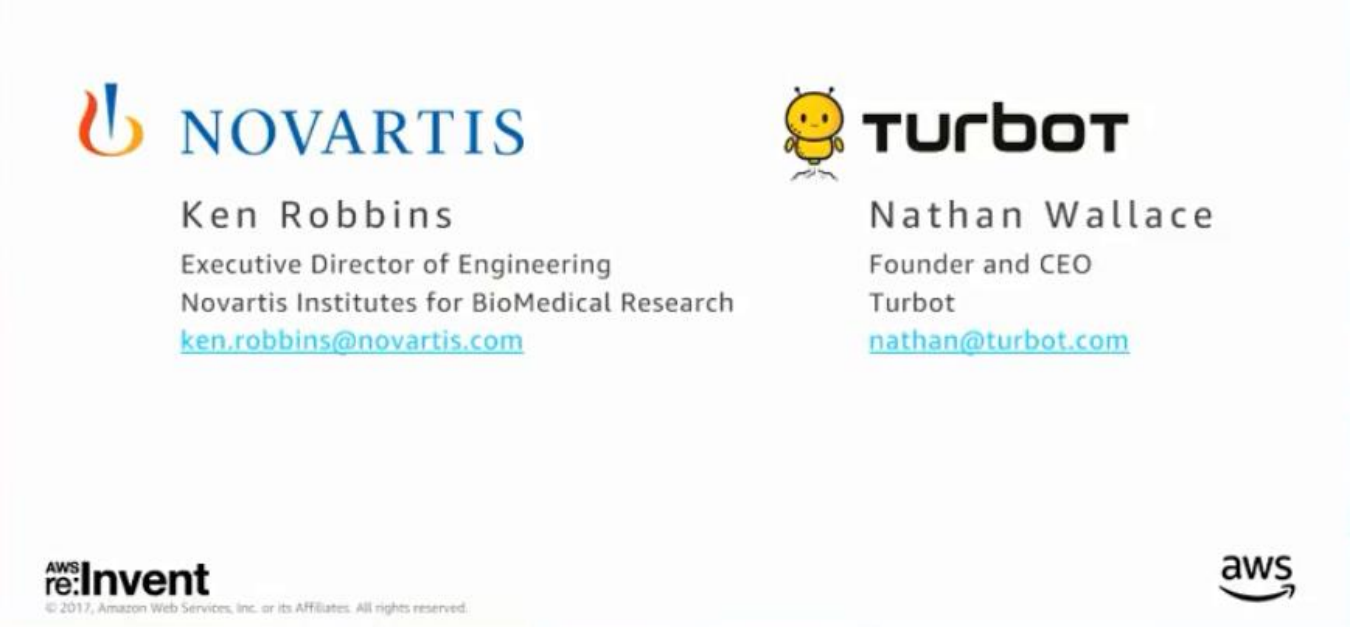
Implementing stringent security and compliance controls, like GxP, across your enterprise cloud ecosystem, while ensuring the agility of the DevSecOps process requires significant expertise and a lot of time to design, build, and maintain custom operations tooling. In this session, you learn how Turbot used AWS services to simplify IT operations to provide continuous compliance to major life sciences customers. You also hear how life sciences companies like Novartis Institutes for Biomedical Research (NIBR) have become agile, ensured control, and automated best practices using automated policy controls to configure, monitor, and maintain their cloud resources. By doing this, they became more supportive of their researchers' application stack. You also learn how data scientists and core researchers can take advantage of the power of DevOps and cloud computing without compromising enterprise security or data protection requirements.



Novartis Institutes for BioMedical Research (NIBR)

Drug discovery and early development

~6,000 Scientists

~400
Research projects

~90
New Molecular Entities

- Autoimmunity, Transplantation & Inflammation
- Cardiovascular & Metabolism
- Infectious Diseases
- Musculoskeletal
- Neuroscience
- Ophthalmology
- Oncology
- Immuno-Oncology
- Respiratory Diseases

Our technical ecosystem

300 engineers

400 informaticians

400 supported apps

Bleeding edge + legacy

Many apps
under-the-radar

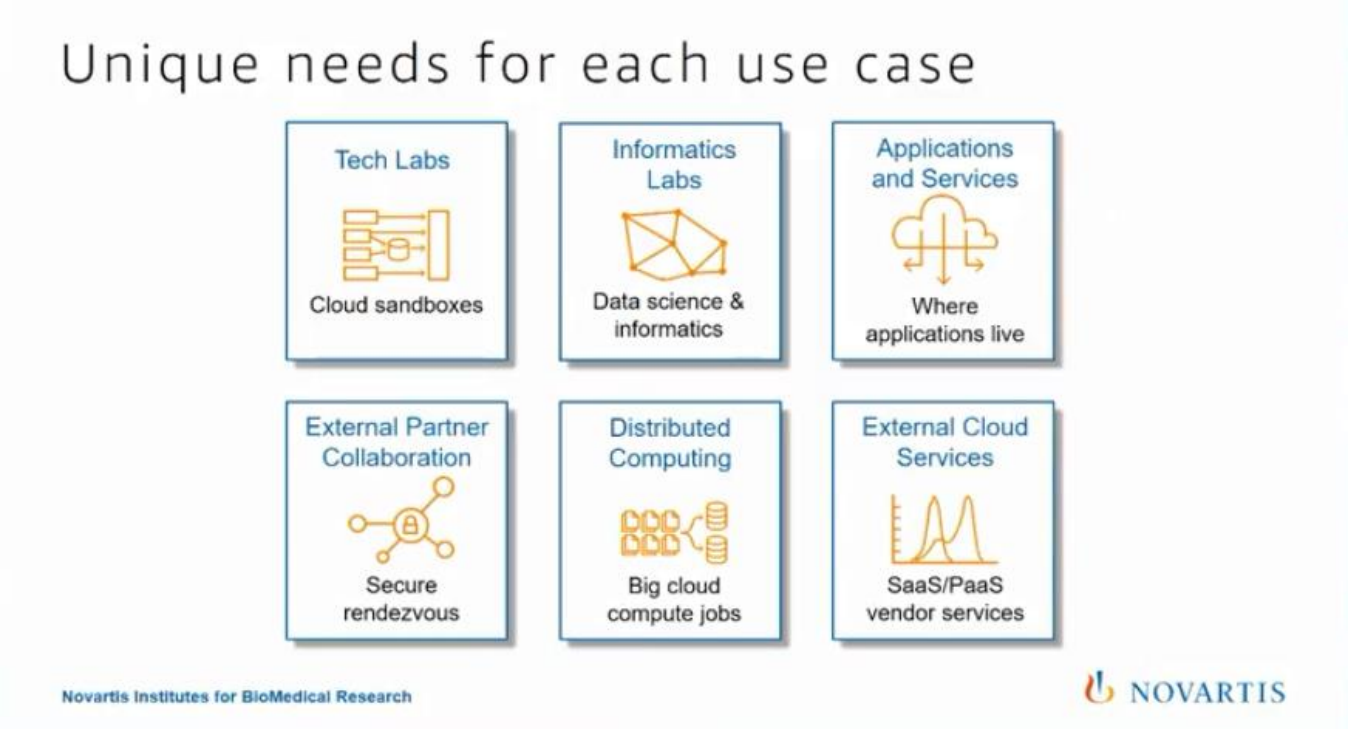
40 PB
↗ 30% YOY

Novartis Institutes for BioMedical Research

NOVARTIS

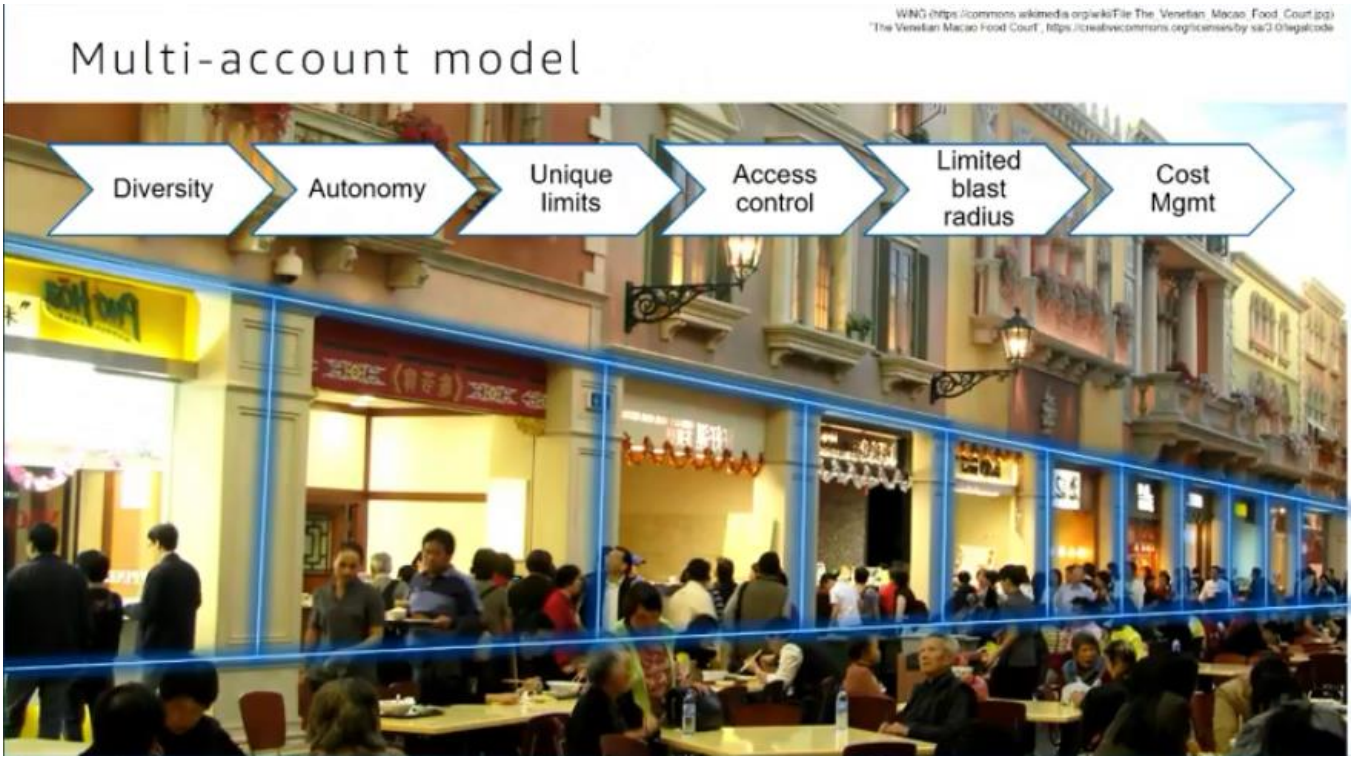
How can we achieve **agility** and **velocity** across a **broad range of needs** while **ensuring control**?

How do we keep up with the science and accelerate direct discovery in the face of this constant change, complexity, diversity and also keep control and diversity in our stacks.

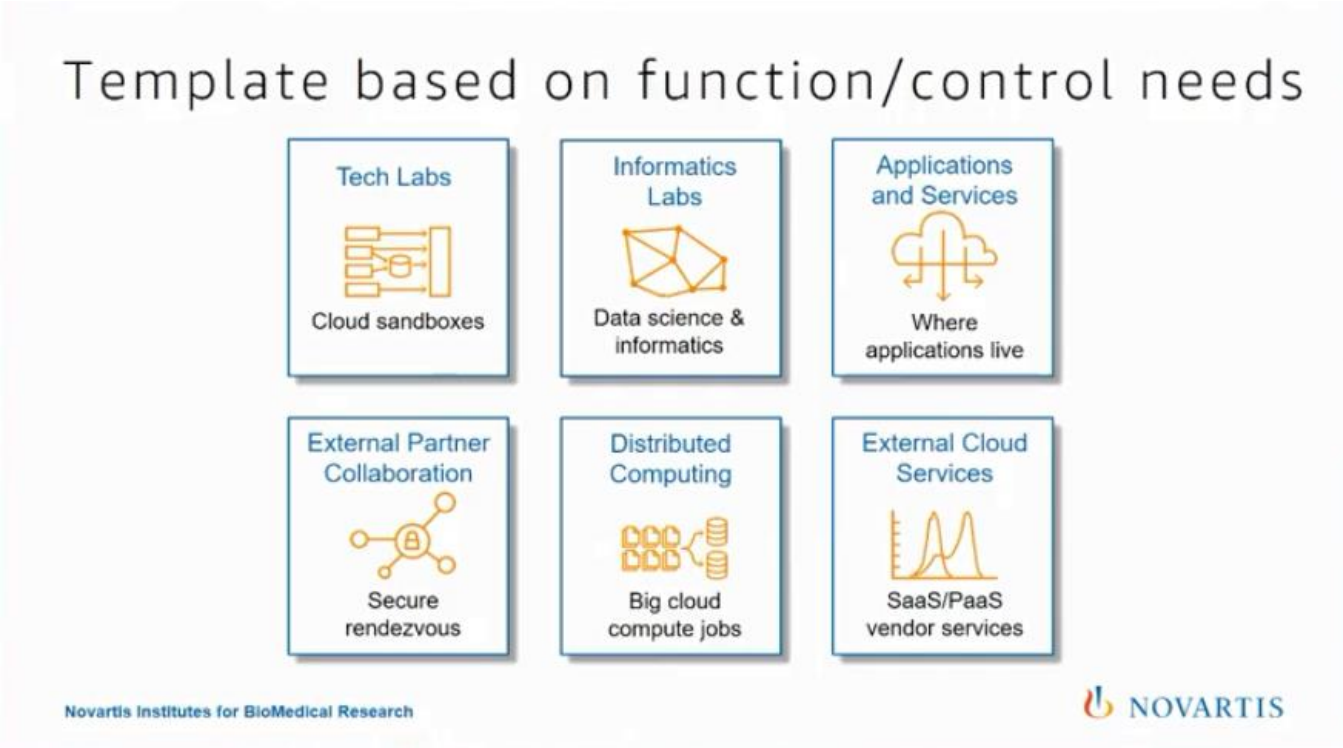


We clustered our apps into 6 fundamental use cases and environments that mattered to us. We are using unique template and boundary

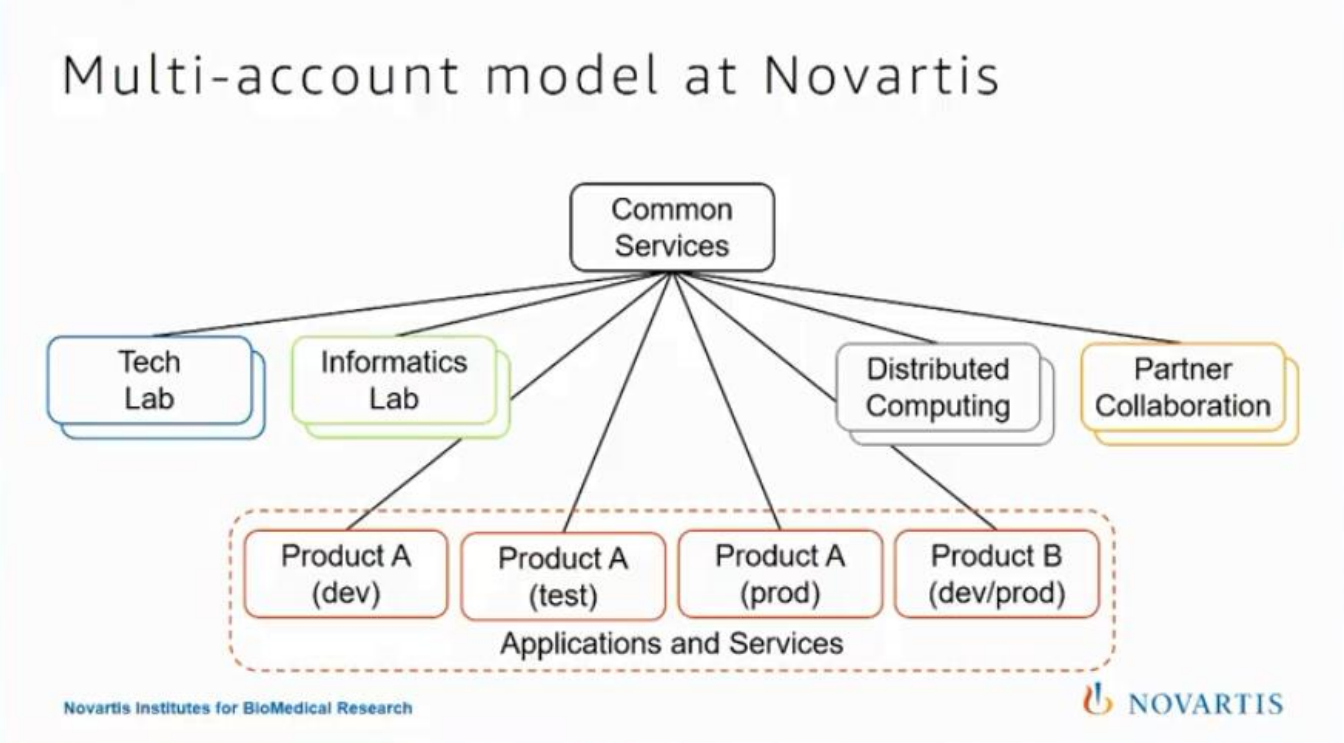
How can we achieve policy control and access management across a vast number of accounts? We thus opted for the single account model having a few accounts like Dev, Test, Prod, an account is a pool of different workloads in it. But this model had problems like who is going to write the IAM Policies for the workloads, what tagging standards to use, etc.



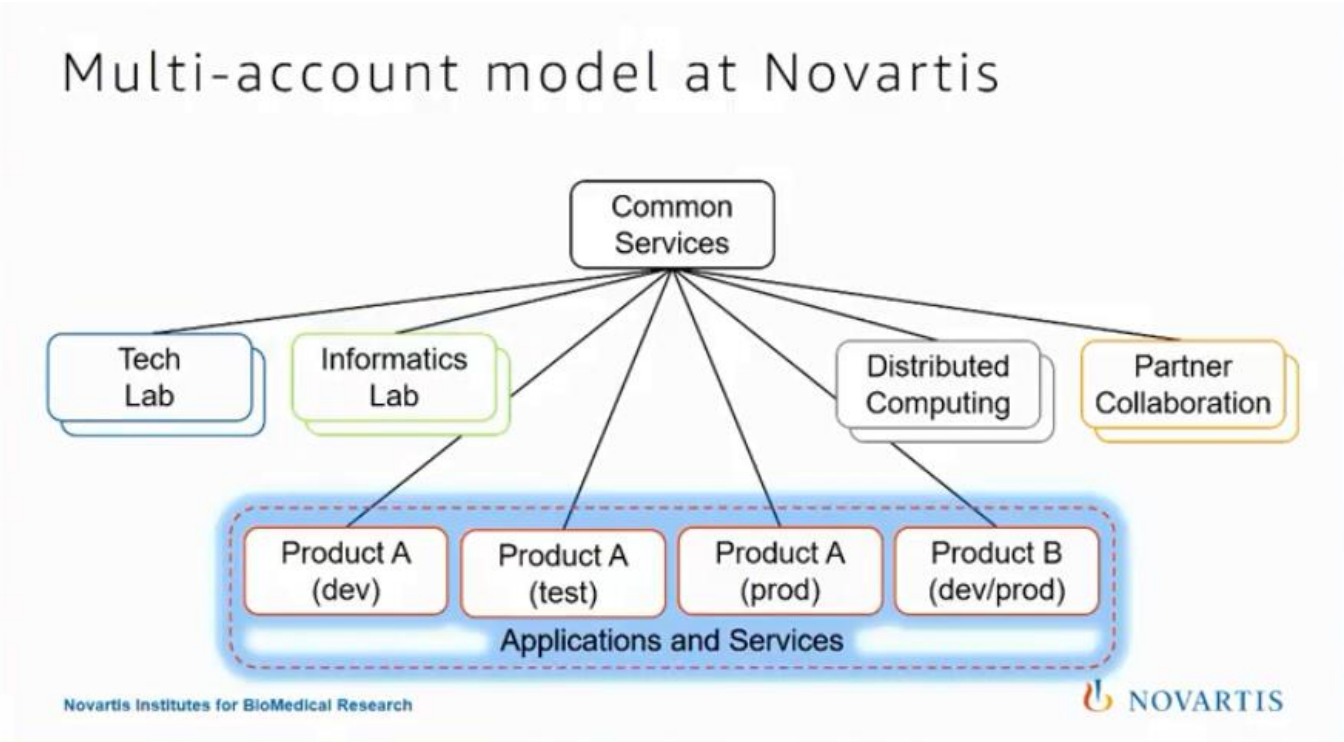
Each restaurant has their own menu, team, cuisine, food supply, etc. the different restaurants are also independent. We can just create a new account every time and give the account its own autonomy. We can also enforce unique limits at the account level and grant each account their own individual resources. We can also give access control per workload for that account vertically to needed managed services and applications. We can also know how much each account is costing by seeing their own invoice across all resources using tags.



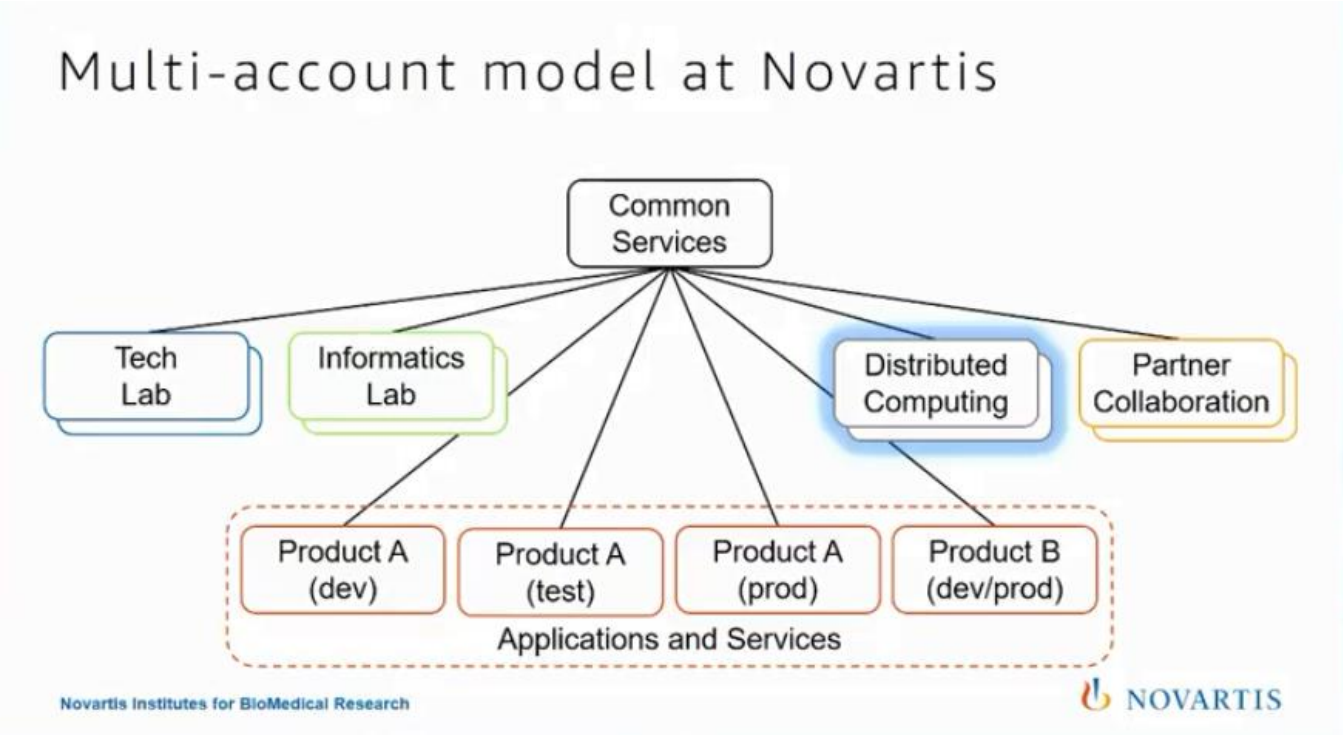
Let us see how we take the use cases and map them to a multi account model



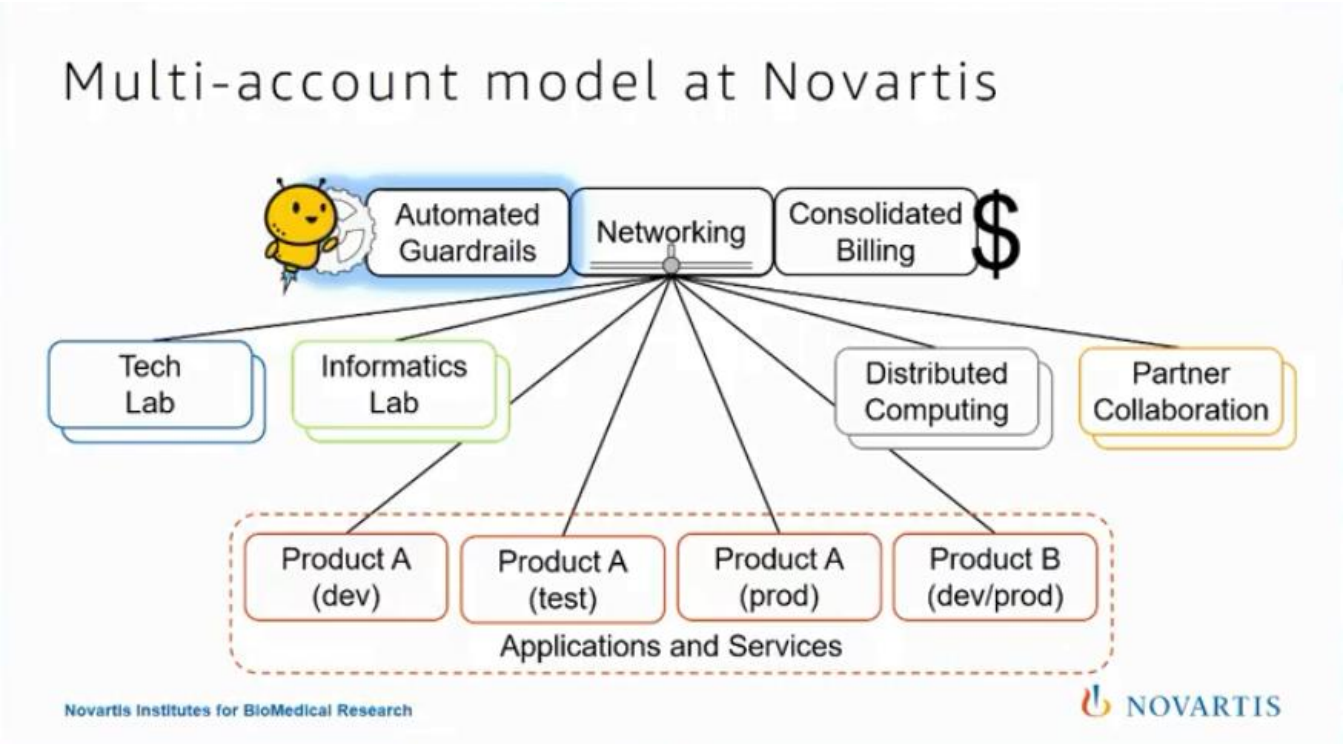
Tech lab has about 30 different accounts, there is a template that says how to build a Tech Lab infrastructure, and there is a set of policy controls for a tech lab. Also, for the other services.

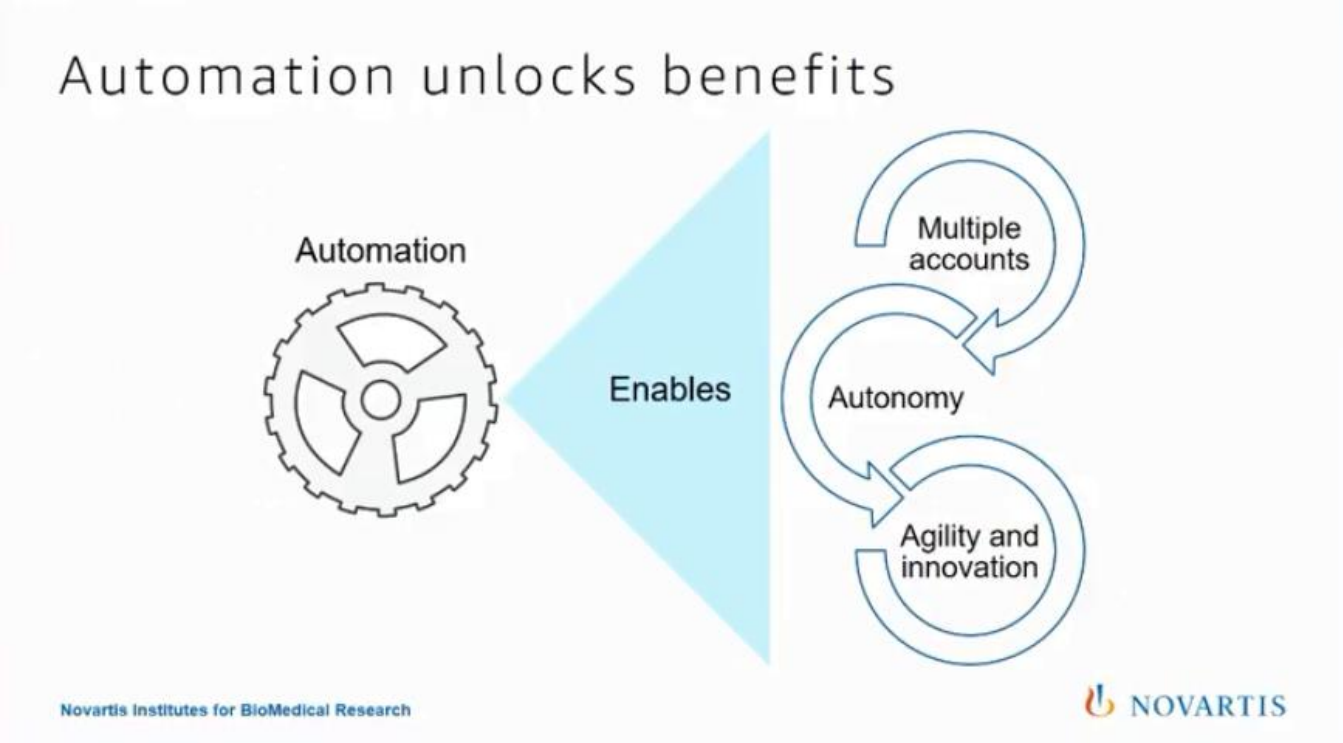


The vast applications and services get separate discrete accounts of Dev, Test, and Prod for each different service team.



Distributed Computing accounts do mostly scheduled jobs and needs a large IP space





We use the account as a container model that enables teams to be agile and innovative via automation using TurBot. We needed to automate the compliance and control guard rails for the accounts and remove all manual processes to keep the agility fast.

Each application now has network isolation, access control, and its own change management

Ride the rocket

Lesson 2

Do not abstract or compete

AWS speed is your advantage

Focus on enabling your business

Unlock the power of open

Do not abstract a new interface to do things that AWS already does for you easily, just use the AWS APIs.

Teach, don't do

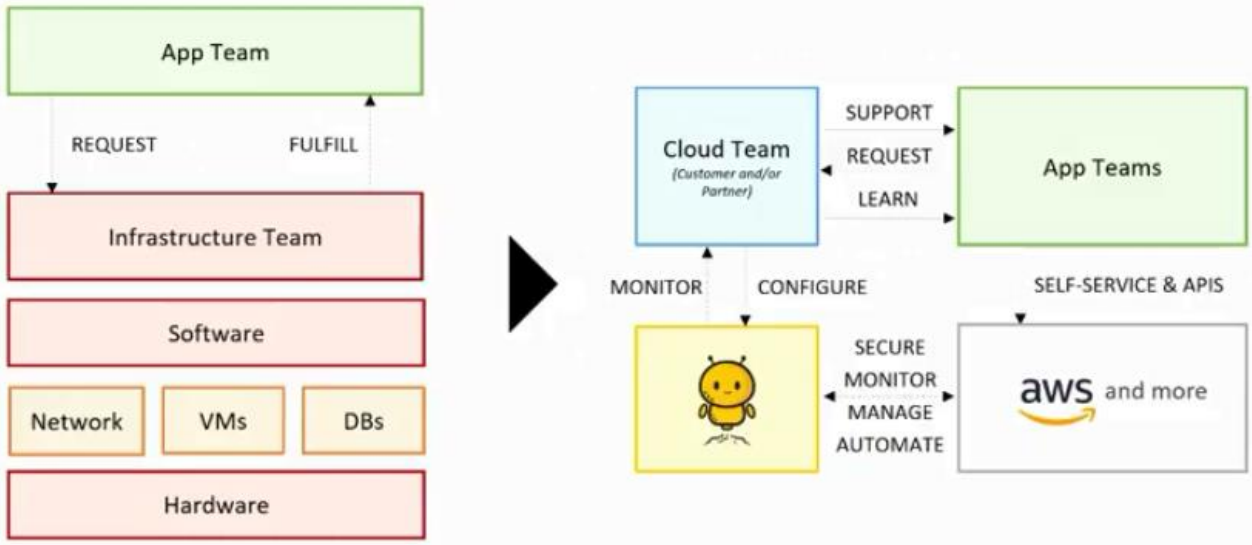
Lesson 3

Avoid being a bottleneck

Eliminate the cycle of blame

Leverage public tutorials and answers

(You can't do it in real-time anyway!)



Policies

Lesson 4

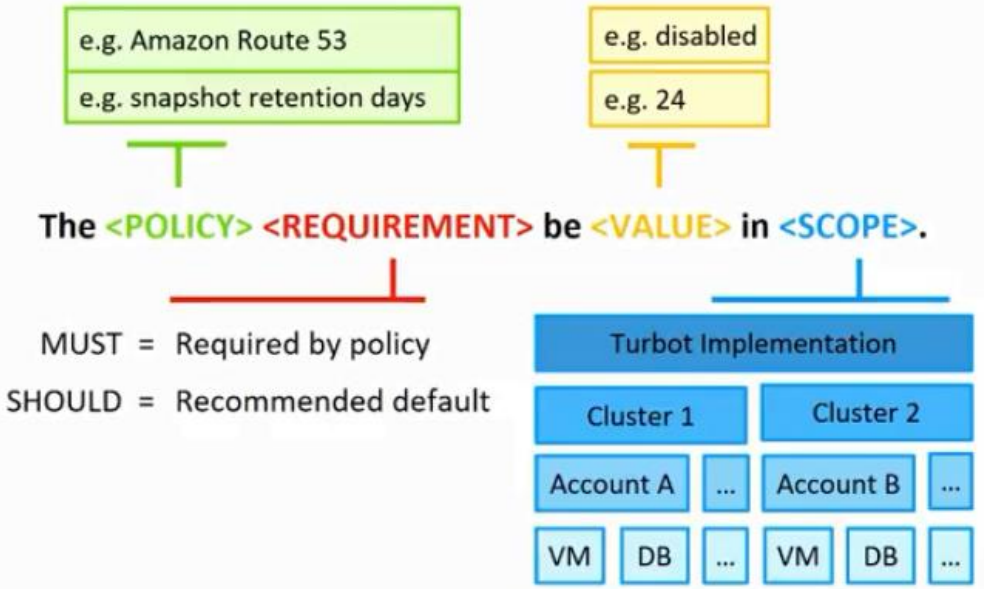
Simple rules behind the controls

Policy (MUST) or recommend (SHOULD)

Full automation requires a lot of policies

There are always exceptions!

Use exceptions to experiment and learn



turbot | aws

Learn by doing

Lesson 5

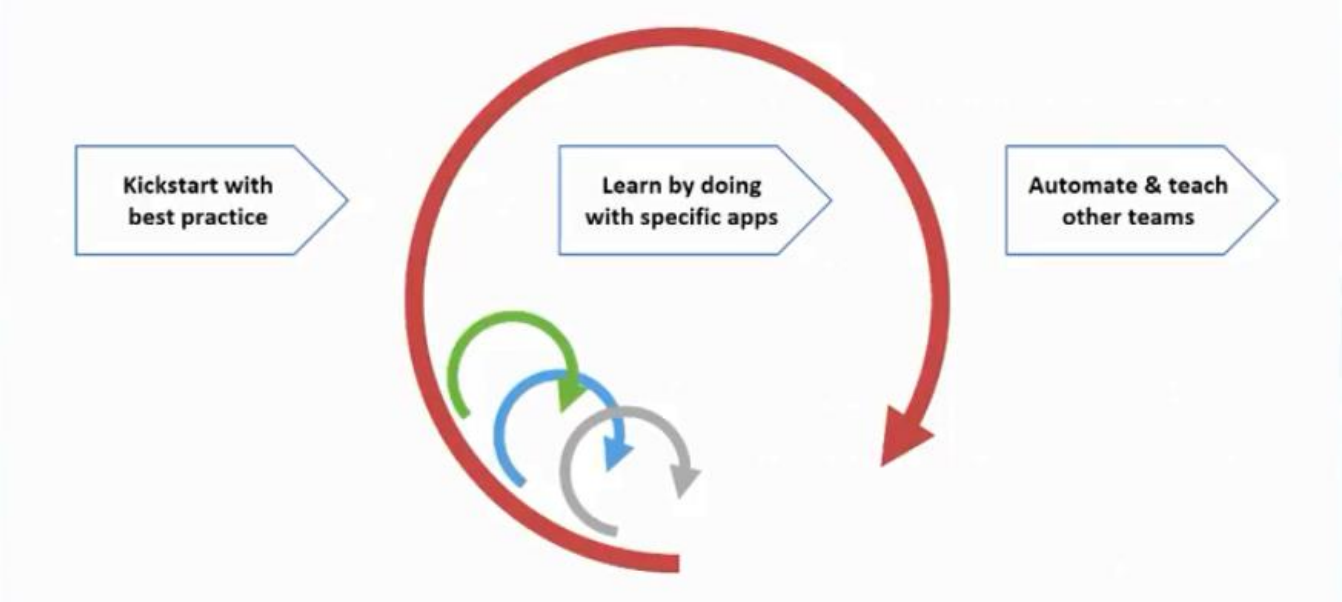
Experiment within blast radius

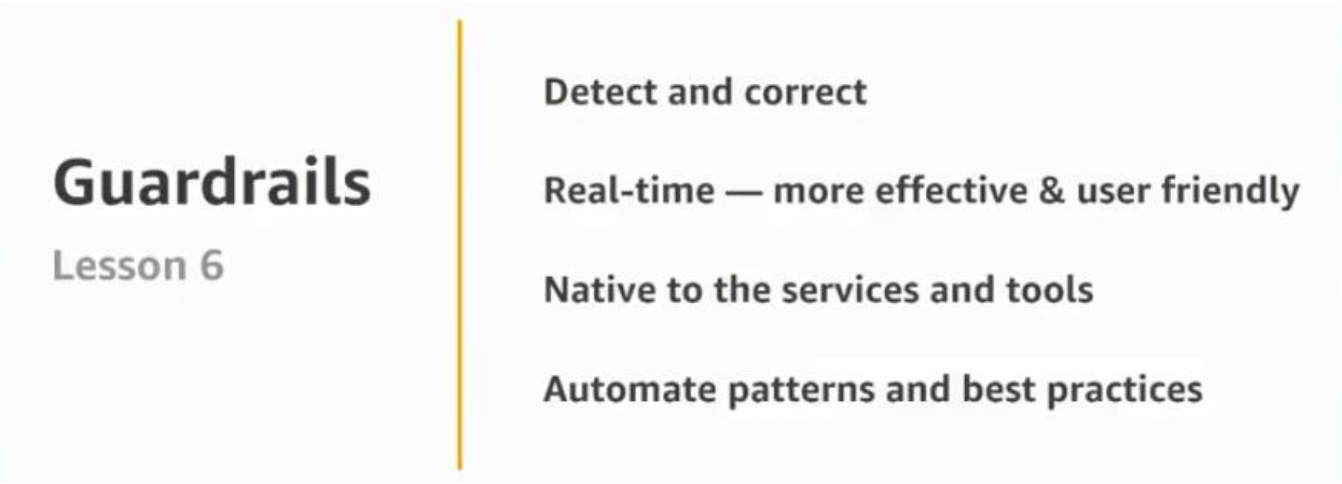
Use exceptions and limited

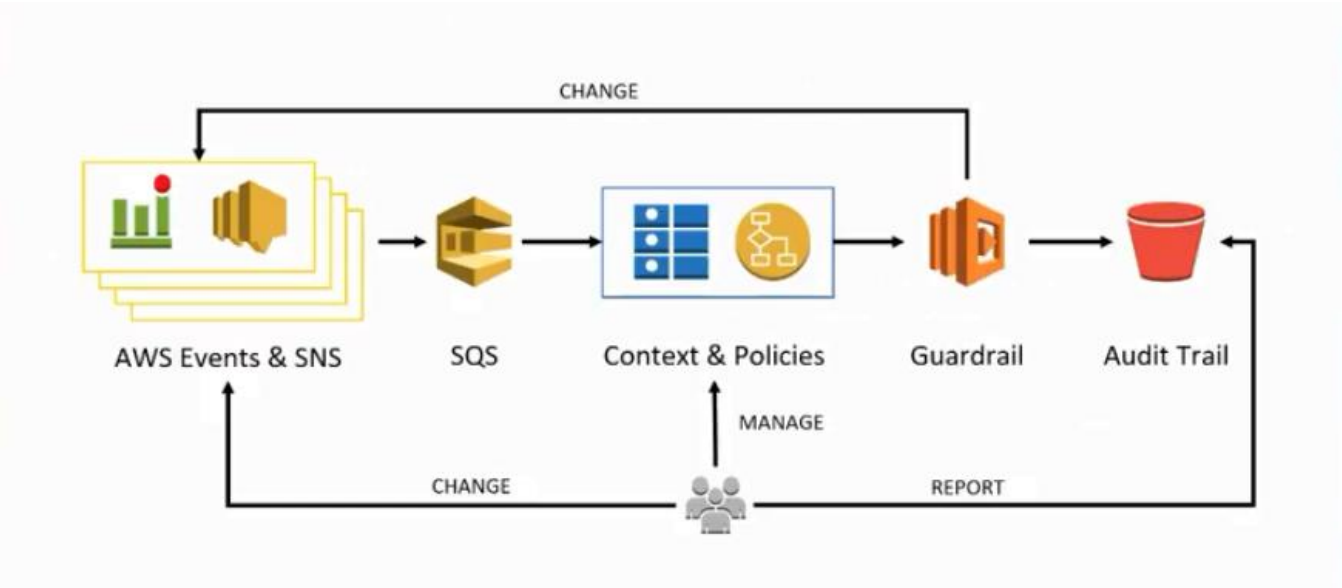
SuperUser

Collaborate on new services

Hand-build > pattern > automation





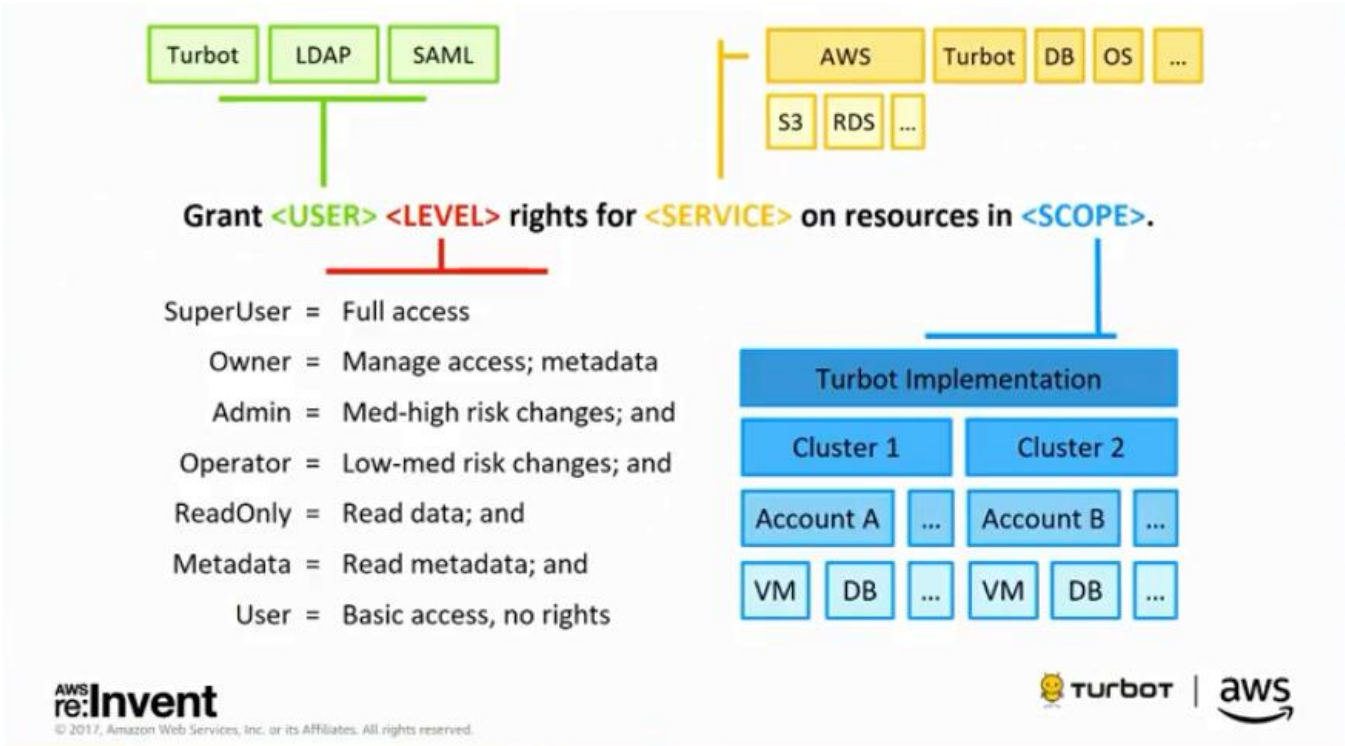


This is the basic pattern for a guardrail. You want to get to a place where you have context to test the condition and use the guard rail to implement the change to the instance, bucket or environment if they are not in compliance.

Patterns at scale

Lesson 7

- Use common language and models
- Automate and repeat patterns
- Avoid custom central services
- Learn and enhance patterns over time
- Accelerate, don't constrain, teams

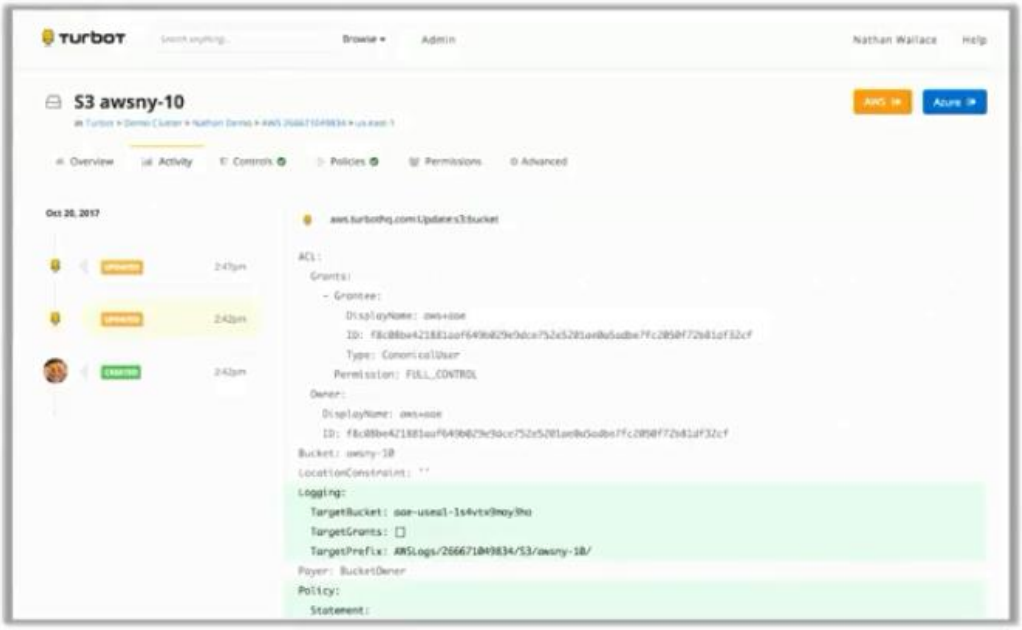


This is an example for IAM

Visibility

Lesson 8

- Audit trail for security and compliance
- Change history to understand behavior
- Review actual configuration, not docs
- Detailed logs for trouble-shooting



You need to give visibility to the users so that they know what happened or is happening

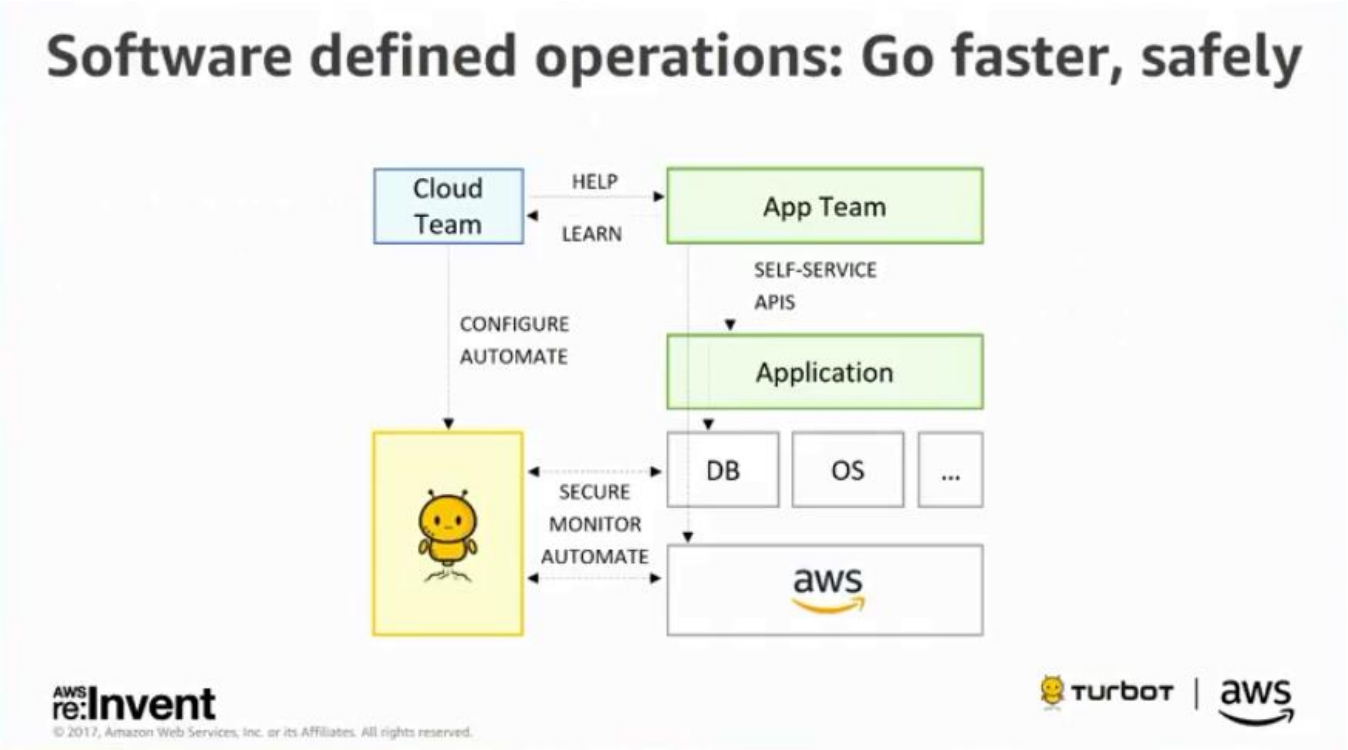
Automate³!

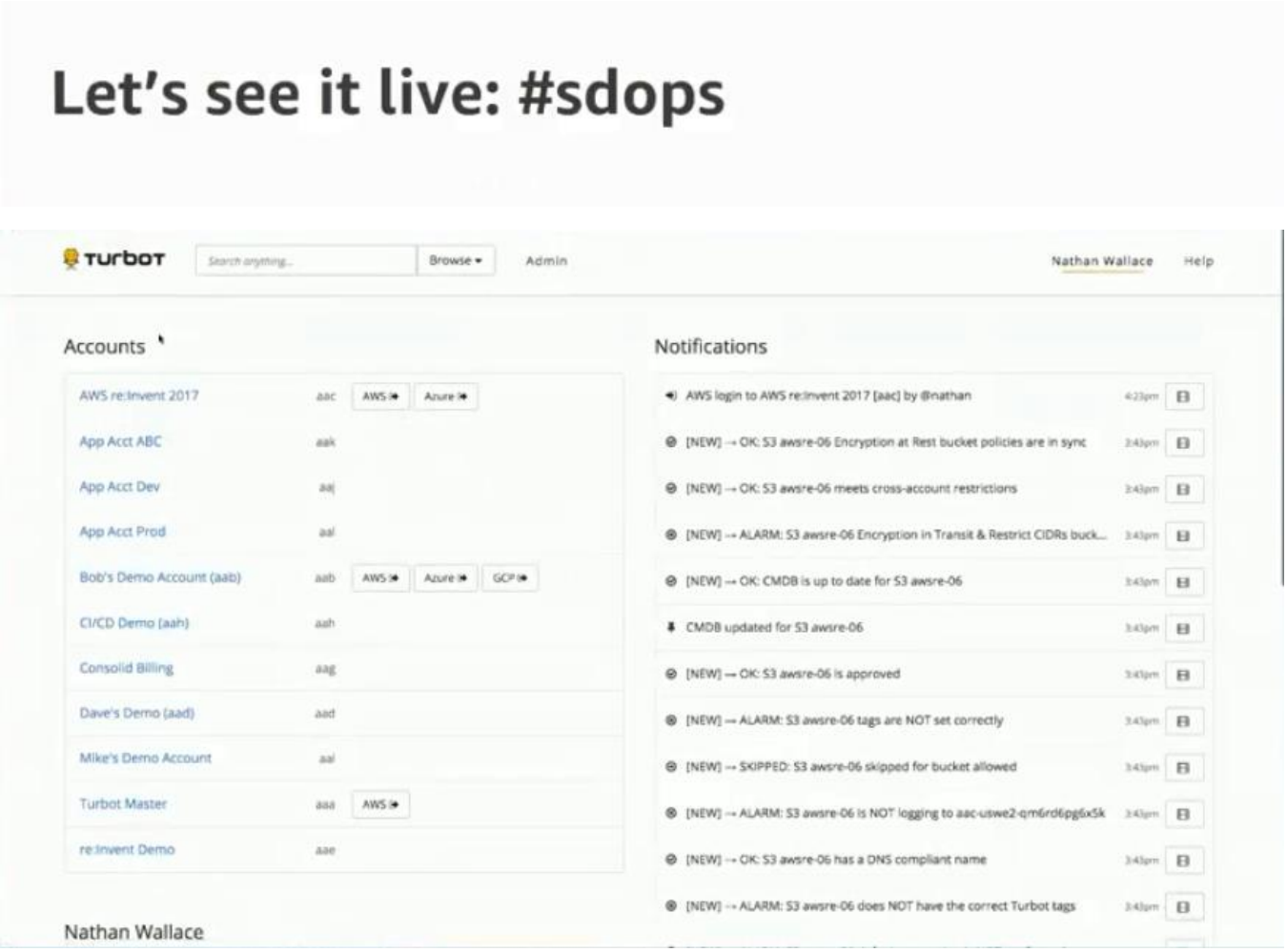
Lesson 9

Kill the ticket

Automate all level 1-2 responses

Invest to elevate and remain agile





This is an example of a Turbot environment that implements a number of automated guard rails.

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

AWS re:Invent 2017 aac

in Turbot > Demo Cluster

AWS | Azure | GCP

Overview | Activity | Controls | Policies | Permissions | Organization | Advanced

- Turbot
- Demo Cluster

AWS re:Invent 2017

AWS
- AWS 831304522281

Azure
- Azure dev-cody-demo

GCP
- GCP cody-dev-demo

Turbot
- Abc RG

H AWS re:Invent 2017

Demo > Yes

831304522281

$121.61

aws | Services | Resource Groups | nathan @ 8313-0452-2281 | Oregon | Support

AWS services

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Recently visited services

- IAM
- S3
- EC2
- CloudWatch
- Simple Queue Service

All services

Build a solution

Get started with simple wizards and automated workflows.

- Launch a virtual machine — With EC2 or Lightsail ~1-2 minutes
- Build a web app — With Elastic Beanstalk ~6 minutes
- Host a static website — With S3, CloudFront, Route 53 ~5 minutes
- Connect an IoT device — With AWS IoT ~5 minutes
- Start a development project — With CodeStar ~5 minutes
- Register a domain — With Route 53 ~3 minutes

See more

Learn to build

See all

Helpful tips

Manage your costs

Get real-time billing alerts based on your cost and usage budgets. Start now

Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts. Start now

Explore AWS

Amazon Relational Database Service (RDS)

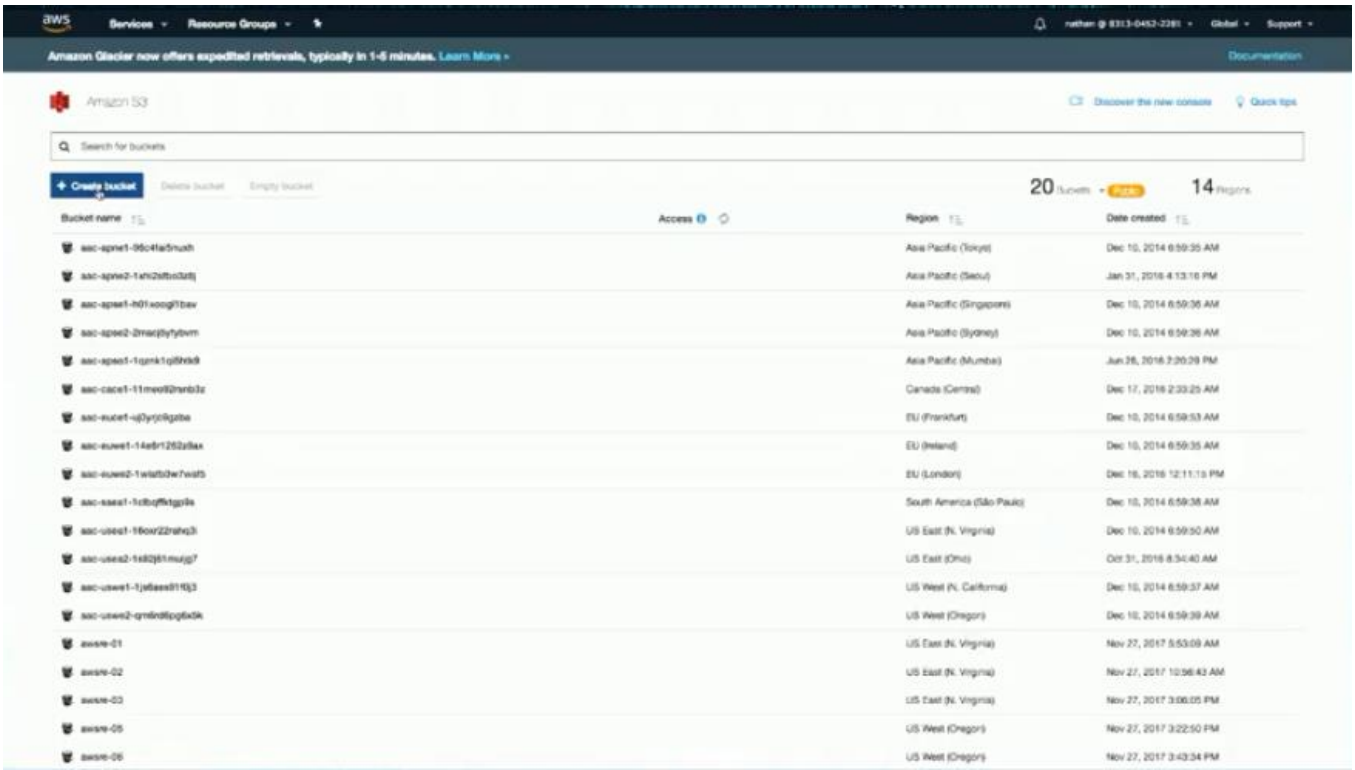
RDS manages and scales your database for you. RDS supports Aurora, MySQL, PostgreSQL, MariaDB, Oracle, and SQL Server. Learn more.

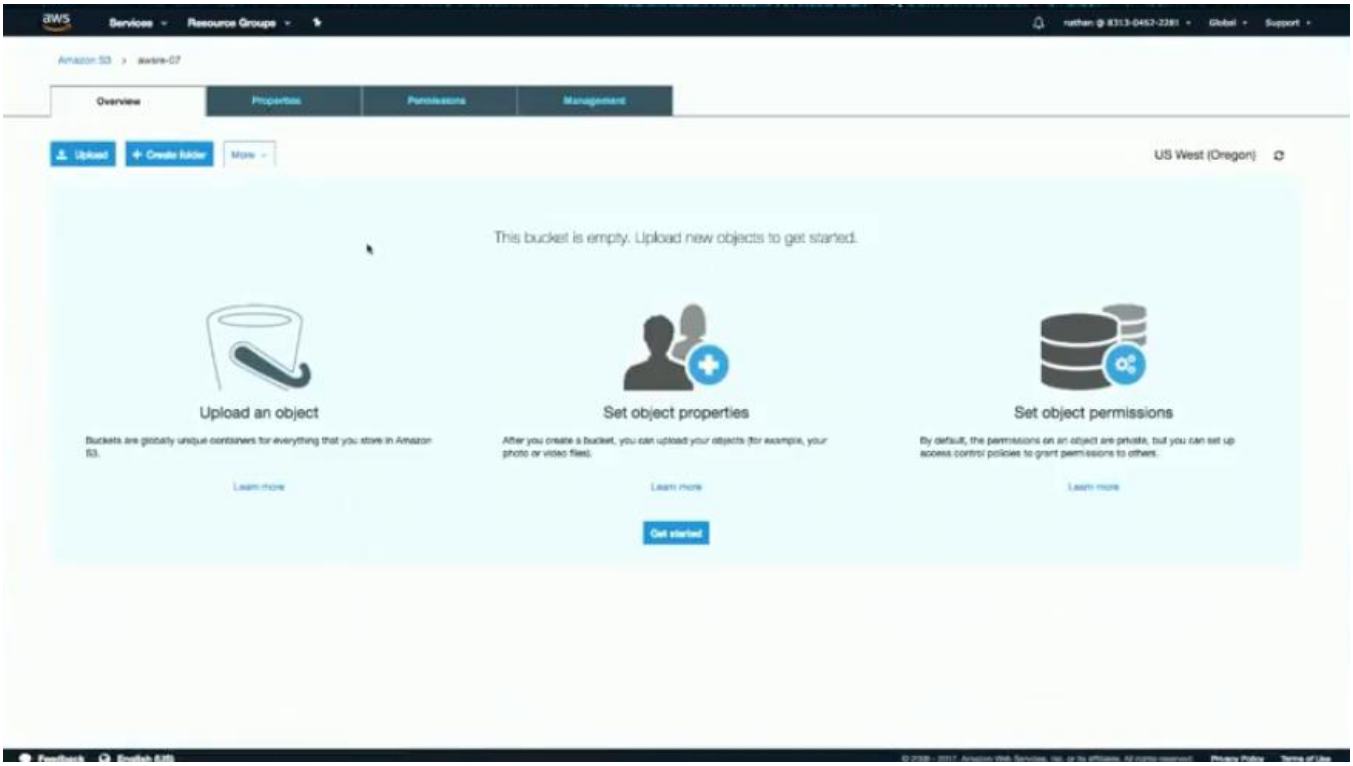
Real-Time Analytics with Amazon Kinesis

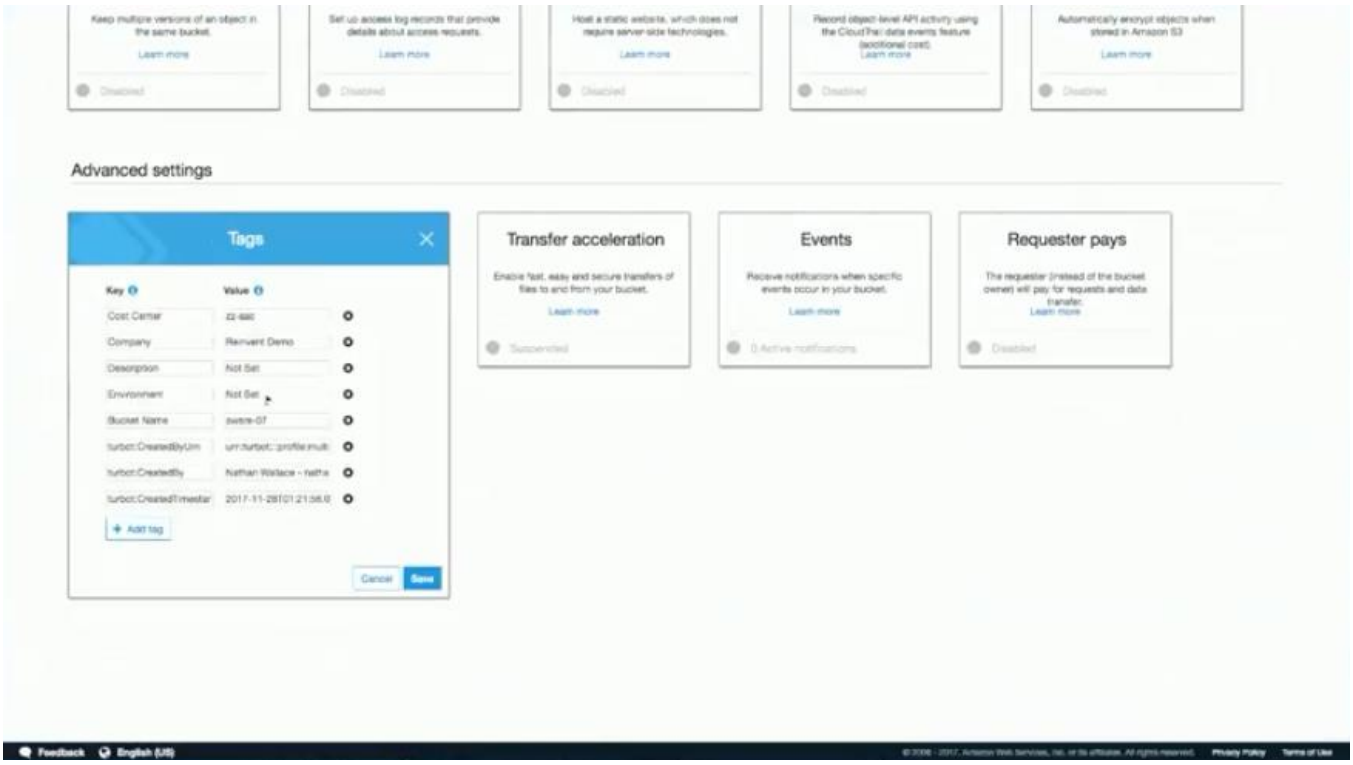
Stream and analyze real-time data, so you can get timely insights and react quickly. Learn more.

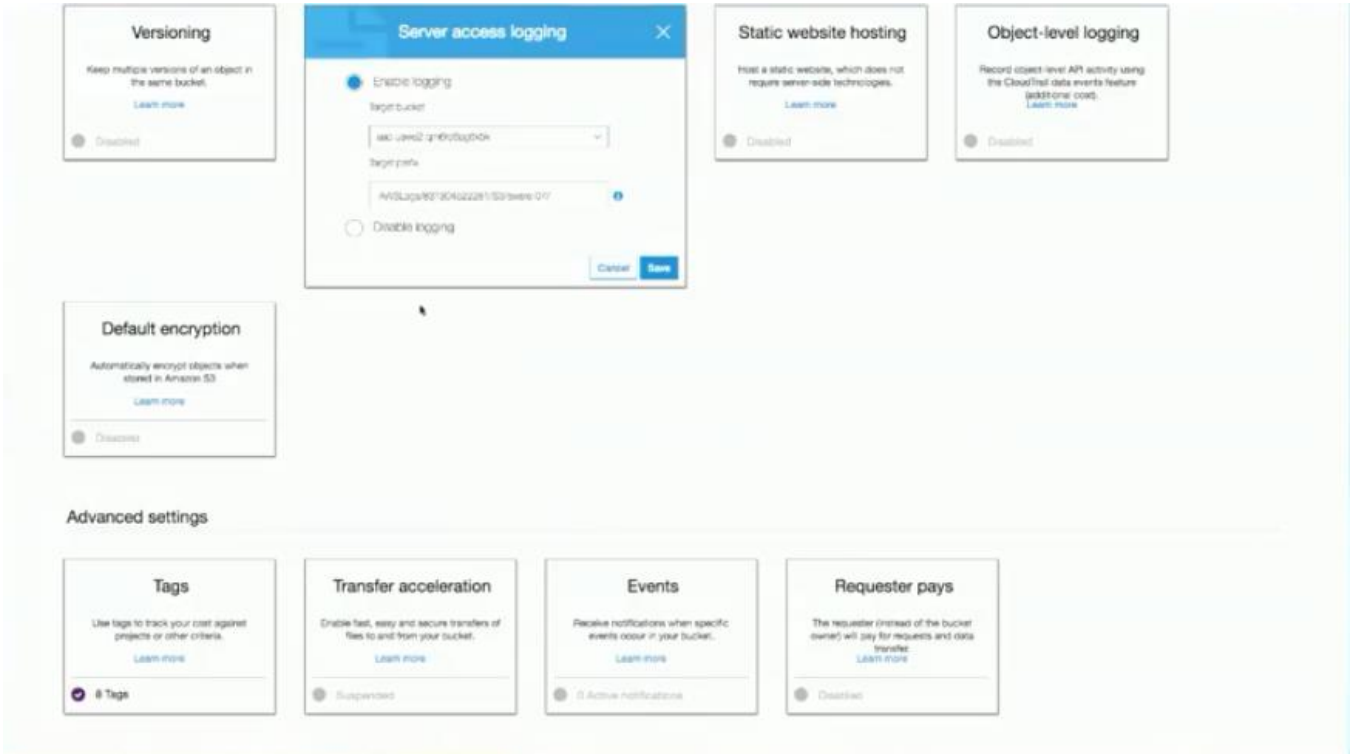
Get Started with Containers on AWS

Amazon ECS helps you build and scale containers for any


Services
Resource Groups
Amazon Glacier now offers expedited retrievals, typically in 1-5 minutes. Learn More
Documentation
Amazon S3
Discover the new console
Quick tips
Search for buckets
Create bucket
Delete bucket
Empty bucket
20 Buckets
14 Regions
Bucket name
Access
Region
Date created
Asia Pacific (Tokyo)
Asia Pacific (Seoul)
Asia Pacific (Singapore)
Asia Pacific (Sydney)
Asia Pacific (Mumbai)
Canada (Central)
EU (Frankfurt)
EU (Ireland)
EU (London)
South America (São Paulo)
US East (N. Virginia)
US West (N. California)
US West (Oregon)
awsre-01
awsre-02
awsre-03
awsre-05
awsre-06


Services
Resource Groups
Amazon S3 > awsre-07
Overview
Properties
Permissions
Management
Upload
Create folder
More
US West (Oregon)
This bucket is empty. Upload new objects to get started.
Upload an object
Buckets are globally unique containers for everything that you store in Amazon S3.
Learn more
Set object properties
After you create a bucket, you can upload your objects (for example, your photo or video files).
Learn more
Get started
Set object permissions
By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.
Learn more


Advanced settings
Tags
Key
Value
Cost Center
Company
Reinvent Demo
Description
Not Set
Environment
Not Set
Bucket Name
Add tag
Cancel
Save
Transfer acceleration
Events
Requester pays


Versioning
Server access logging
Enable logging
Disable logging
Cancel
Save
Static website hosting
Object-level logging
Default encryption
Advanced settings
Tags
Transfer acceleration
Events
Requester pays

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

AWS re:Invent 2017 aac

in Turbot > Demo Cluster

AWS | Azure | GCP

Overview | Activity | Controls 2 | Policies | Permissions | Organization | Advanced

- Turbot
- Demo Cluster

AWS re:Invent 2017

AWS
- AWS 831304522281

Azure
- Azure dev-cody-demo

GCP
- GCP cody-dev-demo

Turbot
- Abc RG

CREATED S3 awsre-07

ACTION REQUIRED: **2 Controls**

AWS re:Invent 2017	831304522281
Demo > Yes	$121.61

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

Filter | level:self,descendant state:alarm,error,ok | Labels

Labels | State | Levels | Sort

- S3 awsre-07 default encryption is NOT configured correctly 5:23pm
  in ALARM since 5:22pm
- CMDB is up to date for S3 awsre-07 5:22pm
  in OK since 5:22pm
- S3 awsre-07 meets cross-account restrictions 5:22pm
  in OK since 5:22pm
- S3 awsre-07 Encryption at Rest bucket policies are in sync 5:22pm
  in OK since 5:22pm
- S3 awsre-07 meets anonymous access restrictions 5:22pm
  in OK since 5:22pm
- S3 awsre-07 has a DNS compliant name 5:22pm
  in OK since 5:22pm
- S3 awsre-07 is approved 5:22pm
  in OK since 5:22pm
- S3 awsre-07 has the correct Turbot tags 5:22pm
  in OK since 5:22pm

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

S3 awsre-07

in Turbot > Demo Cluster > AWS re:Invent 2017 > AWS 831304522281 > us-west-2

AWS | Azure | GCP

Overview | Activity | Controls 1 | Policies | Permissions | Advanced

S3 awsre-07 tags are set correctly

OK

Log | Check | Apply

5:22pm

```
The S3 bucket:

    awsre-07
    urn:turbot:dev:aac:aws:831304522281:us-west-2:s3:awsre-07

in the account:

    AWS re:Invent 2017 [aac]
    urn:turbot:dev:aac

has tags set correctly.
```

Notifications

- ALARM → OK: S3 awsre-07 tags are set correctly — 5:22pm
- S3 awsre-07 tags updated — 5:22pm
- [NEW] → ALARM: S3 awsre-07 tags are NOT set correctly — 5:22pm

Bucket Tags

Check the S3 bucket tags include tags defined in S3 > Bucket Tags Template.

BucketTags
urn:turbot:::guardrail:S3:BucketTa...

aws/s3/bucket
infrastructure/tag

aws:s3:bucket

tick.turbothq.com:EveryDay
s3.amazonaws.com:CreateBucket
s3.amazonaws.com:DeleteBucket...
s3.amazonaws.com:PutBucketTag...
options.turbothq.com:S3:BucketT...
options.turbothq.com:S3:BucketT...

Turbot
Demo Cluster
AWS re:Invent 2017
AWS 831304522281

TERMINATED @ 2017-11-27 17:22:12

Process	urn:turbot:dev:aac:process:faeb4497-fba2-4bcf-90b9-47cc218da207
Context	urn:turbot:dev:aac:aws:831304522281:us-west-2:s3:awsre-07
Handler	urn:turbot:::guardrail:S3:BucketTags

Log | Event | Context | Files | DEBUG


```
▼ Object
  processUrn: "urn:turbot:dev:aac:process:faeb4497-fba2-4bcf-90b9-47cc218da207"
  contextUrn: "urn:turbot:dev:aac:aws:831304522281:us-west-2:s3:awsre-07"
  resourceUrn: "urn:turbot:dev:aac:aws:831304522281:us-west-2:s3:awsre-07"
  handlerId: "52c31ecd285a54da7a4d2048faec82e8"
  handlerUrn: "urn:turbot:::guardrail:S3:BucketTags"
  handlerTimestamp: "2017-11-28T01:22:06.153Z"
  ▶ detail: Object
  eventId: "0d842598-5e5e-41fc-82b0-2d89a96cb050"
  timestamp: "2017-11-28T01:22:04.935Z"
  version: "Turbot/v2.8.0"
  type: "s3.amazonaws.com:CreateBucket"
  id: "faeb4497-fba2-4bcf-90b9-47cc218da207"
  actorUrn: "urn:turbot:::profile:multi:nathan@turbot.com"
  eventTimestamp: "2017-11-28T01:21:56.000Z"
```


Check | Apply | OK

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

S3 awsre-07

in Turbot > Demo Cluster > AWS re:Invent 2017 > AWS 831304522281 > us-west-2

AWS | Azure | GCP

Overview | Activity | Controls 1 | Policies | Permissions | Advanced

Filter | filter:important | Labels | New Setting | Export CSV

Labels | Levels | Sort

Application > S3 > ACL Management
`Disabled` required by Turbot.

Application > S3 > Access Logging
`Enforce: Enabled to Turbot logs` required by Turbot.

Application > S3 > Access Logging Management
`Disabled` is the default.

Application > S3 > Anonymous Access
`Enforce: Explicitly deny invalid bucket policy statements` required by Turbot.

Application > S3 > App Enabled
`Enabled` recommended by Demo Cluster.

Application > S3 > Bucket Allowed - Deprecated

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

Application > S3 > Cross-Account Access
`Enforce: Deny cross-account access except from S3 > Trusted Accou…` required by Turbot.

Application > S3 > DNS Compliant Bucket Name
`Enforce: Delete invalid bucket if new and empty` required by Turbot.

Application > S3 > Encryption at Rest
`Enforce: AWS SSE or higher` required by AWS re:Invent 2017.

Application > S3 > Encryption at Rest KMS Key ID Template
`{{ "KMS:DefaultKeyID" | policy }}` is the default.

Application > S3 > Encryption in Transit
`Enabled` required by Turbot.

Application > S3 > Restrict to CIDRs
`["0.0.0.0/0"]` is the default.

Application > S3 > Rights
`Enforce: Enabled if S3 > App Enabled` is the default.

Application > S3 > Trusted Accounts
`[{"Turbot::Include":"Turbot:Collaboration:TrustedAccounts"}]` is the default.

Application > S3 > Versioning
`Skip` required by AWS re:Invent 2017.

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

S3 awsre-07

in Turbot > Demo Cluster > AWS re:Invent 2017 > AWS 831304522281 > us-west-2

AWS | Azure | GCP

Overview | Activity | Controls | Policies | Permissions | Advanced

S3 > Versioning

EXCEPTION

Enforce: Enabled

Edit | Delete

Active Policy

How is the Active Policy calculated?

	Default	Skip
	Turbot	~~Enforce: Enabled~~
-	Demo Cluster	
	AWS re:Invent 2017	~~Skip~~
-	AWS 831304522281	
-	us-west-2	
	S3 awsre-07 EXCEPTION	ACTIVE **Enforce: Enabled**

Descendant Settings

S3:Versioning

Check if an S3 bucket has versioning enabled.

aws/s3/bucket

aws:s3:bucket

Turbot

Demo Cluster

AWS re:Invent 2017

AWS 831304522281

us-west-2

S3 awsre-07

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

in Turbot > Demo Cluster

Overview | Activity | Controls 1 | Policies | Permissions | Organization | Advanced

S3 > Versioning

EXCEPTION

Skip

Edit | Delete

Active Policy

How is the Active Policy calculated?

	Default	Skip
	Turbot	~~Enforce: Enabled~~
-	Demo Cluster	
	AWS re:Invent 2017 EXCEPTION	ACTIVE **Skip**

Descendant Settings

	S3 awsre-05 EXCEPTION	Enforce: Enabled
	S3 awsre-06 EXCEPTION	Enforce: Enabled
	S3 awsre-07 EXCEPTION	Enforce: Enabled

S3:Versioning

Check if an S3 bucket has versioning enabled.

aws/s3/bucket

aws:s3:bucket

Turbot

Demo Cluster

AWS re:Invent 2017

AWS

AWS 831304522281

Azure

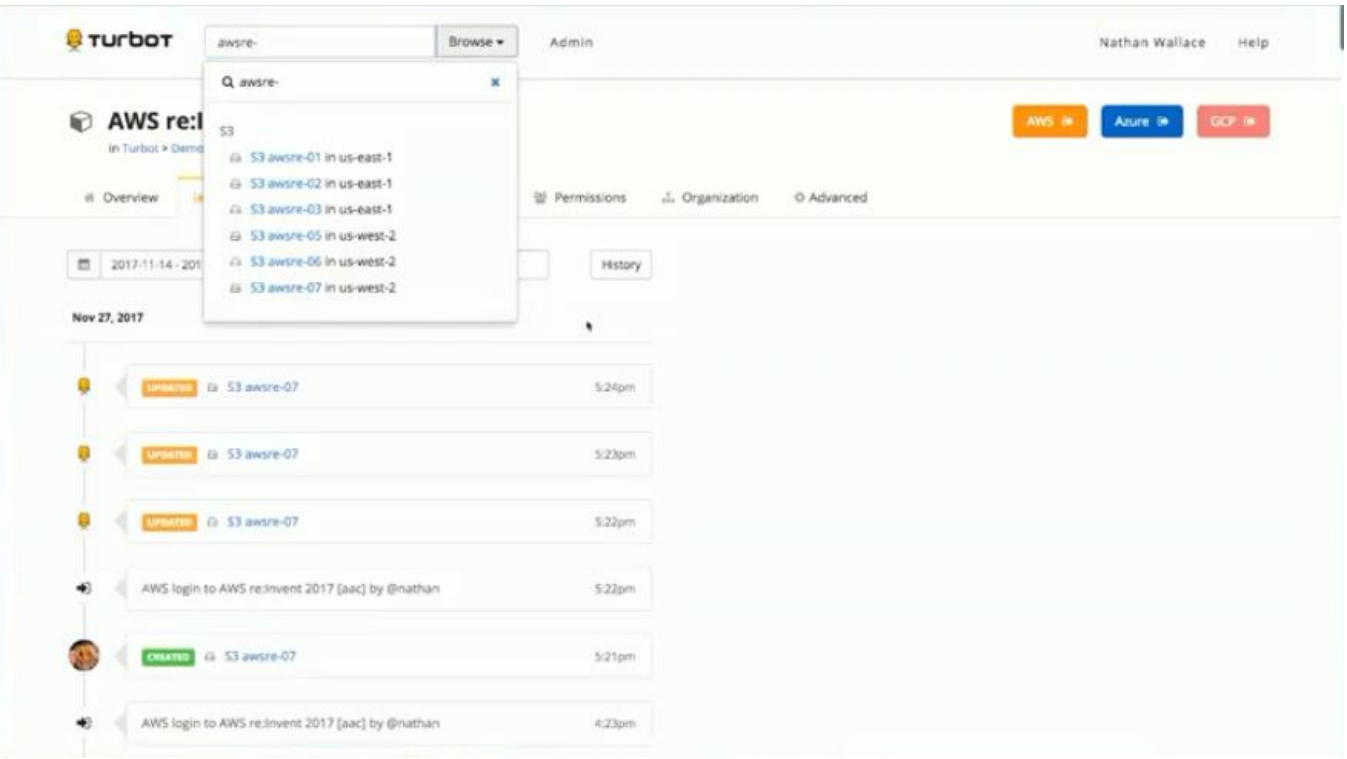
Azure dev-cody-demo

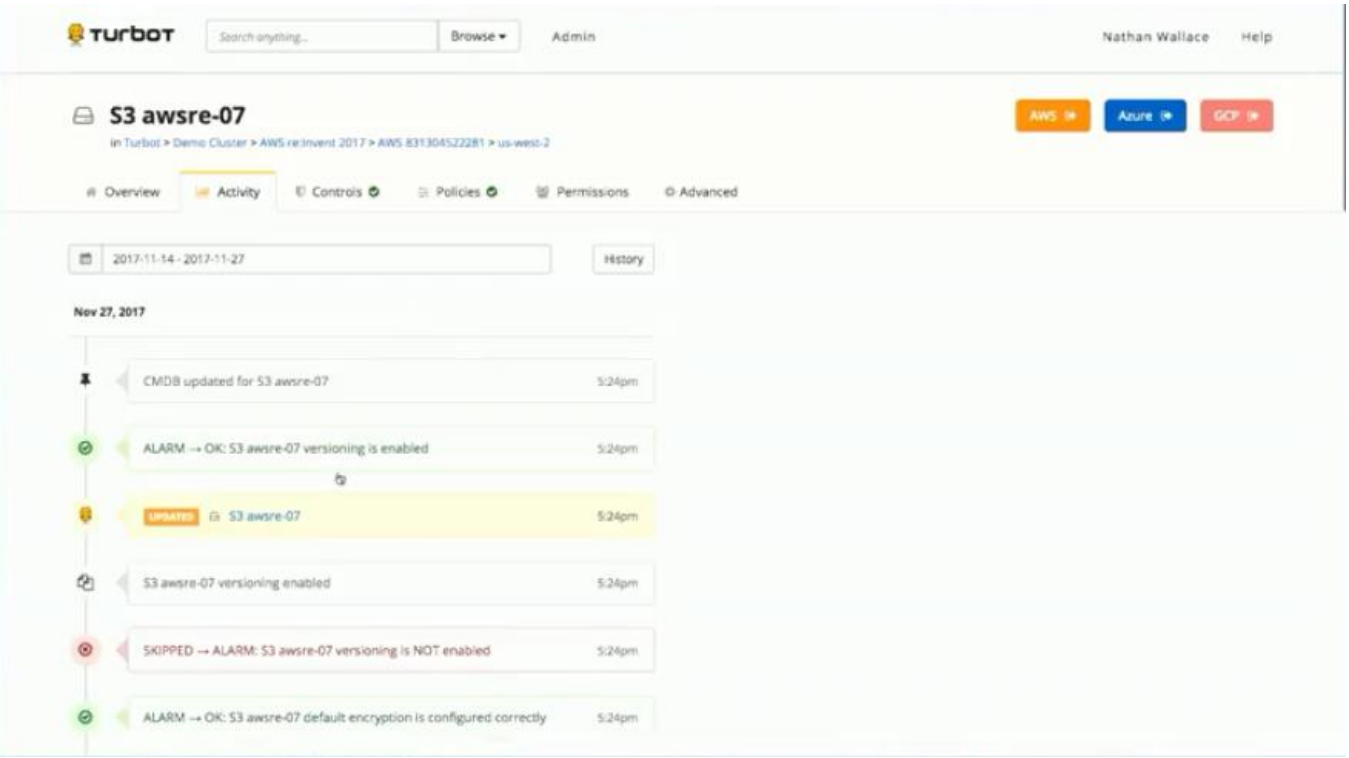
GCP

GCP cody-dev-demo

Turbot

Abc RG


turbot
awsre-
Browse
Admin
Nathan Wallace
Help
awsre-
S3
S3 awsre-01 in us-east-1
S3 awsre-02 in us-east-1
S3 awsre-03 in us-east-1
S3 awsre-05 in us-west-2
S3 awsre-06 in us-west-2
S3 awsre-07 in us-west-2
AWS
Azure
GCP
Overview
Permissions
Organization
Advanced
History
Nov 27, 2017
S3 awsre-07 5:24pm
S3 awsre-07 5:23pm
S3 awsre-07 5:22pm
AWS login to AWS re:Invent 2017 [aac] by @nathan 5:22pm
S3 awsre-07 5:21pm
AWS login to AWS re:Invent 2017 [aac] by @nathan 4:23pm


turbot
Search anything...
Browse
Admin
Nathan Wallace
Help
S3 awsre-07
in Turbot > Demo Cluster > AWS re:Invent 2017 > AWS 831304522281 > us-west-2
AWS
Azure
GCP
Overview
Activity
Controls
Policies
Permissions
Advanced
2017-11-14 - 2017-11-27
History
Nov 27, 2017
CMDB updated for S3 awsre-07 5:24pm
ALARM → OK: S3 awsre-07 versioning is enabled 5:24pm
S3 awsre-07 5:24pm
S3 awsre-07 versioning enabled 5:24pm
SKIPPED → ALARM: S3 awsre-07 versioning is NOT enabled 5:24pm
ALARM → OK: S3 awsre-07 default encryption is configured correctly 5:24pm

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

S3 awsre-07

in Turbot > Demo Cluster > AWS re:Invent 2017 > AWS 831304522281 > us-west-2

AWS | Azure | GCP

Overview | Activity | Controls | Policies | Permissions | Advanced

Nov 27, 2017

- UPDATED 5:24pm
- UPDATED 5:23pm
- UPDATED 5:22pm
- CREATED 5:21pm

aws.turbothq.com:Update:s3:bucket


```
ACL:
  Grants:
    - Grantee:
        DisplayName: aws+aac
        ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
        Type: CanonicalUser
      Permission: FULL_CONTROL
  Owner:
    DisplayName: aws+aac
    ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
Bucket: awsre-07
Encryption:
  ServerSideEncryptionConfiguration:
    Rules:
      - ApplyServerSideEncryptionByDefault:
          SSEAlgorithm: AES256
LocationConstraint: us-west-2
Logging:
```


turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

S3 awsre-07

in Turbot > Demo Cluster > AWS re:Invent 2017 > AWS 831304522281 > us-west-2

AWS | Azure | GCP

Overview | Activity | Controls | Policies | Permissions | Advanced

Nov 27, 2017

- UPDATED 5:24pm
- UPDATED 5:23pm
- UPDATED 5:22pm
- CREATED 5:21pm

aws.turbothq.com:Create:s3:bucket


```
ACL:
  Grants:
    - Grantee:
        DisplayName: aws+aac
        ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
        Type: CanonicalUser
      Permission: FULL_CONTROL
  Owner:
    DisplayName: aws+aac
    ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
Bucket: awsre-07
LocationConstraint: us-west-2
Logging:
  TargetBucket: aac-uswe2-qm6rd6pg6x5k
  TargetGrants: []
  TargetPrefix: AWSLogs/831304522281/S3/awsre-07/
Payer: BucketOwner
Region: us-west-2
```

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

UPDATED 5:23pm

UPDATED 5:22pm

CREATED 5:21pm


```
        DisplayName: aws+aac
        ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
        Type: CanonicalUser
      Permission: FULL_CONTROL
  Owner:
    DisplayName: aws+aac
    ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
Bucket: awsre-07
LocationConstraint: us-west-2
Logging:
  TargetBucket: aac-uswe2-qm6rd6pg6x5k
  TargetGrants: []
  TargetPrefix: AWSLogs/831304522281/S3/awsre-07/
Payer: BucketOwner
Policy:
  Statement:
    - Action: 's3:*'
      Condition:
        Bool:
          'aws:SecureTransport': 'false'
      Effect: Deny
      Principal: '*'
      Resource:
        - 'arn:aws:s3:::awsre-07'
        - 'arn:aws:s3:::awsre-07/*'
      Sid: MustBeEncryptedInTransit
  Version: '2012-10-17'
```


turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

S3 awsre-07

in Turbot > Demo Cluster > AWS re:Invent 2017 > AWS 831304522281 > us-west-2

AWS | Azure | GCP

Overview | Activity | Controls | Policies | Permissions | Advanced

Nov 27, 2017

UPDATED 5:24pm

UPDATED 5:23pm

UPDATED 5:22pm

CREATED 5:21pm

aws.turbothq.com:Update:s3:bucket


```
ACL:
  Grants:
    - Grantee:
        DisplayName: aws+aac
        ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
        Type: CanonicalUser
      Permission: FULL_CONTROL
  Owner:
    DisplayName: aws+aac
    ID: d6f7079a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
Bucket: awsre-07
Encryption:
  ServerSideEncryptionConfiguration:
    Rules:
      - ApplyServerSideEncryptionByDefault:
          SSEAlgorithm: AES256
LocationConstraint: us-west-2
Logging:
```

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

```
  - Key: Company
    Value: Reinvent Demo
  - Key: Description
    Value: Not Set
  - Key: Environment
    Value: Not Set
  - Key: Bucket Name
    Value: awsre-07
  - Key: 'turbot:CreatedByUrn'
    Value: 'urn:turbot:::profile:multi:nathan@turbot.com'
  - Key: 'turbot:CreatedBy'
    Value: Nathan Wallace - nathan@turbot.com
  - Key: 'turbot:CreatedTimestamp'
    Value: '2017-11-28T01:21:56.000Z'
TagsMap:
  Bucket Name: awsre-07
  Company: Reinvent Demo
  Cost Center: zz-aac
  Description: Not Set
  Environment: Not Set
  'turbot:CreatedBy': Nathan Wallace - nathan@turbot.com
  'turbot:CreatedByUrn': 'urn:turbot:::profile:multi:nathan@turbot.com'
  'turbot:CreatedTimestamp': '2017-11-28T01:21:56.000Z'
Versioning:
  Status: Enabled
urn: 'urn:turbot:dev:aac:aws:831304522281:us-west-2:s3:awsre-07'
```

turbot | 10.148.5 | Browse | Admin | Nathan Wallace | Help

S3 awsre

in Turbot > Demo

AWS | Azure | GCP

Overview | Permissions | Advanced

Nov 27, 2017

UPDATED

UPDATED

UPDATED

CREATED

10.148.5

EC2

- Demo Instance 101 in us-east-1 of aae
- Patching Test Windows in us-east-1 of aae
- PatchingTest in us-east-1 of aae

OS

- AmazonLinuxAMI-2017.09 in us-east-1 of aa
- MicrosoftWindowsServer2016Datacenter-1
- Ubuntu-16.04 in us-east-1 of aae

VPC

- aaeusea1 in us-east-1 of aae
- default in us-east-1 of aae
- DMZ us-east-1a 10.148.5.0/26 in us-east-1 o
- DMZ us-east-1c 10.148.5.64/26 in us-east-1
- Route Table vpc-c2393ba7/rtb-d05fb3b4 in
- Route Table vpc-c2393ba7/rtb-d15fb3b5 in
- vpc-069d5161 (aae) <=> vpc-c2393ba7 (aaa)
- vpc-069d5161 (aae) <=> vpc-c2393ba7 (aaa)
- vpc-069d5161 [] [] Main Route Table in us-ea
- vpc-069d5161 [DMZ] [us-east-1a] in us-east-

```
com:Update:s3:bucket

me: aws+aac
379a780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
onicalUser
FULL_CONTROL
aws+aac
780987077a2e224ffc2709b3441d952b5243e68cc06100de3b39ca67
yptionConfiguration:
  Rules:
    - ApplyServerSideEncryptionByDefault:
        SSEAlgorithm: AES256
LocationConstraint: us-west-2
Logging:
```

turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

PatchingTest

in Turbot > Demo Cluster > re:Invent Demo > AWS 266671049834 > us-east-1

AWS

Overview | Activity | Controls | Policies | Permissions | Advanced

Nov 26, 2017

- UPDATED 6:52pm
- UPDATED 6:44pm
- UPDATED 6:42pm
- UPDATED 5:05pm

Nov 8, 2017

- UPDATED 6:51am

aws.turbothq.com:Update:ec2:instance


```
AmiLaunchIndex: 0
Architecture: x86_64
BlockDeviceMappings:
  - DeviceName: /dev/sda1
    Ebs:
      AttachTime: '2017-11-01T13:53:20.000Z'
      DeleteOnTermination: true
      Status: attached
      VolumeId: vol-017cdaecd7c70b299
ClientToken: FuHNN1509544390029
EbsOptimized: false
ElasticGpuAssociations: []
EnaSupport: true
Hostname: devooeauvo05045
Hypervisor: xen
IamInstanceProfile:
  Arn: 'arn:aws:iam::266671049834:instance-profile/ec2_instance_default'
  Id: AIPAJSMXX7PEFZGUSR2KQ
```


turbot | Search anything... | Browse | Admin | Nathan Wallace | Help

re:Invent Demo aae

in Turbot > Demo Cluster

AWS

Overview | Activity | Controls 2 | Policies | Permissions | Organization | Advanced

Filter by User | Filter by Right | Include Inactive | Include Inherited | Add Grant

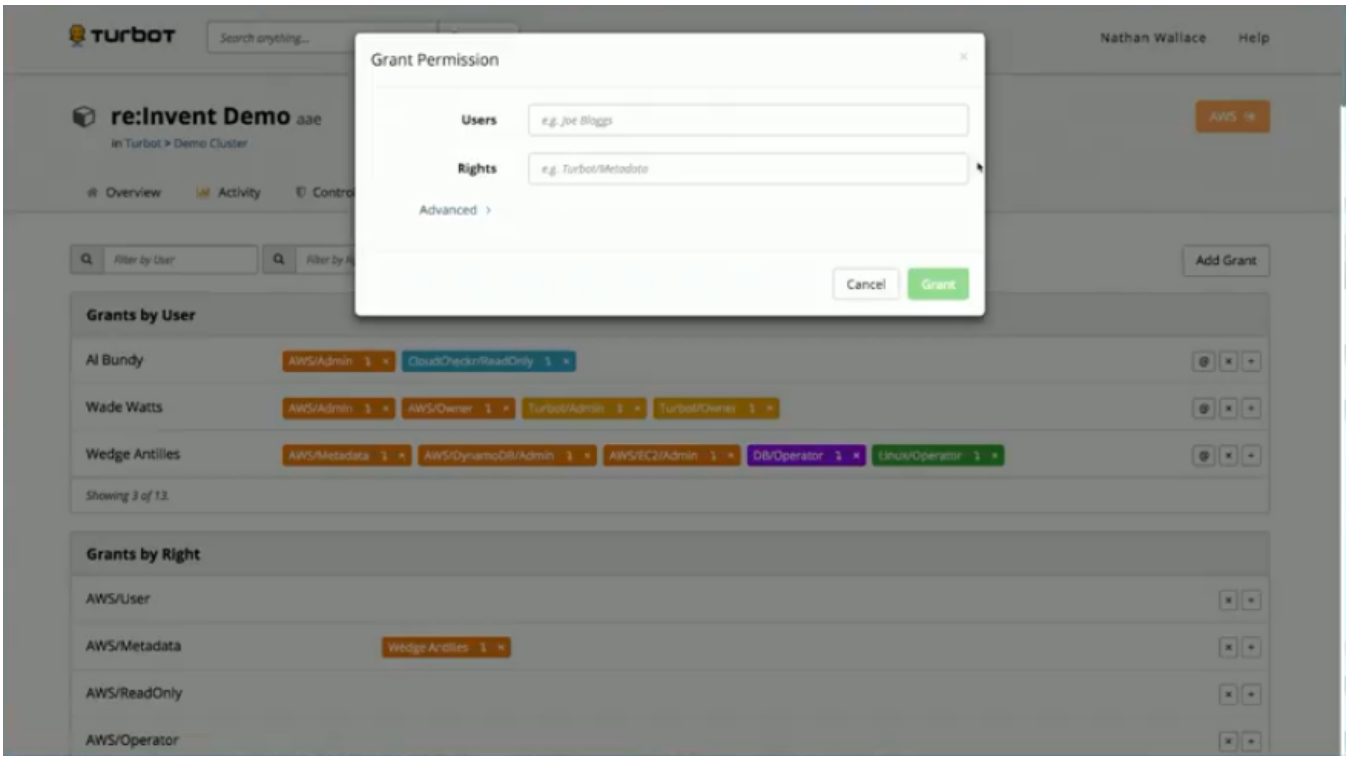
Grants by User

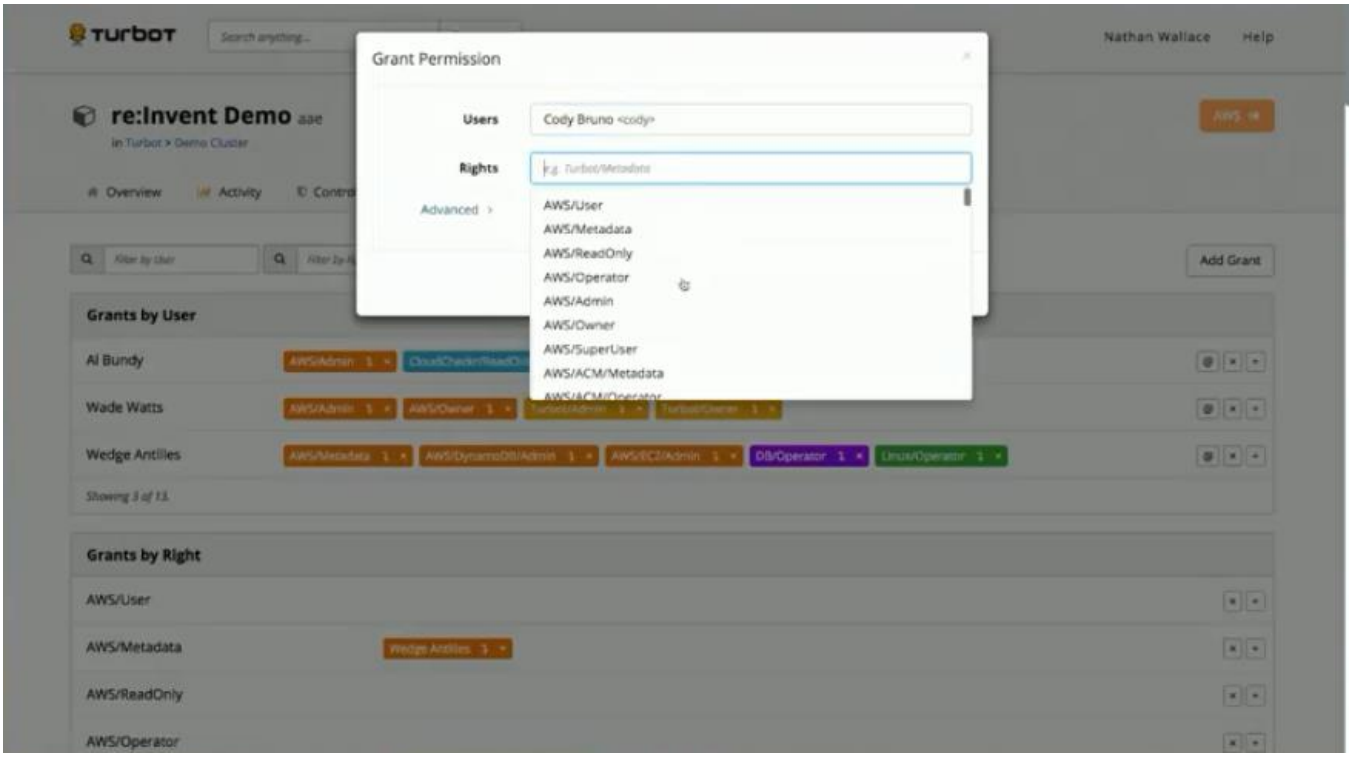
Al Bundy	AWS/Admin 1, CloudCheckr/ReadOnly 1
Wade Watts	AWS/Admin 1, AWS/Owner 1, Turbot/Admin 1, Turbot/Owner 1
Wedge Antilles	AWS/Metadata 1, AWS/DynamoDB/Admin 1, AWS/EC2/Admin 1, DB/Operator 1, Linux/Operator 1

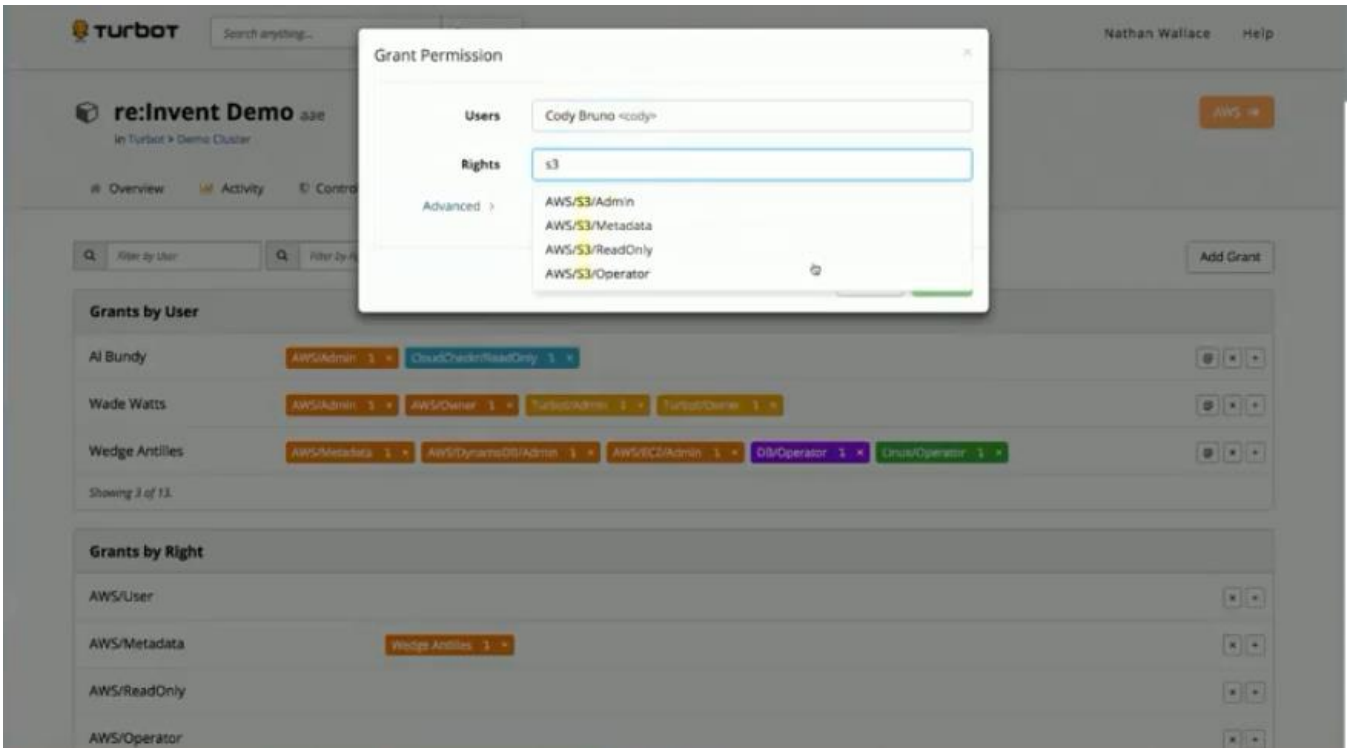
Showing 3 of 13.

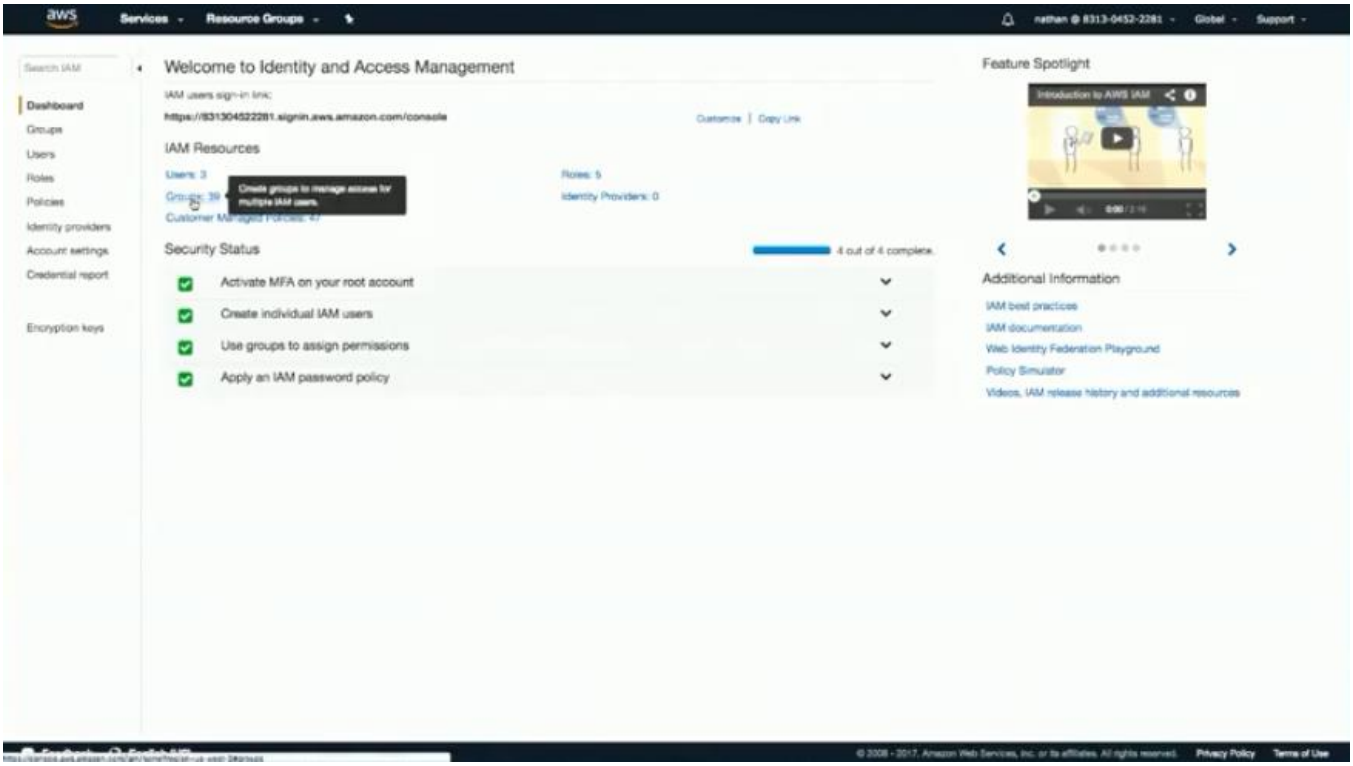
Grants by Right

AWS/User	
AWS/Metadata	Wedge Antilles 1
AWS/ReadOnly	
AWS/Operator	


turbot
Search anything...
Nathan Wallace
Help
re:Invent Demo aae
in Turbot > Demo Cluster
Overview
Activity
Grant Permission
Users
e.g. Joe Bloggs
Rights
e.g. Turbot/Metadata
Advanced
Cancel
Grant
Add Grant
Grants by User
Al Bundy
AWS/Admin 1
CloudChecker/ReadOnly 1
Wade Watts
AWS/Admin 1
AWS/Owner 1
Turbot/Admin 1
Turbot/Owner 1
Wedge Antilles
AWS/Metadata 1
AWS/DynamoDB/Admin 1
AWS/EC2/Admin 1
DB/Operator 1
Linux/Operator 1
Showing 3 of 13.
Grants by Right
AWS/User
AWS/Metadata
Wedge Antilles 1
AWS/ReadOnly
AWS/Operator


turbot
Search anything...
Nathan Wallace
Help
re:Invent Demo aae
in Turbot > Demo Cluster
Overview
Activity
Grant Permission
Users
Cody Bruno <cody>
Rights
e.g. Turbot/Metadata
Advanced
AWS/User
AWS/Metadata
AWS/ReadOnly
AWS/Operator
AWS/Admin
AWS/Owner
AWS/SuperUser
AWS/ACM/Metadata
Add Grant
Grants by User
Al Bundy
Wade Watts
Wedge Antilles
Showing 3 of 13.
Grants by Right
AWS/User
AWS/Metadata
Wedge Antilles 1
AWS/ReadOnly
AWS/Operator


turbot
Nathan Wallace
Help
re:Invent Demo
Overview
Activity
Grant Permission
Users
Cody Bruno
Rights
s3
Advanced
AWS/S3/Admin
AWS/S3/Metadata
AWS/S3/ReadOnly
AWS/S3/Operator
Add Grant
Grants by User
Al Bundy
Wade Watts
Wedge Antilles
Grants by Right
AWS/User
AWS/Metadata
AWS/ReadOnly
AWS/Operator


aws
Services
Resource Groups
Welcome to Identity and Access Management
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
IAM Resources
Security Status
Activate MFA on your root account
Create individual IAM users
Use groups to assign permissions
Apply an IAM password policy
Feature Spotlight
Additional Information
IAM best practices
IAM documentation
Web Identity Federation Playground
Policy Simulator

aws Services Resource Groups nathan @ 8313-0432-2281 Global Support

Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report

Encryption keys

Create New Group Group Actions

Filter

Showing 39 results

Group Name	Users	Inline Policy	Creation Time
admin	2		2016-10-31 08:44 PST
config_admin	0		2016-10-31 08:44 PST
config_metadata	0		2016-10-31 08:44 PST
config_operator	0		2016-10-31 08:44 PST
core_admin	0		2016-10-31 08:44 PST
core_metadata	0		2016-10-31 08:44 PST
core_operator	0		2016-10-31 08:44 PST
core_readonly	0		2016-10-31 08:44 PST
ec2_admin	0		2017-04-11 07:18 PST
ec2_metadata	0		2017-04-11 07:18 PST
ec2_operator	0		2017-04-11 07:18 PST
ec2_owner	0		2017-04-11 07:18 PST
iam_metadata	0		2016-10-31 08:44 PST
iam_operator	0		2016-12-16 12:13 PST
iam_owner	0		2016-10-31 08:44 PST
iam_readonly	0		2017-11-25 10:13 PST
iam_user	0		2016-10-31 08:44 PST
kms_admin	0		2016-10-31 08:44 PST
kms_metadata	0		2016-10-31 08:44 PST
kms_operator	0		2016-10-31 08:44 PST

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

turbot Search anything... Browse Admin Nathan Wallace Help

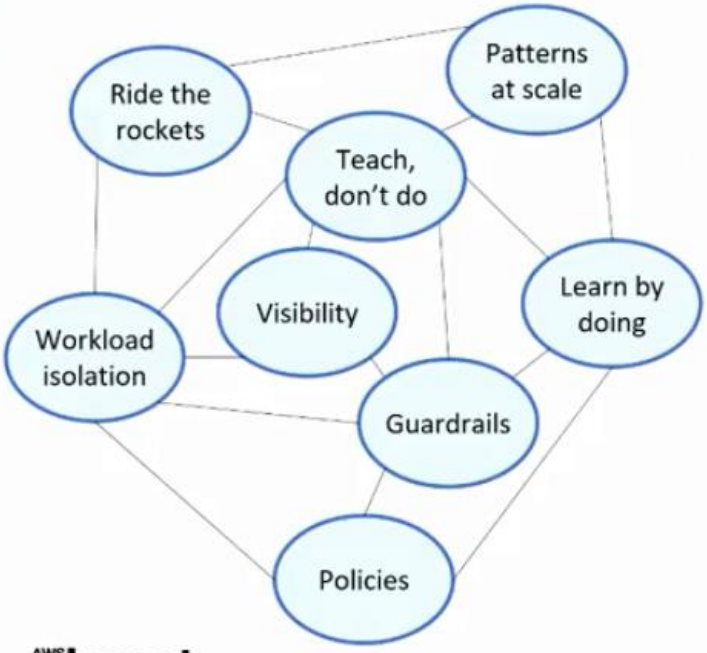
Accounts

AWS re:Invent 2017	aac	AWS Azure
App Acct ABC	aak	
App Acct Dev	aaj	
App Acct Prod	aai	
Bob's Demo Account (aab)	aab	AWS Azure GCP
CI/CD Demo (aah)	aah	
Consolid Billing	aag	
Dave's Demo (aad)	aad	
Mike's Demo Account	aai	
Turbot Master	aaa	AWS
re:Invent Demo	aae	

Notifications

- [NEW] → OK: S3 awsre-07 is approved 5:22pm
- [NEW] → OK: S3 awsre-07 has a DNS compliant name 5:22pm
- [NEW] → ALARM: S3 awsre-07 default encryption is NOT configured corre... 5:22pm
- [NEW] → ALARM: S3 awsre-07 is NOT logging to aac-uswe2-qm6rd6pg6x5k 5:22pm
- [NEW] → ALARM: S3 awsre-07 tags are NOT set correctly 5:22pm
- [NEW] → ALARM: S3 awsre-07 does NOT have the correct Turbot tags 5:22pm
- [NEW] → SKIPPED: S3 awsre-07 versioning enforcement skipped 5:22pm
- [NEW] → OK: S3 awsre-07 meets anonymous access restrictions 5:22pm
- [NEW] → OK: S3 awsre-07 Encryption at Rest bucket policies are in sync 5:22pm
- [NEW] → OK: S3 awsre-07 meets cross-account restrictions 5:22pm
- [NEW] → SKIPPED: S3 awsre-07 skipped for bucket allowed 5:22pm
- [NEW] → OK: CMDB is up to date for S3 awsre-07 5:22pm

Nathan Wallace



- ✓ Move at cloud speed
- ✓ Common language
- ✓ Security and compliance
- ✓ Cost control
- ✓ Close the skills gap
- ✓ Reduced friction

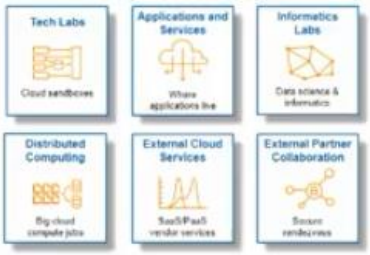
AWS re:Invent

aws

Where is NIBR now?

400 w/console access

170 accounts
+ 10/month



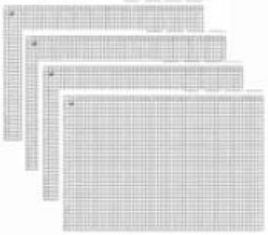
Represents new work per our "**cloud first for new**" strategy
(migrations to follow later)

NOVARTIS

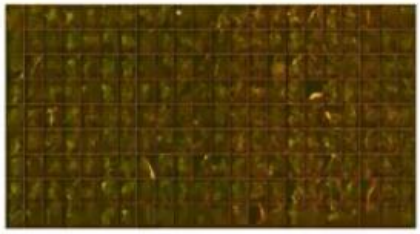
*Multi-Parametric Data Analysis

MPDA*–one of many big data problems

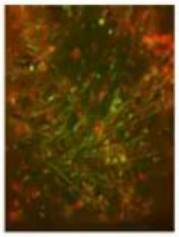
Up to 1000 plates



1536 wells/plate



1k to 5k cells/well



1 screen

Per screen

- **100-1000 billion** observations
- **5-50 TB** data

Occasionally up to

- **15 trillion** observations
- **1 PB** data

200 to 2000 features/cell

Novartis Institutes for BioMedical Research

NOVARTIS

Transformed our species' first population-scale medical genomics effort into actionable data for drug discovery in *weeks*

Public

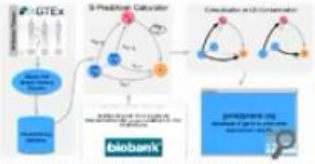
July: UK Biobank data available:
nearly half a million genomes with health records

RAPID GWAS OF THOUSANDS OF PHENOTYPES FOR 337,000 SAMPLES IN THE UK BIOBANK

biobank

August 20th: Neale lab "rapid GWAS" released.
Genome-wide mapping of >2,000 traits by 10M genetic sites 26 billion linear regressions

Credit: Claire Churchhouse and Ben Neale http://www.nealelab.is/



Credit: Hae Kyung Im http://haekyimlab.org/

October 15th: Im lab transcriptome association ties Neale lab GWAS results to putatively causal genes; result deposited in S3

September

October 2017

NIBR

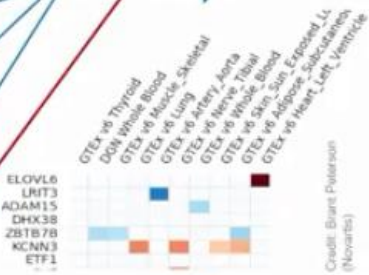
October 16th: transcriptome association data available within a NIBR AWS account

October 18th: preliminary analyses of transcriptome data complete (5 billion QC runs in 2 days in Spark on EC2)

9 days

October 19th: EC2/S3/Spark internal data browser app published to informaticians

October 25th: putative gene targets for over a dozen diseases distributed to NIBR drug discovery teams



Credit: Brant Peterson (Novartis)

Novartis Institutes for BioMedical Research

NOVARTIS

What people think

… hard to explain just how excited …

Thanks for bringing the AWS console safely into developer's hands

… awesome it is to have autonomy!

… control our own environments was an extreme enabler …

Automation drives high productivity

Succeeding with a very small (and amazing!) team

Tips and lessons learned

Transformation	Multi-account	Networking
• Separate use cases	• Essential for diversity	• Networking is hard
• Tech Lab	• Automation required	• VIF limits
• Console access	• API access important	• IP allocation
• Inclusive team		

kenrobbins.link/reinvent

Summary

- Use multi-account if you have any appreciable variety and agility needs
- Account-as-a-container enables rapid org transformation to cloud
- Multi-account requires automation
- Software-defined operations enables agility and control

Acknowledgements

- NIBR
  - Cloud Team
  - Network Operations
  - Cyber Security
  - Information Security & Risk Management
  - Research Computing Platforms
  - Multi-Parametric Data Analysis (MPDA) team
  - Core Data & Analytics team
  - Scientific Data Analysis team
  - Our entire user community
- Turbot
  - Support
  - Product Management
  - Executive team
- AWS
  - Solution Architects
  - Enterprise support team
  - Account management

NOVARTIS