

CloudTrail is a governance, compliance, risk management, and auditing service, and it records all account activity within an AWS account. So any actions taken by users, roles, or AWS services are recorded to CloudTrail. So activity is recorded as a CloudTrail event, and by default, all AWS accounts, or at least all new AWS accounts come with CloudTrail enabled by default. So let's move to the CloudTrail console. Now it used to be that you have to enable CloudTrail manually on any AWS account but thankfully, that was changed to it being enabled by default. So what happens with all new AWS accounts is that CloudTrail events are monitored and recorded by default for 90 days. So this is what a CloudTrail event is. If I go to view event, it's essentially a JSON document, which details a specific action on that account. Now, any APIs calls that are logged against an account will be recorded in CloudTrail, for example, when you create a user that's an API call, when you create an S3 bucket that's an API call, if you change the security group that's an API call. Any API calls inside an AWS account are logged to CloudTrail and **as default, you've got access to all of those events for the last 90 days and that's inside what's known as event history.** So I want you to remember that name event history is the default configuration of CloudTrail, where it stores 90 days of events that are relevant to that account. So the event history allows you to browse through these events. You can search on them. You can interact with them and get a good overall view of anything that's happened inside this AWS account. Now what I personally recommend for any AWS accounts that I have involvement with is that you also create a **trail**, so a trail inside CloudTrail is essentially a unit of configuration. It's how you define advanced options inside the product. So let's go ahead and do that. I'm going to click on create trail now trails of the basic unit of configuration for CloudTrail. They define exactly what is logged and where you want that data logged to. **So, by default, CloudTrail is just logging its information into the event history but if you want to store this data more than 90 days or want to do something specific with this data, then you need to create a trail and the trail is a per region configuration**. So I'm going to go ahead and create a trail and I'm going to call it LATrail for Linux Academy Trail. Now, when you create a trail, you've got a number of important options to pick from.

**Trails are per region objects. So you can either apply this trail to all regions or specific regions. Now, if you do pick all regions, it applies it not only to the current full set of regions, but it also means that if you have any future regions that routed to AWS which tends to happen all the time, that will automatically be updated also with that new region.** So by default, I always suggest that you do apply a trail to all regions and they log data based on what's happening in that region. So to capture all the data for all the regions, you need to apply the trail to all regions and then specify a single output location for that data and I'll talk about what I mean by output location in just a second.   
**Additionally, if you're creating the trail inside an AWS organization then not only can you have the trail apply to all regions, you can also have it apply to all accounts inside the organization, which gives you an organizational wide order trail**. Now, I'm not going to do that. While I do have an organization I want to a limit it at this point to just this account.   
**Now CloudTrail is capable of monitoring two different type of event categories. We've got management events on these events that you were traditionally associate with an API monitor. So these might be things like creating a user, deleting a user, creating a bucket, deleting a bucket, creating a Lambda function, adjusting a security group, anything that's account level interacting with the management plane of the account that will be logged by management events and you can select whether you want this trail to monitor all, read only, write only, or none**. By default, I would definitely recommend leaving this set to the default, which is all.

Now, **you're also able to log data events. Now currently supported services are S3 and Lambda, but you can have it so that any events that occur on object levels, for example, inside S3 buckets you can have those logged additionally by this trail, and I always recommend selecting all S3 buckets for the data events option**.

You got the same for Lambda, **so you can automatically have it logging any invoke operations. So knowing when individual functions are invoked and again you can specify individual functions or have it log all functions and all future functions in all regions and again**, I would always recommend selecting this to make sure you got the full overview of all activities in your account.

Now we get to **storage location**, and I mentioned this earlier in this lesson. By default, you've only got the event history to look at CloudTrail events. What we're doing as part of creating this trail is we're going to make it store all of the data that gets monitored, and we can have it stored in a particular S3 bucket. So I'm going to create an S3 bucket dedicated this. I'm going to call it CloudTrail and then I'm going to add some random digits. So 2, 3, 4, 2, 3, 4 I can go to advanced and if I wanted to do, I could specify some advanced configuration. Maybe I want to encrypt the log files that are stored in this bucket may be using KMS and a specific key. I could enable log file validation, which would allow me to identify if any of the logs have been tampered with and that's really important and I can also enable SNS notification every time these logs are delivered to this S3 bucket. **CloudTrail is not a real time product**. So what it's going to do is deliver these log files on a periodic basis into this S3 bucket. Now, this S3 bucket could be in your own AWS account, but it could also be in a separate AWS account. Maybe you have a separate account with separate identities that's used purely for security, governance, and auditing and if that's the case, then potentially you want to send an SNS notification maybe to a security system to inform it every time logs are delivered and this log validation basically adds checks on this to the data so you can determine if any of these log files have been updated or deleted or otherwise tampered with but at this point I've got everything configured. I've got the trail apply to all regions. I've got it st to monitor all event types and I've got that data going directly to my S3 buckets. I'm going to go ahead and create this CloudTrail.

Now, **in addition to being able to store this data in an S3 bucket, what I'm able to do is edit the trail settings. I can scroll down and that can configure integration with CloudWatch logs**. Remember, we talked about CloudWatch logs in the previous lesson. It's a log, delivery, ingestion, storage and monitoring system it's part of CloudWatch but what we can do is integrate CloudTrail with CloudWatch logs so as well as delivering these logged into S3, we can have them delivered into CloudWatch log. So let's configure that I'll hit configure. I'll need to specify a new or an existing log group. Remember, it's the log group that defines things like permissions or retention, and we can configure metric filters on there. So I want to make sure that I've got a meaningful log group name. So CloudTrail/CefaultLogGroup is the default, and I'm going to go ahead and go with that. It's I'll hit continue. Now **it will need permissions to be able to put this data into CloudWatch logs** and so what it's going to do is ask you for that permission. So it's going to create a new IAM role. So I'm just expanding that so you can see all the details. This IAM role is going to give it permissions to create a log stream and then poll put events. So I wanted to give it that permission. So I'm going to click on allow. So it's going to have created that role in the background. Once it's created it, I'll just scroll down and it's going to take a couple of seconds to validate that it's got all of the necessary permissions. That looks good. Everything is set. So now we've got this CloudTrail delivering these logs both into the S3 bucket and the into the CloudWatch Logs Group.

Now, this will take some time to store the initial set of logs. **It's not immediate and when you first set up a CloudTrail, it comes sometimes take up to an hour to store that first set of logs but once that is done, you should find that it's logging into S3 and CloudWatch logs at least every 15 minutes.** Sometimes it's every five minutes, but it is fairly varied. Once you got it configured, though, it will be doing it consistently, and you'll have access to all of the data inside cloudwatch logs. Now this is the architecture. This is how it looks. Maybe you have a user locking into the AWS console. Maybe that users stops an EC2 instance, using the stop instances API. Maybe we've got that user making a change to a security group using the authorized security group ingress API call but what will happen is in either of those cases, those API calls will be logged. They'll be ingested into CloudTrail and then, based on the configuration of the trail, it will stall that data potentially into S3 and maybe even CloudWatch logs. So that's the architecture, so let's just move across and see if this is actually added any log data yet. I'm just going to switch service and we go to CloudWatch going to go to logs. We have got the CloudTrail default log groups so I'm going to go inside this. We got a log stream for the region that we're in. So we're in North Virginia and that is U.S. East 1. So it's already started configuring at least. So let's open up this log stream and we don't yet have any log event. So if I look back on the previous document, remember, a log event contains timestamp and a raw message, and they're contained inside log streams. So our CloudTrail has gone ahead and created log group on the log stream. We clearly don't have any data yet. So this point, what I'm going to do is I'm going to pause the video, and I'm going to resume it once I have given CloudTrail some time to actually add some events, and it didn't actually take that long at all. It only took about two minutes and a couple of refreshers to show the first couple of items in this log stream. So just let's have a look at some of them and see exactly what they refer to.

So I'm noting that one of them shows auto scaling. So I'm just going to go ahead and click on this particular event, and it looks very much like it's a replication event for DynamoDB. So this actually looks to be for another lesson where I configured replication between two DynamoDB tables to actually refers to a role being assumed. That's to do with replication between two DynamoDB table so it doesn't really matter what the topic of it is, but it does highlight that already we're getting a log of all the API calls that are being action inside this account. So we got all of these auto scaling ones. Now, if I just scroll up to look at something different, we've got some CloudTrail related API calls so I'll expand some of these, and if we look closely, the event name actually tells us that it's a put object API call the event source is S3, so we know that we've got an object being put into history. The region is US East 1, which is North Virginia. It's being done by CloudTrail so we can tell that CloudTrail is putting an object in an S3 bucket. The S3 is ac-cloudtrail234234 so, looking at this, it does appear to be an API call for CloudTrail delivering logs into that S3 bucket for a test that if I move over to the S3 console, CloudTrail has clearly created this S3 buckets. I'll go inside it. AWS logs the account ID. We've got CloudTrail Digest and CloudTrail. I'll go inside the CloudTrail folder because this is a global trail we'll have a subfolder for all of the regions. Now I'm interested in U.S. East One so I'll select that folder and then we've got prefixes based on data and time. So 2019 it's August. It's the 15th of August and then CloudTrail has delivered compressed log files, which contained a complete overview of all of the API actions that are happening on this account in this region, and that's really all there is to CloudTrail. It's not the most glamorous product. It doesn't do anything that super exciting, but it is, in my opinion, one of the most important products to have enabled on every AWS account.

Now from an exam perspective, **is now enabled on every brand new AWS account but for older AWS accounts, you may have to create a trail and enable it explicitly**. I do recommend, though in any case, you do go beyond the default and you create a specific trail and configure it exactly how you want. So you've got it logging to a centralized S3 bucket as well as the S3 bucket you configure the integration with CloudWatch logs, so you've always got access to that data and by doing so, if you do have any situations where anything untoward happens in your account, you've always got the ability to audit and find out exactly who did it and when they did it and it's often too late if you do it after you have some sort of security exploit. So normally, this is the first thing that I do once I have created an account once have secured it, created my billing alarm. The next thing that I do is configure CloudTrail. Now for the exam just remember, **it is not realtime and it is delivered in batches. The initial batch can take some time, but then generally they're delivered in batches between every five minutes and 50 minutes.** Both the S3 and CloudWatch logs.