Case Study

Ascribe EU Deployment

Client: Ascribe

Founded in 1999, Ascribe's leading verbatim analytics solutions and services enable the world's largest research firms, corporate researchers, and customer experience professionals to categorize and analyze verbatim comments quickly and easily. Ascribe's comprehensive and flexible SaaS-based technologies integrate machine learning, automated text analytics, and data visualization to deliver on business goals regardless of channel or language.

Customer challenge	CBTS results

• New EU environment build
• Needed to ensure security and encryption
• No simple method to deploy AWS infrastructure
• Infrastructure not built by AWS Well-Architected Framework principles
• Desire to add new AWS services
  • Web Application Firewall
  • AWS Transfer Family
	• Architecting new solutions
	• Terraform – Infrastructure as Code
	• Cloud Security Posture Management
	• Well-Architected Review

Customer challenges

As Ascribe's business continued to expand globally, they wanted to establish a new data center in the EU to augment the primary production environment running in US-East-1 (Northern Virginia).

Ascribe's goals were to build the new cloud environment with the highest standards of security and privacy where EU customers could store all data collected in the EU to comply with GDPR and comprehensively address compliance for public work in the EU. Following the establishment of an office in 2020 in Germany, AWS' EU-Central-1 Frankfurt was selected for the new cloud instance.

Ascribe was looking to work with the CBTS AWS certified team to design and deploy an updated version of the workload. A Web Application Firewall was required to improve their security posture. Ascribe also wanted to implement an AWS Transfer Family to simplify FTP needs, so files could be written directly to S3, rather than maintaining a dedicated FTP server.

The Ascribe team had limited AWS experience and was not comfortable designing and securely deploying the entire workload. By partnering with CBTS, Ascribe developed a plan for CBTS experts to lead the deployment with Terraform, allowing the company to expand rapidly and confidently.

Finally, Ascribe wanted to engage CBTS in an AWS Well-Architected Review to identify areas to improve automation and efficiency and continuously evolve their workload environment.

CBTS results

Solution #1 - Architecting new solutions

- Web application firewall
  - Added to Application Load Balancer that handles all Internet ingress for the workload
  - Utilized Fortinet OWASP rules subscription
- AWS Transfer Family
  - Replaced EC2 functioning as FTP server
- Encryption
  - Ensured all EBS volumes and S3 buckets are encrypted with AWS managed keys

Solution #2 – Terraform - Infrastructure as Code

- Stored codebase in GitHub for versioning
- Shared S3 back end
  - Enables any privileged user access to the state file so that changes can be made
- Allows the entire workload's infrastructure to be deployed quickly for any future needs
  - New regions
  - DR
- Changes to existing workload's configuration can be checked with the Terraform plan

Solution #3 – Cloud Security Posture Management

- DivvyCloud
- GDPR and NIST insight packs ran against new EU environment
- Results showed no significant issues
- Reviewed results and handed off management to Ascribe

Solution #4 – Well Architected Review (WAR)

- CBTS performed AWS WAR with the customer
- Major future remediation determined:
  - Update workload's code to access S3 directly, rather than using Storage Gateway
  - Migrate from MS SQL to PostgreSQL
    - Allows for the use of RDS managed instances
    - No need for licensing
  - Update internal documentation for troubleshooting
  - Automate software deployment

No matter where you are on your cloud journey, CBTS can help you map which workloads are ideal for AWS, help you build the strategy to get there, and do the heavy lifting for migration and ongoing management.

Driving transformational results takes leadership and vision. Work with a partner with the certifications and experience to help carry the burden of risk and become an extension of your IT department.