[deft]

Cloud Discovery and Assessment

Findings and Recommendations

A SAMPLE ARTIFACT

v21.4

Executive Summary

At Deft, we're experts in converting complexity into success. We work with companies, large and small, that recognize IT as the foundation for their success. We support our customers with managed cloud services, cloud consulting, cloud native software development, managed data center services, and business continuity solutions.

Deft has been asked to assess your company's AWS account(s), including, but not limited to:

- All production and development workloads and related infrastructure;
- CI/CD workflows, platforms and practices that are planned and currently in place; and
- Additional cloud services and on-prem applications and environments that may be relevant to developing a comprehensive understanding of your environment

This high-level overview will outline and explain what we have found during our discovery phase beginning [DATE], while also outlining recommendations for any newly created environments going forward.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Primary Goals

Our primary goals for this Discovery & Assessment include, but are not limited to:

- Identifying pain points related to infrastructure, management and monitoring.
- Identifying areas that can be retooled or modernized to meet internal and external security goals and to increase and improve billing transparency.
- Identifying areas that can be retooled or modernized to provide automation for system scaling to meet future demands, to optimize deployment efforts that allow for improvements in the speed, execution and debugging of development efforts

Through a series of video interviews, working sessions, follow up documentation and diagram validation, we have gathered the information needed to providing recommendations on next steps for remediation and enhancements or changes to existing workflows

Pain Points Encountered

- In order to access logs for troubleshooting, debugging and root cause analysis engineers must currently log directly into instances individually with no central repository being available.
- Deft discovered security and best practice concerns related to AWS root account access, security groups, IAM password policies and credential storage.
- Engineers must currently coordinate offline for use of the staging environment to demo feature branch and code fixes to the platform, at times there are contention for resources.
- Six of the remaining eight applications that are slated for containerization cannot be developed until a reliable produc- tion environment is in place that leverages containerization best practices and automation. Progress on this initiative is currently stalled (next line)
- Your Company does not currently have a DevOps resource to assist with the management of a containerized production environment for the two apps that have been containerized.
- Your Company needs to be able to deploy hotfixes to their production environment quickly via CI/CD workflows that will postpone time-consuming unit tests until after deployment has completed.
- During deployment, assets can be generated either from CI/CD or directly from the instances themselves – there is concern over configuration drift that could lead to delays in debugging issues.
- Hotfix deployments are needed on a faster timeline than CI/CD can provide (with respect to asset / artifact generation, and unit testing), at the cost of unit testing prior to production deployment. As a requirement this might be remediated with further automation / speed enhancements provided by a more robust CI/CD workflow.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Current Environment

Deft conducted a thorough assessment of Your Company's current environment and identified the following short-term recommendations:

Root Account Security – Root Accounts are not secured with Multi-Factor Authentication (MFA);

- Requested Action: Immediate Remediation.
  - » To remediate this situation, we recommend activating (MFA) on your AWS root account. This is an Deft and AWS best practice and will add another layer of protection to help keep your account secure.
  - » The documentation for execution of this process within AWS is available here: (https://docs.aws.amazon.com/IAM/ latest/UserGuide/id_credentials_mfa.html?icmpid=docs_iam_console)
- Please note, the activation of MFA should also be done for any new sub-accounts created for Development, Staging or Production environments once migrations begin.

IAM Password Policies – IAM password policies are currently not in place

- Requested Action: Immediate Remediation.
  - » To remediate this situation, we recommend implementing a password policy. This policy will require your IAM users to create strong passwords and to rotate their passwords on a set schedule.
  - » The documentation for execution of this process within AWS is available here: (https://docs.aws.amazon.com/IAM/ latest/UserGuide/id_credentials_passwords_account-policy.html?icmpid=docs_iam_console)
  - » Please note, a similar policy should be implemented requiring replacement of any personal keypairs used for develop- ment efforts. Service accounts may have a different policy, as needed or required by corporate security and compliance operations.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Single VPC Architecture – All environments are currently running under a single VPC (VPC ID: vpc-xxxyyy "XXXX").

- Requested Action – Immediate Remediation
- Deft and AWS best practices recommend the separation of Development, Staging and Production environments. Each environment should be broken into its own set of VPCs so that an error or misconfiguration in one environment does not impact the others.
  - » Each set of VPCs should be then be setup with individual AWS accounts under a master "Root" AWS Organization account.

Multiple Security Groups with Unrestricted Access – Multiple security groups allow unrestricted access on specific ports to any IP (0.0.0.0/0).

- Requested Action – Immediate Remediation
- Deft and AWS best practices recommend:
  - » Port # allows SSH access. However, this is currently open to the world. We recommend limiting access to specific IP addresses. Additionally, if remote access is needed, we recommend a VPN or bastion host to act as a perimeter wall on the public facing subnet(s) to provide access to private subnets.
  - » The current configuration is vulnerable to brute force attacks that could compromise the security groups listed below with a from/to port of #.
  - » Port # appears to be used for APPLICATION access. This Port should be restricted to only the private subnets requir- ing access. If there are external resources requiring access to this database, we recommend implementing a security group inbound rule that will lock down access to a limited range of IP addresses.
  - » Port X appears to be used for SERVICE. This Port should be restricted to only the private subnets requiring access. If there are external resources requiring access to this database, we recommend implementing a security group inbound rule that will lock down access to a limited range of IP addresses.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Recommendations

Applications

- Containerize all remaining applications.
- APPLICATION should be split from VPC and placed into its own container.
- AWS CloudWatch can be used to store and retrieve container and application logs used for debugging issues with environments, applications, etc.

Containers

- All applications should be hosted on a serverless platform - Amazon ECS Fargate.
- All container images should be using Amazon ECR as the registry.
- Each application should have its own registry for each deployment tier (dev,stage,prod).

Continuous Integration / Continuous Deployment (CI/CD)

- CI/CD APPLICATION will continue to be the tool of choice for building and testing code/containers.
- Modify FILE for CI/CD APPLICATION to test containers in parallel.
- Each container image should be promoted through all deployment tiers to ensure consistency and portability of containers.
- Create a method on AWS Lambda to validate containers health before switching traffic to it if using blue/green deployments.
- Further testing is needed before we can make a final recommendation between deployment orchestration and method.
- Current choices on the table are Blue/Green and Rolling style deployments – this will affect the choice between using CI/ CD APPLICATION + APPLICATION with APPLICATION, or CI/CD APPLICATION alone with Amazon ECR/ECS and Fargate services. We will update this document once a final recommendation is made.

Networking

- AWS CloudMap should be used for service discovery. This will allow microservices type of architectures to quickly commu- nicate with other healthy services internally.
- AWS App Mesh to control application level networking so that application code does not need to change to handle service discovery. This will also provide further logs on traffic between applications.
- A single application load balancer should be used to reduce the complexity of managing multiple load balancers as well as help reduce costs.
- Path base routing on the application load balancer should be used to target different ECS application services.
- Aid with remediation for any existing security issues (Root MFA, Security Groups, NACLs, PW Policies, etc)

Quality of Life Improvements

- Implement ECR lifecycle to remove old images.
- Implement RDS snapshot lifecycles to reduce costs of storing stale data.
- Remove unused AWS S3 data/assets or implement lifecycle policies to remove stale data. Design a method to allow developers to get their own sandbox environments for development.
- Will use CloudFormation templates with CI/CD APPLICATION to achieve this. Implement the ability to bypass testing for quicker deployment of hotfixes. Implement the ability for developers to access application server for data aggregation.

Diagram Links

- Existing Architecture Diagram
- Current Application Stack + CI/CD Pipeline
- Proposed CI/CD Pipeline
- Proposed ECS Architecture Diagram

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Additional Questions

For more information, visit https://www.deft.com/ or contact us at (312) 829-1111 and sales@deft.com

About Deft

At Deft, we are our clients' most Trusted Advisor.

We know that technology promises the world—streamlined infrastructure, instant scalability, seamless cloud migrations, and much more. We also know technology doesn't live up to its promise without the right partner. This is why we design, build, operate, secure, and scale unique technology solutions with a singular purpose—to deftly deliver on the promise of technology for you and your customers.

Learn more at www.deft.com or call us at (312) 829-1111.