

Cross-Account Cross-Region CloudWatch Console

PDF ([acw-ug.pdf#Cross-Account-Cross-Region](#))

Kindle (<https://www.amazon.com/dp/B07643SJ8F>)

RSS ([amazon-cloudwatch-document-history.rss](#))

You can add *cross-account* functionality to your CloudWatch console. This functionality provides you with cross-account visibility to your dashboards, alarms, metrics, and automatic dashboards without having to log in and log out of different accounts.

You can then create dashboards that summarize CloudWatch data from multiple AWS accounts and multiple AWS Regions into a single dashboard.

Many organizations have their AWS resources deployed in multiple accounts, to provide billing and security boundaries. In this case, we recommend that you designate one or more of your accounts as your monitoring accounts, and build your cross-account dashboards in these accounts.

Cross-account functionality is integrated with AWS Organizations, to help you efficiently build your cross-account dashboards.

Cross-Region Functionality

Cross-Region functionality is now built-in automatically. You do not need to take any extra steps to be able to display metrics from different Regions in a single account on the same graph or the same dashboard.

Topics

- [Enabling Cross-Account Functionality in CloudWatch \(#enable-cross-account-cross-Region\)](#)
- [\(Optional\) Integrate With AWS Organizations \(#cross-account-and-AWS-organizations\)](#)
- [Troubleshooting Your CloudWatch Cross-Account Setup \(#troubleshooting-cross-account-cross-Region\)](#)
- [Disabling and cleaning up after using cross-account \(#cleanup-cross-account-cross-Region\)](#)


Enabling Cross-Account Functionality in CloudWatch

To set up cross-account functionality in your CloudWatch console, use the AWS Management Console to set up your sharing accounts and monitoring accounts.

Set Up A Sharing Account

You must enable sharing in each account that will make data available to the monitoring account.

To enable your account to share CloudWatch data with other accounts

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>  (<https://console.aws.amazon.com/cloudwatch/>) .
2. In the navigation pane, choose **Settings**, then choose **Configure**.
3. Choose **Share data**.
4. For **Sharing**, choose **Specific accounts** and enter the IDs of the accounts that you want to share data with.

Any accounts that you specify here can view your account's CloudWatch data. Specify the IDs only of accounts that you know and trust.

5. For **Permissions**, specify how to share your data with one of the following options:

- **Provide read-only access to your CloudWatch metrics, dashboards, and alarms.** This option enables the monitoring accounts to create cross-account dashboards that include widgets that contain CloudWatch data from your account.
- **Include CloudWatch automatic dashboards.** If you select this option, users in the monitoring account can also view the information in this account's automatic dashboards. For more information, see [Getting Started with Amazon CloudWatch \(./GettingStarted.html\)](#).
- **Include X-Ray read-only access for ServiceLens.** If you select this option, users in the monitoring account can also view the ServiceLens service map and X-Ray trace information in this account. For more information, see [Using ServiceLens to Monitor the Health of Your Applications \(./ServiceLens.html\)](#).
- **Full read-only access to everything in your account.** This option enables the accounts that you use for sharing to create cross-account dashboards that include widgets that contain CloudWatch data from your account. It also enables those accounts to look deeper into your account and view your account's data in the consoles of other AWS services.

6. Choose **Launch CloudFormation template**.


In the confirmation screen, type **Confirm**, and choose **Launch template**.

7. Select the **I acknowledge...** check box, and choose **Create stack**.

Sharing With an Entire Organization

Completing the preceding procedure creates an IAM role which enables your account to share data with one account. You can create or edit an IAM role that shares your data with all accounts in an organization. Do this only if you know and trust all accounts in the organization.

To share your CloudWatch account data with all accounts in an organization

1. If you haven't already, complete the preceding procedure to share your data with one AWS account.
2. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>  (<https://console.aws.amazon.com/iam/>).
3. In the navigation pane, choose **Roles**.
4. In the list of roles, choose **CloudWatch-CrossAccountSharingRole**.
5. Choose **Trust relationships**, **Edit trust relationship**.

You see a policy like this:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    }
  ]
}
```

```

    },
    "Action": "sts:AssumeRole"
  }
]
}

```

6. Change the policy to the following, replacing `org-id` with the ID of your organization.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "org-id"
        }
      }
    }
  ]
}

```


7. Choose **Update Trust Policy**.

Set Up a Monitoring Account

Enable each monitoring account if you want to view cross-account CloudWatch data.

When you complete the following procedure, CloudWatch creates a service-linked role that CloudWatch uses in the monitoring account to access data shared from your other accounts. This service-linked role is called **AWSServiceRoleForCloudWatchCrossAccount**. For more information, see [Using Service-Linked Roles for CloudWatch \(./using-service-linked-roles.html\)](#).

To enable your account to view cross-account CloudWatch data

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>  (<https://console.aws.amazon.com/cloudwatch/>).
2. In the navigation pane, choose **Settings**, then choose **Configure**.
3. Under **View cross-account cross-region**, choose one of the following options:
 - **Account Id Input**. This option prompts you to manually input an account ID each time that you want to switch accounts when you view cross-account data.

- **AWS Organization account selector.** This option causes the accounts that you specified when you completed your cross-account integration with Organizations to appear. When you next use the console, CloudWatch displays a dropdown list of these accounts for you to select from when you are viewing cross-account data.

To do this, you must have first used your organization management account to allow CloudWatch to see a list of accounts in your organization. For more information, see [\(Optional\) Integrate With AWS Organizations \(#cross-account-and-AWS-organizations\)](#) .

- **Custom account selector.** This option prompts you to enter a list of account IDs. When you next use the console, CloudWatch displays a dropdown list of these accounts for you to select from when you are viewing cross-account data.

You can also enter a label for each of these accounts to help you identify them when choosing accounts to view.

The account selector settings that a user makes here are retained only for that user, not for all other users in the monitoring account.


4. Choose **Enable**.

After you complete this setup, you can create cross-account dashboards. For more information, see [Cross-Account Cross-Region Dashboards \(./cloudwatch_xaxr_dashboard.html\)](#) .

(Optional) Integrate With AWS Organizations

If you want to integrate cross-account functionality with AWS Organizations, you must make a list of all accounts in the organization available to the monitoring accounts.

To enable cross-account CloudWatch functionality to access a list of all accounts in your organization

1. Log in to your organization's management account.
2. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>  (<https://console.aws.amazon.com/cloudwatch/>) .
3. In the navigation pane, choose **Settings**, then choose **Configure**.
4. For **Grant permission to view the list of accounts in the organization**, choose **Specific accounts** to be prompted to enter a list of account IDs. The list of accounts in your organization are shared with only the accounts that you specify here.
5. Choose **Share organization account list**.
6. Choose **Launch CloudFormation template**.

In the confirmation screen, type **Confirm**, and choose **Launch template**.

Troubleshooting Your CloudWatch Cross-Account Setup


This section contains troubleshooting tips for cross-account, console deployment in CloudWatch.

I am getting access denied errors displaying cross-account data

Check the following:

- Your monitoring account should have a role named **AWSServiceRoleForCloudWatchCrossAccount**. If it does not, you need to create this role. For more information, see [Set Up a Monitoring Account \(#setup_monitoring_account\)](#) .
- Each sharing account should have a role named **CloudWatch-CrossAccountSharingRole**. If it does not, you need to create this role. For more information, see [Set Up A Sharing Account \(#setup_sharing_account\)](#) .
- The sharing role must trust the monitoring account.

To confirm that your roles are set up properly for the CloudWatch cross-account console

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>  (<https://console.aws.amazon.com/iam/>) .
2. In the navigation pane, choose **Roles**.
3. In the list of roles, make sure the needed role exists. In a sharing account, look for **CloudWatch-CrossAccountSharingRole**. In a monitoring account, look for **AWSServiceRoleForCloudWatchCrossAccount**.
4. If you are in a sharing account and **CloudWatch-CrossAccountSharingRole** already exists, choose **CloudWatch-CrossAccountSharingRole**.
5. Choose **Trust relationships**, **Edit trust relationship**.
6. Confirm that the policy lists either the account ID of the monitoring account, or the organization ID of an organization that contains the monitoring account.

I don't see an account drop-down in the console

First, check that you have created the correct IAM roles, as discussed in the preceding troubleshooting section. If those are set up correctly, make sure that you have enabled this account to view cross-account data, as described in [Enable Your Account to View Cross-Account Data \(#view_cross_account\)](#) .

Disabling and cleaning up after using cross-account

To disable cross-account functionality for CloudWatch, follow these steps.

Step 1: Remove the cross-account stacks or roles

The best method is to remove the AWS CloudFormation stacks that were used to enable cross-account functionality.

- In each of the sharing accounts, remove the **CloudWatch-CrossAccountSharingRole** stack.
- If you used AWS Organizations to enable cross-account functionality with all accounts in an organization, remove the **CloudWatch-CrossAccountListAccountsRole** stack in the organization's management account.

If you didn't use the AWS CloudFormation stacks to enable cross-account functionality, do the following:

- In each of the sharing accounts, delete the **CloudWatch-CrossAccountSharingRole** IAM role.
- If you used AWS Organizations to enable cross-account functionality with all accounts in an organization, delete the **CloudWatch-CrossAccountSharing-ListAccountsRole** IAM role in the organization's management account.

Step 2: Remove the service-linked role

In the monitoring account, delete the **AWSServiceRoleForCloudWatchCrossAccount** service-linked IAM role.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.