
Fuzzy Clouds
Using Amazon AWS to fuzz applications

Topics

- Fuzzing
- Amazon AWS
- Using CloudInit to launch a fuzzing campaign
- Bonus: Spot instances

Fuzzing / Fuzz Testing

"... a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks."

- Wikipedia

Basic Fuzzing Framework (BFF)

- Cert-developed fuzzing framework
- Built on open source fuzzer "zzuf"
- Available as a DebianFuzz ISO VM or source package

Basic Fuzzing Framework (BFF)

- Cert-developed fuzzing framework
- Built on open source fuzzer "zzuf"
- Available as a DebianFuzz ISO VM or source package
- Time to leverage the cloud!

Amazon AWS

- Compute and Networking
- File/Object Storage and CDN
- Database
- Application Services
- Deployment and Management

Amazon AWS

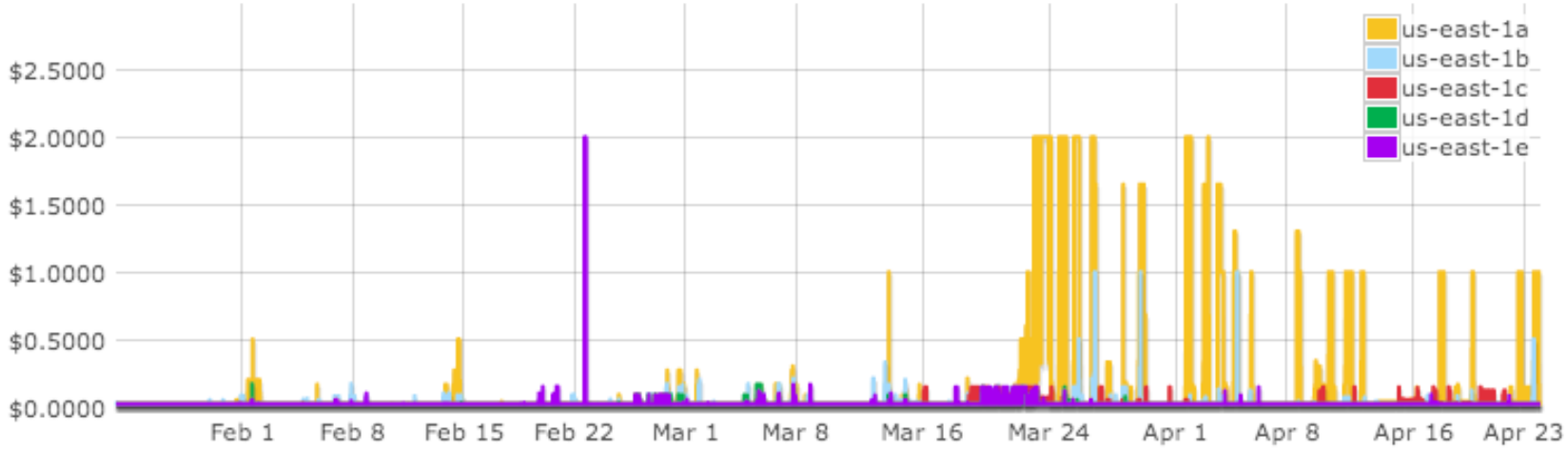
- Compute and Networking
  - **EC2**, Load Balancing, VPC, DNS, etc.
- File/Object Storage and CDN
  - **S3**, Glacier, Elastic Block Storage, Coudfront, etc.
- Database
  - SimpleDB, RDS (Relational), DynamoDB, etc.
- Application Services
  - Email, Search, Transcoding, etc.
- Deployment and Management
  - **Console**, Access Management, Cloudwatch, etc.

BFF in AWS with EC2 and S3

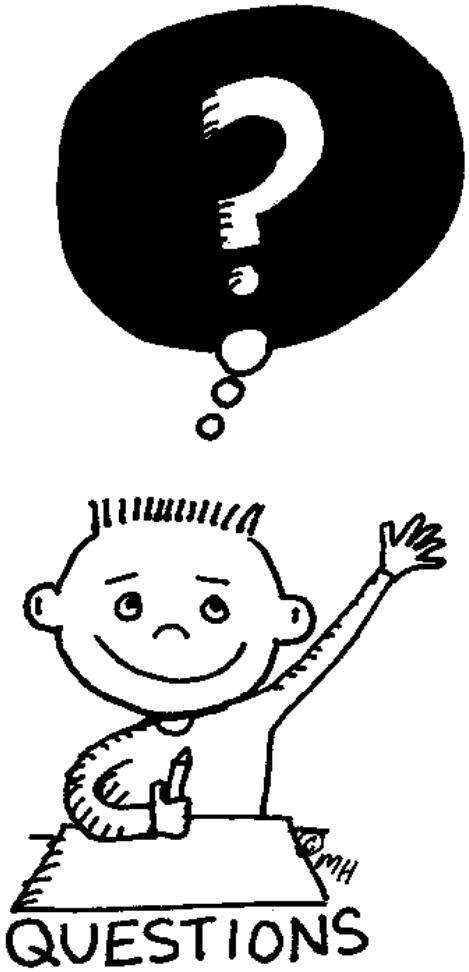
- CloudInit
- Install BFF as usual
- rsync-style sync to S3 with s3cmd
  - http://s3tools.org/s3cmd
- CLI apps fuzz in a "screen" session
- GUI apps
  - Install LXDE
  - Launch LXDE and BFF in a virtual framebuffer using Xvfb
  - x11vnc to attach to the virtual framebuffer
- Demo time

Bonus Tip: Spot Instances

- Market-set rather than standard EC2 prices
  - Standard on-demand prices
  - Spot prices
- Can be volatile with market fluctuations



- Make sure your workload will not be disrupted if prices spike and your servers die.



- Shaun Blackburn
sblackbu@andrew.cmu.edu