



Azure bound ... a tale of discovery



Matt McLane

DevOps Engineer
Criteo Inc.

This month, Matt McLane from Criteo will give everyone a glimpse into Criteo's journey from AWS to Azure including their frustrations, the wins, and the tools they relied on to get them there. Additionally, Matt will delve into their in-house developed solutions for utilizing Azure to its fullest, and expand on how they continue to build new services within the Azure ecosystem.



Matt McLane

DevOps Engineer at Criteo
on the cbs-devops team

2 •

criteo.

- I am a DevOps Engineer on the cbs-devops team here at Criteo.
- I have over 20 years of experience in IT.
- I enjoy long walks through the woods and automating all the things.

Question:

- How many people work in Azure on a regular basis?

A story in three parts



1

Chapter 1:

How we got where we are

2

Chapter 2:

What we built along the way

3

Chapter 3:

Moral of the story

criteo.

Thought I would share our story.

We have been working on a lot of new and interesting things

Others might benefit from what we have learned.

Tell the story in three parts

Not so long ago...



criteo.

Hooklogic was built on AWS

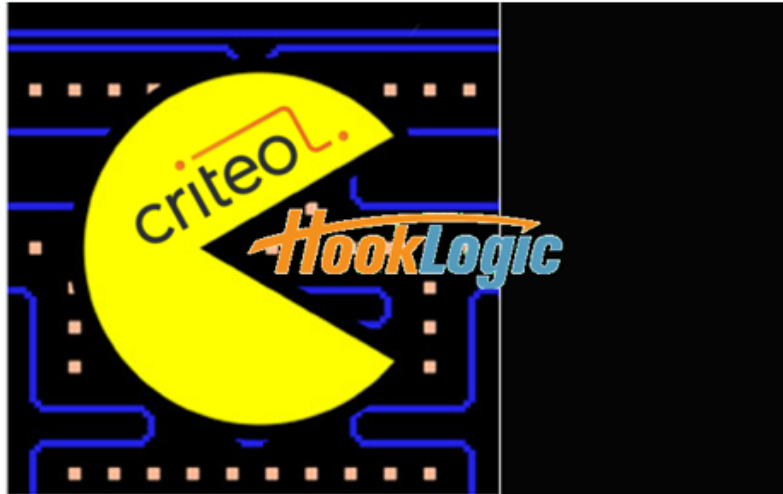


5 •

criteo.

1. In the spring of 2016 I joined hooklogic, an Advertising technology company
 - Hooklogic built an advertising exchange to allow advertisers to reach in-market shoppers, drive traffic to products, and attribute resulting sales.
 - Hooklogic was build on AWS
 - Heavy S3, lambda, etc.
 - our team, the devops team was responsible for the AWS infra and deployment pipeline
 - Asked to build a new version of the pipeline
 - Cloudformation based
 - VPCs
 - Better security
 - etc.

Criteo acquires hooklogic!



6 •

criteo.

- Purchased by Criteo - October 2016
 - Renamed CBS or Criteo Brand Solutions
 - Bare metal infra
 - Very large clusters that would cost more to run in the cloud
 - Ability to have their servers physically closer to servers where their ads are shown.
 - Migrate from AWS to bare metal servers in Criteo data centers.
 - Reduce costs by eliminating redundant systems.
 - Amazon is a competitor, demands of Walmart.

Enter Azure



7 •

criteo.

- We believe the public cloud has a place in Criteo.
- Embraced Azure
 - Criteo already uses Azure in conjunction with Office 365.
 - Existing enterprise agreement.
 - Existing user accounts that are managed by someone else
- Built automated pipeline utilizing existing Criteo services.
- Started building out offerings.
- Took the lessons from before and built a new system.
- We thought we could make it *better than* it was. *Better, stronger, faster.*

What have we built?

.....

criteo.



Starts with Terraform Code



The screenshot displays a code editor with two panels. The left panel shows the Terraform configuration code, and the right panel shows the output of a Terraform command.

```
provider "aws" {
  region = "us-east-1"
}

terraform {
  required_version = "0.12.2"
}

resource "aws_s3_bucket" {
  bucket = "criteo-terraform"
  acl     = "private"
  tags    = {
    Name = "criteo-terraform"
  }
}

resource "aws_s3_bucket_policy" {
  bucket = aws_s3_bucket.bucket
  policy = jsonencode({
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": "*",
        "Action": "s3:ListBucket",
        "Resource": aws_s3_bucket.bucket,
        "Condition": {
          "StringEquals": {
            "aws:PrincipalOrgID": "095503927886"
          }
        }
      }
    ]
  })
}
```

The right panel shows the output of a Terraform command, including the plan and the execution of the Terraform code.

```
terraform init
terraform plan
terraform apply
```

10



We use Terraform to describe our

Code Review

[All](#)
[My](#)
[Projects](#)
[People](#)
[Documentation](#)

[Changes](#)
[Drafts](#)
[Draft Comments](#)
[Edits](#)
[Watched Changes](#)
[Shared Changes](#)
[Groups](#)

Change 438876 - Merged

Add Shared Image Gallery and Files (javier@img...)

Change ID: 2d05d42d943891a68e2231a13a2937326a5455
 310b1-8699e-5437

Owner: Matthew Moline
 Updater: spilot escalation
 Assignee: spilot escalation
 Reviewers: Clark Peters, Harold Doel, Joris De Poeder, Matthew Moline
 Project: src/terraform
 Branch: master
 Topic: sig
 Updated: 8 days ago
 Cherry Pick: [Revert](#)

Code-Review: +2 Harold Doel
 Non-Author Code-Review: +1 Matthew Moline
 Ready-to-Submit: +1 Matthew Moline
 Verified: +1 spilot escalation

Related Changes (6)
 - [SPOT2018: terraform config for cap or static files storage...](#)
 - [Add Shared Image Gallery and first preter image...](#)
 - [Delete external location servers...](#)
 - [Fix validate an syntax...](#)

Author: mmoline@critico.com
 Committer: spilot escalation - spilot@critico.com
 Commit: o4d51a6c2f13b0d8f6a54a7511a8f76b84
 Parent(s): 8b05d0a6f854a7d5e79b751a570a810754a632
 Change ID: b05d0a6f854a7d5e79b751a570a810754a632

Files: [Open All](#) | [Diff](#) | [spilot](#) | [Base](#)

| File Path | Comments | Size |
|--|----------|------|
| new_project.py | 1 | 1 |
| A configurations/hand_image_gallery.sh | 42 | 42 |
| A configurations/hand_image_gallery.sh | 33 | 33 |
| A configurations/hand_image_gallery.sh | 4 | 4 |
| new_project.py | +76, -2 | |

History

[Expand All](#) | [Hide logged comments](#)

| Author | Message | Time |
|-------------------|--|-----------------|
| Matthew Moline | Uploaded patch set 1. | Nov 16 11:23 AM |
| spilot escalation | Patch Set 1: http://build.ortelics.com/terraform-pre-submit/STARTING | Nov 16 11:23 AM |
| spilot escalation | Patch Set 1: Verified 1 Build Failed http://build.ortelics.com/terraform-pre-submit/FAILURE | Nov 16 11:24 AM |
| Matthew Moline | Uploaded patch set 2. | Nov 16 11:41 AM |
| spilot escalation | Patch Set 2: http://build.ortelics.com/terraform-pre-submit/STARTING | Nov 16 11:41 AM |
| spilot escalation | Patch Set 2: Verified 1 http://build.ortelics.com/terraform-pre-submit/SUCCESS | Nov 16 11:45 AM |
| Harold Doel | Patch Set 2: Code-Review-2 FAIL: if you make fixes along the way at least mention them in commits. | Nov 16 5:19 PM |
| Matthew Moline | Patch Set 2: Ready-to-Submit-1 | Nov 19 4:48 PM |
| spilot escalation | Change has been successfully released and submitted as o4d51a6c2f13b0d8f6a54a7511a8f76b84 by spilot escalation | Nov 19 4:48 PM |

11

critico

- Code review done in Gerrit
- Presubmit check validates the change
 - Rubocop
 - Terraform format
 - Terraform validate
 - Workspaces exist
 - Gets plans

Example Plan



Planned Changes - Adds Shared Image Gallery and first jmeter image.

Generated 2018-11-16 16:45:54.745937 UTC

configurations/shared_image_gallery

prod

```
[Create] azurem_resource_group.ng
name: "shared_image_gallery-prod"
tags.Project: "shared_image_gallery"
tags.ManagedBy: "Terraform"
tags.Environment: "prod"
tags.Team: "cbs-devops"
location: "eastus"
tags.%: "4"
id: "<computed>"
```

```
[Create] azurem_shared_image.def
```

```
[Create] azurem_shared_image_gallery.gallery
```

```
[Create] azurem_shared_image_version.v1
```

preprod

```
[Create] azurem_resource_group.ng
```

```
[Create] azurem_shared_image_gallery.gallery
```

12 •

criteo.

Change 435576 - Merged

Adds Shared Image Gallery and first jmeter image.

Change-ID: 2c6fd4329453891ea8ee2231e11e2b367356c5465
 3129a devops-5439

Owner: Matthew McLane
 Uploader: qabot escalation
 Assignee: qabot escalation
 Reviewers: Clark Peters, Harold Dost, Joris De Pooter, Matthew McLane
 Project: azure/terraform
 Branch: master
 Topic: sig
 Updated: 8 days ago

Code-Review: +2 Harold Dost
 Non-Author-Code-Review: +1 Matthew McLane
 Ready-to-Submit: +1 qabot escalation
 Verified: +1 qabot escalation

Related Changes (4)

- (BFLUP2018) Terraform configs for asp ui static files storage...
- Adds Shared Image Gallery and first jmeter image.
- Delete storional bastion servers
- Fix validate.sh syntax

Files

| File Path | Comments | Size |
|--|----------|------|
| Commit Message | | |
| A configurations/shared_image_gallery/global.tf | 1 | |
| A configurations/shared_image_gallery/jmeter-worker.tf | 42 | |
| A configurations/shared_image_gallery/main.tf | 30 | |
| new_project.py | 4 | |
| | +78, -2 | |

History

| Author | Message | Time |
|------------------|---|-----------------|
| Matthew McLane | Uploaded patch set 1. | Nov 16 11:23 AM |
| qabot escalation | Patch Set 1: http://build.criteo.islanjob/azure-terraform-pre-submit/635/ STARTING | Nov 16 11:23 AM |
| qabot escalation | Patch Set 1: Verified-1 Build Failed http://build.criteo.islanjob/azure-terraform-pre-submit/635/ FAILURE | Nov 16 11:24 AM |
| Matthew McLane | Uploaded patch set 2. | Nov 16 11:41 AM |
| qabot escalation | Patch Set 2: http://build.criteo.islanjob/azure-terraform-pre-submit/636/ STARTING | Nov 16 11:41 AM |
| qabot escalation | Patch Set 2: http://build.criteo.islanjob/azure-terraform-pre-submit/636/ STARTING | Nov 16 11:45 AM |
| qabot escalation | Patch Set 2: Verified+1 http://build.criteo.islanjob/azure-terraform-pre-submit/636/ SUCCESS | Nov 16 11:45 AM |
| Harold Dost | Patch Set 2: Code-Review+2 FAR: If you make fixes along the way at least mention them in commits. | Nov 16 5:19 PM |
| Matthew McLane | Patch Set 2: Ready-to-Submit+1 | Nov 19 4:46 PM |
| qabot escalation | Change has been successfully rebased and submitted as c4d5f0eb213fcb46ee0d4de7511e8f76d84 by qabot escalation | Nov 19 4:46 PM |

- Human review's and gives a +2 if they approve.
- Merged

Deployment Pipeline

criteoL Jenkins

Jenkins > azure-terraform-pipeline

- Back to Dashboard
- Status
- Changes
- View Configuration
- Full Stage View
- Job Config History
- Embeddable Build Status
- Pipeline Syntax

Pipeline azure-terraform-pipeline

azure-terraform deployment pipeline

Allowed Production submitters are: [cde-devops, c.peters, h.dost, j.depoiter, m.mclane, s.godbold]

Last Successful Artifact: [plan.html](#) 1.42 KB [view](#)

[Recent Changes](#)

Build History

Find

| Build Number | Status | Timestamp | Duration |
|------------------|---------|----------------------|----------|
| #397 - redline55 | Success | Nov 26, 2018 4:40 PM | 2min 19s |
| #398 - redline55 | Success | Nov 26, 2018 2:48 PM | 1min 53s |
| #397 - redline55 | Success | Nov 26, 2018 2:22 PM | 1min 39s |
| #398 - redline55 | Success | Nov 26, 2018 2:18 PM | 1min 50s |
| #399 - redline55 | Failure | Nov 25, 2018 9:42 PM | 4min 39s |
| #394 - redline55 | Success | Nov 19, 2018 9:44 PM | 4min 39s |
| #393 - redline55 | Success | Nov 19, 2018 9:44 PM | 4min 39s |

Stage View

Average stage times:

| Stage | changeLog | validation | preprod | Waiting for prod approval | prod |
|---------------------------|-----------|------------|---------|---------------------------|----------|
| changeLog | 2min 19s | 152ms | 39s | 70ms | 2min 33s |
| validation | 1min 53s | 585ms | 39s | 50ms | 3min 52s |
| preprod | 1min 39s | 1s | 34s | 96ms | 3min 24s |
| Waiting for prod approval | 1min 50s | 1s | 36s | 67ms | 1min 47s |
| prod | 4min 39s | 605ms | 35s | 79ms | 1min 52s |

14

After merge, a deployment pipeline is created in Jenkins

- Automatically applies to preprod
- Waits for approval to deploy to prod
- Deploys to prod
- Run inspec on environment after each deployment.

The tools



16 •

criteo.

We have integrated other tools too

- Notifications to to slack
- Alerts go to OpsGenie
- etc

Future Enhancements



- Improving our Inspec implementation
- More TF modules
- Delegating to other teams
- Docker...
- TF validation
- Prometheus for alerts
- Project Atlantis

17 •

criteo.

- Improving our inspec implementation
 - Implemented using `azure_generic_resource`
 - Two weeks later they deprecated it
 - We have been contributing to the project to add the resources we need
 - Wrote the book
- More TF modules
 - We use some but we want to use more
- Delegating to other teams
 - They consume our modules and the pipeline deploys their stuff to prod
 - Starting with Storage Accounts
- Docker
 - Containerize the runtime environment in which terraform runs.
 - Waiting on our Jenkins servers to be updated to support docker
- TF validation
 - A mechanism to validate that our TF code is going to succeed, not just

written correctly

- Example: The VM sizes are valid or naming conventions are followed
- Exists for AWS, but not for Azure
- Prometheus for alerts
 - Improved Alerting
- Project Atlantis
 - We would use this if it supported Gerrit.

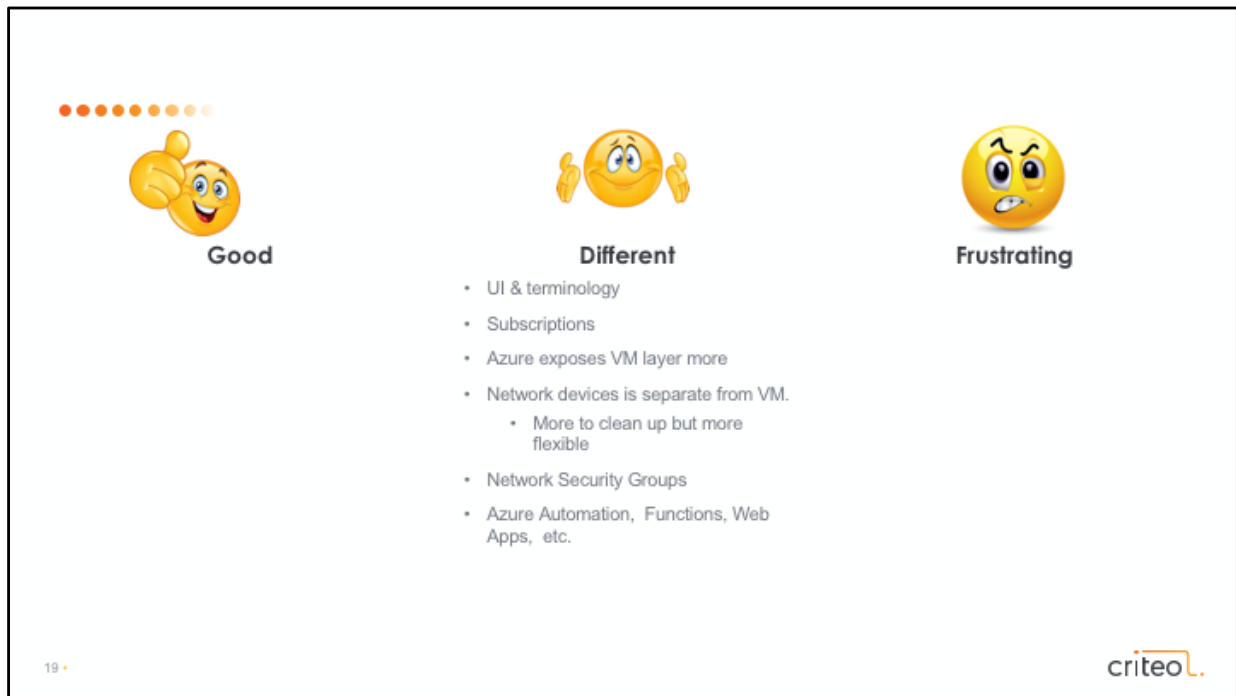
The moral of the story a.k.a: The good, the different, and the frustrating

.....

criteo.

Back to Azure

I sat my team down in a room and we discussed our impressions of Azure. We tried to categorize things as good, different, and frustrating. While I don't have time to go over all of our thoughts in detail, I will try to highlight some of them. Feel free to discuss the others with me, or a team mate afterward.

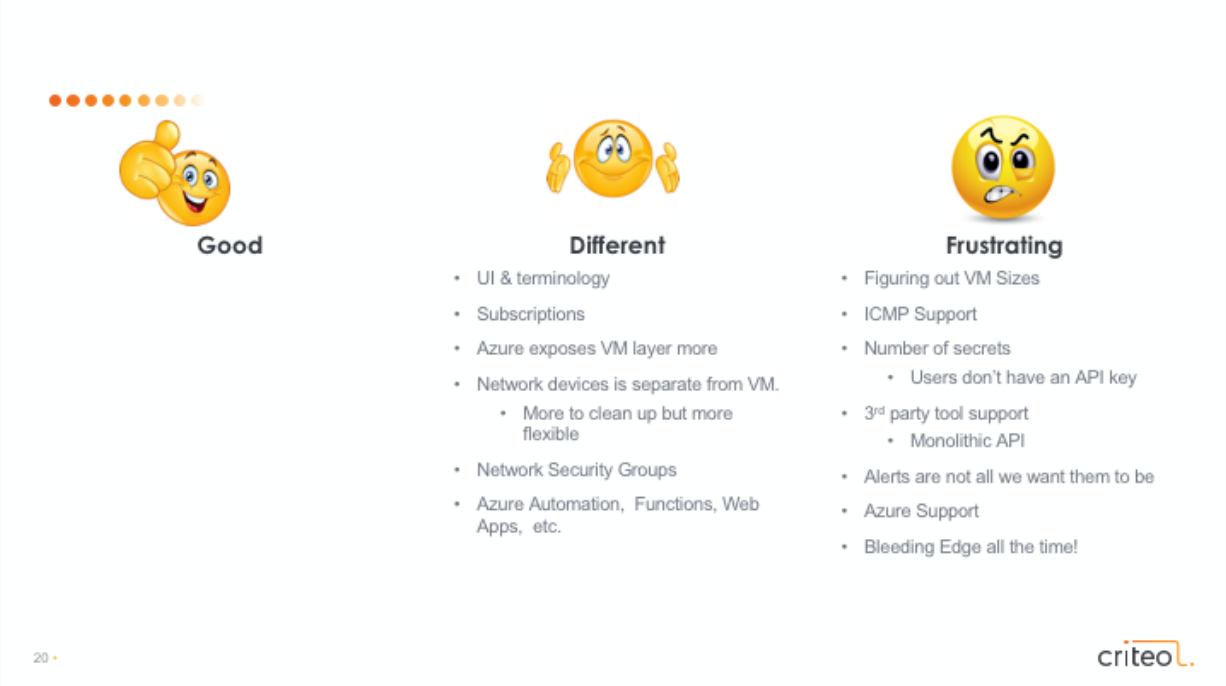


I'll start with different, then go to frustrating, finish with good. Mom always says Its best to end on a good note.

We classified something as different when it wasn't better or worse, just different

- UI & Terminology – Have to get use it it
 - We all agree that you can get a bit lost in the UI at times.
 - We like that we can see all regions at once
- Subscriptions – Sorta like an AWS account, but it isn't.
 - We aren't sure how we feel about these.
 - In the past we have used separate AWS accounts to act as a security boundary. Now we are using subscriptions.
 - Fits into that unified UI experience.
- Azure exposes more of the VM layer.
 - Less of a black box
 - Not sure if that is a good thing.

- Network devices are separate from the VM.
 - More to clean up
 - More flexible
- Network Security Groups
 - More like a firewall than an AWS NSG
 - Two layers of NSGs to manage
 - So.. Maybe better security, but also more to manage
- Azure being serverless first gives more options for serverless computing.
 - Azure Automate
 - Azure Functions
 - Azure Web Apps
 - Etc.
 - Still figuring out when to use what where.



Good

Different

- UI & terminology
- Subscriptions
- Azure exposes VM layer more
- Network devices is separate from VM.
 - More to clean up but more flexible
- Network Security Groups
- Azure Automation, Functions, Web Apps, etc.

Frustrating


- Figuring out VM Sizes
- ICMP Support
- Number of secrets
 - Users don't have an API key
- 3rd party tool support
 - Monolithic API
- Alerts are not all we want them to be
- Azure Support
- Bleeding Edge all the time!

20 • criteo

What do we dislike:


- Figuring out VM Sizes
 - Not as straight forward and harder to find in the documentation
- ICMP Support
 - Lacking
- Number of secrets
 - Users don't have an API key
- 3rd party tool support
 - Not on par with what is available for AWS
 - Tools missing or less
 - Lag behind in new features
 - Monolithic API
- Alerts are not all we want them to be

- Azure Support
 - Beyond level one is slow and sometimes unhelpful
- Bleeding Edge all the time!




Good

- Bleeding Edge all the time!
- Resource Groups
- Networking
- Locations
- Azure CLI
 - shell.azure.com
- Resize an VM on the fly
- Azure Support
- Storage Accounts
 - Bundle things
 - SAS Tokens
- Management Locks



Different

- UI & terminology
- Subscriptions
- Azure exposes VM layer more
- Network devices is separate from VM.
 - More to clean up but more flexible
- Network Security Groups
- Azure Automation, Functions, Web Apps, etc.



Frustrating

- Figuring out VM Sizes
- ICMP Support
- Number of secrets
 - Users don't have an API key
- 3rd party tool support
 - Monolithic API
- Alerts are not all we want them to be
- Azure Support
- Bleeding Edge all the time!

21
criteo

What do we like:

- Bleeding Edge all the time!
 - We have access to all the public previews we want
 - They are actively making improvements at a rapid pace
 - Shared Image Gallery
- Resource Groups
 - We like how everything is grouped together and can be deleted all in once shot
- Networking
 - Its magic
 - Hub and Spoke Networking
 - Sharing ExpressRoute Connection
 - Using the Azure Backbone for Inter-Office connections
- Locations
 - 16 AWS Regions with 42 Availability Zones
 - 54 Azure Regions world wide
- Azure CLI
 - Extensable
 - Aliases

- Shell.azure.com
- Resize a VM on the fly
 - Without rebooting!
- Use case support is high
- Azure support
 - First level support has been great!
- Storage Accounts
 - Bundle all the things
 - SAS tokens
- Management Locks

Final thoughts



- You will love working in Azure if you like working on the bleeding edge!
- Azure has a lot of service offerings to cover any need
- Definitely worth considering

