Building Resilient Systems on AWS

Instructor:
Rock Mutchler
Day 2

Welcome Back!!!
Review / Q&A

Questions from Yesterday?

9:00 – 9:30
Fault-tolerant and self-healing systems
High Availability

- Multi-Region
- Multi-AZ
- Load balancers everywhere
- Operational Visibility
What is Self Healing

- Detecting Failures Automatically and Recovering Automatically
  - When / How does this happen?
    - EC2
      - Status Check Fails on an Instance
    - OpsWorks Layer - EC2
      - Status Check Fails on an Instance
      - Stack Agent loses communication for approximately 5 minutes
  - Scripted
    - Manual Polls of Instances with custom criteria to launch new instances
Self Healing - HealthCheck / AutoScaleing

- AutoScaling Group Behind an ELB has a Failure
  - ELB health check detects this failure
    - Launches a new instance to maintain autoscale group size
    - *note - failed instances in this case will remain active (billing)
      - Terminate Automatically
      - Keep around for debugging then terminate
Self Healing - Recover Action

- Alert Set on an Instance or Group of instances
  - Monitors Single Metric
    - StatusCheckFailed_System
  - Alert Action Setting
    - AutoRecovery
Self Healing - 3rd Party Thresholds

- 3rd Party Monitoring Applications
  - Some 3rd Party Applications
    - Threshold is hit
      - Event is triggered
        - Event Launches New Piece (EC2 or other) via scripts
          - (could be SNS / Lambda could be CLI Script etc...)
Self Healing - 3rd Party Thresholds

- 3rd Party Monitoring Applications
  - Outlier detection
    - Systems that are not behaving like other systems in their group
      - These Systems Marked for ‘Auto Healing’
      - Basically Replacement, then Termination
Self Healing - CloudTrail

- Healing Unhealthy but Running Instances
- CloudTrail logs Stored in S3
  - Athena to query these logs to find unhealthy / failing systems
  - React to query results via AWS CLI to relaunch / replace bad instances
  - Hurdle with this CloudTrail stores logs in JSON format, Athena does not read this natively and SerDe has to be used to aid Athena / Hive with reading the logs.
  - Information on how to do this can be found here:
  - Reaction could be a SNS as a trigger for a Lambda Function
Self Healing - Requires Downtime

- For instance automated DR on a Database
  - How to deal with this
    - Run in a degraded mode (degraded is better than down)
      - S3 and Route53 switch over while process is taking place
      - 100% weight to one or the other for quick shifts
      - Shift can be done automated with AWS CLI

- Understood Not Popular or an Answer Wanted, but something that should be considered if you are not 100% HA
Morning Break

Do what you forgot to on the way here this morning

10:30 – 11:00
Fault-tolerant and self-healing systems

Little Demo

11:00 – 12:30
Fault-tolerant and self-healing systems

- AutoScaling Group in OpsWorks
- OpsWorks Self Healing
- Auto Recovery with EC2 instances
- AutoScaling with EC2 Groups
- RDS multi AZ
  - Trick to test multi AZ db Server
- DC/OS on AWS EC2 Advances
  - Kicking over a node
Disaster Recovery

Disaster recovery and business continuity approaches

1:30 – 2:00
Disaster Recovery & Business Continuity

- Know your Recovery Point Objective (RPO)
- Know your Recovery Time Objective (RTO),
- Complete automation is a hard requirement
- Strategies are usually tied to costs
- The 3 most common DR strategies
Disaster Recovery & Business Continuity

- Pilot light (AZ vs Region)
  - Data replication, complete automation in place
  - Small RPO (no data loss)
  - Short RTO (platform is up in minutes)
  - Inexpensive
Disaster Recovery & Business Continuity

- Failover
  - A complete, fully functional copy running elsewhere
  - Small RPO (no data loss)
  - Short RTO (failover takes a few minutes)
  - Expensive
Disaster Recovery & Business Continuity

- Restore from backups
  - High RPO (hourly vs daily snapshots)
  - Long RTO (hours or days)
  - Expensive, risky, error prone, all hands on deck, panic
Disaster Recovery & Business Continuity

- Test Regularly
  - Measure each test
  - Practice makes you better
    - Build confidence
DDoS Mitigation

Protect and Defend
More than just DDoS to Cover

2:00–3:00
Protection - WAF

- Web Application Firewall (WAF)
  - Associate with a ALB (Application Load Balancer)
  - Control over which traffic to allow and deny
    - Block / Allow
    - Pay by Request and number of rules
  - Rules
    - XXS
      - First Portion of Body Check
    - URI Based
    - Query String
      - Block on exact or patterns
    - SQL Injection
  - View into number of requests / hits
- DNS and CloudFront
- Third Party
  - CloudFlare
    - Offers good protection on Layer 3, 4 and 7,
    - Requires premium account to be truly robust
Protection - WAF

- Quick Setup of a WAF
  - DEMO
Protection - DDoS Shield - Standard

- Automatic Process
- Standard Shield is Free
  - Network Flow Monitoring
- Common DDoS Attacks Blocked
  - UDP reflection attacks
  - SYN Floods
Protection - DDoS Shield - Advanced

- Automatic Process
  - $3000 a month plus transfer fees
  - WAF included
- Standard Shield is Included
  - Network Flow Monitoring
- Common DDoS Attacks Blocked
  - UDP reflection attacks
  - SYN Floods
- Active Monitoring
  - Automated application (layer 7) traffic monitoring
- DDoS Mitigation
  - Access to additional DDoS mitigation capacity
- Visibility and reporting
  - Layer 3/4 attack notification and attack forensic reports
  - Layer 3/4/7 attack historical report
- DDoS Response Team
  - Incident management during server events
Protection - DDoS Shield - Advanced

- DDoS Response Team
  - Custom mitigations during attacks
  - Post-Attack Analysis
- Cost Protection
  - Reimburse related Route 53, CloudFront, and ELB DDoS charges
Protection - AWS Marketplace

- A wealth of third party security products
- Some are tied to specific AWS Regions
- Bring your own license products (great if you recently migrated to AWS)
- Varying cost (some are free)

https://aws.amazon.com/marketplace/b/2649363011?ref_=hmpg_categories_2649363011
Protection - DDoS Mitigation

- Similar 3rd Party Product to AWS Shield
  - CloudFlare
    - https://www.cloudflare.com/
Afternoon Break

Last Break

3:00–3:30
Lab

Implementing a resilient, fault-tolerant design

3:30 – 5:00
Thank you!!!

Slides and links will be provided

Pythian
velocityconf.com
#VelocityConf

Rock Mutchler
mutchler@pythian.com
Links

- External Materials
  - [https://github.com/devopsified/elk_opsworks](https://github.com/devopsified/elk_opsworks)
    - To get them to S3 as a tar.gz
      - `cd elk_opsworks`
      - `berks vendor`
      - `cd ./berks_cookbooks`
      - `mv * ../`
      - `Cd ../`
      - `rm -rf ./berks_cookbooks`
    - Then Tar.GZ them up and upload to S3 bucket for opsworks use
- DC/OS
  - Running it about
    - [https://dcos.io/docs/1.9/installing/cloud/aws/basic/](https://dcos.io/docs/1.9/installing/cloud/aws/basic/)
  - CloudFormation Templates