We will look at:

* **SNS**: notification service
* **cloud watch**: alert level monitoring or event level monitoring
* How to send emails using an **SES** service. and
* if time permits we would also go ahead and set up a **cloud trail** and we will have what it enabled in all our regions and we collect it into a single extreme bucket and any choice of our region.

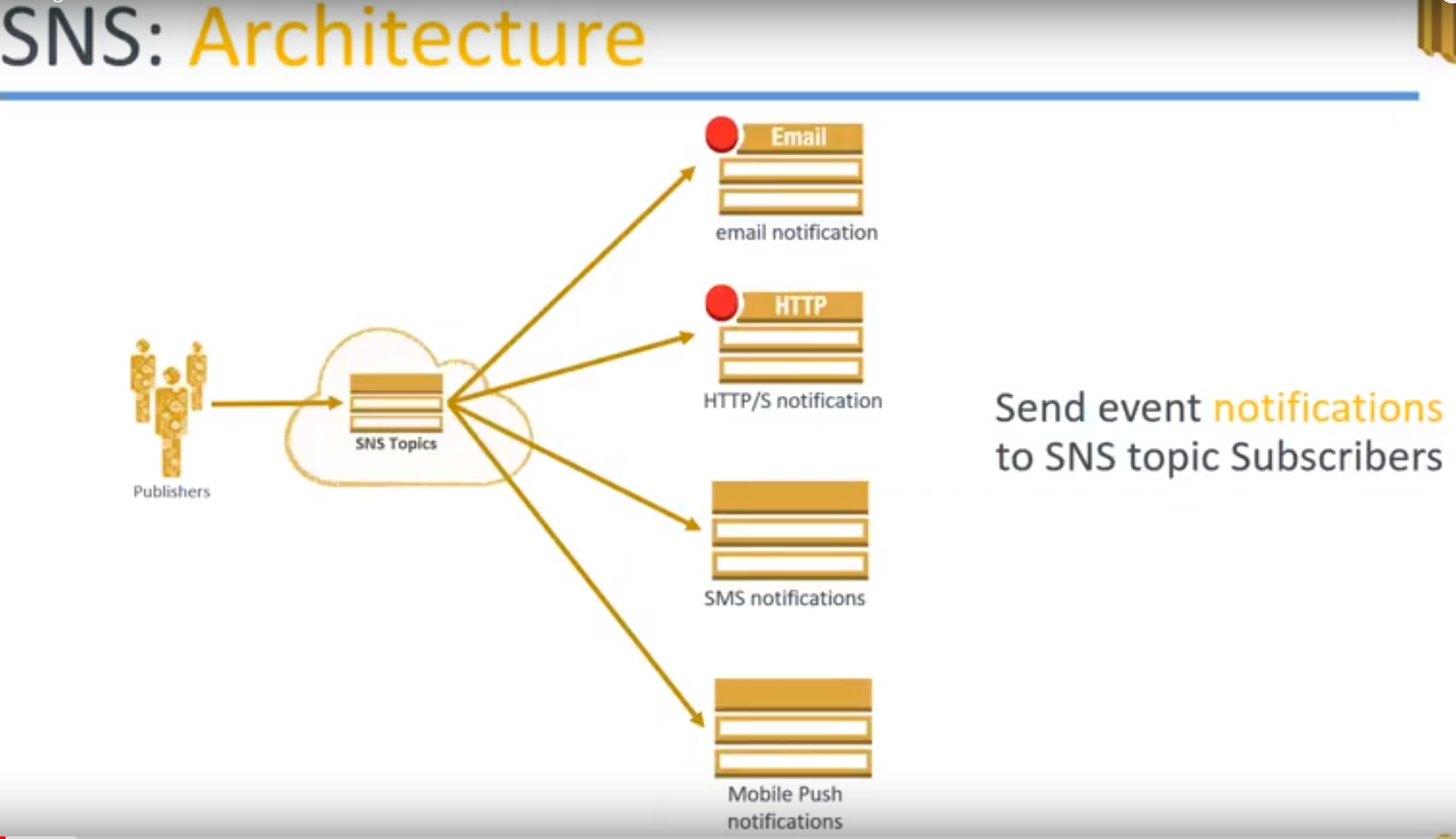
**SNS (simple notification service)**

* it is one of the easiest notification service that you can configure in the cloud whether you are going to publish messages to one application or you are going to reach messages to thousands of endpoints or mobile phones or any other endpoints that you can imagine like IOT devices
* It works on the pub/sub model that is publish and subscribe.

So, anybody wants to who wants to receive your message has to subscribe to your topic mandatorily otherwise they will not be able to receive those messages.

Ex you can think of it like email groups that we might subscribe to or any website offers or **e-commerce portals will give you subscribe to my offers then you will get the coupons on your email** this is how the functionality is built at the back end.

**SNS architecture.**



1. You have **publisher**, who is creating the message that needs to be delivered to a lot of people. Let us call them as publishers now.

They are going to publish their message to the **SNS topic.**

**2) SNS Topics:**

* Ex of topic: coupons which will be giving new offers.
* another topic might be for offers on existing products…. when this is all products level
* for a travel portal they will be offering discounts on holiday packages

You can have n number of topics in your SNS groups.

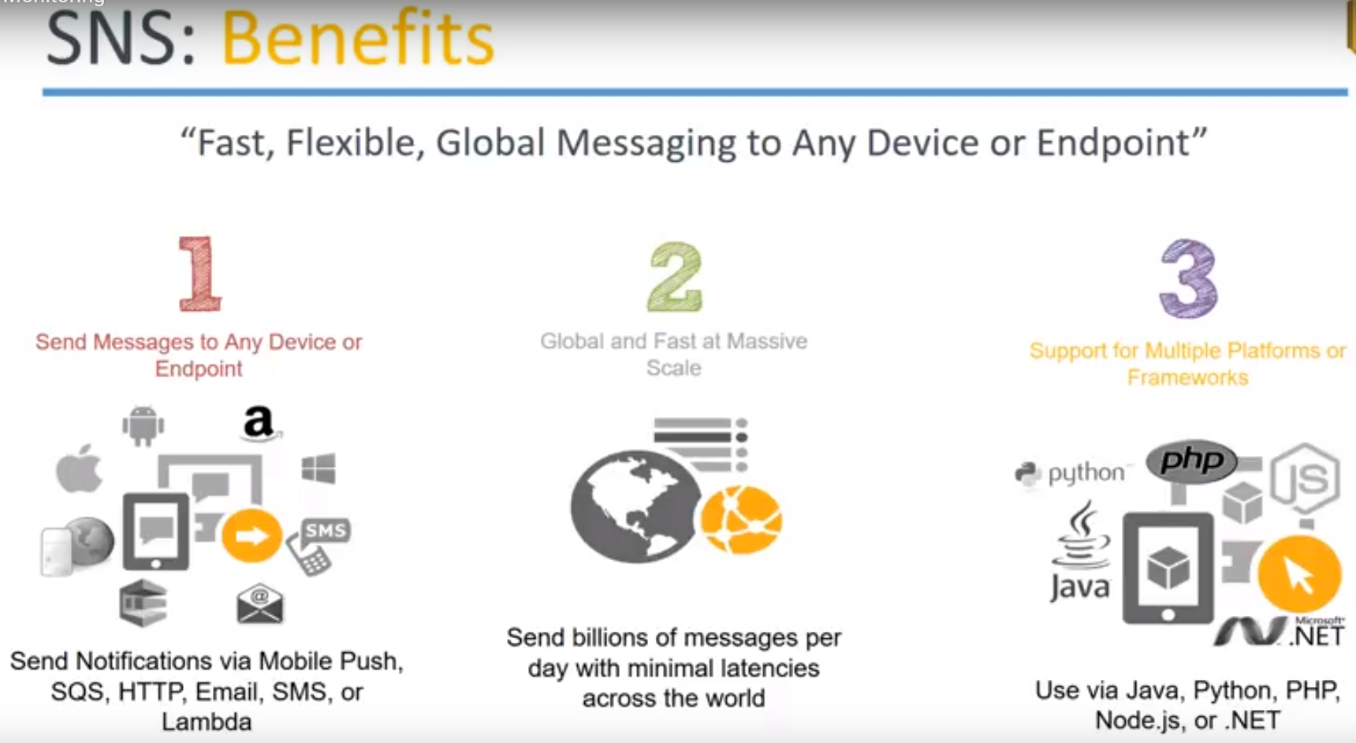
**3.) endpoints**

Then come to the endpoints. you have multiple endpoints or multiple ways of sending messages to your end points...

**Ex:**

* email notification. you can send all your subscribers on email.
* you can send an HTTP or HTTPS notification. This can be useful for your applications to consume the message when you're sending it through HTTP.
* Sending an SMS or OTP kind of notifications.
* Mobile push notifications, which you get on your Android or iPhone mobile.

So these are the two different types of ways you can send your message to your endpoints...

**SNS benefits** 

1. You can send message to any device or end point

Like: mobile push notification, SQS, Lambda, HTTP, SMS email.

**Example:**

* A new processing image has been done by replicate cluster and then you want to notify the data scientist so once the clusters finished processing ..,then you will configure an email service.
* if you want a batch load across processing is completed then you want to do the second level of processing then you will trigger the lambda then the lambda will pick up the process two files and go ahead and do it so.

what type of notification that you choose is absolutely depend upon your application and you have to configure the based on that.

2.) This is a service that scales automatically whether you are sending too few people or spending to a lot of endpoints. This service is global scale and you can send to anybody.

**For example:** I want to send a few SMS to people in the United States.

All I have to do is subscribe that mobile numbers into my SNS topic and I can push an SMS or push notification to their mobile phones are sitting in any other part of the world.

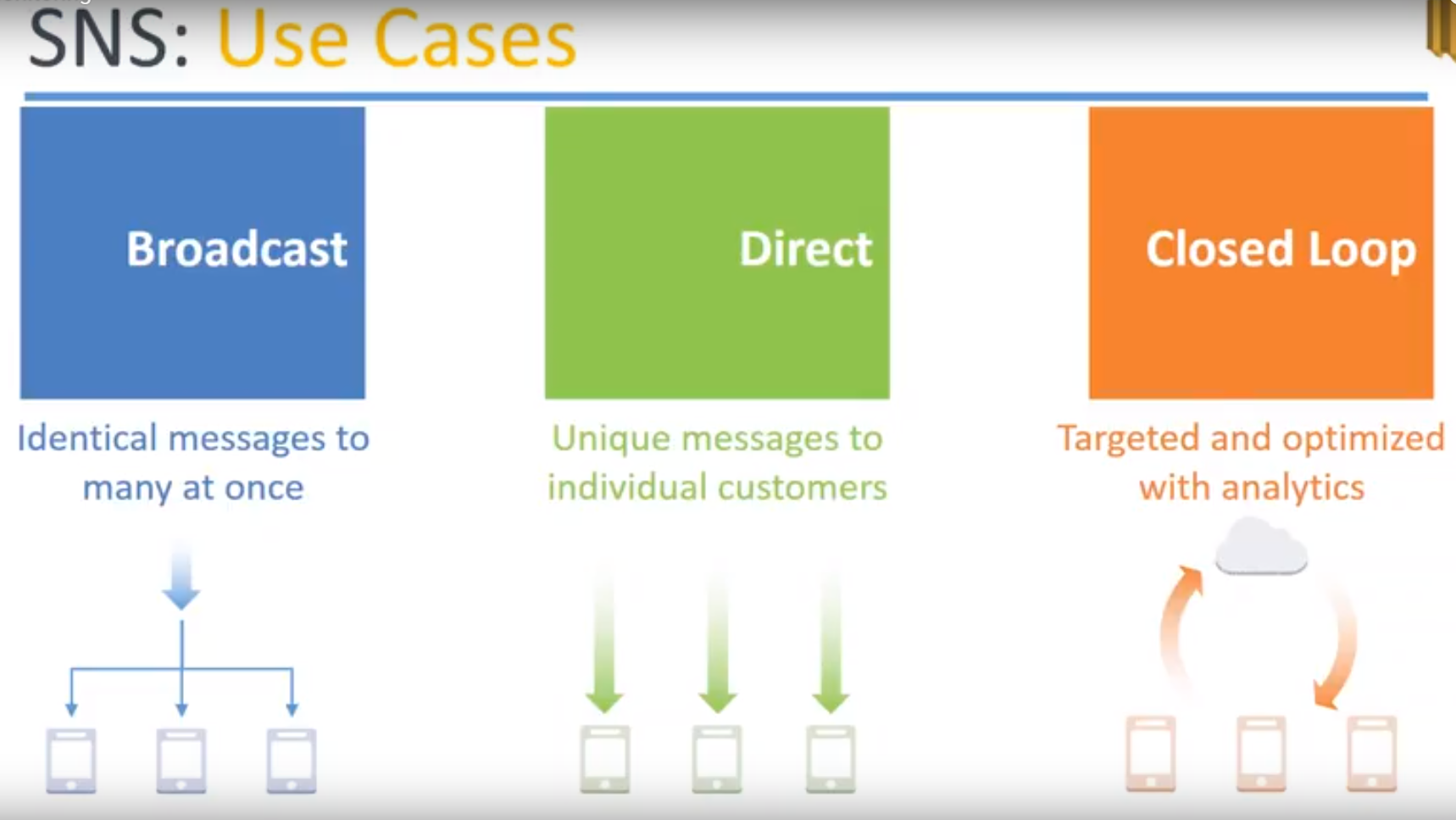
3.) multiple platforms are given to you for writing your SMS messages.

You can write it in a Programmatic way or you can use a dashboard and hand write or hand code you or message also.

When you are choosing a programmatic way through multiple languages Java ,Python ,dotnet, node.js all of them are supported.

You can go ahead and use any of those frameworks to send you push notifications

**SNS Use cases:**



1. One common use case is **broadcast messages**: like a common holiday packages sent to a lot of people that is identical messages to many people at the same time.
2. then there is a **customized** (Direct) **messages** If you have used uber or some kind of a ride-sharing service they know who you are and they know your usage patterns then there will be very customized to offer or a coupon for that sent only to you if you even try to put in the coupon code in somebody else more app or their account it won't work.

So you can send those kind of directed messages to only a very few people so those would cases also you can do with SNS.

1. **Closed loop**:

A certain group of people from a larger population will be taken for a targeted analytics that is in this case there will be a **premium group in the shopping categories.**

**Ex:** Let’s say Amazon Prime customers they will get a separate notification whereas the non prime customers won't get that notification.

**demo**

* how to create your own SNS topic.
* subscribe it and
* send email notifications

**CloudWatch** This is monitoring service provided by Amazon and

It can do monitoring based on metrics CPU networks or state monitoring or event monitoring that is whenever the state of a server changes from stop to running terminated, then you can get an alarm.

This is called as metric based monitoring or alert monitoring and event level monitoring also.

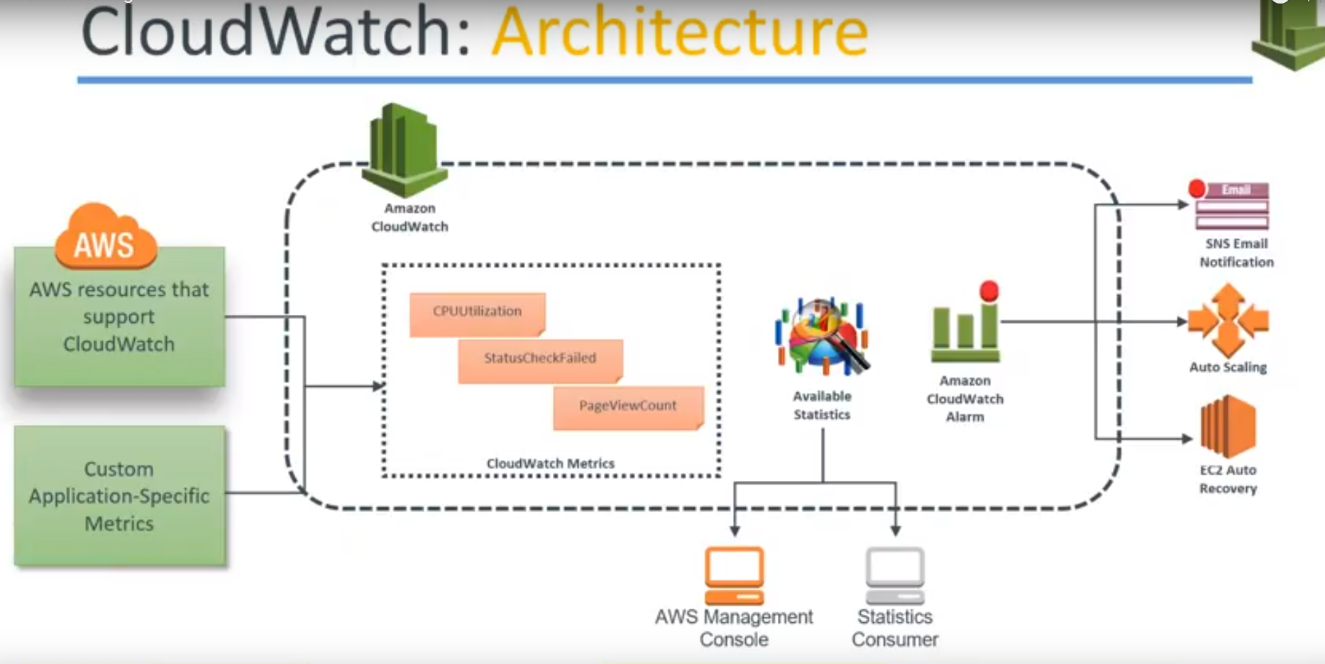


Cloud watch is a monitoring service and it can monitor both your resources as well as applications for you.

* When you want to monitor your applications then you go ahead and add your own custom metrics on top of it and feed it to CloudWatch. And
* You can collect all this log files store it and process it into your log management system.

**Remember** almost all the logs that you generate in Amazon can quite easily be sent to an s3 bucket and from an s3 bucket you can configure any other third party or Amazon's own logging mechanism that is graphing mechanism and visualize those charts.

**CloudWatch Architecture**



1.) let us say there is an Amazon account and there is a cloud watch configured already.

2.) There is a group of resources or group of metrics that are supported by Amazon, like CPU and networks latency, utilization what is many CPU credit balanced, whether my Hardware Health checks fine or my software, instance status checks, system status checks.

**If you notice carefully there will be a metric that will be missing there Amazon doesn't give you the memory metric in the monitoring aspect** **so you need to install some tools or scripts to measure the memory of your server or your application itself** so that possibility is there but by default Amazon does not give you the functionality.

3.) Metrics: Let us say in this case,

1. amazon resources are giving you CPU utilization and status check failed.. and
2. you want to measure the metric or some custom application thing then you have to go ahead and write your own custom application metrics and feed it into Amazon.

Example: there's a page view count how many pages are within my application.

4.) Available Statistics:

All these metrics are taken... So from the logs you get the metrics now.. From this matrix you feed it into the dashboard and the dashboard you can see it from your AWS console or you can have your customized statistics or logging or the visualization platform.

5.)And from here you can trigger alerts now see whether the threshold has been met when a CPU is 80 percentage Or my page view count is going by 1 million pages by every day.,whether it is increasing or decreasing based on that I will trigger a Alarm.

6.)when I configure in Alarm, I will push it to 3 different mechanisms :

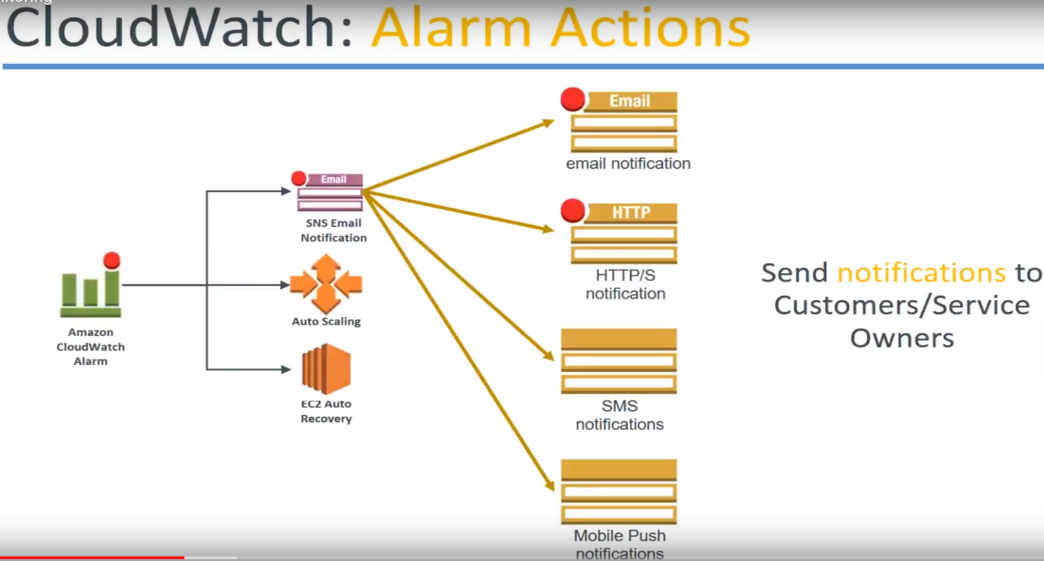
1. I can send an email through SNS or
2. I can trigger an auto scaling so that that server can come up or come offline or
3. if the is an individual server configured for auto recovery then go I will go ahead and reboot the server

So all these actions are possible…

**flow is something like this:**

1. collect the logs..
2. from the logs I will identify the necessary metrics and
3. if the metrics are meeting or not meeting certain thresholds ,I would create an alert and
4. based on that alert I would take some actions.

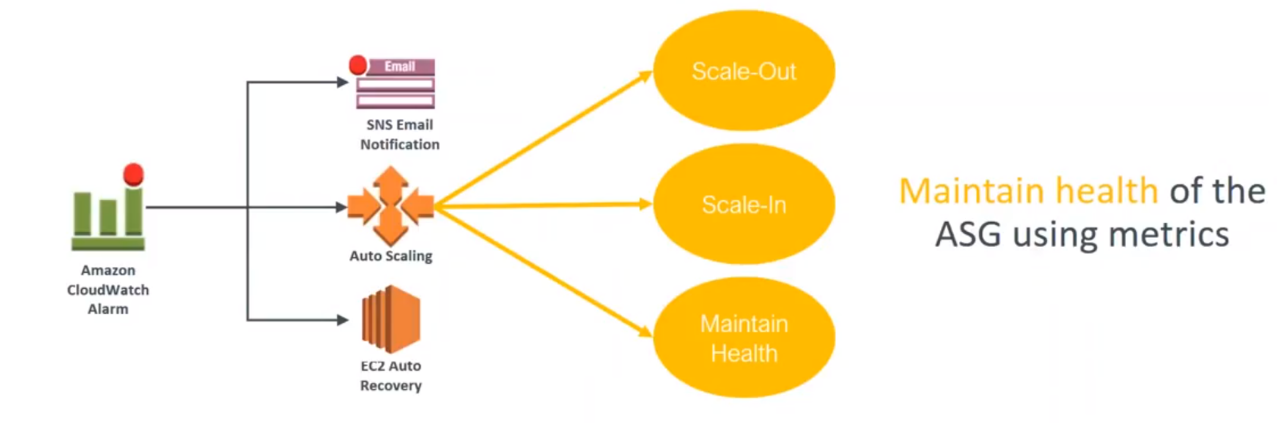
**CloudWatch alarm actions**

****

1. Whenever we are talking about **SNS** you have all this notification mechanisms available for you ..

Email, HTTP, SMS push .

1. **auto scaling**

****

You can take any of these three actions… You can scale out adding more servers scale and remove some of them or maintain the health everything is fine or if there is an unhealthy instance just replace that unhealthy instance of scaling in scale out you just maintain it but at the replace that instance finally auto recovery the option is a default option provided by Amazon you just go ahead and choose whether you want to reboot the server when there is a server failure or whether you want to stop that instance or terminate that instance whenever a server failure happens so these three alarm actions are possible for you so that is what a cloud watch is when you go ahead and do it in the dashboard it makes more familiar to put all these concepts into action so next one that I would like to introduce now is it is auditing mechanism that is provided to you by Amazon when you have anything happening in your account that you want to have a compliant or governance necessity or an operational auditing necessity or the risk auditing clout really can help you satisfy all these three or four types of requirements err so what typically happens is any activity that happens in your account whether you are accessing your account through a mobile or a GUI or CLI or programmatic means you will be interacting through API calls to your account all these API calls whether it is a read access or modification access it when they say modification creation of an ec2 instance or the modification can also be modifying the instance type of the dc2 so any of these changes all of these changes will be recorded in your throat trail as API calls as events and all these events will be stored in your s3 bucket and plow trail by default works from Virginia region only from Virginia you can configure whether all the other regions can be monitored or not but you can go ahead and choose only to monitor a particular region but the logs will come and sit in your Virginia but this will just go to cloud tree it will always say that it will be stored in Virginia so now we have identified what he wants to capture then we are capturing it in a certain region so once you are capturing it in a certain region it is in an s3 bucket then everything else makes simple because it's a log file now from all the events so from your log file then you can configure it is using cloud trail or cloud watch to generate events or you can use a third party logging mechanism to find out what events of your interest they say for example if you want to get notified whenever there is a modification of a security group or if you want to get notified whenever the administrative password for an account is changed so you can configure all this business rules by saying if my account is going to be accessed every day from morning 9:00 a.m. to 10:00 p.m. and suddenly there is an access out of these hours I want to be notified yes that is also possible because cloud trail logs everything log in log out modifications all those things so you can pick up those events trigger a notification and you can corrective actions so typically a cloud trail will lock all these items who made that event that who created that API call and when the API call was made and what was inside that API call weather modification or creation or deletion of an event and what resources were impacted by that API call and finally where is the IP address and timestamp and also the region also based on the IP address they'll have a region as well weather and it will also see whether from a tea while you are coming in whether you are choosing the API from episode or any region also so all this information will be there in your cloud rain logs so the flow is something like this on the left hand side you have people accessing your account through the GUI or SDK or CLI all these three different mechanisms are possible then they are accessing the cloud trail monitoring services and this each of those services will be feeding in those events to your cloud rain and cloud rain will be storing it in an s3 bucket as well as it will be triggering events in your throat watch if you configure it or if you want to go ahead and do some real-time monitoring and troubleshooting all those things that is also possible let us take one use case here how a monitoring alert is triggered up let us say some person has gone ahead and created some accounts or deleted some accounts so automatically you are going to configure some notifications showing that whenever an account is deleted saying that event immediately or trigger an alarm in your watch and cloud watch can go ahead and create an action now it can send an email or it can create a lambda function to revert it or anything is possible so in short that is outlaw trail works people trigger events trout trail monitors those events and if you are watching those events then cloud watch will trigger an alarm for you in short the cloud really helps you to achieve a lot of compliance activities some of them unlisted here for example security analysis and tracking the changes made and if you want to provide your auditors what is the compliance log of what question modified when then have those kind of logs and you can also prove that you will not the wrong wage and say GDP our or some kind of data production law is there then you can show and say that all my resources are in the newest region or Europe region only and I am not using any other region and in case there is a accidental deletion or modification of some resource you can go ahead quickly check it for watch and troubleshoot an operational issue also using the events apart from this there is analytics also you can use those logs to find out what is being modified more which of the sources getting changed quite often so we create a bigger resource or should be queue more granular controllers so that those modifications doesn't happen so you can do a lot of different types of analytics then you can also redistribute the trail sort so one of the common trail configuration is shown on your left hand side you can now you have the master account on the middle and if you can notice the cloud trial logs from the account B and C are being fed into the master account what this technically does is if your account B and C gets compromised for some reason the logs or the event of those logs will not be compromised because you will still have those lockwise and still you will be able to trace back the steps and recover your events go ahead and configure cloud trail in all the regions because you will not know where your next compromising attack will come from you might be using the resources in Virginia but some attacker might try to get into your Oregon region or maybe Ireland region and you will not be able to notice that until it is too late so go ahead and configure that and for all the logs that is stored in s3 bucket go ahead and enable versioning so that if somebody is going to tell it some versions you will still have the older files and you should be able to get some notification out of those versioning as well and encrypt your log files it's all a checkbox that is provided when you're configuring cloud trail so if you want to be really secure go ahead and enable log validation through versioning and then you can go ahead and enable the encryption as well so if somebody copies a lot of files they will still not be able to understand them without your keys and centralize your logs from all accounts as I show in the previous screen we have one master account or an administrative account where all the logs are coming in so it is easier to administer and to compliance activities from centralized accounts and it is also possible to integrate code watch so if you want to do it go ahead and do it I always go ahead and create some custom events for identifying whenever there is a resource modification in your accounts so that is what the cloud watch pro trail offers to you in short so the next group the simplest to service is simple email service this is so quite interesting in my opinion if you are a email promotion campaign manager then you want to send the millions of emails from your mailbox it is not possible whether you are trying to use a gmail personal account or if you are using any other question unless the email accounts were because once you reach a certain threshold you will be triggering some filters and automatically your account will be temporarily suspended or permanently banned so you for sending mass promotional emails you cannot use your personalized account you need to purchase a professional paid account for those services and how Mazon services is called as a simple email service and Amazonas tied up with a lot of ISPs and they comply with the is P standards because if one ApS is consistently sending millions of messages quite often ISPs banned those IP addresses so that they don't receive those more messages and that SMTP servers are not overloaded but in this case Amazon has tied up with ISPs so what happens is you any message coming from a CA service there is a guarantee of that message reaching the inbox of your subscriber and not the spam box or the jump box so these are the advantages of getting using CS and once again it scales automatically whether you send the messages to one person or ten percents or 1 billion people the messages are delivered and the services is also scaled and you get a failure notification for each of those messages also you can configure what is successful what is unsuccessful and you can read trigger the unsuccessful messages also so all of this management is built into its very simplified console and you can just go ahead and launch your message anytime so one caveat is is just not that you have a target email addresses that you can start firing that won't work each of those target email addresses have to subscribe to you that is they have to pre-approve so that they are ok to receive messages from SCS in other words it's like a subscription service only and once they have your email addresses if they approve then you can go ahead and send messages to all those email addresses so that is what caseous offers what we are going to do now is we are going to see a demo of all of the services that we just now discovered we starting with SES SNS then we'll go to cloud watch and you set up a cloud trail at the end of it here we are at the Amazon SES homepage and I have chosen the Virginia region because it is not available in all the regions it's available as of now to my knowledge only in three regions as it showed just now so if you have a particular domain name saying my website calm and you want to send bulk emails from that domain name then you have to verify that you own the domain name by adding the domain name here it will send an email to the administrator of that domain name and it'll send some verification code and then you have to go ahead and do that then your domain key identification settings will be done because these are all the things that an Internet service providers Amazon does so that people don't use the service for spamming purposes so I don't have a domain name but I can still send email addresses because I have approved of one particular email address of mine from which we can send email addresses so you can see there is one email address already I am going to verify another email address that I have given here the other interesting thing about ACS is kotas and max rate your quota is something like 50 thousand emails per 24 hour period you can of course go ahead and raise the support requester by explaining your business case and Amazon is convinced they will increase this quota to a higher limit and as of now I can send only fourteen emails per second so if I multiply it 86,400 I can send about close to about 2 lakh emails per second for a day so that is the max I can send I cannot send millions of emails every day so if you want to increase your limits go ahead and click on this and find out how to increase your limits and of course you need to justify damage on saying that you are using it for legitimate purposes and not for spamming or any other unauthorized or unethical use so the first thing that we need to do when you're using an SNS service is going to create in topic so you will have here the big icon here create a topic and then I'm going to say is it all you want and display name always has to be less than if I go ahead and type something that is going to give me a nice small and click on create there's a talk with are identified by their names so display names so it has to be 10 characters and their address or they are uniquely identified and you can see here there is a sophomore subscriptions in the bottom of the page and I can create my subscription by using this icon on the left hand side but if you do that you need to copy this air and number also there if we go and choose that come on for some reason I'm not able to click that let me go to something else let me refresh my screen itself let us go ahead and it is a written you should be getting a notification email to subscribe but let me also show that because I have done it is my email address as well on create subscription and let us go to our email box now so we have couple of subscriptions here and looks like mr. Durbin has already subscribed to our topic let me go ahead and check my email address now is it you can see here there is an SNS demo notification this is a topic that I created SNS demo and then we can see here it is giving me the topic and click on subscription or I am going to do is go ahead and click on that and it should automatically subscribe me so for contrary s3 event notifications let me choose one bucket let us say a static website galaxy demo let me choose this bucket for our demo pop versa and here under that properties and if we scroll down under properties there will be something called as events and let us choose that and go ahead and configure our events here I am going to say add event I'm going to modify for uploads I'm going to choose paid all delete all that means that all the event for creation and deletion not just put post everything I don't want individually do that I want to get motivate for all of them and I'm going to leave the prefix as empty itself so any object whether it is images or jpg or HTML anything you get and here if I get the different choices whether I want to send it to lamda sqs or SMS choose SNS and since we have already done created our topic and subscribe to it also all I have to do is just choose this from here chili through what region am I in and because okay I need to add the topic policy also that always I will not be get it here just one moment let me create another bucket itself in Virginia region so that we can choose s and s topic so you know three by me I'm just going to click on create I don't need anything else so my bucket is created in Virginia let me go ahead and choose that and let me also update my policy now itself if I go to permissions and if I have got a bucket policies I need to update my policy here so that it will work and policy is in the article that is here and this is policy and only have to change here is two things one is my SNS a are a number and then my but getname either you can do it at bucket level policy or you can go ahead and do it in a SNS topic policy so either way you can do it in this case I am given here and everything so you upload this into an SNS topic policy so let us not do it here but whatever policy will just keep the bucket clean and let me go ahead and just do the properties of and events click on add events by who SMS for all of this and the latest you SNS topic and if it is not coming that is because your sonís topic demo topic and click on save there will be an error message saying that policy is not there you can see here unable to validate the destination configuration permissions on the destination topic is blah blah blah it is not there I'm just going to go ahead and do that now for you go to topics select the topic that I am interested in click on actions edit topic policy and go to advanced view you're going to remove everything that is already there and not because I will need it it's a are a number leave the error number copied policy from this code the code just pasting it and you can see here have mentioned it very clearly value natok it update your SNS air and here I'm just going to copy this whole thing and you're going to update here next thing is I need to update my bucket name here just going to get my name from my s3 dashboard let me go ahead and pick it up my tree packet name is SNSs you notified smoke going to update it here again the corn save or update policy so now my policy is updated with the necessary permissions if i go back to my s3 dashboard and go to my events section and click on save it is going to validate it and accept that configuration so my congregation is updated so let us go ahead and upload some objects so I'm just going to choose a simple file cloud small dot jpg click on upload and upload progress is happening let me go to my email now it is successfully completed let me go to our email it'll be tricky because I I am receiving a lot of I configured a cloud trail and getting a lot of messages mr. Thurmond if you can confirm me whether you got the message so I can go ahead and check it to my myself over here you can see here there is a key called object cloud small dot a jpg and it is coming from air and of s and s topic so that is how you get an email you see all the other emails it is because I have configured some other demos and I can also do it more this is my topic name but should be able to filter by those messages only the phone is the configuration confirmation and second 1s are coming through the bucket itself whenever I am uploading it so that is how simple it is to configure senesce to work with your server let us go ahead and do the same two more with my ec2 server so the first thing that we are going to setup in cloud watch is we are going to learn how to set up an alarm so when you go to allow I can go ahead and create an along here and you have a lot of metrics for different services for easy to 96 4lbs someone metrics and for building and like that a lot of different services are there and if you have having a premium account a paid account or enabled to detail the monitoring you will have some more services enabled for you by default if you remember it will have only five minute monitoring and somewhere when you're launching an ec2 it will ask you do you want to enable detailed monitoring and once you enable that here we go so let me go ahead and click on enable detailed monitoring and you can see here additional charges will apply and enabling detail modeling will get the metrics at one-minute frequency so let us go ahead and enable that you can enable it but for instance or perfect resource level so now this instance has a detailed monitoring configured and I will be getting metrics at every minute let us go back to dashboard and I'm interested in monitoring this CPU of this server let me go to ec2 matrix and it's going to take the instance ID so we can filter data based on zài jiàn it up h/h so my instanceid is going to be here just copy this and what to create alarm by the CC two metrics here going to put it here coin select metric let's just go to all metrics but I don't have any instances of that name you can see here all the resources that we hit at all that was in my account we all the target group that we created for easy all the older ones are also there as well from all there are no metrics for easy through let me write again I'm in the same region yeah and let me go to easy to for instance metrics let go ahead and do what else it has so that I've no matrix s of now appearing for the toilet let me just give it a few minutes at least for the metrics to appear just start at the server and there is nothing available for that server right now finally we got some metrics for some of those items that you would like to know for example CPU utilization if we filter into by the instance that you are interested in you look at those metrics go ahead and select in this case I'm saying CP utilization go ahead and click on next and here I'm just going to call it has the CPU monitor and I want to notification whenever my CPU is to say beyond 250 minutes and how many data points I want to measure I want to measure the data point like two data points love that even if you want data point so I only notified and I did no points have collected as of now you can see here it is every 15 min I'm in five minutes I want to reduce it to say for example one minute because it is a smallest interval that I am monitoring my server right now so I'm going to choose that and for missing data what you wanted alarm let us treat it as missing only it does not do extrapolation of past history just leave it as it is as missing here is the interesting part but what you want to do you want to trigger an alarm or there are three states for any alarm that is it just along that means alarm is triggered state this okay means the condition has not been met or the alarm doesn't have enough data to decide whether the alarm has to be triggered or stages okay so that is why it is called as insufficient data so whenever this alarm happens I want to trigger an alarm so I put the two stages along and do I want to send a notification yes I would like to send a notification so I'm going to choose this one as an sto topic and automatically all the email addresses picked up in this topic will be sent a notification whenever this alarm is triggered so do I want to add more notifications here is the part I was told you about easy to auto recovery actions do you want to recover this instance stop this instance or terminate this instance whenever certain actions happen say for example a hardware failure in this case we are triggering an alarm for CPU utilization so let us not do that you'll see that separately and auto-scaling actions also here it is whether you are target to group that you would have had here and what kind of action with addresses scale in or scale out now we are talking about the CPU more at 80 percentage so you probably see a scale out the event had more solar so that is how you take the other actions for now let us have a simple SMS notification and click on create an alarm so it is going to go ahead and check the last to two minutes and it is going to show me the history and you say is that warning the email subscription is a pending that is one of those email addresses is not subscribed that is because that email address is wrong or in character so one of us should be getting an email let me go ahead and stress the CPU as of now you can see here if you go to my server and if I go to monitoring and if I go to CP utilization it will be like a bare minimum like a soft now you can see here the dot is at about 0.1% age so let us go ahead and do something to increase our CPU and see whether we can trigger an alarm stress - I will CPU run ten different threads and random parallely and I motor 400 seconds so if you are interested in people who might know or might not know Linux there is a command to call it a top that will show you the performance of your CPU in 12-time so if I just go ahead and execute it up right now and this is the CPU metrics and as of now you can see here it just fluctuates between 0 v 1 or 2 percentage it is go ahead and execute this stress command and it is the initiated all the things like mine go over here and you can see here my CP utilization is despite due to all the 100 way so this is the top command which is showing you the 100 person is the CP utilization and this is the stress command running parallel threats at maximum utilization so you can go and run any number of threats any number of time this is the commander here so anyway this is all I am doing just to trigger an alarm so that we will get an SMS notification and alarm state will go also as from ok state 2 alarm state floor watch dashboard to refresh my screen and it is going to take some time you can see here the spike in the CPU slowly it is appearing because we are monitoring it for every 1 minute so from the last one minute less CPU is going to spike slowly it has gone from 0.1 on to something like a 2 in a few minutes it's sure to go beyond 100 percentage you can see here along is that ok state right now and we should be able to see that in alarm state after that we can see here the blue line has crashed across to that red line so my alarm state is changing as you can see here my alarm state has triggered and my CPU notification must have triggered one email at least to this email address you can see here that is the CPU monitor the klom for l1 support that is the new SNS topic that we just now created and you can see here it is taken from Jericho alarm Stata because one of the data points was at 71 percentage at average and that is triggered my alarm because I was saying that video should have monitor whenever the CPU utilization is less than 80 percentage so this is a convoluted way because last time our SMS topic did not have one email it just is configured properly so the notification did not trigger but if you get your SNS topic up and write it running and you should be able to get along alarm configurations working so that is one way of triggering an alarm just based on metrics the another way of triggering an alarm is based on let us say when you have events here events you will have to create the rule and the revenge rule is the way to quit user friendly we're going to use this service which service that you are going to trigger an alarm for I'm going to go ahead and choose an ec2 here go ahead and choose ec2 and I want to get notifications whenever there is a change in my event type so when we choose all events if you want a particular state codification go ahead and change state notification and whether you want to change all states or particular states for example running or shutting down anything you can go and change let us say any state I wanted to get a notification so the next thing is we are going to put in some more details and configure our targets now let us see we have done here it is now what you need to do when this event is triggered whether the state change currently my ec2 server is up and running it is in the running state and it changes to stop the state or termination state what should I do I am going to send an SMS notification once again and Here I am going to send the hello and supports topic or l1 support team I'm going to send the notification what type of event I want to send all the messages are part of the message or full event so I'm going to say at the end add event itself click on half I don't want to add another target just create one target and then make sure you're choosing SNS Elwin support and match the full event scroll down you will have configured details how often do you want to trigger it what is the name you want to give it I want to say it monitor give it clear state monitor I make sure it enabled on it fool so my rule is enabled now server is running state and I'm not getting going to get any email so what I'm going to do is I'm just going to turn off this server now so I'm going to get at least two emails now because the first state changes is stopping that is from running it has gone to stopping state and then from stopping it will go ahead and three just stop the state after some time so I will get an alarm for that as well let me go to my email now here there is an l1 support a notification let me go ahead and open that and if I can highlight it to here you can see here that is an instance ID here and then it says it is stopping so that is the first state notification email that I am going to get and in a short while you can see here there is a new email let us come here and who will notifies me let us go ahead and refresh my screen Gordon to control and you can see here that it is the server has stopped so this is another way of configuring alerts for your servers whenever the state of the server changes from one state to another state so you can go ahead and see all the trails that are all the recent events that has been configured in my account if I want to go ahead and see more active events just click on it and approach that so let me go to trails section and this is how you are going to create a trail now so click on create trail and I'm just going to say as all friends in and there you want to apply to hot regions or you want to apply specific is anything going to queue though it is going to be only for this region and it is going to be collecting so in best practice always connect in all regions and whether you want to collect all events or certain read-only events or write only events or and what what type of events that you want to collect so there was a question here whether I want to the monitor read-only events whether things are captured probably if I am going to sell it read only events here I'm going to collect that humans as well so let me do everything and s3 have additional events configured whether you want a bucket notification for the gate object or foot object or lambda electrical or not along - phrase or not if you want those kind of notifications or so then you can go ahead and choose for those services select for all s3 buckets or if for lambda which functions that you want to monitor so that type of data events are also you can send to cloud trail so let's just match to that right now and where do you want to store all these messages do you want to create a new bucket or an existing but let me say you have an existing bucket and it is going to ask you what is the bucket name and I'm going to say logs kind of activities and everyone says what is the things I want you it gives a friendly message saying this is how it will appear but I am going to put the club in and put I mean I don't need a for / it which means saying how the logs are going to appear for me and do I want to encrypt my files go ahead and choose it it's simple you can go ahead and choose your kms key or if you have an existing key there in your account go ahead and choose that if you don't want it I don't want to create it so go ahead and choose that but mostly if you are in production your clients will give you the key with which they want to configure your cloud ring going to be encrypted and you will configure it here and do you want an SNS topic notification like the one that you are seeing in my gmail address I have one configured so if I go ahead and select it now to create a new topic I can go ahead and select the SNS topic which you are interested in and that email address will receive all the events that are happening here let's say every five minutes the events will be aggregated and say this packet is stored and I will get a notification saying that these events are dumped here and click on create so that's all you have to do for configuring club trail okay bucket policy also you need to do if you just go ahead and click on it how much one will give you the bucket policy to configure a club trails that is once again like SNS we will have some bucket policies and I have done that in my logs bucket let me show you that here you can see here this is the bucket policy you just all you have to do is copy this bucket policy and let me update the hair and off the bucket name and then you need to have optional prefixes and all those things and then give your account name also then you would be able to configure editor I mean you will be here your bucket will be able to receive it let me just open an existing a bucket which has its working each suffix or subdirectory will need to have approval for plural - right on top of that so for example in this logs bucket I'll have an root-level permission let me go to bucket policy here and you can see here the bucket level policy is there for a closed rail - right on top of that so you can see your bucket has full control and then this is the logs output and here is the AWS logs this is what the prefix cloud trail will add to you if you are creating a bucket if I go back here you can see here this cloud rail logs by account numbers and in cloud and then the region for which the log is collected so you the air and will ensure that this bucket has the necessary policies to allow cloud trained to write all that information here just copy this and put it in your bucket policy after changing this rate parameters to whatever parameters you need to change this is the bucket name and any prefix you are giving and then the account ID and it will work after that