



CloudHealth IAM Role Update

External – Bytes AWS Services – 11/08/2020

1 PREFACE

The information contained within this document will be treated with confidentiality and shall be only used by Bytes Software Services for the required project(s) assigned by the client.

1.1 AUTHORS

| Name | Role |
|------------|--------------------|
| Alan White | Solution Architect |
| | |
| | |

1.2 REVISION DETAILS

| Revision | Date | Author | Comments |
|----------|------------|------------|---|
| 1.0 | 06/04/2020 | Alan White | Initial Release |
| 1.1 | 11/08/2020 | Alan White | Mionor update to wording and screenshot |

1.3 DISCLAIMER

Whilst every precaution has been taken in the preparation of this document, no responsibility is assumed for errors or omissions nor is any liability assumed for loss or damage resulting from the use of the information it contains, to the extent such error or omission is a result of any information, data or documents provided to Bytes by the Customer and relied on by Bytes in the preparation of this document.

2 TABLE OF CONTENTS

| | | |
|----------|---|----------|
| 1 | PREFACE..... | 2 |
| 1.1 | AUTHORS | 2 |
| 1.2 | REVISION DETAILS | 2 |
| 1.3 | DISCLAIMER | 2 |
| 2 | TABLE OF CONTENTS | 3 |
| 3 | INTRODUCTION..... | 4 |
| 3.1 | OVERVIEW | 4 |
| 3.2 | PURPOSE | 4 |
| 3.3 | PRE-REQUISITES..... | 4 |
| 4 | CLOUDFORMATION UPDATE INSTRUCTIONS | 6 |
| 4.1 | SUMMARY STEPS | 6 |
| 4.2 | INSTRUCTIONS | 6 |
| 5 | MANUAL UPDATE INSTRUCTIONS | 9 |
| 5.1 | SUMMARY STEPS | 9 |
| 5.2 | INSTRUCTIONS | 9 |

3 INTRODUCTION

3.1 OVERVIEW

Occasionally AWS and/or CloudHealth release new features that require adjustments to the permissions required by CloudHealth to access the target cost optimized AWS account. Updating these permissions allows new features and capabilities to be leveraged by the customer to give greater control and/or visibility of their cloud environments.

3.2 PURPOSE

This guide will help you through the steps required to update the CloudHealth IAM role in each AWS account in order to take advantage of the new features and gain enhanced visibility of your AWS cloud environment.

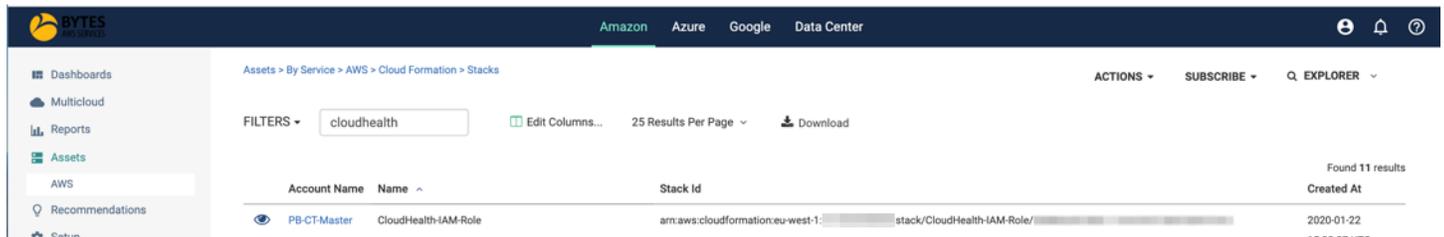
3.3 PRE-REQUISITES

Before making the change, please answer the following questions:

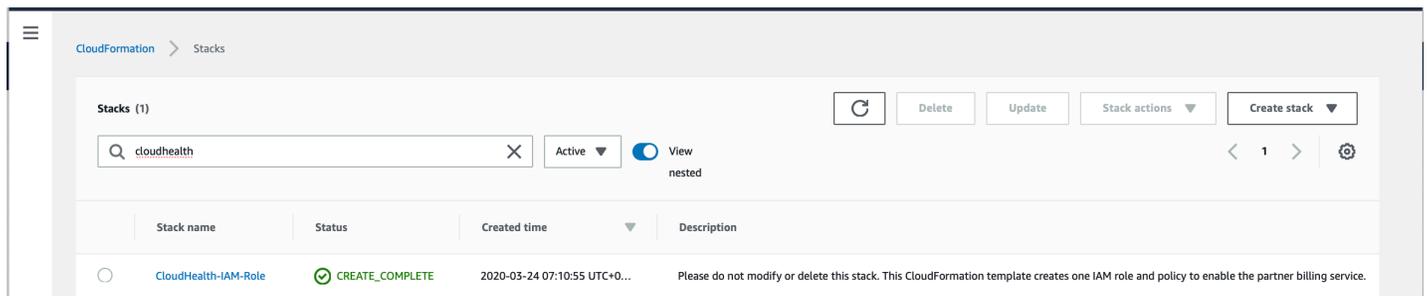
1. Was the current CloudHealth IAM role created manually or by using CloudFormation?

How to check:

- a) Log into your CloudHealth portal, go to 'Assets->AWS->CloudFormation->Stacks' and filter the list by 'cloudhealth' in order to see whether there are any CloudFormation stacks related to creating IAM roles for CloudHealth in any of your accounts.



- b) Log into the target AWS account, go to the 'CloudFormation' service and filter the list by 'cloudhealth'.
Note: Cloudformation stacks are regional so you may need to check in more than one region.



2. Is the target account a 'Standalone', 'Master/Consolidated Billing' or 'Linked' account?

How to check:

Log into the account, go to the 'AWS Organizations' service and check against the screenshots below.

Standalone accounts

Master/Consolidated accounts

| Account name | Email | Account ID | Status |
|--------------|------------|------------|--------------------|
| ★ Master | [REDACTED] | [REDACTED] | Joined on 2/20/20 |
| Audit | [REDACTED] | [REDACTED] | Created on 2/20/20 |
| Checker | [REDACTED] | [REDACTED] | Joined on 2/21/20 |

Linked accounts

Depending on the answer to question 1, please proceed to either Section 4 (CloudFormation Update Instructions) or Section 5 (Manual Update Instructions) below.

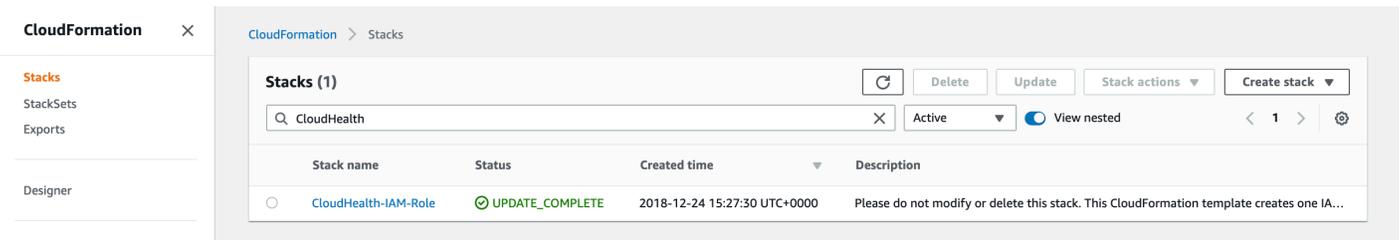
4 CLOUDFORMATION UPDATE INSTRUCTIONS

4.1 SUMMARY STEPS

- Select the existing CloudHealth CloudFormation stack
- Update it by pointing to the new provided CloudFormation template version
- Wait a few moments for the update to complete

4.2 INSTRUCTIONS

1. Log into the target AWS account
2. Go to the CloudFormation service, select the region where you ran the original template and locate the CloudHealth stack



3. Select the existing CloudFormation Stack and click 'Update'
4. On the 'Update stack' page, select the 'Replace current template' and 'Amazon S3 URL' options and paste in **ONE** of the links below into the 'Amazon S3 URL' field' and click 'Next'.

For Consolidated or Standalone accounts:

<https://s3.eu-west-2.amazonaws.com/documents.aws-bytes.co.uk/cloudhealth/CloudFormation/consolidated-account-read-only>

For Linked accounts:

<https://s3.eu-west-2.amazonaws.com/documents.aws-bytes.co.uk/cloudhealth/CloudFormation/linked-account-read-only>

CloudFormation > Stacks > CloudHealth-IAM-Role > Update stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Update stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Use current template Replace current template Edit template in designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL Upload a template file

Amazon S3 URL

Amazon S3 template URL

S3 URL: Will be generated when URL is provided

5. On the 'Specify stack details' page, click 'Next' (Note: Leave all field values if any, the same)

CloudFormation > Stacks > CloudHealth-IAM-Role > Update stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

CloudTrailBucketName
Enter the S3 bucket name where AWS CloudTrail logs are saved. If CloudTrail is not enabled, please ignore this step.

ConfigBucketName
Enter the S3 bucket name where AWS Config logs are saved. If Config is not enabled, please ignore this step.

ExternalID
If Bytes has provided a different ExternalID please overwrite this.

6. On the 'Configure stack options' page, click 'Next'

CloudFormation > Stacks > CloudHealth-IAM-Role > Update stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Configure stack options

Tags
You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. [Learn more](#)

Key Value Remove

Add tag

Permissions
Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

IAM role - optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name Sample-role-name Remove

Advanced options
You can set additional options for your stack, like notification options and a stack policy. [Learn more](#)

Stack policy
Defines the resources that you want to protect from unintentional updates during a stack update.

Rollback configuration
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. [Learn more](#)

Notification options

Cancel Previous Next

7. On the 'Review' page, select the 'I acknowledge.....' checkbox and click 'Update stack'

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Cancel Previous View change set Update stack

8. Wait for CloudFormation stack status to show 'UPDATE_COMPLETE'

CloudFormation > Stacks > CloudHealth-IAM-Role

Stacks (1) CloudHealth

Active View nested

CloudHealth-IAM-Role
2018-12-24 15:27:30 UTC+0000
UPDATE_COMPLETE

CloudHealth-IAM-Role

Delete Update Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets

Events (18)

Search events

| Timestamp | Logical ID | Status | Status reason |
|------------------------------|----------------------|-------------------------------------|---------------|
| 2020-04-05 07:48:49 UTC+0100 | CloudHealth-IAM-Role | UPDATE_COMPLETE | - |
| 2020-04-05 07:48:48 UTC+0100 | CloudHealth-IAM-Role | UPDATE_COMPLETE_CLEANUP_IN_PROGRESS | - |

5 MANUAL UPDATE INSTRUCTIONS

5.1 SUMMARY STEPS

- Select the existing CloudHealth IAM role
- Update the policy attached to it by copy/pasting the provided code
- Save the changes

5.2 INSTRUCTIONS

1. Log into the target AWS account
2. Go to the IAM service and locate the CloudHealth IAM role (Hint: It will be called something like 'role-cloudhealth', 'CH-Role', 'CHT-Role', 'CloudHealth-Role')

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Roles' highlighted. The main content area shows a search bar with 'CloudHealth' entered and a table with one result: 'role-cloudhealth'. The table columns are 'Role name', 'Trusted entities', and 'Last activity'. The 'Trusted entities' column shows 'Account: [redacted]' and the 'Last activity' column shows 'Today'.

3. Click on the role and go to the 'Permissions' tab

The screenshot shows the 'Summary' page for the 'role-cloudhealth' role in the AWS IAM console. The 'Permissions' tab is selected. It displays 'Permissions policies (1 policy applied)' with a table showing 'policy-cloudhealth' as a 'Managed policy'. There are also buttons for 'Attach policies' and 'Add inline policy'. Other tabs like 'Trust relationships', 'Tags', 'Access Advisor', and 'Revoke sessions' are visible at the top of the permissions section.

4. Click on the policy to view the details

The screenshot shows the AWS IAM console interface. On the left is a navigation menu for 'Identity and Access Management (IAM)'. The main content area is titled 'Policies > policy-cloudhealth Summary'. It displays the 'Policy ARN' as 'arn:aws:iam::[account-id]:policy/policy-cloudhealth' and the 'Description' as 'Policy giving permissions for CloudHealth to read AWS information'. Below this, there are tabs for 'Permissions', 'Policy usage', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is active, showing a 'Policy summary' and a 'JSON' button. The JSON content is partially visible, showing the 'Version' as '2012-10-17' and a list of actions including 'autoscaling:Describe*', 'aws-portal:ViewBilling', 'aws-portal:ViewUsage', 'cloudformation:ListStacks', 'cloudformation:ListStackResources', 'cloudformation:DescribeStacks', 'cloudformation:DescribeStackEvents', 'cloudformation:DescribeStackResources', and 'cloudformation:GetTemplate'.

5. Click on 'Edit policy' and select the 'JSON' tab

Edit policy-cloudhealth

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

The screenshot shows the 'Edit policy' screen in the AWS IAM console. The 'JSON' tab is selected, and the policy content is displayed in a code editor. The JSON content is as follows:

```

1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "autoscaling:Describe*",
8-         "aws-portal:ViewBilling",
9-         "aws-portal:ViewUsage",
10-        "cloudformation:ListStacks",
11-        "cloudformation:ListStackResources",
12-        "cloudformation:DescribeStacks",
13-        "cloudformation:DescribeStackEvents",
14-        "cloudformation:DescribeStackResources",
15-        "cloudformation:GetTemplate",
16-        "cloudfront:Get*",
17-        "cloudfront:List*",
18-        "cloudtrail:DescribeTrails",
19-        "cloudtrail:GetEventSelectors",
20-        "cloudtrail:ListTags",
21-        "cloudwatch:Describe*",
22-        "cloudwatch:Get*",
23-        "cloudwatch:List*",
24-        "config:Get*",
25-        "config:Describe*",
26-        "config:Deliver*",
27-        "config:List*",
28-        "cur:Describe*",
29-        "dms:Describe*",
30-        "dms:List*"

```

At the bottom of the screen, there is a 'Character count: 2,740 of 6,144.' indicator, a 'Cancel' button, and a 'Review policy' button.

6. Copy and paste the new policy code from the links below:

For Linked accounts

<https://s3.eu-west-2.amazonaws.com/documents.aws-bytes.co.uk/cloudhealth/IAM-Policies/CHT-IAM-Policy.json>

For Consolidated or Standalone accounts

IMPORTANT: ONLY COPY/PASTE THE LINES BETWEEN THE 1ST 'ACTION' AND 'RESOURCE' PARAMETERS

<https://s3.eu-west-2.amazonaws.com/documents.aws-bytes.co.uk/cloudhealth/IAM-Policies/CHT-IAM-Policy-Consolidated.json>

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:Describe*",
        "aws-portal:ViewBilling",
        "aws-portal:ViewUsage",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:ListTags",
        "cloudwatch:Describe*"
      ]
    }
  ]
}
```

```
.....
.....
  "sdb:List*",
  "ses:Get*",
  "ses:List*",
  "sns:Get*",
  "sns:List*",
  "sqs:GetQueueAttributes",
  "sqs:ListQueues",
  "storagegateway:List*",
  "storagegateway:Describe*",
  "workspaces:Describe*"
],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:Get*",
    "s3:List*"
  ],
  "Resource": [
    "arn:aws:s3:::M-DBBucket"
  ]
}
```

7. Click 'Review policy'

Edit policy-cloudhealth

1 2

Review policy

Review this policy before you save your changes.

Save as default

Summary

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining**. [Learn more](#)

| Service | Access level | Resource | Request condition |
|---|----------------------------|---------------|-------------------|
| Allow (38 of 226 services) Show remaining 188 | | | |
| Billing | Limited: Read | All resources | None |
| CloudFormation | Limited: List, Read | All resources | None |
| CloudFront | Full: List, Read | All resources | None |
| CloudTrail | Limited: Read | All resources | None |
| CloudWatch | Full: List, Read | All resources | None |
| CloudWatch Logs | Limited: List | All resources | None |
| Config | Full: List Limited: Read | All resources | None |
| Cost and Usage Report | Full: Read | All resources | None |
| DMS | Full: List Limited: Read | All resources | None |
| DynamoDB | Full: List Limited: Read | All resources | None |
| EC2 | Limited: List, Read, Write | All resources | None |
| EC2 Auto Scaling | Full: List, Read | All resources | None |
| EFS | Full: List Limited: Read | All resources | None |
| Elastic Beanstalk | Full: List Limited: Read | All resources | None |
| Elastic Container Service | Full: List, Read | All resources | None |

* Required

Cancel

Previous

Save changes

8. Click 'Save changes'

9. If you receive a message saying that you've reached the maximum number of saved versions, select 'Remove oldest non-default version' and click 'Delete version and save'.

This policy already has the maximum of 5 saved versions: ✕

Remove oldest non-default policy version (version v1 - created 510 days ago)

Select policy versions to remove

Cancel Delete version and save