AWS Access Analyzer

AWS Access Analyzer is a security service that helps identify unintended access to your AWS resources. It analyzes resource policies to detect any potential security risks and provides insights into resource access patterns. Access Analyzer simplifies the process of ensuring that your resources are only accessible by authorized entities and helps you maintain a secure AWS environment.

What is AWS Access Analyzer Used For:

1. **Security Assessment:** Access Analyzer identifies unintended or overly permissive access to your AWS resources, helping you mitigate security risks and enforce least privilege access.
2. **Policy Validation:** It evaluates resource policies to ensure compliance with security best practices and regulatory requirements.
3. **Incident Investigation:** Access Analyzer provides insights into resource access patterns, facilitating incident investigation and security incident response.
4. **Access Monitoring:** It monitors changes to resource policies and alerts you to any modifications that could potentially compromise security.

Information Provided by AWS Access Analyzer:

1. **Vulnerable Resources:** Access Analyzer identifies AWS resources (e.g., S3 buckets, IAM roles) with potentially unintended or overly permissive access.
2. **Access Paths:** It provides information on the access paths and principals (e.g., IAM users, roles, or AWS accounts) that have access to the resources.
3. **Policy Violations:** Access Analyzer flags policy violations and provides recommendations for remediation to enforce least privilege access.
4. **Access Logs Analysis:** It analyzes access logs to detect suspicious or unauthorized access attempts to your AWS resources.

Services Monitored by AWS Access Analyzer:

AWS Access Analyzer primarily monitors resource policies associated with various AWS services, including but not limited to:

- Amazon S3 buckets
- AWS Identity and Access Management (IAM) roles and policies
- AWS Key Management Service (KMS) keys and policies
- AWS Lambda function policies
- Amazon Simple Queue Service (SQS) queues
- Amazon Simple Notification Service (SNS) topics
- AWS Key Management Service (KMS) keys

Differences between External and Unused access analyzer:

1. **External Access Analysis:**

   This aspect of Access Analyzer focuses on identifying resources that are accessible from outside of an AWS account, potentially due to overly permissive permissions or misconfigurations. It helps in identifying resources such as S3 buckets, IAM roles, KMS keys, and SQS queues that are exposed to the public internet or to other AWS accounts. By identifying such resources, users can take appropriate actions to restrict access to only authorized entities, thereby enhancing security and reducing the risk of unauthorized access or data breaches.

2. **Unused Access Analyzer:**

   This aspect of Access Analyzer highlights unused roles, access keys, and passwords for IAM users, while also offering insight into inactive services and actions. Notification workflows can be automated to assist development teams in removing unused access. Furthermore, it integrates with AWS Security Hub to aggregate findings, providing a comprehensive view to enhance overall AWS security.

How to Enable AWS Access Analyzer:

1. Log in to the AWS Management Console.
2. Open the AWS Access Analyzer service from the list of available AWS services.
3. Click on "Create analyzer" to create a new access analyzer for your AWS account.
4. Select the findings type.
5. Specify the name and description for the access analyzer, and configure any additional settings as needed.
6. Review the settings and confirm to create the access analyzer for your AWS account.

How to Use AWS Access Analyzer:

1. **View Analyzer Findings:**
   - Access Analyzer generates findings that highlight potential security risks and policy violations associated with your AWS resources.
2. **Review Access Insights:**
   - Analyze the access insights provided by Access Analyzer to understand the access paths and principals with access to your resources.
3. **Remediate Policy Violations:**
   - Follow the recommendations provided by Access Analyzer to remediate policy violations and enforce least privilege access.
4. **Monitor Changes:**
   - Monitor changes to resource policies and access patterns using Access Analyzer to ensure ongoing security and compliance.

Cost of AWS Access Analyzer:

AWS Access Analyzer pricing is based on a pay-as-you-go model, where you are charged for the number of resource analyses performed. There is no upfront cost or minimum fee, and you only pay for what you use. Pricing varies by region and depends on factors such as the number of resources analyzed and the frequency of analysis.

Docs: AWS Acess Analyzer pricing

AWS Access Analyzer is a valuable security service that helps identify and remediate unintended access to your AWS resources. By analyzing resource policies and access patterns, Access Analyzer provides insights into potential security risks and policy violations, enabling you to maintain a secure and compliant AWS environment. With its seamless integration with AWS services and easy-to-use interface, Access Analyzer empowers organizations to proactively manage and enhance their security posture on AWS.