AWS Account Best Practices

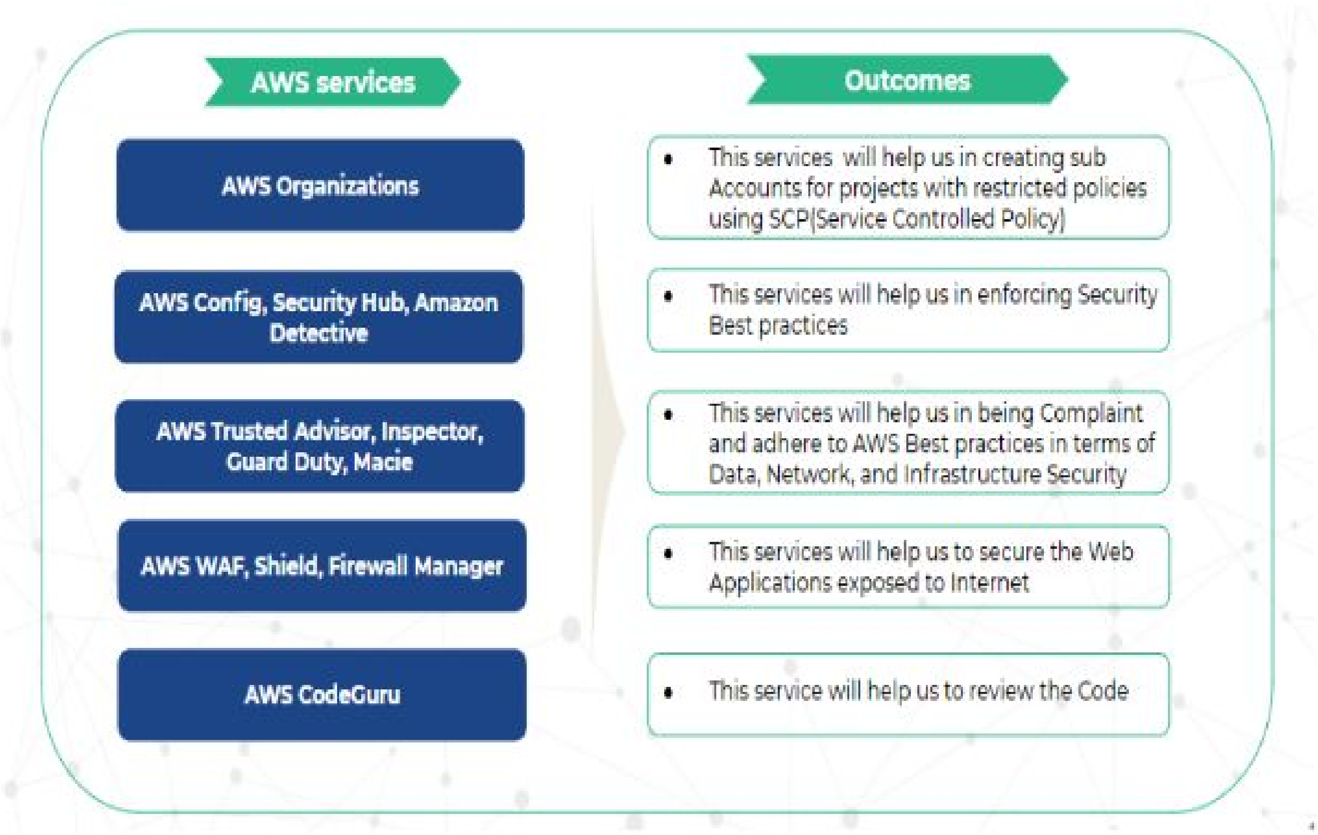
using Terraform and Shell scripts

Contributor: Sanket Surendra Wagh

Document creation date: May 16, 2020

Last update date: May 16, 2020

Overview:



AWS services	Outcomes
AWS Organizations	- This services will help us in creating sub Accounts for projects with restricted policies using SCP(Service Controlled Policy)
AWS Config, Security Hub, Amazon Detective	- This services will help us in enforcing Security Best practices
AWS Trusted Advisor, Inspector, Guard Duty, Macie	- This services will help us in being Complaint and adhere to AWS Best practices in terms of Data, Network, and Infrastructure Security
AWS WAF, Shield, Firewall Manager	- This services will help us to secure the Web Applications exposed to Internet
AWS CodeGuru	- This service will help us to review the Code

The figure depicts various AWS services and their outcomes

How can we restrict users from a project not to modify other project resources?

- Resolved the issue by assigning **resource-level IAM** *Policy* based on tags (i.e using the **project-specific** tag)

NOTE: Here **GroupA** refers to the **project** name to be used at the time of **ec2 creation** or else the policy won't allow the user to create the resource. The **region** in the policy is **strictly restricted** to **us-east-1 (North Virginia).** After the resource creation, no user will be allowed to modify the resource tags for **better control** of the resource. This **IAM policy** can be attached to an **IAM Group** and the respective **users** can be placed under this **group** indicating they are working under the **same project** (GroupA in our case)

What if there are exceptions i.e, a particular user is working into multiple projects?

- Such **exceptional users** can be added to a **separate IAM group** and assigned permissions to a group level or using **IAM roles.**

How can we delete the default VPC's and the resources associated with it from all the regions inside a fresh AWS Account?

- In order to **delete** the **default VPC**, you can trigger a shell *Script* from an EC2 instance in the same account which has an IAM role attached to it with all the **admin privileges**.

NOTE: *This script can be* ***executed*** *in* ***2 ways*** *-* ***First*** *by manually specifying the regions in a* ***regions.txt*** *file by* ***commenting out*** *the describe-regions part in the script.* ***Second*** *by* ***uncommenting*** *the* ***describe-regions*** *part which will include all the regions and the VPC resources in it for deletion.*

How to create a member/child account using AWS Organizations inside an existing AWS Organization?

- In order to create a **member/child** account to an **existing AWS Organization**, you can use the terraform *Script*. This terraform script expects only **3 parameters** i.e, member account name, email ID, and parent ID(OU ID).

NOTE: *This script expects the **terraform client** to be already set up onto an **EC2 machine** in order to execute **successfully**. The installation steps are Here.*

How can I enforce the default security best practices prescribed by AWS for securing my fresh AWS account using AWS Config rules?

- In order to **enforce** the security best practices using **AWS Config rules**, this terraform *Script* can be used which contains **16 such must-have** config rules. This script only **expects** your **AWS Account ID** and it has **us-east-1(North Virginia)** as the **default** region selected for **creating** the rules.

NOTE: *All the above-described ways, methods, scripts can easily be collated inside a single terraform script and the respective shell scripts can be invoked via a single terraform script as per the requirement. This will help you in triggering the single terraform script from a different AWS account altogether as well.*

Proposed Resources:

Services	Where to use them?	Pricing	Cost Model	Reference	Comments
AWS Organizations	In each sub-account	Free	Free	AWS Organizations Pricing	Free and should be incorporated only in the root account
AWS Config	In each sub-account	~$10/month (estimated in our case subject to config rules configured)	Pay-as-you-go	AWS Config Pricing	Config rules in each sub-account won't go above 500 as per our estimations
AWS Security Hub	In each sub-account	~$20/month	Pay-as-you-go	AWS Security Hub Pricing	Security Hub's compliance checks are not charged.
Amazon Detective	Depends upon account	$2/GB for first 1,000 GB data/account/region/month	Pay-as-you-go	Amazon Detective Pricing	Amazon Detective is currently in preview. During the preview, there is no charge for using Amazon Detective.
AWS Trusted Advisor	Depends upon account	$100/month	Pay-as-you-go	AWS Trusted Advisor Pricing	If you have a Business plan for support which is $100/month that is sufficient for the root account
Amazon Inspector	Depends upon account	$0.30/month for first 250 agent-assessments	Pay-as-you-go	Amazon Inspector Pricing	Free for first 90-days Using Amazon Inspector
Amazon GuardDuty	Depends upon account	$1.00/GB/month for first 500 GB - VPC Flow Log and DNS Log Analysis $4.00 per 1 million events/month - AWS CloudTrail Event Analysis	Pay-as-you-go	Amazon GuardDuty Pricing	$1.00/GB/month for first 500 GB - VPC Flow Log and DNS Log Analysis $4.00 per 1 million events/month - AWS CloudTrail Event Analysis

Services	Where to use them?	Pricing	Cost Model	Reference	Comments
Amazon Macie	Only in production accounts	$533/106GB S3 data for 90 days NOTE-In our scenario it won't cost more $100 (again depends upon project and data consumed)	Pay-as-you-go	Amazon Macie Pricing	No charge for the first 1 GB processed by the content classification engine After first GB, $5.00 per GB processed by the content classification engine No charge for the first 100,000 events After first 100,000 events, $4.00 per 1,000,000 events A charge of $0.05 per GB processed for each month beyond the initial 30 days
AWS WAF	POC and R&D accounts only	~$30/month	Pay-as-you-go	AWS WAF Pricing	Web ACL - $5.00 per month (prorated hourly) Rule - $1.00 per month (prorated hourly) Request - $0.60 per 1 million requests
AWS Shield	In each sub-account	Free	Free	AWS Shield Pricing	Free
AWS Shield Advanced	Only in production account(Depends on client requirements)	$3,000	Yearly	AWS Shield Pricing	To be implemented only after getting approval from the client
AWS Firewall Manager	Depends upon account	$106/Month	Per month/ per region	AWS Firewall Manager Pricing	AWS Firewall Manager handles three types of protection policies - AWS WAF, AWS Shield, and Amazon VPC security groups. AWS Firewall Manager protection policies are priced with a monthly fee per Region.
AWS Code Guru	In each sub-account	$18 per developer per month	Pay-as-you-go	Amazon CodeGuru Pricing	Free tier -90-day free trial Post that $0.75 per 100 lines of code scanned per month

References:

- AWS Security
- AWS Organizations
- AWS Config
- AWS Security Hub
- Amazon Detective
- Amazon Inspector
- Amazon GuardDuty
- Amazon Macie
- AWS Trusted Advisor
- AWS CodeGuru
- AWS WAF
- AWS Shield
- Amazon Firewall Manager
- AWSBest Practices