AWS Best Practices

References / Resources

- AWS tips by Rich Adams
- AWS Open Guide

Development

- [ ] Do not store application state on servers
- [ ] Store extra information in your logs
- [ ] If you need to interact with AWS, use the official SDK
- [ ] Have tools to view application logs

Billing

- [ ] Set up granular billing alerts.

Security

- [ ] Prefer EC2 roles over app level IAM account.
- [ ] Assign permissions to groups, not users.
- [ ] Set up automated security auditing.
- [ ] Use CloudTrail to keep an audit log.

ELB

- [ ] Terminate SSL on the load balancer.
- [ ] Pre-warm your ELBs if you're expecting heavy traffic.

RDS

- [ ] Set up event subscriptions for failover.

CloudWatch

- [ ] Use CLI tools.
- [ ] Use the free metrics.
- [ ] Use the custom metrics.
- [ ] Use detailed monitoring.

IAM

- [ ] Use IAM roles.
- [ ] Users can have multiple API keys.
- [ ] Use multi-factor auth for IAM users

Miscellaneous

- [ ] Scale horizontally
- [ ] Your application may require changes to work on AWS.
- [ ] Always be redundant across availability zones (AZs).
- [ ] Be aware of AWS service limits before you deploy.
- [ ] Decide on a naming convention early, and stick to it.
- [ ] Decide on a key-management strategy from the start.
- [ ] Make sure AWS is right for your workload.

Operations

- [ ] Disable SSH access to all servers (Optional)
- [ ] Care about service as a whole instead of servers.
- [ ] Don't give servers static/elastic IPs.
- [ ] Automate everything.
- [ ] Everyone gets an IAM account. Never login to the master.
- [ ] Get your alerts to become notifications.

S3

- [ ] Use "-" instead of "." in bucket names for SSL.
- [ ] Avoid filesystem mounts (FUSE, etc).
- [ ] Having CloudFront in front of S3 is optional (but it can help).
- [ ] Use random strings at the start of your keys.

EC2/VPC

- [ ] Assign tags to everything.
- [ ] Use termination protection for non-auto-scaling instances.
- [ ] Use a VPC
- [ ] Use reserved instances to save big $$$.
- [ ] Lock down your security groups.
- [ ] Don't keep unassociated Elastic IPs.

Elasticache

- [ ] Use configuration endpoints over individual node endpoints.

Auto-Scaling

- [ ] Scale down on INSUFFICIENT_DATA as well as ALARM.
- [ ] Use ELB health check instead of EC2 health checks.
- [ ] Only use the availability zones (AZs) your ELB is configured for.
- [ ] Avoid multiple scaling triggers on the same group.

Route53

- [ ] Use ALIAS records.

Elastic MapReduce

- [ ] Specify a directory on S3 for Hive results.