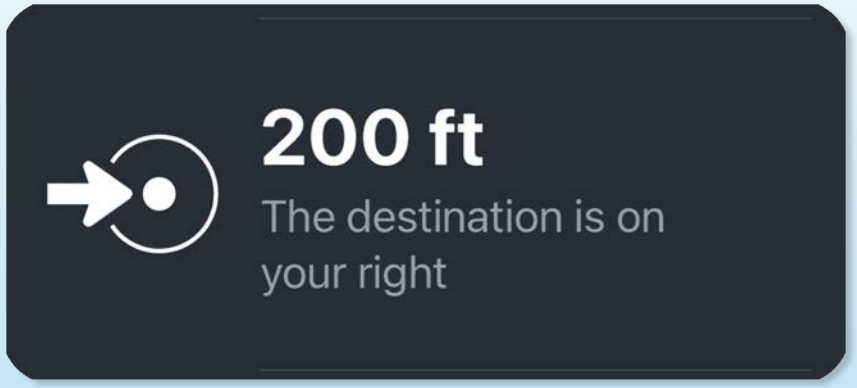
Matthew Rich
Cloud Systems Engineering Manager,
Northwestern University

2023 Education Champion
https://aws.amazon.com/education/education-champions/matthew-rich/

How did we get here?

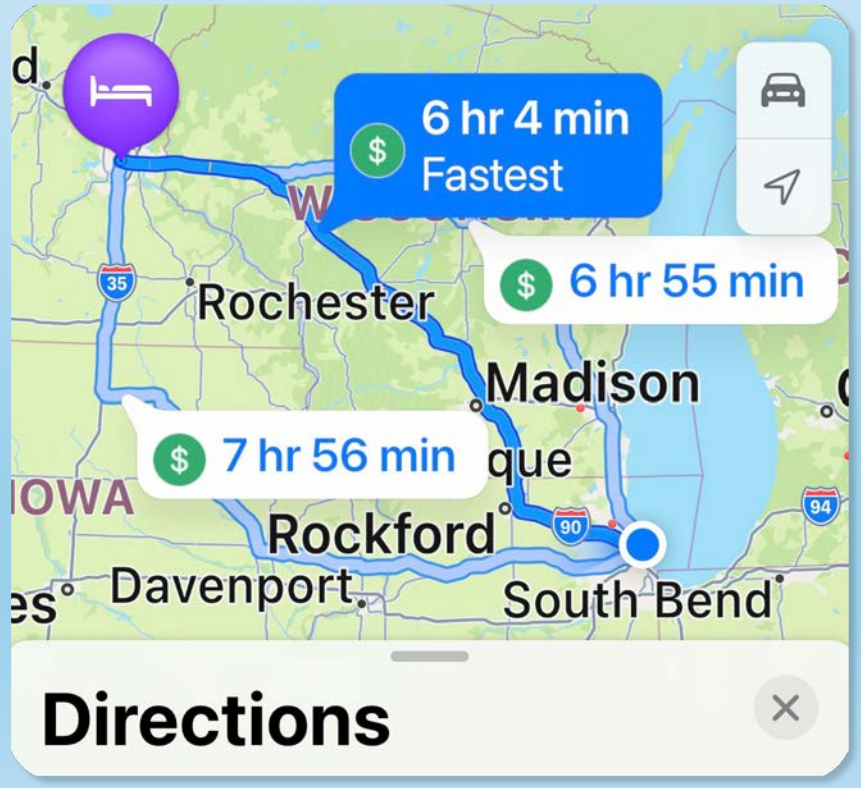
Every destination is different:

- No two Research Initiatives are alike



Multiple route options:

- More than one cloud provider
- Different ways to accomplish research goals



Start by Aligning Closely with IT Partners

- Befriend your distributed IT staff.
- Cloud Providers and their resources
- Resellers (if you have them)
- Facilitate Training

Research Objectives

- Conduct a needs assessment to understand the specific research objectives and requirements of the researchers.
- Is there a level of sophistication or existing experience?
- Who will be doing the work in the Cloud?
- Projects may have varying needs regarding computational power, networking, storage, and data privacy.

Dealing with Data

- Understand the kind of data and how will it be used.
- Ensure that data security and compliance with relevant regulations (e.g., GDPR, HIPAA) are maintained throughout the research process.
- Backup and recovery

Costs and Funding

- Know how the project is being funding and funds available.
- Services can be expensive and intimidating, assist with estimates and ongoing cost management.
- Provide tools and transparency into how funds are being spent.
- Leverage discounts (e.g., STRIDES).

Which Cloud is Right?

- Understand how these decisions made at the beginning of a project affect ongoing research support.
- What provider aligns best with Researcher needs, tools, compute, cost and compliance.
- Managed solutions can still be better options for some.

Resources and Training

- Remember those IT Partners?
- Establish a support system for researchers to report issues and seek assistance with cloud-related problems.
- Leverage the specialists when possible.
- Seek out and provide workshop and training opportunities to help Researchers and their staff effectively utilize cloud resources and best practices

Ongoing Support

- Monitoring and maintenance.
- Conduct regular touchpoints with researchers to re-assess needs, utilization, and spending, adjusting as needed.

Arrive at Research in the Cloud


INTERNET2
TECH ex 23
QUESTIONS?