AFTでAWSアカウントをばら撒いてみた

アップデート紹介とちょっぴり DiveDeep する AWS の時間
2023/08/21

HENNGE株式会社
Cloud Product Development Division | 土居 俊也
Internal IT Section | 穂坂 栄一

HENNGE

AWSアカウント管理

HENNGE が Account Factory for Terraform を導入して実現できたこと

2023-08-02
ビジネス x クラウド

土居俊也, 穂坂栄一 (HENNGE K.K.)

こんにちは、HENNGE 株式会社 (以下 HENNGE) の土居と穂坂です。

Account Factory for Terraform (AFT) とは何か、という ブログが公開 されました。AFT を使うことで AWS Control Tower と連携して Terraform から AWS アカウント作成ができます。AFT を利用する目的の 1 つとして AWS 内でのリソース管理だけでなく、AWS アカウントの作成も Terraform で実施することができるようになる点があります。

今回は実際に AFT を使っている私たちから、なぜ AFT を導入したのか、AFT を導入する際に困った点、導入によって変わったことについてお伝えいたします。

40アカウント超えたあたりでスプレッドシートでの管理を辞める検討を開始

AWS Control Tower Account Factory for Terraform (AFT) for 100+ AWS accounts

悩み

1. 複数アカウントの運用
2. IAMポリシーの制限

悩み1

- AWSベストプラクティスに従い、stagingとproductionを常に用意
  - AWS Well-Architected
  - AWS FTR
  - AWS Whitepaper
    - Organizing Your AWS Environment Using Multiple Accounts

→ 年々、AWSアカウントが増加。

→ 40を超えたあたりからいよいよカオスに。

悩み2

- AWSベストプラクティスに従い、IAMの権限設定は常に必要最小限
- IAM RoleとIAM Policyはterraformで管理
- 権限付与はPull Request経由の相互承認によって行う
- Productionとstagingの環境と極力同じにするため、stagingでもAWS ConsoleからIAMの直接編集を制限

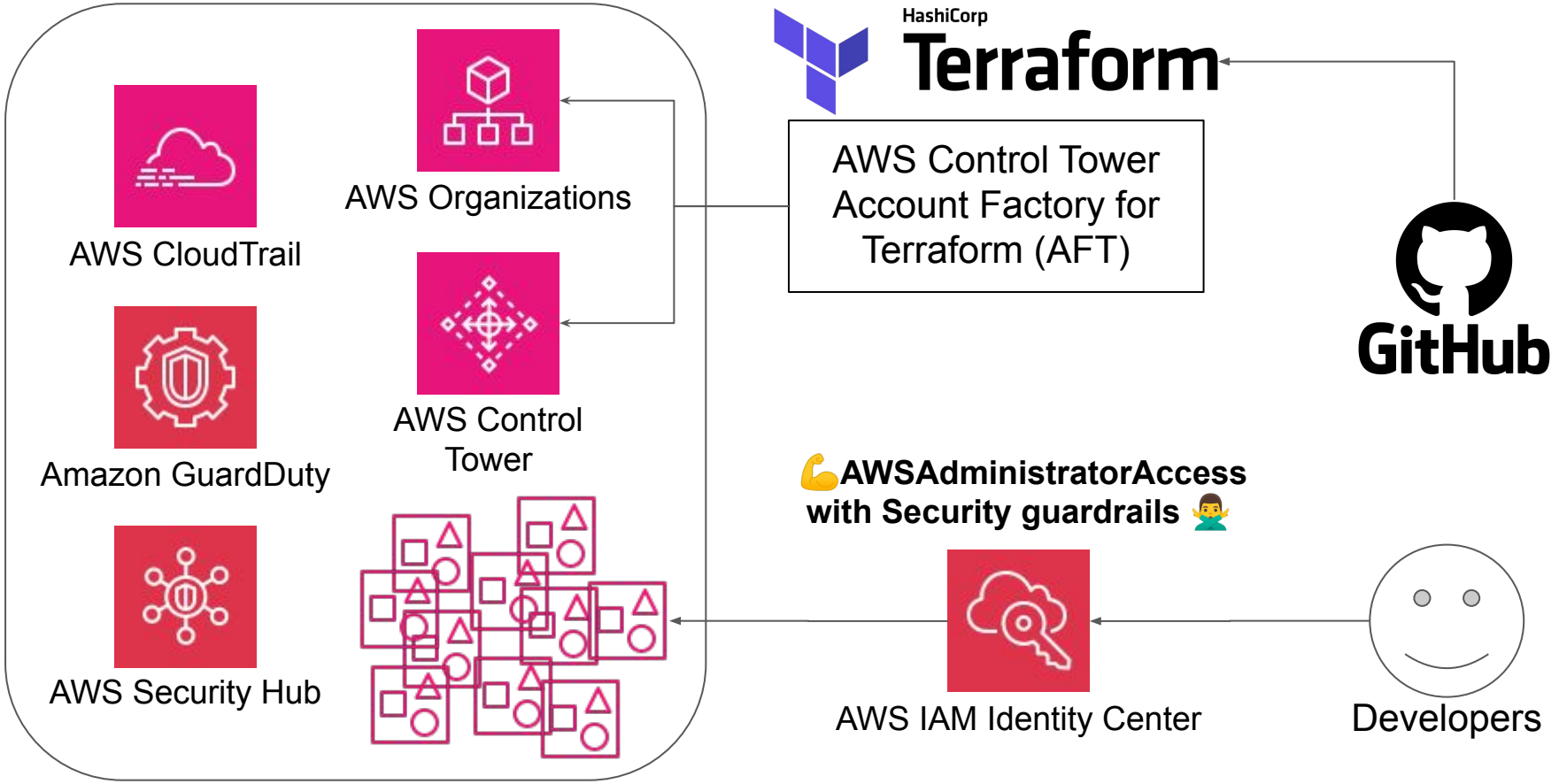
→ PoC/R&D的な開発体験はお世辞にも良いとは言えない...

→ 新しいサービスを試すハードルがいちいち高い...

楽に管理したい
セキュリティも担保したい
人的リソースは多くない

方針:
Only Managed Services
二人で頑張る💪

実装の全体像



得られた効果

- クラウドのコスト構造への理解促進
- IAMへの理解促進
- 新サービスを試す機会創出
- AWS Certificate
- PoC
- iamliveによるterraform applyで必要な権限チェック
  - https://github.com/iann0036/iamlive

AWSアカウント管理の変遷

Before AWS Organizations

特に明文化されたプロセスもなく、知っている人に作り方を教えてもらう、もしくは勝手に作ってしまうような状態。

請求の紐付けを依頼されて初めて存在を把握するような体制でした……

状態を改善すべく、まずAWS Organizationsの全ての機能を有効にし、アカウント作成プロセスの巻き取りとAWS IAM Identity Centerによるアクセス制御、Service Control Policyを使った緩やかな制限の導入からスタートしました。

After AWS Organizations

AWS Organizations

Organizationsの有効化により、多少は改善したものの、メンバーが限られていたこともありなかなか対応できない部分もありました。

そんな中、マネージドでガバナンスを効かせることができるAWS Control Towerが利用可能になったのを知り、すぐに利用を開始しました。

（当時のSlackを確認したところ、アナウンスの五日後に有効化していました）

After AWS Control Tower

AWS Control Tower

AWS Control Towerを利用することでますますアカウント管理が容易になり、ガードレールの整備もできたのですが、複数の作業を並行できないなど（当時）課題もまだありました。

そんな時にAccount Factory for Terraform (AFT)の存在を知り、苦戦しながらも無事導入し、今に至っています。

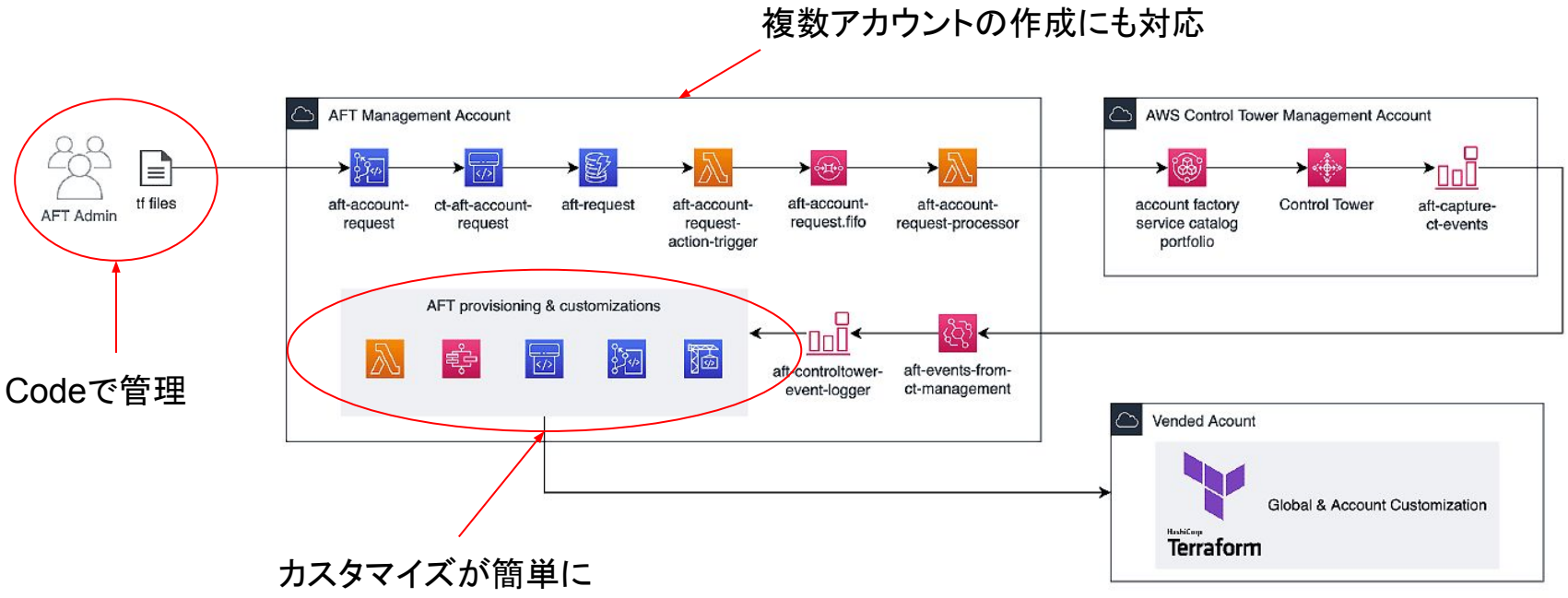
With AFT（現在）

AWS Control Tower

AFTを導入することでアカウントの作成が容易になり、当初から悲願だった開発者用のSandboxアカウントを全員に配布する事が可能になりました。

また、現在ではほぼほぼ全てのAWSアカウントをAFT配下で管理しています。（一部本番環境はControlTower配下に移動した際の影響が大きいため、そのままとしています）

AFTを導入してよかったポイント



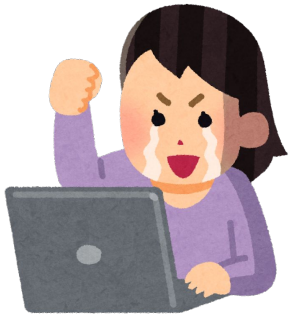
劇的ビフォーアフター

Before

UI上での操作。一つの作業が終わるたびにポチポチが発生し、待ち時間が発生していた。

After

tfファイルを編集し、pushして（ほぼほぼ）終わり。複数アカウントの発行も簡単に。



AWS Control TowerとAFTにより実現できたガードレール

自由を与えつつ、予期せぬ事故を防げれば良しといった考えをベースにしています。

・Rootアカウントの無効化とMFAの徹底

・Amazon GuardDuty, AWS Security Hub, AWS CloudTrailなどのマネージドセキュリティサービスの有効化

・Region制限

・IAM Userの制限

・Instance Familyの制限

・購入系APIの制限

AFTのカスタマイズ機能により実現したこと

・各種AWSアカウントに対して正確なタグ付け。これにより、アカウント単位でのコスト管理がより楽になりました。

・コストをモニタリングし、自動でSlackにポストする仕組み

・各SandboxアカウントのAmazon Route 53に自由に利用できるhosted zoneを自動で作成

・AWS CloudTrailを有効化するアカウントの制御

今後の展望

・PoCの開発をより加速させるため、AWS ProtonやAWS App Runnerのテンプレートの準備

・Sandbox以外のアカウントにてよりセキュアなアクセス制御を行うため、Temporary elevated access management (TEAM)の導入

AWS Proton

AWS App Runner

TEAM

ご清聴
ありがとうございました