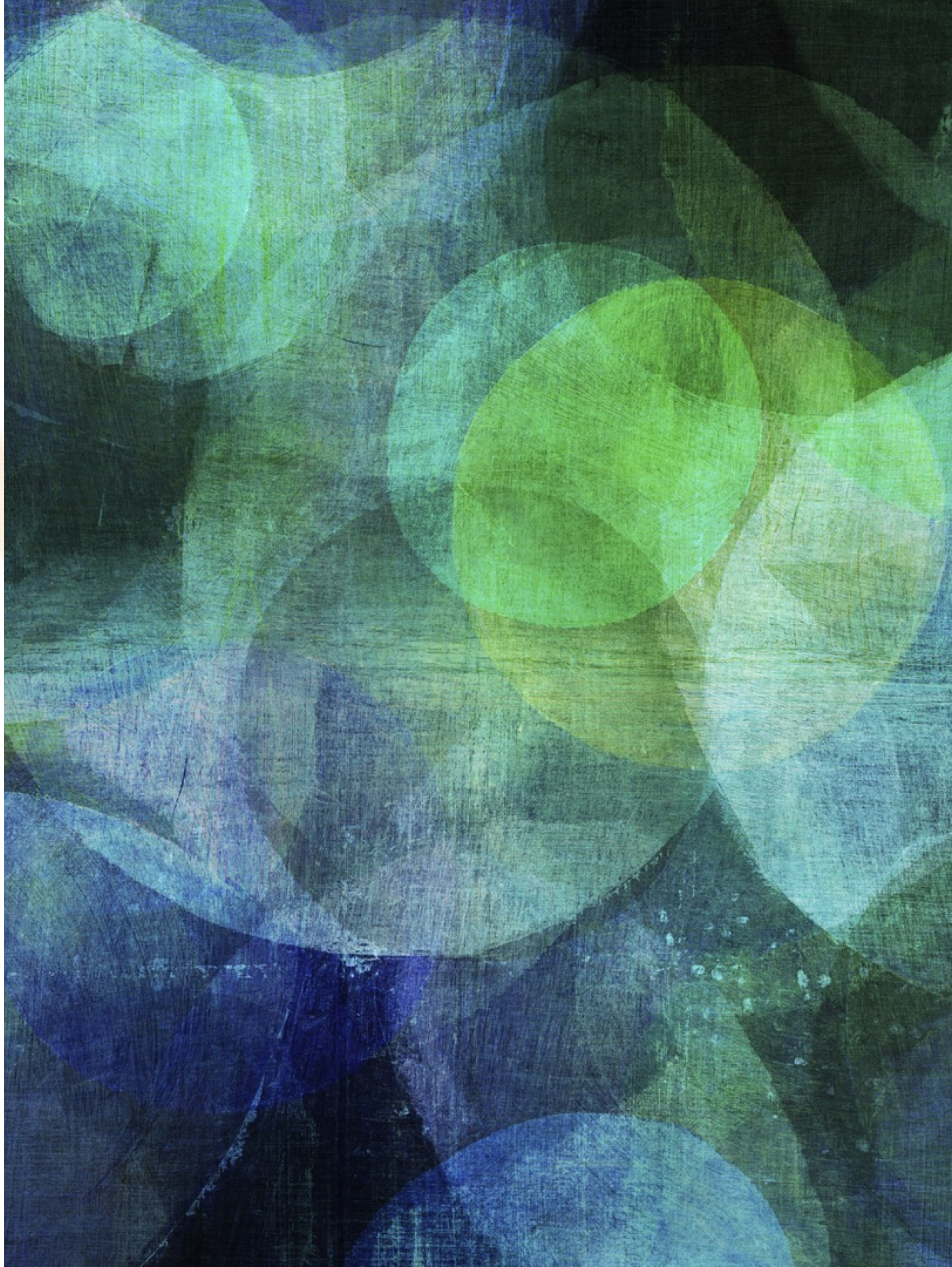
AWS DATA PROCESSING INFRASTRUCTURE 2B

Nan Dun
nan.dun@acm.org



COPYRIGHT POLICY 版权声明

All content included on the Site or third-party platforms as part of the class, such as text, graphics, logos, button icons, images, audio clips, video clips, live streams, digital downloads, data compilations, and software, is the property of BitTiger or its content suppliers and protected by copyright laws.

Any attempt to redistribute or resell BitTiger content will result in the appropriate legal action being taken.

We thank you in advance for respecting our copyrighted content.

For more info see https://www.bittiger.io/termsofuse and https://www.bittiger.io/termsofservice

所有太阁官方网站以及在第三方平台课程中所产生的课程内容，如文本，图形，徽标，按钮图标，图像，音频剪辑，视频剪辑，直播流，数字下载，数据编辑和软件均属于太阁所有并受版权法保护。

对于任何尝试散播或转售BitTiger的所属资料的行为，太阁将采取适当的法律行动。

我们非常感谢您尊重我们的版权内容。

有关详情，请参阅
https://www.bittiger.io/termsofuse
https://www.bittiger.io/termsofservice

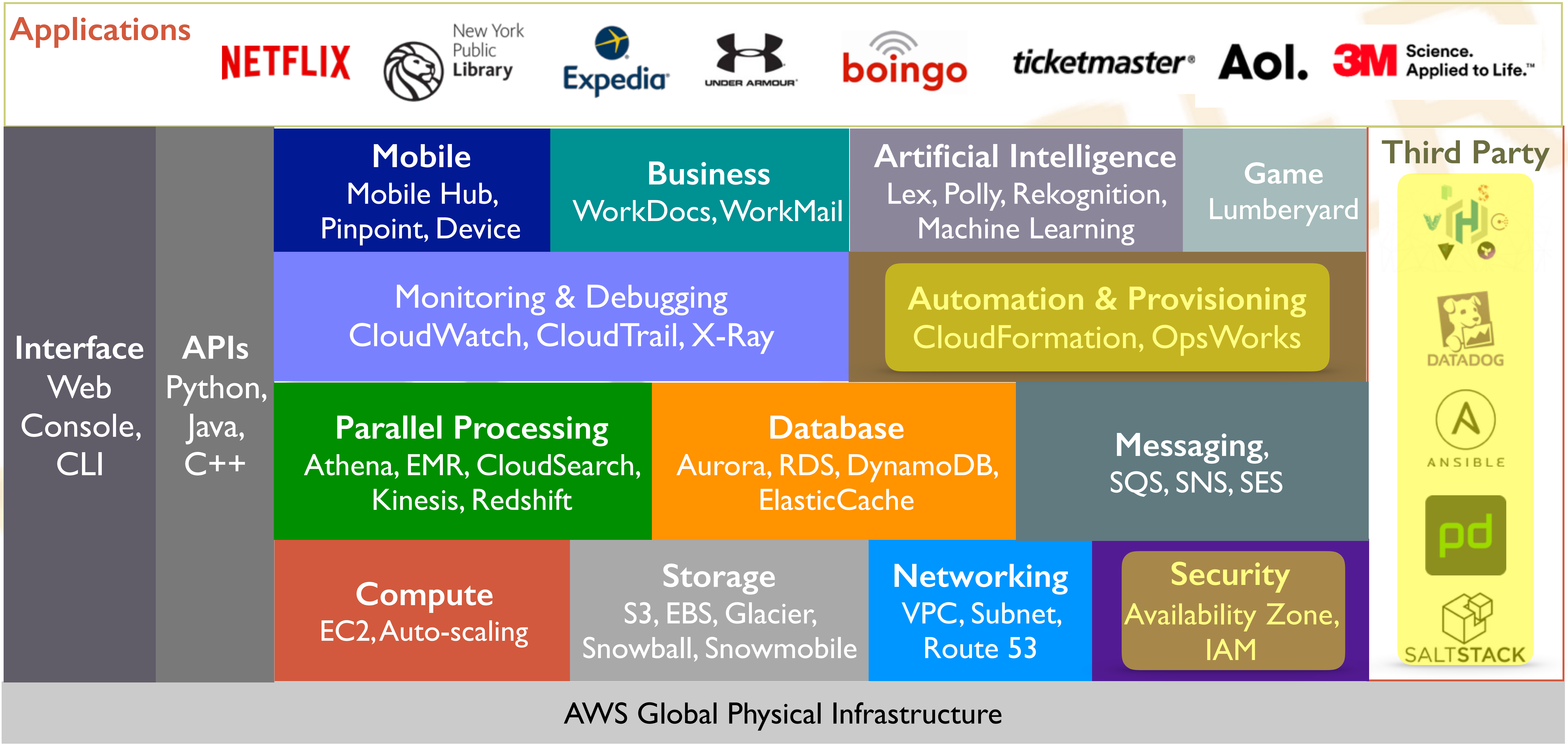
DISCLAIMER

I. “All data, information, and opinions expressed in this presentation is for informational purposes only. I do not guarantee the accuracy or reliability of the information provided herein.This is a personal presentation.The opinions expressed here represent my own and not those of my employer.”

II. “The copyright of photos, icons, charts, trademarks presented here belong to their authors.”

III. “I could be wrong.”

TODAY'S TOPIC



Applications

NETFLIX

New York Public Library

Expedia

UNDER ARMOUR

boingo

ticketmaster

Aol.

3M Science. Applied to Life.™

Interface
Web Console, CLI

APIs
Python, Java, C++

Mobile
Mobile Hub, Pinpoint, Device

Business
WorkDocs, WorkMail

Artificial Intelligence
Lex, Polly, Rekognition, Machine Learning

Game
Lumberyard

Monitoring & Debugging
CloudWatch, CloudTrail, X-Ray

Automation & Provisioning
CloudFormation, OpsWorks

Parallel Processing
Athena, EMR, CloudSearch, Kinesis, Redshift

Database
Aurora, RDS, DynamoDB, ElasticCache

Messaging,
SQS, SNS, SES

Compute
EC2, Auto-scaling

Storage
S3, EBS, Glacier, Snowball, Snowmobile

Networking
VPC, Subnet, Route 53

Security
Availability Zone, IAM

Third Party

DATADOG

ANSIBLE

pd

SALTSTACK

AWS Global Physical Infrastructure

IAM

EXAMPLES

- Limit Users to Launch Certain Types of EC2 Instances
- Decode the EC2 authorization message
- Allow User to Start, Stop, and Terminate his/her own instances
- Allow Users to Access a Personal "Home Directory" in Amazon S3 (Homework)
    - https://aws.amazon.com/blogs/security/writing-iam-policies-grant-access-to-user-specific-folders-in-an-amazon-s3-bucket/

DEMO

- Create a user
  - Login console: https://${accound_id}.signin.aws.amazon.com/console
- Limit a User to Launch Certain Types (t2 and m3) of EC2 Instances

1. Create a managed policy to limit instance type using policy generator
    1. Allow all EC2 access
    2. Deny access based on conditions
2. Attach policy to a user

DEMO

- Decode authorization failure message
  - Administrator must log IAM events in CloudTrail (next lesson)
  - $ aws sts decode-authorization-message --encoded-message

DEMO

- Limit a User to Terminate his/her own EC2 Instances
  1. Create "User" tag for EC2 instance
  2. Grant user to access all EC2 instances
  3. Limit users by matching "User" tag

POLICY SIMULATOR

- https://policysim.aws.amazon.com
  - Test S3 bucket access

TERRAFORM

PREPARE

- Route53
  - Register a domain
  - Find the Hosted Zone ID
    - https://console.aws.amazon.com/route53/home?region=us-west-2#hosted-zones:
    - $ aws route53 list-hosted-zones
- EC2 Instance Profile
  - Allow access S3, and other resources
- Double check
  - VPC ID, Subnet ID

TERRAFORM CONFIGURATION

- Provider
- Resources
    - EC2
    - Route53
    - Security Group (multiple)
- Input variables
- Command line usage

ANSIBLE

ANSIBLE CONFIGURATION

- Load order
  - ANSIBLE_CONFIG (an environment variable)
  - ansible.cfg (in the current directory)
  - ansible.cfg (in the home directory)
  - /etc/ansible/ansible.cfg
- Use template
  - Only change values required

INVENTORY GENERATION

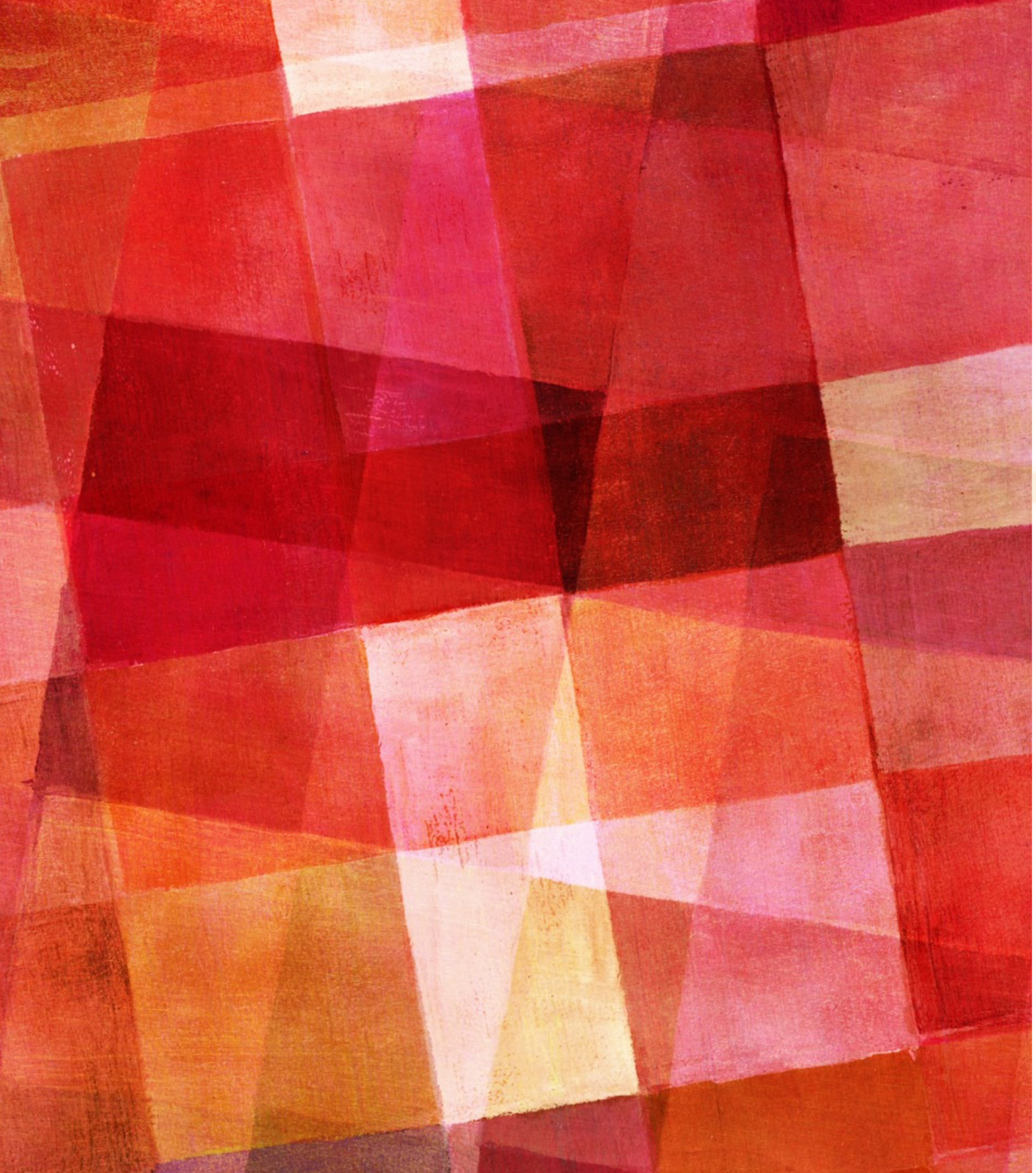
- Python JSON parser
  - cluster/json2ini.py

ANSIBLE PLAYBOOK

- Change configuration variables
- Commands
  - $ ansible-playbook playbook.yaml --list-hosts
  - $ ansible-playbook playbook.yaml --list-tasks
  - $ ansible-playbook playbook.yaml
  - $ ansible-playbook playbook.yaml - -step
  - $ ansible-playbook --start-at-task

HOMEWORK

- Try all examples in demo and scripts/
- Check scripts/ec2_limited_instance_types.json, find out how it is different from the example we used in “Limit a User to Launch Certain Types (t2 and m3) of EC2 Instances” (p. 7)
- Create an AMI with Packer
- Setup your Terraform configuration and ansible.cfg
  - Use your own: AMI, VPC, Subnet, Hosted Zone, SSH Key
- Start a cluster and validate web server is running
- Run command using Ansible on all servers
- Destroy cluster



QUESTIONS

- bittiger-aws@googlegroups.com