

Description

This document is intended for [CustomerName] [WorkloadName].

[Insert short description of what the workload is intended for].

Step: Priority

Priority actions

1. When a case is created with Incident Detection and Response, lock the case to yourself, verify the Customer Stakeholders in the Case from *Engagement Plans - Initial Engagement*.
2. Send the first correspondence on the support case to the customer as below. If there is no support case or if it is not possible to use the support case then backup communication details are listed in the steps that follow.


[AWS Support](#) > [Your support cases](#) > Details

Case ID 12345678912345 [Info](#) [Resolve case](#)

Case details

Subject Incident Detection and Response - Immediate Attention Required [Account: 12345678912]	Status Pending amazon action
Case ID 12345678912345	Severity Business-critical system down
Created 2023-11-17T14:21:23.388Z	Category -
Case type Technical	Language English
Opened by xyz@email.com	Additional contacts -

Correspondence

AWS

Amazon Web Services

Fri Nov 17 2023
16:27:25 GMT+0200
(South Africa Standard Time)

Translate ▼

Hello,

AWS Incident Detection and Response has been engaged by a metric in alarm for your workload.
We are currently investigating and will update you in a few minutes once we have finished our initial investigation.

Alarm Identifier - arn:aws:cloudwatch:us-east-1:12345678912:alarm:production-test-test-api-Alert-CRITICAL

We value your feedback. Please share your experience by rating this and other correspondences in the AWS Support Center.
You can rate a correspondence by selecting the stars in the top right corner of the correspondence.

Best regards,
AWS Engineer,
Amazon Web Services

Was this response helpful? Click here to rate:
★ ★ ★ ★ ★

Compliance and regulatory requirements for the workload

<<e.g. The workload deals with patient health records which must be kept secured and confidential. Information not to be shared with any third parties.>>

Actions required from Incident Detection and Response in complying

<<e.g Incident Management Engineers must not shared data with third parties.>>

Step: Information

Review of common information

- This section provides a space for defining common information which may be needed through the life of the incident.
 - The target user of this information is the Incident Management Engineer and Operations Engineer.
 - The following steps may reference this information to complete an action (for example, execute the "Initial Engagement" plan).
-

Engagement plans

Describe the engagement plans applicable to this runbook. This section contains only contact details. Engagement plans will be referenced in the step by step **Communication Plans**.

- **Initial engagement**

AWS Incident Detection and Response Team will add customer stakeholder addresses below to the Support Case. AWS Stakeholders are for additional stakeholders that may need to be made aware of any issues.

When updating customer stakeholders details in this plan also update the Backup Mailto links.

- **Customer Stakeholders:** customeremail1; customeremail2; etc
- **AWS Stakeholders:** aws-idr-oncall@amazon.com; tam-team-email; etc.
- **One Time Only Contacts:** [These are email contacts that are included on only the first communication. Remove these contacts after the first communication has gone out. These could be customer paging email addresses such as pager-duty that must not be paged for every correspondence]
- **Backup Mailto Impact Template:** <Insert Impact Template Mailto Link here>
 - Use the backup Mailto when communication over cases is not possible.
- **Backup Mailto No Impact Template:** <Insert No Impact Mailto Link here>
 - Use the backup Mailto when communication over cases is not possible.

- **Incident call setup** Indicate if the customer requires Incident Detection and Response to create a bridge, if the customer uses a static bridge or if the customer will provide a bridge when an incident is opened. (Choose one and delete the rest)
 - Incident Detection and Response create a Chime Bridge
 - Customer uses a static Bridge
 - Conference Number: < Insert Conference number >
 - Customer provides bridge details for every incident by responding to communication sent out by AWS Incident Detection and Response Team.
 - Other - Specify details.

- **Engagement Escalation**
 AWS Incident Detection and Response will reach out to the following contacts when the contacts from the **Initial engagement** plan do not respond to incidents.
 For each Escalation Contact indicate if they must be added to the support case, phoned or both.
 - **First Escalation Contact:** [escalationEmailAddress#1] / [PhoneNumber] - Wait XX Minutes before escalating to this contact.
 - [add Contact to Case / phone] this contact.
 - **Second Escalation Contact:** [escalationEmailAddress#2] / [PhoneNumber] - Wait XX Minutes before escalating to this contact.
 - [add Contact to Case / phone] this contact.
 - Etc;

Communication plans

Describe how Incident Management Engineer communicates with designated stakeholders outside the incident call and communication channels.

- **Impact Communication plan**
 This plan is initiated when Incident Detection and Response have determined from step **Triage** that an alert indicates potential impact to a customer.
 Incident Detection and Response will request the customer to join the predetermined bridge (Chime Bridge/Customer Provided Bridge / Customer Static Bridge) as indicated in **Engagement plans - Incident call setup**.
 All backup email templates for use when cases can't be used are in **Engagement plans - Initial engagement**.

- 1 – Before sending the impact notification, verify then remove and/or add customer contacts from the Support Case CC based on the contacts listed in the **Initial engagement** Engagement plan.
- 2 – Send the engagement notification to the customer based the following Template:
(choose one and remove the rest)

Impact Template - Chime Bridge

[AWS Support](#) > [Your support cases](#) > Details

Case ID 12345678912345 [Info](#)

Resolve case

Case details

Subject Incident Detection and Response - Immediate Attention Required [Account: 12345678912]	Status Pending amazon action
Case ID 12345678912345	Severity Business-critical system down
Created 2023-11-17T14:21:23.388Z	Category -
Case type Technical	Language English
Opened by xyz@email.com	Additional contacts yxz@email.com;email@email.com

Correspondence

Reply

Amazon Web Services

Fri Nov 17 2023
17:15:54 GMT+0200
(South Africa Standard Time)

Translate ▼

Hello

The following alarm has engaged AWS Incident Detection and Response to an Incident bridge:
 Alarm Identifier - arn:aws:cloudwatch:us-east-1:12345678912:alarm:production-test-test-api-Alert-CRITICAL
 Alarm State Change Reason - TBC
 Alarm Start Time - 1 January 2023, 3:30 PM UTC
 Please join the Chime Bridge below so we can start the steps outlined in your Runbook:
 <Insert Chime Meeting ID>
 <Insert Link to Chime Bridge>
 International dial-in numbers: <https://chime.aws/dialinnumbers/>

We value your feedback. Please share your experience by rating this and other correspondences in the AWS Support Center. You can rate a correspondence by selecting the stars in the top right corner of the correspondence.

Best regards,
AWS Engineer.
Amazon Web Services

Was this response helpful? Click here to rate:

★ ★ ★ ★ ★

Impact Template - Customer Provided Bridge

[AWS Support](#) > [Your support cases](#) > Details

Case ID 12345678912345

Info

Resolve case

Case details

Subject

Incident Detection and Response - Immediate Attention Required
[Account: 12345678912]

Case ID

12345678912345

Created

2023-11-17T14:21:23.388Z

Case type

Technical

Opened by

xyz@email.com

Status

Pending amazon action

Severity

Business-critical system down

Category

-

Language

English

Additional contacts

-

Correspondence

Reply



Amazon Web Services

Fri Nov 17 2023
17:23:20 GMT+0200
(South Africa Standard Time)

Translate

The following alarm has engaged AWS Incident Detection and Response to an Incident bridge:
Alarm Identifier - arn:aws:cloudwatch:us-east-1:12345678912:alarm:production-test-test-api-Alert-CRITICAL
Alarm State Change Reason - TBC
Alarm Start Time - 1 January 2023, 3:30 PM UTC

Please respond with your internal bridge details so we can join and start the steps outlined in your Runbook.

We value your feedback. Please share your experience by rating this and other correspondences in the AWS Support Center. You can rate a correspondence by selecting the stars in the top right corner of the correspondence.

Best regards,
AWS Engineer.
Amazon Web Services

Was this response helpful? Click here to rate:

★★★★★

Impact Template - Customer Static Bridge

[AWS Support](#) > [Your support cases](#) > Details


Case ID 12345678912345 [Info](#) [Resolve case](#)

Case details

Subject Incident Detection and Response - Immediate Attention Required [Account: 12345678912]	Status Pending customer action
Case ID 12345678912345	Severity Business-critical system down
Created 2023-11-17T14:21:23.388Z	Category -
Case type Technical	Language English
Opened by xyz@email.com	Additional contacts -

Correspondence

[Reply](#)


Amazon Web Services
Fri Nov 17 2023
17:29:37 GMT+0200
(South Africa Standard Time)

[Translate](#)
Hello
The following alarm has engaged AWS Incident Detection and Response to an Incident bridge:
Alarm Identifier - arn:aws:cloudwatch:us-east-1:12345678912:alarm:production-test-test-api-Alert-CRITICAL
Alarm State Change Reason - TBC
Alarm Start Time - 1 January 2023, 3:30 PM UTC

Please join the Bridge below so we can start the steps outlined in your Runbook:
Conference Number: +XXXXXXXXXXXXX
Conference URL : bridge12345@bridge.com [🔗](#)

We value your feedback. Please share your experience by rating this and other correspondences in the AWS Support Center. You can rate a correspondence by selecting the stars in the top right corner of the correspondence.

Best regards,
AWS Engineer.
Amazon Web Services

Was this response helpful? Click here to rate:
★ ★ ★ ★ ★

- 3 - Set the Case to Pending Customer Action
- 4 - Follow **Engagement Escalation** plan as mentioned above.
- 5 - If the customer does not respond within 30 minutes, disengage and continue to monitor until the alarm recovers.

- **No Impact Communication plan**

This plan is initiated when an alarm recovers before Incident Detection and Response have completed initial **Triage**.

- 1 - Before sending the no impact notification, verify then remove and/or add customer contacts from the Support Case CC based on the contacts listed in the **Engagement plans - Initial engagement** Engagement plan.
- 2 - Send a no engagement notification to the customer based on the below template:

No Impact Template

The screenshot shows an AWS Support case page. At the top, there's a breadcrumb trail: [AWS Support](#) > [Your support cases](#) > [Details](#). The case ID is 12345678912345, with an [Info](#) link. A [Resolve case](#) button is in the top right.

Case details

Subject Incident Detection and Response - Immediate Attention Required [Account: 12345678912] Case ID 12345678912345 Created 2023-11-17T14:21:23.388Z Case type Technical Opened by xzy@amazon.com	Status Pending customer action Severity Business-critical system down Category - Language English Additional contacts -
---	---

Correspondence [Reply](#)

Amazon Web Services

Fri Nov 17 2023
17:36:20 GMT+0200
(South Africa Standard Time)

[Translate](#)

AWS Incident Detection and Response received an alarm that has recovered for your workload.

Alarm Identifier - arn:aws:cloudwatch:us-east-1:12345678912:alarm:production-test-test-api-Alert-CRITICAL

Alarm State Change Reason - TBC

Alarm Start Time - 1 January 2023, 3:30 PM UTC

Alarm End Time - 1 January 2023, 3:35 PM UTC

This may indicate a brief customer impact that is currently not ongoing. If there is an ongoing impact to your workload, please let us know and we will engage to assist.

We value your feedback. Please share your experience by rating this and other correspondences in the AWS Support Center. You can rate a correspondence by selecting the stars in the top right corner of the correspondence.

Best regards,
AWS Engineer.
Amazon Web Services

Was this response helpful? Click here to rate:
★★★★★

- 3 - Put the case in to Pending Customer Action.
- 4 - If the customer does not respond within 30 minutes Resolve the case.

- **Updates**

If AWS Incident Detection and Response is expected to provide regular updates to customer stakeholders, list those stakeholders here. Updates must be sent via the same support case.

Remove this section if not needed.

- Update Cadence: Every XX minutes
- External Update Stakeholders: customeremailaddress1; customeremailaddress2; etc
- Internal Update Stakeholders: awsemailaddress1; awsemailaddress2; etc

Application architecture overview

This section provides an overview of the application/workload architecture for Incident Management Engineer and Operations Engineer awareness.

- **AWS Accounts and Regions with key services** - list of AWS accounts with regions supporting this application. Assists Engineers in assessing underlying infrastructure supporting the application.
 - 123456789012
 - US-EAST-1 - brief desc as appropriate
 - EC2 - brief desc as appropriate
 - DynamoDB - brief desc as appropriate
 - etc.
 - US-WEST-1 - brief desc as appropriate
 - etc.
 - another-account-etc.
- **Resource identification** - describe how engineers determine resource association with application
 - Resource groups: etc.
 - Tag key/value: AppId=123456
- **CloudWatch Dashboards** - list dashboards relevant to key metrics and services
 - 123456789012
 - us-east-1
 - some-dashboard-name
 - etc.
 - some-other-dashboard-name-in-current-acct

Step: Triage

Evaluate incident and impact

This section provides instructions for triaging of the incident to determine correct impact, description, and overall correct runbook being executed.

- **Evaluation of initial incident information**
 - 1 - Review Incident Alarm, noting time of first detected impact as well as the alarm start time.
 - 2 - Identify which service(s) in the customer application is seeing impact.
 - 3 - Review AWS Service Health for services listed under **AWS Accounts and Regions with key services**.
 - 4 - Review any customer provided dashboards listed under **CloudWatch Dashboards**

- **Impact**

Impact is determined when either the customer's metrics do not recover, appear to be trending worse or if there is indication of AWS Service Impact.

- 1 – Start **Communication plans - Impact Communication plan**

- 2 - Start **Engagement plans - Engagement Escalation** if no response is received from the **Initial Engagement** contacts.
- 3 - Start **Communication plans - Updates** if specified in **Communication plans**
- **No Impact**
No Impact is determined when the customer's alarm recovers before Triage is complete and there are no indications of AWS service impact or sustained impact on the customer's CloudWatch Dashboards.
 - 1 - Start **Communication plans - No Impact Communication plan**

Step: Investigate

Investigation

This section describes performing investigation of known and unknown symptoms.

Known issue

- *List all known issues with the application and their standard actions here*

Unknown issues

- Investigate with the customer and AWS Premium Support.
- Escalate internally as required.

Step: Mitigation

Collaborate

- Communicate any changes or important information from the **Investigate** step to the members of the incident call.

Implement mitigation

- *List customer failover plans / Disaster Recovery plans / etc here for implementing mitigation.

Step: Recovery

Monitor customer impact

- Review metrics to confirm recovery.
- Ensure recovery is across all Availability Zones / Regions / Services
- Get confirmation from the customer that impact is over and the application has recovered.

Identify action items

- Record key decisions and actions taken, including temporary mitigation that might have been implemented.
- Ensure outstanding action items have assigned owners.
- Close out any Communication plans that were opened during the incident with a final confirmation of recovery notification.