

Sanjeev Agrawal Global Educational University, Bhopal



Lab File of Cloud Security

Course Code: CA21B503P

Prepared by:

Aditya Nair

Enrollment No. – 22BCA3CCM10005

**School of Computer
Application**

Session: Autumn 2023-24

Index

Sr. No.	Aim of Experiment	Scheduled date	Actual date	Remarks
1	Report on Cloud Compliance and Jurisdictional issues.			
2	Implementing Multifactor authentication system for login security.			
3	Security groups configurations to manage inbound/outbound traffic to the resources.			
4	Implementation of Security token, Security key and Access token			
5	Use of Identity and Access Management (IAM) to restrict the accesses to the resources.			
6	Case study on vulnerability assessments on cloud.			
7	Provision, manage, and deploy public and private SSL/TLS certificates.			
8	Investigate potential cloud security issues.			
9	Analyze application security with the help of Amazon inspector.			
10	Implement DDOS protection and Filter malicious web traffic using Amazon Web Services			
11	Case study on Data protection and compliance by cloud providers like Amazon, Microsoft and Google.			
12	Track user activity and API usage with AWS CloudTrail			

Experiment-1

Title: Report on Cloud Compliance and Jurisdictional issues.

The Challenges of Cloud Compliance

As you navigate the cloud, you'll encounter several compliance issues that can be overwhelming. Let's break them down:

1. **Data Sovereignty:** This concept refers to the idea that data is subject to the laws and regulations of the country where it's stored. Think about it – your data might be stored in multiple locations around the world, each with its own set of laws and regulations. This raises concerns about data protection, privacy, and security.
2. **Data Protection Regulations:** You'll need to comply with regulations like the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Each of these regulations has its own set of rules and guidelines.
3. **Industry-Specific Regulations:** If you're in a specific industry, like healthcare or finance, you'll need to comply with regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the Payment Card Industry Data Security Standard (PCI DSS) globally.
4. **Cloud Security Standards:** You'll also need to comply with cloud security standards like the Cloud Security Alliance (CSA) and the International Organization for Standardization (ISO) 27001. These standards provide guidelines for securing cloud infrastructure and data.

Jurisdictional Issues: A Web of Complexity

As you navigate the cloud, you'll also encounter jurisdictional issues that can be complex and confusing. Here are a few examples:

1. **Country-Specific Laws:** Cloud providers must comply with country-specific laws, like the USA PATRIOT Act in the United States or the Investigatory Powers Act in the United Kingdom.
2. **Cross-Border Data Transfers:** When you transfer data across borders, you'll need to comply with regulations that govern data protection, privacy, and security.
3. **Cloud Provider Liability:** Cloud providers may be liable for data breaches or other security incidents, depending on the jurisdiction and applicable laws.
4. **Dispute Resolution:** If you have a dispute with your cloud provider, you'll need to navigate different laws and jurisdictions, depending on the location of the parties involved.

The Opportunities and Challenges

While cloud compliance and jurisdictional issues can be complex and overwhelming, they also present opportunities for organizations to differentiate themselves, build trust with customers, and establish themselves as leaders in the cloud market.

However, non-compliance can result in significant fines, reputational damage, and loss of business. The cost of compliance can also be high, particularly for small and medium-sized organizations.

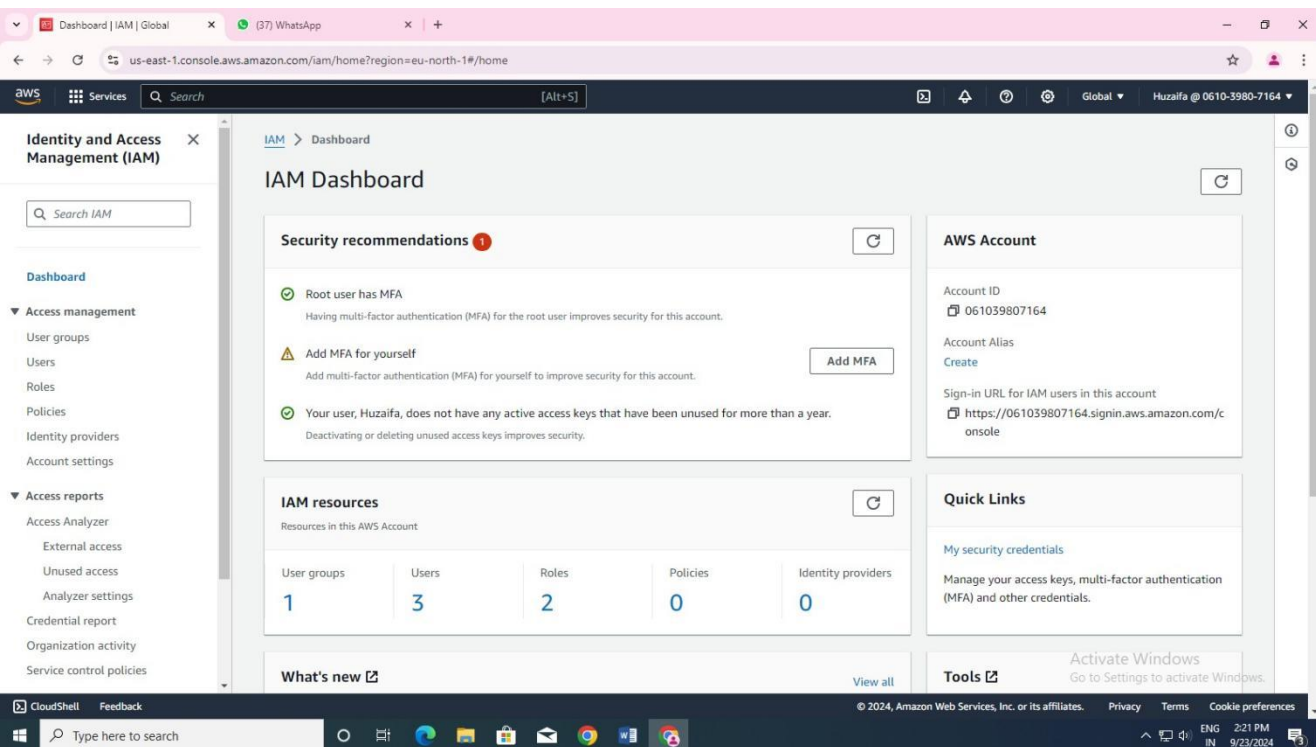
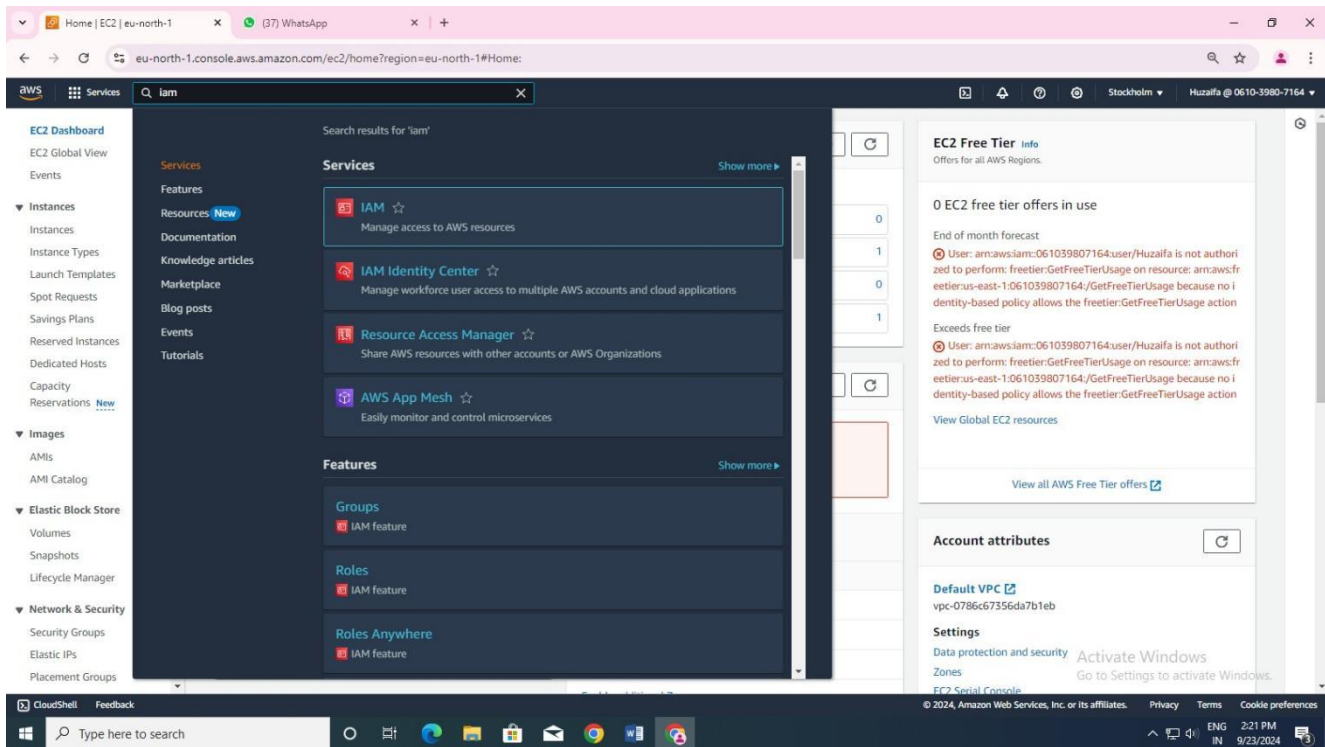
Best Practices for Navigating Cloud Compliance

So, how can you navigate the complex world of cloud compliance and jurisdictional issues? Here are a few best practices to keep in mind:

1. **Conduct a Risk Assessment:** Take the time to identify potential compliance and jurisdictional issues that may affect your organization.
2. **Develop a Compliance Strategy:** Develop a compliance strategy that takes into account multiple regulations, laws, and standards.
3. **Choose a Cloud Provider Wisely:** Choose a cloud provider that has experience with compliance and jurisdictional issues.
4. **Monitor and Review:** Continuously monitor and review your compliance and jurisdictional issues to ensure that you remain up-to-date and compliant.

By following these best practices and staying informed about the latest developments in cloud compliance and jurisdictional issues, you can build trust with your customers, establish yourself as a leader in the cloud market, and take advantage of the opportunities presented by the cloud.

Title: Implementing Multifactor authentication system for login security.



S

Dashboard | IAM | Global | Assign MFA device | IAM | Global | (37) WhatsApp

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/security_credentials/mfa

Services Search [Alt+S]


IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Set up device

Authenticator app
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.
[See a list of compatible applications](#)
- 2  Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)
- 3 Type two consecutive MFA codes below
Enter a code from your virtual app below

Wait 30 seconds, and enter a second code entry.

Cancel Previous **Add MFA**

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback

Type here to search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG 2:23 PM
IN 9/23/2024

Dashboard | IAM | Global | Assign MFA device | IAM | Global | (37) WhatsApp

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/security_credentials/mfa

Services Search [Alt+S]

IAM > Security credentials > Assign MFA device

Step 1
Select MFA device

Step 2
Set up device

Select MFA device

MFA device name

Device name
This name will be used within the identifying ARN for this device.

Maximum 64 characters. Use alphanumeric and '+', '-', '@', and '_' characters.

MFA device

Device options
In addition to username and password, you will use this device to authenticate into your account.

- ☐ **Passkey or security key**
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.
- ☒ **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.
- ☐ **Hardware TOTP token**
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Cancel **Next**

Activate Windows
Go to Settings to activate Windows.

CloudShell Feedback

Type here to search

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG 2:22 PM
IN 9/23/2024

