😊 Cross Account Logging CloudTrail

AWS CloudTrail is a service provided by Amazon Web Services (AWS) that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. It records API calls made on your AWS account and delivers log files containing events that describe those API calls. These events include information such as the identity of the caller, the time of the call, the source IP address, the request parameters, and the response elements returned by the AWS service.

Here are some key aspects and use cases of AWS CloudTrail:

1. **Visibility:** CloudTrail provides visibility into user activity by recording API calls made on your AWS account. This helps you understand who did what and when across your AWS infrastructure.
2. **Security and Compliance:** CloudTrail aids in security analysis, resource change tracking, and compliance auditing by providing a detailed history of API calls. This enables you to monitor for security breaches, track changes to resources, and demonstrate compliance with regulatory requirements.
3. **Operational Troubleshooting:** CloudTrail logs can be used for operational troubleshooting and debugging. By examining the API calls made to AWS services, you can identify issues, diagnose errors, and analyze behavior patterns.
4. **Alerting and Monitoring:** CloudTrail integrates with AWS CloudWatch to deliver real-time monitoring and alerting based on API activity. You can set up CloudWatch alarms to notify you of specific API events or suspicious activity.
5. **Log File Integrity:** CloudTrail logs are encrypted and stored in Amazon S3, providing protection against tampering and ensuring the integrity of log files. You can also configure multi-region logging for redundancy and compliance purposes.
6. **Comprehensive Coverage:** CloudTrail captures API activity for most AWS services, including compute, storage, database, networking, security, and identity services. This provides comprehensive coverage of your AWS environment.

😄 Use cases of CloudTrail:

AWS CloudTrail can be applied across various scenarios and industries to address different use cases. Here are some common ones:

1. **Security Monitoring and Threat Detection:** CloudTrail logs can be used to monitor user activity and detect security threats in real-time. By analyzing API calls, organizations can identify unauthorized access attempts, suspicious behavior, and potential security breaches. For example, detecting unauthorized IAM role changes, unusual API calls from unexpected IP addresses, or API calls to sensitive resources can help prevent security incidents.
2. **Compliance and Audit Trail:** CloudTrail provides a detailed audit trail of all API activity, which is essential for compliance with industry regulations and internal policies. Organizations can use CloudTrail logs to demonstrate compliance with standards such as PCI DSS, HIPAA, GDPR, and SOC 2. Auditors can review the logs to verify that security controls are implemented effectively, access is granted appropriately, and data is handled securely.

3. **Operational Troubleshooting and Debugging:** CloudTrail logs are valuable for troubleshooting operational issues and diagnosing errors in AWS environments. When applications or services are not functioning as expected, administrators can analyze CloudTrail logs to understand the sequence of API calls, identify misconfigurations, and trace the root cause of problems. For example, diagnosing permission issues, resource provisioning failures, or network connectivity issues.
4. **Change Management and Resource Tracking:** CloudTrail helps organizations track changes to AWS resources over time, facilitating change management and resource governance. By monitoring API calls related to resource creation, modification, and deletion, administrators can maintain an accurate inventory of resources, track changes to configurations, and enforce compliance with change management processes. This is particularly useful in large-scale environments with multiple users and resources.
5. **Forensic Analysis and Incident Response:** In the event of a security incident or data breach, CloudTrail logs can be used for forensic analysis and incident response. Security teams can reconstruct the timeline of events leading up to the incident, identify the initial point of compromise, and assess the impact on affected resources. By analyzing CloudTrail logs alongside other security data sources, such as AWS Config and VPC Flow Logs, organizations can effectively mitigate and remediate security incidents.
6. **Cost Management and Optimization:** CloudTrail logs can also be leveraged for cost management and optimization purposes. By analyzing API calls related to resource provisioning and usage, organizations can identify opportunities to optimize resource utilization, eliminate unused resources, and reduce unnecessary costs. For example, identifying idle EC2 instances, oversized RDS databases, or unused S3 buckets can help optimize AWS spending and improve cost efficiency.

🤔 What are we doing in this Lab?

In this lab, you're setting up a cross-account configuration to securely collect and store AWS CloudTrail logs from one account (Account B) into an S3 bucket located in another account (Account A). Here's a brief summary:

1. **Create an S3 Bucket in Account A**: This bucket will store the CloudTrail logs.
2. **Set Up Bucket Policy**: A policy is added to the S3 bucket to allow the CloudTrail service to write logs into it.
3. **Create CloudTrail in Account B**: CloudTrail is configured to send logs to the S3 bucket in Account A.

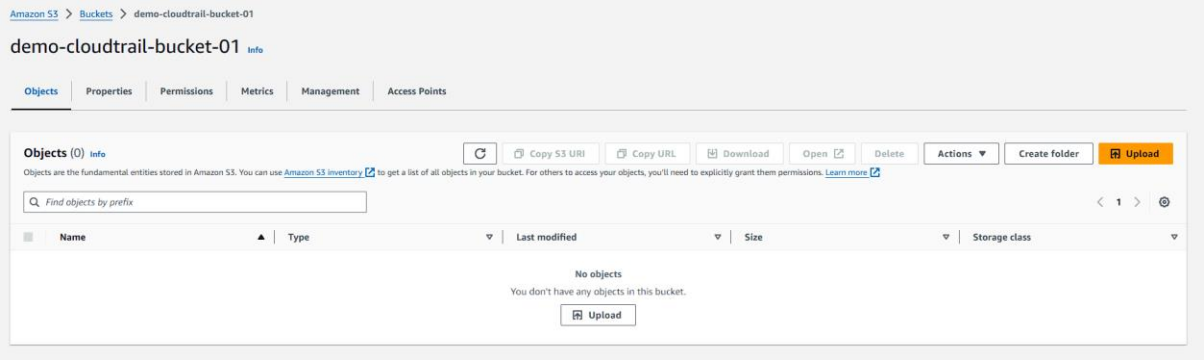
Challenges and Solution: A potential security risk is that any CloudTrail could write logs to the S3 bucket. To prevent unauthorized access, a conditional statement is added to the bucket policy using aws:SourceArn, specifying the exact CloudTrail that can write to the bucket.

End Goal: The end goal is to securely collect and store activity logs from one AWS account (where events are tracked) in a storage bucket in another AWS account. This setup ensures that only authorized logs can be added to the bucket, protecting the data and keeping it organized in one place for easy access and review.

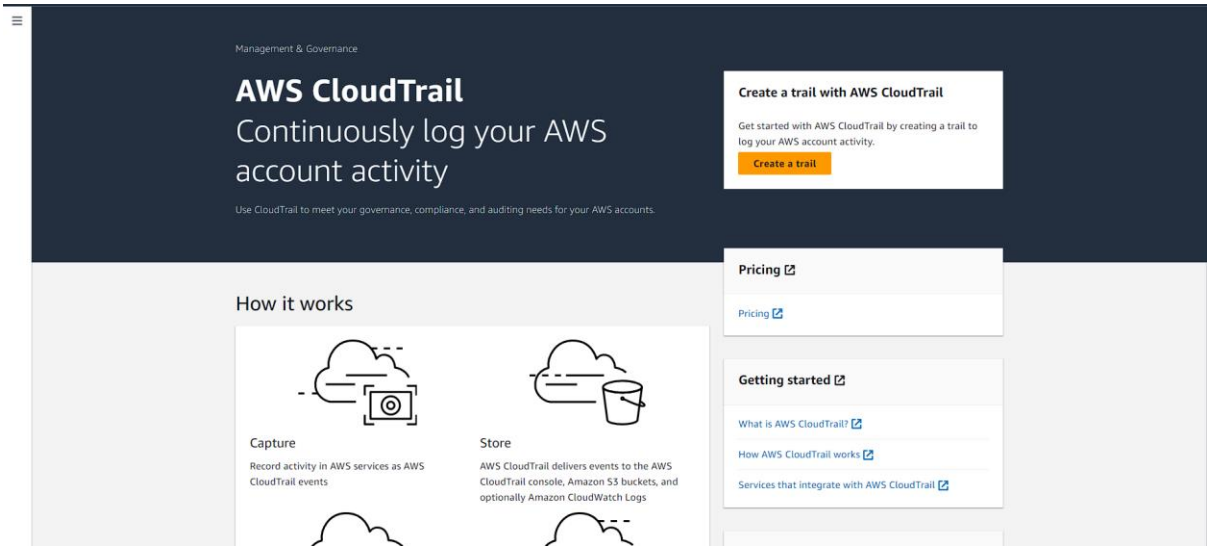
😄 To begin with the Lab:

1. For this lab you should have two accounts and you should be logged in both of them.
2. Here is what we are doing in the first account we will create our S3 bucket then we will create CloudTrail in account B. Then the CloudTrail will send data to the S3 bucket. So, here we setting up a cross-account setup.
3. Now in your account A create an S3 bucket. Once your bucket is created now you are going to add a bucket policy to your bucket.
4. This bucket policy allows Cloud Trail to add the logs to the bucket. Add the below code to your bucket policy and change the ARN with your bucket ARN.

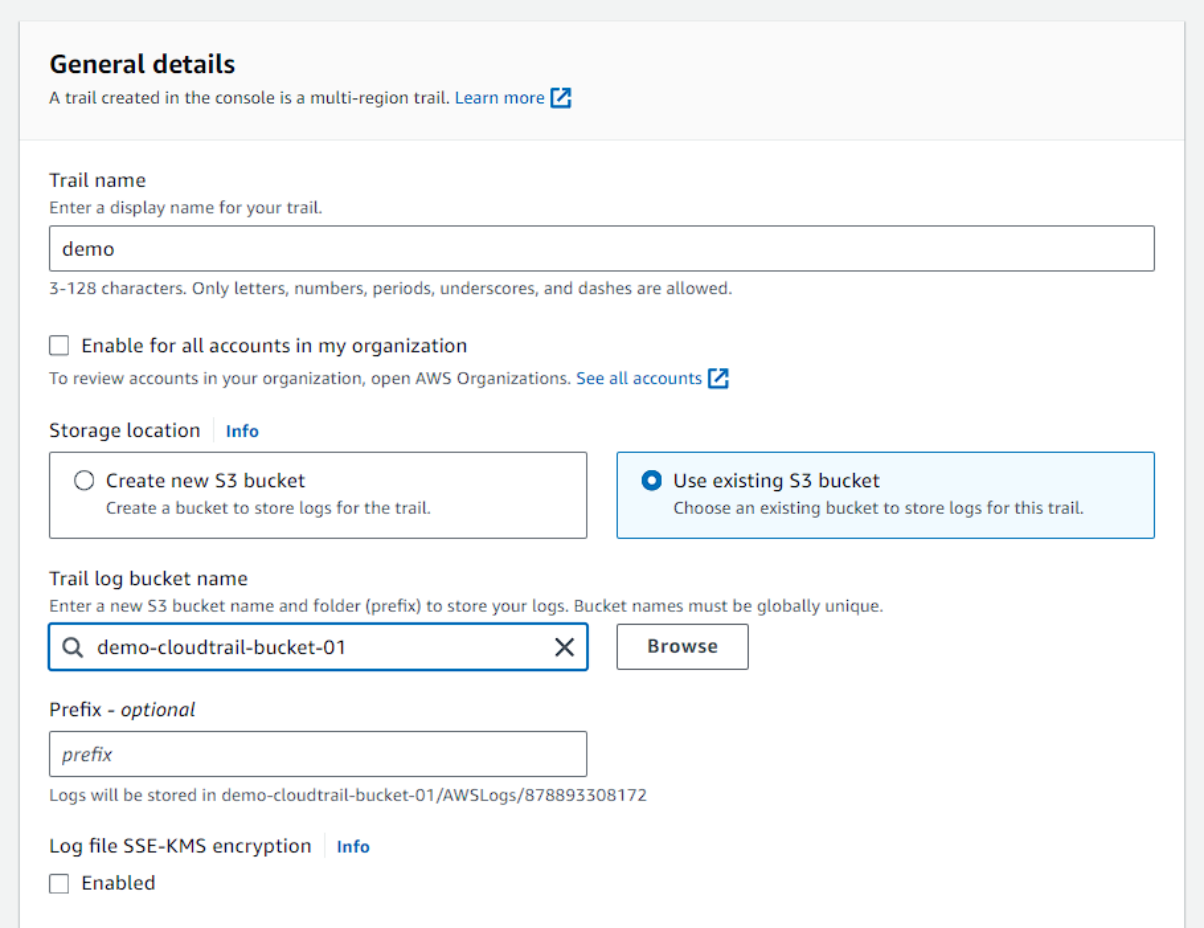
```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSCloudTrailAclCheck20131101",
   "Effect": "Allow",
   "Principal": {
    "Service": "cloudtrail.amazonaws.com"
   },
   "Action": "s3:GetBucketAcl",
   "Resource": "arn:aws:s3:::demo-cloudtrail-bucket-01"
  },
  {
   "Sid": "AWSCloudTrailWrite20131101",
   "Effect": "Allow",
   "Principal": {
    "Service": "cloudtrail.amazonaws.com"
   },
   "Action": "s3:PutObject",
   "Resource": "arn:aws:s3:::demo-cloudtrail-bucket-01/*",
   "Condition": {
    "StringEquals": {
     "s3:x-amz-acl": "bucket-owner-full-control"
    }
   }
  }
 ]
}
```



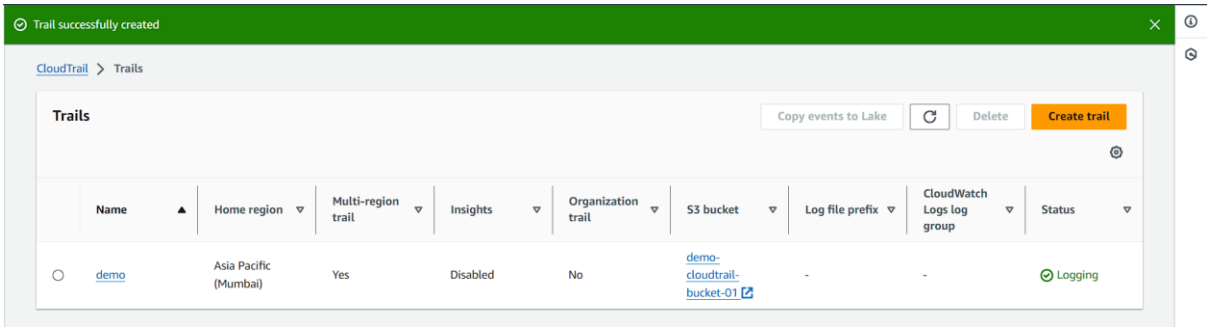
5. In account B you are navigating to CloudTrail. From the dashboard of cloud trail click on create.



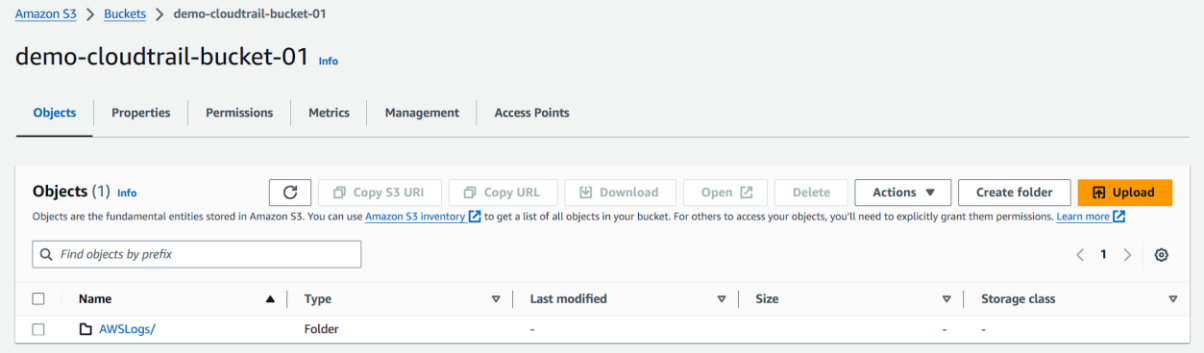
6. Now here you have to give it a name then in the storage location first choose use existing S3 bucket then specify the bucket name from account A.
7. After that disable KMS we don't need that. Then just create your trail and keep the things to default as they are.



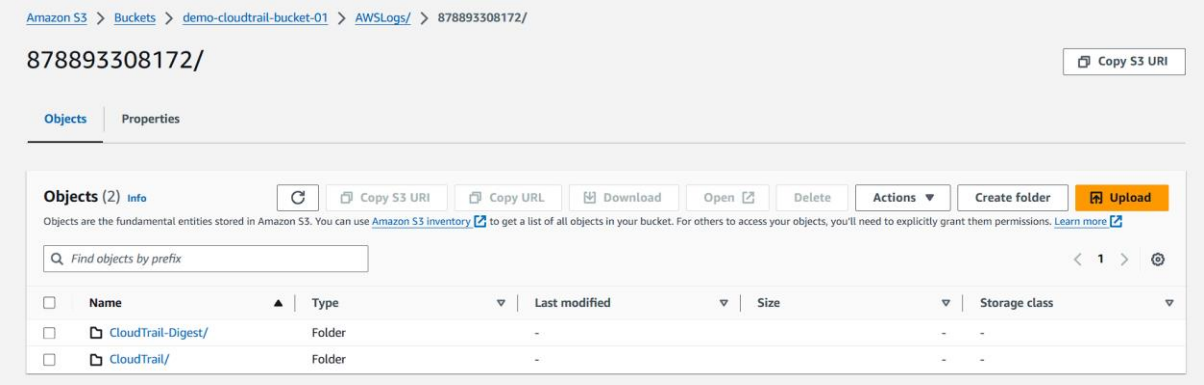
8. Below you can see that your trail is created.



9. Now if you will go to account A in your S3 bucket and refresh it.
10. You can see your logs that have been generated.



11. You can further go inside to see the logs that are created.



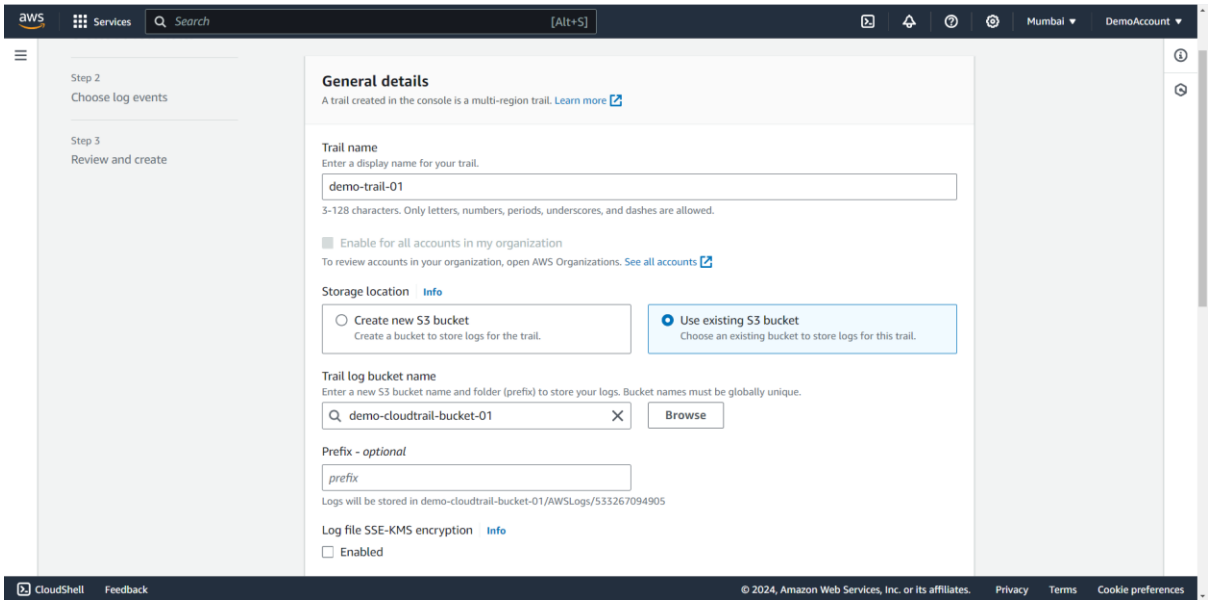
😄 Challenges with S3 Bucket policy:

1. Now, one of the challenges that you will see in this type of configuration is that any account can belong to you, it cannot belong to you. If someone has created a new cloud trail-based trail and has specified your S3 bucket, then the cloud trail of that account will be able to easily add some data to your S3 bucket. So, this is one of the primary challenges while you are adding such kind of a policy.
2. So, in order to overcome this, you can add a conditional statement within your bucket policy.
3. So as a security-based practice, you can add an aws:SourceARN condition key to your S3 bucket policy, and this will prevent unauthorized access to your S3 bucket.
4. We have added a condition and, in this condition, we have a source and here we are adding the exact area of your cloud trail. So, you have the region, you have the account number and you even have the trail name. So, in such kind of approach, no other trail will be able to add the contents to your S3 bucket.
5. In the last condition state you have to mention ARN of your cloud trail. Then just save your changes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::demo-cloudtrail-bucket-01"
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
```

```
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::demo-cloudtrail-bucket-01/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn":                    "arn:aws:cloudtrail:ap-south-
1:878893308172:trail/demo",
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

6. Now to verify this bucket policy I have a third account which account C.
7. Now here I went to cloud trail and I created a cloud trail. Give the trail name and then specified the bucket name where I want to save my logs.



8. Now when I tried to create the cloud trail immediately I got this error which states bucket access policy cannot be fetched.