AWS Case Playbook

Case Severity

AWS ITIL Incident Priority Matrix				
Urgency + Impact = Severity		Urgency		
		Low	Medium	High
Impact	Low	Low	Normal	High
	Medium	Normal	High	Urgent
	High	High	Urgent	Critical

Severity Level	Response Time	Examples for Reference
Business-critical system down	15 min	Major outage – loss of control of the entire enterprise, entire customer base, or have the potential for a large revenue loss.
Production system down	1 hr	You can't work around the problem, and your business is significantly impacted. Important functions of your application are unavailable.
Production system impaired	4 hrs	You can't work around the problem. Critical functions of your application are impaired or degraded.
System impaired	12 hrs	You can work around the problem. Non-critical functions of your application are behaving abnormally. You have a time-sensitive development question.
General guidance	24 hrs	You have a general development question or want to request a feature.

Case Template

Case General Template

Severity : Low / Normal / High / Urgent / Critical

- Subject : Instance health check failure
- Description :

Hi,

There was instance health check failure. Please check whether there was host issue at the below time.

* Account ID : 123456789012
* Region : Seoul(or ap-northeast-2)
* Resource : i-12345678/elb endpoint/rds endpoint/etc
* Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00

Thanks,
Customer Name

- Requirement
  - ✓ Account ID
  - ✓ Region
  - ✓ Resources
  - ✓ Timeline + TimeZone (Start Time ~ End Time)
  - ✓ Your name
- If Korean support is needed, please open cases during Sydney working hours.
(07:00 ~ 03:00 KST)

amazon web services

Account and Billing Case Template

Severity : Low

- Subject : Account Activation
- Description :
  Hi,

  I have created the below account, but I cannot activate the account. In addition, I cannot call any APIs related to EC2. Please let me know what I should do to activate the account properly.

  * Account ID : 123456789012

  Thanks,
  Customer Name

- When you have any account/billing issues, you can open a case.
  - ✓ Activation
  - ✓ MFA Token
  - ✓ Reserved Instances

General Question

Severity : Low / Normal

- Subject : A question about DynamoDB
- Description :
  Hi,

  We are considering using DynamoDB to store the session. Are there any use cases or best practices to store data on DynamoDB? In addition, is there any way to delete useless data automatically?

  Thanks,
  Customer Name

- You can ask a general question through a case as well.

Bad Cases (1)

Severity : Critical

- Subject : Something wrong on my instance!!!
- Description :
  My instance is crazy. Please fix it ASAP!

- No information at all.

Bad Cases (2)

Severity : High

- Subject : I have experienced something wrong.
- Description :
  Hi,

  I launched an EC2 instance yesterday, and I installed the Apache web server. It was fine for a while, and suddenly my web server went down. I don't know why. So, I checked my instance, and it looked fine because the instance was totally healthy. "httpd" process was working, but I could not connect to the web server through Chrome browser.

  So, I killed the process, and restarted the Apache web server, but I could not restart the Apache web server. I felt that something wrong happened. So, I logged out the instance, and tried to ssh the instance, but I was not able to connect to the instance at all! I checked the security group rules, but everything looked fine.

  Finally, I decided to stop and start the instance, but I failed to stop the instance because it was stopping for 30 minutes! Then, the instance was stopped finally, and I started the instance, and sshed the instance. Starting the Apache web server, it worked at this time. And, I was able to connect to the web page on Chrome browser.

  So, my question is why I was not able to connect to the instance and web page, and why I was not able to restart the Apache web server when the issue was occurred. Is that my fault or your fault? I guess this was because of AWS problem!!!

  Wish me luck!

- No information at all.
- Too lengthy to find out the real issue.

Bad Cases (3)

Severity : Critical

- Subject : Please check an instance!!
- Description :
  Please check an instance!! It is normal, but had an issue!!!

  Instance ID : i-12345678

- Not a good case, but not the worst case either.
- At least there is instance ID, it could be a trigger to develop the case.
- Not a critical case because the issue has been gone.
- Needs more information.

Case Example

EC2 - Status check failure (0/2)

Severity : Low / Normal / High

- Subject : Instance health check failure
- Description :

Hi,

An instance went down. I would like to know why the instance failure happened.

* Account ID : 123456789012
* Region : Seoul(or ap-northeast-2)
* Instance ID: i-12345678
* Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-01 11:00

Thanks,
Customer Name

- System status check failure can happen because of below reason:
  - ✓ Loss of network connectivity
  - ✓ Loss of system power
  - ✓ Software issues on the physical host
  - ✓ Hardware issues on the physical host
- Generally when an EC2 instances goes down, you generally need to stop and start the instance to recover from failure.
- When you need to figure out why the instance goes down, you can open a case lower than or equal to “High”.

EC2 - Cannot stop an instance

Severity : High / Urgent / Critical

- Subject : An instance is stuck to stop
- Description :
  Hi,

  An instance cannot be stopped for XX minutes/hours even though I tried to do “Force Stop” the instance. Please force-stop the instance.

  * Account ID : 123456789012
  * Region : Seoul(or ap-northeast-2)
  * Instance ID: i-12345678
  * Timeline(UTC) : 2016-04-01 10:00 ~

  Thanks,
  Customer Name

- When the underlying host hardware has an issue, a stuck instance can be happened. Then, you sometimes cannot stop the instance for a while.
- If the instance is stuck so it is not possible to do “Force Stop”, then you can open a case to ask doing “Force Stop” the instance. In this case, you can open an “Urgent” or a “Critical” case depending on the sense of urgency.
- You cannot ask to do “Force Stop” the instance if the instance goes down because of the scheduled maintenance event. AWS only can accept the case when the scheduled maintenance event is due to degraded host hardware.

EC2 - Unexpected rebooting

Severity : Low / Normal / High

- Subject : An instance was rebooted unexpectedly
- Description :
  Hi,

  We experienced unexpected instance rebooting. As far as I can see, there was no scheduled maintenance event on the time, and no one has rebooted or stopped the instance. Could you verify if there was a host hardware failure?

  * Account ID : 123456789012
  * Region : Seoul(or ap-northeast-2)
  * Instance ID : i-12345678
  * Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00

  Thanks,
  Customer Name

- At first, you need to check if there is scheduled maintenance event.
- Secondly, you need to check if any IAM user rebooted or stopped/started the instance through CloudTrail logs.
- If there is no scheduled maintenance event and history of rebooting(stopping/starting) the instance, you can open a case to check if there was a underlying host hardware issue.
- You need to check the instance log to figure out when the issue happened.

amazon web services

EC2 - Ephemeral Disk Recovery

Severity : Low / Normal / High

- Subject : Ephemeral disk was broken
- Description :
  Hi,

  One of the ephemeral disk was broken. Would you recover the ephemeral disk(/dev/sdb)?

  * Account ID : 123456789012
  * Region : Seoul(or ap-northeast-2)
  * Instance ID : i-12345678

  Thanks,
  Customer Name

- Note that do not store important data on ephemeral disks.
- When you already stopped an instance, the data cannot be recoverable.
- AWS does not guarantee the data recovery, and it takes time to recover the data.

EBS - Unable to detach a volume

Severity : Low / Normal / High / Urgent / Critical

- Subject : Unable to detach a volume even though we tried to force-detach the volume
- Description :
  Hi,

  We are trying to detach a volume, vol-12345678, from an instance, i-12345678. We already tried to force-detach the volume, but it is still detaching for XX minutes/hours. Can you detach the volume and tell us what the issue is?

  * Account ID : 123456789012
  * Region : Seoul(or ap-northeast-2)
  * Instance ID : i-12345678
  * EBS ID: vol-12345678
  * Timeline(UTC) : 2016-04-01 10:00 ~

  Thanks,
  Customer Name

- Generally, you can do “Force Detach” a volume.
- When the customer cannot detach the volume even though the customer tries to do “Force Detach”, you can open a case.
- Depending on the sense of urgency, you can choose the right severity.

EBS - Degraded performance (Throughput/IOPS/Latency)

Severity : Low / Normal / High / Urgent / Critical

- Subject : EBS degraded performance
- Description :
  Case 1)
  Hi,

  We are experiencing degraded performance on an EBS volume, vol-12345678. Throughput/IOPS were suddenly dropped on 2016-04-01 10:00 UTC, and it is still happening. We have checked our application, but have not found any issues. Could you investigate this issue?

  Case 2)
  Hi,

  We experienced high write latency on an EBS volume, vol-12345678. Spikes in latency were happened from 2016-04-01 10:00 to 2016-04-01 11:00, and it is not happening right now. Could you investigate if there was an issue on the volume?

  * Account ID : 123456789012
  * Region : Seoul(or ap-northeast-2)
  * Instance ID : i-12345678
  * EBS ID: vol-12345678
  * Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00

  Thanks,
  Customer Name

- When you experience degraded performance (more than 10%)on a volume, then you can open a case to check if there was an issue.
- If the issue is not on going, AWS recommends you to choose the severity lower than or equal to “High”.
- If the issue is on going, and it is critical to the service, you can open an “Urgent” or a “Critical” case.

ELB - Pre-warming

Severity : Low / Normal / High

- Subject : ELB Pre-warming request
- Description :

Hi,

We need the ELB to be pre-warmed because we have a new game launching event.

* Account ID :
* ELB DNS Name :
* Event start date/time(If traffic has already started, is the lack of this prewarm causing impact to a live application?)
* Event end date/time
* Expected percent of traffic going through the ELB that will be using SSL termination.
* An approximate percentage increase in traffic, or expected requests/sec that will go through the load balancer (whichever is easier to answer).
* If different from current load, what is the average amount of data passing through the ELB per request/response pair?
* Number of Availability Zones enabled
* Is the back-end currently scaled to the level it will be during the event?
  - If not, when do you expect to add the required back-end instance count?
* A description of the traffic pattern you are expecting:
  - Is this a single increase in traffic that will be sustained afterwards, or will there be periods of inactivity followed by high traffic? If there are periods of inactivity, please describe the pattern (e.g. weekly spikes on Monday)
  - Large file uploads/downloads?
* A brief description of your use case.
  - What is driving this traffic? (e.g. application launch, event driven like marketing/product launch/sale, etc)
* Are the back-end instances using persistent connections (keep-alive)?

Thanks,
Customer Name

- ELB is automatically scaling by itself, so basically you do not need to open a case to request ELB pre-warming.
- When you have a certain event, which can cause higher traffic than usual, you can request ELB pre-warming.
- A case for ELB Pre-warming should be opened at least 3 business days before a certain event.

amazon web services

ELB – 5xx

Severity : Low / Normal / High / Urgent / Critical

- Subject : Continuous ELB 5XX errors
- Description :
  Hi,

  We are experiencing 5XX errors continuously. We have checked backend instance capacity, and found the number of backend instances is fine. In addition, maximum latency is not so high. We also checked our application logs, but we have not found any issues. I have attached ELB access logs, so could you investigate this issue?

  * Account ID : 123456789012
  * Region : Seoul(or ap-northeast-2)
  * ELB : test-1732137940.ap-northeast-1.elb.amazonaws.com
  * Timeline(UTC) : 2016-04-01 10:00 ~

  Thanks,
  Customer Name

- First of all, you need to check ELB Idle timeout and backend instance's keepAlive connection timeout.
  - ✓ KeepAlive connection timeout >= ELB Idle Timeout
- Secondly, you need to check if your backend instances are too busy to handle request, and if there is an issue related to your application.
- Providing ELB logs would be better to investigate the issue.

amazon web services

RDS - Failover

Severity : Low / Normal / High

- Subject : Unexpected RDS failover
- Description :

Hi,

RDS instance was failovered unexpectedly. Were there any issues on the underlying host hardware? Or was it because of another reason?

* Account ID : 123456789012
* Region : Seoul(or ap-northeast-2)
* RDS : test-rds
* Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00

Thanks,
Customer Name

- RDS failover could be happened when the underlying host hardware has an issue.
- When your RDS instance was failovered unexpectedly, you can open a case.

RDS – Performance (General)

Severity : Low / Normal / High / Urgent / Critical

- Subject : RDS performance issue
- Description :

Hi,

We have experienced RDS performance issue at the time. Read/Write IOPS were extremely dropped at 2016-04-01 10:00, and recovered several hours later(2016-04-01 12:00). During the time, we had degraded performance of our application. Would you investigate if there were any issues on RDS instances?

* Account ID : 123456789012
* Region : Seoul(or ap-northeast-2)
* RDS : test-rds
* Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00

Thanks,
Customer Name

- When performance issue related IOPS, CPU utilization, and so on, you can open a case to check if there is a RDS issue.
- Describe the “issue” you have in detail as much as possible, but not so lengthy.

RDS – Performance (Latency)

Severity : Low / Normal / High / Urgent / Critical

- Subject : Latency spikes on RDS
- Description :
  Hi,

  We have experienced irregular latency spikes, and whenever it happens, many slow queries has been occurred. We have investigated slow queries, but nothing special has been executed, and most of queries were small queries. It is still happening irregularly. Could you investigate if there was infrastructure issue particularly at 2016-04-01 10:00 UTC?

  I have attached sample slow queries.

  * Account ID : 123456789012
  * Region : Seoul(or ap-northeast-2)
  * RDS : test-rds
  * Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00

  Thanks,
  Customer Name

- Latency can be related to usage patterns. For examples, if you executes big queries frequently, latency could be high.
- You need a DBA to investigate the issue in your side before opening a case.

S3 - Performance

Severity : Low / Normal / High / Urgent / Critical

- Subject : S3 performance issue
- Description :
  Hi,

  We are experiencing S3 performance issue, so please see the detail information below:

  * Account ID :
  * Bucket and object name (i.e. s3://bucket/folder1/object1)
  * HTTP or HTTPS
  * Is this only on for PUT requests, or GETs as well?
  * Endpoint used (i.e. s3-us-west-2.amazonaws.com)
  * Source and destination IP addresses for the request (can be obtained with tools like netstat or packet captures)
  * traceroute (preferably tcptraceroute) or MTR (especially if the issue is intermittent) to S3 IP address above from client (if possible please provide both)
  * Specific time and timestamp of the request
  * Are you connecting from EC2? If so, are you making requests using VPC Endpoints, IGW (VPC), or EC2 Classic?

  Thanks,
  Customer Name

- When you experience S3 performance issue, you can open a case to find out the issue.

CloudFront - Performance Issue

Severity : Low / Normal / High / Urgent / Critical

- Subject : Getting contents from CloudFront is slow
- Description :

Hi,

Getting contents from CloudFront is slow from instances in Seoul region, so I have checked the routing path, and it looks like reaching out to other region, the United States.

* Account ID : 123456789012
* Distribution ID : E1EEE1EEEEEE1
* Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00
* traceroute :

```
ubuntu@ip-10-20-13-122:~$ traceroute du5ar2l6dy86v.cloudfront.net
traceroute to du5ar2l6dy86v.cloudfront.net (52.85.142.45), 30 hops max, 60 byte packets
 1  ec2-52-79-0-2.ap-northeast-2.compute.amazonaws.com (52.79.0.2)  15.746 ms
15.792 ms  15.865 ms
 2  100.64.2.10 (100.64.2.10)  14.120 ms 100.64.1.10 (100.64.1.10)  13.959 ms
100.64.0.202 (100.64.0.202)  58.574 ms
 3  100.64.1.133 (100.64.1.133)  14.412 ms 100.64.2.7 (100.64.2.7)  19.292 ms
100.64.2.133 (100.64.2.133)  14.406 ms
...
17  server-52-85-142-45.iad12.r.cloudfront.net (52.85.142.45)  177.545 ms  175.218 ms *
```

Please investigate if there is an issue on Seoul edge location, or it is another issue.

Thanks,
Customer Name

- Each of your end users is routed to the edge location closest to them, in terms of internet latency.

Network Performance/Connectivity

Severity : Low / Normal / High / Urgent / Critical

- **Subject** : Network performance issue/Network connectivity issue
- **Description** :

Case 1)
Hi,

We are currently experiencing network connectivity issue between an ISP(KT/SKT/LG U+) in Korea and instances in Seoul region. We cannot connect to specific servers with TCP 80 port even though we added a rule at the security group. Please investigate if there is any known network connectivity issues between the ISP and AWS.

Case 2)
Hi,

We have experienced high latency between instances in Seoul region and instances in Tokyo region. Normally, the latency is about 30ms, but the latency was higher than 200ms for 3 hours. It is not happening right now. Please see the above traceroute(mtr) result, and investigate if there was a network issue between two regions.

* Account ID : 123456789012
* Timeline(UTC) : 2016-04-01 10:00 ~ 2016-04-10 10:00
* Source IP/Destination IP : Source) 123.456.789.0, Destination) 234.567.890.1
* Source to Destination traceroute(tracetcp) or MTR :
* Destination to Source traceroute(tracetcp) or MTR :

Thanks,
Customer Name

- You need to provide as much data as you can. When you provide data, AWS recommends you to provide data with service port.
- For example, traceroute (tcptraceroute or tracetcp) or MTR data with service port is preferred.
  - ✓ mtr -rw -c 10 --no-dns --tcp --port 80 google.com
- Data which is gathered at the time the issue was occurred would be useful to investigate the issue.
- If the issue is not on going, AWS recommends you to open a case lower than or equal to “High”.