Enterprise Infrastructure in the Amazon Web Services (AWS) Cloud

David Zych, Erik Coleman, Phil Winans
got AWS?

- http://aws.illinois.edu
- Let’s go!

But...

- IT services have **dependencies**
  - Active Directory
  - *private* resources on campus network
  - *private* resources in other AWS accounts
- packets need roads (routes)
Where we’re going...

VPC Networking Concepts

- Fantastic Enterprise VPCs and How to Build Them
- Using Active Directory in the Cloud
- There And Back Again: a Packet’s Journey from UIUC to AWS
VPC Basics

• **Virtual Private Cloud (VPC):**
  a logically isolated virtual network in the AWS cloud which is dedicated to your AWS account

• an AWS account may have multiple VPCs

• each VPC may contain multiple **Subnets**
Location, Location, Location

- a VPC belongs to a single Region (us-east-2: Ohio)
- a Subnet belongs to a single Availability Zone (us-east-2a)
Public-facing Subnets

- bi-directional communication with any host on the public Internet
  - if permitted by Security Groups

- private IPv4 addresses internally

- 1:1 Network Address Translation (NAT) maps each private IP to an Elastic IP or transient public IP
Network Address Translation (Example)

DNS: example.com IN A 52.15.99.99
Campus-facing Subnets

- bi-directional to campus, without NAT
  - using Technology Services VPN connection
- outbound-only to Internet (optional)
Where we’re going...

• VPC Networking Concepts

➢ Fantastic Enterprise VPCs and How to Build Them

• Using Active Directory in the Cloud

• There And Back Again: a Packet’s Journey from UIUC to AWS
Enterprise VPC (vs Independent VPC)

• Enterprise networking features
  • Campus-facing subnets
  • VPC Peering to other Enterprise VPCs
    • including Core Services VPCs

• Restrictions
  • Private IPv4 space centrally allocated by Technology Services
  • us-east-2 (Ohio) only
Recursive DNS Resolution

- AmazonProvidedDNS: default, preferred

- Cannot resolve University-restricted DNS zones
  - ad.uillinois.edu
  - reverse-mapping zones for RFC1918 private IPv4 space
    - on campus
    - in AWS Enterprise VPCs (if managed in IPAM)
Recursive DNS Resolution (Options)
Recursive DNS Resolution (Options)
Building Your Enterprise VPC

1. Plan your requirements
   - Which features?
   - What subnets? (types, sizes, Availability Zones)
   - How much private IPv4 space?

2. Request allocation from Technology Services

3. Deploy using Infrastructure-as-Code (IaC)
   - Download, customize, run!
   - Terraform

See Knowledgebase for details.
Where we’re going...

- VPC Networking Concepts
- Fantastic Enterprise VPCs and How to Build Them
- Using Active Directory in the Cloud
- There And Back Again: a Packet’s Journey from UIUC to AWS
Active Directory Hybrid Architecture

US-East-2 (Ohio) Region
Core Services VPC
Zone
Zone
“AWS” AD Site
900s
900s
30s
360s
360s
30s

PPSB
Node 9
“Urbana” AD Site

DCL
RRB
“Radius” AD Site

HAB
Node 9
“Urbana” AD Site

Node 9
“Chicago” AD Site

EC2
EC2
US-East-2 (Ohio) Region
Core Services VPC
AD Extended to AWS

Core Services VPC

- AWSDC1
  - Campus-facing subnet 10.224.n.64/27
- AWSDC2
  - Campus-facing subnet 10.224.n.96/27

Enterprise Services VPC

- EC2
- Campus-facing subnet 10.x.y.0/27
- Public-facing subnet 10.x.y.64/27
- Campus-facing subnet 10.x.y.128/27

LDAP (389)
LDAPS (636)
Kerberos (88)

ldap-ad-aws.ldap.illinois.edu:389
krb-ad-aws.kerberos.illinois.edu:88
Support for Domain-Join

• Previously unsupported
• Announcing full support today! June 8th, 2017
• AD Site Boundaries for AWS IP space
• Preferred for AWS campus-facing subnets
• Reduced functionality for private-facing and public-facing subnets
Support for Domain-Join for Enterprise VPCs

<table>
<thead>
<tr>
<th>Feature</th>
<th>Private subnet</th>
<th>Campus-facing subnet</th>
<th>Public-facing subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Synchronization</td>
<td>15 min delay</td>
<td>✓</td>
<td>15 min delay</td>
</tr>
<tr>
<td>AD Site Failover</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Global Catalog Lookup</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

* DDNS registers private IP only. Best practice is to always use campus-published DNS (IPAM) for application use. Never publicize the AD-registered IP or DNS hostname.
What’s next?

- Evaluate need for LDAP over SSL (port 636)
- Exploring Amazon IAM Integration
- Evaluate AWS-hosted AD options
  - AWS Directory Services for Microsoft AD
  - Simple AD
  - AD Connector
- What else do you need?
Where we’re going...

- VPC Networking Concepts
- Fantastic Enterprise VPCs and How to Build Them
- Using Active Directory in the Cloud

- There And Back Again: a Packet’s Journey from UIUC to AWS
AWS US Regions

- GovCloud: us-gov-west
- Oregon: us-west2
- N. California: us-west1
- Ohio: us-east2
- N. Virginia: us-east1
To AWS From Campus

- DCL DC
- CORE
- VPN TUNNEL
- EXIT
- ICCN
- VPC
- AWS

IT Professionals Forum
University of Illinois
At Urbana - Champaign
Spring 2017
Different Ways Networks Connect to AWS

- Public Bilateral Peering
- DirectConnect
- Internet2
- Commodity Internet
- Regional ISP
UofI to Internet2 to us-east-2
UofI to WiscNet to us-east-2
Resources

- [http://aws.illinois.edu](http://aws.illinois.edu)
- Knowledgebase: search for “AWS”
- [aws-support@illinois.edu](mailto:aws-support@illinois.edu)
- David Zych <[dmrz@illinois.edu](mailto:dmrz@illinois.edu)>
- Erik Coleman <[ecc@illinois.edu](mailto:ecc@illinois.edu)>
- Phil Winans <[pwinans@illinois.edu](mailto:pwinans@illinois.edu)>