Identity and Access Management (IAM)

ROGER SIGGS
22FEB2017

Best Practices and Hints

- Basics
- Some more basics
- No really- it’s all basics
- Next Steps
- Q/A

Basics (IAM 102)

- CREATE AND USE IAM USERS RATHER THAN THE ROOT ACCOUNT
- GRANT LEAST PRIVILEGE
- USE GROUPS FOR ROLE MANAGEMENT
- CONFIGURE A STRONG PASSWORD POLICY (*DEBATABLE*)
- USE EC2 ROLES

User/Group/Policy Tips (pt 1)

- USE ENVIRONMENT/ACCOUNT IDENTIFIER WHERE POSSIBLE
  - (roger.siggs-dev; roger.siggs-prod)
- AUTOMATE CREATION OF RESOURCES
  - IAM users and groups are just another resource type to manage. Use your tooling to maintain them
- USE GROUPS AS YOUR 'POLICY CONTAINER'
  - Inline policies at the user level are a pain to manage. Groups are a nice mid-tier layer to work with
- ENSURE ROTATION OF CREDENTIALS REGULARLY
  - Minimize the threat window, decrease time to recover
- USE EC2 AND IAM ROLES
  - Allows for system access to AWS resources without the need for key and credential management

More Basics (IAM 102)

- ENABLE AUDITING OF API CALLS (CLOUDTRAIL)
- REQUIRE MFA FOR CONSOLE AND API ACCESS
- USE ACCESS ADVISOR TO IDENTIFY PERMISSIVE POLICIES
- USE IAM ROLES
- USE EC2 ROLES

Tips (pt2)

- REQUIRE MFA
  - Enable User self-service and require MFA by policy
- CREATE AN 'EVERYONE' GROUP
  - Default container for MFA policies, as well as an easy audit verification for user management
- USE AWS TOOLS FOR AUDITING
  - Cloudtrail for API calls; SNS topic for alerts
  - Config and Cloudwatch for system and state logging
- AUTOMATE!
  - Make as much of your account management automated as possible – prevent errors, protect against costs. Easy to audit and report against

No really- It's all basics

- USERS – CREATE INDIVIDUAL USERS
- GROUPS – MANAGE PERMISSIONS AT THIS LEVEL
- AUTHENTICATION – USE COMPLEX AND ROTATED CREDENTIALS
- MFA – 2ND LAYER OF PROTECTION, FOR API AND CONSOLE
- ROLES – IAM AND EC2 FOR EPHEMERAL ACCESS (NO KEYS NEEDED)

Contact

- ROGER SIGGS -
  - rsiggs@gmail.com
  - @rsiggs

- HTTPS://WWW.LINKEDIN.COM/IN/ROGERSIGGS

- HTTPS://GITHUB.COM/RSIGGS
  - https://github.com/rsiggs/AWS_2017_Meetup