

# Description

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

## Step: Priority

### Priority actions

1. Send the first correspondence on the support case to the customer as below.

Hello,

This is <<Engineer's name>> from AWS Incident Detection and Response. An alarm has triggered for your workload <<Application\_Name>>. I am currently investigating and will update you in a few minutes once I have finished initial investigation.

Alarm Identifier -  
<insert\_CloudWatch\_Alarm\_ARN\_or\_APM\_Response\_Identifier>

## Step: Information

### Engagement plans

This section describes the engagement plans applicable to this runbook and only contains 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.

- **Customer Stakeholders:** Customeremail1; customeremail2; mobile1
- **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. Explicitly add instructions in "Priority" section, "Communication plans" on how to use these only if *One Time Only Contacts* is available.]

- **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 option based on customer preference)

- Incident Detection and Response create a Chime/Zoom Bridge
- Customer's provided 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.

  - Make sure that you have called Initial Engagement contact, if applicable, before escalating.
  - **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

This section describes how Incident Management Engineers communicate 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 as indicated in **Engagement plans - Incident call setup**.

(choose one depending on whether *One Time Only Contacts* is available or not)

- 1. Ensure **Customer Stakeholders** from **Engagement plans - Initial engagement** are added to the case CC.

OR

- 1. Ensure **Customer Stakeholders** and **One Time Only Contacts** from **Engagement plans - Initial engagement** are added to the case CC.
- 2. Send the engagement notification to the customer based the following Template:

(choose one)

**Impact Template - Chime Bridge**

The following alarm has engaged AWS Incident Detection and Response to an Incident bridge:

Alarm Identifier -

<insert\_CloudWatch\_Alarm\_ARN\_or\_APM\_Response\_Identifier>

Alarm State Change Reason - <insert\_state\_change\_reason>

Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>

Please join the Chime Bridge below so we can start the steps outlined in your Runbook:

Chime Meeting ID: <insert\_Meeting\_ID\_here>

Link to Chime Bridge: <insert\_Link\_here>

International dial-in numbers: <https://chime.aws/dialinnumbers/>

### ***Impact Template - Customer Provided Bridge***

The following alarm has engaged AWS Incident Detection and Response:

Alarm Identifier -

<insert\_CloudWatch\_Alarm\_ARN\_or\_APM\_Response\_Identifier>

Alarm State Change Reason - <insert\_state\_change\_reason>

Alarm Start Time - <Example: 1 January 2025 3:30 PM UTC>

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

### ***Impact Template - Customer Static Bridge***

The following alarm has engaged AWS Incident Detection and Response to an Incident bridge:

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>

Alarm State Change Reason - <insert\_state\_change\_reason>

Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>

Please join the Bridge below so we can start the steps outlined in your Runbook:

Conference Number: <insert\_conference\_number>

Conference URL : <insert\_bridge\_URL>

- 3. Set the Case to Pending Customer Action
- 4. REMOVE ***One Time Only Contacts*** from the case after sending above Impact Communication.  
(If *One Time Only Contacts* is available.)
- 5. Follow **Engagement Escalation** plan as mentioned above.
- 6. 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.

["DO NOT add **One Time Only Contacts**."] (Applicable if *One Time Only Contacts* is available.)

2. Send a no engagement notification to the customer based on the below template:

***No Impact Template***

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

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>

Alarm State Change Reason - <insert\_state\_change\_reason>

Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>

Alarm End Time - <Example: 1 January 2025, 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.

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

---

## **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