INTERNET2

2022 TECHNOLOGY exchange

THE BEST OF THE CLOUD FORUM

SHELLEY ROSSELL, University of Chicago
BOB FLYNN, Internet2
MATTHEW RICH, Northwestern University

INTERNET2

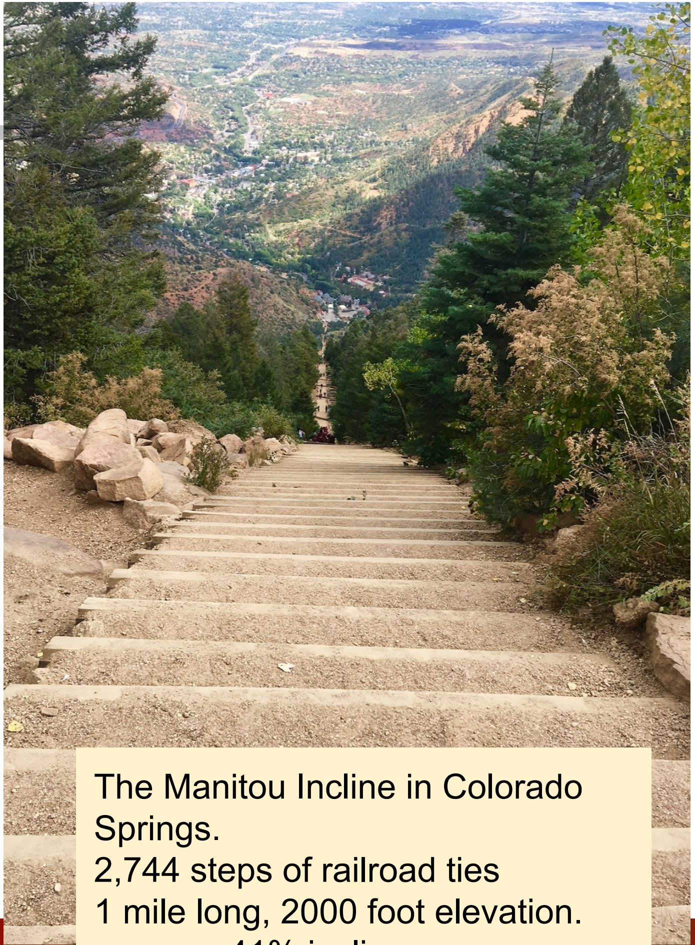
Agenda

- AWS Account Migration at the University of Chicago
- ⚡ So, You Want to Move to the Cloud. What Could Go Wrong?
- ⚡ Let a Thousand PaaSes Bloom
- ⚡ Provisioning GovCloud Accounts

AWS Account Migration Steps at the University of Chicago

Shelley Rossell

shelley@uchicago.edu



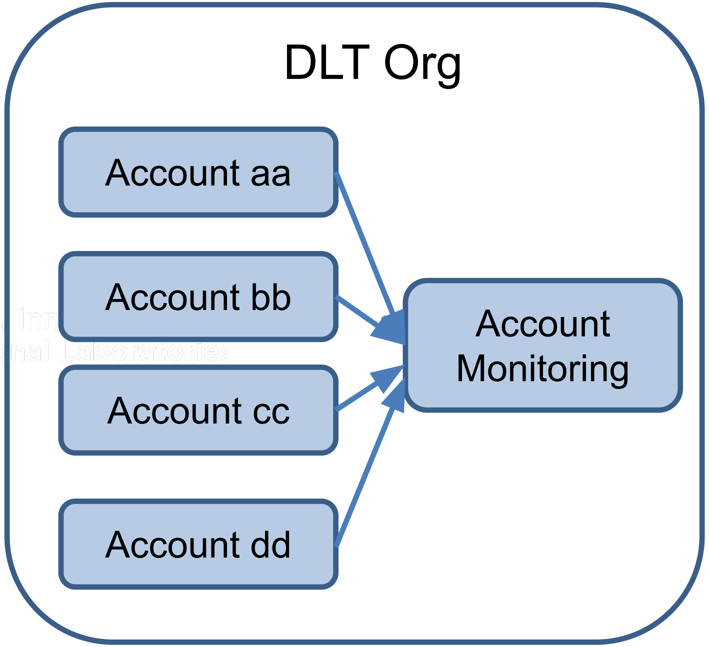
The Manitou Incline in Colorado Springs.
2,744 steps of railroad ties
1 mile long, 2000 foot elevation.
average 41% incline

AWS Account Migration

Where we started

Individual AWS accounts within an Organization managed by DLT ('DLT Org')

- ~20 individual accounts for central IT, Unit IT, researchers
- SSO configured per account
- Used account within this org for central monitoring (because no Control Tower)



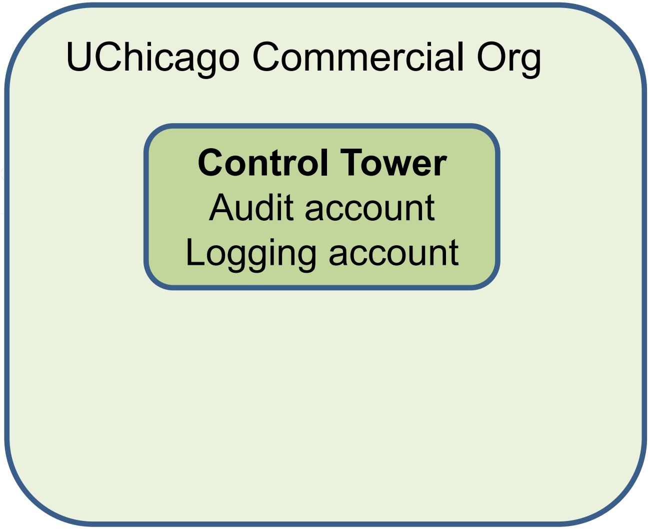
AWS Account Migration

Next step

Got our own AWS Organization via DLT ('UChicago Commercial Org')

Benefits:

- SSO configured at Organization level
- Centralized management (Control Tower)
- Increased visibility: Organize/view accounts by OU
- Use of Service Control Policies
- Ease of centralized monitoring: GuardDuty, SecurityHub, CloudTrail, VPC flows

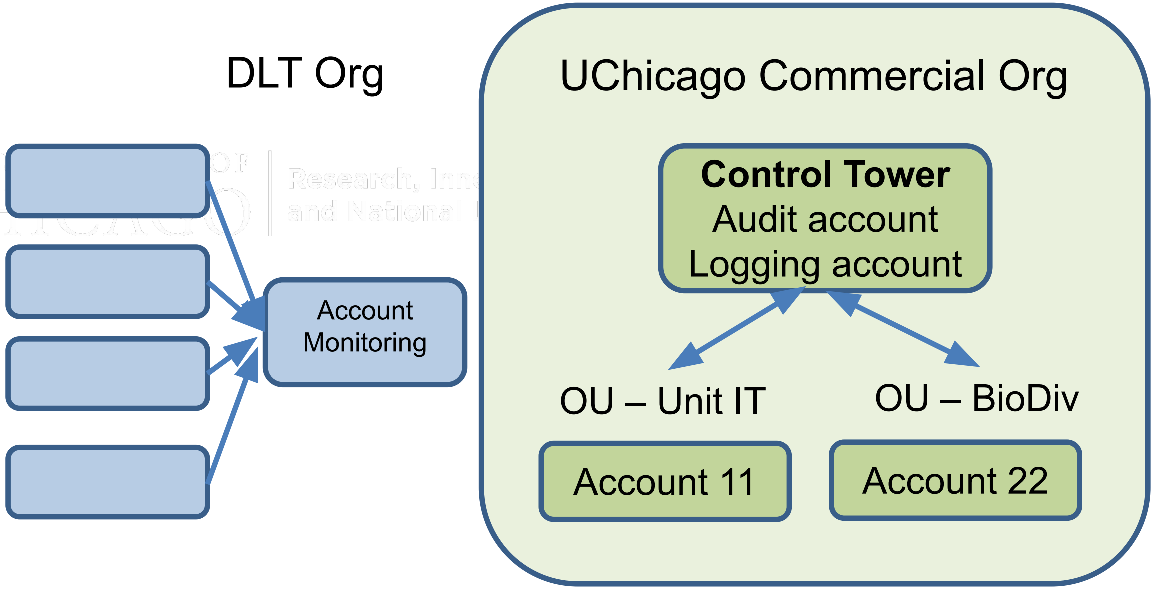


AWS Account Migration

Any new accounts were created within our UChicago commercial org

PROBLEM:

- No unified visibility across all accounts
- More administrative overhead
  - Multiple ‘central’ monitoring setups
  - Different ways to manage accounts, depending on which organization



AWS Account Migration

SOLUTION: Migrate DLT AWS accounts into new UChicago AWS organization

Catalyst:

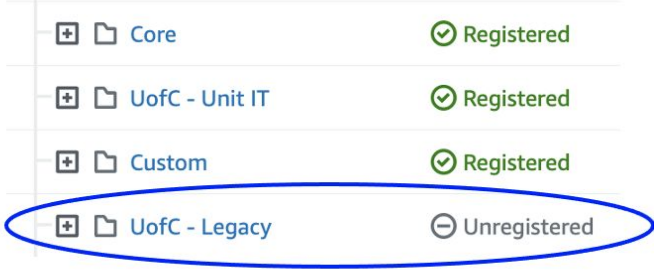
- Change in SSO - Shibboleth setup for each DLT Org account was ending
- Migrate these accounts to take advantage of new UChicago Org level SSO

Test Case: Migrate a non-production Central IT account from the DLT Org to the UChicago Org

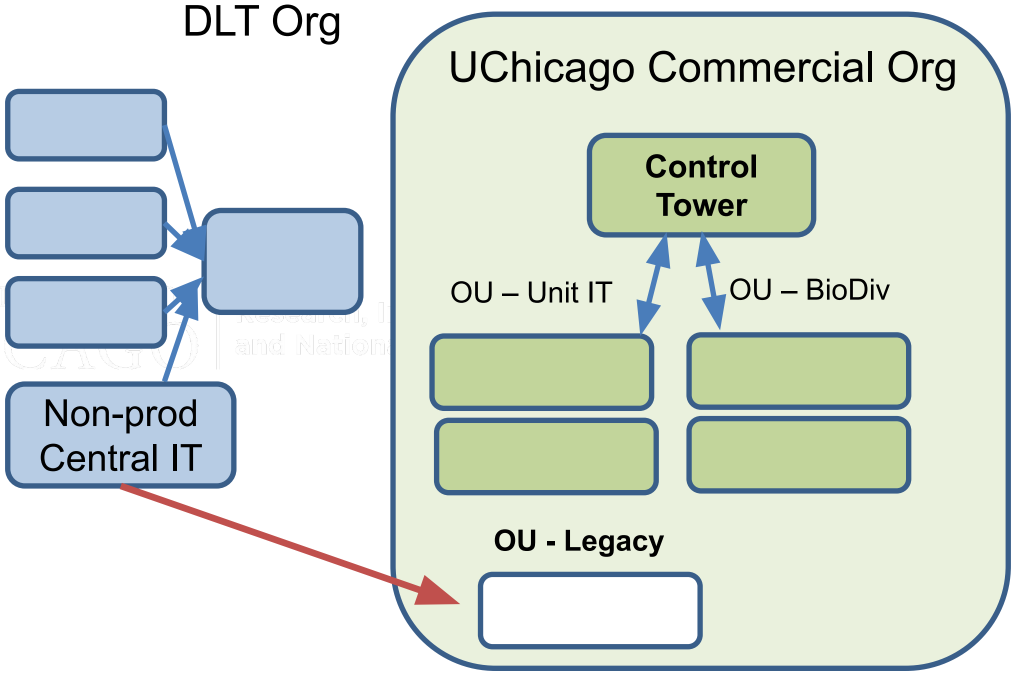
AWS Account Migration: DLT Org to new UChicago Org

- Created a ‘legacy OU’ in the new UChicago Org that was <u>*NOT managed by control tower*</u>

  ‘unregistered with Control Tower’
- To minimize potential disruption or issues
- No SCPs applied
- No region restrictions



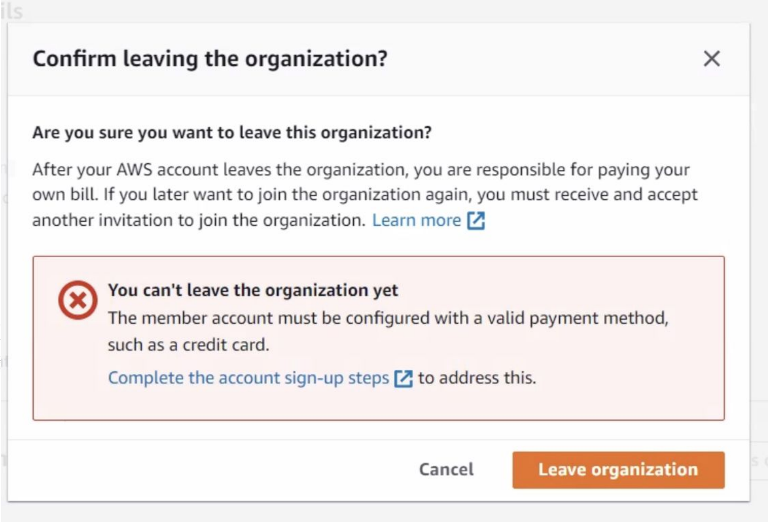
⊞ 🗀 Core	✓ Registered
⊞ 🗀 UofC - Unit IT	✓ Registered
⊞ 🗀 Custom	✓ Registered
⊞ 🗀 UofC - Legacy	⊖ Unregistered



AWS Account Migration: DLT Org to new UChicago Org

What we learned:

- Need to be root to leave an organization and accept new org invitation
- Need to have funding source in place to leave an org: Credit card OR coordinate with DLT
- Invite the account to your new Organization.
- View and accept the invitation



Confirm leaving the organization?

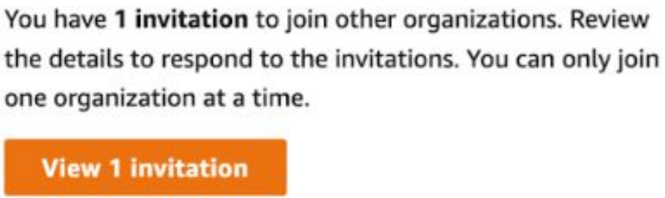
Are you sure you want to leave this organization?

After your AWS account leaves the organization, you are responsible for paying your own bill. If you later want to join the organization again, you must receive and accept another invitation to join the organization. Learn more

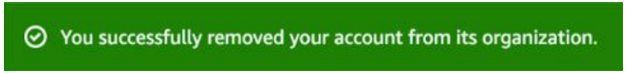
You can't leave the organization yet

The member account must be configured with a valid payment method, such as a credit card.

Complete the account sign-up steps to address this.



You have **1 invitation** to join other organizations. Review the details to respond to the invitations. You can only join one organization at a time.



You successfully removed your account from its organization.

- You should see the new account in your Organization view

AWS Account Migration: DLT Org to new UChicago Org

What we learned continued:

- SSO login: Both legacy account Shibboleth AND Organization SSO worked concurrently for migrated accounts
  - Less user disruption and coordination needed since old and new way worked concurrently
  - We eventually redirected the legacy login URL to the new one
- Needed to recreate, prepopulate, and sync the Grouper groups so they would show up in the new UChicago Organization to be associated with permissions for the migrated account.

AWS Account Migration: DLT Org to new UChicago Org

Next steps

- Now that we verified the migration was successful, we reached out to other owners of DLT Org accounts about the upcoming SSO change and need to migrate to the UChicago Org
- Gave a timeframe
- Coordinated with DLT (ticket and zoom set up in advance) due to most having existing PO for payment
- After successful, notified account owners - let us know if access issues
- *Bonus: Learned some accounts could close*

AWS Account Migration

RESULT

Now all *known* AWS accounts in our new UChicago Organization

PROBLEM:

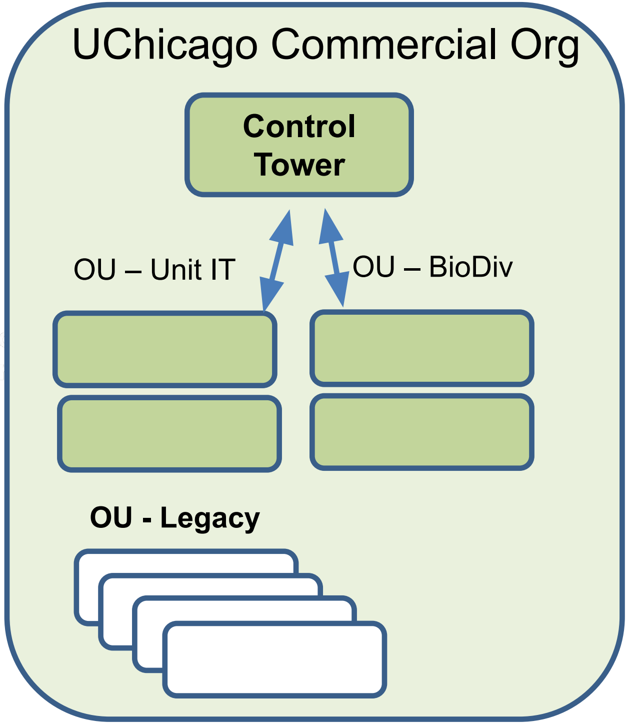
Difficult if some accounts are managed by Control Tower and some are not

- Organizational CloudTrail
- Automatic central VPC flow monitoring
- Central Security Hub and Config
- Central GuardDuty
- Use of CloudFormation and StackSets

AWS Control Tower

The easiest way to set up and govern a secure, compliant multi-account AWS environment

DLT Org
<empty>



UChicago Commercial Org

Control Tower

OU – Unit IT

OU – BioDiv

OU - Legacy

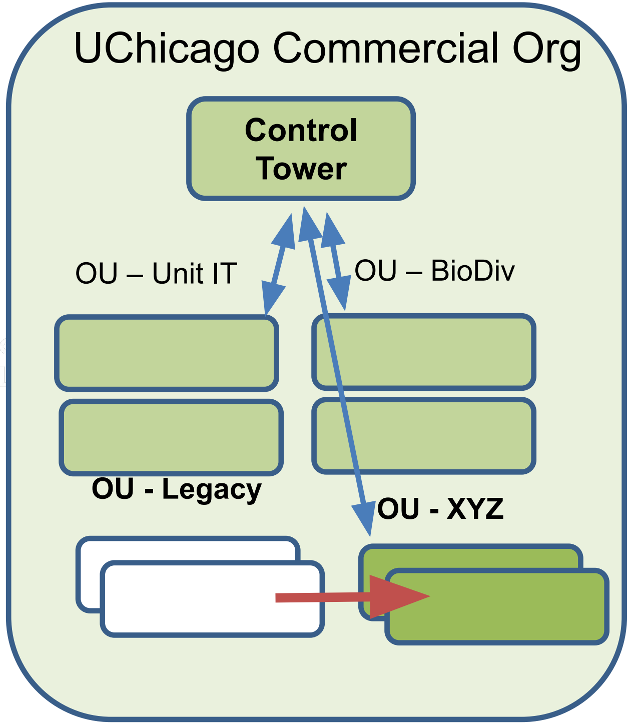
AWS Account Migration

SOLUTION

Migrate unmanaged AWS accounts to control tower management

In practice

Move accounts from the Legacy ‘unregistered’ OU to a Control-Tower registered OU



AWS Account Migration: Unmanaged to Control Tower Managed

STEPS

1. Met with account owners 1:1
   a. How using AWS? Future plans?
   b. How can we help support them? What do they need?
   c. Remind them of resources
   d. Explain benefits of being in the managed UChicago Organization
   e. Set up a time for the migration and note any follow ups

Our experience:

- Account owners - receptive, appreciate the outreach
- Want to be in the managed Organization (they can focus on their work, we help focus on security and monitoring)
- Identified follow up opportunities (review IAM, review Security Hub recommendations, suggest training, put in contact with AWS SME)

AWS Account Migration: Unmanaged to Control Tower Managed

2. Need to create a Control Tower Execution Role in the account to be migrated

https://docs.aws.amazon.com/en_us/controltower/latest/userguide/enroll-manually.html

3. Delete the existing Configuration recorder and delivery channel

Why? Only one per account, and Control Tower creates its own

```
aws configservice delete-configuration-recorder
--configuration-recorder-name default
```

```
aws configservice delete-delivery-channel --delivery-channel-name default
```

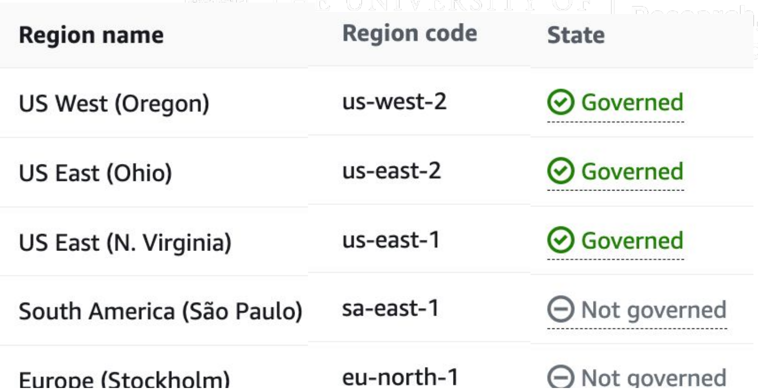
NOTE: If it isn’t called ‘default’, get the name:

```
aws configservice describe-delivery-channels
```

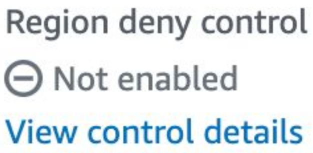
AWS Account Migration: Unmanaged to Control Tower Managed

4. Check that no resources exist in non-supported regions (per our SCPs)

- We restrict to Virginia, Ohio, and Oregon
- Note: Control Tower not (yet?) in California
- We have one OU in which exceptions are allowed (regional SCP not enforced)
- We do not enforce this at the Landing Zone for flexibility (legacy, permitted exceptions)



Region name	Region code	State
US West (Oregon)	us-west-2	✓ Governed
US East (Ohio)	us-east-2	✓ Governed
US East (N. Virginia)	us-east-1	✓ Governed
South America (São Paulo)	sa-east-1	⊖ Not governed
Europe (Stockholm)	eu-north-1	⊖ Not governed



Region deny control

⊖ Not enabled

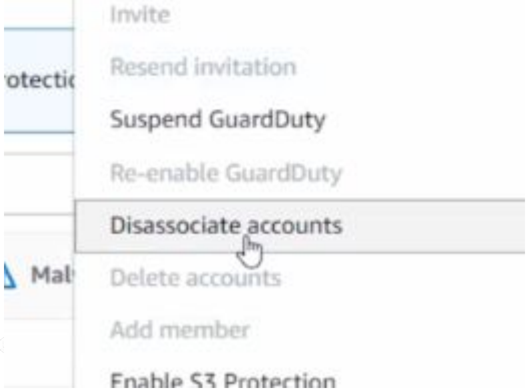
View control details

AWS Account Migration: Unmanaged to Control Tower Managed

5. Disassociate accounts in legacy monitoring account GuardDuty and Security Hub

6. Remove CloudTrail sent to legacy S3 bucket

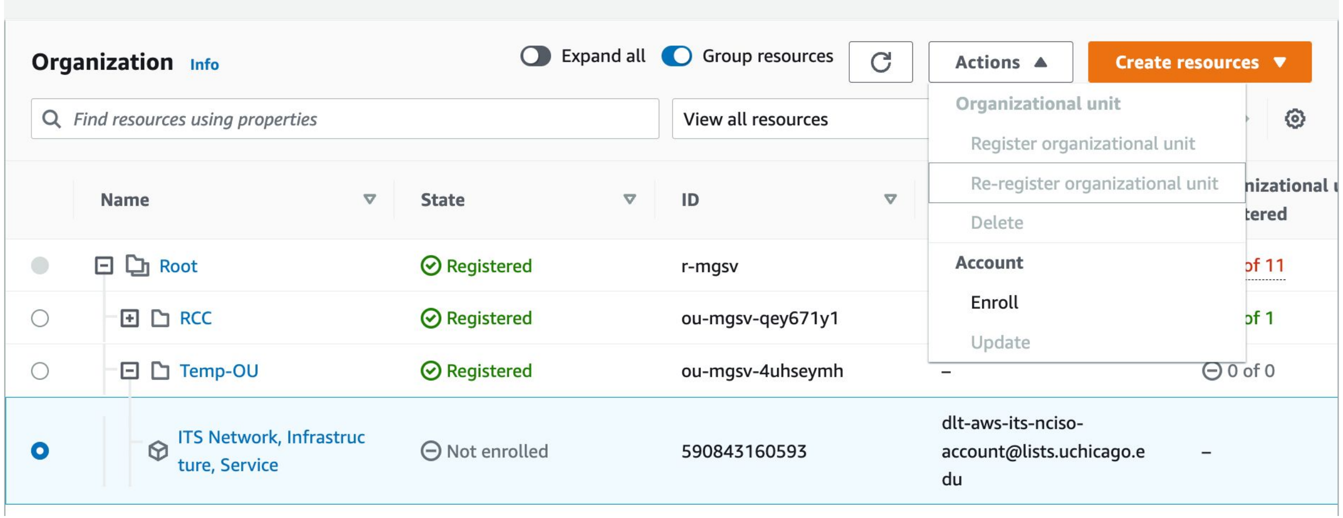
7. Remove VPC Flow sent to legacy S3 bucket



AWS Account Migration: Unmanaged to Control Tower Managed

9. From Organizations, move the account from the Legacy OU to the target OU

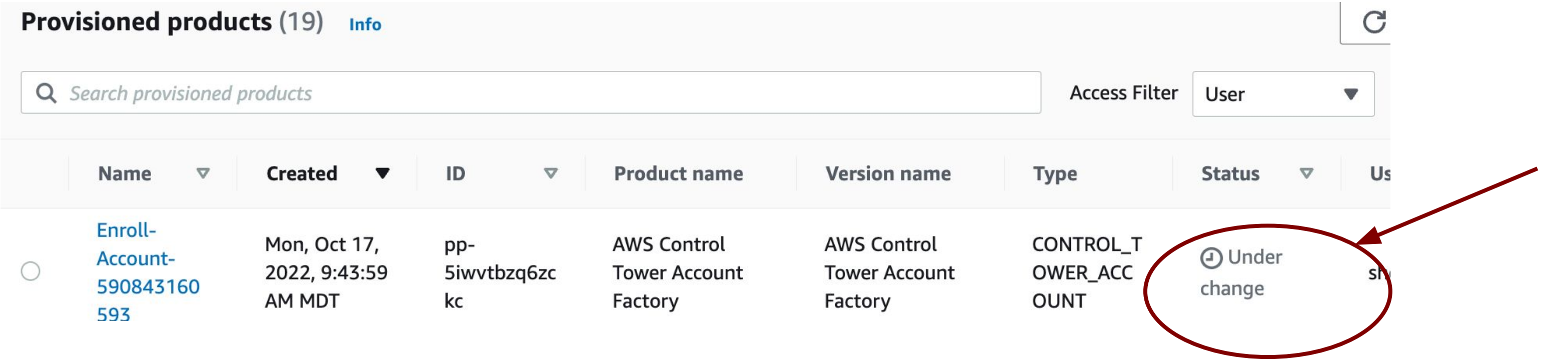
10. Select the account, then under Actions → Enroll



	Name	State	ID		nizational tered
○	Root	Registered	r-mgsv		of 11
○	RCC	Registered	ou-mgsv-qey671y1		of 1
○	Temp-OU	Registered	ou-mgsv-4uhseymh	–	0 of 0
●	ITS Network, Infrastructure, Service	Not enrolled	590843160593	dlt-aws-its-nciso-account@lists.uchicago.edu	–

AWS Account Migration: Unmanaged to Control Tower Managed

You should see the status in Service Catalog → Provisioned Products



Provisioned products (19) Info

	Name ▽	Created ▼	ID ▽	Product name	Version name	Type	Status ▽	Us
○	Enroll-Account-590843160593	Mon, Oct 17, 2022, 9:43:59 AM MDT	pp-5iwvtbzq6zckc	AWS Control Tower Account Factory	AWS Control Tower Account Factory	CONTROL_TOWER_ACCOUNT	Under change	sh

If enrollment fails: From Provisioned Products, terminate the instance

After addressing the issue, go to Organization view, select the failed account, move it to the root. Then from Actions → Update (*Enroll might no longer be an option*).

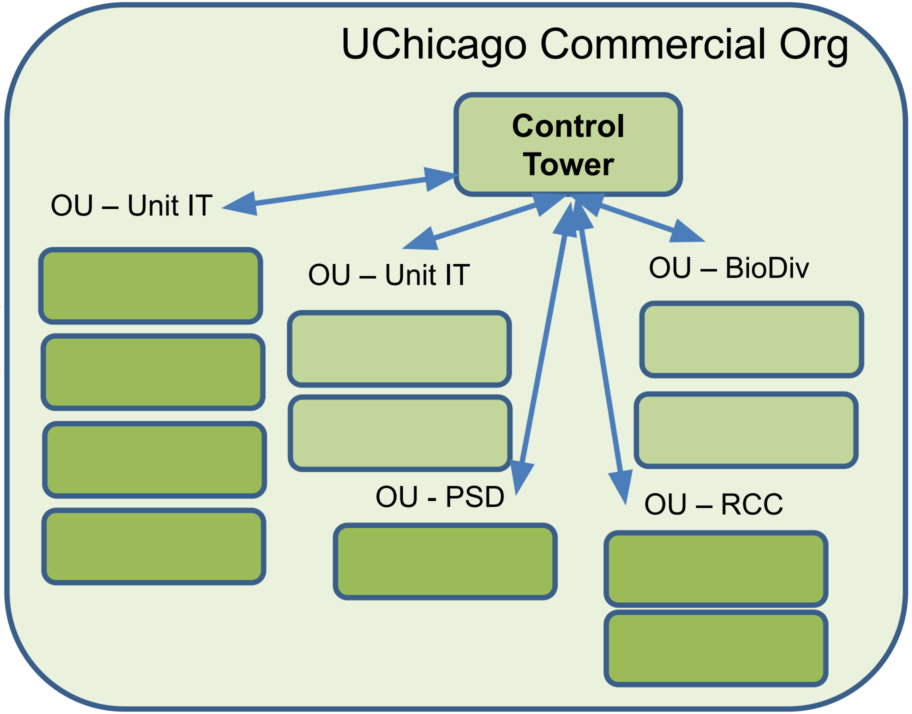
11. Inform account owner of migration schedule in advance. After successful, ask them to test

AWS Account Migration

Met our goal

- All known AWS accounts in our UChicago commercial Org*
- Accounts are in organized OUs
  - Managed by Control Tower
  - Consistent SCPs
  - Centrally use CloudFormation

*We also have a GovCloud Org



AWS Account Migration

Hello?
Is it answers you’re looking for?

Shelley Rossell

shelley@uchicago.edu

LIGHTNING TALKS

So, You Want to Move to the Cloud. What Could Go Wrong?

Let a Thousand PaaSes Bloom

Provisioning GovCloud Accounts

So, You Want to Move to the Cloud

What Could Go Wrong?

cc: philjrenaud - https://www.flickr.com/photos/59716929@N04

cc: freshwater2006 - https://www.flickr.com/photos/77422674@N00

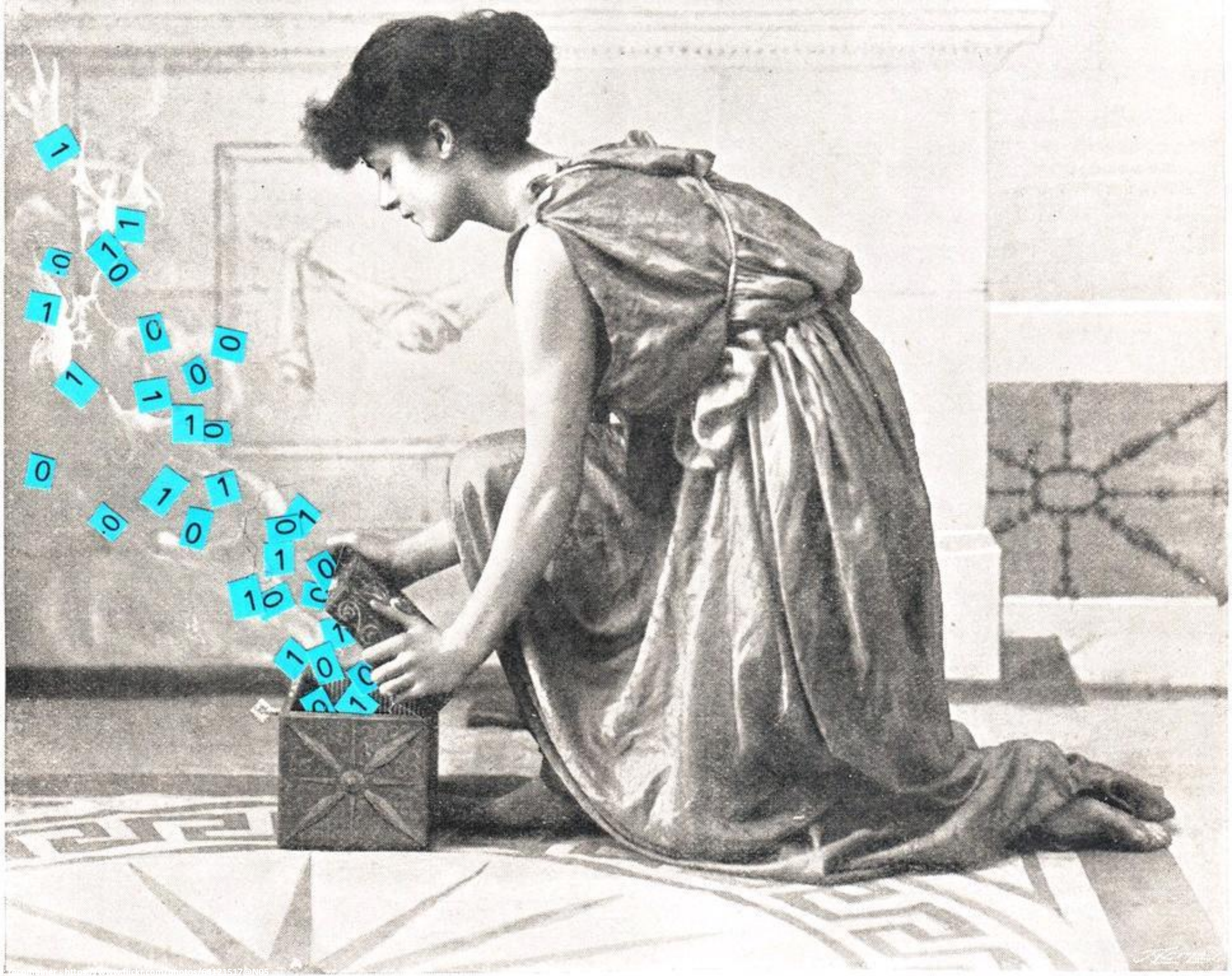
Teaching & Learning

cc: Mikael Kristenson - https://unsplash.com/@mikael_k?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

cc: guiskatenator - https://www.flickr.com/photos/34719728@N05

cc: Danielle Cerullo - https://unsplash.com/@dncerullo?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

cc: rosipaw - https://www.flickr.com/photos/8542711@N08



recombiner - https://www.flickr.com/photos/64121517@N05

cc: Johnson Cameraface - https://www.flickr.com/photos/54459164@N00

cc: jeffmarks.net - https://www.flickr.com/photos/53616069@N08

cc: Trey Ratcliff - https://www.flickr.com/photos/95572727@N00

Research

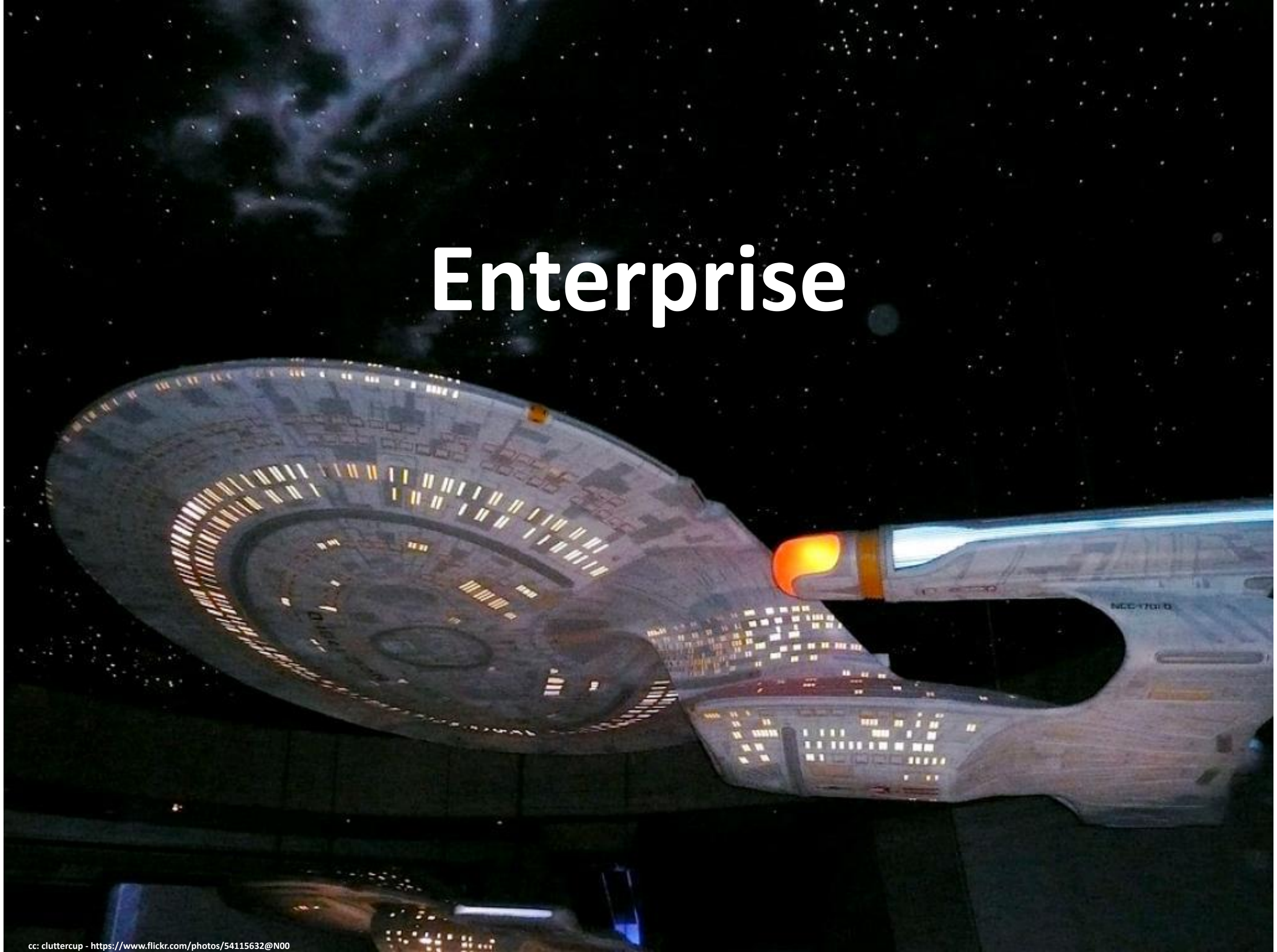
cc: Louis Reed - https://unsplash.com/@_louisreed?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

cc: Osarugue Igbinoba - https://unsplash.com/@osarugue?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

cc: fatboyke (Luc) - https://www.flickr.com/photos/8264376@N03

cc: Danist Soh - https://unsplash.com/@danist07?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

Enterprise



cc: cluttercup - https://www.flickr.com/photos/54115632@N00

cc: Aleksandr Barsukov - https://unsplash.com/@aleksandr_barsukov?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

cc: Ervins Strauhmanis - https://www.flickr.com/photos/76523360@N03

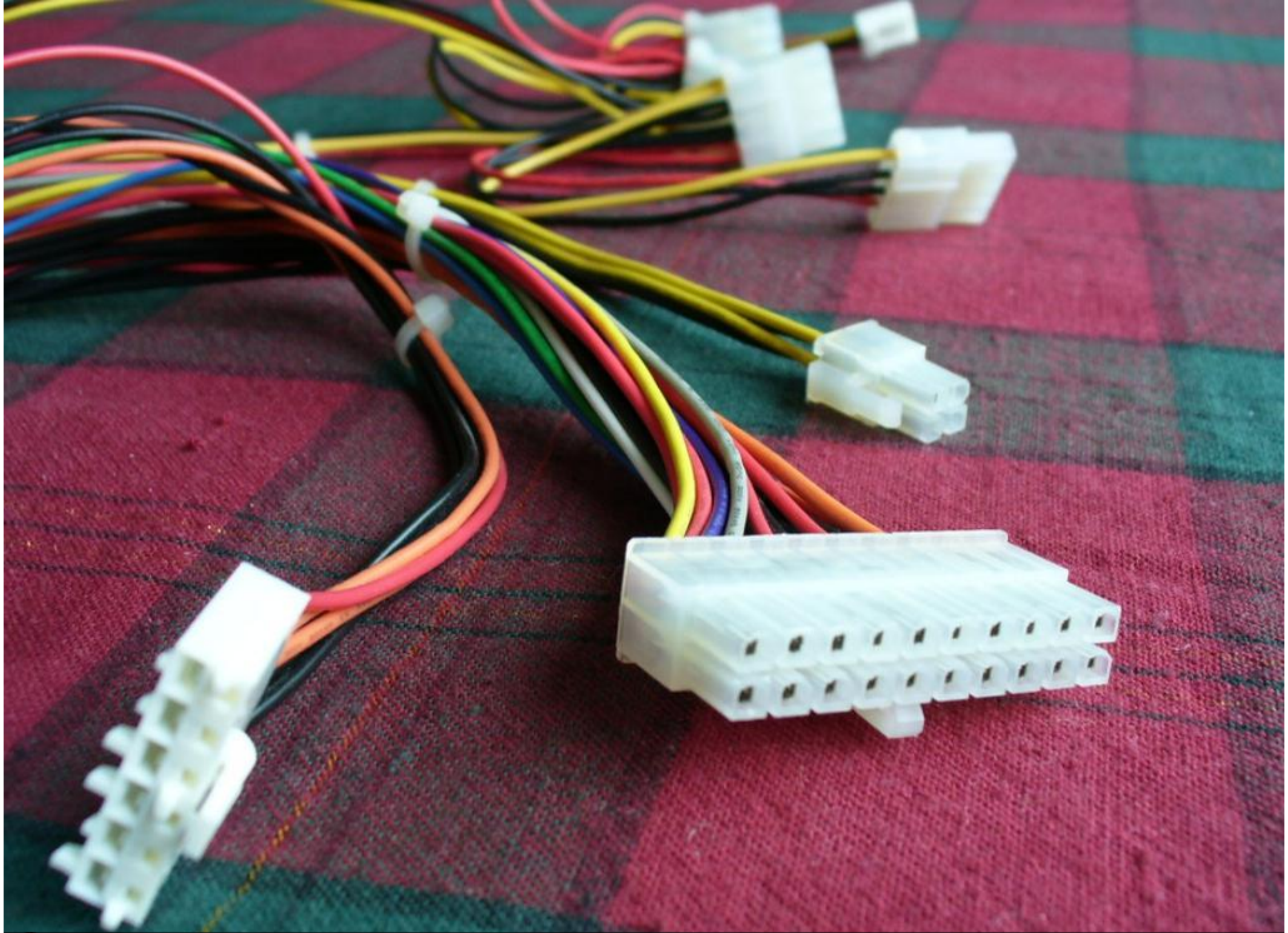


Photo by osde8info - Creative Commons Attribution-ShareAlike License https://www.flickr.com/photos/8764442@N07

cc: Álvaro Serrano - https://unsplash.com/@alvaroserrano?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

cc: Tegan Mierle - https://unsplash.com/@tegan?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

cc: jacqui.brown33 - https://www.flickr.com/photos/120600995@N07

cc: keith ellwood - https://www.flickr.com/photos/76377775@N05

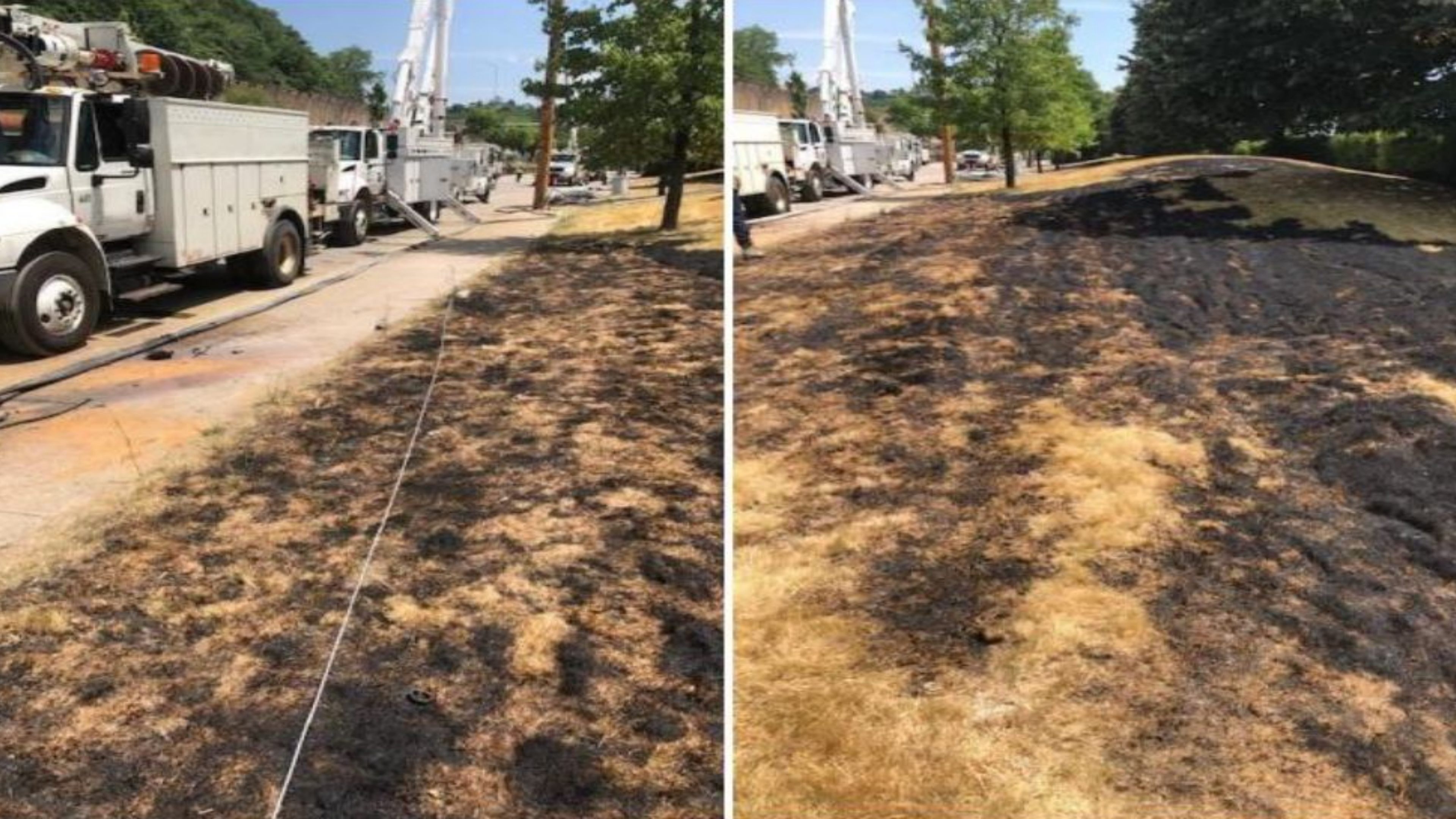
Photo by Andre Mouton - Creative Commons No known copyright restrictions

Created with Haiku Deck

cc: Jp Valery - https://unsplash.com/@jpvalery?utm_source=haikudeck&utm_medium=referral&utm_campaign=api-credit

Photo by Artem Maltsev - Creative Commons No known copyright restrictions

Created with Haiku Deck



cc: wwarby - https://www.flickr.com/photos/26782864@N00

cc: Public Places - https://www.flickr.com/photos/78019868@N05

cc: AliceNWondrlnd - https://www.flickr.com/photos/12227737@N07

Thank you!

Photo by Rishabh Dharmani - Creative Commons No known copyright restrictions

Created with Haiku Deck

Let a thousand PaaSes Bloom

Matthew Rich, Northwestern University

A brief history of deploying web apps

- 1994 – 2001: FTP your Perl CGI script to a server
- 2001 – 2006: FTP your PHP script to a server
- 2006 – 2010: Rails is rad! How do I deploy this thing
- 2010 – 2015: Heroku 💪
- 2015 – present: Docker I guess?

Heroku was really amazing

- It enabled “web 2.0” frameworks incl. Rails and Django, to be easily deployed
- Very opinionated (Created the highly useful 12 Factor App methodology)
- Copied by Amazon as Elastic Beanstalk, Google as App Engine

Docker killed Heroku

- Docker made containers easy to work with
- Monolithic web apps became un-cool
- Salesforce has not continued to develop the platform

- BUT the *idea* of Heroku never died

Frontend frameworks

- Circa 2013 React and Angular were released
- Powerful, real-time-ish applications could now be created and deployed *directly to the browser*
- But the JavaScript development toolchain is a nightmare

JAMstack & a new generation of PaaS

- A new architectural approach: Javascript + APIs + Markup
- New opinionated PaaS platforms:
  - Intelligent, automated build systems
  - CDNs
  - Functions-as-a-service

- Primary examples: Netlify, Vercel, Fly.io

Why do we care?

- A new generation of developers is learning this approach
- What will governance look like?

Provisioning AWS GovCloud

Shelley Rossell

shelley@uchicago.edu

AWS GovCloud

What is AWS GovCloud?

Particular AWS regions designed to host sensitive data, regulated workloads, and comply with stringent U.S. government security and compliance requirements.

Use if compliance needed with requirements for:

- Department of Defense (DoD)
- Criminal Justice Information Systems (CJIS)
- FedRAMP High baseline
- .. and similar

Our first use case: Account would use CJIS data

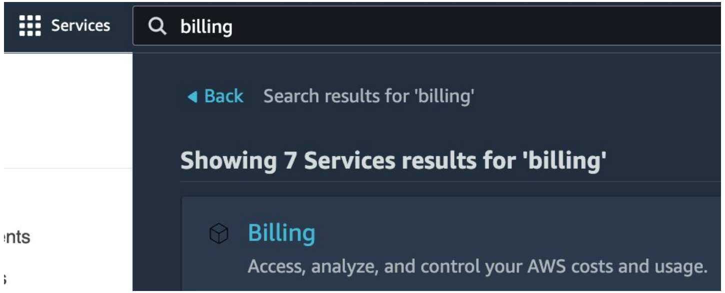
AWS GovCloud vs. Commercial Organizations

AWS Commercial Organization

- Root account
- Control Tower
- Regions around the world

AWS GovCloud Organization

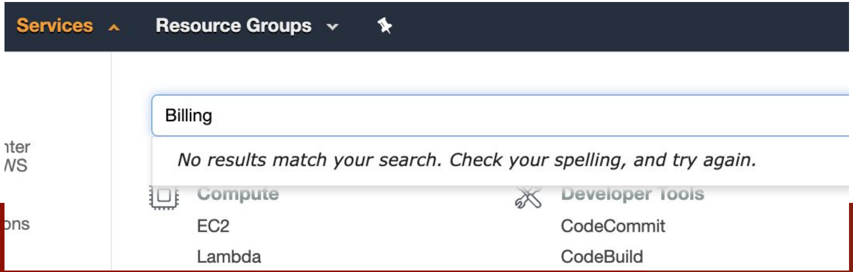
- No root account, uses administrator account
- No Control Tower
- Only US-East and US-West regions
- Linked with new account in your commercial org for billing
- No cost explorer or billing services



Search results for 'billing'

Showing 7 Services results for 'billing'

Billing
Access, analyze, and control your AWS costs and usage.

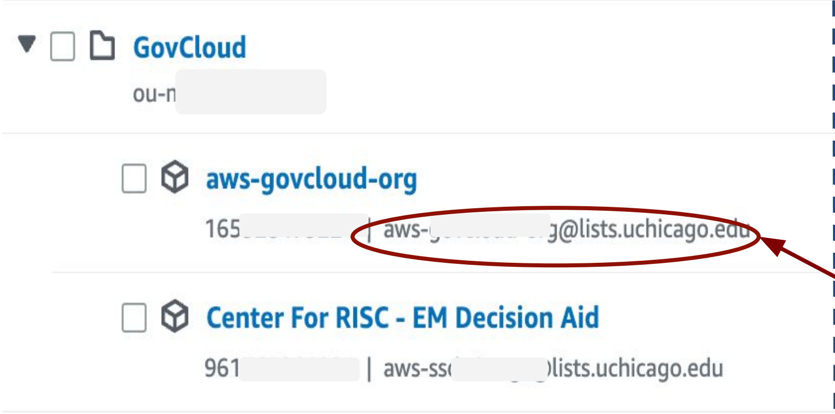


Billing

No results match your search. Check your spelling, and try again.

AWS GovCloud Architecture - mapping to commercial org

UChicago AWS Commercial Org



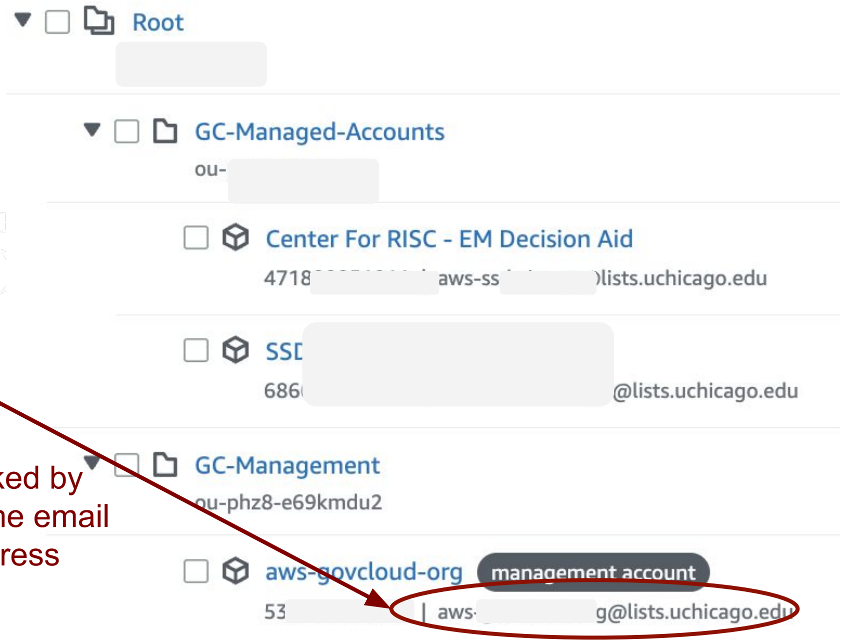
▼ □ GovCloud
ou-n[redacted]

□ aws-govcloud-org
165[redacted] | aws-[redacted]g@lists.uchicago.edu

□ Center For RISC - EM Decision Aid
961[redacted] | aws-ss[redacted]lists.uchicago.edu

How they link: Same email address, different account number

UChicago AWS GovCloud Org



▼ □ Root
[redacted]

▼ □ GC-Managed-Accounts
ou-[redacted]

□ Center For RISC - EM Decision Aid
4718[redacted] aws-ss[redacted]lists.uchicago.edu

□ SSD[redacted]
686[redacted]@lists.uchicago.edu

▼ □ GC-Management
ou-phz8-e69kmdu2

□ aws-govcloud-org management account
53[redacted] | aws-[redacted]g@lists.uchicago.edu

Linked by same email address

AWS GovCloud - How to get started

1. **Request a GovCloud account using the DLT portal** https://i2portal.dlt.com/

   Items of note:

   a. *If you don’t yet have a GovCloud org – this needs to be YOU, not the PI*
   b. Request type: New AWS account
   c. Check the GovCloud box
   d. Root email: Will be used to link the associated commercial account
   e. Lead Technical Contact Name and Email: Will receive the instructions on how to log in as Administrator in the GovCloud account

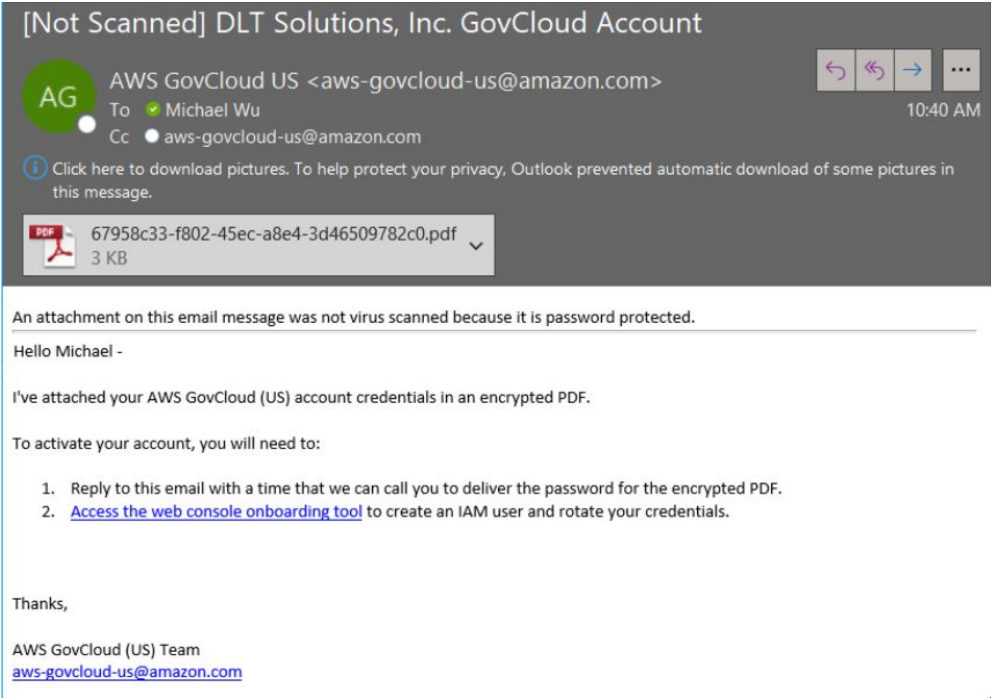
AWS GovCloud - How to get started

2. DLT: Creates the linked account in the commercial org (billing account)

   - You: Reset the root password and enable MFA

3. AWS: Creates the GovCloud account and adds the first IAM user: Administrator

4. AWS: Sends Technical Contact an email with encrypted Administrator credentials



[Not Scanned] DLT Solutions, Inc. GovCloud Account

AWS GovCloud US <aws-govcloud-us@amazon.com>
To Michael Wu
Cc aws-govcloud-us@amazon.com

10:40 AM

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

67958c33-f802-45ec-a8e4-3d46509782c0.pdf
3 KB

An attachment on this email message was not virus scanned because it is password protected.

Hello Michael -

I've attached your AWS GovCloud (US) account credentials in an encrypted PDF.

To activate your account, you will need to:

1. Reply to this email with a time that we can call you to deliver the password for the encrypted PDF.
2. Access the web console onboarding tool to create an IAM user and rotate your credentials.

Thanks,

AWS GovCloud (US) Team
aws-govcloud-us@amazon.com

AWS GovCloud - How to get started

5. Schedule time to receive a call from AWS for the PDF password

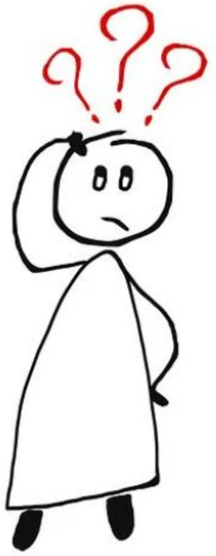
6. Open the PDF and get the Access Key ID and Secret Access Key

7. Login to *AWS GovCloud (US) Management Console - Onboard Tool* (govcloud-onboarding-tool.us-east-1.amazonaws.com) with the keys. It will prompt to reset the Administrator password.

8. Log into the account as “Administrator” with the new password and set MFA

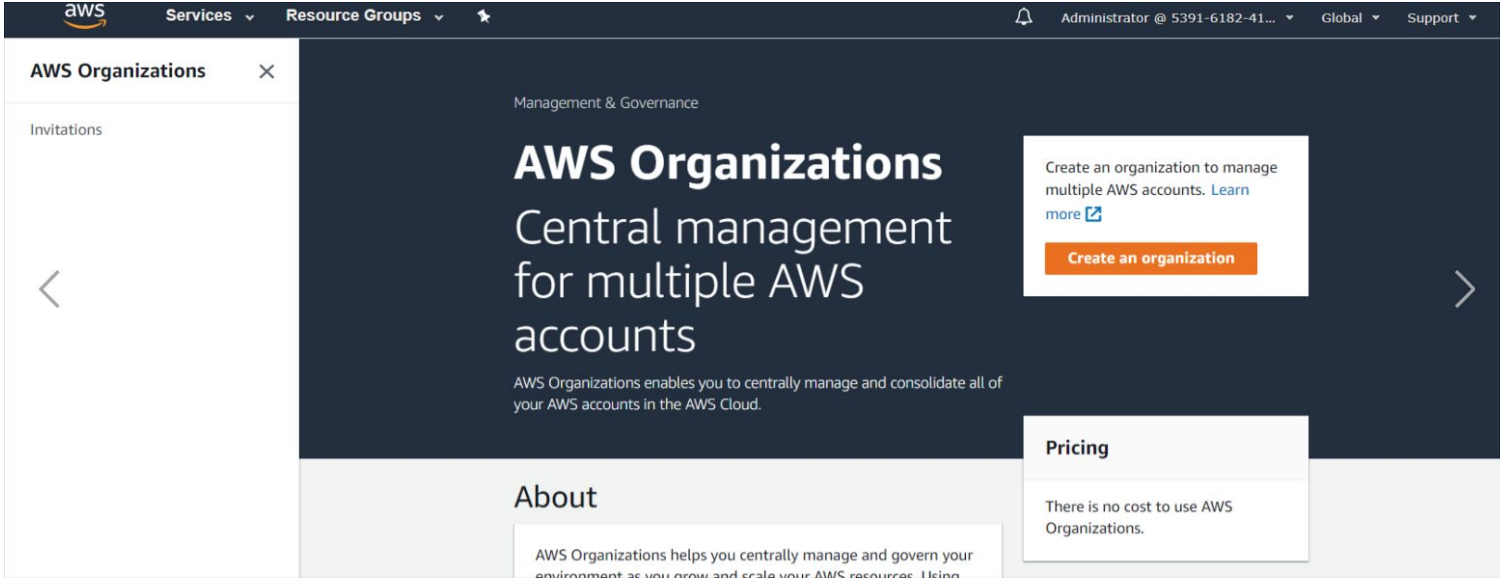
9. Create IAM users for cloud team and account owners

So … is this my GovCloud Org?



AWS GovCloud - How to get started

10. Create the GovCloud Organization using this account



Management & Governance

AWS Organizations

Central management for multiple AWS accounts

AWS Organizations enables you to centrally manage and consolidate all of your AWS accounts in the AWS Cloud.

Create an organization to manage multiple AWS accounts. Learn more

Pricing

There is no cost to use AWS Organizations.

About

AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Using

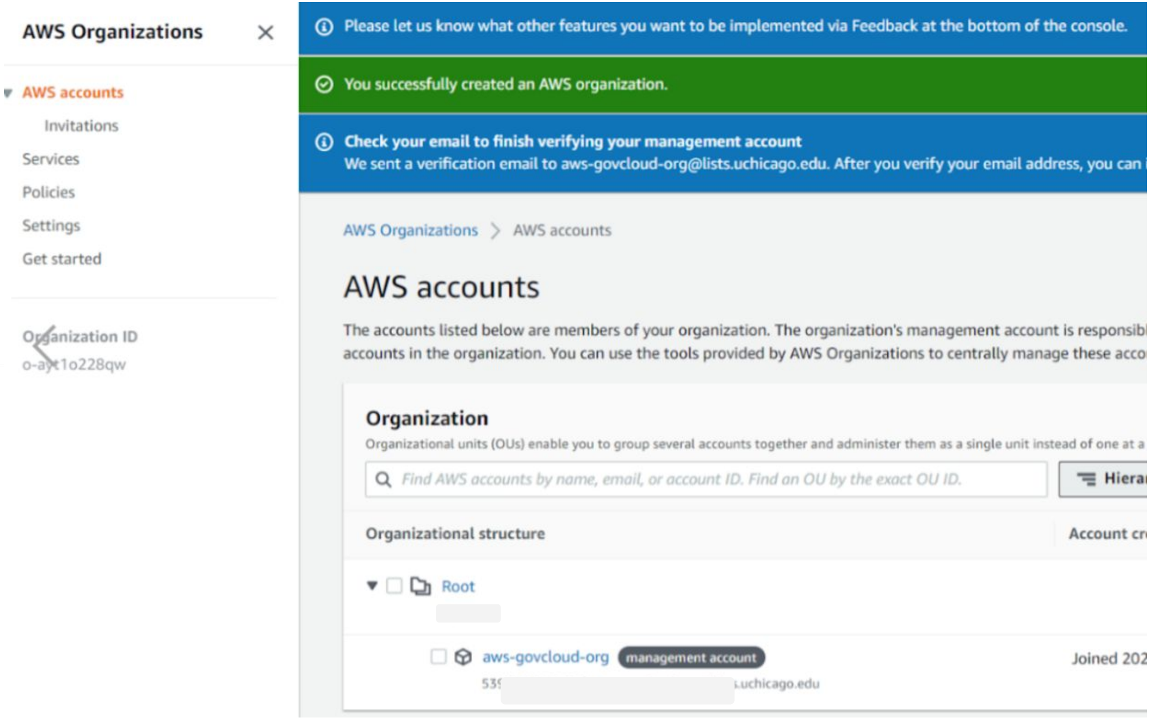
AWS GovCloud

Now you have a GovCloud Organization with a management account

Request future GovCloud accounts the same way, if *you* manage the administrator account. (Don't do step 10 - create org)

Thank you

shelley@uchicago.edu



AWS Organizations ×

▾ AWS accounts

Invitations

Services

Policies

Settings

Get started

Organization ID

o-ayt1o228qw

ⓘ Please let us know what other features you want to be implemented via Feedback at the bottom of the console.

✓ You successfully created an AWS organization.

ⓘ **Check your email to finish verifying your management account**
We sent a verification email to aws-govcloud-org@lists.uchicago.edu. After you verify your email address, you can i

AWS Organizations > AWS accounts

AWS accounts

The accounts listed below are members of your organization. The organization's management account is responsibl
accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these acco

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a

Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.

Hiera

Organizational structure | Account cr

▾ □ Root
[redacted]

□ aws-govcloud-org management account Joined 202
53[redacted].uchicago.edu