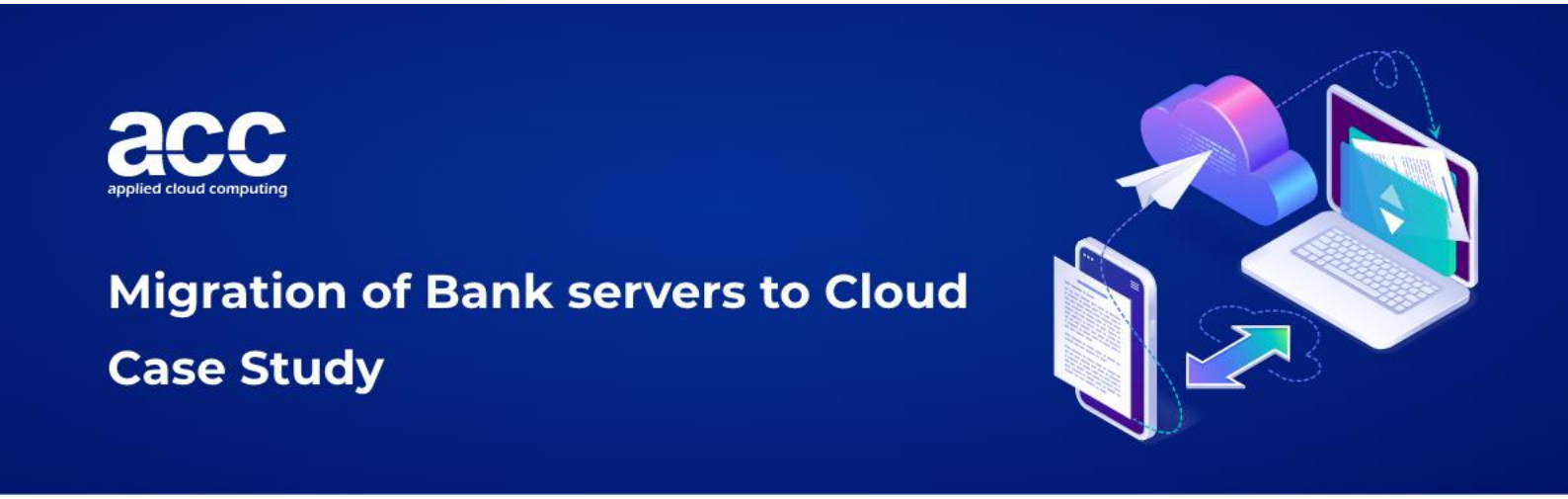


Migration of Bank servers to Cloud

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Amazon Web Services (AWS).

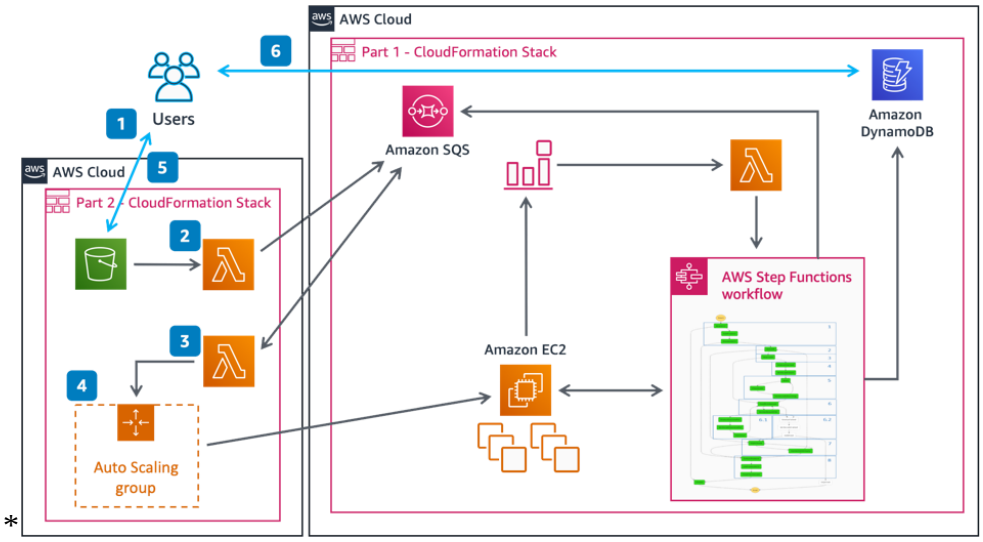
What is a Cloud Virtual Machines?

Amazon Elastic Compute Cloud (EC2) is a part of Amazon's cloud-computing platform, Amazon Web Services (AWS), that allows users to rent virtual computers on which to run their own computer applications. EC2 encourages scalable deployment of applications by providing a web service through which a user can boot an Amazon Machine Image (AMI) to configure a virtual machine, which Amazon calls an "instance", containing any software desired. A user can create, launch, and terminate server-instances as needed, paying by the second for active servers – hence the term "elastic". EC2 provides users with control over the geographical location of instances that allows for latency optimization and high levels of redundancy. In November 2010, Amazon switched its own retail website platform to EC2 and AWS.

How does it function?

Elastic Compute Cloud (EC2) is an important aspect of the Amazon Web Services ecosystem. In the AWS cloud, EC2 provides on-demand, scalable computing capability. Amazon EC2 instances eliminate the upfront hardware expenditure and eliminate the requirement to maintain rented hardware. It allows you to create and launch applications more quickly. You can launch as many virtual servers as you need with AWS' EC2. When website traffic increases or decreases, you can also scale up or down. Elastic Compute

Cloud's 'elastic' refers to the system's capacity to react to changing workloads and provision or de-provision resources in response to demand.



Benefits of Switching from On-Premise to the Cloud

1) **Cost Savings: -** A Cloud Hosted Desktop gives you scalable processing capacity while reducing IT requirements and physical data storage, resulting in considerable cost savings
2) **Security: -** Security is the major concern when it comes to banking . However, more people are realizing that these fears are unfounded. Cloud IT service companies actually deliver superior levels of security and data integrity than traditional IT service providers. Companies invest more in cloud technologies as well as a competent team of IT specialists and engineers, which smaller firms just cannot afford
3) **Connectivity and accessibility: -** Maintain user connectivity and accessibility no matter where they work with anytime, anywhere access. Users can access files from any device, at any time. This eliminates the possibility of files being saved on any computer and reduce the risk of piracy
4) **Reduced Data Loss Risk:-** Data loss is the major concern in the banking sector. By backing up data offsite, customers gain even greater security, reducing the risk of hackers, viruses, Ransomware, and other cybersecurity issues. More security, let me say it again.
5) **Faster Deployment:-** Cloud-based services can be deployed within just an hour or a few days rather than the weeks, months or years it can take to strategically plan, buy, build and implement an internal IT infrastructure with internal personnel
6) **Increased Collaboration:-** Cloud computing allows personnel in different places to effortlessly collaborate. Cloud computing improves employee collaboration and productivity by allowing for simultaneous syncing, working, and sharing of documents and records in real time.

7) **Improved Efficiency:-** Once you've moved to the cloud, you won't have to worry about power requirements, space constraints, costly computer gear, or software updates. You can keep your entire firm focused on sales and connections rather than IT

Getting Started with Cloud Computing:-

Cloud adoption does not have to be difficult. The advantages of cheaper per-unit expenses, reduced costs and complexity, and flexible scalability are simply too appealing to pass up. Security, pricing, and support concerns are reasonable, but not being in the cloud today may actually expose your firm to more breach vulnerabilities.

The notion that data must be stored on-site in order to be genuinely secure is as erroneous as the notion that money is safer under your mattress than in a bank. When compared to trying to run it on your own equipment, a reputable cloud IT service provider may invest significantly more in security.

What's in Store for the Company ?

With the goal of relocating in mind, it was only natural for the company to look into ways to upgrade its current IT infrastructure. Lower total cost of ownership, better infrastructure control, decreased operational complexity, and enhanced overall performance were among the other restructuring opportunities uncovered by the team. The corporation may also improve scalability and replace some resources that are nearing the end of their useful lives.
Despite the fact that the company could have continued to operate effectively with its on-premises data centre and traditional applications, the leadership team believed that the cloud would enable the company to achieve even more. The organisation decided to move to Amazon Web Services with the help of ACC, an AWS Premier Consulting Partner (AWS). ACC has helped hundreds of companies migrate to the AWS cloud.

ACC Solution

Our team worked closely with the client to gain a thorough understanding of their business goals, functional requirements, and systems.
ACC delivered a complete migration road map from on premise data to cloud well-balanced, technically adept team to the project, which seamlessly integrated into the start-strategic up's roadmap.
ACC leveraged a variety of AWS services and cloud technologies for the company's modernization effort.
The company's solution incorporated – at the most basic level.

1. **Robust security features**

2. **Firewall for cloud security**
3. **Landing zone**
   - **AWS Organization**
   - **Guard Rails**
4. **Multi-Tier Account structure Inspection**
   Control Tower
5. **VPC**
6. **WAF**

1) **Robust Security Features:-** The architects at ACC began by constructing a landing zone based on Amazon Web Services best practises. The landing zone would serve as a starting point for networking, security, management, and governance.

   Security measures such as identification and access management had to be included (IAM). AWS Key Management Service (AWS KMS) makes it simple to establish, manage, and control cryptographic keys across a number of AWS services and in your applications. As a result, KMS was utilised to encrypt data at rest and data in transit.

2) Firewall for cloud security :- Cloud Firewalls are software-based, cloud deployed network devices, built to stop or mitigate unwanted access to private networks. As a new technology, they are designed for modern business needs, and sit within online application environments

- A cloud firewall, like a traditional firewall, is a security solution that filters out potentially dangerous network traffic. Cloud firewalls, unlike traditional firewalls, are hosted in the cloud. This cloud-based firewall delivery approach is also known as firewall-as-a-service (FWaaS)
- Traditional firewalls build a virtual barrier around an organization's internal network, while cloud-based firewalls form a virtual barrier surrounding cloud platforms, infrastructure, and applications. On-premise infrastructure can also be protected by cloud firewalls

3) Landing Zone:- Customers can use AWS Landing Zone to swiftly set up a secure, multi-account AWS environment using AWS best practises. Setting up a multi-account environment can take a long time, include several accounts and services, and necessitate a thorough understanding of AWS services due to the enormous number of design options.

By automating the setup of an environment for executing safe and scalable workloads while establishing an initial security baseline through the creation of core accounts and resources, AWS Landing Zone can help save time. It also gives you a starting point for multi-account architecture, identity and access control, governance, data security, network design, and logging.

- **AWS Organizations:-** As your AWS resources develop and scale, AWS Organizations helps you centrally manage and administer your environment. You may create new AWS accounts and allocate resources programmatically, group accounts to manage your processes, apply policies to accounts or groups for governance, and simplify billing by using a single payment method for all of your accounts with AWS Organizations.

  AWS Organizations is also connected with other AWS services, allowing you to create central configurations, security methods, audit requirements, and

resource sharing across your organization's accounts. AWS Organizations is a free service provided to all AWS customers.

- **Guard Rails:-** A guardrail is a high-level regulation that ensures your overall AWS environment is well-governed. It's written in simple terms. A guardrail applies to a full organisational unit (OU), and it affects all AWS accounts within that OU. As a result, when users operate in any AWS account in your landing zone, the guardrails that govern their account's OU apply to them at all times.

4) **Multi-Tier Account structure Inspection:-** A multi-tier account AWS environment enables you to use the cloud to move faster and build differentiated products and services, all while ensuring you do so in secure, scalable and resilient manner.

Benefits of using Multi-Tier account:-

- Applies distinct security controls by environment
- Constrain access to sensitive data
- Promotes innovation and agility
- Limit scope of impact from adverse events
- Supports multiple IT operating models

Control Tower :- AWS Control Tower is a service that allows you to enforce and administer security, operational, and compliance governance rules at scale across all of your AWS Cloud organisations and accounts. AWS Control Tower allows end users on your remote teams to quickly supply new AWS accounts using Account Factory's customised account templates. Meanwhile your central cloud administrators can make sure that all accounts follow the company's defined compliance requirements. In a nutshell, AWS Control Tower makes it simple to set up and manage a secure, compliant, multi-account AWS environment, based on best practises learned from working with thousands of businesses.

AWS Control Tower has the following features:-

- Landing zone
- Guardrails
- Account Factory
- Dashboard

5) **VPC**

Amazon VPC:-

Amazon Virtual Private Cloud (VPC) is a commercial cloud computing service that provisions a logically isolated piece of Amazon Web Services (AWS) Cloud to users. Enterprise clients can use an IPsec-based virtual private network to connect to the Amazon Elastic Compute Cloud (EC2). [Unlike standard EC2 instances, where Amazon assigns internal and external IP addresses, customers can assign IP addresses from one or more subnets. VPC enables far more granular security management by allowing the user

to choose which AWS resources are public facing and which are not. It's an endorsement of the hybrid approach, but it's also aimed to offset the growing demand in private clouds, according to Amazon.

Comparison to private clouds:- Amazon Virtual Private Cloud seeks to deliver a service similar to private clouds. Private clouds, on the other hand, frequently employ technology such as OpenShift application hosting and various database systems. Cloud security specialists warned that there are compliance concerns when using public resources, such as a loss of control or service cancellation, that do not exist with in-house systems. If Amazon receives a National Security Letter requesting transaction records for a VPC, they may not be legally able to notify the customer of the system's security violation. Even if the actual VPC resources were in another nation, this would be true. AWS API is only partially compatible.

6) WAF

Amazon WAF: -

AWS WAF is a web application firewall that helps protect your online applications or APIs from typical web exploits and bots that can cause downtime, compromise security, or waste a lot of resources. By allowing you to establish security rules that govern bot traffic and stop typical attack types like SQL injection and cross-site scripting, AWS WAF offers you control over how traffic reaches your applications. You can also create custom rules to exclude specific traffic patterns. Controlled Rules for AWS WAF are a pre-configured collection of rules managed by AWS or AWS Marketplace Sellers to handle concerns such as the OWASP Top 10 security threats and automated bots that consume excessive resources, skew metrics, or create downtime.

Benefits of WAF:-

1) **Agile protection against web attacks:-** The propagation and changes of AWS WAF rules take less than a minute, allowing you to swiftly update security throughout your environment when problems develop. WAF has hundreds of rules that can analyse any portion of a web request with little impact on incoming traffic delay. AWS WAF defends web applications against threats by filtering traffic according to rules you provide. For example, you can filter IP addresses, HTTP headers, HTTP content, and URI strings from a web request. This allows you to prevent typical attacks like SQL injection and cross-site scripting.
2) **Save time with managed rules:-** You can rapidly get started and secure your web application or APIs against typical risks with Managed Rules for AWS WAF. You can choose from a variety of rule types, including those that target the Top 10 security concerns identified by the Open Web Application Security Project (OWASP), threats particular to Content Management Systems (CMS), and developing Common Vulnerabilities and Exposures (CVE). Managed rules are updated automatically as new concerns arise, allowing you to spend more time developing applications.

3) **Improved web traffic visibility: -** AWS WAF provides near-real-time visibility into your web traffic, which you may use to develop new Amazon CloudWatch rules or alerts. You have fine control over how the metrics are displayed, allowing you to monitor everything from individual rules to all inbound traffic. In addition, AWS WAF provides complete logging by capturing the full header data of each examined web request for use in security automation, analytics, or auditing.
4) **Ease of deployment & maintenance: -** AWS WAF makes it simple to set up and safeguard applications that are hosted on Amazon CloudFront as part of your CDN solution, the Application Load Balancer, Amazon API Gateway for REST APIs, or AWS AppSync for GraphQL APIs. There is no need to install additional software, configure DNS, handle SSL/TLS certificates, or set up a reverse proxy. You can centrally define and maintain your rules with AWS Firewall Manager integration, and reuse them across all the web apps you need to secure.

Applied Cloud Computing (ACC) is an advanced AWS consulting partner. ACC accelerates end-to-end cloud adoption with the best implementation services, software and processes available.

To learn more, go to : www.appliedcloudcomputing.com